Contents

Preface 8

1 Chapter 1 11

Complex Numbers 11
1.0.1 Roadmap . . . 13
1.0.2 Named moves . . . 13

1.1 The Complex Numbers as Pairs of Reals 14
1.1.1 Building the new numbers . . . 14
1.1.2 The real numbers inside the complex numbers . . . 15
1.1.3 The laws of arithmetic . . . 18
1.1.4 Powers and a factorization . . . 19
1.1.5 Exercises . . . 22
1.1.5.1 A. Check your understanding . . . 22
1.1.5.2 B. Practice . . . 22
1.1.5.3 C. Going deeper . . . 24

1.2 Conjugate, Modulus, and Division 25
1.2.1 Conjugate and modulus . . . 26
1.2.2 Rules for conjugate and modulus . . . 27
1.2.3 Division . . . 29
1.2.4 Exercises . . . 31
1.2.4.1 A. Check your understanding . . . 31
1.2.4.2 B. Practice . . . 32
1.2.4.3 C. Going deeper . . . 33

1.3 The Triangle Inequality 34
1.3.1 Why the old proof does not transfer . . . 34
1.3.2 The real part is at most the modulus . . . 35
1.3.3 The triangle inequality . . . 36
1.3.4 Three variants . . . 38
1.3.5 Exercises . . . 39
1.3.5.1 A. Check your understanding . . . 39
1.3.5.2 B. Practice . . . 40
1.3.5.3 C. Going deeper . . . 41

1.4 Square Roots, Quadratic Equations, and the Missing Order 43
1.4.1 Square roots from real square roots . . . 43
1.4.2 The quadratic formula . . . 46
1.4.3 No order on the complex numbers . . . 47
1.4.4 The square-root rule does not survive . . . 48

1.4.5 Exercises . . . 48
1.4.5.1 A. Check your understanding . . . 48
1.4.5.2 B. Practice . . . 49
1.4.5.3 C. Going deeper . . . 50

1.5 The Unit Circle and Polar Form 52
1.5.1 Length and direction . . . 52
1.5.2 What this volume borrows about cosine and sine . . . 54
1.5.3 Polar form . . . 55
1.5.4 Powers . . . 58
1.5.5 Exercises . . . 60
1.5.5.1 A. Check your understanding . . . 60
1.5.5.2 B. Practice . . . 61
1.5.5.3 C. Going deeper . . . 62

1.6 Higher Roots, Roots of Unity, and a Look Ahead 64
1.6.1 Real n-th roots . . . 64
1.6.2 Solving the equation z to the n equals c . . . 66
1.6.3 Roots of unity . . . 68
1.6.4 Polynomial equations, and a look ahead . . . 70
1.6.5 Exercises . . . 71
1.6.5.1 A. Check your understanding . . . 71
1.6.5.2 B. Practice . . . 72
1.6.5.3 C. Going deeper . . . 73
1.6.5.4 R. Review . . . 74

2 Chapter 2 77

Fields 77
2.0.1 Roadmap . . . 79
2.0.2 Named moves . . . 80

2.1 The Field Axioms and the First Examples 81
2.1.1 What solving equations needs . . . 81
2.1.2 The definition . . . 81
2.1.3 Rules that hold in every field . . . 83
2.1.4 Solving linear equations in a field . . . 86
2.1.5 Examples . . . 87
2.1.6 Non-examples . . . 88
2.1.7 Why these axioms . . . 89
2.1.8 Exercises . . . 89
2.1.8.1 A. Check your understanding . . . 89
2.1.8.2 B. Practice . . . 90
2.1.8.3 C. Going deeper . . . 92

2.2 Finite Fields from Modular Arithmetic 93
2.2.1 Arithmetic modulo n, recalled . . . 93
2.2.2 Which moduli give fields . . . 94
2.2.3 The fields with p elements . . . 95
2.2.4 Exercises . . . 98
2.2.4.1 A. Check your understanding . . . 98
2.2.4.2 B. Practice . . . 98

2.2.4.3 C. Going deeper . . . 99

2.3 Subfields 102
2.3.1 Fields inside fields . . . 102
2.3.2 The subfield test . . . 103
2.3.3 Square roots of two and of minus one . . . 105
2.3.4 The smallest subfield . . . 107
2.3.5 Exercises . . . 108
2.3.5.1 A. Check your understanding . . . 108
2.3.5.2 B. Practice . . . 109
2.3.5.3 C. Going deeper . . . 111

2.4 Field Homomorphisms 112
2.4.1 Maps that respect both operations . . . 113
2.4.2 What a homomorphism must do . . . 114
2.4.3 Examples, and pairs of fields with no map between them . . . 116
2.4.4 Exercises . . . 117
2.4.4.1 A. Check your understanding . . . 117
2.4.4.2 B. Practice . . . 118
2.4.4.3 C. Going deeper . . . 120

2.5 Integer Multiples, the Characteristic, and the Prime Subfield 121
2.5.1 Integer multiples . . . 121
2.5.2 The characteristic . . . 124
2.5.3 The characteristic under subfields and homomorphisms . . . 127
2.5.4 The prime subfield . . . 129
2.5.5 Exercises . . . 133
2.5.5.1 A. Check your understanding . . . 133
2.5.5.2 B. Practice . . . 134
2.5.5.3 C. Going deeper . . . 136

2.6 The Binomial Theorem, the Frobenius Map, and Fermat's Little Theorem 138
2.6.1 Sums and powers in a commutative ring . . . 138
2.6.2 Binomial coefficients . . . 140
2.6.3 The binomial theorem . . . 142
2.6.4 The Frobenius map . . . 144
2.6.5 Fermat's little theorem . . . 145
2.6.6 Exercises . . . 147
2.6.6.1 A. Check your understanding . . . 147
2.6.6.2 B. Practice . . . 147
2.6.6.3 C. Going deeper . . . 148
2.6.6.4 R. Review . . . 150

3 Chapter 3 153

Groups, Subgroups, and Homomorphisms 153
3.0.1 Roadmap . . . 155
3.0.2 Named moves . . . 156

3.1 Groups 157
3.1.1 Four situations side by side . . . 157

3.1.2 The basic laws, proved once . . . 160
3.1.3 Products of many factors . . . 161
3.1.4 Integer powers . . . 163
3.1.5 The units of a commutative ring form a group . . . 166
3.1.6 Exercises . . . 167
3.1.6.1 A. Check your understanding . . . 167
3.1.6.2 B. Practice . . . 168
3.1.6.3 C. Going deeper . . . 169

3.2 Subgroups and the Subgroups of the Integers 171
3.2.1 Subgroups . . . 171
3.2.2 The subgroup generated by one element . . . 174
3.2.3 The subgroups of the integers . . . 175
3.2.4 Exercises . . . 177
3.2.4.1 A. Check your understanding . . . 177
3.2.4.2 B. Practice . . . 177
3.2.4.3 C. Going deeper . . . 179

3.3 Homomorphisms and Isomorphisms 182
3.3.1 Maps that respect the operation . . . 182
3.3.2 Basic properties of homomorphisms . . . 185
3.3.3 Isomorphic and non-isomorphic groups . . . 188
3.3.4 Exercises . . . 190
3.3.4.1 A. Check your understanding . . . 190
3.3.4.2 B. Practice . . . 191
3.3.4.3 C. Going deeper . . . 192

3.4 Permutations and Cycle Notation 194
3.4.1 Permutations and two-line notation . . . 194
3.4.2 Cycles . . . 195
3.4.3 Counting permutations . . . 197
3.4.4 Disjoint cycles and the decomposition theorem . . . 199
3.4.5 Exercises . . . 202
3.4.5.1 A. Check your understanding . . . 202
3.4.5.2 B. Practice . . . 203
3.4.5.3 C. Going deeper . . . 205

3.5 Transpositions Generate the Symmetric Group 206
3.5.1 Cycles as products of transpositions . . . 207
3.5.2 Every permutation is a product of transpositions . . . 208
3.5.3 The word is not unique . . . 210
3.5.4 Adjacent transpositions . . . 211
3.5.5 Exercises . . . 212
3.5.5.1 A. Check your understanding . . . 212
3.5.5.2 B. Practice . . . 213
3.5.5.3 C. Going deeper . . . 214
3.5.5.4 R. Review . . . 217

4 Chapter 4 220

Formal Polynomials 220
4.0.1 Roadmap . . . 221

4.0.2 Named moves . . . 222

4.1 Polynomials as Coefficient Sequences 223
4.1.1 What goes wrong with "an expression in x" . . . 223
4.1.2 Polynomials over a commutative ring . . . 223
4.1.3 Sums, powers and multiples . . . 226
4.1.4 Exercises . . . 228
4.1.4.1 A. Check your understanding . . . 228
4.1.4.2 B. Practice . . . 229
4.1.4.3 C. Going deeper . . . 230

4.2 The Polynomial Ring 231
4.2.1 Adding and multiplying coefficient sequences . . . 231
4.2.2 Monomials do the work . . . 233
4.2.3 The ring laws . . . 235
4.2.4 Exercises . . . 238
4.2.4.1 A. Check your understanding . . . 238
4.2.4.2 B. Practice . . . 239
4.2.4.3 C. Going deeper . . . 240

4.3 Degree, Leading Coefficients, and Integral Domains 242
4.3.1 Degree and leading coefficient . . . 242
4.3.2 The degree of a sum . . . 244
4.3.3 The degree of a product . . . 245
4.3.4 Integral domains . . . 246
4.3.5 Units of a polynomial ring . . . 248
4.3.6 Polynomials of bounded degree . . . 249
4.3.7 Exercises . . . 250
4.3.7.1 A. Check your understanding . . . 250
4.3.7.2 B. Practice . . . 251
4.3.7.3 C. Going deeper . . . 253

4.4 Evaluation, Substitution, and Polynomial Functions 254
4.4.1 Evaluating a polynomial . . . 255
4.4.2 Evaluation respects the operations . . . 256
4.4.3 Ring homomorphisms . . . 257
4.4.4 The substitution principle . . . 258
4.4.5 Changing coefficients and composing . . . 260
4.4.6 Polynomials and polynomial functions . . . 262
4.4.7 Exercises . . . 264
4.4.7.1 A. Check your understanding . . . 264
4.4.7.2 B. Practice . . . 265
4.4.7.3 C. Going deeper . . . 266

4.5 The Formal Derivative 270
4.5.1 The derivative by coefficients . . . 271
4.5.2 The rules of differentiation . . . 273
4.5.3 When the derivative vanishes . . . 276
4.5.4 Exercises . . . 278
4.5.4.1 A. Check your understanding . . . 278
4.5.4.2 B. Practice . . . 278
4.5.4.3 C. Going deeper . . . 280

4.5.4.4 R. Review . . . 282

5 Chapter 5 **286**

Polynomials over a Field **286**
5.0.1 Roadmap . . . 289
5.0.2 Named moves . . . 289

5.1 Division with Remainder **290**
5.1.1 Divisibility over a field . . . 291
5.1.2 Division with remainder . . . 293
5.1.3 Roots and factors of degree one . . . 296
5.1.4 Exercises . . . 297
5.1.4.1 A. Check your understanding . . . 297
5.1.4.2 B. Practice . . . 298
5.1.4.3 C. Going deeper . . . 299

5.2 Ideals, the Greatest Common Divisor, and the Euclidean Algorithm **301**
5.2.1 The ideal generated by finitely many polynomials . . . 301
5.2.2 Every ideal has one generator . . . 303
5.2.3 The greatest common divisor . . . 304
5.2.4 The Euclidean algorithm . . . 306
5.2.5 Changing the field . . . 309
5.2.6 Exercises . . . 311
5.2.6.1 A. Check your understanding . . . 311
5.2.6.2 B. Practice . . . 312
5.2.6.3 C. Going deeper . . . 313

5.3 Irreducible Polynomials and Unique Factorization **315**
5.3.1 Irreducible polynomials . . . 316
5.3.2 Euclid's lemma for polynomials . . . 317
5.3.3 Factors that cannot be split further . . . 319
5.3.4 Unique factorization . . . 320
5.3.5 Rational roots . . . 323
5.3.6 Exercises . . . 325
5.3.6.1 A. Check your understanding . . . 325
5.3.6.2 B. Practice . . . 326
5.3.6.3 C. Going deeper . . . 327

5.4 Roots, Multiplicity, and the Formal Derivative **331**
5.4.1 Counting roots . . . 331
5.4.2 Values determine the polynomial . . . 332
5.4.3 Re-centering at a point . . . 334
5.4.4 Multiplicity . . . 335
5.4.5 Repeated roots and the derivative . . . 339
5.4.6 Exercises . . . 341
5.4.6.1 A. Check your understanding . . . 341
5.4.6.2 B. Practice . . . 342
5.4.6.3 C. Going deeper . . . 344

5.5 Interpolation, Quotient Rings, and the Chinese Remainder Theorem **345**
5.5.1 Polynomials through given points . . . 345

5.5.2 Congruence modulo a polynomial . . . 348
5.5.3 The ring of classes modulo a polynomial . . . 349
5.5.4 The Chinese remainder theorem for polynomials . . . 353
5.5.5 Exercises . . . 358
5.5.5.1 A. Check your understanding . . . 358
5.5.5.2 B. Practice . . . 359
5.5.5.3 C. Going deeper . . . 361

5.6 The Fundamental Theorem of Algebra 362
5.6.1 Two estimates . . . 362
5.6.2 The smallest value of the modulus is attained . . . 364
5.6.3 A direction in which the modulus decreases . . . 367
5.6.4 The theorem, and complex polynomials . . . 370
5.6.5 Real polynomials . . . 372
5.6.6 Exercises . . . 375
5.6.6.1 A. Check your understanding . . . 375
5.6.6.2 B. Practice . . . 376
5.6.6.3 C. Going deeper . . . 377
5.6.6.4 R. Review . . . 380

Preface

Number Systems: From $\mathbb{N}$ *to* $\mathbb{R}$ ended with the real numbers as a complete ordered field, and with the integers modulo n as a commutative ring. This volume takes those two results and builds the algebra that linear algebra and the algebra volumes assume on their first page. It constructs the complex numbers, studies fields as objects of their own, introduces groups through permutations, makes polynomials into formal objects, and proves that polynomials over a field have the arithmetic of the integers. It ends with the Fundamental Theorem of Algebra: every non-constant complex polynomial has a root.

Who it is for. The reader we have in mind has worked through *Logic and Proof*, *Sets, Relations, and Cardinality* and the main line of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, or has their habits from elsewhere. That means running an induction, checking that an operation on classes is well defined, and proving a statement about every element of a ring from the ring axioms alone. The chapters point back to those volumes wherever they use a definition or a result, with a link, so a reader who is unsure of a step can look it up. Much of the material is familiar in outline from school or from a first linear algebra course; what is new is that every rule is proved, and that nothing is used before it is proved.

What it covers.

Chapter	Title	What it does
1	Complex Numbers	$\mathbb{C}$ as pairs of real numbers, proved a field containing $\mathbb{R}$; conjugate, modulus and the triangle inequality; square roots and the quadratic formula; why $\mathbb{C}$ has no order; polar form, De Moivre's formula and the roots of unity
2	Fields	The field axioms and their consequences; the finite fields $\mathbb{F}_p$; subfields and the subfield test; field homomorphisms; the characteristic and the prime subfield; the binomial theorem, the Frobenius map and Fermat's little theorem

Chapter	Title	What it does
3	Groups, Subgroups, and Homomorphisms	Groups, products of many factors and integer powers; subgroups and the subgroups of $\mathbb{Z}$; homomorphisms, kernels and isomorphisms; permutations, cycle notation and the disjoint cycle decomposition; transpositions generate the symmetric group
4	Formal Polynomials	A polynomial as a sequence of coefficients; the ring $R[x]$ over a commutative ring; degree and integral domains; evaluation and substitution as ring homomorphisms, and why a polynomial is not its function; the formal derivative
5	Polynomials over a Field	Division with remainder, the greatest common divisor and the Euclidean algorithm in $F[x]$; irreducible polynomials and unique factorization; roots, multiplicity and repeated roots; interpolation, the rings $F[x]/\langle m\rangle$ and the Chinese remainder theorem; the Fundamental Theorem of Algebra and the factorization of real polynomials

Chapter 1 gives the volume its most important example, and Chapter 2 names what that example has in common with $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{Z}/p\mathbb{Z}$. Chapter 3 uses Chapters 1 and 2 only in examples, remarks and one review exercise. Chapters 4 and 5 form a pair. Chapter 4 builds polynomials over any commutative ring and asks only what can be done without dividing; Chapter 5 takes the coefficients in a field and runs again, with the degree in place of size, the arithmetic that *Number Systems*, Chapter 3 ran in $\mathbb{Z}$.

How to read it. Read the chapters in order; each uses the ones before it. Every section has Quick checks with folded answers; answer each one before you unfold it. The exercises of a section come in three groups, A to check understanding, B for practice and C to go deeper, and the last section of each chapter adds R items that reach back to earlier chapters. A chapter's opening page lists what it needs, with links, and the time it takes. Second-reading folds hold edge cases and longer justifications. They can stay closed on a first reading, but they are not optional, since later proofs may use what they contain.

One borrowed fact. This volume does not define cosine, sine or π: defining them needs limits and power series, which belong to analysis. Section 1.5 states five facts about them, numbered (T1)–(T5), as an assumption, and *Analysis on the Real Line*, Chapter 10 proves them. They

are used only for polar form and for the roots of complex numbers in Sections 1.5 and 1.6, and each proof that uses one names it. Nothing else in the volume depends on *Analysis on the Real Line*. In particular, Chapter 5 proves the Fundamental Theorem of Algebra from the square roots of Section 1.4 and the completeness of $\mathbb{R}$ alone, without the borrowed facts.

Time. The chapter openings add up to about 130 hours on the core track and about 190 hours for everything.

What comes next. The linear algebra volumes, beginning with *Spaces and Maps*, take their scalars from a field and use the complex numbers, polynomials and their roots throughout: Chapter 2's fields and subfields, Chapter 4's evaluation of a polynomial, Chapter 5's division with remainder and the Fundamental Theorem of Algebra, and Chapter 3's permutations, which *Determinants and the Structure of Operators* needs for the determinant. The algebra volumes start where this one stops. *Groups* continues Chapter 3 with cyclic groups, the sign of a permutation, cosets and Lagrange's theorem; *Rings and Fields* continues Chapters 2, 4 and 5 with fraction fields, polynomials over the integers, Gauss's lemma and field extensions. Many of their first definitions are the ones proved here, under the same names.

Chapter 1

Complex Numbers

No real number squares to -1: in an ordered field a non-zero square is positive (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)), so $x^2 + 1 = 0$ has no solution in $\mathbb{R}$. The usual remedy, "invent a symbol i with $i^2 = -1$", leaves open why such a symbol is safe when "a number z with $0 \cdot z = 1$" is not. This chapter does not invent anything. It takes pairs of real numbers, objects the reader already trusts, adds them coordinate by coordinate, and multiplies them by the one formula that $i^2 = -1$ would force. Then it checks, law by law, that nothing breaks: the complex numbers $\mathbb{C}$ form a field in the sense of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2, and they contain $\mathbb{R}$ as the pairs $(a, 0)$. Every later volume that computes with complex numbers, from inner products in linear algebra to roots of unity in algebra, starts from this field.

Two habits of $\mathbb{R}$ do not survive the passage. No order on $\mathbb{C}$ is compatible with its arithmetic, and no choice of "the" square root of each complex number keeps the rule $\sqrt{x}\sqrt{y} = \sqrt{xy}$. One new habit takes the place of order: measure a complex number by its modulus, a non-negative real, and compute with $|u|^2 = u\overline{u}$, which is algebra. The first four sections need nothing but the real numbers, and they reach far: division, the triangle inequality, and square roots and the quadratic formula without a single angle. The picture of multiplication as a turn and a stretch does need angles, and angles need cosine and sine, which belong to analysis. The chapter borrows exactly five facts about them, says so in one place, and derives everything else from those five: the familiar special values, De Moivre's formula, the n different n-th roots of every non-zero complex number, and the roots of unity. It ends with a look ahead at the Fundamental Theorem of Algebra, which Chapter 5 proves without the borrowed facts.

What you need. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$ above all, and in it chiefly Chapters 2, 4 and 6. From its Chapter 5: the real numbers as a complete ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3, Number Systems: From \(\nN\) to \(\nR\), Definition 5.6.1), the standing setting of the whole chapter. From its Chapter 6: square roots of non-negative reals, existing and unique (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), which define the modulus in Section 1.2 and build complex square roots in Section 1.4; the uniqueness of the complete ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 6.3.1), which lets Section 1.5 carry the borrowed facts over to our $\mathbb{R}$; the automorphism theorem (Number Systems: From \(\nN\) to \(\nR\), Theorem 6.3.4), used in the solution of review exercise R1 and compared there with the two such maps of $\mathbb{C}$; and the cube roots of its Exercise B2 of Section 6.2 (Number Systems: From \(\nN\) to \(\nR\), Exercise (B2: Cube roots)), whose method Section 1.6 runs for every exponent. From its Chapter 2: the axioms of a field and of an ordered field and their rules (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1, Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5), used on nearly every page; the finite ring that cannot be ordered

(Number Systems: From \(\nN\) to \(\nR\), Example (A field with two elements that cannot be ordered)), compared with in Section 1.4; and the gap at $\sqrt{2}$ in $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1), which shows in Section 1.2 why the modulus needs completeness. From its Chapter 4: the rules for fractions in a field (Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1), the absolute value of an ordered field (Number Systems: From \(\nN\) to \(\nR\), Definition 4.1.1, Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3), which the modulus extends and whose triangle inequality Section 1.3 reproves by a new route, and the natural numbers and powers in an ordered field (Number Systems: From \(\nN\) to \(\nR\), Definition 4.2.1); a remark of Section 1.4 recalls its exercise on fields with a square root of -1 (Number Systems: From \(\nN\) to \(\nR\), Exercise (C1: A field that cannot be ordered)). From its Chapter 3: division with remainder, divisibility and parity in $\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1, Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3), in Exercise B1 of Section 1.1 and in Sections 1.5 and 1.6; and the rings $\mathbb{Z}/n\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3), in a remark and Exercise C2 of Section 1.4 and in review exercise R2. From its Chapter 1: the citing rule by which induction and recursion apply to $\mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3), and the laws of powers in $\mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 1.6.4), compared with in Section 1.1. From *Sets, Relations, and Cardinality*: ordered pairs, Cartesian products and injective maps, Chapter 1 (Sets, Relations, and Cardinality, Definition 1.3.1, Sets, Relations, and Cardinality, Definition 1.3.2, Sets, Relations, and Cardinality, Definition 1.4.3); divisibility, Section 2.2 (Sets, Relations, and Cardinality, Definition 2.2.1); the recursion theorem, powers and finite sums, Section 2.3 (Sets, Relations, and Cardinality, Theorem 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.2, Sets, Relations, and Cardinality, Proposition 2.3.4, Sets, Relations, and Cardinality, Definition 2.3.1), whose recursions Section 1.1 reuses in any commutative ring; and finite sets, Section 3.1 (Sets, Relations, and Cardinality, Definition 3.1.2), for counting n-th roots. From *Logic and Proof*: induction, Chapter 3 (Logic and Proof, Axiom 4.2.1); the contrapositive, Chapter 2 (Logic and Proof, Proposition 2.3.2), in Exercise B3 of Section 1.1; and the catalogue of what a proof may not do, Chapter 5 (Logic and Proof, Example (What is not allowed)), in the proof-ordering and find-the-error exercises of Sections 1.4 and 1.6. Section 1.4 also proves the complex square roots that *Logic and Proof*, Section 4.11 took as a school fact. Nothing from linear algebra is used, and nothing from analysis before the box of borrowed facts in Section 1.5.

Which real numbers. The chapter builds $\mathbb{C}$ on the real numbers of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 5, whose elements are classes of Cauchy sequences of rationals (Number Systems: From \(\nN\) to \(\nR\), Definition 5.2.1). No proof looks inside a real number: every step uses only that $\mathbb{R}$ is a complete ordered field. By the uniqueness theorem of that volume's Chapter 6 (Number Systems: From \(\nN\) to \(\nR\), Theorem 6.3.1), any complete ordered field would give the same $\mathbb{C}$, up to the one isomorphism between the two fields.

What this chapter borrows. Everything in Sections 1.1–1.4, and in Section 1.5 up to its box of borrowed facts, is proved from the real numbers. From that box on, five facts (T1)–(T5) about cos, sin and π are used without proof: the circle identity, the addition formulas, where the cosine equals 1, that every point of the unit circle is reached, and the sign of the sine on the first half turn. *Analysis on the Real Line*, Chapter 10 defines the two functions and the number and proves the five facts. No other fact about cosine and sine is used, and the results that rest on the five say so in their dependency ledgers.

Time. About 25 hours on the core track (all of A, one B and one C per section, the exit checks); about 35 hours for everything.

1.0.1 Roadmap

- **The Complex Numbers as Pairs of Reals.** $\mathbb{C}$ defined as $\mathbb{R} \times \mathbb{R}$ with the product that $i^2 = -1$ would force; the real numbers inside $\mathbb{C}$ as the pairs $(a, 0)$, which makes $a + bi$ honest notation and $i^2 = -1$ a computation; a product with one sign changed, which has zero divisors; the laws of arithmetic, which make $\mathbb{C}$ a commutative ring with $1 \neq 0$; powers and their laws in any commutative ring; and the factorization of $z^n - w^n$.
- **Conjugate, Modulus, and Division.** The conjugate and the modulus, a non-negative real square root and the place where the completeness of $\mathbb{R}$ enters; the modulus as an extension of the absolute value of $\mathbb{R}$; the rules for conjugate and modulus, with $|zw| = |z||w|$ proved by squaring; the inverse $\overline{z}/|z|^2$ of a non-zero z; the theorem that $\mathbb{C}$ is a field in which $\mathbb{R}$ is closed under the field operations; and division by the conjugate of the denominator.
- **The Triangle Inequality.** Why the trapping proof for ordered fields cannot run in $\mathbb{C}$; comparing squares of non-negative reals; real and imaginary parts at most the modulus; the triangle inequality, by expanding $|z+w|^2$ and recognizing the cross term as a real part; and three variants: the reverse inequality, the inequality for n terms, and a lower bound for the modulus of a sum.
- **Square Roots, Quadratic Equations, and the Missing Order.** An explicit formula for a square root of a complex number, built from two real square roots, and the count of exactly two square roots of every non-zero number; the quadratic formula with complex coefficients; the proof that no order makes $\mathbb{C}$ an ordered field; and why no choice of square roots keeps the product rule $\sqrt{z}\sqrt{w} = \sqrt{zw}$.
- **The Unit Circle and Polar Form.** The unit circle $\mathbb{T}$, closed under products and inverses, and every non-zero number as a length times a direction in exactly one way, all without angles; the five borrowed facts about cosine and sine; $e^{i\theta}$ as an abbreviation for $\cos\theta + i\sin\theta$, multiplication as "multiply moduli, add angles", and polar form, unique up to a multiple of 2π in the argument; De Moivre's formula; and the values of cosine and sine at $\pi/6$, $\pi/4$, $\pi/3$, $\pi/2$ and π, derived from the five facts.
- **Higher Roots, Roots of Unity, and a Look Ahead.** The unique non-negative n-th root of a non-negative real, constructed as a supremum; exactly n solutions of $z^n = c$ for every non-zero c, listed by polar form; the roots of unity, the set μ_n, and the sums of their powers; a look ahead at the Fundamental Theorem of Algebra; the conjugate of a solution of an equation with real coefficients as a second solution; and review exercises on the maps of $\mathbb{C}$ to itself that respect sums, products and 1 and send $\mathbb{R}$ into $\mathbb{R}$, on $\mathbb{Z}/n\mathbb{Z}$ and μ_n, on the triangle inequality of an ordered field, and on the equation $\overline{z} = z^2$.

1.0.2 Named moves

- **Compare real and imaginary parts.** One equation between complex numbers is two equations between real numbers: for real a, b, c, d, $a + bi = c + di$ if and only if $a = c$ and $b = d$. It is named in Section 1.1, where it proves the laws of arithmetic; Section 1.4 uses it to turn $w^2 = z$ into two real equations, and Section 1.5 to turn $e^{i\theta} = 1$ into $\cos\theta = 1$ and $\sin\theta = 0$. The warning of Section 1.1 marks the hypothesis it needs: the four numbers must be real. Exercise C1 of Section 1.1 proves the same uniqueness of parts in any field that contains $\mathbb{R}$ and a square root of -1.
- **Square the modulus.** The modulus is a square root, and square roots do not expand; its square $|u|^2 = u\overline{u}$ is a product, and products do. So square, expand with conjugates, bound or compare the real numbers that appear, and take the non-negative square root back, which is legitimate because non-negative reals compare as their squares do. Section 1.2 uses it first, for $|zw| = |z||w|$; Section 1.3 names it and runs it in full for the triangle inequality. Exercise B2 of Section 1.3 leaves the last step to you, and Exercise C2 of

Section 1.3 the last half.

- **Multiply moduli, add angles.** In polar form a product is the product of the moduli and the sum of the arguments, so an equation $z^n = c$ splits into a real equation $r^n = \rho$ for the length and an angle condition $n\theta \in \alpha + 2\pi\mathbb{Z}$. It is named in Section 1.5, after the multiplication theorem, and gives De Moivre's formula there; Section 1.6 uses it to solve $z^n = c$ and to count the solutions. The warning of Section 1.6 shows what goes wrong when the angle condition is read as an equation $n\theta = \alpha$: all roots but one are lost.

1.1 The Complex Numbers as Pairs of Reals

The equation $x^2 + 1 = 0$ has no real solution. In an ordered field every square is non-negative (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e) for a non-zero element, and $0^2 = 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)), so $x^2 + 1 \geq 0 + 1 = 1 > 0$ for every real x (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b), (e)). For most of school mathematics this gap is harmless. Later volumes cannot live with it: the linear-algebra volumes meet real matrices, such as a rotation of the plane, whose most useful data are not real numbers. This section builds the complex numbers, the number system that closes the gap, and proves that they obey the familiar laws of arithmetic.

Standing setting. Throughout the chapter, $\mathbb{R}$ is the complete ordered field built in *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 5 (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3). In particular $\mathbb{R}$ is a field in the sense of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1, and every rule that book proved for ordered fields holds in it. No proof below looks inside a real number. Letters a, b, c, d, e, f, x, y stand for real numbers, and z, w, u, v for complex numbers, unless we say otherwise.

1.1.1 Building the new numbers

The quick way to introduce complex numbers is to say "invent a symbol i with $i^2 = -1$ and compute as usual". That raises a fair worry. How do we know that such a symbol does not lead to a contradiction, the way "invent a number z with $0 \cdot z = 1$" does? The answer is to build the new numbers out of objects we already trust: pairs of real numbers.

Here is the recurring expression that suggests the definition. If we pretend $i^2 = -1$ and expand, we get

$$(a + bi)(c + di) = ac + adi + bci + bd\,i^2 = (ac - bd) + (ad + bc)i.$$

So a "number $a+bi$" is really the pair (a, b), and the product should be the pair $(ac-bd, ad+bc)$. We take this formula as the definition, so nothing is pretended.

A complex number is a pair of real numbers, multiplied as if $i^2 = -1$.

Definition 1.1.1. Complex Numbers

The set of **complex numbers** is

$$\mathbb{C} := \mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\},$$

the Cartesian product of Sets, Relations, and Cardinality, Definition 1.3.2, with **addition**

and **multiplication** defined **for all** $(a,b),(c,d) \in \mathbb{C}$ by

$$(a,b)+(c,d) \coloneqq (a+c,\ b+d),$$
$$(a,b)(c,d) \coloneqq (ac-bd,\ ad+bc).$$

We write $i \coloneqq (0,1)$. For $z=(a,b)\in\mathbb{C}$, the **real part** of z is $\operatorname{Re} z \coloneqq a$ and the **imaginary part** of z is $\operatorname{Im} z \coloneqq b$.

In words: addition is coordinate by coordinate, as for points of the plane. Multiplication is the formula found by expanding. Both right-hand sides are pairs of real numbers, computed with the operations of $\mathbb{R}$, so both operations are functions $\mathbb{C}\times\mathbb{C}\to\mathbb{C}$. The point i is the point one unit up the vertical axis. The real part and the imaginary part of z are its two coordinates, and both are **real** numbers.

There is nothing to check for well-definedness: a pair determines its coordinates, by the characteristic property of ordered pairs (Sets, Relations, and Cardinality, Definition 1.3.1),

$$(a,b)=(c,d) \iff a=c \text{ and } b=d.$$

In the language of the definition: two complex numbers z and w are equal **if and only if** $\operatorname{Re} z = \operatorname{Re} w$ **and** $\operatorname{Im} z = \operatorname{Im} w$. So one equation between complex numbers is two equations between real numbers. This is the first named move of the chapter, **compare real and imaginary parts**, and the proofs of Proposition 1.1.1 and Proposition 1.1.2 below rest on it.

The equation that motivated everything is now a computation:

$$i\cdot i=(0,1)(0,1)=(0\cdot 0-1\cdot 1,\ 0\cdot 1+1\cdot 0)=(-1,0).$$

To read the right-hand side as "-1", we have to see the real numbers inside $\mathbb{C}$.

1.1.2 The real numbers inside the complex numbers

The real number a should be the point $(a,0)$ on the horizontal axis. Before we write a for $(a,0)$, we check that nothing is lost: different real numbers stay different, and adding or multiplying two real numbers gives the same answer in $\mathbb{C}$ as in $\mathbb{R}$.

Proposition 1.1.1. The Real Numbers inside the Complex Numbers

Let $\iota\colon \mathbb{R}\to\mathbb{C}$ be the map $\iota(a) \coloneqq (a,0)$. Then ι is injective (Sets, Relations, and Cardinality, Definition 1.4.3), and for all $a,c\in\mathbb{R}$,

$$\iota(a+c)=\iota(a)+\iota(c), \qquad \iota(ac)=\iota(a)\,\iota(c), \qquad \iota(1)=(1,0).$$

Moreover $(a,b)=\iota(a)+\iota(b)\,i$ for all $a,b\in\mathbb{R}$, and $i\cdot i=\iota(-1)$.

Idea. Each claim is one application of the definitions: write both sides as pairs and compare coordinates. The facts about $\mathbb{R}$ needed are that 0 is neutral for addition (so subtracting 0 changes nothing), that 1 is neutral for multiplication, and that a product with 0 is 0, which kills the extra terms of the multiplication formula.

Proof. Let $a, c \in \mathbb{R}$. If $\iota(a) = \iota(c)$, then $(a, 0) = (c, 0)$, so $a = c$ by Sets, Relations, and Cardinality, Definition 1.3.1; hence ι is injective. By Definition 1.1.1,

$$\iota(a) + \iota(c) = (a + c,\ 0 + 0) = (a + c,\ 0) = \iota(a + c),$$

and, since $a \cdot 0 = 0 \cdot c = 0 \cdot 0 = 0$ in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)),

$$\iota(a)\,\iota(c) = (ac - 0 \cdot 0,\ a \cdot 0 + 0 \cdot c) = (ac,\ 0) = \iota(ac).$$

The equation $\iota(1) = (1, 0)$ is the definition of ι. Next, for $a, b \in \mathbb{R}$,

$$\iota(b)\, i = (b, 0)(0, 1) = (b \cdot 0 - 0 \cdot 1,\ b \cdot 1 + 0 \cdot 0) = (0, b),$$

so $\iota(a) + \iota(b)\, i = (a, 0) + (0, b) = (a, b)$. Finally $i \cdot i = (-1, 0) = \iota(-1)$ by the computation before the proposition.

■

Identification. From now on we write a for $\iota(a)$ and regard $\mathbb{R}$ as a subset of $\mathbb{C}$. In particular $0 = (0, 0)$ and $1 = (1, 0)$. This is a convenient abuse of notation made honest by the injective embedding, exactly as *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 2.2 wrote n for the integer $\iota(n)$: because ι is injective, different real numbers stay different, and because it preserves $+$ and $\cdot$, a sum or product of real numbers is the same whether computed in $\mathbb{R}$ or in $\mathbb{C}$.

With this convention the proposition reads

$$(a, b) = a + bi \quad \text{for all } a, b \in \mathbb{R}, \qquad i^2 = i \cdot i = -1.$$

So the notation $a + bi$ is honest: it is a computation with the definitions, not a new symbol. Comparing real and imaginary parts now reads: for $a, b, c, d \in \mathbb{R}$,

$$a + bi = c + di \iff a = c \text{ and } b = d.$$

For $z = a + bi$ with $a, b \in \mathbb{R}$ we have $\operatorname{Re} z = a$ and $\operatorname{Im} z = b$. A real number $a = a + 0i$ is a complex number whose imaginary part is 0, and $0 = 0 + 0i$ is the only complex number with both parts 0. The point $i = 0 + 1i$ has real part 0 and imaginary part 1.

Warning. The rule "$a + bi = c + di$ gives $a = c$ and $b = d$" needs a, b, c, d to be **real**. Without that it fails: $0 + 1 \cdot i = i + 0 \cdot i$, yet $0 \neq i$. Before comparing parts, write each side as $a + bi$ with a and b known to be real.

Example. First Computations in $\mathbb{C}$

Compute $(2 + 3i)(1 - i)$, the products $i \cdot i$, $(i \cdot i) \cdot i$ and $((i \cdot i) \cdot i) \cdot i$, and the product $(a + bi)(a - bi)$ for real a, b.

Solution. Here $1 - i$ is $1 + (-1)i$. By the multiplication rule with $a = 2$, $b = 3$, $c = 1$, $d = -1$,

$$(2 + 3i)(1 - i) = \big(2 \cdot 1 - 3 \cdot (-1)\big) + \big(2 \cdot (-1) + 3 \cdot 1\big)i = 5 + i.$$

We already know $i \cdot i = -1 = (-1, 0)$. Then

$$(i \cdot i) \cdot i = (-1, 0)(0, 1) = (0 - 0,\ -1 + 0) = (0, -1) = -i,$$

writing $-i$ for $0 + (-1)i$, and

$$\big((i \cdot i) \cdot i\big) \cdot i = (0, -1)(0, 1) = \big(0 - (-1),\ 0 + 0\big) = (1, 0) = 1.$$

Finally, with $a - bi = a + (-b)i$,

$$(a + bi)(a - bi) = \big(a^2 - b(-b)\big) + \big(a(-b) + ba\big)i = a^2 + b^2,$$

where $a^2 = aa$ and $b^2 = bb$ are computed in $\mathbb{R}$. This product is a real number, and it is **non-negative**, since $a^2 \geq 0$ and $b^2 \geq 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e) for a non-zero real, and $0^2 = 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)), so $a^2 + b^2 \geq 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b). We meet it again in Section 1.2, as the square of the length of $a + bi$.

The last product is the first hint of how division will work: multiplying $a + bi$ by $a - bi$ lands in the real numbers, where division is familiar.

Quick check. Compute $(1 + i)(1 + i)$. Is $\mathrm{Im}(3 - 4i)$ equal to $-4i$?

Solution. By the multiplication rule, $(1 + i)(1 + i) = (1 \cdot 1 - 1 \cdot 1) + (1 \cdot 1 + 1 \cdot 1)i = 2i$. No: $3 - 4i = 3 + (-4)i$ with $3, -4 \in \mathbb{R}$, so $\mathrm{Im}(3 - 4i) = -4$, a real number. The number $-4i$ is not real, since its imaginary part is $-4 \neq 0$.

A non-example by minimal change. Change one sign in the multiplication rule: define

$$(a, b) * (c, d) \coloneqq (ac + bd,\ ad + bc),$$

which is what expanding gives if we pretend $j^2 = +1$ instead. Addition is unchanged. This product is still commutative, by commutativity in $\mathbb{R}$, and $(1, 0)$ is still an identity element: $(a, b) * (1, 0) = (a + 0,\ 0 + b) = (a, b)$. But

$$(1, 1) * (1, -1) = \big(1 - 1,\ -1 + 1\big) = (0, 0),$$

so two non-zero elements multiply to zero. Division breaks down too: $(1, 1) * (c, d) = (c + d,\ d + c)$ can never equal the identity element $(1, 0)$, because that would need $c + d = 1$ and $d + c = 0$ at once. So the non-zero element $(1, 1)$ has no inverse. *The single sign in $ac - bd$ is what makes division possible*, as Section 1.2 will show. Exercise B3 finds every element that goes wrong in this way.

Why this definition. We could have tried to postulate a number i with $i^2 = -1$, but a postulate is only as safe as the consistency of what it asserts. Pairs of reals are sets we already have, so $\mathbb{C}$ exists as soon as $\mathbb{R}$ does, and every law we want must now be **proved**. The multiplication formula is not a free choice either: Exercise C1 shows that in any field K containing $\mathbb{R}$, whose sum and product agree with those of $\mathbb{R}$ on real numbers, and containing a square root j of -1, the product of $a + bj$ and $c + dj$ is forced to be $(ac - bd) + (ad + bc)j$. The minimal change above shows that a different formula really does give a different, and worse, system.

1.1.3 The laws of arithmetic

Before computing freely, we should confirm that rearranging, regrouping and expanding brackets are legal in $\mathbb{C}$. The definition does not promise this; it has to be checked.

Proposition 1.1.2. Arithmetic Laws in $\mathbb{C}$

For all $z, w, u \in \mathbb{C}$:

(a) $z + w = w + z$ and $zw = wz$;
(b) $(z + w) + u = z + (w + u)$ and $(zw)u = z(wu)$;
(c) $z(w + u) = zw + zu$;
(d) $z + 0 = z$, $z \cdot 1 = z$, and $z + (-z) = 0$, where $-(a + bi) := (-a) + (-b)i$ for $a, b \in \mathbb{R}$.

Idea. Every law reduces to the corresponding law for real numbers once both sides are written as pairs and compared part by part. Addition is coordinate by coordinate, so its laws are immediate. For multiplication the only real work is associativity: expand both sides and see that they produce the same four terms in each coordinate.

Proof. Let $z = a+bi$, $w = c+di$ and $u = e+fi$ with $a, b, c, d, e, f \in \mathbb{R}$. In each part we compute both sides with Definition 1.1.1 and compare real and imaginary parts, using the field laws of $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1) and the algebra of Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2. Since addition acts coordinate by coordinate, the laws for addition in (a), (b) and (d) are the same laws in $\mathbb{R}$, applied to each coordinate; for (d), $z+0 = (a+0)+(b+0)i = z$ and $z+(-z) = (a+(-a))+(b+(-b))i = 0$.

(a) By definition $zw = (ac - bd) + (ad + bc)i$ and $wz = (ca - db) + (cb + da)i$. These are equal because real multiplication and addition are commutative.

(b) Expanding with the definition twice gives

$$\begin{aligned}(zw)u = &\big((ac - bd)e - (ad + bc)f\big)\\ &+ \big((ac - bd)f + (ad + bc)e\big)i\end{aligned}$$

and

$$\begin{aligned}z(wu) = &\big(a(ce - df) - b(cf + de)\big)\\ &+ \big(a(cf + de) + b(ce - df)\big)i.\end{aligned}$$

Multiplying out with the distributive law of $\mathbb{R}$, both real parts equal $ace-adf-bcf-bde$, and both imaginary parts equal $acf + ade + bce - bdf$. Hence $(zw)u = z(wu)$.

(c) We have $w + u = (c + e) + (d + f)i$, so

$$\begin{aligned}z(w + u) &= \big(a(c + e) - b(d + f)\big) + \big(a(d + f) + b(c + e)\big)i\\ &= \big((ac - bd) + (ae - bf)\big) + \big((ad + bc) + (af + be)\big)i,\end{aligned}$$

which is $zw + zu$ by the definitions of the product and the sum.

(d) With $1 = 1 + 0i$, we get $z \cdot 1 = (a \cdot 1 - b \cdot 0) + (a \cdot 0 + b \cdot 1)i = a + bi = z$. The equations for addition were shown above. This proves the proposition.

■

In the language of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 2.3, the proposition checks the axioms of a commutative ring (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1): (a) is (F1) and (F6), (b) is (F2) and (F5), (c) is (F9), and (d) is (F3), (F7) and (F4). Moreover $1 \neq 0$ in $\mathbb{C}$, since $(1,0) \neq (0,0)$ by Sets, Relations, and Cardinality, Definition 1.3.1, as $1 \neq 0$ in $\mathbb{R}$.

Remark. So $\mathbb{C}$, with the operations of Definition 1.1.1, is a **commutative ring** with $1 \neq 0$. Every result proved for commutative rings therefore holds in $\mathbb{C}$ without a new proof. From Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2: 0, 1 and negatives are unique, $-(-z) = z$, $z \cdot 0 = 0$, $(-z)w = -(zw)$, $(-z)(-w) = zw$, and $(z+w)^2 = z^2 + 2zw + w^2$, where $z^2 := zz$. The remaining field axiom (F8), inverses of non-zero elements, is the subject of Section 1.2.

From now on we compute in $\mathbb{C}$ exactly as in $\mathbb{R}$: expand brackets, collect terms, and replace i^2 by -1. The proposition is what makes that habit legitimate. For instance, $(a+bi)(a-bi) = a^2 - abi + abi - b^2 i^2 = a^2 + b^2$ agrees with Example (First Computations in $\mathbb{C}$).

1.1.4 Powers and a factorization

Powers in $\mathbb{C}$ are defined exactly as powers in an ordered field were, and that definition never used the order. We state it, and the laws of powers, for an arbitrary commutative ring, because the same proofs serve every commutative ring and later chapters need them in that generality.

Powers. Let R be a commutative ring and $z \in R$. The **powers** z^n, for $n \in \mathbb{N}$, are given by Sets, Relations, and Cardinality, Theorem 2.3.1, read on $\mathbb{N} = \omega$ through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b), with $X = R$, starting value 1 and step $(k, y) \mapsto yz$:

$$z^0 := 1, \qquad z^{n+1} := z^n z \quad \text{for every } n \in \mathbb{N}.$$

This is the recursion of *Sets, Relations, and Cardinality*, Section 2.3 (Sets, Relations, and Cardinality, Definition 2.3.2), stated there for real numbers, and the same recursion as Number Systems: From \(\nN\) to \(\nR\), Definition 4.2.1 (b). In particular $z^1 = 1 \cdot z = z$ and $z^2 = z^1 z = zz$, matching the z^2 of Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d).

Proposition 1.1.3. Laws of Powers in a Commutative Ring

Let R be a commutative ring (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1), let $z, w \in R$, and let $m, n \in \mathbb{N}$.

(a) $z^{m+n} = z^m z^n$.
(b) $(z^m)^n = z^{mn}$.
(c) $(zw)^n = z^n w^n$.
(d) If R is a field and $z \neq 0$, then $z^n \neq 0$.

Idea. The definition of z^n is a recursion on n, so every law is proved by induction on n, peeling off the last factor with $z^{n+1} = z^n z$. Each inductive step rests on one ingredient: associativity (F5) for (a), the law (a) for (b), associativity and commutativity (F5), (F6) for (c), and the absence of zero divisors in a field for (d).

Proof. Each part is proved by Logic and Proof, Axiom 4.2.1 (through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) on n, with z, w and m fixed.

(a) For $n = 0$: $z^{m+0} = z^m = z^m \cdot 1 = z^m z^0$, by (F7). If $z^{m+n} = z^m z^n$, then

$$z^{m+(n+1)} = z^{(m+n)+1} = z^{m+n} z = (z^m z^n) z = z^m (z^n z) = z^m z^{n+1},$$

by the recursion, the hypothesis and associativity (F5).

(b) For $n = 0$: $(z^m)^0 = 1 = z^0 = z^{m \cdot 0}$. If $(z^m)^n = z^{mn}$, then $(z^m)^{n+1} = (z^m)^n z^m = z^{mn} z^m = z^{mn+m} = z^{m(n+1)}$, by the recursion, the hypothesis and (a).

(c) For $n = 0$: $(zw)^0 = 1 = 1 \cdot 1 = z^0 w^0$. If $(zw)^n = z^n w^n$, then

$$(zw)^{n+1} = (zw)^n (zw) = (z^n w^n)(zw) = (z^n z)(w^n w) = z^{n+1} w^{n+1},$$

where the third equality regroups and reorders the four factors by (F5) and (F6).

(d) Let R be a field and $z \neq 0$. For $n = 0$: $z^0 = 1 \neq 0$, by the definition of a field. If $z^n \neq 0$, then $z^{n+1} = z^n z$ is a product of two non-zero elements, so it is non-zero, since a field has no zero divisors (Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d)).

■

Parts (a)–(c) are the laws of *Sets, Relations, and Cardinality*, Section 2.3 (Sets, Relations, and Cardinality, Proposition 2.3.4 (a)–(c)), proved there for real numbers; on $\mathbb{N} = \omega$, which is not a ring, law (a) is Number Systems: From \(\nN\) to \(\nR\), Proposition 1.6.4 (a), proved by the same induction. The proofs above are the same inductions, and they use only the ring axioms.

For a real number a, the power a^n is the same whether computed in $\mathbb{R}$ or in $\mathbb{C}$. Indeed $\iota(a^0) = \iota(1) = 1$, and if $\iota(a^n) = \iota(a)^n$, then $\iota(a^{n+1}) = \iota(a^n a) = \iota(a^n)\,\iota(a) = \iota(a)^{n+1}$, by Proposition 1.1.1; induction (Logic and Proof, Axiom 4.2.1) does the rest. So the identification of $\mathbb{R}$ with a subset of $\mathbb{C}$ is safe for powers too.

In the notation of powers, Example (First Computations in $\mathbb{C}$) computed $i^2 = -1$, $i^3 = -i$ and $i^4 = 1$; by (a), (b), every multiple of 4 gives $i^{4q} = (i^4)^q = 1^q = 1$, since $1^{q+1} = 1^q \cdot 1$ and induction give $1^q = 1$. Exercise B1 turns this into a rule for every power of i.

Quick check. Compute i^{10} and $(1+i)^4$, citing the parts of Proposition 1.1.3 you use.

Solution. By (a) and (b), $i^{10} = i^8 i^2 = (i^4)^2 i^2 = 1^2 \cdot (-1) = -1$. By (b), $(1+i)^4 = \left((1+i)^2\right)^2 = (2i)^2$, and by (c), $(2i)^2 = 2^2 i^2 = 4 \cdot (-1) = -4$, using $(1+i)^2 = 2i$ from the first Quick check.

Finite sums. One identity about powers is used repeatedly in this chapter and later, and it needs sums of several terms. For elements $a_0, a_1, a_2, \ldots$ of a commutative ring R and $n \in \mathbb{N}$, the sum $\sum_{k=0}^{n} a_k$ is defined by the recursion of Sets, Relations, and Cardinality, Definition 2.3.1,

with R as the set of values and the index starting at 0: the empty sum $\sum_{k=0}^{-1} a_k$ is 0, and

$$\sum_{k=0}^{n} a_k := \sum_{k=0}^{n-1} a_k + a_n \quad \text{for every } n \in \mathbb{N}.$$

So the recursion appends the last term. We also write $a_0 + a_1 + \cdots + a_n$ for this sum. Multiplying a sum by $c \in R$ multiplies each term: $(\sum_{k=0}^{n} a_k)c = \sum_{k=0}^{n} a_k c$, by induction on n, since $0 \cdot c = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)) and the step is one use of the distributive law (F9).

Lemma 1.1.4. Difference of Powers

Let R be a commutative ring, let $z, w \in R$, and let $n \in \mathbb{N}$ with $n \geq 1$. Then

$$z^n - w^n = (z - w) \sum_{k=0}^{n-1} z^k w^{n-1-k}.$$

In particular $z^n - 1 = (z - 1)(1 + z + z^2 + \cdots + z^{n-1})$.

Idea. For $n = 2$ this is $z^2 - w^2 = (z - w)(w + z)$, and for $n = 3$ it is $z^3 - w^3 = (z - w)(w^2 + zw + z^2)$. To pass from n to $n + 1$, split $z^{n+1} - w^{n+1}$ so that the case n appears: $z^{n+1} - w^{n+1} = (z^n - w^n)w + z^n(z - w)$. The first piece is $(z - w)$ times the old sum times w, and the second supplies the one new term z^n, which the recursion appends at the end.

Proof. For $n \geq 1$ write $S_n := \sum_{k=0}^{n-1} z^k w^{n-1-k}$. We prove $z^{m+1} - w^{m+1} = (z - w)S_{m+1}$ for every $m \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1 (through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) on m.

For $m = 0$: $S_1 = z^0 w^0 = 1$, so $(z - w)S_1 = z - w = z^1 - w^1$.

Let $n := m + 1 \geq 1$ and suppose $z^n - w^n = (z - w)S_n$. Expanding with (F9) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c),

$$(z^n - w^n)w + z^n(z - w) = z^n w - w^n w + z^n z - z^n w = z^{n+1} - w^{n+1},$$

by the recursion for powers. By the hypothesis and the rule for multiplying a sum by w,

$$(z^n - w^n)w = (z - w)S_n w = (z - w) \sum_{k=0}^{n-1} z^k w^{n-k},$$

since $w^{n-1-k}w = w^{n-k}$ for $k \leq n - 1$ (Proposition 1.1.3 (a)). Since $z^n = z^n w^0$, the recursion for sums gives

$$\begin{aligned} z^{n+1} - w^{n+1} &= (z - w)\Big(\sum_{k=0}^{n-1} z^k w^{n-k} + z^n w^0\Big) \\ &= (z - w) \sum_{k=0}^{n} z^k w^{n-k} = (z - w)S_{n+1}. \end{aligned}$$

This completes the induction. The particular case is $w = 1$, since $1^j = 1$ for every $j \in \mathbb{N}$.

■

The lemma is the algebra behind the formula for a finite geometric sum: if $z-1$ has an inverse, then $1+z+\cdots+z^{n-1}=(z^n-1)(z-1)^{-1}$. Section 1.6 uses it again, for real numbers, to show that $0\le s<t$ gives $s^n<t^n$. Here we need only the identity.

1.1.5 Exercises

1.1.5.1 A. Check your understanding

Exercise. A1

(a) Compute $(2-i)(3+4i)$, and the real and imaginary parts of $i(1+i)$.

(b) True or false, with a reason: the equation $(a,b)=a+bi$, for $a,b\in\mathbb{R}$, needs a proof.

(c) Which laws in Proposition 1.1.2 need a genuine computation, and which follow coordinate by coordinate from the same laws in $\mathbb{R}$?

(d) True or false, with a reason: if $z\in\mathbb{C}$ and $z^2=0$, then $z=0$. Prove it by comparing real and imaginary parts, without using that $\mathbb{C}$ is a field.

Solution.

(a) $(2-i)(3+4i)=6+8i-3i-4i^2=6+4+5i=10+5i$. And $i(1+i)=i+i^2=-1+i$, so $\mathrm{Re}(i(1+i))=-1$ and $\mathrm{Im}(i(1+i))=1$.

(b) True. The symbols a, b and i denote the pairs $(a,0)$, $(b,0)$, $(0,1)$, and $a+bi$ is a sum and a product of pairs. That it equals (a,b) is a computation with Definition 1.1.1; it is part of Proposition 1.1.1.

(c) The laws for addition, in (a), (b) and (d), hold coordinate by coordinate. Commutativity of multiplication, distributivity and $z\cdot 1=z$ are one-line computations. Associativity of multiplication is the one law that needs a genuine expansion: both sides have four terms in each part, and they agree only after multiplying out.

(d) True. Let $z=a+bi$. Then $z^2=(a^2-b^2)+2abi$, so $z^2=0$ gives $a^2-b^2=0$ and $2ab=0$, by comparing parts. Since $2\neq 0$ in $\mathbb{R}$ and $\mathbb{R}$ has no zero divisors (Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d)), $a=0$ or $b=0$. If $a=0$, then $-b^2=0$, so $b^2=0$ and $b=0$ by the same rule; if $b=0$, then $a^2=0$ and $a=0$. So $z=0$. (Once Section 1.2 has shown that $\mathbb{C}$ is a field, this follows at once from Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d) in $\mathbb{C}$.)

1.1.5.2 B. Practice

Exercise. B1: Powers of i

Let $n\in\mathbb{N}$, and let r be the remainder of n on division by 4. Prove that $i^n=i^r$. Hence compute i^{2026}.

Solution. By division with remainder (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2, with $n\in\mathbb{N}\subseteq\mathbb{Z}$ and divisor 4) there are integers q,r with $n=4q+r$ and $0\le r<4$. Also $q\ge 0$: if $q\le -1$, then $n\le -4+r<0$, which is false. So $q,r\in\mathbb{N}$. By

Proposition 1.1.3 (a) and (b), and $i^4 = 1$ (Example (First Computations in $\mathbb{C}$)),

$$i^n = i^{4q} i^r = (i^4)^q i^r = 1^q i^r = i^r,$$

where $1^q = 1$ by induction on q ($1^{q+1} = 1^q \cdot 1$). So i^n is $1, i, -1, -i$ according as $r = 0, 1, 2, 3$.

Hence, since $2026 = 4 \cdot 506 + 2$, $i^{2026} = i^2 = -1$.

Exercise. B2

(a) Use Lemma 1.1.4 to factor $z^3 - 1$ and $z^4 - 1$ in $\mathbb{C}$, and check the second factorization at $z = i$.

(b) Verify $(1 + i)^4 = -4$ using $(1 + i)^2 = 2i$ and Proposition 1.1.3. Hence show that, for every $z \in \mathbb{C}$,

$$z^4 + 4 = \big(z - (1 + i)\big)\big(z^3 + (1 + i)z^2 + 2iz + (-2 + 2i)\big).$$

Solution.

(a) With $n = 3$ and $n = 4$,

$$z^3 - 1 = (z - 1)(1 + z + z^2), \qquad z^4 - 1 = (z - 1)(1 + z + z^2 + z^3).$$

At $z = i$: the left side is $i^4 - 1 = 0$, and on the right $1 + i + i^2 + i^3 = 1 + i - 1 - i = 0$, so both sides are 0.

(b) By (b) of the proposition with $m = n = 2$, and then (c),

$$(1 + i)^4 = \big((1 + i)^2\big)^2 = (2i)^2 = 2^2 i^2 = -4.$$

Let $w := 1 + i$. Then $w^2 = 2i$ and $w^3 = w^2 w = 2i(1 + i) = -2 + 2i$. By Lemma 1.1.4 with $n = 4$, whose sum is $w^3 + zw^2 + z^2 w + z^3$,

$$z^4 - w^4 = (z - w)(z^3 + wz^2 + w^2 z + w^3).$$

Since $w^4 = -4$, the left side is $z^4 + 4$, and substituting w, w^2, w^3 gives the displayed factorization. In particular $1 + i$ is a root of $z^4 + 4$.

Exercise. B3: The zero divisors of the minimal change

Let $*$ be the product $(a, b) * (c, d) := (ac + bd,\ ad + bc)$ on $\mathbb{R}^2$ of the non-example in this section. Call a non-zero $p \in \mathbb{R}^2$ a **zero divisor** if $p * q = (0, 0)$ for some non-zero $q \in \mathbb{R}^2$. Prove that a non-zero (a, b) is a zero divisor if and only if $a^2 = b^2$, that such an (a, b) has no inverse (no q gives $(a, b) * q = (1, 0)$), and that if $a^2 \neq b^2$, then $(a, b) * (ta, -tb) = (1, 0)$ for $t := (a^2 - b^2)^{-1}$.

Solution. First, for any real t,

$$(a, b) * (ta, -tb) = (ta^2 - tb^2,\ -tab + tab) = (t(a^2 - b^2),\ 0).$$

If $a^2 \neq b^2$, then $a^2 - b^2 \neq 0$ has an inverse in $\mathbb{R}$, and $t := (a^2 - b^2)^{-1}$ gives $(1, 0)$.

($\Leftarrow$) Let $(a, b) \neq (0, 0)$ with $a^2 = b^2$. Then $(a - b)(a + b) = a^2 - b^2 = 0$, so $b = a$ or $b = -a$ (Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d) in $\mathbb{R}$). If $b = a$, then $(a, a) * (1, -1) = (a - a,\ -a + a) = (0, 0)$; if $b = -a$, then $(a, -a) * (1, 1) = (a - a,\ a - a) = (0, 0)$. In both cases the second factor is non-zero, so (a, b) is a zero divisor. Such an element also has no inverse: $(a, a) * (c, d) = \big(a(c + d),\ a(c + d)\big)$ has equal coordinates and $(a, -a) * (c, d) = \big(a(c - d),\ -a(c - d)\big)$ has opposite coordinates, while $(1, 0)$ has neither, since $1 \neq 0$ and $1 \neq -0 = 0$.

($\Rightarrow$) We prove the contrapositive (Logic and Proof, Proposition 2.3.2). Let $a^2 \neq b^2$, and suppose $(a, b) * (c, d) = (0, 0)$, that is, $ac + bd = 0$ and $ad + bc = 0$. Multiply the first equation by a and the second by b, and subtract: $a^2c + abd - abd - b^2c = 0$, that is, $(a^2 - b^2)c = 0$. Multiply the first by b and the second by a, and subtract: $(b^2 - a^2)d = 0$. Since $a^2 - b^2 \neq 0$ and $\mathbb{R}$ has no zero divisors, $c = 0$ and $d = 0$. So the only q with $(a, b) * q = (0, 0)$ is $q = (0, 0)$, and (a, b) is not a zero divisor. No associativity of $*$ was needed.

For example, $(1, 1)$ is a zero divisor, as in the text, and $(2, 1)$ is not: $(2, 1) * (2/3, -1/3) = (4/3 - 1/3,\ -2/3 + 2/3) = (1, 0)$.

1.1.5.3 C. Going deeper

Exercise. C1: There is only one way to adjoin a square root of minus one

Let K be a field (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1) with $\mathbb{R} \subseteq K$, such that the sum and the product of K, applied to two real numbers, are their sum and product in $\mathbb{R}$. Let $j \in K$ with $j^2 = -1$.

(a) Show that 0, 1, negatives and inverses of non-zero real numbers are the same in K as in $\mathbb{R}$.

(b) Show that if $a + bj = c + dj$ with $a, b, c, d \in \mathbb{R}$, then $a = c$ and $b = d$.

(c) Let $\varphi\colon \mathbb{C} \to K$, $\varphi(a + bi) := a + bj$ for $a, b \in \mathbb{R}$. Show that φ is injective, $\varphi(1) = 1$, and $\varphi(z + w) = \varphi(z) + \varphi(w)$, $\varphi(zw) = \varphi(z)\varphi(w)$ for all $z, w \in \mathbb{C}$.

Solution (Hint 1). For (a), start from $0 + 0 = 0$ and $1 \cdot 1 = 1$ in $\mathbb{R}$ and cancel in K: add the negative of $0_{\mathbb{R}}$; for 1, multiply by the inverse of $1_{\mathbb{R}}$, which exists because $1_{\mathbb{R}} \neq 0_{\mathbb{R}} = 0_K$. For $-a$ and a^{-1}, use that each is the **only** element with its property (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a), Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (a)). For (b), ask what happens if $b \neq d$.

Solution (Hint 2). For (b): suppose $b \neq d$. Then $(d - b)j = a - c$, and $d - b$ is a non-zero real number.

Solution.

(a) In $\mathbb{R}$, $0_{\mathbb{R}} + 0_{\mathbb{R}} = 0_{\mathbb{R}}$; the same equation holds in K, since the sum of K on reals is that of $\mathbb{R}$. Adding $-0_{\mathbb{R}}$ (the negative in K) to both sides gives $0_{\mathbb{R}} = 0_K$. Next, $1_{\mathbb{R}} \cdot 1_{\mathbb{R}} = 1_{\mathbb{R}}$ in K, and $1_{\mathbb{R}} \neq 0_{\mathbb{R}} = 0_K$; multiplying by the inverse of $1_{\mathbb{R}}$ in K gives

$1_{\mathbb{R}} = 1_K$. For $a \in \mathbb{R}$, the real negative $-a$ satisfies $a + (-a) = 0_{\mathbb{R}} = 0_K$ in K, so it is the negative of a in K, by uniqueness of negatives (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)). Likewise, for real $a \neq 0$, the real inverse satisfies $aa^{-1} = 1_{\mathbb{R}} = 1_K$ in K, so it is the inverse of a in K (Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (a)). So sums, products, differences and quotients of real numbers computed in K are real numbers.

(b) Suppose $a+bj = c+dj$, and suppose, for contradiction, that $b \neq d$. Then $(d-b)j = a-c$, with $d - b$ a non-zero real number, so $j = (a - c)(d - b)^{-1}$, which is real by (a). Then j^2 is the square of a real number, computed in $\mathbb{R}$. Here $j \neq 0$, since $0^2 = 0 \neq -1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)), so $j^2 > 0$ in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)). But $j^2 = -1 < 0$ in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e), (a)), and $0 < j^2 < 0$ contradicts (O1). Hence $b = d$, and then $a = c$ by adding $-bj$ to both sides.

(c) The map is a function, since $a + bi$ determines a and b (Proposition 1.1.1). It is injective by (b): $a + bj = c + dj$ gives $a = c$ and $b = d$, so $a + bi = c + di$. Also $\varphi(1) = \varphi(1 + 0i) = 1 + 0j = 1$. For $z = a + bi$ and $w = c + di$, the field laws of K give

$$\varphi(z) + \varphi(w) = (a + c) + (b + d)j = \varphi(z + w),$$

and, with $j^2 = -1$,

$$\begin{aligned}\varphi(z)\varphi(w) &= ac + adj + bcj + bdj^2 \\ &= (ac - bd) + (ad + bc)j = \varphi(zw),\end{aligned}$$

by Definition 1.1.1. This proves (c).

So any field that contains $\mathbb{R}$ and a square root j of -1 contains an exact copy of $\mathbb{C}$, namely $\{a + bj : a, b \in \mathbb{R}\}$, and its arithmetic is forced to be the arithmetic of Definition 1.1.1. Chapter 2 meets more fields of this shape, built from a smaller field and one new element, such as $\{a + bi : a, b \in \mathbb{Q}\}$.

Marking scheme. (10 points) - 2: (a) identifies 0 and 1 of $\mathbb{R}$ in K by cancellation, and negatives and inverses of reals by uniqueness. - 3: (b) shows that $b \neq d$ would make j real, with the division justified by $d - b \neq 0$. - 2: (b) derives the contradiction from $j^2 > 0$ in $\mathbb{R}$ (with $j \neq 0$) and $-1 < 0$, naming the ordered-field rule. - Second route for (b): squaring $(b - d)j = c - a$ with $j^2 = -1$, and noting by (a) that the result is an equation between real numbers, earns the 3 points; concluding from $(c - a)^2 + (b - d)^2 = 0$ that $a = c$ and $b = d$, from squares ≥ 0 in $\mathbb{R}$, naming the ordered-field rule, earns the 2 points. - 1: (c) injectivity, from (b). - 2: (c) the sum and the product, expanding with $j^2 = -1$ and comparing with Definition 1.1.1. Fatal errors (0 for the step): treating j as i (the point is that K is any field); claiming $j^2 \geq 0$ in K (there is no order on K).

1.2 Conjugate, Modulus, and Division

Section 1.1 built $\mathbb{C}$ and showed that it is a commutative ring with $1 \neq 0$ (Proposition 1.1.2). One field axiom is still missing: (F8), which asks for an inverse of every non-zero element. To divide by $3+4i$, we want a number to multiply by that lands in the real numbers, where division is familiar. The product $(a + bi)(a - bi) = a^2 + b^2$ of Example (First Computations in $\mathbb{C}$) shows which number does the job. This section gives its two ingredients names, the conjugate and the modulus, proves the rules they obey, and concludes that $\mathbb{C}$ is a field.

1.2.1 Conjugate and modulus

A complex number $z = a + bi$ is a point (a, b) of the plane. Two pieces of plane geometry turn out to be algebra in disguise: the mirror image of z in the horizontal axis, and the distance of z from 0. The mirror image changes the sign of b. The distance, by Pythagoras, is the square root of $a^2 + b^2$, the very number that appeared in Example (First Computations in $\mathbb{C}$). Square roots of non-negative real numbers exist and are unique in every complete ordered field (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), so we may use them in $\mathbb{R}$: for $x \in \mathbb{R}$ with $x \geq 0$, $\sqrt{x}$ is the **unique** $y \in \mathbb{R}$ with $y \geq 0$ and $y^2 = x$.

Conjugating reflects a point in the real axis; the modulus is its distance from the origin.

Definition 1.2.1. Conjugate and Modulus

Let $z = a + bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$. The **complex conjugate** of z is

$$\overline{z} := a - bi.$$

The **modulus** (or absolute value) of z is the real number

$$|z| := \sqrt{a^2 + b^2},$$

the **non-negative** square root of Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4 in $\mathbb{R}$.

In words: the conjugate keeps the real part and flips the sign of the imaginary part, $\operatorname{Re}\overline{z} = \operatorname{Re} z$ and $\operatorname{Im}\overline{z} = -\operatorname{Im} z$. The modulus is a **real** number, never negative, and its square is $a^2 + b^2 = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2$.

Well-definedness. Since z determines a and b (compare real and imaginary parts, Section 1.1), the right-hand sides depend only on z. The square root exists because its argument is non-negative: $a^2 \geq 0$ and $b^2 \geq 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e), with $0^2 = 0$ when the number is 0), so $a^2 + b^2 \geq 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b)). And $\mathbb{R}$ is complete (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3), which is the hypothesis of Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4. This is where the completeness of $\mathbb{R}$ enters the chapter. Over $\mathbb{Q}$ alone the definition would break down at once: $|1 + i|$ would have to be a rational number whose square is 2, and there is none (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1).

Examples.

A point with integer distance. For $z = 3+4i$: $\overline{z} = 3-4i$, and $|z| = \sqrt{9 + 16} = \sqrt{25} = 5$. The last step is the uniqueness clause of Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4: $5 \geq 0$ and $5^2 = 25$, so 5 is **the** non-negative square root of 25.

The unit i. $\overline{i} = \overline{0 + 1i} = 0 - 1i = -i$, and $|i| = \sqrt{0 + 1} = 1$, since $1 \geq 0$ and $1^2 = 1$.

The degenerate case $z = 0$. $\overline{0} = 0$ and $|0| = \sqrt{0} = 0$. We show below that 0 is the **only** complex number with modulus 0; that one fact is what makes division possible.

A real number. For $a \in \mathbb{R}$, $\overline{a} = a$ and $|a| = \sqrt{a^2}$. The symbol $|a|$ already had a meaning for real a: the absolute value of an ordered field (Number Systems: From \(\nN\) to \(\nR\), Definition 4.1.1). The next proposition shows the two meanings agree, so the notation does not clash.

Proposition 1.2.1. The Modulus Extends the Absolute Value

Let $a \in \mathbb{R} \subseteq \mathbb{C}$. Then $\overline{a} = a$, and the modulus $\sqrt{a^2 + 0^2}$ of a equals the absolute value of a in the ordered field $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 4.1.1).

Proof. Write $a = a + 0i$. Then $\overline{a} = a - 0i = a$, since $0 \cdot i = i \cdot 0 = 0$ by (F6) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), and $-0 = 0$ because $0 + 0 = 0$ and negatives are unique (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)), all in the commutative ring $\mathbb{C}$. The modulus of a is $\sqrt{a^2 + 0^2} = \sqrt{a^2}$, the unique non-negative real number whose square is a^2. The absolute value $|a|$ of the ordered field $\mathbb{R}$ is non-negative and satisfies $|a|^2 = a^2$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (a), (b)). By the uniqueness clause of Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4, the two are equal. ∎

So the modulus **extends** the absolute value: on $\mathbb{R} \subseteq \mathbb{C}$ it is the old $|\cdot|$, and every result about $|x|$ for real x stays true with the new reading. For instance $|-3| = 3$, whichever definition we use.

Quick check. Find $\overline{z}$ and $|z|$ for $z = -2i$ and for $z = 1 - i$. For which of the two is $\overline{z} = z$?

Solution. For $z = -2i = 0 + (-2)i$: $\overline{z} = 0 - (-2)i = 2i$ and $|z| = \sqrt{0 + 4} = 2$, since $2 \geq 0$ and $2^2 = 4$. For $z = 1 - i$: $\overline{z} = 1 + i$ and $|z| = \sqrt{1 + 1} = \sqrt{2}$. In neither case is $\overline{z} = z$: comparing imaginary parts, $\overline{z} = z$ needs $\operatorname{Im} z = -\operatorname{Im} z$, that is $\operatorname{Im} z = 0$, and both numbers have non-zero imaginary part.

Why this definition. The square root is what makes the modulus a length. Without it, the simpler quantity $N(z) := a^2 + b^2$ would do some of the same jobs: it is $z\overline{z}$, and it vanishes only at 0. But on real numbers it is $N(a) = a^2$, not $|a|$, so it does not extend the absolute value: $N(2) = 4$. And it is not a sensible distance: $N(1+1) = 4$, while $N(1) + N(1) = 2$, so the "side" from 0 to 2 would be longer than the two sides through 1. The modulus keeps the convenient algebra of N, since $|z|^2 = N(z)$, and adds the right size. Section 1.3 exploits exactly this square.

Warning. The modulus squared is $z\overline{z}$, **not** zz. In general $|z|^2 \neq z^2$: for $z = i$, $|i|^2 = 1$ but $i^2 = -1$. The two agree only when z is real. For $z = a + bi$, $z^2 = (a^2 - b^2) + 2abi$ and $|z|^2 = a^2 + b^2$; if they are equal, comparing real parts gives $a^2 - b^2 = a^2 + b^2$, so $2b^2 = 0$. Since $2 > 0$ in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h)), $2 \neq 0$, so $b^2 = 0$ by part (f), and $b = 0$ by part (e). Conversely, for real $z = a$, $|a|^2 = a^2 + 0^2 = a^2$.

1.2.2 Rules for conjugate and modulus

The following rules are used constantly, in this chapter and much later for complex inner products. They say that conjugation respects both operations, and that the modulus respects prod-

ucts.

Theorem 1.2.2. Properties of Conjugation and Modulus

For all $z, w \in \mathbb{C}$:

(a) $\overline{z+w} = \overline{z} + \overline{w}$ and $\overline{\overline{z}} = z$;
(b) $\overline{zw} = \overline{z}\,\overline{w}$;
(c) $z\overline{z} = |z|^2$ and $z + \overline{z} = 2\operatorname{Re} z$;
(d) $|zw| = |z|\,|w|$ and $|\overline{z}| = |z|$;
(e) $|z| = 0$ if and only if $z = 0$.

Idea. Parts (a)–(c) and (e) are direct computations with real and imaginary parts. For (d), expanding $|zw|$ directly is legitimate but messy, since a square root of a long sum appears. It is cleaner to square: by (c) a squared modulus is a product with a conjugate, and (b) lets the conjugate split across the product. Two non-negative real numbers with the same square are equal, and that brings us back from squares to moduli.

Proof. Let $z = a + bi$ and $w = c + di$ with $a, b, c, d \in \mathbb{R}$.

(a) We have $\overline{z+w} = (a+c)-(b+d)i = (a-bi)+(c-di) = \overline{z}+\overline{w}$, since $-(b+d) = (-b)+(-d)$: $(b+d)+\big((-b)+(-d)\big) = 0$, and negatives are unique (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a) in $\mathbb{R}$). And $\overline{z} = a+(-b)i$, so $\overline{\overline{z}} = a-(-b)i = a+bi = z$, by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a) in $\mathbb{R}$.

(b) Since $zw = (ac-bd)+(ad+bc)i$, we get $\overline{zw} = (ac-bd)-(ad+bc)i$. On the other hand, by Definition 1.1.1 and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c) in $\mathbb{R}$,

$$\begin{aligned}\overline{z}\,\overline{w} &= \big(a+(-b)i\big)\big(c+(-d)i\big)\\ &= \big(ac-(-b)(-d)\big) + \big(a(-d)+(-b)c\big)i\\ &= (ac-bd)-(ad+bc)i.\end{aligned}$$

(c) By Example (First Computations in $\mathbb{C}$), $z\overline{z} = a^2+b^2$, and $a^2+b^2 = |z|^2$ because $|z|$ is a square root of a^2+b^2. Also $z+\overline{z} = (a+a)+(b-b)i = 2a = 2\operatorname{Re} z$.

(d) By (c), then (b), then Proposition 1.1.2 to regroup and reorder the four factors,

$$|zw|^2 = (zw)\,\overline{zw} = zw\overline{z}\,\overline{w} = (z\overline{z})(w\overline{w}) = |z|^2|w|^2.$$

In $\mathbb{R}$, $|z|^2|w|^2 = \big(|z||w|\big)^2$ (Proposition 1.1.3 (c)), and $|z||w| \geq 0$: it is 0 if one factor is 0 (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)), and positive otherwise, since a product of two positive elements of an ordered field is positive ((O4) of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.2). So $|zw|$ and $|z||w|$ are both non-negative real numbers whose square is $|z|^2|w|^2$. By the uniqueness clause of Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4 they are equal. Finally $|\overline{z}| = \sqrt{a^2+(-b)^2} = \sqrt{a^2+b^2} = |z|$, since $(-b)^2 = b^2$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)).

(e) If $z = 0$, then $|z| = \sqrt{0} = 0$. Conversely, let $|z| = 0$, so $a^2+b^2 = |z|^2 = 0$. If $a \neq 0$, then $a^2 > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)) and $b^2 \geq 0$, so $a^2+b^2 > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5

(b)), a contradiction; hence $a = 0$. Then $b^2 = 0$, and the same rule gives $b = 0$. So $z = 0$. This proves the theorem.

■

The proof of (d) is our first use of a move that runs through the whole chapter: a statement about a modulus $|u|$ becomes a statement about $|u|^2 = u\overline{u}$, which is algebra; we compute there, and come back by taking non-negative square roots. Section 1.3 names it, *square the modulus*, and uses it to prove the triangle inequality.

Two remarks on what the theorem says. First, (a) and (b) say that conjugation respects sums and products, and it fixes 1. Not every reflection does: the reflection in the vertical axis, $z \mapsto -\overline{z}$, respects sums, but it sends 1 to -1, and $1 \cdot 1 = 1$ to -1, while the product of the images is $(-1)(-1) = 1$. Second, (d) says that the size of a product is the product of the sizes. In the plane picture, multiplying by w stretches every length by $|w|$; Section 1.5 completes this picture with angles.

1.2.3 Division

The first payoff is division. If $z \neq 0$, then $|z| \neq 0$ by (e), so $|z|^2$ is a **strictly** positive real number, and we may divide by it in $\mathbb{R}$.

Proposition 1.2.3. Inverse of a Complex Number

Let $z \in \mathbb{C}$ with $z \neq 0$. Then

$$w := \frac{1}{|z|^2}\,\overline{z}$$

satisfies $zw = 1$. We write z^{-1} or $\dfrac{1}{z}$ for this w.

Proof. Since $z \neq 0$, $|z| \neq 0$ by Theorem 1.2.2 (e), so $|z|^2 > 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e). In particular $|z|^2 \neq 0$, so it has an inverse $1/|z|^2$ in the field $\mathbb{R}$. By Proposition 1.1.2 and Theorem 1.2.2 (c),

$$zw = \frac{1}{|z|^2}\,(z\overline{z}) = \frac{1}{|z|^2}\,|z|^2 = 1,$$

where the last product is computed in $\mathbb{R}$, which gives the same result as in $\mathbb{C}$ (Proposition 1.1.1). This proves the proposition.

■

The hypothesis $z \neq 0$ is used exactly once, to make $|z|^2$ non-zero, so that $1/|z|^2$ exists. For $z = 0$ there is nothing to rescue: $0 \cdot w = 0 \neq 1$ for every w (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)). The proposition gives one inverse; that it is the only one is a fact about all fields, which we can cite as soon as we know that $\mathbb{C}$ is one.

Theorem 1.2.4. The Complex Numbers Form a Field

The set $\mathbb{C}$, with the operations of Definition 1.1.1, is a field in the sense of Number Systems:

From \(\nN\) to \(\nR\), Definition 2.3.1. Moreover $\mathbb{R} \subseteq \mathbb{C}$ (Proposition 1.1.1) is closed under the field operations of $\mathbb{C}$: for $a, c \in \mathbb{R}$, the sum $a + c$, the product ac, the negative $-a$ and, if $a \neq 0$, the inverse a^{-1}, computed in $\mathbb{C}$, are the real numbers computed in $\mathbb{R}$.

Proof. By Proposition 1.1.2 and the remark after it, $\mathbb{C}$ satisfies (F1)–(F7) and (F9), and $1 \neq 0$ in $\mathbb{C}$. By Proposition 1.2.3, every non-zero $z \in \mathbb{C}$ has an element z^{-1} with $zz^{-1} = 1$, which is (F8). So $\mathbb{C}$ is a field.

For $a, c \in \mathbb{R}$, the sum and product are those of $\mathbb{R}$ by Proposition 1.1.1. The real negative $-a$ satisfies $a + (-a) = 0$ in $\mathbb{R}$, hence in $\mathbb{C}$, so it is the negative of a in $\mathbb{C}$, by uniqueness of negatives (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)). If $a \neq 0$, the real inverse a^{-1} satisfies $aa^{-1} = 1$ in $\mathbb{R}$, hence in $\mathbb{C}$; and $a \neq 0$ in $\mathbb{C}$, since ι is injective. So a^{-1} is the inverse of a in $\mathbb{C}$, by uniqueness of inverses in the field $\mathbb{C}$ (Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (a)).

■

Everything proved for an arbitrary field now holds in $\mathbb{C}$, without a new proof. From Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1: the inverse z^{-1} is the **only** y with $zy = 1$, and $(zw)^{-1} = z^{-1}w^{-1}$ for non-zero z, w; fractions $z/w := zw^{-1}$ add and multiply by the usual rules; and $\mathbb{C}$ has **no zero divisors**: $zw = 0$ forces $z = 0$ or $w = 0$. By Proposition 1.1.3 (d), $z^n \neq 0$ whenever $z \neq 0$. These are the facts that the rest of the chapter uses when it cancels a non-zero factor.

Remark. Chapter 2 collects fields as a notion with many examples, finite and infinite. This theorem is the one it cites for $\mathbb{C}$, and $\mathbb{R} \subseteq \mathbb{C}$, with the closure just proved, is one of its examples of one field inside another.

In practice, a quotient is computed by "multiplying top and bottom by the conjugate". For $w \neq 0$, Proposition 1.2.3 gives

$$\frac{z}{w} = zw^{-1} = \frac{z\overline{w}}{|w|^2},$$

which is the fraction z/w multiplied by $\overline{w}/\overline{w} = 1$ (here $\overline{w} \neq 0$, since $|\overline{w}| = |w| \neq 0$ by Theorem 1.2.2 (d), (e)) and simplified with the product rule for fractions (Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (b)): the new denominator $w\overline{w} = |w|^2$ is real.

Example. Dividing Complex Numbers

Write $\dfrac{1}{3+4i}$ and $\dfrac{5+i}{1-i}$ in the form $a + bi$ with $a, b \in \mathbb{R}$.

Solution. For the first, $|3 + 4i|^2 = 25$ and $\overline{3 + 4i} = 3 - 4i$, so by Proposition 1.2.3

$$\frac{1}{3+4i} = \frac{3-4i}{25} = \frac{3}{25} - \frac{4}{25}i.$$

Check: $(3 + 4i)(3 - 4i) = 9 + 16 = 25$, so the product with $3 + 4i$ is $25/25 = 1$.

For the second, $|1-i|^2 = 2$ and $\overline{1-i} = 1+i$, so

$$\frac{5+i}{1-i} = \frac{(5+i)(1+i)}{2} = \frac{5+5i+i+i^2}{2} = \frac{4+6i}{2} = 2+3i.$$

This agrees with $(2+3i)(1-i) = 5+i$ from Example (First Computations in $\mathbb{C}$): since $1-i \neq 0$, the quotient is the **only** u with $u(1-i) = 5+i$. Indeed, if $u(1-i) = 5+i$, then $u = u \cdot 1 = u((1-i)(1-i)^{-1}) = (u(1-i))(1-i)^{-1} = (5+i)(1-i)^{-1}$, by (F7), (F8) and (F5) in the field $\mathbb{C}$ (Theorem 1.2.4).

Quick check. Compute $|(1+i)(1-i)|$ in two ways: by multiplying first, and by Theorem 1.2.2 (d). Then compute $1/i$.

Solution. Multiplying first, $(1+i)(1-i) = 1+1 = 2$, so the modulus is $|2| = 2$. By (d), it is $|1+i|\,|1-i| = \sqrt{2} \cdot \sqrt{2} = 2$, since $\sqrt{2}\sqrt{2} = (\sqrt{2})^2 = 2$. And $1/i = \bar{i}/|i|^2 = -i/1 = -i$; check: $i(-i) = -i^2 = 1$.

1.2.4 Exercises

1.2.4.1 A. Check your understanding

Exercise. A1

(a) Define the complex conjugate $\overline{z}$ and the modulus $|z|$ of $z = a+bi$, where $a, b \in \mathbb{R}$. Which earlier result guarantees that $|z|$ exists?

(b) True or false, with a reason: $z\overline{z}$ is a non-negative real number for every $z \in \mathbb{C}$.

(c) Where exactly is the hypothesis $z \neq 0$ used in the proof of Proposition 1.2.3?

(d) Write $1/(1+2i)$ in the form $a+bi$ with $a, b \in \mathbb{R}$.

Solution.

(a) $\overline{z} := a - bi$ and $|z| := \sqrt{a^2+b^2}$, the non-negative square root. It exists by Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4, since $\mathbb{R}$ is a complete ordered field and $a^2 + b^2 \geq 0$.

(b) True. By Theorem 1.2.2 (c), $z\overline{z} = |z|^2$, the square of a real number, and squares of real numbers are non-negative (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e) when $|z| \neq 0$, and $0^2 = 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) when $|z| = 0$).

(c) It gives $|z| \neq 0$ by Theorem 1.2.2 (e), hence $|z|^2 > 0$, so that $1/|z|^2$ exists in $\mathbb{R}$. Nowhere else.

(d) $|1+2i|^2 = 1+4 = 5$ and $\overline{1+2i} = 1-2i$, so $1/(1+2i) = (1-2i)/5 = \frac{1}{5} - \frac{2}{5}i$. Check: $(1+2i)(1-2i) = 5$.

1.2.4.2 B. Practice

Exercise. B1: Arithmetic

Write each of the following in the form $a + bi$ with $a, b \in \mathbb{R}$, or as a real number where indicated.

(a) $(3 - 2i)(4 + i)$.

(b) $\dfrac{1 + 2i}{2 - i}$.

(c) $|(3 + 4i)(5 - 12i)|$, without expanding the product.

(d) $\operatorname{Re} \dfrac{1}{1 + i}$ and $\operatorname{Im} \dfrac{1}{1 + i}$.

Solution.

(a) $(3 - 2i)(4 + i) = 12 + 3i - 8i - 2i^2 = 14 - 5i$.

(b) By Proposition 1.2.3, multiply by $\overline{2 - i} = 2 + i$ and divide by $|2 - i|^2 = 5$:

$$\frac{1 + 2i}{2 - i} = \frac{(1 + 2i)(2 + i)}{5} = \frac{2 + i + 4i + 2i^2}{5} = \frac{5i}{5} = i.$$

Check: $i(2 - i) = 2i - i^2 = 1 + 2i$.

(c) By Theorem 1.2.2 (d), $|(3 + 4i)(5 - 12i)| = |3 + 4i|\,|5 - 12i| = 5 \cdot 13 = 65$, since $|5 - 12i| = \sqrt{25 + 144} = \sqrt{169} = 13$ ($13 \geq 0$ and $13^2 = 169$).

(d) $\dfrac{1}{1 + i} = \dfrac{1 - i}{2} = \dfrac{1}{2} - \dfrac{1}{2}i$, so the real part is $1/2$ and the imaginary part is $-1/2$.

Exercise. B2

Let $z \in \mathbb{C}$. Prove:

(a) $\operatorname{Re} z = \dfrac{z + \overline{z}}{2}$ and $\operatorname{Im} z = \dfrac{z - \overline{z}}{2i}$;

(b) $z \in \mathbb{R}$ if and only if $\overline{z} = z$;

(c) $\operatorname{Re} z = 0$ if and only if $\overline{z} = -z$.

Solution. Write $z = a + bi$ with $a, b \in \mathbb{R}$.

(a) By Theorem 1.2.2 (c), $z + \overline{z} = 2a$, and $2 \neq 0$, so $(z + \overline{z})/2 = a = \operatorname{Re} z$. Also $z - \overline{z} = (a - a) + (b + b)i = 2bi$, and $2i \neq 0$, so $(z - \overline{z})/(2i) = (b(2i))(2i)^{-1} = b((2i)(2i)^{-1}) = b = \operatorname{Im} z$, using $2bi = b \cdot (2i)$ and (F5), (F8), (F7) in the field $\mathbb{C}$ (Theorem 1.2.4).

(b) $\overline{z} = z$ means $a - bi = a + bi$, which by comparing imaginary parts holds if and only if $-b = b$, that is $2b = 0$, that is $b = 0$ (as $2 \neq 0$ in $\mathbb{R}$). And $b = 0$ means $z = a \in \mathbb{R}$.

(c) $\overline{z} = -z$ means $a - bi = -a - bi$, which by comparing parts holds if and only if $a = -a$ (the imaginary parts agree), that is $2a = 0$, that is $a = 0$ (as in (b)).

Exercise. B3

Let $z, w \in \mathbb{C}$ with $w \neq 0$. Prove that $\overline{z/w} = \overline{z}/\overline{w}$ and $|z/w| = |z|/|w|$.

Hint: start from $w \cdot (z/w) = z$.

Solution. Let $q := z/w = zw^{-1}$, so $wq = z$. By Theorem 1.2.2 (b), $\overline{w}\,\overline{q} = \overline{z}$. Here $\overline{w} \neq 0$: $|\overline{w}| = |w| \neq 0$ by Theorem 1.2.2 (d), (e). Multiplying by $\overline{w}^{-1}$ gives $\overline{q} = \overline{z}/\overline{w}$.

Likewise, by Theorem 1.2.2 (d), $|w|\,|q| = |z|$, with $|w| \neq 0$ by (e). Dividing by $|w|$ in $\mathbb{R}$ gives $|q| = |z|/|w|$.

1.2.4.3 C. Going deeper

Exercise. C1: Exit check: the complex numbers form a field

Prove Theorem 1.2.2 (b) and (d) and Proposition 1.2.3, and conclude that $\mathbb{C}$ satisfies (F8). You may use Definition 1.1.1, Proposition 1.1.2, Proposition 1.1.1, Theorem 1.2.2 (c) and (e), and the rules of the ordered field $\mathbb{R}$, including Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4.

Solution. (b). Let $z = a+bi$, $w = c+di$. Then $zw = (ac-bd)+(ad+bc)i$, so $\overline{zw} = (ac-bd)-(ad+bc)i$. And $\overline{z}\,\overline{w} = (a-bi)(c-di) = (ac-(-b)(-d))+(-ad-bc)i = (ac-bd)-(ad+bc)i$. The two agree.

(d). By (c), (b), and commutativity and associativity of multiplication (Proposition 1.1.2 (a), (b)),

$$|zw|^2 = (zw)\overline{zw} = (zw)(\overline{z}\,\overline{w}) = (z\overline{z})(w\overline{w}) = |z|^2|w|^2 = \big(|z||w|\big)^2.$$

Both $|zw|$ and $|z||w|$ are non-negative ($|z||w|$ is 0 if a factor is 0, by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), and positive by (O4) of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.2 otherwise), so both are the non-negative square root of $|z|^2|w|^2$, and they are equal by the uniqueness clause of Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4. Also $|\overline{z}| = \sqrt{a^2+(-b)^2} = \sqrt{a^2+b^2} = |z|$.

Inverse. Let $z \neq 0$. By (e), $|z| \neq 0$, so $|z|^2 > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)), and $r := 1/|z|^2$ exists in $\mathbb{R}$. With $w := r\overline{z}$, Proposition 1.1.2 and (c) give $zw = r(z\overline{z}) = r|z|^2 = 1$, where the last product is computed in $\mathbb{R}$, which agrees with the product in $\mathbb{C}$ (Proposition 1.1.1).

(F8). Every non-zero $z \in \mathbb{C}$ has an element w with $zw = 1$, which is (F8) of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1.

Marking scheme. (10 points) - 2: (b) by expanding both sides in real and imaginary parts and comparing. - 3: (d) via $|zw|^2 = (zw)\overline{zw}$ and (b), with commutativity named for the reordering. - 1: equal non-negative squares give equal numbers, with a reason (uniqueness of the non-negative square root, or Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g) with trichotomy). - 2: $|z|^2 > 0$ for $z \neq 0$, with a reason. - 2: $zw = 1$ for $w = (1/|z|^2)\overline{z}$, and the conclusion stated as (F8). Fatal errors (0 for the step): dividing by z or by $|z|$ before showing it is non-zero; "$|zw| = |z||w|$ because the modulus is a length and multiplication scales lengths" (circular: the scaling picture is a consequence of (d)). A

second route to (d), expanding $(ac-bd)^2+(ad+bc)^2=(a^2+b^2)(c^2+d^2)$ and then taking square roots, earns the 3 points of the (d) step in full.

Exercise. C2: Gaussian rationals

Let $\mathbb{Q}(i) := \{a+bi : a,b \in \mathbb{Q}\} \subseteq \mathbb{C}$, where $\mathbb{Q} \subseteq \mathbb{R}$ as in *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 5 (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3). Prove that $\mathbb{Q}(i)$ is closed under addition, negatives, multiplication, inverses of non-zero elements, and conjugation.

Solution. Under the identification of q with $\kappa(q)$, κ sends sums, products, negatives and inverses of non-zero rationals to the same operations in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.4.1 (a), (c)), so the copy of $\mathbb{Q}$ in $\mathbb{R}$ is closed under $+$, $\cdot$, negatives and inverses of non-zero elements.

Let $z=a+bi$ and $w=c+di$ with $a,b,c,d \in \mathbb{Q}$. Then $z+w=(a+c)+(b+d)i$, $-z=(-a)+(-b)i$ and $zw=(ac-bd)+(ad+bc)i$ have rational parts, and so does $\overline{z}=a+(-b)i$. If $z \neq 0$, then $a^2+b^2=|z|^2 \neq 0$ by Theorem 1.2.2 (e), and $a^2+b^2 \in \mathbb{Q}$. By Proposition 1.2.3,

$$z^{-1}=\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}\,i,$$

whose parts are quotients of rational numbers by a non-zero rational number, hence rational. So all five operations stay in $\mathbb{Q}(i)$. For example, $(1+2i)^{-1}=\frac{1}{5}-\frac{2}{5}i \in \mathbb{Q}(i)$.

Chapter 2 calls a subset of a field a subfield when it contains 0 and 1 and has these closure properties. $\mathbb{Q}(i)$ contains $0=0+0i$ and $1=1+0i$, and it is one of the examples there.

Marking scheme. (10 points) - 2: the copy of $\mathbb{Q}$ in $\mathbb{R}$ is closed under $+$, $\cdot$, negatives and inverses of non-zero elements, with a reason (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.4.1 (a), (c)). - 2: $z+w$, $-z$ and $\overline{z}$ have rational real and imaginary parts. - 2: $zw=(ac-bd)+(ad+bc)i$ has rational parts. - 3: for $z \neq 0$, a^2+b^2 is non-zero (Theorem 1.2.2 (e)) and rational, and the formula of Proposition 1.2.3 then gives rational parts. - 1: the conclusion that all five operations stay in $\mathbb{Q}(i)$. Fatal errors (0 for the step): dividing by a^2+b^2 without first using $z \neq 0$ to show it is non-zero; assuming without a reason that $\mathbb{Q} \subseteq \mathbb{R}$ is closed under the operations.

1.3 The Triangle Inequality

The modulus of Section 1.2 measures a complex number by a real one. Picture $z=a+bi$ as the point (a,b) of the plane: by Pythagoras, $|z|=\sqrt{a^2+b^2}$ is its distance from the origin, and $|z-w|$ is the distance between the points z and w. In a triangle, one side is never longer than the other two together. This section proves the algebraic form of that fact, $|z+w| \leq |z|+|w|$, from the definitions alone. The picture motivates it; no step of the proof uses it.

1.3.1 Why the old proof does not transfer

For an ordered field, *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 4 proved $|x+y| \leq |x|+|y|$ by trapping (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (e)). Each of x and y

lies between $\pm$ its absolute value, $-|x| \le x \le |x|$ (part (c) there); adding the two traps traps $x+y$ between $\pm(|x|+|y|)$, and part (d) reads that as the inequality.

That route needs $x \le |x|$: a comparison between x itself and a number. For a complex z, "$z \le |z|$" compares a complex number with a real one, and $\mathbb{C}$ has been given no order in which to make the comparison. Section 1.4 shows that no order compatible with the arithmetic of $\mathbb{C}$ exists (Proposition 1.4.3). So the proof must compare **real** numbers only.

Two kinds of real number are at hand. Moduli are real, and so are real parts. The device that connects them to the arithmetic of $\mathbb{C}$ is the identity $|u|^2 = u\overline{u}$ of Theorem 1.2.2 (c). A modulus is a square root, and square roots do not add well; its square is a product, and products expand. So we will compare squares and then come back.

Comparing squares. Coming back from squares to the numbers needs one rule about the real numbers. Let $p, q \in \mathbb{R}$ with $p \ge 0$ and $q \ge 0$. Then

$$p \le q \iff p^2 \le q^2, \qquad p = q \iff p^2 = q^2,$$

and likewise with $<$ on both sides. The strict form is Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g). For the first equivalence: if $p < q$, then $p^2 < q^2$ by (g), and if $p = q$ the squares agree. Conversely, if $p^2 \le q^2$ and yet $q < p$, then (g) gives $q^2 < p^2$, which contradicts $p^2 \le q^2$ by trichotomy (O1); so $p \le q$. The second equivalence follows from the first, applied in both directions, and trichotomy. In words: *for non-negative reals, squaring neither creates nor destroys a comparison.* Both hypotheses $p \ge 0$ and $q \ge 0$ matter: $(-2)^2 > 1^2$, and yet $-2 < 1$.

1.3.2 The real part is at most the modulus

The single estimate the proof needs is that a real part never exceeds the modulus. It comes with two companions, which say that the modulus and the "taxicab size" $|\operatorname{Re} u| + |\operatorname{Im} u|$ are comparable.

Lemma 1.3.1. Real and Imaginary Parts against the Modulus

For every $u \in \mathbb{C}$,

$$|\operatorname{Re} u| \le |u|, \qquad |\operatorname{Im} u| \le |u|, \qquad |u| \le |\operatorname{Re} u| + |\operatorname{Im} u|.$$

In particular $\operatorname{Re} u \le |u|$.

Here $|\operatorname{Re} u|$ is the absolute value of a real number. By Proposition 1.2.1 it is the same whether it is read as the absolute value of the ordered field $\mathbb{R}$ from *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 4 (Number Systems: From \(\nN\) to \(\nR\), Definition 4.1.1) or as the modulus of a complex number that happens to be real, so the lemma has only one reading.

Idea. Every quantity in the lemma is a non-negative real, so compare squares. The square of $|u|$ is $x^2 + y^2$, and the squares of $|x|$ and $|y|$ are x^2 and y^2, each at most the sum; the square of $|x| + |y|$ is the sum plus the non-negative cross term $2|x||y|$.

Proof. Write $u = x + yi$ with $x, y \in \mathbb{R}$. By Definition 1.2.1 and the defining property of the square root (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), $|u| \geq 0$ and $|u|^2 = x^2 + y^2$.

Since $y^2 \geq 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e) if $y \neq 0$; $0^2 = 0$ otherwise), adding x^2 gives $x^2 \leq x^2 + y^2$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b). Also $|x|^2 = x^2$ and $|x| \geq 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (a), (b)). Hence $|x|^2 \leq |u|^2$, with both $|x|$ and $|u|$ non-negative, and comparing squares gives $|x| \leq |u|$. The same argument with the roles of x and y exchanged gives $|y| \leq |u|$. Then $\operatorname{Re} u = x \leq |x|$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (c), so $\operatorname{Re} u \leq |u|$.

For the last inequality, expand with Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d):

$$\begin{aligned}\big(|x| + |y|\big)^2 &= |x|^2 + 2|x||y| + |y|^2 \\ &= x^2 + y^2 + 2|x||y| \geq x^2 + y^2 = |u|^2,\end{aligned}$$

where the inequality holds because $|x||y| \geq 0$ as a product of non-negative reals, so $2|x||y| \geq 0$, and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b) adds it. Both $|x| + |y|$ and $|u|$ are non-negative, so comparing squares gives $|u| \leq |x| + |y|$. This proves the lemma.

■

For $u = 3 - 4i$ the three inequalities read $3 \leq 5$, $4 \leq 5$ and $5 \leq 7$. For $u = 2$ they read $2 \leq 2$, $0 \leq 2$ and $2 \leq 2$: a real u makes the first and third equalities. The inequality $\operatorname{Re} u \leq |u|$ is strict for $u = -1$, where it reads $-1 \leq 1$; the absolute value inside the first inequality is what makes it sharp for real u of either sign.

Quick check. Find a non-zero $u \in \mathbb{C}$ with $\operatorname{Re} u = 0$. What do the three inequalities of Lemma 1.3.1 say for it?

Solution. For example $u = 2i$, with $\operatorname{Re} u = 0$, $\operatorname{Im} u = 2$ and $|u| = \sqrt{0 + 4} = 2$. The inequalities read $0 \leq 2$, $2 \leq 2$ and $2 \leq 0 + 2$. Any $u = yi$ with $y \neq 0$ works the same way: $|u| = |y|$, so the second and third inequalities are equalities.

1.3.3 The triangle inequality

We can now state the theorem. Its proof is the first full run of the move this chapter is built around.

Theorem 1.3.2. Triangle Inequality for Complex Numbers

For all $z, w \in \mathbb{C}$,

$$|z + w| \leq |z| + |w|.$$

Try it first (ten minutes): show $|z + w|^2 \leq (|z| + |w|)^2$ by expanding both sides with $|u|^2 = u\bar{u}$, and note which term you cannot yet bound.

Idea. Expanding the left side with $|u|^2 = u\overline{u}$ and conjugation of sums gives $|z|^2 + z\overline{w} + \overline{z}w + |w|^2$; the right side is $|z|^2 + 2|z||w| + |w|^2$. Everything matches except the cross term $z\overline{w} + \overline{z}w$, and an attempt usually stops there: it looks like a complex number, and complex numbers cannot be compared with $2|z||w|$. The way out is to notice that $\overline{z}w$ is the conjugate of $z\overline{w}$, so the cross term is $u + \overline{u} = 2\operatorname{Re} u$ with $u = z\overline{w}$: a **real** number after all. A real part is at most the modulus, and $|z\overline{w}| = |z||w|$. Squares compare, so the moduli do.

Before reading on: where is $\operatorname{Re} u \leq |u|$ *used, and why may we compare squares?*

Proof. Let $z, w \in \mathbb{C}$. By Theorem 1.2.2 (c), then (a), then Proposition 1.1.2 (c) together with (a) and (b) (distributivity, commutativity, associativity),

$$\begin{aligned} |z+w|^2 &= (z+w)\,\overline{(z+w)} = (z+w)(\overline{z}+\overline{w}) \\ &= z\overline{z} + z\overline{w} + \overline{z}w + w\overline{w}. \end{aligned}$$

By Theorem 1.2.2 (b) and (a), $\overline{z\overline{w}} = \overline{z}\,\overline{\overline{w}} = \overline{z}w$. So with $u := z\overline{w}$, the two middle terms are $u + \overline{u} = 2\operatorname{Re} u$, by Theorem 1.2.2 (c). Using (c) once more for $z\overline{z}$ and $w\overline{w}$,

$$|z+w|^2 = |z|^2 + 2\operatorname{Re}(z\overline{w}) + |w|^2.$$

Every term here is real, and sums and products of real numbers are the same in $\mathbb{C}$ as in $\mathbb{R}$ (Proposition 1.1.1), so the inequalities below take place in the ordered field $\mathbb{R}$. By Lemma 1.3.1, $\operatorname{Re}(z\overline{w}) \leq |z\overline{w}|$, and by Theorem 1.2.2 (d), $|z\overline{w}| = |z|\,|\overline{w}| = |z|\,|w|$. Adding this inequality to itself ($2a = (1+1)a = a + a$ by distributivity) and then adding $|z|^2 + |w|^2$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b) twice), and expanding the square with Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d),

$$|z+w|^2 \leq |z|^2 + 2|z||w| + |w|^2 = \big(|z| + |w|\big)^2.$$

Both $|z+w|$ and $|z|+|w|$ are non-negative real numbers, so comparing squares gives $|z+w| \leq |z| + |w|$. This proves the triangle inequality.

■

The proof answers its prompt in two lines. $\operatorname{Re} u \leq |u|$ is used once, to bound the cross term $2\operatorname{Re}(z\overline{w})$ by $2|z\overline{w}|$. Comparing squares is legitimate because the two quantities being compared, $|z+w|$ and $|z| + |w|$, are both non-negative; without that, a smaller square would say nothing about the numbers.

This route has a name in this chapter: **square the modulus**. *The modulus is a square root, and square roots are hard to handle; its square* $|u|^2 = u\overline{u}$ *is a product, so square, expand with conjugates, bound or compare the real numbers you get, and take the non-negative square root back.* Section 1.2 used the same move once already, for $|zw| = |z||w|$ (Theorem 1.2.2 (d)). The linear algebra volumes take the same route, square, expand, bound the cross term, for the length of a vector in an inner product space.

Warning. The square of the modulus is $u\overline{u}$, not u^2. Expanding $|z+w|^2$ as $(z+w)^2 = z^2 + 2zw + w^2$ gives nonsense: for $z = w = i$, $(z+w)^2 = (2i)^2 = -4$, while $|z+w|^2 = |2i|^2 = 4$. The cross term of the correct expansion is $z\overline{w} + \overline{z}w$, and only that form is real.

Remark. The inequality can be strict: for $z = 1$ and $w = -1$, the left side is $|0| = 0$ and the right side is 2. For real z, w, every modulus in the statement is the absolute value of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 4 (Proposition 1.2.1), and the theorem is Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (e), reached by a different route.

Quick check. Compute $|3+4i|+|-3+4i|$ and $|(3+4i)+(-3+4i)|$, and check them against the triangle inequality.

Solution. $|3+4i| = \sqrt{9+16} = 5$ and $|-3+4i| = \sqrt{9+16} = 5$, so the right side is 10. The sum is $8i$, and $|8i| = \sqrt{0+64} = 8$. Indeed $8 \le 10$. In the picture, the two points and $8i$ are three corners of a parallelogram with the origin as the fourth, and the diagonal 8 is shorter than the two sides $5+5$.

1.3.4 Three variants

Three consequences are used often enough to be stated once: a lower bound for the modulus of a difference, the inequality for any finite number of terms, and a lower bound for the modulus of a sum.

Corollary 1.3.3. Variants of the Triangle Inequality

Let $z, w \in \mathbb{C}$.

(a) *(Reverse triangle inequality.)* $||z| - |w|| \le |z - w|$.

(b) For every $n \in \mathbb{N}$ with $n \ge 1$ and all $z_1, \dots, z_n \in \mathbb{C}$, $\left|\sum_{k=1}^{n} z_k\right| \le \sum_{k=1}^{n} |z_k|$.

(c) $|z| - |w| \le |z + w|$.

In (a), the outer bars are the absolute value of the real number $|z| - |w|$. In words: (a) says that two points at distance $|z-w|$ from each other have distances from the origin that differ by at most that much; (b) says that a path of n steps is at least as long as the straight line from start to end; (c) says that adding w can lower the modulus by at most $|w|$.

Idea. For (a), split z as $(z - w) + w$ and apply the theorem; that bounds $|z| - |w|$ from above, and swapping z and w bounds it from below. For (b), add one term at a time. For (c), apply (a) to z and $-w$.

Proof.

(a) Since $z = (z - w) + w$, Theorem 1.3.2 gives $|z| \le |z - w| + |w|$, so $|z| - |w| \le |z - w|$. Exchanging z and w gives $|w| - |z| \le |w - z|$. Moreover $w - z = (-1)(z - w)$, so by Theorem 1.2.2 (d), $|w-z| = |-1|\,|z-w| = |z-w|$, where $|-1| = 1$ by Proposition 1.2.1. Let $t := |z| - |w| \in \mathbb{R}$. We have shown $t \le |z - w|$ and $-t \le |z - w|$, that is,

$-|z-w| \le t \le |z-w|$: if $-t < |z-w|$, then $-|z-w| < -(-t) = t$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (a) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a), and if $-t = |z-w|$, then $-|z-w| = -(-t) = t$. By Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (d), $|t| \le |z-w|$.

(b) By induction on $n \ge 1$ (Logic and Proof, Axiom 4.2.1, through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b), applied to the statement for $n = m+1$, $m \in \mathbb{N}$), with the sums defined by appending the last term, as for real sums (Sets, Relations, and Cardinality, Definition 2.3.1). For $n = 1$, both sides are $|z_1|$. Suppose the inequality holds for n, and let $z_1, \dots, z_{n+1} \in \mathbb{C}$. Then

$$\begin{aligned}\left|\sum_{k=1}^{n+1} z_k\right| &= \left|\sum_{k=1}^{n} z_k + z_{n+1}\right| \le \left|\sum_{k=1}^{n} z_k\right| + |z_{n+1}| \\ &\le \sum_{k=1}^{n} |z_k| + |z_{n+1}| = \sum_{k=1}^{n+1} |z_k|,\end{aligned}$$

by Theorem 1.3.2, then the induction hypothesis with Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b).

(c) Apply (a) to z and $-w$. Since $z - (-w) = z + w$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)) and $|-w| = |-1||w| = |w|$ as in (a), it reads $||z| - |w|| \le |z+w|$. By Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (c), $|z| - |w| \le ||z| - |w||$. This proves the corollary.

■

Part (b) with $n = 2$ is the theorem itself, so the corollary contains it. Chapter 5 uses (b) and (c) to show that a polynomial expression of degree at least 1 is large in modulus when $|z|$ is large, a step towards the Fundamental Theorem of Algebra.

Quick check. Take $z = 5$ and $w = 3i$. Compute both sides of (a) and of (c).

Solution. $|z| = 5$ and $|w| = 3$, so $|z| - |w| = 2$. For (a): $|z - w| = |5 - 3i| = \sqrt{34}$, and $2 \le \sqrt{34}$ because $2^2 = 4 \le 34$ (comparing squares). For (c): $|z + w| = |5 + 3i| = \sqrt{34}$ too, and again $2 \le \sqrt{34}$. Both bounds are far from sharp here; (a) is an equality when $w = 0$, for instance.

1.3.5 Exercises

1.3.5.1 A. Check your understanding

Exercise. A1

These questions are about the proof of Theorem 1.3.2.

(a) Where in the proof is $\operatorname{Re} u \le |u|$ used, and for which u?

(b) Why may the proof pass from $|z+w|^2 \le (|z| + |w|)^2$ back to $|z+w| \le |z| + |w|$?

(c) Run the proof on $z = 3$ and $w = 4i$: compute the cross term $2\operatorname{Re}(z\overline{w})$, then both sides

of the squared inequality.

(d) State the idea of the proof in two sentences.

(e) True or false: $|z+w| = |z| + |w|$ for all $z, w \in \mathbb{C}$. Justify your answer.

Solution.

(a) Once, to bound the cross term: with $u = z\overline{w}$, $2\,\mathrm{Re}(z\overline{w}) \leq 2|z\overline{w}|$.

(b) Both $|z+w|$ and $|z|+|w|$ are non-negative reals, and for non-negative reals $p \leq q$ if and only if $p^2 \leq q^2$ (comparing squares, from Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g) and trichotomy).

(c) $\overline{w} = -4i$, so $z\overline{w} = 3 \cdot (-4i) = -12i$, with real part 0: the cross term is 0. Then $|z+w|^2 = 9 + 0 + 16 = 25$ and $(|z| + |w|)^2 = (3+4)^2 = 49$, and $25 \leq 49$. So $|3+4i| = 5 \leq 7$.

(d) Square both sides and expand with $|u|^2 = u\overline{u}$: everything matches except the cross term, which is $2\,\mathrm{Re}(z\overline{w})$. A real part is at most the modulus, and $|z\overline{w}| = |z||w|$, so the squares compare, and so do the non-negative moduli.

(e) False. For $z = 1$ and $w = -1$, $|z+w| = 0$, but $|z| + |w| = 2$.

1.3.5.2 B. Practice

Exercise. B1: The equality case

Let $z, w \in \mathbb{C}$. Prove that $|z+w| = |z| + |w|$ if and only if $z\overline{w}$ is a non-negative real number, that is, $\mathrm{Im}(z\overline{w}) = 0$ and $\mathrm{Re}(z\overline{w}) \geq 0$.

Hint: trace the proof of the triangle inequality and ask where an inequality could be strict.

Solution. Let $u \coloneqq z\overline{w} = x + yi$ with $x, y \in \mathbb{R}$. By the proof of Theorem 1.3.2,

$$|z+w|^2 = |z|^2 + 2x + |w|^2,$$
$$(|z| + |w|)^2 = |z|^2 + 2|u| + |w|^2,$$

the second because $|z||w| = |u|$ (Theorem 1.2.2 (d)). Both moduli are non-negative, so (comparing squares) $|z+w| = |z| + |w|$ holds if and only if the squares are equal, that is, if and only if $2x = 2|u|$, that is, $x = |u|$.

It remains to show that $x = |u|$ holds exactly when $y = 0$ and $x \geq 0$. If $x = |u|$, then $x \geq 0$, and squaring gives $x^2 = x^2 + y^2$, so $y^2 = 0$ and $y = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e): a non-zero square is positive). Conversely, if $y = 0$ and $x \geq 0$, then $|u| = \sqrt{x^2} = x$, since $x \geq 0$ and $x^2 = x^2$ (uniqueness in Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4). Hence $|z+w| = |z| + |w|$ if and only if $z\overline{w}$ is a non-negative real number.

For instance $z = 1+i$, $w = 2+2i$: $z\overline{w} = (1+i)(2-2i) = 4 \geq 0$, and indeed $|3+3i| = \sqrt{18} = 3\sqrt{2} = \sqrt{2} + 2\sqrt{2} = |1+i| + |2+2i|$. In the picture: equality holds exactly when one of z, w is 0 or they point in the same direction from the origin. The linear algebra volumes prove the version for n terms.

Exercise. B2: A distance that does not change

Let $z \in \mathbb{C}$ with $|z| = 1$. Prove that $|z - w| = |1 - \overline{z}w|$ for every $w \in \mathbb{C}$. The first two steps are done:

$$|z - w|^2 = |z|^2 - z\overline{w} - \overline{z}w + |w|^2,$$
$$|1 - \overline{z}w|^2 = 1 - z\overline{w} - \overline{z}w + |z|^2|w|^2,$$

both by expanding $u\overline{u}$ with Theorem 1.2.2. *Name the move, then complete it.*

Solution. The move is **square the modulus**: compare the squares, which are algebra, and take the non-negative square roots back.

Substitute $|z|^2 = 1$ into both lines. The first becomes $1 - z\overline{w} - \overline{z}w + |w|^2$, and so does the second, since $|z|^2|w|^2 = |w|^2$. So $|z - w|^2 = |1 - \overline{z}w|^2$. Both $|z - w|$ and $|1 - \overline{z}w|$ are non-negative, and non-negative reals with equal squares are equal (comparing squares). Hence $|z - w| = |1 - \overline{z}w|$.

(For the record, the given lines. Conjugation respects differences: $\overline{-v} = \overline{(-1)v} = \overline{-1}\,\overline{v} = -\overline{v}$ by Theorem 1.2.2 (b), Proposition 1.2.1 and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c), so with (a), $\overline{u - v} = \overline{u} - \overline{v}$; and $\overline{1} = 1$ by Proposition 1.2.1. Then $(z - w)(\overline{z} - \overline{w}) = z\overline{z} - z\overline{w} - w\overline{z} + w\overline{w}$, and $\overline{1 - \overline{z}w} = 1 - z\overline{w}$, so $(1 - \overline{z}w)(1 - z\overline{w}) = 1 - z\overline{w} - \overline{z}w + (z\overline{z})(w\overline{w})$.)

Exercise. B3

Prove that $|z| \le |\operatorname{Re} z| + |\operatorname{Im} z| \le \sqrt{2}\,|z|$ for every $z \in \mathbb{C}$, and, for each of the two inequalities, find a non-zero z for which it is an equality.

Solution. The first inequality is the last part of Lemma 1.3.1. For the second, write $z = x + yi$. Both sides are non-negative ($\sqrt{2} \ge 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), so it suffices to compare squares. The right side squared is $(\sqrt{2})^2|z|^2 = 2(x^2 + y^2)$, and the left side squared is $x^2 + 2|x||y| + y^2$, using $|x|^2 = x^2$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (b)). Their difference is

$$\begin{aligned} 2(x^2 + y^2) - (x^2 + 2|x||y| + y^2) &= |x|^2 - 2|x||y| + |y|^2 \\ &= (|x| - |y|)^2 \ge 0, \end{aligned}$$

a square in the ordered field $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)). So $(|x| + |y|)^2 \le 2|z|^2$, and $|x| + |y| \le \sqrt{2}\,|z|$.

Equality: $z = 1$ gives $1 = 1 + 0$ in the first; $z = 1 + i$ gives $1 + 1 = 2 = \sqrt{2} \cdot \sqrt{2}$ in the second.

1.3.5.3 C. Going deeper

Exercise. C1: Exit check: the triangle inequality

State and prove the triangle inequality for complex numbers. Your proof must include a proof that $\operatorname{Re} u \le |u|$ for every $u \in \mathbb{C}$.

Solution. Statement. For all $z, w \in \mathbb{C}$, $|z + w| \leq |z| + |w|$.

The estimate. Let $u = x + yi$ with $x, y \in \mathbb{R}$. Then $|u|^2 = x^2 + y^2 \geq x^2 = |x|^2$, since $y^2 \geq 0$. Both $|x|$ and $|u|$ are non-negative, so $|x| \leq |u|$ by comparing squares (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g) with trichotomy). Hence $\operatorname{Re} u = x \leq |x| \leq |u|$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (c)).

The inequality. Let $z, w \in \mathbb{C}$. By Theorem 1.2.2 (a)–(c),

$$\begin{aligned} |z + w|^2 &= (z + w)(\overline{z} + \overline{w}) = |z|^2 + (z\overline{w} + \overline{z\overline{w}}) + |w|^2 \\ &= |z|^2 + 2\operatorname{Re}(z\overline{w}) + |w|^2. \end{aligned}$$

By the estimate and Theorem 1.2.2 (d), $2\operatorname{Re}(z\overline{w}) \leq 2|z\overline{w}| = 2|z||w|$. Hence $|z+w|^2 \leq (|z| + |w|)^2$. Both $|z+w|$ and $|z|+|w|$ are non-negative, so comparing squares gives $|z+w| \leq |z|+|w|$.

Marking scheme. (10 points) - 2: proves $\operatorname{Re} u \leq |u|$, with a reason for passing from squares to moduli. - 3: expands $|z + w|^2$ with conjugates and identifies the cross term as $2\operatorname{Re}(z\overline{w})$, a real number. - 2: bounds the cross term by $2|z||w|$, citing $|z\overline{w}| = |z||w|$. - 1: concludes $|z+w|^2 \leq (|z|+|w|)^2$. - 2: takes square roots, justified by the non-negativity of both sides. A second route, with coordinates $z = a+bi$, $w = c+di$: expanding $(a+c)^2+(b+d)^2$ and isolating the cross term $2(ac + bd)$ earns the 3 points of the second line; proving $ac + bd \leq |z||w|$, for instance from $(ac + bd)^2 \leq (a^2 + b^2)(c^2 + d^2)$, which follows from $(ad - bc)^2 \geq 0$, earns the 2 points of the third line if proved, not if quoted; the last two lines are marked as above. The 2 points for $\operatorname{Re} u \leq |u|$ are still owed on that route, since the problem asks for it. Fatal errors (0 for the step): writing $z \leq |z|$ or any inequality between non-real complex numbers; dropping the conjugate, as in $|u|^2 = u^2$.

Exercise. C2: Inside the unit disc

Let $z, w \in \mathbb{C}$ with $|z| < 1$ and $|w| < 1$. Prove that $|z - w| < |1 - \overline{z}w|$. Here is the start of a proof: square both sides and expand. *Name the move, then complete it.*

Solution. The move is **square the modulus**. Both sides are non-negative, so it is enough to show $|z - w|^2 < |1 - \overline{z}w|^2$ (comparing squares, strict form: Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g)). Expanding each as $u\overline{u}$, exactly as in Exercise (B2: A distance that does not change),

$$\begin{aligned} |z - w|^2 &= |z|^2 - z\overline{w} - \overline{z}w + |w|^2, \\ |1 - \overline{z}w|^2 &= 1 - z\overline{w} - \overline{z}w + |z|^2|w|^2. \end{aligned}$$

The non-real terms cancel in the difference:

$$\begin{aligned} |1 - \overline{z}w|^2 - |z - w|^2 &= 1 - |z|^2 - |w|^2 + |z|^2|w|^2 \\ &= (1 - |z|^2)(1 - |w|^2). \end{aligned}$$

Since $0 \leq |z| < 1$, comparing squares gives $|z|^2 < 1^2 = 1$, so $1 - |z|^2 > 0$; likewise $1 - |w|^2 > 0$. A product of two positive reals is positive ((O4)). So the difference is positive, $|z - w|^2 < |1 - \overline{z}w|^2$, and $|z - w| < |1 - \overline{z}w|$.

In particular $1-\overline{z}w \neq 0$. Since $|1-\overline{z}w| = |1-z\overline{w}|$ (a modulus is unchanged by conjugation, Theorem 1.2.2 (d)), the inequality says that $|z-w|/|1-\overline{w}z| < 1$ for all z, w in the open unit disc: the map $z \mapsto (z-w)/(1-\overline{w}z)$ sends the open unit disc into itself, a fact complex analysis builds on.

Marking scheme. (10 points) - 2: reduces to the squared inequality, with the non-negativity of both sides as the reason. - 3: expands both squares with conjugates. - 3: factors the difference as $(1-|z|^2)(1-|w|^2)$. - 2: shows both factors positive, from $|z|, |w| < 1$, and concludes strictly. Fatal errors (0 for the step): expanding $|z-w|^2$ as $(z-w)^2$; comparing $z\overline{w}$ with a real number.

1.4 Square Roots, Quadratic Equations, and the Missing Order

Logic and Proof, Section 4.11 needed, in one of its checks, the fact that every complex number has a complex square root, and took it there as a school fact about polar form. This section proves it, with no angles at all: a square root of a complex number is built from two square roots of non-negative reals, which *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 6 provides (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4). The quadratic formula follows, for complex coefficients. Then we see what $\mathbb{C}$ has lost on the way from $\mathbb{R}$: it has no order compatible with its arithmetic, and the rule $\sqrt{x}\sqrt{y} = \sqrt{xy}$ has no complex version.

1.4.1 Square roots from real square roots

The question is: given $z = a + bi$, find $w = x + yi$ with $w^2 = z$. Since $w^2 = (x^2 - y^2) + 2xyi$, comparing real and imaginary parts turns the question into two real equations,

$$x^2 - y^2 = a, \qquad 2xy = b.$$

The answer is an explicit formula in a, b and $|z|$.

Proposition 1.4.1. Square Roots of Complex Numbers

Let $z = a + bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$ and $z \neq 0$, and let $r := |z|$. Put $s := 1$ if $b \geq 0$ and $s := -1$ if $b < 0$, and

$$x := \sqrt{\frac{r+a}{2}}, \qquad y := s\sqrt{\frac{r-a}{2}}, \qquad w := x + yi.$$

Then:

(a) $w^2 = z$;

(b) for $u \in \mathbb{C}$, $u^2 = z$ if and only if $u = w$ or $u = -w$;

(c) $w \neq -w$.

For $z = 0$: $u^2 = 0$ if and only if $u = 0$.

In words: every non-zero complex number has ***exactly two*** *square roots, w and $-w$, and the formula finds one of them; 0 has exactly one.*

Try it first (ten minutes): find w with $w^2 = 3 + 4i$ by writing $w = x + yi$. What do you do with the two equations you get?

Idea. For $3+4i$ the two equations are $x^2-y^2=3$ and $2xy=4$. The natural attempt eliminates $y=2/x$ and arrives at $x^4-3x^2-4=0$, a quartic; it can be solved, but it hides what is going on, and in general it needs the quadratic formula before we have it. The missing piece is a **third** equation, and it comes from the modulus. If $w^2=z$, then $|w|^2=|w^2|=|z|$ by Theorem 1.2.2 (d), that is, $x^2+y^2=r$. Now the first equation and the third give x^2 and y^2 by adding and subtracting: $x^2=(r+a)/2$, $y^2=(r-a)/2$. That fixes x and y up to sign, and the second equation $2xy=b$ says which signs go together: xy has the sign of b. For $3+4i$: $r=5$, $x^2=4$, $y^2=1$, $xy>0$, so $w=\pm(2+i)$.

The proof runs this forward: define x and y by the formulas, check $w^2=z$, and get "only $\pm w$" from the field axioms.

Before reading on: why does the sign of b decide whether x and y have the same sign?

The proof uses one small rule about real square roots: for $p,q\in\mathbb{R}$ with $p,q\geq 0$,

$$\sqrt{p}\,\sqrt{q}=\sqrt{pq}.$$

Both sides are non-negative (a product of non-negative reals is non-negative), and the square of the left side is $(\sqrt{p})^2(\sqrt{q})^2=pq$, by commutativity; so the left side is the non-negative number whose square is pq, which is the right side by the uniqueness in Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4. The rule is about non-negative **reals** only; the last part of this section shows that it has no complex version.

Proof. *The roots exist.* By Lemma 1.3.1, $|a|=|\operatorname{Re} z|\leq r$, so $-r\leq a\leq r$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (d)). Hence $r+a\geq 0$ and $r-a\geq 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (a), (b)). Halving keeps this: for $p\geq 0$, either $p>0$ and then $p/2>0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.2 (b), with $\varepsilon=p$), or $p=0$ and then $p/2=0\cdot(1/2)=0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)). So $(r+a)/2\geq 0$ and $(r-a)/2\geq 0$. So the two square roots in the definition of x and y exist (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4).

(a) Since $s^2=1$,

$$x^2-y^2=\frac{r+a}{2}-s^2\frac{r-a}{2}=\frac{r+a}{2}-\frac{r-a}{2}=a.$$

For the imaginary part, the rule for real square roots gives

$$\begin{aligned}2xy&=2s\sqrt{\frac{r+a}{2}}\sqrt{\frac{r-a}{2}}=2s\sqrt{\frac{r^2-a^2}{4}}\\&=s\sqrt{r^2-a^2}=s\sqrt{b^2}=s|b|=b.\end{aligned}$$

Here the third equality is $2\sqrt{t/4}=\sqrt{4}\sqrt{t/4}=\sqrt{t}$, by the same rule and $\sqrt{4}=2$; the fourth uses $r^2=a^2+b^2$ (Definition 1.2.1); the fifth holds because $|b|\geq 0$ and $|b|^2=b^2$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (a), (b)), with uniqueness in Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4; and the last because $s|b|=b$ by the definitions of s and of $|b|$ (Number Systems: From \(\nN\) to \(\nR\), Definition 4.1.1), in each of the two cases $b\geq 0$ and $b<0$. Hence $w^2=(x^2-y^2)+2xyi=a+bi=z$, by the multiplication rule of Definition 1.1.1.

(b) Let $u\in\mathbb{C}$. Since $\mathbb{C}$ is a commutative ring, $(u-w)(u+w)=u^2-w^2$ (Proposition 1.1.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)). If $u^2=z$, then

$u^2 - w^2 = z - z = 0$ by (a), so $(u-w)(u+w) = 0$. Since $\mathbb{C}$ is a field (Theorem 1.2.4), it has no zero divisors (Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d)), so $u - w = 0$ or $u + w = 0$, that is, $u = w$ or $u = -w$. Conversely $w^2 = z$ by (a), and $(-w)^2 = w^2 = z$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c).

(c) First $w \neq 0$, since $w^2 = z \neq 0$ and $0^2 = 0$. Suppose $w = -w$. Then $2w = w + w = 0$. But $2 = 1 + 1 \neq 0$ in $\mathbb{C}$: it is the real number 2, which is positive in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h)), and $\mathbb{R} \subseteq \mathbb{C}$ by the injective embedding of Proposition 1.1.1. So $2w = 0$ with $2 \neq 0$ and $w \neq 0$ contradicts the absence of zero divisors. Hence $w \neq -w$.

Finally, for $z = 0$: $0^2 = 0$, and if $u^2 = u \cdot u = 0$, then $u = 0$ by Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d). This proves the proposition.

■

The answer to the prompt: x is non-negative by construction, and y is s times a non-negative number, so xy is s times a non-negative number, and $2xy$ must equal b. If $b > 0$, then x and y must both be non-zero with the same sign; if $b < 0$, opposite signs. When $b = 0$ the choice of s does not matter, because then one of x, y is 0.

The proposition proves what *Logic and Proof*, Section 4.11 assumed, and it is stronger: it counts the roots. It uses only the field $\mathbb{C}$, its modulus, and square roots of non-negative reals; no angle, cosine or sine appears. That matters later: Chapter 5 proves the Fundamental Theorem of Algebra using square roots in exactly this form.

Example. Square Roots of $5 - 12i$

Find all $w \in \mathbb{C}$ with $w^2 = 5 - 12i$.

Solution. Write $w = x + yi$ with $x, y \in \mathbb{R}$. Comparing real and imaginary parts in $(x^2 - y^2) + 2xyi = 5 - 12i$ gives

$$x^2 - y^2 = 5 \qquad \text{and} \qquad xy = -6.$$

Taking moduli, by Theorem 1.2.2 (d), $x^2 + y^2 = |w|^2 = |5 - 12i| = \sqrt{25 + 144} = 13$. Adding and subtracting, $x^2 = 9$ and $y^2 = 4$, so $x = \pm 3$ and $y = \pm 2$. Since $xy = -6 < 0$, x and y have opposite signs. Hence $w = 3 - 2i$ or $w = -3 + 2i$. Check: $(3 - 2i)^2 = 9 - 12i + 4i^2 = 5 - 12i$, and $(-3 + 2i)^2 = (3 - 2i)^2$.

The formula of Proposition 1.4.1 gives the same root: $a = 5$, $b = -12 < 0$, so $s = -1$; $r = 13$, $x = \sqrt{18/2} = 3$ and $y = -\sqrt{8/2} = -2$. By part (b) there are no other roots.

Quick check. Find the square roots of -4 and of $2i$.

Solution. For -4: $a = -4$, $b = 0$, $r = 4$, so $x = \sqrt{0} = 0$ and $y = \sqrt{8/2} = 2$; the roots are

$\pm 2i$, and indeed $(2i)^2 = -4$. For $2i$: $a = 0$, $b = 2$, $r = 2$, so $x = \sqrt{1} = 1$ and $y = 1$; the roots are $\pm(1 + i)$, and $(1 + i)^2 = 1 + 2i - 1 = 2i$.

1.4.2 The quadratic formula

With square roots in hand, a quadratic equation with complex coefficients is solved exactly as in school: complete the square. The only difference is that we never need to ask whether the discriminant is negative.

Corollary 1.4.2. Quadratic Formula over the Complex Numbers

Let $a, b, c \in \mathbb{C}$ with $a \neq 0$, and let $d \in \mathbb{C}$ be a square root of $b^2 - 4ac$ (one exists by Proposition 1.4.1). Then for $z \in \mathbb{C}$,

$$az^2 + bz + c = 0 \iff z = \frac{-b + d}{2a} \quad \text{or} \quad z = \frac{-b - d}{2a}.$$

The two solutions coincide if and only if $b^2 - 4ac = 0$.

Here a, b, c are complex numbers, in a departure from the chapter's habit of reserving these letters for reals; the statement is the school formula, and keeps its letters. The choice of d does not matter: the other square root is $-d$ (Proposition 1.4.1 (b)), which swaps the two solutions.

Idea. Complete the square, as in school: after multiplying by $4a$, the equation says that $2az + b$ is a square root of $b^2 - 4ac$. The square roots of $b^2 - 4ac$ are exactly d and $-d$, and solving the two linear equations $2az + b = \pm d$ gives the formula.

Proof. Multiply by $4a$ and complete the square. By the ring laws (Proposition 1.1.2) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d),

$$4a(az^2 + bz + c) = 4a^2z^2 + 4abz + 4ac = (2az + b)^2 - (b^2 - 4ac).$$

Now $4a \neq 0$, since $4 \neq 0$ in $\mathbb{C}$ (as for 2 in the proof of Proposition 1.4.1 (c)) and $a \neq 0$, and $\mathbb{C}$ has no zero divisors (Theorem 1.2.4, Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d)). So $az^2+bz+c = 0$ if and only if $(2az+b)^2 = d^2$, that is, $(2az+b-d)(2az+b+d) = 0$, as in the proof of Proposition 1.4.1 (b). By the absence of zero divisors again, this holds if and only if $2az + b = d$ or $2az + b = -d$. Since $2a \neq 0$, these say $z = (-b + d)/(2a)$ or $z = (-b - d)/(2a)$.

The two solutions coincide if and only if $d = -d$, that is, $2d = 0$, that is, $d = 0$ (as $2 \neq 0$). And $d = 0$ if and only if $d^2 = 0$ (no zero divisors), that is, $b^2 - 4ac = 0$. This proves the corollary.

■

Example. Solve $z^2 - (3 + i)z + (2 + 2i) = 0$. Here $a = 1$, and the discriminant is

$$(3 + i)^2 - 4(2 + 2i) = (8 + 6i) - (8 + 8i) = -2i.$$

The formula of Proposition 1.4.1, applied to $-2i$ (real part 0, imaginary part $-2 < 0$, modulus

2), gives $x = \sqrt{2/2} = 1$ and $y = -\sqrt{2/2} = -1$, so $d = 1 - i$; indeed $(1-i)^2 = 1 - 2i - 1 = -2i$. The solutions are

$$z = \frac{(3+i)+(1-i)}{2} = 2 \qquad \text{and} \qquad z = \frac{(3+i)-(1-i)}{2} = 1 + i.$$

Check: their sum is $3 + i$ and their product is $2 + 2i$, the negative of the middle coefficient and the constant term, as they should be for $(z - 2)(z - (1 + i))$.

1.4.3 No order on the complex numbers

In $\mathbb{R}$, and in every ordered field, a non-zero square is positive (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)). In $\mathbb{C}$, i is non-zero and its square is -1. If $\mathbb{C}$ carried an order of the kind $\mathbb{R}$ has, -1 would have to be positive, and so would 1. That is already the proof.

Proposition 1.4.3. The Complex Numbers Cannot Be Ordered

There is **no** relation $<$ on $\mathbb{C}$ with which $(\mathbb{C}, +, \cdot, <)$ is an ordered field in the sense of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.2.

Proof. Suppose $<$ is a relation on $\mathbb{C}$ with which $\mathbb{C}$ is an ordered field. Since $i = (0, 1) \neq (0, 0) = 0$, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e) gives $i^2 > 0$, that is, $-1 > 0$ (Proposition 1.1.1: $i \cdot i = -1$). Since $1 \neq 0$ in the field $\mathbb{C}$, the same part (e) gives $1 > 0$. Adding, by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b), $0 = 1 + (-1) > 0 + 0 = 0$. But $0 < 0$ is impossible: (O1), with both elements equal to 0, says that exactly one of $0 < 0$ and $0 = 0$ holds, and $0 = 0$ does. So no such relation exists. ∎

The proof never asks whether $i > 0$ or $i < 0$: part (e) covers both at once. It also never assumes that the hypothetical order agrees with the order of $\mathbb{R}$ on real numbers. It concludes $1 > 0$ and $-1 > 0$ in whatever order is supposed, and that is the contradiction.

Remark. Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Chapter 4 showed, in an exercise (Number Systems: From \(\nN\) to \(\nR\), Exercise (C1: A field that cannot be ordered)), that a field containing a square root of -1 cannot be ordered, and named the complex numbers as such a field; the proposition proves that fact for $\mathbb{C}$ on its own. Compare Number Systems: From \(\nN\) to \(\nR\), Example (A field with two elements that cannot be ordered) and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (e): there the obstacle to an order is $n \cdot 1 = 0$ for some $n \geq 1$. That obstacle is absent here, since $n \cdot 1$ in $\mathbb{C}$ is $\iota(n \cdot 1)$, the image of the real number $n \cdot 1 > 0$ of $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h)), which is non-zero as ι is injective. (The identity $n \cdot 1 = \iota(n \cdot 1)$ is proved by Logic and Proof, Axiom 4.2.1 on n, as for powers in Section 1.1: $0 \cdot 1 = 0 = \iota(0)$, and if $n \cdot 1 = \iota(n \cdot 1)$, then $(n + 1) \cdot 1 = \iota(n \cdot 1) + \iota(1) = \iota((n + 1) \cdot 1)$ by Proposition 1.1.1.) The obstacle in $\mathbb{C}$ is $i^2 = -1$ instead.

Warning. An inequality $z < w$ between complex numbers means nothing: by Proposition 1.4.3 no order on $\mathbb{C}$ is compatible with its arithmetic. Apart from arguments that suppose an order on $\mathbb{C}$ in order to reach a contradiction (the proof above and Exercises B2

and C2), every inequality in this chapter compares **real** numbers in the order of $\mathbb{R}$: moduli, real parts, imaginary parts, or quantities proved to be real, as $2\,\mathrm{Re}(z\overline{w})$ was in Section 1.3. Writing $i > 0$ leads, by the proof above, to $0 > 0$; so does writing $i < 0$.

Quick check. Is the following a proof that $\mathbb{C}$ cannot be ordered? "Every real square is ≥ 0, and $i^2 = -1 < 0$. So i is not a square of anything, a contradiction."

Solution. No. The argument proves nothing about orders on $\mathbb{C}$. "$-1 < 0$" is a statement in $\mathbb{R}$'s order, and a hypothetical order on $\mathbb{C}$ need not agree with it on the reals; the argument never even introduces the hypothetical order. And "i is not a square" is false: $i = (\pm(1+i)/\sqrt{2})^2$ by Proposition 1.4.1. The correct proof works inside the supposed order, where $i^2 > 0$ because $i \neq 0$.

1.4.4 The square-root rule does not survive

In $\mathbb{R}$, $\sqrt{x}\sqrt{y} = \sqrt{xy}$ for $x, y \geq 0$: that is the rule for real square roots used above. A non-zero complex number has two square roots and no preferred one, and no way of preferring one keeps the rule alive.

Warning. No choice of "the" square root $\sqrt{z}$ of each complex z can satisfy $\sqrt{z}\sqrt{w} = \sqrt{zw}$ for all $z, w \in \mathbb{C}$. Whatever is chosen for $\sqrt{-1}$, it is i or $-i$ (Proposition 1.4.1 (b)), and in both cases $\sqrt{-1}\cdot\sqrt{-1} = (\pm i)^2 = -1$. But $\sqrt{(-1)(-1)} = \sqrt{1}$, and the rule itself forces $\sqrt{1} = 1$: since $\sqrt{1}$ is a square root of 1, $1 = \sqrt{1}\cdot\sqrt{1} = \sqrt{1\cdot 1} = \sqrt{1}$. So the rule would give $-1 = 1$, which is false in $\mathbb{C}$ (the real parts $-1 < 1$ differ). So in this volume the symbol $\sqrt{\ }$ is applied only to non-negative reals; for any other z, say "a square root of z" and solve $w^2 = z$.

1.4.5 Exercises

1.4.5.1 A. Check your understanding

Exercise. A1

(a) True or false: if $z, w \in \mathbb{C}$ and $z^2 = w^2$, then $z = w$. Justify your answer, and state what **is** true.

(b) Run the formula of Proposition 1.4.1 on $z = -4$: compute a, b, r, s, x, y and both square roots.

(c) Where in the proof of Proposition 1.4.1 is $r \geq |a|$ used?

(d) State the idea of the proof of Proposition 1.4.1 in two sentences.

Solution.

(a) False: $z = 1$, $w = -1$ have $z^2 = w^2 = 1$ and $z \neq w$. What is true: $z^2 = w^2$ implies $z = w$ or $z = -w$, since $(z-w)(z+w) = z^2 - w^2 = 0$ and $\mathbb{C}$ has no zero divisors (this

is the argument of Proposition 1.4.1 (b)).

(b) $a = -4$, $b = 0$, $r = |-4| = 4$, $s = 1$ (as $b \geq 0$), $x = \sqrt{(4-4)/2} = 0$, $y = \sqrt{(4+4)/2} = 2$. So $w = 2i$, and the square roots are $\pm 2i$.

(c) To take the square roots at all: $r \geq |a|$ gives $r + a \geq 0$ and $r - a \geq 0$, so $\sqrt{(r+a)/2}$ and $\sqrt{(r-a)/2}$ exist.

(d) Comparing parts gives $x^2 - y^2 = a$ and $2xy = b$; taking moduli gives a third equation $x^2 + y^2 = r$, and the first and third give x^2 and y^2 by adding and subtracting. The signs are then fixed by $2xy = b$, and the absence of zero divisors shows that $\pm w$ are the only roots.

1.4.5.2 B. Practice

Exercise. B1

(a) Find all $w \in \mathbb{C}$ with $w^2 = -3 + 4i$.

(b) Hence solve $z^2 + 2z + 4 - 4i = 0$.

Solution.

(a) Write $w = x + yi$. Comparing parts, $x^2 - y^2 = -3$ and $xy = 2$. Taking moduli (Theorem 1.2.2 (d)), $x^2+y^2 = |-3+4i| = \sqrt{9+16} = 5$. Adding and subtracting, $x^2 = 1$ and $y^2 = 4$. Since $xy = 2 > 0$, x and y have the same sign, so $w = 1+2i$ or $w = -1-2i$, and by Proposition 1.4.1 (b) there are no others. Check: $(1+2i)^2 = 1+4i-4 = -3+4i$.

(b) By Corollary 1.4.2 with $a = 1$, $b = 2$, $c = 4 - 4i$: the discriminant is $4 - 4(4 - 4i) = -12 + 16i = 4(-3 + 4i)$, with square root $d = 2(1 + 2i) = 2 + 4i$ by (a), since $(2(1 + 2i))^2 = 4(1 + 2i)^2$. So

$$z = \frac{-2 + (2 + 4i)}{2} = 2i \qquad \text{or} \qquad z = \frac{-2 - (2 + 4i)}{2} = -2 - 2i.$$

Equivalently, completing the square, $z^2 + 2z + 4 - 4i = (z + 1)^2 - (-3 + 4i)$, so $z + 1 = \pm(1 + 2i)$. Check: $(2i)^2 + 2(2i) + 4 - 4i = -4 + 4i + 4 - 4i = 0$.

Exercise. B2: Put the proof in order

The nine lines below include the seven lines of a proof of Proposition 1.4.3, shuffled, and two lines that do not belong. Write the seven lines in an order that makes a proof, and say what is wrong with each of the other two.

(i) $i^2 = -1$, so $-1 > 0$.

(ii) Since $i \neq 0$, we have $i > 0$.

(iii) Suppose $<$ is a relation on $\mathbb{C}$ that makes $\mathbb{C}$ an ordered field.

(iv) $0 < 0$ is impossible by (O1), so no such relation exists.

(v) So $i^2 > 0$, because non-zero squares are positive in an ordered field.

(vi) $1 \neq 0$, so $1 = 1^2 > 0$.

(vii) $i^2 = -1 < 0$, because $-1 < 0$ in $\mathbb{R}$.

(viii) $i \neq 0$, since $i = (0, 1) \neq (0, 0)$.

(ix) Adding, $0 = 1 + (-1) > 0 + 0 = 0$.

Solution. An admissible order is (iii), (viii), (v), (i), (vi), (ix), (iv). The constraints are what each line uses: (v), (vi), (i), (ix) and (iv) work in the supposed order, so they come after (iii); (v) also uses (viii); (i) uses (v); (ix) uses (i) and (vi); (iv) uses (ix). Line (viii) is a fact about $\mathbb{C}$ and uses no order, so it may stand anywhere before (v), even before (iii); line (vi) may stand anywhere after (iii) and before (ix). For instance (iii), (vi), (viii), (v), (i), (ix), (iv) and (viii), (iii), (v), (i), (vi), (ix), (iv) are also admissible. The admissible orders are exactly those that respect these constraints.

Line (ii) drops a case: from $i \neq 0$, trichotomy (O1) gives $i > 0$ **or** $i < 0$, and the line keeps only the first. That is (N7) of Logic and Proof, Example (What is not allowed), a missing case. Line (v) needs neither case, which is why the proof does not split.

Line (vii) cites a reason that is not available: the supposed order on $\mathbb{C}$ is arbitrary, and nothing says that it agrees with the order of $\mathbb{R}$ on the real numbers. The proposition is about **every** relation on $\mathbb{C}$, and (vii) quietly replaces "every" by "one that extends $\mathbb{R}$'s order". (The inequality $-1 < 0$ does hold in any ordered field, by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (a) applied to $1 > 0$, so the line could be repaired by citing that; as written its reason is (N9) of Logic and Proof, Example (What is not allowed), a fact that is not available.)

Exercise. B3

Let $a, b, c \in \mathbb{R}$ with $a \neq 0$ and $b^2 - 4ac < 0$. Prove that the equation $az^2 + bz + c = 0$ has exactly the two solutions

$$z = \frac{-b + i\sqrt{4ac - b^2}}{2a} \qquad \text{and} \qquad z = \frac{-b - i\sqrt{4ac - b^2}}{2a}$$

in $\mathbb{C}$, and that they are conjugate to each other.

Solution. Since $4ac - b^2 > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (a)), $q := \sqrt{4ac - b^2}$ exists, $q > 0$, and $d := iq$ satisfies $d^2 = i^2q^2 = -(4ac - b^2) = b^2 - 4ac$. So Corollary 1.4.2 with this d gives exactly the two solutions displayed, and they are distinct since $b^2 - 4ac \neq 0$. Since a, b, q are real and $2a \neq 0$, the two solutions are

$$-\frac{b}{2a} + \frac{q}{2a}\,i \qquad \text{and} \qquad -\frac{b}{2a} - \frac{q}{2a}\,i,$$

with the same real part and opposite imaginary parts: each is the conjugate of the other (Definition 1.2.1). For instance $z^2 - 2z + 5 = 0$ has $b^2 - 4ac = -16$, $q = 4$, and the solutions $1 \pm 2i$.

1.4.5.3 C. Going deeper

Exercise. C1: Find the error

Here is an argument.

Claim. For $z, w \in \mathbb{C}$, if $z^2 = w^2$, then $z = w$ or $z = -w$.

Proof. If $w = 0$, then $z^2 = 0$, so $z = 0 = w$, since $\mathbb{C}$ has no zero divisors. If $w \neq 0$, put $u := z/w$, which exists because $\mathbb{C}$ is a field; then $u^2 = z^2/w^2 = 1$. Taking square roots, $u = \sqrt{u^2} = \sqrt{1} = 1$. In particular, $u = 1$ or $u = -1$. Multiplying by w, $z = w$ or $z = -w$.

Is the claim true? Does the argument prove it? If not, name the line that fails and the reason, give a counterexample to that line, and repair the argument.

Solution. The claim is true: it is the argument of Proposition 1.4.1 (b), and it also follows directly from $(z - w)(z + w) = z^2 - w^2 = 0$ and the absence of zero divisors in $\mathbb{C}$.

The argument does not prove it. The failing line is "$u = \sqrt{u^2} = \sqrt{1} = 1$". It uses the rule "$u = \sqrt{u^2}$ whenever u^2 is a non-negative real", which is neither proved nor true: it is a general "fact" of the kind (N9) of Logic and Proof, Example (What is not allowed) forbids. The symbol $\sqrt{\ }$ is defined only on non-negative reals, and u is a complex number; even for real u, $\sqrt{u^2} = |u|$, not u. Counterexample to the step: $u = -1$ has $u^2 = 1$, but $\sqrt{u^2} = \sqrt{1} = 1 \neq u$.

The next line, "$u = 1$ or $u = -1$", is a valid weakening of $u = 1$ (a disjunction follows from either part), so it is not itself an error; it only papers over the loss of the root -1 one line earlier. The rest of the argument (the case $w = 0$, the division, and multiplying back by w) is correct.

Repair: replace the two middle lines by "Then $(u - 1)(u + 1) = u^2 - 1 = 0$, and $\mathbb{C}$ has no zero divisors, so $u = 1$ or $u = -1$."

Marking scheme. (10 points) - 2: says the claim is true, with a reason. - 3: names the line $u = \sqrt{u^2} = \sqrt{1} = 1$ as the failing one, and its illegal rule $u = \sqrt{u^2}$. - 2: a counterexample **to that step** ($u = -1$, or any u with $u^2 = 1$, $u \neq 1$). - 3: a correct repair, by factoring $u^2 - 1$ and using no zero divisors (or by Proposition 1.4.1 (b) applied to $z = 1$). Fatal errors (0 for the step): declaring the claim false; naming the "In particular" line instead of the $\sqrt{\ }$ line as the failing one, since it is a valid weakening.

Exercise. C2: A second proof that there is no order

(a) Use Proposition 1.4.1 to give a second proof of Proposition 1.4.3 in which the element i is never mentioned.

(b) Say why the argument in (a) does not need the special element i.

(c) Is the converse of the principle behind (a) true? That is: if a commutative ring with $1 \neq 0$ admits no order, must -1 be a square in it? Test the ring $\mathbb{Z}/3\mathbb{Z}$.

Solution (Hint 1). In an ordered field, which elements can be squares? For (c), list the squares of the three classes.

Solution.

(a) Suppose $<$ makes $\mathbb{C}$ an ordered field. Every square is then ≥ 0: a non-zero square

is positive by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e), and $0^2 = 0$. First, $-1 \neq 0$, since otherwise $1 = -(-1) = -0 = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)), against $1 \neq 0$ in the field $\mathbb{C}$ (Theorem 1.2.4). By Proposition 1.4.1 (a), applied to the non-zero number -1, some $d \in \mathbb{C}$ has $d^2 = -1$. So $-1 = d^2 \geq 0$, and as $-1 \neq 0$, $-1 > 0$. By part (e) again, $1 > 0$. Adding (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b)), $0 = 1 + (-1) > 0$, which (O1) forbids. This is the argument of Number Systems: From \(\nN\) to \(\nR\), Exercise (C1: A field that cannot be ordered), with the square root of -1 supplied by a formula.

(b) The argument uses only that -1 is a square in $\mathbb{C}$, and that is a property of the field, not of any named element. It does not matter that the formula of Proposition 1.4.1, applied to -1, happens to produce i ($a = -1$, $b = 0$, $r = 1$: $x = 0$, $y = 1$). The same argument shows that no field in which -1 is a square can be ordered; in particular no field in which **every** element is a square.

(c) No. The ring $\mathbb{Z}/3\mathbb{Z}$ is a commutative ring with $[1] \neq [0]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (a), (c)), and no relation makes it an ordered commutative ring (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (e)). Its three elements are $[0], [1], [2]$ (part (b) there), with squares $[0]^2 = [0]$, $[1]^2 = [1]$, $[2]^2 = [4] = [1]$. So the squares are $[0]$ and $[1]$, while $-[1] = [2]$. Hence -1 is not a square in $\mathbb{Z}/3\mathbb{Z}$, and yet the ring cannot be ordered: the obstacle there is $3 \cdot [1] = [0]$, not a square root of -1.

1.5 The Unit Circle and Polar Form

Addition in $\mathbb{C}$ is addition of arrows in the plane: $(a, b) + (c, d) = (a + c, b + d)$ puts the second arrow at the tip of the first. Multiplication has a picture too, and Section 1.2 already holds half of it: the modulus of a product is the product of the moduli (Theorem 1.2.2 (d)). The other half is about angles, and angles need the functions cosine and sine, which this volume does not construct. This section first proves everything about directions that needs no angle at all, then states exactly five facts about cosine and sine that it borrows, and from those five builds the polar form of a complex number and the rule "multiply the lengths, add the angles".

1.5.1 Length and direction

Every non-zero complex number should be a length times a direction. The length is the modulus. The directions are the complex numbers of length 1, and they deserve a name.

The unit circle is the set of complex numbers at distance 1 *from* 0.

We write

$$\mathbb{T} := \{u \in \mathbb{C} : |u| = 1\}$$

for the **unit circle**. For $u = x + yi$ with $x, y \in \mathbb{R}$, the condition $|u| = 1$ says $\sqrt{x^2 + y^2} = 1$, that is, $x^2 + y^2 = 1$: both sides of the first equation are non-negative, so it holds exactly when the squares agree (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g)). So $\mathbb{T}$ is the circle of radius 1 about 0 in the plane. It contains 1, -1, i and $-i$, and also $\frac{3}{5} + \frac{4}{5}i$, since $\frac{9}{25} + \frac{16}{25} = 1$. It does not contain $1 + i$, whose modulus is $\sqrt{2} \neq 1$.

The next proposition collects what the multiplication of $\mathbb{C}$ does on $\mathbb{T}$. None of it uses an angle.

Proposition 1.5.1. The Unit Circle

(a) $1 \in \mathbb{T}$. If $u, v \in \mathbb{T}$, then $uv \in \mathbb{T}$. If $u \in \mathbb{T}$, then $u \neq 0$ and $u^{-1} = \overline{u} \in \mathbb{T}$.

(b) For every $z \in \mathbb{C}$ with $z \neq 0$ there is **exactly one** pair (r, u) with $r \in \mathbb{R}$, $r > 0$, $u \in \mathbb{T}$ and $z = ru$, namely $r = |z|$ and $u = z/|z|$.

(c) For $z \in \mathbb{C}$ with $z \neq 0$: $1/z = \overline{z}$ if and only if $|z| = 1$.

Idea. Every part is a statement about moduli, so each follows from the rules of Section 1.2: moduli multiply, $u\overline{u} = |u|^2$, and only 0 has modulus 0. For (b), divide z by its length; for the uniqueness, take moduli of $z = ru$.

Proof.

(a) By Proposition 1.2.1, the modulus of the real number 1 is its absolute value, which is 1; so $1 \in \mathbb{T}$. If $|u| = |v| = 1$, then $|uv| = |u||v| = 1$ by Theorem 1.2.2 (d). Let $u \in \mathbb{T}$. Then $u \neq 0$, since $|0| = 0 \neq 1$ (Theorem 1.2.2 (e)). By Theorem 1.2.2 (c), $u\overline{u} = |u|^2 = 1$, so $\overline{u}$ satisfies the defining equation of u^{-1}. Since $\mathbb{C}$ is a field (Theorem 1.2.4), inverses are unique (Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (a)), and $u^{-1} = \overline{u}$. Finally $|\overline{u}| = |u| = 1$ by Theorem 1.2.2 (d).

(b) *Existence.* Let $r := |z|$. Then $r \geq 0$, and $r \neq 0$ because $z \neq 0$ (Theorem 1.2.2 (e)); so $r > 0$, and its inverse r^{-1} is a positive real number (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.5.2 (a)). By Theorem 1.2.4 the inverse of r in $\mathbb{C}$ is this real number, so $u := z/|z| = r^{-1}z$ is defined, and $z = ru$. By Theorem 1.2.2 (d) and Proposition 1.2.1, $|u| = |r^{-1}||z| = r^{-1}r = 1$, where $|r^{-1}| = r^{-1}$ because the absolute value of a positive real number is the number itself (Number Systems: From \(\nN\) to \(\nR\), Definition 4.1.1). So $u \in \mathbb{T}$.
Uniqueness. Let $z = ru$ with $r > 0$ and $u \in \mathbb{T}$. Taking moduli, $|z| = |r||u| = r \cdot 1 = r$, again by Theorem 1.2.2 (d) and Proposition 1.2.1. Then $u = r^{-1}z = z/|z|$. So the pair is the one named in the statement.

(c) Since inverses are unique, $1/z = \overline{z}$ holds if and only if $z\overline{z} = 1$, that is, by Theorem 1.2.2 (c), if and only if $|z|^2 = 1 = 1^2$. Both $|z|$ and 1 are non-negative, so by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g) neither can be strictly smaller than the other, and $|z|^2 = 1$ holds if and only if $|z| = 1$.

■

Part (b) is the picture we wanted: $z = |z| \cdot u$, a length times a direction, and both factors are forced. Part (a) says that the directions are closed under multiplication and inversion and contain 1; Chapter 3 calls a set with these properties, under an associative product, a group, and $\mathbb{T}$ is one of its first examples. Part (c) is a practical test: on the unit circle, and only there, dividing by z is the same as conjugating.

Quick check. Write $z = 3 + 4i$ as ru with $r > 0$ and $u \in \mathbb{T}$. What is $1/u$?

Solution. By Proposition 1.5.1 (b), $r = |3+4i| = 5$ and $u = \frac{3}{5}+\frac{4}{5}i$. By (a), $1/u = \overline{u} = \frac{3}{5}-\frac{4}{5}i$. Check: $(\frac{3}{5}+\frac{4}{5}i)(\frac{3}{5}-\frac{4}{5}i) = \frac{9}{25}+\frac{16}{25} = 1$.

So far a direction is a point u of $\mathbb{T}$, and multiplying two directions gives a third. What we cannot yet say is **how much** a direction turns the plane. For that we need to measure positions on the circle by a real number, an angle, so that multiplying directions adds angles. That is a job for cosine and sine.

1.5.2 What this volume borrows about cosine and sine

An angle should be a real number θ that walks around the circle: a point $(\cos\theta, \sin\theta)$ on $\mathbb{T}$, moving as θ moves, returning to its start after a full turn of length 2π. Defining such functions needs limits of functions, by power series or by integrals. This volume develops no limits of functions, so it does not define cosine and sine. *Analysis on the Real Line*, Chapter 10 does: there cos and sin are defined by power series, π is defined as twice the least positive zero of cos, and the facts below are proved. Its $\mathbb{R}$ is a complete ordered field, so by Number Systems: From \(\nN\) to \(\nR\), Theorem 6.3.1 it is our $\mathbb{R}$, up to the one order-preserving field isomorphism; the functions and the number carry over along it.

We write $2\pi\mathbb{Z} \coloneqq \{2\pi k : k \in \mathbb{Z}\}$, the integer multiples of 2π in $\mathbb{R}$.

Axiom 1.5.2. What This Volume Borrows about Cosine and Sine

There are functions $\cos, \sin\colon \mathbb{R} \to \mathbb{R}$ and a real number $\pi > 0$ with the following properties. They are **assumed here and proved in *Analysis on the Real Line*, Chapter 10**.

(T1) $\cos^2\theta + \sin^2\theta = 1$ for every $\theta \in \mathbb{R}$.

(T2) For all $\theta, \varphi \in \mathbb{R}$,

$$\cos(\theta+\varphi) = \cos\theta\cos\varphi - \sin\theta\sin\varphi,$$
$$\sin(\theta+\varphi) = \sin\theta\cos\varphi + \cos\theta\sin\varphi.$$

(T3) For $\theta \in \mathbb{R}$: $\cos\theta = 1$ if and only if $\theta \in 2\pi\mathbb{Z}$.

(T4) For every $(x, y) \in \mathbb{R}^2$ with $x^2 + y^2 = 1$ there is $\theta \in \mathbb{R}$ with $\cos\theta = x$ and $\sin\theta = y$.

(T5) $\sin\theta > 0$ whenever $0 < \theta < \pi$.

In words: (T1) puts the point $(\cos\theta, \sin\theta)$ on the unit circle; (T2) is the pair of addition formulas; (T3) says that the cosine reaches 1 exactly at the multiples of a full turn; (T4) says that every point of the circle is reached; (T5) says that during the first half turn the point stays in the upper half plane.

This box is where the chapter borrows. Like Logic and Proof, Axiom 4.2.1, which *Logic and Proof* assumed and *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 1 proved, it is a statement assumed in one volume and proved in another. Nothing in Sections 1.1–1.4, and nothing in this section above the box, uses it. From here on we use these five facts about cos, sin and π and **no others**: no value such as $\cos(\pi/3) = \frac{1}{2}$, no periodicity, no picture of a graph. Whatever else we need, we derive, and each proof that uses one of the facts names it by its number. Two consequences come at once.

- $\cos 0 = 1$, by (T3), since $0 = 2\pi \cdot 0 \in 2\pi\mathbb{Z}$. Then (T1) gives $\sin^2 0 = 1 - 1 = 0$, so $\sin 0 = 0$, because a non-zero real number has a positive square (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)).
- $\cos(2\pi k) = 1$ and $\sin(2\pi k) = 0$ for every $k \in \mathbb{Z}$, by (T3) and then (T1) in the same way.

Warning. The five facts are about cos, sin and π only. A school fact such as $\sin(\pi/6) = \frac{1}{2}$ is not among them, and a proof in this volume may not quote it: Example (Special Angles) below derives the few values we use. Nor do the facts say that cos and sin are "periodic with period 2π" as functions; that is true, and derivable from (T2) and (T3), but no proof here needs it.

1.5.3 Polar form

With angles available, we can name the point of $\mathbb{T}$ at angle θ.

$e^{i\theta}$ is the point of the unit circle at angle θ.

Definition 1.5.1. Polar Form

For $\theta \in \mathbb{R}$ we write

$$e^{i\theta} := \cos\theta + i\sin\theta.$$

Let $z \in \mathbb{C}$ with $z \neq 0$. A **polar form** of z is an expression $z = re^{i\theta}$ with $r \in \mathbb{R}$, $r > 0$, and $\theta \in \mathbb{R}$. Then θ is **an** argument of z.

In words: the first line is an abbreviation, not an exponential. This volume has no exponential function, the letter e on its own means nothing here, and the only rule of exponents we will use for $e^{i\theta}$ is the one proved below (Theorem 1.5.3 (a)). *Analysis on the Real Line*, Chapter 10 shows that $e^{i\theta}$ is indeed the value of the complex exponential function at $i\theta$; the notation anticipates that, and the linear algebra volumes write their roots of unity with it. The exponent may be written in any form equal to $i\theta$ with θ real, and the symbol then means $e^{i\theta}$: for example $e^{-i\theta} = e^{i(-\theta)}$, $e^{2\pi i} = e^{i\cdot 2\pi}$, $e^{in\theta} = e^{i(n\theta)}$ and $e^{-2\pi i} = e^{i(-2\pi)}$. This is unambiguous, because the real number θ is determined by $i\theta$ (it is its imaginary part). The second part asks for a **positive** real r and allows **any** real θ.

The point $e^{i\theta}$ lies on $\mathbb{T}$. Indeed $|e^{i\theta}| = \sqrt{\cos^2\theta + \sin^2\theta} = \sqrt{1} = 1$, by Definition 1.2.1 and (T1). So $re^{i\theta}$ is a length r times a direction, as in Proposition 1.5.1 (b), and that proposition gives $r = |z|$ for every polar form of z.

Examples.

- $e^{i0} = \cos 0 + i\sin 0 = 1$, by the consequences of the box. So $1 = 1 \cdot e^{i0}$ and $5 = 5e^{i0}$ are polar forms.
- $e^{2\pi i} = \cos 2\pi + i\sin 2\pi = 1$, by the second consequence with $k = 1$. So $1 = 1 \cdot e^{2\pi i}$ as well: 0 and 2π are both arguments of 1, and they differ, since $\pi > 0$.
- The number 0 has no polar form, since $|re^{i\theta}| = r > 0$.

A non-example by minimal change. Allow $r < 0$: then $-1 = (-1) \cdot e^{i0}$ looks like a polar form of -1 with argument 0. The clause that fails is $r > 0$, and it matters: with negative r allowed, the length could no longer be read off as $|z|$, and $1 = 1 \cdot e^{i0}$ and $-1 = (-1)e^{i0}$ would share the argument 0. We will see in Example (Special Angles) that $-1 = 1 \cdot e^{i\pi}$ is a genuine polar form.

The examples already show why the definition says **an** argument: $1 = e^{i0} = e^{2\pi i}$. How much freedom there is, exactly, is part (b) of Proposition 1.5.4 below. First, the reason for the notation: these numbers multiply the way exponentials do.

Theorem 1.5.3. Multiplication in Polar Form

(a) $e^{i\theta}e^{i\varphi} = e^{i(\theta+\varphi)}$ for all $\theta, \varphi \in \mathbb{R}$.

(b) $e^{i0} = 1$, and $(e^{i\theta})^{-1} = e^{-i\theta} = \overline{e^{i\theta}}$ for every $\theta \in \mathbb{R}$.

(c) If $r, s \in \mathbb{R}$ with $r, s > 0$ and $\theta, \varphi \in \mathbb{R}$, then $(re^{i\theta})(se^{i\varphi}) = rs\, e^{i(\theta+\varphi)}$, and this is a polar form of the product.

Idea. Multiply out $(\cos\theta + i\sin\theta)(\cos\varphi + i\sin\varphi)$ with the rule of Definition 1.1.1: the real and imaginary parts that appear are exactly the right-hand sides of the addition formulas (T2). The rest is bookkeeping with inverses and moduli.

Proof.

(a) By the multiplication rule of Definition 1.1.1,

$$\begin{aligned} e^{i\theta}e^{i\varphi} &= (\cos\theta\cos\varphi - \sin\theta\sin\varphi) + (\cos\theta\sin\varphi + \sin\theta\cos\varphi)i \\ &= \cos(\theta+\varphi) + i\sin(\theta+\varphi), \end{aligned}$$

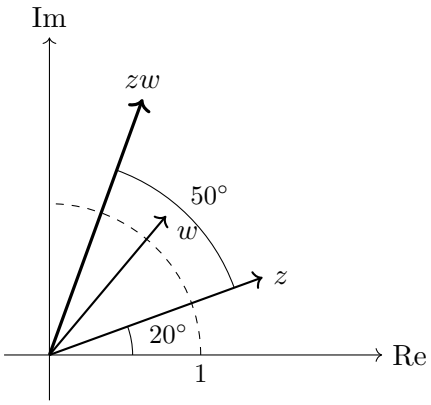
where the second equality is (T2), with the two products in the imaginary part reordered by commutativity in $\mathbb{R}$. The right-hand side is $e^{i(\theta+\varphi)}$.

(b) $e^{i0} = 1$ was shown in the first example above. By (a) with $\varphi = -\theta$, $e^{i\theta}e^{-i\theta} = e^{i0} = 1$, so $e^{-i\theta}$ is the inverse of $e^{i\theta}$, by uniqueness of inverses in the field $\mathbb{C}$ (Theorem 1.2.4, Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (a)). Since $e^{i\theta} \in \mathbb{T}$, its inverse is also its conjugate (Proposition 1.5.1 (a)).

(c) By Proposition 1.1.2 (commutativity and associativity of $\cdot$), $(re^{i\theta})(se^{i\varphi}) = (rs)(e^{i\theta}e^{i\varphi})$, and (a) turns this into $rs\, e^{i(\theta+\varphi)}$. Here $rs > 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (c) (multiply $0 < r$ by $s > 0$), so this is a polar form.

■

In words: **to multiply two complex numbers, multiply their moduli and add their arguments**. This is the chapter's third named move, **multiply moduli, add angles**. Multiplying by a fixed $w = se^{i\varphi}$ therefore turns the plane about 0 by the angle φ and stretches it by the factor s. The picture shows z, w and zw for $|z| = 1.5$, $|w| = 1.2$, and arguments of 20° and 50° (a full turn being 360°, that is, 2π).



The arrow for zw has length $1.5 \times 1.2 = 1.8$ and makes the angle $20° + 50° = 70°$ with the positive real axis: it is the arrow for z, turned by the argument of w and stretched by the modulus of w. The small arc marks the argument of z, the large arc the extra turn by the argument of w, and the dashed arc is part of the unit circle, where the numbers $e^{i\theta}$ live.

Now the freedom in the argument. Every non-zero number has a polar form, and its arguments are determined up to a whole number of full turns.

Proposition 1.5.4. Existence and Uniqueness of Polar Form

(a) Every $z \in \mathbb{C}$ with $z \neq 0$ has a polar form, and every polar form $z = re^{i\theta}$ has $r = |z|$.

(b) For $r, s \in \mathbb{R}$ with $r, s > 0$ and $\theta, \varphi \in \mathbb{R}$,

$$re^{i\theta} = se^{i\varphi} \iff r = s \text{ and } \theta - \varphi \in 2\pi\mathbb{Z}.$$

Proof.

(a) By Proposition 1.5.1 (b), $z = |z| \cdot u$ with $u = x + yi \in \mathbb{T}$, so $x^2 + y^2 = 1$. By (T4) there is $\theta \in \mathbb{R}$ with $\cos\theta = x$ and $\sin\theta = y$, that is, $u = e^{i\theta}$. Hence $z = |z|e^{i\theta}$, with $|z| > 0$. Conversely, if $z = re^{i\theta}$ is a polar form, then $e^{i\theta} \in \mathbb{T}$, and the uniqueness in Proposition 1.5.1 (b) gives $r = |z|$.

(b) Suppose first that $re^{i\theta} = se^{i\varphi}$. The number $re^{i\theta}$ is non-zero: $r \neq 0$, $e^{i\theta} \in \mathbb{T}$ is non-zero (Proposition 1.5.1 (a)), and a product of non-zero elements of the field $\mathbb{C}$ is non-zero (Theorem 1.2.4, Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d)). So both sides are polar forms of the same non-zero number, and $r = s$ by (a). Multiplying by r^{-1} gives $e^{i\theta} = e^{i\varphi}$. In the other direction, if $r = s$, the two sides are equal exactly when $e^{i\theta} = e^{i\varphi}$. So it remains to show that $e^{i\theta} = e^{i\varphi}$ if and only if $\theta - \varphi \in 2\pi\mathbb{Z}$.

Multiplying by $e^{-i\varphi}$, and back by $e^{i\varphi}$, shows that $e^{i\theta} = e^{i\varphi}$ holds if and only if $e^{i\theta}e^{-i\varphi} = e^{i\varphi}e^{-i\varphi}$, that is, by Theorem 1.5.3 (a) and (b), if and only if $e^{i(\theta-\varphi)} = 1$. Comparing real and imaginary parts, this says $\cos(\theta - \varphi) = 1$ and $\sin(\theta - \varphi) = 0$. The second condition follows from the first: by (T1), $\cos(\theta - \varphi) = 1$ gives $\sin^2(\theta - \varphi) = 0$, hence $\sin(\theta - \varphi) = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)). So $e^{i\theta} = e^{i\varphi}$ if and only if $\cos(\theta - \varphi) = 1$, and by (T3) that holds if and only if $\theta - \varphi \in 2\pi\mathbb{Z}$.

■

Existence came from (T4), and uniqueness from (T3), with (T1) helping and (T2) entering through Theorem 1.5.3. "Comparing arguments" therefore always means comparing them up to

a multiple of 2π, and the next warning is the trap this sets.

Warning. From $e^{i\theta} = e^{i\varphi}$ one may **not** conclude $\theta = \varphi$: $e^{i0} = e^{2\pi i} = 1$, and $0 \neq 2\pi$. Only $\theta - \varphi \in 2\pi\mathbb{Z}$ follows (Proposition 1.5.4 (b)). Forgetting this loses solutions as soon as an equation is solved for an angle; Section 1.6 meets an equation where it would lose all but one of them.

1.5.4 Powers

Repeating Theorem 1.5.3 gives powers. The powers z^n are those of the recursion $z^0 = 1$, $z^{n+1} = z^n z$ (Proposition 1.1.3).

Theorem 1.5.5. De Moivre's Formula

For every $\theta \in \mathbb{R}$ and every $n \in \mathbb{N}$,

$$(e^{i\theta})^n = e^{in\theta}, \quad \text{that is,} \quad (\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

Consequently $(re^{i\theta})^n = r^n e^{in\theta}$ for every real $r > 0$, and this is a polar form.

Idea. A power is a repeated product, and each new factor $e^{i\theta}$ adds θ to the argument, by Theorem 1.5.3 (a). So induction on n, along the recursion $z^{n+1} = z^n z$.

Proof. We use Logic and Proof, Axiom 4.2.1 on n, read on $\mathbb{N} = \omega$ through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b); here $n\theta$ is the product in $\mathbb{R}$ of $n \cdot 1_{\mathbb{R}}$ and θ (Number Systems: From \(\nN\) to \(\nR\), Definition 4.2.1 (a)). For $n = 0$, the left side is $(e^{i\theta})^0 = 1$ by the recursion, and the right side is $e^{i0} = 1$ by Theorem 1.5.3 (b). Suppose $(e^{i\theta})^n = e^{in\theta}$ for some $n \in \mathbb{N}$. Then

$$(e^{i\theta})^{n+1} = (e^{i\theta})^n e^{i\theta} = e^{in\theta} e^{i\theta} = e^{i(n\theta+\theta)} = e^{i(n+1)\theta},$$

by the recursion, the induction hypothesis, Theorem 1.5.3 (a), and $(n+1)\cdot 1_{\mathbb{R}} = n \cdot 1_{\mathbb{R}} + 1_{\mathbb{R}}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 4.2.1 (a)) with distributivity in $\mathbb{R}$. This proves the formula for every $n \in \mathbb{N}$.

For the consequence, Proposition 1.1.3 (c) gives $(re^{i\theta})^n = r^n (e^{i\theta})^n = r^n e^{in\theta}$. The power r^n is the same whether it is computed in $\mathbb{R}$ or in $\mathbb{C}$, by the remark after Proposition 1.1.3 in Section 1.1, and $r^n > 0$ because a product of positive reals is positive (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (c); induction on n, with $r^0 = 1 > 0$).

■

For a negative exponent, Exercise C1 below defines z^{-n} locally and proves the matching formula; nothing in the text uses it.

The five borrowed facts give no particular value of cos or sin except at multiples of 2π. Every other value this chapter uses is derived next, from (T1)–(T5) and the algebra of Sections 1.1–1.4.

Example. Special Angles

Show, using only (T1)–(T5) and the results proved so far, that

$$e^{i\pi} = -1, \qquad e^{i\pi/2} = i, \qquad e^{i\pi/3} = \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i,$$
$$e^{i\pi/6} = \tfrac{\sqrt{3}}{2} + \tfrac{1}{2}i, \qquad e^{i\pi/4} = \tfrac{1}{\sqrt{2}} + \tfrac{1}{\sqrt{2}}i.$$

Solution. Each value is found the same way: a power of the unknown point is a point we already know, and (T5) chooses between the candidates. Since $\pi > 0$, each of $\pi/2$, $\pi/3$, $\pi/4$, $\pi/6$ lies strictly between 0 and π, so (T5) gives $\operatorname{Im} e^{i\theta} = \sin\theta > 0$ for each of them.

(i) $e^{i\pi} = -1$. Let $u := e^{i\pi}$. By Theorem 1.5.5, $u^2 = e^{2\pi i} = 1$, so $(u-1)(u+1) = u^2 - 1 = 0$, and since $\mathbb{C}$ has no zero divisors (Theorem 1.2.4, Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d)), $u = 1$ or $u = -1$. Suppose $u = 1$. Then $\cos\pi = 1$, so $\pi = 2\pi k$ for some $k \in \mathbb{Z}$ by (T3); dividing by $\pi \neq 0$ gives $1 = 2k$ in $\mathbb{R}$, an equation between images of integers. The embedding of $\mathbb{Z}$ into $\mathbb{R}$, through $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4) and κ (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3), is injective and preserves $+$ and $\cdot$, so $1 = 2k$ holds in $\mathbb{Z}$. But $1 = 2 \cdot 0 + 1$ is odd, and an odd integer is not of the form $2k$ (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a)). So $u \neq 1$, and $e^{i\pi} = -1$.

(ii) $e^{i\pi/2} = i$. Let $u := e^{i\pi/2}$. By Theorem 1.5.3 (a), $u^2 = e^{i\pi} = -1 = i^2$, so $(u-i)(u+i) = 0$ and $u = \pm i$. Since $\operatorname{Im} u > 0$ and $\operatorname{Im}(-i) = -1 < 0$, $u = i$.

(iii) $e^{i\pi/3} = \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i$. Let $u := e^{i\pi/3}$. By Theorem 1.5.5, $u^3 = e^{i\pi} = -1$. Multiplying out shows $(u+1)(u^2-u+1) = u^3+1 = 0$. Now $u \neq -1$, since $\operatorname{Im} u > 0$; so $u^2-u+1 = 0$. By Corollary 1.4.2 with $a = 1$, $b = -1$, $c = 1$, and $d := \sqrt{3}\,i$, a square root of $b^2 - 4ac = -3$ (indeed $(\sqrt{3}\,i)^2 = 3i^2 = -3$),

$$u = \frac{1 + \sqrt{3}\,i}{2} \quad \text{or} \quad u = \frac{1 - \sqrt{3}\,i}{2}.$$

Since $\operatorname{Im} u > 0$, $u = \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i$.

(iv) $e^{i\pi/6} = \tfrac{\sqrt{3}}{2} + \tfrac{1}{2}i$. Since $\pi/6 = \pi/2 + (-\pi/3)$, Theorem 1.5.3 (a) and (b) give

$$e^{i\pi/6} = e^{i\pi/2}e^{-i\pi/3} = i \cdot \overline{e^{i\pi/3}} = i\Big(\frac{1}{2} - \frac{\sqrt{3}}{2}i\Big) = \frac{\sqrt{3}}{2} + \frac{1}{2}i,$$

by (ii) and (iii).

(v) $e^{i\pi/4} = \tfrac{1}{\sqrt{2}} + \tfrac{1}{\sqrt{2}}i$. Let $u := e^{i\pi/4}$. By Theorem 1.5.3 (a) and (ii), $u^2 = e^{i\pi/2} = i$. The formula of Proposition 1.4.1 for $z = i$ (so $a = 0$, $b = 1$, $r = |i| = 1$) gives the square root $w = \sqrt{1/2} + \sqrt{1/2}\,i$, and $\sqrt{1/2} = 1/\sqrt{2}$, since both are non-negative and square to $\tfrac{1}{2}$. By Proposition 1.4.1 (b), $u = w$ or $u = -w$, and $\operatorname{Im} u > 0$ rules out $-w$. So $u = w$.

Comparing real and imaginary parts turns these into values of cos and sin:

θ	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$	π
$\cos\theta$	1	$\sqrt{3}/2$	$1/\sqrt{2}$	$1/2$	0	-1
$\sin\theta$	0	$1/2$	$1/\sqrt{2}$	$\sqrt{3}/2$	1	0

These are the familiar values, now proved from the five facts.

Two special cases of the rotation picture are worth isolating. Multiplying by $i = e^{i\pi/2}$ turns the plane by a quarter turn, counterclockwise; two quarter turns make a half turn, and this is the picture behind $i^2 = -1 = e^{i\pi}$. And multiplying by $e^{-i\theta} = \overline{e^{i\theta}}$ undoes the turn by θ (Theorem 1.5.3 (b)).

Powers that are tedious to expand become one line in polar form.

Example. A Power via Polar Form

Compute $(\sqrt{3}+i)^6$.

Solution. We have $\sqrt{3}+i = 2(\frac{\sqrt{3}}{2}+\frac{1}{2}i) = 2e^{i\pi/6}$, by Example (Special Angles) (iv). By Theorem 1.5.5 and Example (Special Angles) (i),

$$(\sqrt{3}+i)^6 = 2^6 e^{i\cdot 6\pi/6} = 64\, e^{i\pi} = -64.$$

By hand: $(\sqrt{3}+i)^2 = 3+2\sqrt{3}\,i-1 = 2+2\sqrt{3}\,i = 2(1+\sqrt{3}\,i)$, and $(1+\sqrt{3}\,i)^3 = (1+\sqrt{3}\,i)(-2+2\sqrt{3}\,i) = -2-6 = -8$, so $(\sqrt{3}+i)^6 = \left(2(1+\sqrt{3}\,i)\right)^3 = 8\cdot(-8) = -64$ (Proposition 1.1.3 (b), (c)), the same answer.

Quick check. Use polar form to compute $(1+i)^8$, and check the answer with $(1+i)^2 = 2i$.

Solution. By Example (Special Angles) (v), $1+i = \sqrt{2}(\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i) = \sqrt{2}\,e^{i\pi/4}$. By Theorem 1.5.5, $(1+i)^8 = (\sqrt{2})^8 e^{i\cdot 8\pi/4} = 16\,e^{2\pi i} = 16$, since $(\sqrt{2})^8 = \left((\sqrt{2})^2\right)^4 = 2^4 = 16$ and $e^{2\pi i} = 1$. Check: $(1+i)^8 = \left((1+i)^2\right)^4 = (2i)^4 = 16i^4 = 16$, by Proposition 1.1.3 (b), (c).

1.5.5 Exercises

1.5.5.1 A. Check your understanding

Exercise. A1

(a) Give a polar form of -2 and of $3i$.

(b) True or false: if $e^{i\theta} = e^{i\varphi}$, then $\theta = \varphi$. Justify your answer.

(c) In Proposition 1.5.4, which of the borrowed facts (T1)–(T5) gives the existence of a polar form, and which gives the uniqueness of the argument up to $2\pi\mathbb{Z}$?

(d) Which results of Sections 1.1–1.5 use none of the borrowed facts? Is Proposition 1.5.1 among them?

Solution.

(a) $-2 = 2e^{i\pi}$ and $3i = 3e^{i\pi/2}$, by Example (Special Angles) (i) and (ii); the moduli 2 and 3 are positive, as a polar form requires. (Any $\pi + 2\pi k$, respectively $\pi/2 + 2\pi k$, with $k \in \mathbb{Z}$, is also an argument, by Proposition 1.5.4 (b).)

(b) False. $e^{i0} = 1 = e^{2\pi i}$, but $0 \neq 2\pi$ since $\pi > 0$. What is true is $\theta - \varphi \in 2\pi\mathbb{Z}$ (Proposition 1.5.4 (b)).

(c) Existence: (T4), which provides an angle for the point $z/|z|$ of $\mathbb{T}$. Uniqueness: (T3), which turns $\cos(\theta - \varphi) = 1$ into $\theta - \varphi \in 2\pi\mathbb{Z}$; (T1) is used alongside it, to see that $\sin(\theta - \varphi) = 0$ follows from $\cos(\theta - \varphi) = 1$, and (T2) enters through Theorem 1.5.3, which turns $e^{i\theta} = e^{i\varphi}$ into $e^{i(\theta-\varphi)} = 1$.

(d) Everything in Sections 1.1–1.4, and the part of this section before Axiom 1.5.2; after the box, only Exercise C2, which is set up to avoid them. In particular Proposition 1.5.1 uses none of them: its proof uses only the modulus rules of Section 1.2, the field properties of $\mathbb{C}$, and order facts about $\mathbb{R}$ from *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*.

1.5.5.2 B. Practice

Exercise. B1

Compute $(1 - \sqrt{3}\,i)^6$.

Solution. We have $1 - \sqrt{3}\,i = 2(\frac{1}{2} - \frac{\sqrt{3}}{2}i) = 2\,\overline{e^{i\pi/3}} = 2e^{-i\pi/3}$, by Example (Special Angles) (iii) and Theorem 1.5.3 (b). By Theorem 1.5.5,

$$(1 - \sqrt{3}\,i)^6 = 2^6 e^{-6i\pi/3} = 64\,e^{-2\pi i} = 64,$$

since $-2\pi = 2\pi \cdot (-1) \in 2\pi\mathbb{Z}$, so $\cos(-2\pi) = 1$ and $\sin(-2\pi) = 0$ by (T3) and (T1), and $e^{-2\pi i} = 1$.

Exercise. B2: Symmetries of Cosine and Sine

Prove that for every $\theta \in \mathbb{R}$:

$$\cos(-\theta) = \cos\theta, \quad \sin(-\theta) = -\sin\theta, \quad \cos(\theta + \pi) = -\cos\theta,$$
$$\sin(\theta + \pi) = -\sin\theta, \quad \cos\theta = \sin(\theta + \pi/2).$$

Hint: write each left side as a part of some $e^{i\psi}$, and compute that $e^{i\psi}$ with Theorem 1.5.3.

Solution. By Theorem 1.5.3 (b), $e^{-i\theta} = \overline{e^{i\theta}}$, that is, $\cos(-\theta) + i\sin(-\theta) = \cos\theta - i\sin\theta$. Comparing real and imaginary parts gives $\cos(-\theta) = \cos\theta$ and $\sin(-\theta) = -\sin\theta$.

By Theorem 1.5.3 (a) and Example (Special Angles) (i), $e^{i(\theta+\pi)} = e^{i\theta}e^{i\pi} = -e^{i\theta}$, that is, $\cos(\theta + \pi) + i\sin(\theta + \pi) = -\cos\theta - i\sin\theta$. Comparing parts gives the next two identities.

By Theorem 1.5.3 (a) and Example (Special Angles) (ii), $e^{i(\theta+\pi/2)} = ie^{i\theta} = i\cos\theta - \sin\theta$.

Comparing imaginary parts gives $\sin(\theta + \pi/2) = \cos\theta$. (Comparing real parts gives, in addition, $\cos(\theta + \pi/2) = -\sin\theta$.)

Exercise. B3

Let $\theta \in \mathbb{R}$. Show that $|e^{i\theta} - 1|^2 = 2 - 2\cos\theta$. Hence show again that $e^{i\theta} = 1$ if and only if $\cos\theta = 1$.

Solution. Let $u := e^{i\theta}$, so $u\overline{u} = |u|^2 = 1$. Squaring the modulus, by Theorem 1.2.2 (a)–(c),

$$|u-1|^2 = (u-1)\overline{(u-1)} = (u-1)(\overline{u}-1) = u\overline{u} - (u+\overline{u}) + 1 = 2 - 2\operatorname{Re} u,$$

and $\operatorname{Re} u = \cos\theta$. Hence $|u-1|^2 = 2 - 2\cos\theta$.

Now $u = 1$ if and only if $|u-1| = 0$ (Theorem 1.2.2 (e)), if and only if $|u-1|^2 = 0$ (a real number is 0 exactly when its square is: $0^2 = 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), and a non-zero square is positive by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)), if and only if $2 - 2\cos\theta = 0$, that is, $\cos\theta = 1$.

1.5.5.3 C. Going deeper

Exercise. C1: Triple Angles and Negative Powers

(a) Prove that $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ and $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$ for every $\theta \in \mathbb{R}$.

(b) For $z \in \mathbb{C}$ with $z \neq 0$ and $n \in \mathbb{N}$, put $z^{-n} := (z^{-1})^n$ (a definition local to this exercise). Show that $(e^{i\theta})^{-n} = e^{-in\theta}$.

Solution.

(a) Write $c := \cos\theta$ and $s := \sin\theta$. By Theorem 1.5.5, $\cos 3\theta + i\sin 3\theta = (c+is)^3$. Now $(c+is)^2 = (c^2 - s^2) + 2cs\,i$, and

$$\begin{aligned}(c+is)^3 &= \big((c^2-s^2) + 2cs\,i\big)(c+is)\\ &= (c^3 - 3cs^2) + (3c^2 s - s^3)i.\end{aligned}$$

Comparing real parts and using $s^2 = 1 - c^2$ (T1), $\cos 3\theta = c^3 - 3c(1-c^2) = 4c^3 - 3c$. Comparing imaginary parts and using $c^2 = 1 - s^2$, $\sin 3\theta = 3(1-s^2)s - s^3 = 3s - 4s^3$.

(b) By Theorem 1.5.3 (b), $(e^{i\theta})^{-1} = e^{-i\theta} = e^{i(-\theta)}$. By Theorem 1.5.5 applied to $-\theta$, $(e^{i\theta})^{-n} = (e^{i(-\theta)})^n = e^{in(-\theta)} = e^{-in\theta}$.

Nothing in this chapter uses negative powers of complex numbers; the definition in (b) is for practice only.

Exercise. C2: Points on the Circle without Angles

For $t \in \mathbb{R}$ put

$$u_t \coloneqq \frac{1+it}{1-it}.$$

(a) Show that u_t is defined, that $u_t \in \mathbb{T}$, and that $u_t \neq -1$.

(b) Show that every $u \in \mathbb{T}$ with $u \neq -1$ equals u_t for **exactly one** $t \in \mathbb{R}$, namely $t = \operatorname{Im} u/(1+\operatorname{Re} u)$.

(c) Compute $u_{1/2}$ in the form $a+bi$.

Use none of the borrowed facts (T1)–(T5).

Solution (Hint 1). For (b), on the unit circle the conjugate is the inverse: $\overline{u} = 1/u$.

Solution (Hint 2). Clearing the denominator, $u = u_t$ is equivalent to $u - 1 = it(u+1)$, and $u + 1 \neq 0$, so t is determined; it remains to show that $(u-1)/(i(u+1))$ is real.

Solution.

(a) The real part of $1-it$ is 1, so $1-it \neq 0$ and the quotient is defined. The numbers $1+it$ and $1-it$ are conjugate, so they have the same modulus (Theorem 1.2.2 (d)), which is non-zero. From $u_t(1-it) = 1+it$ and Theorem 1.2.2 (d), $|u_t||1-it| = |1+it| = |1-it|$, and canceling the non-zero real number $|1-it|$ gives $|u_t| = 1$. If $u_t = -1$, then $1+it = -(1-it) = -1+it$, so $1 = -1$, which is false. So $u_t \neq -1$.

(b) Let $u \in \mathbb{T}$ with $u \neq -1$, and let $t \in \mathbb{R}$. Since $1-it \neq 0$, the equation $u = u_t$ is equivalent to $u(1-it) = 1+it$, that is, to

$$u - 1 = it(u+1).$$

Since $i(u+1) \neq 0$, this holds if and only if $t = t_0$, where $t_0 \coloneqq (u-1)/(i(u+1)) \in \mathbb{C}$. So at most one real t has $u_t = u$, and one does exactly when t_0 is real. Using $u\overline{u} = 1$,

$$(u-1)(\overline{u}+1) = u\overline{u} + u - \overline{u} - 1 = u - \overline{u} = 2i \operatorname{Im} u,$$

where $u - \overline{u} = 2i \operatorname{Im} u$ by Definition 1.2.1 (with $u = a+bi$, $(a+bi)-(a-bi) = 2bi$); and $(u+1)(\overline{u}+1) = |u+1|^2 = 2 + 2\operatorname{Re} u$, by Theorem 1.2.2 (a), (c). This is a positive real number, since $u + 1 \neq 0$. Multiplying numerator and denominator of $(u-1)/(u+1)$ by $\overline{u}+1 = \overline{u+1} \neq 0$,

$$t_0 = \frac{1}{i} \cdot \frac{2i \operatorname{Im} u}{2 + 2\operatorname{Re} u} = \frac{\operatorname{Im} u}{1 + \operatorname{Re} u},$$

a real number. So exactly one $t \in \mathbb{R}$ has $u_t = u$, namely t_0.

(c) Multiplying numerator and denominator by the conjugate $1 + \frac{1}{2}i$ of the denominator,

$$u_{1/2} = \frac{(1+\frac{1}{2}i)^2}{1+\frac{1}{4}} = \frac{\frac{3}{4}+i}{\frac{5}{4}} = \frac{3}{5} + \frac{4}{5}i.$$

Check against (b): $\operatorname{Im} u/(1+\operatorname{Re} u) = \frac{4}{5}/\frac{8}{5} = \frac{1}{2}$.

So the map $t \mapsto u_t$ is a bijection from $\mathbb{R}$ onto $\mathbb{T} \setminus \{-1\}$, and it was found with no angle. For rational t, the point u_t has rational coordinates: the computation in (c) with t in place of $\frac{1}{2}$ gives $u_t = ((1-t^2) + 2t\,i)/(1+t^2)$, and $t = 1/2$ gives the point $(3/5, 4/5)$ behind the right triangle with sides 3, 4, 5.

Marking scheme. (10 points) - 2: $1 - it \neq 0$ with a reason, and $|u_t| = 1$ from the equal moduli of conjugates. - 1: $u_t \neq -1$. - 2: $u = u_t$ rewritten as a linear equation in t, with $u + 1 \neq 0$ used to solve it uniquely. - 3: shows that the unique solution is real and equals $\operatorname{Im} u/(1 + \operatorname{Re} u)$, with $1 + \operatorname{Re} u \neq 0$ justified (for example by multiplying by $\overline{u+1}$ and using $u\overline{u} = 1$, with $2 + 2\operatorname{Re} u > 0$). - Second route (coordinates $u = x + yi$, $x^2 + y^2 = 1$): the two lines above (5 points) become 2 for splitting $u - 1 = it(u + 1)$ into $x - 1 = -ty$ and $y = t(1 + x)$, showing $x \neq -1$ (otherwise $u = -1$) and so $t = y/(1 + x)$ is forced; and 3 for checking that this t satisfies $x - 1 = -ty$, using $x^2 + y^2 = 1$. - 2: (c) computed and checked. Fatal errors (0 for the step): writing $u = e^{i\theta}$ and using a half-angle formula (borrowed facts, and values not derived here); dividing by $1 + \operatorname{Re} u$ without showing it is non-zero.

1.6 Higher Roots, Roots of Unity, and a Look Ahead

Section 1.4 solved $z^2 = c$ with real square roots alone. Polar form turns the general equation $z^n = c$ into a question about lengths and angles: by De Moivre's formula (Theorem 1.5.5), raising to the n-th power raises the modulus to the n-th power and multiplies the argument by n. The angle part is a linear equation for a real number, with the ambiguity $2\pi\mathbb{Z}$ of Proposition 1.5.4 attached. The length part is the real equation $r^n = \rho$ with $\rho > 0$, and before anything else we must know that it has exactly one positive solution. This section proves that, solves $z^n = c$, counts the solutions, studies the case $c = 1$, and ends with a look ahead at polynomial equations in general.

1.6.1 Real n-th roots

For $n = 2$, *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 6 built the square root by the move **construct a point as a supremum** (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), and an exercise there ran the same move for cube roots (Number Systems: From \(\nN\) to \(\nR\), Exercise (B2: Cube roots)). For a general exponent the move is the same; only the estimate for $(s + h)^n$ needs a new tool, and Lemma 1.1.4 supplies it. Here $n \cdot 1_{\mathbb{R}}$ is written n, and powers in $\mathbb{R}$ are those of Proposition 1.1.3 with $R = \mathbb{R}$, the same recursion as Number Systems: From \(\nN\) to \(\nR\), Definition 4.2.1 (b).

Lemma 1.6.1. Real n-th Roots

Let $n \in \mathbb{N}$ with $n \geq 1$.

(a) If $s, t \in \mathbb{R}$ and $0 \leq s < t$, then $s^n < t^n$.

(b) For every $a \in \mathbb{R}$ with $a \geq 0$ there is **exactly one** $b \in \mathbb{R}$ with $b \geq 0$ and $b^n = a$. We write $\sqrt[n]{a} := b$. For $n = 2$ it is the square root $\sqrt{a}$ of Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4.

Idea. Part (a) is the factorization $t^n - s^n = (t-s)(t^{n-1} + t^{n-2}s + \cdots + s^{n-1})$: both factors are positive. For (b), let s be the supremum of the set S of non-negative y with $y^n \le a$, and rule out $s^n < a$ and $s^n > a$.

If $s^n < a$, we want $h > 0$ with $(s+h)^n \le a$. Working backwards: for $0 < h \le 1$, the same factorization writes $(s+h)^n - s^n$ as h times a sum of n terms, each at most $(s+1)^{n-1}$. So $(s+h)^n - s^n \le h \cdot n(s+1)^{n-1}$, and it is enough that this be at most half the room $a - s^n$. That gives $h \coloneqq \min\{1, (a-s^n)/(2n(s+1)^{n-1})\}$.

If $s^n > a$, we want $h > 0$ with $(s-h)^n \ge a$ still, which makes $s-h$ a smaller upper bound. Now $s^n - (s-h)^n \le h \cdot ns^{n-1}$, and it is enough that this equal the excess $s^n - a$. That gives $h \coloneqq (s^n - a)/(ns^{n-1})$.

Proof. Three facts are used throughout: a power of a non-negative real number is non-negative and a power of a positive one is positive (induction on the exponent with Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (c)); if $0 \le y \le 1$ then $y^k \le y$ for every $k \ge 1$, while if $y \ge 1$ then $y^k \ge y$ (induction: $y^{k+1} = y^k y$, and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (c) or equality); and if $0 \le x \le x'$ and $0 \le y \le y'$, then $xy \le x'y \le x'y'$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (c) twice, or equality).

(a) By Lemma 1.1.4 in the commutative ring $\mathbb{R}$,

$$t^n - s^n = (t-s)\sum_{k=0}^{n-1} t^k s^{n-1-k}.$$

Every term of the sum is ≥ 0, and the term with $k = n-1$ is $t^{n-1} > 0$, since $t > s \ge 0$. So the sum is $\ge t^{n-1} > 0$. Also $t - s > 0$. Hence $t^n - s^n > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (c)).

(b) *Uniqueness.* If $b, c \ge 0$ and $b \ne c$, say $b < c$, then $b^n < c^n$ by (a); so at most one non-negative b has $b^n = a$.

Existence. If $a = 0$, then $b \coloneqq 0$ works, since $0^n = 0^{n-1} \cdot 0 = 0$. Let $a > 0$, and let

$$S \coloneqq \{y \in \mathbb{R} : y \ge 0 \text{ and } y^n \le a\}.$$

Put $m \coloneqq \min\{1, a\} > 0$. Since $0 < m \le 1$, $m^n \le m \le a$, so $m \in S$. Put $M \coloneqq \max\{1, a\}$. If $y > M$, then $y > 1$, so $y^n \ge y > M \ge a$ and $y \notin S$; hence M is an upper bound of S. Since $\mathbb{R}$ is a complete ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3, Number Systems: From \(\nN\) to \(\nR\), Definition 5.6.1), S has a supremum; let $s \coloneqq \sup S$. Then $s \ge m > 0$.

Case $s^n < a$. Let

$$h \coloneqq \min\Big\{1, \frac{a - s^n}{2n(s+1)^{n-1}}\Big\}.$$

It depends only on a, n and s, and $h > 0$, since $a - s^n > 0$ and $2n(s+1)^{n-1} > 0$. By Lemma 1.1.4,

$$(s+h)^n - s^n = h\sum_{k=0}^{n-1}(s+h)^k s^{n-1-k}.$$

Since $0 \le s < s+h \le s+1$, each term satisfies $(s+h)^k s^{n-1-k} \le (s+1)^k (s+1)^{n-1-k} = (s+1)^{n-1}$, by (a) (or equality), the third fact, and Proposition 1.1.3 (a). A sum of n terms, each at most $(s+1)^{n-1}$, is at most $n(s+1)^{n-1}$. Hence

$$(s+h)^n \le s^n + h \cdot n(s+1)^{n-1} \le s^n + \frac{a-s^n}{2} < a.$$

So $s+h \in S$, and $s+h > s$, against s being an upper bound of S.

Case $s^n > a$. Let

$$h := \frac{s^n - a}{ns^{n-1}},$$

which depends only on a, n and s, and is positive. Since $a > 0$, we have $s^n - a < s^n \le ns^n$, so $h < s^n/(ns^{n-1}) = s/n \le s$; thus $0 < s-h < s$. By Lemma 1.1.4 and the same bound, with $0 < s-h < s$, each of the n terms of $\sum_{k=0}^{n-1} s^k (s-h)^{n-1-k}$ is at most s^{n-1}, so

$$s^n - (s-h)^n \le h \cdot ns^{n-1} = s^n - a,$$

that is, $(s-h)^n \ge a$. Now let $y \in S$. If $y > s-h$, then (a) gives $y^n > (s-h)^n \ge a$, against $y \in S$. So $y \le s-h$, and $s-h$ is an upper bound of S smaller than s, against s being the **least** upper bound.

Both cases are impossible, so $s^n = a$ by trichotomy, and $b := s \ge 0$ works.

For $n = 2$, the number $\sqrt[2]{a}$ is non-negative and squares to a, so it is $\sqrt{a}$, by the uniqueness in Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4.

■

The constants were found backwards in the Idea and placed first in the proof, and each depends on a, n and s only. Completeness was used once, to produce s. For $a > 0$ the root is positive, since $0^n = 0 \ne a$. For instance $\sqrt[3]{8} = 2$ and $\sqrt[4]{4} = \sqrt{2}$, since $2^3 = 8$ and $(\sqrt{2})^4 = ((\sqrt{2})^2)^2 = 4$, and both are non-negative. The symbol $\sqrt[n]{a}$ is used only for **non-negative real** a; the next theorem shows why it could not mean "the" n-th root of a complex number.

1.6.2 Solving the equation z to the n equals c

Now the main result. Every non-zero complex number has exactly n different n-th roots, and polar form lists them.

Theorem 1.6.2. n-th Roots of a Complex Number

Let $n \in \mathbb{N}$ with $n \ge 1$, and let $c \in \mathbb{C}$ with $c \ne 0$. Let $c = \rho e^{i\alpha}$ be a polar form of c (Proposition 1.5.4), and for $k \in \mathbb{Z}$ put

$$z_k := \sqrt[n]{\rho}\, e^{i(\alpha+2\pi k)/n}.$$

(a) For $z \in \mathbb{C}$: $z^n = c$ if and only if $z = z_k$ for some $k \in \mathbb{Z}$.

(b) For $k, l \in \mathbb{Z}$: $z_k = z_l$ if and only if $n \mid k-l$ (Sets, Relations, and Cardinality, Definition 2.2.1).

(c) The map $\{0, 1, \ldots, n-1\} \to \{z \in \mathbb{C} : z^n = c\}$, $k \mapsto z_k$, is a bijection. So c has exactly n n-th roots (Sets, Relations, and Cardinality, Definition 3.1.2).

In particular every non-zero complex number has an n-th root, and every $u \in \mathbb{T}$ has one in $\mathbb{T}$.

Idea. Write the unknown in polar form, $z = re^{i\theta}$. De Moivre turns $z^n = c$ into $r^n e^{in\theta} = \rho e^{i\alpha}$, and the uniqueness half of polar form splits that into a real equation for the length, $r^n = \rho$, and an equation for the angle, $n\theta \in \alpha + 2\pi\mathbb{Z}$. The first has one solution, $r = \sqrt[n]{\rho}$. The second has the solutions $\theta = (\alpha + 2\pi k)/n$, one for each integer k. Different k can give the same point, and they do exactly when the angles differ by a whole number of turns, that is, when $n \mid k - l$. So the k that matter are the remainders $0, \dots, n-1$.

Before reading on: where is the uniqueness half of the polar form used, and where the uniqueness of the real n-th root?

Proof. Here $\rho = |c| > 0$ by Proposition 1.5.4 (a), so $\sqrt[n]{\rho} > 0$ exists by Lemma 1.6.1 (b).

(a) Let $z \in \mathbb{C}$. If $z = 0$, then $z^n = 0^{n-1} \cdot 0 = 0 \neq c$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)), and z is no z_k, since every z_k has modulus $\sqrt[n]{\rho} > 0$. So let $z \neq 0$, and fix a polar form $z = re^{i\theta}$ (Proposition 1.5.4 (a)). By Theorem 1.5.5, $z^n = r^n e^{in\theta}$, a polar form with $r^n > 0$. By Proposition 1.5.4 (b),

$$z^n = c \iff r^n = \rho \text{ and } n\theta - \alpha \in 2\pi\mathbb{Z}.$$

Since $r > 0$, the uniqueness in Lemma 1.6.1 (b) gives $r^n = \rho \iff r = \sqrt[n]{\rho}$. And $n\theta - \alpha = 2\pi k$ holds for a given $k \in \mathbb{Z}$ exactly when $\theta = (\alpha + 2\pi k)/n$.
($\Rightarrow$) If $z^n = c$, then $r = \sqrt[n]{\rho}$ and $\theta = (\alpha + 2\pi k)/n$ for some $k \in \mathbb{Z}$, so $z = z_k$.
($\Leftarrow$) If $z = z_k$, use the polar form $r := \sqrt[n]{\rho}$, $\theta := (\alpha + 2\pi k)/n$ of z in the equivalence above. Both conditions on the right hold, so $z^n = c$.

(b) The numbers z_k and z_l are given in polar form with the same modulus. By Proposition 1.5.4 (b), $z_k = z_l$ if and only if

$$\frac{\alpha + 2\pi k}{n} - \frac{\alpha + 2\pi l}{n} = \frac{2\pi(k-l)}{n} \in 2\pi\mathbb{Z},$$

that is, if and only if $2\pi(k-l)/n = 2\pi m$ for some $m \in \mathbb{Z}$. Multiplying by $n/(2\pi)$, and back, this says $k - l = mn$, an equation between integers. So $z_k = z_l$ if and only if $n \mid k - l$.

(c) By (a), each z_k is a solution, so the map is into the set of solutions. *Injective:* let $0 \leq l < k \leq n-1$. Then $0 < k - l < n$. If $z_k = z_l$, then $n \mid k - l$ by (b), and since $n > 0$ and $k - l > 0$, Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e) gives $n \leq k - l$, a contradiction. So $z_k \neq z_l$. *Surjective:* let $z^n = c$. By (a), $z = z_k$ for some $k \in \mathbb{Z}$. Division with remainder (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2 (a)) gives $k = qn + j$ with $q \in \mathbb{Z}$ and $0 \leq j \leq n-1$. Then $n \mid k - j$, so $z = z_k = z_j$ by (b). Hence the map is a bijection. Composing it with the bijection $\{1, \dots, n\} \to \{0, \dots, n-1\}$, $j \mapsto j - 1$, shows that the set of solutions has n elements (Sets, Relations, and Cardinality, Definition 3.1.2).

Finally, z_0 is an n-th root of c. If $|c| = 1$, then $\rho = 1$ and $\sqrt[n]{1} = 1$, since $1 \geq 0$ and $1^n = 1$; so every z_k has modulus 1 and lies in $\mathbb{T}$.

■

The answer to the prompt: the uniqueness half of the polar form, Proposition 1.5.4 (b), turns the one complex equation $z^n = c$ into the two real conditions, and is used again in (b) to decide when two of the z_k coincide. The uniqueness of the real root forces the modulus, $r = \sqrt[n]{\rho}$. The ambiguity $2\pi\mathbb{Z}$ in the angle is what produces n roots instead of one.

Warning. Dividing the angle equation by n too early loses roots. From $z^3 = 1$, $z = e^{i\theta}$, one might write $e^{3i\theta} = e^{i0}$, "so $3\theta = 0$ and $z = 1$". But $e^{3i\theta} = e^{i0}$ only gives $3\theta \in 2\pi\mathbb{Z}$ (Proposition 1.5.4 (b)), and the angles $2\pi/3$ and $4\pi/3$ give two more cube roots of 1. Only the remainders $0, \dots, n-1$ of k matter, but all of them do.

1.6.3 Roots of unity

The most important case is $c = 1$.

Example. Roots of Unity

Let $n \geq 1$ be an integer. Find all $z \in \mathbb{C}$ with $z^n = 1$, and draw them for $n = 6$.

Solution. Apply Theorem 1.6.2 with $c = 1 = 1 \cdot e^{i0}$ (Theorem 1.5.3 (b)): $\rho = 1$, $\alpha = 0$, and $\sqrt[n]{1} = 1$. The solutions are

$$z_k = e^{2\pi i k/n}, \qquad k \in \mathbb{Z}.$$

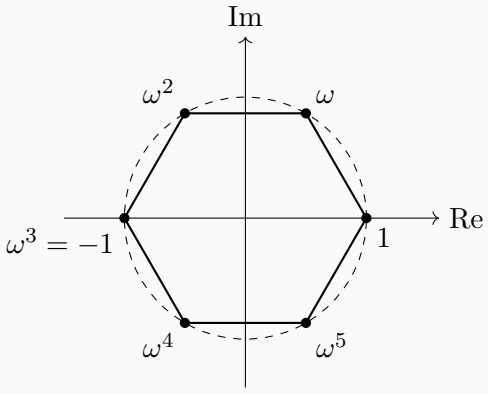
Put $\omega := e^{2\pi i/n}$. By Theorem 1.5.5, $z_k = (e^{2\pi i/n})^k = \omega^k$ for $k \in \mathbb{N}$. By Theorem 1.6.2 (c), there are exactly n solutions,

$$1,\ \omega,\ \omega^2,\ \dots,\ \omega^{n-1},$$

the **n-th roots of unity**. They lie on $\mathbb{T}$, at the arguments $2\pi k/n$, equally spaced around the circle: multiplying by ω turns each one into the next (Theorem 1.5.3 (a)), and ω^{n-1} back into $\omega^n = z_n = z_0 = 1$ (Theorem 1.6.2 (b)). For $n \geq 3$ they are the corners of a regular polygon with n corners, one of them at 1; for $n = 2$ they are 1 and $\omega = e^{i\pi} = -1$ (Example (Special Angles) (i)); for $n = 1$ only 1.

For $n = 6$, $\omega = e^{i\pi/3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ (Example (Special Angles) (iii)), and $\omega^3 = e^{i\pi} = -1$. Hence $\omega^2 = \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^2 = \frac{1}{4} - \frac{3}{4} + \frac{\sqrt{3}}{2}i = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\omega^4 = -\omega$ and $\omega^5 = -\omega^2$. The six roots are

$$1, \quad \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, \quad -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, \quad -1, \quad -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i, \quad \tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i.$$



The six roots sum to 0: since $\omega^3 = -1$, we have $\omega^{k+3} = -\omega^k$, so the roots cancel in the

opposite pairs $\{1,\omega^3\}$, $\{\omega,\omega^4\}$, $\{\omega^2,\omega^5\}$. In the picture, the hexagon is symmetric about its center 0. In general the sum is Proposition 1.6.3 below.

We write $\mu_n := \{z \in \mathbb{C} : z^n = 1\} = \{1, \omega, \dots, \omega^{n-1}\}$ for the set of n-th roots of unity. It is a subset of $\mathbb{T}$, since each element is some $z_k = e^{2\pi ik/n}$ (Theorem 1.6.2 (a)). It contains 1, and it is closed under products, since $(\zeta\eta)^n = \zeta^n\eta^n = 1$ for $\zeta, \eta \in \mu_n$ (Proposition 1.1.3 (c)). It is closed under inverses, since $\zeta \cdot \zeta^{n-1} = \zeta^n = 1$ gives $\zeta^{-1} = \zeta^{n-1}$, a product of elements of μ_n (for $n = 1$, $\zeta^0 = 1$). Chapter 3 treats μ_n, like $\mathbb{T}$, as an example of a group.

The roots of unity also describe the roots of any $c \neq 0$: the root $z_0 = \sqrt[n]{\rho}\, e^{i\alpha/n}$ of Theorem 1.6.2 satisfies $z_k = z_0\,\omega^k$ for $k \in \mathbb{N}$, by Theorem 1.5.3 (a) and Theorem 1.5.5, since $(\alpha + 2\pi k)/n = \alpha/n + 2\pi k/n$. So by Theorem 1.6.2 (c) the n-th roots of c are $z_0, z_0\omega, \dots, z_0\omega^{n-1}$: one of them times the n-th roots of unity.

The six roots canceled in pairs. The same pairing works for every even n, since $\omega^{n/2} = e^{i\pi} = -1$ (Theorem 1.5.5, Example (Special Angles) (i)) gives $\omega^{k+n/2} = -\omega^k$; but for odd n there are no opposite pairs: if ζ and $-\zeta$ were both n-th roots of unity, then $1 = (-\zeta)^n = (-1)^n\zeta^n = -1$. A different argument is needed. It is Lemma 1.1.4 once more.

Proposition 1.6.3. Sums of Roots of Unity

Let $n \in \mathbb{N}$ with $n \geq 2$, and let $\omega := e^{2\pi i/n}$.

(a) For $m \in \mathbb{N}$: $\omega^m = 1$ if and only if $n \mid m$. In particular $\omega \neq 1$.

(b) $\displaystyle\sum_{k=0}^{n-1} \omega^k = 0.$

(c) For $m \in \mathbb{N}$,

$$\sum_{k=0}^{n-1} \omega^{mk} = \begin{cases} n & \text{if } n \mid m, \\ 0 & \text{otherwise.} \end{cases}$$

Idea. Put $\zeta := \omega^m$. The sum in (c) is $1 + \zeta + \cdots + \zeta^{n-1}$, and Lemma 1.1.4 multiplies it by $\zeta - 1$ to give $\zeta^n - 1 = 0$. If $\zeta \neq 1$ we may cancel, and the sum is 0; if $\zeta = 1$ it is n. Part (a) decides which case occurs.

Proof. We use the notation of Example (Roots of Unity): $z_k = e^{2\pi ik/n}$ are the roots of $c = 1$ in Theorem 1.6.2, and $\omega^m = z_m$ for $m \in \mathbb{N}$ (Theorem 1.5.5).

(a) Since $1 = z_0$, Theorem 1.6.2 (b) gives $\omega^m = 1 \iff z_m = z_0 \iff n \mid m$. For $m = 1$: if $n \mid 1$, then $n \leq 1$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e), against $n \geq 2$. So $\omega \neq 1$.

(b) Let $\zeta := \omega^m$. By Proposition 1.1.3 (b), $\omega^{mk} = \zeta^k$ for each k, and $\zeta^n = \omega^{mn} = (\omega^n)^m = 1^m = 1$, since $\omega^n = z_n = z_0 = 1$ by Theorem 1.6.2 (b).

Case $n \mid m$. Then $\zeta = 1$ by (a), and the sum is $\sum_{k=0}^{n-1} 1 = n$.

Case $n \nmid m$. Then $\zeta \neq 1$ by (a). By Lemma 1.1.4 with $w = 1$,

$$0 = \zeta^n - 1 = (\zeta - 1)\sum_{k=0}^{n-1} \zeta^k.$$

Since $\zeta - 1 \neq 0$ and $\mathbb{C}$ has no zero divisors (Theorem 1.2.4, Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (d)), the sum is 0.

(b) This is (c) with $m = 1$, since $n \nmid 1$ by (a).

■

Comparing real and imaginary parts in (b), with $\omega^k = \cos(2\pi k/n) + i\sin(2\pi k/n)$ (Theorem 1.5.5), gives two real identities that are awkward to prove any other way: for $n \geq 2$,

$$\sum_{k=0}^{n-1} \cos\frac{2\pi k}{n} = 0 \qquad \text{and} \qquad \sum_{k=0}^{n-1} \sin\frac{2\pi k}{n} = 0.$$

Part (c) says more: the sum of the m-th powers of the roots of unity detects whether n divides m.

Quick check. Write the three cube roots of unity in the form $a + bi$.

Solution. By Example (Roots of Unity) with $n = 3$, they are 1, ω, ω^2 with $\omega = e^{2\pi i/3} = (e^{i\pi/3})^2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ (Theorem 1.5.5, and the square computed for $n = 6$ above). Since $\omega \in \mathbb{T}$ and $\omega \cdot \omega^2 = \omega^3 = 1$, $\omega^2 = \omega^{-1} = \overline{\omega} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ (Proposition 1.5.1 (a)). So the cube roots of unity are 1 and $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. Without angles: $z^3 - 1 = (z-1)(z^2 + z + 1)$, and Corollary 1.4.2 applied to $z^2 + z + 1 = 0$, with $d = \sqrt{3}\,i$ a square root of $1 - 4 = -3$, gives $z = (-1 \pm \sqrt{3}\,i)/2$.

1.6.4 Polynomial equations, and a look ahead

An n-th root of c solves $z^n - c = 0$, a polynomial equation of degree n with only two non-zero coefficients. The general question is whether every equation

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0, \qquad a_0, \ldots, a_n \in \mathbb{C},\ a_n \neq 0,\ n \geq 1,$$

has a solution in $\mathbb{C}$. Here the left side is a **polynomial expression** $\sum_{k=0}^{n} a_k z^k$, a finite sum; Chapter 4 makes polynomials objects in their own right. We built $\mathbb{C}$ so that one such equation, $z^2 + 1 = 0$, has a solution, and Section 1.4 solved every equation of degree 2. It turns out that nothing more ever needs to be added.

Remark (Looking ahead). Section 5.6 proves that every such equation has a solution in $\mathbb{C}$: the Fundamental Theorem of Algebra. Its proof uses only the square roots of Section 1.4 and the completeness of $\mathbb{R}$, not polar form and not the borrowed facts about cosine and sine. With division of polynomials, Chapter 5 deduces that every complex polynomial of degree $n \geq 1$ is a non-zero constant times a product of n factors of the form $z - z_j$. Nothing in Chapters 1–4 uses the theorem.

One companion fact needs no heavy machinery: when the coefficients are real, the solutions that are not real come in conjugate pairs.

Proposition 1.6.4. Real Coefficients and Conjugate Roots

Let $n \in \mathbb{N}$, let $a_0, \dots, a_n \in \mathbb{R}$, and let $z \in \mathbb{C}$. Then

$$\overline{\sum_{k=0}^{n} a_k z^k} = \sum_{k=0}^{n} a_k \, \overline{z}^{\,k}.$$

Hence, if $\sum_{k=0}^{n} a_k z_0^k = 0$ for some $z_0 \in \mathbb{C}$, then also $\sum_{k=0}^{n} a_k \overline{z_0}^{\,k} = 0$.

Proof. First, $\overline{z^k} = \overline{z}^{\,k}$ for every $k \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1 on k: $\overline{z^0} = \overline{1} = 1 = \overline{z}^{\,0}$, since 1 is real (Proposition 1.2.1); and if $\overline{z^k} = \overline{z}^{\,k}$, then $\overline{z^{k+1}} = \overline{z^k z} = \overline{z^k}\,\overline{z} = \overline{z}^{\,k}\overline{z} = \overline{z}^{\,k+1}$, by Theorem 1.2.2 (b). Next, $\overline{a_k} = a_k$ since a_k is real (Proposition 1.2.1), so $\overline{a_k z^k} = a_k \overline{z}^{\,k}$, again by Theorem 1.2.2 (b). Finally, the conjugate of a finite sum is the sum of the conjugates, by induction on the number of terms along the recursion for finite sums, with Theorem 1.2.2 (a) in the step. This proves the identity. If $\sum a_k z_0^k = 0$, then $\sum a_k \overline{z_0}^{\,k} = \overline{0} = 0$. ∎

A solution z_0 that is not real gives a **second** solution: $\overline{z_0} \neq z_0$, since $z_0 = x + yi$ with $y \neq 0$ has $\overline{z_0} = x - yi$, and $-y \neq y$. For example, $z^2 - 2z + 5 = 0$ has the solution $1 + 2i$, since $(1+2i)^2 - 2(1+2i) + 5 = (-3+4i) - (2+4i) + 5 = 0$; so it also has the solution $1 - 2i$. Chapter 5 uses this to factor real polynomials into real factors of degree 1 and 2.

1.6.5 Exercises

1.6.5.1 A. Check your understanding

Exercise. A1

(a) Find all $z \in \mathbb{C}$ with $z^4 = 1$.

(b) In the proof of Theorem 1.6.2, where is the uniqueness half of Proposition 1.5.4 used?

(c) In the same proof, why is the modulus r of a solution forced to be $\sqrt[n]{\rho}$?

(d) True or false: $z^3 = 1$ has exactly three solutions in $\mathbb{C}$, and exactly one of them is real. Justify your answer.

(e) State the idea of the proof of Theorem 1.6.2 in two sentences.

Solution.

(a) By Example (Roots of Unity) with $n = 4$, the solutions are ω^k for $k = 0, 1, 2, 3$, where $\omega = e^{2\pi i/4} = e^{i\pi/2} = i$ (Example (Special Angles) (ii)): 1, i, -1, $-i$.

(b) Twice. In (a), to turn $r^n e^{in\theta} = \rho e^{i\alpha}$ into the two conditions $r^n = \rho$ and $n\theta - \alpha \in 2\pi\mathbb{Z}$. In (b), to decide when $z_k = z_l$.

(c) Because $r > 0$ and $r^n = \rho$, and Lemma 1.6.1 (b) says that $\sqrt[n]{\rho}$ is the **only** non-negative real number with n-th power ρ.

(d) True. By Theorem 1.6.2 (c) there are exactly three. By the Check above they are 1 and $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$; the last two have imaginary part $\pm\frac{\sqrt{3}}{2} \neq 0$, so only 1 is real.

(e) Polar form and De Moivre split $z^n = c$ into a real equation for the modulus, which has exactly one positive solution, and an equation for the argument, which is solved up to the ambiguity $2\pi\mathbb{Z}$. That ambiguity, divided by n, produces n different roots, one for each remainder modulo n.

1.6.5.2 B. Practice

Exercise. B1

Find all $z \in \mathbb{C}$ with $z^3 = -8i$, in the form $a + bi$.

Solution. By Example (Special Angles) (ii) and Theorem 1.5.3 (b), $e^{-i\pi/2} = \overline{e^{i\pi/2}} = \bar{i} = -i$, so $-8i = 8e^{-i\pi/2}$ is a polar form, with $\rho = 8$ and $\alpha = -\pi/2$. Also $\sqrt[3]{8} = 2$. By Theorem 1.6.2, the solutions are $z_k = 2e^{i(-\pi/2+2\pi k)/3} = 2e^{i(-\pi/6+2\pi k/3)}$ for $k = 0, 1, 2$, with arguments $-\pi/6$, $\pi/2$ and $7\pi/6$:

$$z_0 = 2e^{-i\pi/6} = 2\,\overline{e^{i\pi/6}} = \sqrt{3} - i, \qquad z_1 = 2e^{i\pi/2} = 2i,$$

$$z_2 = 2e^{i\pi}e^{i\pi/6} = -2\Big(\frac{\sqrt{3}}{2} + \frac{1}{2}i\Big) = -\sqrt{3} - i,$$

by Example (Special Angles) (i), (ii), (iv) and Theorem 1.5.3. Check: $(2i)^3 = 8i^3 = -8i$, and $(\sqrt{3}-i)^2 = 2 - 2\sqrt{3}\,i$, so $(\sqrt{3}-i)^3 = (2-2\sqrt{3}\,i)(\sqrt{3}-i) = 2\sqrt{3} - 2i - 6i - 2\sqrt{3} = -8i$.

Exercise. B2

Find all $z \in \mathbb{C}$ with $z^4 = -4$, in the form $a + bi$, and check one of them directly.

Solution. A polar form is $-4 = 4e^{i\pi}$ (Example (Special Angles) (i)), and $\sqrt[4]{4} = \sqrt{2}$, since $\sqrt{2} \geq 0$ and $(\sqrt{2})^4 = 4$. By Theorem 1.6.2, the solutions are $z_k = \sqrt{2}\,e^{i(\pi+2\pi k)/4}$ for $k = 0, 1, 2, 3$. First, $z_0 = \sqrt{2}\,e^{i\pi/4} = 1 + i$ (Example (Special Angles) (v)). Next, $(\pi + 2\pi(k+1))/4 = (\pi + 2\pi k)/4 + \pi/2$, so $z_{k+1} = z_k e^{i\pi/2} = iz_k$ (Theorem 1.5.3 (a), Example (Special Angles) (ii)). Hence

$$z_0 = 1 + i, \quad z_1 = -1 + i, \quad z_2 = -1 - i, \quad z_3 = 1 - i,$$

that is, $z = \pm 1 \pm i$ with all four choices of signs. Check: $(1+i)^2 = 2i$, so $(1+i)^4 = (2i)^2 = -4$.

Exercise. B3

Let $n \geq 1$ and $\omega := e^{2\pi i/n}$. Show that $1 \in \mu_n$, that μ_n is closed under multiplication, that for $k = 1, \ldots, n-1$ the inverse of ω^k is ω^{n-k}, and that $\mu_n \subseteq \mathbb{T}$.

Solution. $1^n = 1$, so $1 \in \mu_n$. If $\zeta^n = \eta^n = 1$, then $(\zeta\eta)^n = \zeta^n\eta^n = 1$ by Proposition 1.1.3 (c). For $1 \leq k \leq n-1$, $\omega^k\omega^{n-k} = \omega^n = 1$ by Proposition 1.1.3 (a) and Proposition 1.6.3 (a) (or

Example (Roots of Unity)), so ω^{n-k} is the inverse of ω^k, and it lies in μ_n. Finally let $\zeta \in \mu_n$. Then $|\zeta|^n = |\zeta^n| = |1| = 1$, where the first equality is Theorem 1.2.2 (d) applied n times (induction on n). Since $|\zeta| \geq 0$ and also $1 \geq 0$ with $1^n = 1$, the uniqueness in Lemma 1.6.1 (b) gives $|\zeta| = 1$. So $\zeta \in \mathbb{T}$. (This last argument uses no borrowed fact.)

1.6.5.3 C. Going deeper

Exercise. C1: Exit check: n-th roots

Let $n \geq 1$ and $c \in \mathbb{C}$ with $c \neq 0$, and let $c = \rho e^{i\alpha}$ be a polar form. Prove parts (a) and (b) of Theorem 1.6.2: the solutions of $z^n = c$ are exactly the numbers $z_k = \sqrt[n]{\rho}\, e^{i(\alpha+2\pi k)/n}$, $k \in \mathbb{Z}$, and $z_k = z_l$ if and only if $n \mid k - l$. Cite the polar form, De Moivre's formula and the real n-th root where you use them.

Solution. Here $\rho = |c| > 0$ (Proposition 1.5.4 (a)). The number 0 is not a solution, since $0^n = 0 \neq c$, and is no z_k, since $|z_k| = \sqrt[n]{\rho} > 0$ (Lemma 1.6.1 (b)). For $z \neq 0$, fix a polar form $z = re^{i\theta}$ with $r > 0$ (Proposition 1.5.4 (a)); then $z^n = r^n e^{in\theta}$ (Theorem 1.5.5), a polar form with $r^n > 0$, and by the uniqueness of polar form (Proposition 1.5.4 (b)), $z^n = \rho e^{i\alpha}$ if and only if $r^n = \rho$ and $n\theta - \alpha \in 2\pi\mathbb{Z}$. The first condition is $r = \sqrt[n]{\rho}$, by existence and uniqueness of the real n-th root (Lemma 1.6.1 (b)); the second is $\theta = (\alpha + 2\pi k)/n$ for some $k \in \mathbb{Z}$. So $z^n = c$ implies $z = z_k$; conversely, applied to the polar form $r := \sqrt[n]{\rho}$, $\theta := (\alpha + 2\pi k)/n$ of $z = z_k$, the equivalence gives $z^n = c$. For (b), z_k and z_l are given in polar form with the same modulus, so the same uniqueness gives $z_k = z_l$ if and only if $2\pi(k - l)/n \in 2\pi\mathbb{Z}$, if and only if $k - l = mn$ for some $m \in \mathbb{Z}$, that is, $n \mid k - l$.

Marking scheme. (10 points) - 1: rules out $z = 0$, with the reason $0^n = 0 \neq c$. - 2: writes z (and c) in polar form and applies De Moivre's formula to get $z^n = r^n e^{in\theta}$. - 3: splits $z^n = c$ into $r^n = \rho$ and $n\theta - \alpha \in 2\pi\mathbb{Z}$, citing the uniqueness of polar form, and states both directions (every z_k is a solution, every solution is some z_k). - 1: $r = \sqrt[n]{\rho}$, with both existence and uniqueness of the real n-th root cited (the point is lost if either is assumed without citation). - 3: (b), $z_k = z_l \iff n \mid k - l$, both directions. Fatal errors (0 for the step): concluding $n\theta = \alpha$, or $\theta = \alpha/n$, from $e^{in\theta} = e^{i\alpha}$ (dropping $2\pi\mathbb{Z}$); writing $\sqrt[n]{c}$ for a complex c. Second route: find one root z_0 and show that $z^n = c$ if and only if $(z/z_0)^n = 1$, then solve $w^n = 1$ by polar form. The same points apply, with the 3 points of the third line awarded for the roots of unity, and (b) replaced by the distinctness of $1, \omega, \ldots, \omega^{n-1}$ and the periodicity $\omega^{k+n} = \omega^k$.

Exercise. C2: Find the error

Here is an argument.

> **Claim.** For $n \geq 2$, the n-th roots of unity sum to 0.
>
> (1) Let $\omega := e^{2\pi i/n}$ and $S := 1+\omega+\cdots+\omega^{n-1}$. (2) Then $\omega S = \omega+\omega^2+\cdots+\omega^n = S$, since $\omega^n = 1$. (3) So $(\omega - 1)S = 0$. (4) Since ω is an n-th root of unity, $\omega^n = 1$, so $\omega \neq 1$. (5) Hence $\omega - 1 \neq 0$, and $S = 0$.

Is the claim true? Does the argument prove it? If not, name the first line that fails, say what is wrong with it, give a counterexample to the step, and repair the argument.

Solution. The claim is true: it is Proposition 1.6.3 (b).

The argument does not prove it. Lines (1)–(3) are correct: $\omega^n = 1$ by Example (Roots of Unity), and (3) is (2) rearranged. Line (5) is correct **given** (4), since $\mathbb{C}$ has no zero divisors. Line (4) fails. "$\omega^n = 1$, so $\omega \neq 1$" cites a general "fact", that an n-th root of unity is not 1, which is false: this is the error (N9) of Logic and Proof, Example (What is not allowed). *Counterexample to the step:* 1 itself satisfies $1^n = 1$, and $1 = 1$. Being an n-th root of unity gives no information that separates ω from 1; the information is in the particular choice $\omega = e^{2\pi i/n}$ with $n \geq 2$.

Repair. If $\omega = e^{2\pi i/n} = 1 = e^{i0}$, then $2\pi/n \in 2\pi\mathbb{Z}$ by Proposition 1.5.4 (b), so $1/n = m$ for some $m \in \mathbb{Z}$, that is, $1 = mn$ and $n \mid 1$. Since $n \geq 2 > 0$, Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e) gives $n \leq 1$, a contradiction. So $\omega \neq 1$, and lines (5) and the conclusion stand. (This repair uses (T1)–(T3) of Axiom 1.5.2, through Proposition 1.5.4 (b), and no value of the cosine.)

1.6.5.4 R. Review

Exercise. R1

Let $\sigma\colon \mathbb{C} \to \mathbb{C}$ satisfy $\sigma(z+w) = \sigma(z) + \sigma(w)$ and $\sigma(zw) = \sigma(z)\sigma(w)$ for all $z, w \in \mathbb{C}$, $\sigma(1) = 1$, and $\sigma(a) \in \mathbb{R}$ for every $a \in \mathbb{R}$.

(a) Prove that either $\sigma(z) = z$ for every $z \in \mathbb{C}$, or $\sigma(z) = \overline{z}$ for every $z \in \mathbb{C}$.

(b) Show that conjugation $z \mapsto \overline{z}$ satisfies all the hypotheses on σ.

Solution.

(a) Since σ maps $\mathbb{R}$ into $\mathbb{R}$, it restricts to a map $\tau\colon \mathbb{R} \to \mathbb{R}$, $\tau(a) := \sigma(a)$, which preserves sums and products and sends 1 to 1. Since $\mathbb{R}$ is a complete ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3), Number Systems: From \(\nN\) to \(\nR\), Theorem 6.3.4 gives $\tau = \mathrm{id}_{\mathbb{R}}$: $\sigma(a) = a$ for every real a. In particular $\sigma(-1) = -1$, so

$$\sigma(i)^2 = \sigma(i \cdot i) = \sigma(-1) = -1 = i^2.$$

So $(\sigma(i) - i)(\sigma(i) + i) = 0$, and $\sigma(i) = i$ or $\sigma(i) = -i$ (no zero divisors in $\mathbb{C}$; or Proposition 1.4.1 (b)). For $z = a + bi$ with $a, b \in \mathbb{R}$,

$$\sigma(z) = \sigma(a) + \sigma(b)\sigma(i) = a + b\,\sigma(i).$$

If $\sigma(i) = i$, then $\sigma(z) = z$ for every z; if $\sigma(i) = -i$, then $\sigma(z) = a - bi = \overline{z}$ for every z.

(b) Conjugation preserves sums and products by Theorem 1.2.2 (a), (b), and $\overline{a} = a$ for every real a (Proposition 1.2.1), so in particular $\overline{1} = 1$ and real numbers go to real numbers.

The comparison with *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 6 (Number Systems: From \(\nN\) to \(\nR\), Theorem 6.3.4) is the point: $\mathbb{R}$ has only the identity, while $\mathbb{C}$ has exactly two such maps. In $\mathbb{R}$ the order can be read off from the field operations (the non-negative numbers are exactly the squares, Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), and a map preserving $+$ and $\cdot$ must preserve it. In $\mathbb{C}$ there is no order (Proposition 1.4.3), and nothing written with $+$, $\cdot$ and real numbers alone tells i from $-i$.

Exercise. R2

Let $n \geq 1$. Show that $[k] \mapsto e^{2\pi ik/n}$ is a well-defined bijection $f\colon \mathbb{Z}/n\mathbb{Z} \to \mu_n$, and that $f([k]+[l]) = f([k])\,f([l])$ for all $k, l \in \mathbb{Z}$.

Solution. Write $z_k := e^{2\pi ik/n}$, the roots of $c = 1$ in Theorem 1.6.2 (with $\rho = 1$, $\alpha = 0$, as in Example (Roots of Unity)). The classes of Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2 are congruence classes: $[k] = [l]$ if and only if $n \mid k - l$. By Theorem 1.6.2 (b), $n \mid k - l$ if and only if $z_k = z_l$. Reading this equivalence from left to right, $f([k]) := z_k$ does not depend on the representative k of the class, so f is well defined; reading it from right to left, f is injective. Each z_k lies in μ_n by Theorem 1.6.2 (a), and every element of μ_n is some z_k, again by (a); so f is surjective. Finally, $[k]+[l] = [k+l]$, and by Theorem 1.5.3 (a),

$$f([k]+[l]) = z_{k+l} = e^{2\pi ik/n}e^{2\pi il/n} = f([k])\,f([l]).$$

As a check on the count, both sets have n elements (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b) and Theorem 1.6.2 (c)). In the language of Chapter 3, f is an isomorphism from the additive structure of $\mathbb{Z}/n\mathbb{Z}$ to the multiplicative structure of μ_n.

Exercise. R3

Let F be an ordered field and $x, y \in F$.

(a) Prove that $|x+y| \leq |x| + |y|$ by comparing the squares of the two sides.

(b) The proof of the same inequality by "trapping" x between $-|x|$ and $|x|$, and adding the traps for x and y, works in every ordered field. Which step of it cannot be carried out for complex x, y, and what replaces it in the complex triangle inequality?

Solution.

(a) Both sides are non-negative. By Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (b), $|x|^2 = x^2$, $|y|^2 = y^2$, $|x+y|^2 = (x+y)^2$ and $|x||y| = |xy|$. Hence

$$(|x| + |y|)^2 - |x+y|^2 = |x|^2 + 2|x||y| + |y|^2 - x^2 - 2xy - y^2 = 2(|xy| - xy) \geq 0,$$

since $xy \leq |xy|$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (c)). So $|x+y|^2 \leq (|x| + |y|)^2$. If $|x+y| > |x| + |y|$, then Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g), applied to these non-negative elements, would give $|x+y|^2 > (|x| + |y|)^2$; so $|x+y| \leq |x| + |y|$.

(b) The trapping proof (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (e), proved from (c)) uses $-|x| \leq x \leq |x|$: it compares x itself with real numbers. For a complex x that is not real such a comparison means nothing, since no order on $\mathbb{C}$ is compatible with its arithmetic (Proposition 1.4.3). The squaring proof of (a) is the one that survives: in the complex triangle inequality (Theorem 1.3.2) the cross term $2\,\mathrm{Re}(z\overline{w})$ is bounded by a comparison between **real** numbers, $\mathrm{Re}\,u \leq |u|$ (Lemma 1.3.1), which replaces $xy \leq |xy|$ here.

Exercise. R4

Find all $z \in \mathbb{C}$ with $\overline{z} = z^2$.

Solution. The tool: take moduli first. If $\overline{z} = z^2$, then $|z| = |\overline{z}| = |z^2| = |z|^2$ (Theorem 1.2.2 (d)), so $|z|(|z| - 1) = 0$ and $|z| = 0$ or $|z| = 1$.

If $|z| = 0$, then $z = 0$ (Theorem 1.2.2 (e)), and $z = 0$ is a solution.

If $|z| = 1$, multiply $\overline{z} = z^2$ by z: $1 = z\overline{z} = z^3$ (Theorem 1.2.2 (c)). So z is a cube root of unity: $z = 1$ or $z = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ (the Check above). Conversely, each cube root of unity ζ lies in $\mathbb{T}$ (Exercise B3), so $\overline{\zeta} = \zeta^{-1}$ (Proposition 1.5.1 (a)), and $\zeta^{-1} = \zeta^2$ because $\zeta \cdot \zeta^2 = \zeta^3 = 1$. So each is a solution.

The solutions are 0, 1, $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$.

Why the look-alike tools are worse. Comparing real and imaginary parts, with $z = x + yi$, gives $x^2 - y^2 = x$ and $2xy = -y$, which can be solved, but only with a case split by hand ($y = 0$ or $x = -\frac{1}{2}$). "Divide $\overline{z} = z^2$ by z" silently loses the solution $z = 0$. Polar form works, but it is not needed: the moduli settle $|z|$, and the cube roots of unity can be found without angles, as in the Check.

Chapter 2

Fields

Linear algebra solves equations by adding, subtracting, multiplying, and dividing by numbers that are not zero, and by nothing else. A field is a number system in which exactly these moves work, under the usual rules. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$ already defined fields and built three kinds of them: $\mathbb{Q}$, $\mathbb{R}$, and the integers modulo a prime p. Chapter 1 added $\mathbb{C}$. This chapter studies fields as a kind of object in their own right. It covers the rules every field obeys, the finite fields $\mathbb{F}_p$ and how to compute in them, fields inside fields, maps between fields that respect both operations, and one number, the **characteristic**, that says whether $1+1+\cdots+1$ can ever be 0. That number decides whether "$2x = 0$, so $x = 0$" is a valid step, and the linear-algebra volumes ask about it again and again.

Two facts organize the chapter. A homomorphism of fields is forced to be injective, because a non-zero element has an inverse and its image must have one too. And every field contains exactly one smallest subfield, a copy of $\mathbb{Q}$ or of exactly one $\mathbb{F}_p$, onto which there is exactly one homomorphism. The chapter ends with the identity $(x + y)^p = x^p + y^p$, which holds in every field of characteristic p and fails for other exponents and in rings of composite characteristic. Fermat's little theorem then takes a few lines: on $\mathbb{F}_p$ the map $x \mapsto x^p$ is a homomorphism of $\mathbb{F}_p$ to itself, and the only such map is the identity.

One definition, two books. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2 defined "field" (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1), and the linear-algebra volumes cite the definition as Definition 2.1.1. Section 2.1 restates it under that name with the clauses (F1)–(F9) numbered as both books number them. A remark there proves that the two definitions describe the same objects; they differ only in where the condition $1 \neq 0$ is filed, inside (F7) here and as a clause of its own in *Number Systems*. Where *Number Systems* already proved a result, this chapter cites it. So Theorem 2.1.1 takes parts (a), (d) and (e) and the uniqueness of negatives from Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2, and the uniqueness of inverses, the absence of zero divisors and the inverse identities of part (g) from the paragraphs on units after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1, and proves cancellation and the fraction rules itself, and the proof of Theorem 2.2.2 is a citation of Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2.

What you need. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapters 2 and 3 above all; Chapter 1 of this volume, for examples; and smaller pieces of *Sets, Relations, and Cardinality* and *Logic and Proof*.

- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2: commutative rings and fields and their algebra (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2), on nearly every page; the integers as a com-

mutative ring (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1), for the non-examples of Section 2.1; the copy of $\mathbb{N}$ in $\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3), in Sections 2.1, 2.3 and 2.4 and for integer multiples in Section 2.5; the integers as an ordered ring (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.4), for negative multiples in Section 2.5; and the least element of a set of integers bounded below (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6), which makes the characteristic well defined in Section 2.5; the multiples $n \cdot a$ of the "Multiples" paragraph of its Section 2.3, which Section 2.5 extends to negative n; ordered fields and their rules (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5), and the order on $\mathbb{Q}$ from its positive elements (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.3), in a quick check of Section 2.1; the field $\mathbb{Q}$, built as classes of pairs (Number Systems: From \(\nN\) to \(\nR\), Definition 2.4.1, Number Systems: From \(\nN\) to \(\nR\), Definition 2.4.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 2.2.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3, Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4), which Section 2.5 maps into every field of characteristic 0; the irrationality of $\sqrt{2}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1), used in Section 2.3; and the two-element ring that cannot be ordered (Number Systems: From \(\nN\) to \(\nR\), Example (A field with two elements that cannot be ordered)), compared with in Section 2.2.

- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3: division with remainder, parity and the rules for divisibility (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2, Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3, Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1); the gcd, Bézout's theorem, Euclid's lemma and the test for primes (Number Systems: From \(\nN\) to \(\nR\), Definition 3.2.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.2.1, Number Systems: From \(\nN\) to \(\nR\), Corollary 3.2.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.3.1, Number Systems: From \(\nN\) to \(\nR\), Corollary 3.3.2, Number Systems: From \(\nN\) to \(\nR\), Lemma 3.3.4); quotient rings and the rings $\mathbb{Z}/n\mathbb{Z}$, with the example $\mathbb{Z}/6\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1, Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3, Number Systems: From \(\nN\) to \(\nR\), Example (Multiplication modulo six and modulo five)); and units, their inverses modulo n, and the field $\mathbb{Z}/p\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2). Section 2.2 gives these fields the name $\mathbb{F}_p$ that its Section 3.5 left to this chapter. Its move "least positive element, then divide" proves Proposition 2.5.2.
- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapters 4–6, for examples, comparisons and a few exercises only: $\mathbb{R}$ as a complete ordered field containing $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.2.3, Number Systems: From \(\nN\) to \(\nR\), Theorem 5.3.3, Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3, Number Systems: From \(\nN\) to \(\nR\), Definition 5.4.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 5.4.1), from its Chapter 5; square roots in $\mathbb{R}$, the field $\mathbb{Q}(\sqrt{2})$ and its conjugation, and the theorem that $\mathbb{R}$ has no automorphism but the identity (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4, Number Systems: From \(\nN\) to \(\nR\), Definition 6.4.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 6.4.5, Number Systems: From \(\nN\) to \(\nR\), Proposition 6.4.6, Number Systems: From \(\nN\) to \(\nR\), Example (Conjugation in $\mathbb{Q}(\sqrt{2})$), Number Systems: From \(\nN\) to \(\nR\), Definition 6.1.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 6.3.4, Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.1), from its Chapter 6; and the fraction rules and the embedding of $\mathbb{Q}$ into an ordered field (Number Systems: From \(\nN\)

to \(\nR\), Lemma 4.1.1, Number Systems: From \(\nN\) to \(\nR\), Proposition 4.2.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 4.2.2), from its Chapter 4, which remarks in Sections 2.1 and 2.5 compare with.

- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 1: the citing rule by which induction and recursion apply to $\mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3), in Sections 2.4–2.6, and the axioms (Z5) and (Z6) (Number Systems: From \(\nN\) to \(\nR\), Axiom 1.1.1) that make the set of subfields containing a given set a set, in Section 2.3.
- From Chapter 1 of this volume, for examples and review exercises only: $\mathbb{C}$ as a field containing $\mathbb{R}$ (Definition 1.1.1, Proposition 1.1.1, Proposition 1.1.2, Proposition 1.2.3, Theorem 1.2.4); conjugation and its rules (Definition 1.2.1, Theorem 1.2.2), the first automorphism of Section 2.4; complex square roots (Proposition 1.4.1), compared with in Section 2.1 and used in Exercise R1 of Section 2.6; the power laws in a commutative ring (Proposition 1.1.3), compared with in Section 2.6; and the method by which $\mathbb{C}$ cannot be ordered (Proposition 1.4.3), reused in Exercise R3 of Section 2.6.
- From *Sets, Relations, and Cardinality*: functions, composition, bijections, inverse functions and images, and intersections of families of sets (Sets, Relations, and Cardinality, Definition 1.4.5, Sets, Relations, and Cardinality, Definition 1.4.2, Sets, Relations, and Cardinality, Theorem 1.4.4, Sets, Relations, and Cardinality, Definition 1.5.2, Sets, Relations, and Cardinality, Theorem 1.5.4, Sets, Relations, and Cardinality, Definition 1.6.1, Sets, Relations, and Cardinality, Definition 1.2.4), from its Chapter 1; primes, quotient sets, and the recursion theorem with its sums and powers, whose proofs Section 2.6 reuses in any commutative ring (Sets, Relations, and Cardinality, Definition 2.2.2, Sets, Relations, and Cardinality, Definition 2.5.4, Sets, Relations, and Cardinality, Theorem 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.2, Sets, Relations, and Cardinality, Proposition 2.3.4), from its Chapter 2; finite and infinite sets and the pigeonhole principle (Sets, Relations, and Cardinality, Definition 3.1.2, Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations, and Cardinality, Example (Hilbert's Hotel), Sets, Relations, and Cardinality, Theorem 3.1.2, Sets, Relations, and Cardinality, Corollary 3.1.3, Sets, Relations, and Cardinality, Theorem 3.1.9), from its Chapter 3.
- From *Logic and Proof*: induction (Logic and Proof, Axiom 4.2.1), from its Section 3.2, and, for the five find-the-error exercises and the proof-ordering exercise of Section 2.3, the catalogue of moves that are not allowed (Logic and Proof, Example (What is not allowed)), from its Section 5.6.

No proof of a result rests on $\mathbb{R}$ or $\mathbb{C}$: they enter through examples, remarks and exercises. Nothing from linear algebra is used, and polynomials appear only as equations between elements, never as objects; Chapters 4 and 5 build them.

Time. About 25 hours on the core track (all of A, one B and one C per section, the exit checks); about 40 hours for everything.

2.0.1 Roadmap

- **The Field Axioms and the First Examples.** What elimination needs, and the definition of a field with the clauses (F1)–(F9) and its agreement with the definition in *Number Systems*; the rules of every field, collected from the commutative-ring rules with the fraction rules added; the two square roots $\pm y$, with $\mathbb{Z}/8\mathbb{Z}$ as the ring where there are more; one linear equation and a system of two, solved in any field; $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ as fields; and $\mathbb{N}$, $\mathbb{Z}$, the zero ring and $\mathbb{Z}/6\mathbb{Z}$ as non-examples, each with the clause that fails.
- **Finite Fields from Modular Arithmetic.** The arithmetic of $\mathbb{Z}/n\mathbb{Z}$ recalled, with the

tables of $\mathbb{F}_2$; Bézout's lemma in the form the linear-algebra volumes cite, and $\mathbb{Z}/n\mathbb{Z}$ as a field exactly for prime n; the fields $\mathbb{F}_p$, with inverses found by trial and by the Euclidean algorithm and the elimination of Section 2.1 run over $\mathbb{F}_5$; why a non-zero class modulo a composite cannot always be divided by, and why $\mathbb{F}_p$ has no order; and, as an exercise, a field with four elements that is not $\mathbb{Z}/4\mathbb{Z}$.

- **Subfields.** Subfields, with examples and one-clause non-examples; the subfield test, which shows that a subfield is a field with the zero and one of the big field and reduces the check to 1, differences and quotients; $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ and $\mathbb{Q}(i) \subseteq \mathbb{C}$ as subfields, with $\mathbb{Z}[i]$ failing only at inverses; the warning that $\{[0],[3]\} \subseteq \mathbb{Z}/6\mathbb{Z}$ is a field with another one; and intersections of subfields, the smallest subfield containing a set, and the prime subfield, which for $\mathbb{F}_p$ is $\mathbb{F}_p$ itself.
- **Field Homomorphisms.** Homomorphisms, isomorphisms and automorphisms, and why $\varphi(1) = 1$ is required; the theorem that a homomorphism keeps 0, negatives and inverses, is injective, and maps its domain onto a subfield isomorphic to it; conjugation of $\mathbb{C}$ and of $\mathbb{Q}(\sqrt{2})$ as automorphisms, and $\mathbb{R}$ with none but the identity; and the pairs $\mathbb{C} \to \mathbb{R}$, $\mathbb{F}_2 \to \mathbb{Q}$ and $\mathbb{Q} \to \mathbb{F}_p$ with no homomorphism at all.
- **Integer Multiples, the Characteristic, and the Prime Subfield.** Integer multiples $n \cdot a$ in a commutative ring, negative n included, with the proof for negative n in a second-reading fold; the characteristic, the theorem that $n \cdot 1 = 0$ exactly when $\operatorname{char} F$ divides n (so 2 is invertible exactly when $\operatorname{char} F \neq 2$), and the theorem that it is 0 or a prime; its invariance under subfields and homomorphisms, and the characteristics of the standard fields; the prime subfield as the image of the unique homomorphism from $\mathbb{Q}$ or $\mathbb{F}_p$, so that a homomorphism has no choice on it and $\mathbb{Q}$ and $\mathbb{F}_p$ have no automorphism but the identity; and finite fields, which have prime characteristic.
- **The Binomial Theorem, the Frobenius Map, and Fermat's Little Theorem.** Finite sums in a commutative ring; binomial coefficients by Pascal's rule, with no division, and the absorption identity; the binomial theorem in a commutative ring and the prime dividing the middle coefficients of row p; the Frobenius map $x \mapsto x^p$, a homomorphism in characteristic p and an automorphism of a finite field; Fermat's little theorem, with powers and inverses computed in $\mathbb{F}_7$, $\mathbb{F}_{31}$ and $\mathbb{F}_{101}$; and review exercises on complex square roots (Chapter 1), square roots in $\mathbb{Q}(\sqrt{2})$, fields that cannot be ordered, and the homomorphisms $\mathbb{Q}(\sqrt{2}) \to \mathbb{R}$.

2.0.2 Named moves

- **Test inside the big field.** For a subset K of a field L, the identities (F1), (F2), (F5), (F6) and (F9) hold in K because they hold for all elements of L; only closure and the elements 0, 1, $-a$ and a^{-1} need checking. It is named in the Idea of the subfield test (Proposition 2.3.1) in Section 2.3. Through that test it shows that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$ are fields and that an intersection of subfields is a subfield in Section 2.3, and that the image of a homomorphism is a subfield in Section 2.4. The warning of Section 2.3 marks its limit: inside a ring that is not a field, a subset can be a field whose one is not that of the ring, as $\{[0],[3]\} \subseteq \mathbb{Z}/6\mathbb{Z}$ is.
- **Push the equation through φ.** To find $\varphi(x)$, apply φ to an equation that x satisfies, such as $a+(-a) = 0$, $aa^{-1} = 1$, $i^2 = -1$ or $p \cdot 1 = 0$, and solve the resulting equation in the target field, where it often has only one solution. It is named in Section 2.4, after the proof of Proposition 2.4.1, whose parts (a) and (b) run it in full. Exercise B1 of Section 2.4 leaves its last step to you, and Exercise B2 there its last half. When the pushed equation has no solution in the target, it proves that no homomorphism exists (Example (Pairs of Fields with No Homomorphism)). Section 2.5 uses it for the uniqueness half of Theorem 2.5.5, and Exercise R4 of Section 2.6 to find the homomorphisms $\mathbb{Q}(\sqrt{2}) \to \mathbb{R}$.

- **Count copies of 1.** A question about integers acting on a field becomes a question about the elements $n \cdot 1$: by Lemma 2.5.1, $n \cdot a = (n \cdot 1)a$, and $n \mapsto n \cdot 1$ respects sums and products. Then the move of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3, "take the least positive element, then divide by it", turns "$n \cdot 1 = 0$" into "$\operatorname{char} F$ divides n" (Proposition 2.5.2). Section 2.5 names only the second step; the name "count copies of 1" is given here. Since a homomorphism sends $n \cdot 1$ to $n \cdot 1$, it has no choice on the prime subfield (Corollary 2.5.6). In Section 2.6 the same counting kills the middle terms of $(x+y)^p$, and that rigidity turns the Frobenius map of $\mathbb{F}_p$ into Fermat's little theorem.

2.1 The Field Axioms and the First Examples

Number Systems: From $\mathbb{N}$ *to* $\mathbb{R}$ defined fields (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1) and built $\mathbb{Q}$, $\mathbb{R}$ and, for each prime p, the field $\mathbb{Z}/p\mathbb{Z}$. Chapter 1 added $\mathbb{C}$. This chapter looks at fields as a kind of object in their own right. Its first section restates the definition under the name that the linear-algebra volumes use, collects the rules that hold in every field, solves one and two linear equations in any field, and sorts the standard examples from the standard non-examples, naming in each case the clause that fails.

2.1.1 What solving equations needs

Here is a small system of equations, solved the way it is solved at school:

$$\begin{aligned} 2x + 3y &= 7, \\ x - y &= 1. \end{aligned}$$

Subtract twice the second equation from the first: $5y = 5$. Divide by 5: $y = 1$. Then $x = 1 + y = 2$. Check: $2 \cdot 2 + 3 \cdot 1 = 7$ and $2 - 1 = 1$.

List the moves. Equations were combined by sums and differences, one equation was scaled by a number, and one was divided by a number that is **not zero**. Silently, terms were also reordered, regrouped, and brackets were multiplied out. Elimination, the method the linear-algebra volumes run on systems of any size, uses these moves and nothing else.

Now stay inside $\mathbb{Z}$. The equation $2x = 1$ has integer coefficients and no integer solution: $2x$ is even and $1 = 2 \cdot 0 + 1$ is odd, and no integer is both (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a)). The move "divide by 2" leads out of $\mathbb{Z}$. So the dividing line between $\mathbb{Z}$ and $\mathbb{Q}$ is division, and division by every non-zero element is what the definition must ask for.

A field is a number system where you can add, subtract, multiply, and divide by anything non-zero, with the usual rules.

2.1.2 The definition

The definition lists the rules once, as clauses that can be checked and cited. The numbering is the one *Number Systems* used for commutative rings, and the one the linear-algebra volumes cite.

Definition 2.1.1. Field

A **field** is a set F together with two functions, **addition** $+\colon F \times F \to F$, $(a, b) \mapsto a + b$, and

multiplication $\cdot\colon F \times F \to F$, $(a, b) \mapsto a \cdot b = ab$, satisfying the following clauses.

(F1) $a + b = b + a$ **for all** $a, b \in F$.
(F2) $(a + b) + c = a + (b + c)$ **for all** $a, b, c \in F$.
(F3) **There is** an element $0 \in F$ such that $a + 0 = a$ **for every** $a \in F$.
(F4) **For every** $a \in F$ there is an element $-a \in F$ such that $a + (-a) = 0$.
(F5) $(ab)c = a(bc)$ **for all** $a, b, c \in F$.
(F6) $ab = ba$ **for all** $a, b \in F$.
(F7) **There is** an element $1 \in F$ with $1 \neq 0$ such that $a \cdot 1 = a$ **for every** $a \in F$.
(F8) **For every non-zero** $a \in F$ there is an element $a^{-1} \in F$ such that $aa^{-1} = 1$.
(F9) $a(b + c) = ab + ac$ **for all** $a, b, c \in F$.

We write $a - b \coloneqq a + (-b)$, and $a/b \coloneqq ab^{-1}$ for $b \neq 0$.

Read the clauses in three groups.

- **(F1)–(F4)** speak only of addition. The order and the grouping of a sum do not matter, 0 changes nothing when added, and each element can be undone by its negative. Subtraction is built from these.
- **(F5)–(F8)** repeat those four statements for multiplication, with one change: an inverse is demanded only of a **non-zero** element. So division is defined only by non-zero elements, and no clause ever calls for division by 0. Clause (F7) also demands that the two neutral elements differ.
- **(F9)**, the distributive law, is the single bridge between the two operations: it alone mentions both, and multiplying out brackets rests on it, with (F6) for a bracket on the left.

Mind the order of the quantifiers in (F3): there is **one** element 0 that works **for every** a. The weaker reading, "each a has its own z with $a + z = a$", would let z change with a, and it is not what (F3) says. In (F4) the order is the other way round, as it has to be: the negative $-a$ depends on a.

Both operations are functions **into** F: a sum or product of two elements of F is again in F. For a candidate field cut out of a larger number system, that closure is where checking starts. We say "F is a field" when the two operations are understood, and write $(F, +, \cdot)$ when they must be named.

Remark (The same definition in *Number Systems*). Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1 calls a set with two operations a **commutative ring** when (F1)–(F7) and (F9) hold, its (F7) asking only for an element 1 with $a \cdot 1 = a$; it calls a commutative ring a **field** when, in addition, $1 \neq 0$ and (F8) hold. Clause by clause, these are the conditions of Definition 2.1.1: the nine clauses are worded alike, and the only difference is where the condition $1 \neq 0$ is filed, inside (F7) here and as a separate clause there. So F is a field in the sense of Definition 2.1.1 **if and only if** it is a field in the sense of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1. Every result that *Number Systems* proves for fields, or for commutative rings, therefore applies to every field of this chapter, and conversely. The separate filing there has a purpose: it lets the one-element set $\{0\}$ count as a commutative ring (the zero ring) while keeping it out of the fields.

Quick check. Is $\mathbb{Q}_{>0}$, the set of positive rationals with the usual $+$ and $\cdot$ of $\mathbb{Q}$, a field?

Solution. No. Addition and multiplication do map $\mathbb{Q}_{>0} \times \mathbb{Q}_{>0}$ into $\mathbb{Q}_{>0}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1, with (P1) of Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.3). But (F3) fails. An element $z \in \mathbb{Q}_{>0}$ with $1 + z = 1$ would satisfy $z = 0 + z = ((-1) + 1) + z = (-1) + (1 + z) = (-1) + 1 = 0$ in the field $\mathbb{Q}$, by (F1), (F3), (F4) and (F2), and $0 \notin \mathbb{Q}_{>0}$. (Once (F3) fails, (F4) cannot even be stated.)

2.1.3 Rules that hold in every field

The definition's notation takes something for granted. The symbols 0, $-a$ and a^{-1} are written as names of single elements, while (F3), (F4), (F7) and (F8) assert only that suitable elements **exist**. Were there two different zeros in some field, the symbols 0, $a - b$ and a/b would be ambiguous. The next theorem removes the worry and collects the rules of school algebra that every field obeys. Most of it was proved in *Number Systems* for every commutative ring; we collect it under one name, citing the proofs there, and add the rules for fractions as part (g).

Theorem 2.1.1. Basic Properties of Fields

Let F be a field and let $a, b, c, d \in F$.

(a) The element 0 in (F3) is unique, and the element 1 in (F7) is unique.

(b) (Cancellation) If $a + b = a + c$, then $b = c$. If $ab = ac$ and $a \neq 0$, then $b = c$.

(c) The negative $-a$ in (F4) is unique, and for $a \neq 0$ the inverse a^{-1} in (F8) is unique.

(d) $0 \cdot a = 0$.

(e) $(-1)a = -a$.

(f) If $ab = 0$, then $a = 0$ or $b = 0$.

(g) If $b \neq 0$ and $d \neq 0$, then $bd \neq 0$, $(bd)^{-1} = b^{-1}d^{-1}$, $(b^{-1})^{-1} = b$, and

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Idea. Work backwards from each goal to the clause that could produce it; each part then takes a few lines. For uniqueness, take two candidates and prove them equal. No clause says anything about $0 \cdot a$, so for (d) we manufacture a place where (F9) can act: $0 = 0 + 0$, distribute, cancel. In (f) the hypothesis $a \neq 0$ has exactly one use, which is to unlock (F8). The fraction rules in (g) come from one move: an element is identified by showing that it satisfies the defining equation of the element we want, and uniqueness finishes.

Proof. By the remark after Definition 2.1.1, F is a commutative ring in the sense of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1, so Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 applies to it.

(a) This is Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a).

(b) Suppose $a + b = a + c$. Put $-a$ in front of each side and regroup with (F2): this gives $((-a) + a) + b = ((-a) + a) + c$. By (F1) and (F4), $(-a) + a = a + (-a) = 0$, so $0 + b = 0 + c$, and by (F1) and (F3) this says $b = c$.

Now suppose $ab = ac$ and $a \neq 0$. By (F8), a^{-1} exists. Using (F7), (F8), (F6) and (F5),

$$\begin{aligned} b = b \cdot 1 = b(aa^{-1}) = (ba)a^{-1} = (ab)a^{-1} \\ = (ac)a^{-1} = (ca)a^{-1} = c(aa^{-1}) = c \cdot 1 = c. \end{aligned}$$

(c) The negative is unique by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a). For $a \neq 0$, clause (F8) says that a is a unit of F in the sense of Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1, and the inverse of a unit is unique (the well-definedness paragraph after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1).

(d) By Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), $a \cdot 0 = 0$, and $0 \cdot a = a \cdot 0$ by (F6).

(e) By Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c) with $a = 1$, $(-1)b = -(1 \cdot b)$ for every $b \in F$; and $1 \cdot b = b \cdot 1 = b$ by (F6) and (F7). Applied to $b = a$, this gives $(-1)a = -a$.

(f) Suppose $ab = 0$. If $a = 0$ there is nothing to prove, so suppose $a \neq 0$. By (F8), a is a unit of F (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1), and a unit is not a zero divisor (the paragraph after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1): from $ab = 0$ it follows that $b = 0$. So $a = 0$ or $b = 0$.

(g) Let $b \neq 0$ and $d \neq 0$. If $bd = 0$, then (f) would give $b = 0$ or $d = 0$; so $bd \neq 0$. By (F8), b and d are units of F. A product of units is a unit, with $(bd)^{-1} = b^{-1}d^{-1}$, and the inverse of a unit is a unit, with $(b^{-1})^{-1} = b$ (the closure paragraph after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1). Here $b^{-1} \neq 0$, since $1 \neq 0$ by (F7) and so 0 is not a unit (the paragraph "Why this definition" after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1); thus $(b^{-1})^{-1}$ is also the inverse that (F8) supplies, by (c).

For the sum, multiply out with (F9) and reorder with (F5) and (F6):

$$\begin{aligned} (ab^{-1} + cd^{-1})(bd) &= a(b^{-1}b)d + c(d^{-1}d)b \\ &= ad + cb = ad + bc, \end{aligned}$$

by (F8) and (F7) and then (F6). Multiplying both ends by $(bd)^{-1}$, and using $(bd)(bd)^{-1} = 1$ with (F5) and (F7) on the left, gives $ab^{-1}+cd^{-1} = (ad+bc)(bd)^{-1}$, which is the first displayed rule. For the product, (F5) and (F6) give $(ab^{-1})(cd^{-1}) = (ac)(b^{-1}d^{-1}) = (ac)(bd)^{-1}$, by the formula for $(bd)^{-1}$ just proved. This proves the theorem.

■

From now on we use $0 + a = a$ and $1 \cdot a = a$ silently; they follow from (F1), (F3), (F6) and (F7). The larger gain is that any school identity whose proof uses only (F1)–(F9) is true in every field: for instance $(a + b)^2 = a^2 + 2ab + b^2$, where $a^2 \coloneqq aa$ and $2 \coloneqq 1 + 1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d)), and $(-a)(-b) = ab$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)). Part (f) is the rule we will lean on most: a product of non-zero elements is non-zero.

Remark. Part (g), with the uniqueness of inverses in (c), is the content of Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1 (a) and (b), which *Number Systems* proved for every field when it studied ordered fields. Part (f) and the inverse identities of (g) come from the paragraphs on units after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1;

the two fraction formulas are proved here rather than cited from Number Systems: From \(\nN\) to \(\nR\), Lemma 4.1.1, so that no theorem of this section rests on that chapter; only the examples $\mathbb{R}$ and $\mathbb{C}$ below lean on it.

Quick check. In a field, does $a^2 = 0$ imply $a = 0$?

Solution. Yes. $a^2 = aa = 0$, so by Theorem 2.1.1 (f) with $b = a$, $a = 0$ or $a = 0$.

Warning. Cancellation needs its hypothesis. "If $ab = ac$, then $b = c$" is **false** without $a \neq 0$: in $\mathbb{Q}$, $0 \cdot 1 = 0 \cdot 2$, yet $1 \neq 2$. Every time a factor is canceled, say why it is not 0.

Part (f) has a consequence that school algebra uses all the time without naming it: an element has at most two square roots, and they are negatives of each other.

Corollary 2.1.2. Equal Squares

Let F be a field and $x, y \in F$. Then $x^2 = y^2$ if and only if $x = y$ or $x = -y$. In particular, $x^2 = 1$ if and only if $x = 1$ or $x = -1$.

Idea. Move everything to one side and factor: $x^2 - y^2 = (x - y)(x + y)$, the school identity, which holds in every field. A product is zero only when a factor is, by part (f), and the two factors give the two cases.

Proof. First, $(x - y)(x + y) = x^2 - y^2$. Indeed, by (F9) and (F6), $(x + (-y))(x + y) = xx + xy + (-y)x + (-y)y$, and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c) turns the last two terms into $-(yx)$ and $-(yy)$. Since $yx = xy$ by (F6), the terms xy and $-(xy)$ add to 0 by (F4), and what is left is $x^2 - y^2$.

($\Rightarrow$) If $x^2 = y^2$, then $x^2 - y^2 = y^2 + (-y^2) = 0$ by (F4), so $(x - y)(x + y) = 0$. By Theorem 2.1.1 (f), $x - y = 0$ or $x + y = 0$. In the first case, adding y to both sides gives $x = y$, by (F2), (F1), (F4) and (F3). In the second, y satisfies the defining equation of $-x$, so $y = -x$ by Theorem 2.1.1 (c), and then $x = -(-x) = -y$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a).

($\Leftarrow$) If $x = y$, there is nothing to prove. If $x = -y$, then $x^2 = (-y)(-y) = yy = y^2$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c).

For the last sentence take $y = 1$, with $1^2 = 1$ by (F7).

■

Remark. The two square roots y and $-y$ can coincide even when $y \neq 0$: in the field with two elements of the next section, $1+1=0$, so $-1=1$. And the corollary needs (f), so it can fail in a commutative ring with zero divisors. In $\mathbb{Z}/8\mathbb{Z}$ we have $[3]^2=[9]=[1]$, yet $[3]\neq[1]$ and $[3]\neq[-1]=[7]$, since 8 divides neither $3-1=2$ nor $3-7=-4$. For $\mathbb{C}$, Chapter 1 proved the same fact directly from real and imaginary parts (Proposition 1.4.1 (b)); the corollary gives it in every field at once.

2.1.4 Solving linear equations in a field

The opening slogan promised that a field is where elimination works. Here is that promise kept for one equation in one unknown and for two equations in two unknowns.

Proposition 2.1.3. Linear Equations in a Field

Let F be a field and let $a, b, c, d, e, f \in F$.

(a) If $a \neq 0$, the equation $ax = b$ has **exactly one** solution $x \in F$, namely $x = a^{-1}b$.

(b) If $ad - bc \neq 0$, the system

$$\begin{aligned} ax + by &= e, \\ cx + dy &= f \end{aligned}$$

has **exactly one** solution $(x, y) \in F \times F$, namely

$$x = \frac{ed - bf}{ad - bc}, \qquad y = \frac{af - ce}{ad - bc}.$$

Idea. Uniqueness and existence are separate jobs. For uniqueness, assume a solution and run the school elimination on it: one combination of the two equations kills y, another kills x, and each leaves an equation of the form (a). For existence, substitute the candidate and multiply out. The quantity $ad - bc$ is exactly the coefficient elimination produces, and the hypothesis lets us divide by it.

Proof.

(a) By (F5), (F8) and (F7), $a(a^{-1}b) = (aa^{-1})b = 1 \cdot b = b$, so $x = a^{-1}b$ is a solution. If $ax = b$ and $ax' = b$, then $ax = ax'$ with $a \neq 0$, so $x = x'$ by cancellation (Theorem 2.1.1 (b)).

(b) Write $D := ad - bc$, so $D \neq 0$.

Uniqueness. Let (x, y) be a solution. Multiply the first equation by d, the second by b, and subtract. Multiplying out with (F9), reordering with (F5) and (F6), and using Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c) for the signs,

$$\begin{aligned} d(ax + by) - b(cx + dy) &= (ad)x + (bd)y - (bc)x - (bd)y \\ &= (ad - bc)x = Dx, \end{aligned}$$

while the right-hand sides give $de - bf = ed - bf$. So $Dx = ed - bf$. In the same way, $a(cx + dy) - c(ax + by) = (ad - bc)y = Dy$ and the right-hand sides give $af - ce$, so

$Dy = af - ce$. By (a), applied twice with the non-zero coefficient D, $x = D^{-1}(ed - bf)$ and $y = D^{-1}(af - ce)$. These are the displayed values, since $D^{-1}u = uD^{-1} = u/D$ by (F6).

Existence. Put $x_0 \coloneqq (ed - bf)D^{-1}$ and $y_0 \coloneqq (af - ce)D^{-1}$. By (F5), (F6) and (F9), multiplying out and reordering with (F5) and (F6), and using Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c) for the signs,

$$\begin{aligned} ax_0 + by_0 &= \big(a(ed - bf) + b(af - ce)\big)D^{-1} \\ &= (ade - abf + abf - bce)D^{-1} \\ &= e(ad - bc)D^{-1} = eDD^{-1} = e, \end{aligned}$$

by (F8) and (F7) at the end. Likewise

$$\begin{aligned} cx_0 + dy_0 &= \big(c(ed - bf) + d(af - ce)\big)D^{-1} \\ &= (cde - bcf + adf - cde)D^{-1} \\ &= f(ad - bc)D^{-1} = f. \end{aligned}$$

So (x_0, y_0) is a solution, and by uniqueness it is the only one.

■

Both hypotheses have a job. Over $\mathbb{Z}$, part (a) fails: $2 \neq 0$, and $2x = 1$ has no integer solution, because the inverse 2^{-1} of (F8) is missing. And if $ad - bc = 0$, part (b) fails in every field: the system $x + y = 1$, $x + y = 0$ has no solution, since it would give $1 = 0$, while $x + y = 0$, $2x + 2y = 0$ has the solutions $(t, -t)$ for every $t \in F$, at least two of them ($t = 0$ and $t = 1$). The linear-algebra volumes treat n equations in n unknowns by the same elimination.

2.1.5 Examples

Three fields are already at hand. Each was proved a field in the sense of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1, and the remark after Definition 2.1.1 translates.

Example. The Fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Explain why $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, with their usual addition and multiplication, are fields.

Solution. For $\mathbb{Q}$, built as classes of pairs of integers, Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3 proves that it is a field in the sense of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1. For $\mathbb{R}$, built as classes of Cauchy sequences of rationals, Number Systems: From \(\nN\) to \(\nR\), Theorem 5.2.3 does the same; there $1 \neq 0$ is part of the field clause. For $\mathbb{C} \coloneqq \mathbb{R} \times \mathbb{R}$, Theorem 1.2.4 proves it, resting on the arithmetic laws Proposition 1.1.2 and the inverse Proposition 1.2.3. In each case the remark after Definition 2.1.1 turns "field in the sense of *Number Systems*" into "field in the sense of Definition 2.1.1", with the same zero, one, negatives and inverses.

These three are infinite: each contains an injective image of the infinite set $\mathbb{N}$ (Sets, Relations, and Cardinality, Example (Hilbert's Hotel)), through Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (a), Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4, Number Systems: From \(\nN\) to \(\nR\), Theorem 5.4.1 (b) and Proposition 1.1.1. A finite

set has only finite subsets (Sets, Relations, and Cardinality, Proposition 3.1.6). The next section produces finite fields, and Section 2.3 produces fields strictly between $\mathbb{Q}$ and $\mathbb{R}$.

Changing an operation on a familiar set can give a new field; deciding means checking every clause.

Example. A New Multiplication on $\mathbb{Q}$

Show that $\mathbb{Q}$, with the usual addition and the new multiplication $a \odot b := -(ab)$, is a field, and find its one.

Solution. Addition is that of $\mathbb{Q}$, so (F1)–(F4) hold with the usual 0 and negatives. The new product is a function $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$. Each identity below is computed in the field $\mathbb{Q}$ (Example (The Fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$)), the signs by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a) and (c). For all $a, b, c \in \mathbb{Q}$:

- (F5): $(a \odot b) \odot c = -((-(ab))c) = abc = -(a(-(bc))) = a \odot (b \odot c)$.
- (F6): $-(ab) = -(ba)$.
- (F9): $a \odot (b + c) = -(ab + ac) = -(ab) + (-(ac)) = a \odot b + a \odot c$, since $-(u + v) = (-1)(u + v) = -u + (-v)$ by Theorem 2.1.1 (e).
- (F7): the one is -1, since $a \odot (-1) = -(a(-1)) = -(-a) = a$, and $-1 \neq 0$ (otherwise $1 = -(-1) = -0 = 0$, where $-0 = 0$ by Theorem 2.1.1 (c), since $0 + 0 = 0$).
- (F8): a non-zero a has the inverse a^{-1}, the usual one, since $a \odot a^{-1} = -(aa^{-1}) = -1$, the one of this field.

The one of a field need not be the number 1.

2.1.6 Non-examples

Each system below falls short of the slogan somewhere. For each, find the precise clause that breaks; a vague "it is not like $\mathbb{Q}$" teaches nothing.

Example. Four Systems That Are Not Fields

For each of the following, with its usual operations, name the clauses of Definition 2.1.1 that fail, with a witness: (i) $\mathbb{N}$; (ii) $\mathbb{Z}$; (iii) the zero ring $\{0\}$, with $0 + 0 := 0$ and $0 \cdot 0 := 0$; (iv) $\mathbb{Z}/6\mathbb{Z}$.

Solution.

(i) *Number Systems* checked the minimal change from $\mathbb{N}$ to $\mathbb{Z}$: $\mathbb{N}$ satisfies (F1)–(F3), (F5)–(F7) and (F9), and (F4) fails at $a = 1$, since $1 + x \neq 0$ for every $x \in \mathbb{N}$ (the non-example after Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1). The condition $1 \neq 0$ holds, since it holds in $\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1), and $\mathbb{N} \subseteq \mathbb{Z}$ with ι injective (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (a)). Clause (F8) fails too, at $a = 2$: a natural number x with $2x = 1$ would be an integer with $2x = 1$ (ι preserves products, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (a)), and there is none (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a)).

(ii) $\mathbb{Z}$ is a commutative ring with $1 \neq 0$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1), so (F1)–(F7) and (F9) hold. Only (F8) fails, at $a = 2$, by the same parity argument.

(iii) Every clause other than (F7) and (F8) is an equation between elements of $\{0\}$, and each such equation reads $0 = 0$; (F8) holds because there is no non-zero element to invert. The only candidate for the element 1 of (F7) is 0, and (F7) demands $1 \neq 0$. So exactly the condition $1 \neq 0$ inside (F7) fails. This is the reason the condition is there: without it, a one-element "field" would make every statement of the form "a field has a non-zero element" false.

(iv) $\mathbb{Z}/6\mathbb{Z}$ is a commutative ring with $[1] \neq [0]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (a), (c)), so (F1)–(F7) and (F9) hold. But $[2][3] = [6] = [0]$ (Number Systems: From \(\nN\) to \(\nR\), Example (Multiplication modulo six and modulo five)), while $[2] \neq [0]$ and $[3] \neq [0]$, since 6 divides neither 2 nor 3. If $[2]$ had an inverse u, then $[3] = (u[2])[3] = u([2][3]) = u[0] = [0]$, by (F7), (F8), (F6), (F5) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), which is false. So (F8) fails at $[2]$. Had $\mathbb{Z}/6\mathbb{Z}$ been a field, Theorem 2.1.1 (f) would have forbidden the product $[2][3] = [0]$ outright.

The first linear-algebra volume meets one more kind of non-example, the square matrices, where (F6) fails: two matrices can give different products in the two orders.

2.1.7 Why these axioms

Drop a clause and something we use breaks.

- **Without (F8)**, elimination halts at the first coefficient that cannot be inverted, as $2x = 1$ over $\mathbb{Z}$ showed.
- **Without (F6)**, numbers would not commute with each other. Linear algebra swaps scalars constantly (in the first linear-algebra volume, when a vector is multiplied by two numbers in turn), so commutativity is kept.
- **Without** $1 \neq 0$, the zero ring of Example (Four Systems That Are Not Fields) (iii) would count as a field.

The word "field" is a historical label; nothing in it is meant literally.

Warning. Order is not part of a field. Clauses (F1)–(F9) say nothing about $<$, so "squares are ≥ 0" has no meaning in a general field, and read in $\mathbb{C}$ it is false, since $i^2 = -1$ (Chapter 1). Likewise "$1 + 1 \neq 0$" is not a clause, and it fails in the field with two elements of the next section. In a general field, never use an inequality.

2.1.8 Exercises

2.1.8.1 A. Check your understanding

Exercise. A1

(a) State the definition of a field.

(b) Which clauses of Definition 2.1.1 does each of $\mathbb{N}$, $\mathbb{Z}$ and the zero ring $\{0\}$ fail?

(c) True or false: in every field, $ab = ac$ implies $b = c$. Justify your answer.

(d) Which parts of Theorem 2.1.1 fail in the commutative ring $\mathbb{Z}/6\mathbb{Z}$? Give a witness for each.

(e) Use Proposition 2.1.3 to solve $3x + 2y = 1$, $x - y = 2$ in $\mathbb{Q}$.

Solution.

(a) A field is a set F with two functions $+, \cdot : F \times F \to F$ satisfying (F1)–(F9) of Definition 2.1.1, where (F7) includes $1 \neq 0$ and (F8) asks for inverses of non-zero elements only.

(b) $\mathbb{N}$: (F4), at $a = 1$, and (F8), at $a = 2$. $\mathbb{Z}$: only (F8), at $a = 2$. $\{0\}$: only the condition $1 \neq 0$ in (F7). (See Example (Four Systems That Are Not Fields).)

(c) False. With $a = 0$, $b = 1$, $c = 2$ in $\mathbb{Q}$: $0 \cdot 1 = 0 = 0 \cdot 2$, but $1 \neq 2$. Cancellation needs $a \neq 0$ (Theorem 2.1.1 (b)).

(d) Multiplicative cancellation in (b) fails: $[2][1] = [2]$ and $[2][4] = [8] = [2]$, but $[1] \neq [4]$, since 6 does not divide $4 - 1 = 3$. Part (f) fails: $[2][3] = [0]$ with $[2], [3] \neq [0]$. The first clause of (g) fails for the same pair: $[2] \neq [0]$, $[3] \neq [0]$, but $[2][3] = [0]$. The uniqueness of inverses in (c) is not violated, but for $[2]$ it says nothing, since $[2]$ has no inverse (Example (Four Systems That Are Not Fields) (iv)). Parts (a), (d) and (e) hold in every commutative ring (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)–(c), with (F6), (F7)), and so does additive cancellation, whose proof in (b) uses only (F1)–(F4).

(e) Here $a = 3$, $b = 2$, $c = 1$, $d = -1$, $e = 1$, $f = 2$, and $ad - bc = -3 - 2 = -5 \neq 0$. So

$$x = \frac{1 \cdot (-1) - 2 \cdot 2}{-5} = \frac{-5}{-5} = 1, \qquad y = \frac{3 \cdot 2 - 1 \cdot 1}{-5} = \frac{5}{-5} = -1.$$

Check: $3 \cdot 1 + 2 \cdot (-1) = 1$ and $1 - (-1) = 2$.

2.1.8.2 B. Practice

Exercise. B1

Let F be a field and $a, b, x \in F$. Prove:

(a) $-(a - b) = b - a$;

(b) if $a \neq 0$, then $-a \neq 0$ and $(-a)^{-1} = -(a^{-1})$;

(c) $x^2 = x$ if and only if $x = 0$ or $x = 1$;

(d) $x^2 + x = 0$ if and only if $x = 0$ or $x = -1$.

Solution.

(a) By (F1) and (F2), $(a - b) + (b - a) = (a + (-a)) + (b + (-b)) = 0 + 0 = 0$, using (F4) and (F3). So $b - a$ satisfies the defining equation of $-(a - b)$, and $-(a - b) = b - a$ by the uniqueness of negatives (Theorem 2.1.1 (c)).

(b) If $-a = 0$, then $a = -(-a) = -0 = 0$, by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a) and $0 + 0 = 0$; so $-a \neq 0$. By Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c) and (F8), $(-a)(-(a^{-1})) = aa^{-1} = 1$. So $-(a^{-1})$

satisfies the defining equation of $(-a)^{-1}$, and the two are equal by Theorem 2.1.1 (c).

(c) By (F7), (F9) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c), $x(x-1) = xx + x(-1) = x^2 - x$. So $x^2 = x$ if and only if $x(x-1) = 0$, adding $-x$ or x to both sides. By Theorem 2.1.1 (f), $x(x-1) = 0$ gives $x = 0$ or $x - 1 = 0$, that is, $x = 1$. Conversely, $0^2 = 0$ by Theorem 2.1.1 (d), and $1^2 = 1$ by (F7).

(d) By (F7) and (F9), $x(x+1) = x^2 + x$. So $x^2 + x = 0$ means $x(x+1) = 0$, which by Theorem 2.1.1 (f) gives $x = 0$ or $x + 1 = 0$, and the latter means $x = -1$ by the uniqueness of negatives (Theorem 2.1.1 (c)). Conversely, $0^2 + 0 = 0$ by Theorem 2.1.1 (d) and (F3), and $(-1)^2 + (-1) = 1 + (-1) = 0$, since $(-1)(-1) = 1 \cdot 1 = 1$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c).

Exercise. B2

Let F be a field and $a, b, c, d \in F$ with $b \neq 0$ and $d \neq 0$. Prove that $a/b = c/d$ if and only if $ad = bc$.

Solution. ($\Rightarrow$) Multiply both sides of $ab^{-1} = cd^{-1}$ by bd. Reordering with (F5) and (F6), and using (F8) and (F7), the left side becomes $a(b^{-1}b)d = ad$ and the right side $c(d^{-1}d)b = cb = bc$. So $ad = bc$.

($\Leftarrow$) By Theorem 2.1.1 (g), $bd \neq 0$ and $(bd)^{-1} = b^{-1}d^{-1}$. Multiply both sides of $ad = bc$ by $b^{-1}d^{-1}$: reordering as before, the left side becomes $ab^{-1}(dd^{-1}) = ab^{-1}$ and the right side $(bb^{-1})cd^{-1} = cd^{-1}$. So $a/b = c/d$.

Exercise. B3: Which Are Fields?

Determine which of the following are fields. Justify your answer.

(a) $\mathbb{Q}$, with the usual addition and the new multiplication $a \odot b := 2ab$.

(b) $\mathbb{Q}$, with the usual addition and the new multiplication $a \odot b := ab + 1$.

(c) The set $\{0, 1\} \subseteq \mathbb{Q}$, with the addition and multiplication of $\mathbb{Q}$.

Solution.

(a) **A field.** Addition is that of $\mathbb{Q}$, so (F1)–(F4) hold with the usual 0 and negatives. The new product is a function $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$. For all $a, b, c \in \mathbb{Q}$: (F5) $(a \odot b) \odot c = 2(2ab)c = 4abc = 2a(2bc) = a \odot (b \odot c)$; (F6) $2ab = 2ba$; (F9) $a \odot (b+c) = 2a(b+c) = 2ab + 2ac = a \odot b + a \odot c$. For (F7) the one is $\frac{1}{2}$: $a \odot \frac{1}{2} = 2a \cdot \frac{1}{2} = a$, and $\frac{1}{2} \neq 0$. For (F8), a non-zero a has the inverse $\frac{1}{4a}$, since $a \odot \frac{1}{4a} = \frac{2a}{4a} = \frac{1}{2}$, the one of this field. Each identity is computed in the field $\mathbb{Q}$ (Example (The Fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$)). The one of a field need not be the number 1; Exercise B3 of Section 2.4 shows that this field is $\mathbb{Q}$ in disguise.

(b) **Not a field:** (F9) fails. For all a, b, c, $a \odot (b + c) = ab + ac + 1$, while $a \odot b + a \odot c = ab + ac + 2$, and $1 \neq 2$. For instance $a = b = c = 0$ gives $1 \neq 2$.

(c) **Not a field:** addition is not a function $\{0, 1\} \times \{0, 1\} \to \{0, 1\}$, since $1 + 1 = 2 \notin \{0, 1\}$. (The next section puts a different addition on a two-element set and obtains a field.)

2.1.8.3 C. Going deeper

Exercise. C1: Exit check: rules from the axioms

Let F be a field and $a, b, x, y \in F$. Prove the following from (F1)–(F9), using of Theorem 2.1.1 only part (c) (uniqueness of negatives and inverses) and part (e) ($(-1)a = -a$), and citing no result of *Number Systems*.

(a) $0 \cdot a = 0$.

(b) If $ab = 0$, then $a = 0$ or $b = 0$.

(c) $x^2 = y^2$ if and only if $x = y$ or $x = -y$.

Solution.

(a) By (F3), $0+0=0$, so by (F9), $a\cdot 0 = a(0+0) = a\cdot 0 + a\cdot 0$. Add $-(a\cdot 0)$, which exists by (F4), to both sides. On the left this gives 0. On the right, by (F2), (F4) and (F3), $(a\cdot 0 + a\cdot 0) + (-(a\cdot 0)) = a\cdot 0 + (a\cdot 0 + (-(a\cdot 0))) = a\cdot 0 + 0 = a\cdot 0$. So $0 = a\cdot 0$, and $0\cdot a = a\cdot 0 = 0$ by (F6).

(b) Suppose $ab = 0$. If $a = 0$, we are done. Otherwise a^{-1} exists by (F8), and by (F7), (F8), (F5) and (F6),

$$b = b\cdot 1 = b(aa^{-1}) = (ba)a^{-1} = (ab)a^{-1} = 0\cdot a^{-1} = 0,$$

the last step by (a).

(c) *Two sign rules.* For $u, v \in F$, part (e), (F5) and (F6) give $(-u)v = ((-1)u)v = (-1)(uv) = -(uv)$. Hence $(-1)(-1) = -(1\cdot(-1)) = -(-1) = 1$, where $1\cdot(-1) = -1$ by (F6), (F7), and $-(-1) = 1$ by part (c), since $(-1)+1 = 0$ by (F1), (F4). So $(-y)(-y) = ((-1)y)((-1)y) = ((-1)(-1))(yy) = yy$, by (F5) and (F6).

The factorization. By (F9), (F6) and the first sign rule,

$$\begin{aligned}(x+(-y))(x+y) &= xx + xy + (-y)x + (-y)y \\ &= xx + xy + (-(xy)) + (-(yy)),\end{aligned}$$

using $yx = xy$ by (F6). By (F2), (F4) and (F3) the middle terms cancel, so $(x-y)(x+y) = x^2 - y^2$.

($\Rightarrow$) If $x^2 = y^2$, then $x^2 - y^2 = 0$ by (F4), so $(x-y)(x+y) = 0$, and (b) gives $x - y = 0$ or $x + y = 0$. From $x - y = 0$, adding y and using (F2), (F1), (F4), (F3) gives $x = y$. From $x + y = 0$, x satisfies the defining equation of $-y$ (with (F1)), so $x = -y$ by part (c).

($\Leftarrow$) If $x = y$ there is nothing to prove; if $x = -y$, then $x^2 = (-y)(-y) = y^2$ by the sign rules.

Marking scheme. (10 points)

- 2: for (a), writes $0 = 0+0$ and multiplies out $a(0+0)$ by (F9).
- 2: cancels $a\cdot 0$ by adding its negative, naming (F2), (F4) and (F3).
- 1: obtains $0\cdot a$ from $a\cdot 0$ by (F6).
- 2: for (b), treats the case $a = 0$ separately and spends $a \neq 0$ on (F8).
- 1: writes the chain $b = b\cdot 1 = \cdots = 0$ with each clause named.
- 1: proves $(x-y)(x+y) = x^2 - y^2$, justifying the cancellation of xy against $-(yx)$, and concludes by (b).

- 1: proves the converse, deriving $(-y)(-y) = yy$ from part (e), (F5) and (F6).

Fatal errors (0 for the step): dividing by a without $a \neq 0$; "$0 \cdot a = 0$ is obvious"; citing (b) of the exercise inside the proof of (a). A proof of (c) that factors as $(x + y)(x - y)$ or that cites (b) as "no zero divisors" earns the same points.

Exercise. C2: Find the error

Here is a claim with a proof.

> **Claim.** In a field F, if $x \in F$ and $x^2 = x$, then $x = 0$ or $x = 1$.
>
> **Proof.** (1) Let $x^2 = x$. (2) Dividing both sides by x gives $x = 1$. (3) So $x = 0$ or $x = 1$.

Is the claim true? Does the proof prove it? If not, name the line that fails, the error, and give a counterexample to the step.

Solution. The **claim is true**: it is Exercise (B1) (c).

The **proof is wrong**, at line (2). Dividing by x means multiplying by x^{-1}, which (F8) supplies only when $x \neq 0$. No line provides $x \neq 0$, so the step cites an unavailable "fact", cancellation of x without $x \neq 0$: entry (N9) of Logic and Proof, Example (What is not allowed). Line (3) is a correct weakening of (2) by $\vee$I; the proof fails only at (2).

A counterexample to the step: $x = 0$ satisfies $x^2 = x$, and "$x = 1$" is false for it, in every field. The step's conclusion fails, although the claim's does not.

A repair: $x^2 = x$ gives $x(x - 1) = 0$, and Theorem 2.1.1 (f) gives $x = 0$ or $x - 1 = 0$, which treats both cases at once.

2.2 Finite Fields from Modular Arithmetic

Every field of Section 2.1 is infinite. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$ has already met finite ones: it proved that the integers modulo a prime p form a field (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2). This section restates that result in the language of Definition 2.1.1, gives these fields a name of their own, $\mathbb{F}_p$, and computes in them: inverses, linear equations, and the elimination method of Section 2.1, now run modulo 5. Finite fields are not a curiosity; coding theory and computer algebra do linear algebra over them every day.

2.2.1 Arithmetic modulo n, recalled

Fix an integer $n \geq 1$. The ring $\mathbb{Z}/n\mathbb{Z}$ of Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2 consists of the classes $[a]$ of integers a under congruence modulo n, and two classes are equal exactly when their representatives differ by a multiple of n:

$$[a] = [b] \iff n \mid a - b.$$

This is the class test of *Number Systems* (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (a), read with Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2). Sums

and products are computed on representatives. The first example collects what is known about this arithmetic, in the language of Definition 2.1.1.

Example. Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$

Let $n \geq 1$, and define $[a] + [b] := [a + b]$ and $[a][b] := [ab]$ for $a, b \in \mathbb{Z}$. Show that these operations are well defined, that they satisfy every clause of Definition 2.1.1 except possibly (F8) and the condition $1 \neq 0$ in (F7), and that $[1] \neq [0]$ holds exactly when $n \geq 2$. Then write out the addition and multiplication tables for $n = 2$.

Solution. All of this was proved in *Number Systems*, and we collect it.

Well-definedness. The formulas use representatives, so the answer must not depend on which representatives are chosen. For the ideal $n\mathbb{Z}$ of $\mathbb{Z}$ this is Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (b), and $\mathbb{Z}/n\mathbb{Z}$ is defined as that quotient (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2).

The clauses. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (a), $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with zero $[0]$ and one $[1]$: clauses (F1)–(F6) and (F9) hold, and so does (F7) without the condition $1 \neq 0$. The negative of $[a]$ is $[-a]$, since $[a] + [-a] = [a + (-a)] = [0]$.

The condition $1 \neq 0$. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (c), $[1] \neq [0]$ if and only if $n \geq 2$. For $n = 1$ every class equals $[0]$, and $\mathbb{Z}/1\mathbb{Z}$ is the zero ring.

Size. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b), each class is $[r]$ for exactly one $r \in \{0, 1, \ldots, n-1\}$, the remainder of any representative on division by n. So $\mathbb{Z}/n\mathbb{Z}$ has exactly n elements.

The tables for $n = 2$. Write 0 and 1 for $[0]$ and $[1]$. Since $1 + 1 = 2$ and $2 - 0 = 2 \cdot 1$, the class test gives $[1] + [1] = [2] = [0]$; the other entries are read off directly:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Here (F8) holds as well: the only non-zero element is 1, and $1 \cdot 1 = 1$. So $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$ is a field. In it $1 + 1 = 0$, and therefore $-1 = 1$.

The tables of $\mathbb{F}_2$ are those of the two-element field of Number Systems: From \(\nN\) to \(\nR\), Example (A field with two elements that cannot be ordered), with 0 and 1 read as classes. The one surprise is $1 + 1 = 0$: it says that 2 is even, and nothing more. It is also the field promised by the warning on order in Section 2.1, where "$1 + 1 \neq 0$" fails.

2.2.2 Which moduli give fields

For $n \geq 2$, whether $\mathbb{Z}/n\mathbb{Z}$ is a field now comes down to one clause, (F8): does every non-zero class have an inverse? An inverse of $[a]$ is a class $[x]$ with $[ax] = [1]$, that is, an integer x with $n \mid ax - 1$, that is, integers x, y with $ax + ny = 1$. Such a combination is what Bézout's theorem produces. The linear-algebra volumes cite it in the following special form.

Lemma 2.2.1. Bézout's Lemma for Integers

Let $a, n \in \mathbb{Z}$ with $n \geq 1$, and suppose that the only positive integer dividing both a and n is 1. Then there are $x, y \in \mathbb{Z}$ with

$$ax + ny = 1.$$

Proof. Since $n \geq 1$, $(a, n) \neq (0, 0)$, so $g \coloneqq \gcd(a, n)$ is a common divisor of a and n with $g \geq 1$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.2.2 and the well-definedness paragraph after it). By hypothesis, $g = 1$. So a and n are coprime, and Number Systems: From \(\nN\) to \(\nR\), Corollary 3.2.2 gives $x, y \in \mathbb{Z}$ with $ax + ny = 1$. ∎

The general statement, for any pair of integers not both zero and with $\gcd(a, n)$ in place of 1, is Number Systems: From \(\nN\) to \(\nR\), Theorem 3.2.1; the Euclidean algorithm computes the x and y. We keep the special case under its own name because the linear-algebra volumes cite it in this form.

Theorem 2.2.2. $\mathbb{Z}/n\mathbb{Z}$ Is a Field Exactly for Prime n

Let $n \geq 2$ be an integer. Then $\mathbb{Z}/n\mathbb{Z}$ is a field (Definition 2.1.1) if and only if n is prime.

Idea. By Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$), only (F8) is in question. If $n = p$ is prime and $[a] \neq [0]$, then $p \nmid a$, so the only positive common divisor of a and p is 1, and Lemma 2.2.1 hands over $ax + py = 1$, that is, $[a][x] = [1]$. If instead $n = rs$ with $1 < r, s < n$, then $[r][s] = [n] = [0]$ with both factors non-zero, which Theorem 2.1.1 (f) forbids in a field. *Number Systems* ran this argument, with Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1 in the role of the lemma.

Proof. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2, $\mathbb{Z}/n\mathbb{Z}$ is a field in the sense of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1 if and only if n is prime. By the remark after Definition 2.1.1, a field in that sense is the same as a field in the sense of Definition 2.1.1. This proves the theorem. ∎

So for each prime p there is a field with exactly p elements, and for each composite $n \geq 4$ the ring $\mathbb{Z}/n\mathbb{Z}$ is not a field. The fields deserve a short name.

2.2.3 The fields with p elements

Definition 2.2.1. The Field $\mathbb{F}_p$

Let p be a prime. The field $\mathbb{F}_p$ is $\mathbb{Z}/p\mathbb{Z}$, with the operations of Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$). It has exactly p elements (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)), which we write $0, 1, \ldots, p-1$, without brackets: the number

$r \in \{0, \dots, p-1\}$ stands for the class $[r]$. For integers a, b, "$a = b$ in $\mathbb{F}_p$" means $[a] = [b]$, that is, $p \mid a - b$.

So $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{11}$, ... are fields, by Theorem 2.2.2, while $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$ are not. To decide that a given p is prime, the remark after Number Systems: From \(\nN\) to \(\nR\), Lemma 3.3.4 says it is enough to check that no $d \geq 2$ with $d \cdot d \leq p$ divides p.

Computing in $\mathbb{F}_p$ is computing with integers and replacing the answer by its remainder on division by p. The words "in $\mathbb{F}_p$" must be said whenever an equation would be false in $\mathbb{Z}$: "$3 \cdot 5 = 1$ in $\mathbb{F}_7$" is true, because $15 - 1 = 2 \cdot 7$; "$3 \cdot 5 = 1$" alone is false. Every result of Section 2.1 now holds in $\mathbb{F}_p$. For instance, by Corollary 2.1.2 the only elements of $\mathbb{F}_p$ whose square is 1 are 1 and $-1 = p - 1$.

Quick check. Find the inverse of 3 in $\mathbb{F}_7$.

Solution. The inverse is the $x \in \{1, \dots, 6\}$ with $7 \mid 3x - 1$. Testing the candidates in turn, the products $3, 6, 9, 12, 15$ leave remainders $3, 6, 2, 5, 1$, and $3 \cdot 5 = 15 = 2 \cdot 7 + 1$. So $3^{-1} = 5$ in $\mathbb{F}_7$, and by Theorem 2.1.1 (c) it is the only inverse.

For small p, trial is fast. For larger p the Euclidean algorithm of *Number Systems* finds the inverse directly: if $ax + py = 1$, then $\gcd(a, p) = 1$ by Number Systems: From \(\nN\) to \(\nR\), Corollary 3.2.2, and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1 gives $[a]^{-1} = [x]$.

Example. Inverses in $\mathbb{F}_7$ and in $\mathbb{F}_{101}$

(i) List the inverses of the non-zero elements of $\mathbb{F}_7$. (ii) Find the inverse of 17 in $\mathbb{F}_{101}$.

Solution.

(i) In $\mathbb{F}_7$:

$$1 \cdot 1 = 1, \quad 2 \cdot 4 = 8 = 1, \quad 3 \cdot 5 = 15 = 1, \quad 6 \cdot 6 = 36 = 1,$$

since $8 - 1 = 7$, $15 - 1 = 2 \cdot 7$ and $36 - 1 = 5 \cdot 7$. So $1^{-1} = 1$, $2^{-1} = 4$, $4^{-1} = 2$, $3^{-1} = 5$, $5^{-1} = 3$, $6^{-1} = 6$, using (F6) for the reversed pairs. Each element of $\mathbb{F}_7^\times := \mathbb{F}_7 \setminus \{0\}$ appears exactly once as an inverse, as it must: the inverse of a^{-1} is a (Theorem 2.1.1 (g)), so two elements with the same inverse are equal. The elements 1 and $6 = -1$ are their own inverses, and by Corollary 2.1.2 no others are.

(ii) First, 101 is prime, by the criterion recalled after Definition 2.2.1: no d with $2 \leq d \leq 10$ divides it (the remainders of 101 on division by $2, 3, \dots, 10$ are $1, 2, 1, 1, 5, 3, 5, 2, 1$), and $11 \cdot 11 = 121 > 101$. Run the Euclidean algorithm on $(101, 17)$:

$$101 = 5 \cdot 17 + 16, \qquad 17 = 1 \cdot 16 + 1.$$

Back-substitute from the last line:

$$1 = 17 - 16 = 17 - (101 - 5 \cdot 17) = 6 \cdot 17 - 101.$$

So $17 \cdot 6 + 101 \cdot (-1) = 1$, hence $\gcd(17, 101) = 1$ (Number Systems: From \(\nN\)

to \(\nR\), Corollary 3.2.2), and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1 gives $17^{-1} = 6$ in $\mathbb{F}_{101}$. Check: $17 \cdot 6 = 102 = 101 + 1$.

Since $\mathbb{F}_p$ is a field, each result of Section 2.1 about equations holds there word for word; what changes is how the numbers are computed. An elimination of the same kind as Section 2.1's opening one, done over $\mathbb{F}_5$, looks like this.

Example. Elimination over $\mathbb{F}_5$

Solve the system $2x + y = 3$, $3x + 2y = 4$ over $\mathbb{F}_5$.

Solution. In $\mathbb{F}_5$ the inverses are $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$ and $4^{-1} = 4$, since $2 \cdot 3 = 6 = 5 + 1$ and $4 \cdot 4 = 16 = 3 \cdot 5 + 1$.

By elimination. Scale the first equation by $2^{-1} = 3$. In $\mathbb{F}_5$, $3 \cdot 2 = 1$, $3 \cdot 1 = 3$ and $3 \cdot 3 = 9 = 4$, so the scaled equation reads $x + 3y = 4$. Taking 3 times it away from the second equation removes x and leaves

$$(2 - 9)y = 4 - 12, \quad \text{that is,} \quad 3y = 2 \ \text{ in } \mathbb{F}_5,$$

since $-7 = -10 + 3$ and $-8 = -10 + 2$. Multiply by $3^{-1} = 2$: $y = 4$. Then $x = 4 - 3y = 4 - 12 = -8 = 2$ in $\mathbb{F}_5$.

By the formula. With $a = 2$, $b = 1$, $c = 3$, $d = 2$, $e = 3$, $f = 4$, the coefficient $ad - bc = 4 - 3 = 1$ is non-zero, so Proposition 2.1.3 (b) applies:

$$x = \frac{3 \cdot 2 - 1 \cdot 4}{1} = 2, \qquad y = \frac{2 \cdot 4 - 3 \cdot 3}{1} = -1 = 4 \ \text{ in } \mathbb{F}_5.$$

The two methods agree. Check: $2 \cdot 2 + 4 = 8 = 3$ and $3 \cdot 2 + 2 \cdot 4 = 14 = 4$ in $\mathbb{F}_5$. By Proposition 2.1.3 (b), $(x, y) = (2, 4)$ is the only solution.

Quick check. Which elements $x \in \mathbb{F}_{11}$ satisfy $x^2 = 1$?

Solution. Exactly 1 and 10. By Corollary 2.1.2, $x^2 = 1$ if and only if $x = 1$ or $x = -1$, and $-1 = 10$ in $\mathbb{F}_{11}$, since $10 - (-1) = 11$. Check: $10^2 = 100 = 9 \cdot 11 + 1$.

Warning. A non-zero class of $\mathbb{Z}/n\mathbb{Z}$ need not have an inverse. In $\mathbb{Z}/6\mathbb{Z}$ the equation $[2]x = [1]$ has **no** solution, since $[2]x$ is always one of $[0]$, $[2]$, $[4]$; and $[2]x = [4]$ has **two** solutions, $x = [2]$ and $x = [5]$ (as $10 - 4 = 6$). So division by $[a]$ modulo n is allowed when n is prime and $[a] \neq [0]$, or more generally when $\gcd(a, n) = 1$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1), and not otherwise.

Remark (No order on $\mathbb{F}_p$). For $n \geq 2$, no relation $<$ makes $\mathbb{Z}/n\mathbb{Z}$ an ordered commutative ring (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (e)). So the inequalities of *Number Systems* have no meaning in $\mathbb{F}_p$, as the warning on order in Section 2.1 said. The representatives $0, 1, \ldots, p-1$ are ordered as integers, but that order is not compatible with the arithmetic: $0 < p-1$ as integers, and adding 1 to both sides would give $1 < 0$, since $(p-1)+1 = 0$ in $\mathbb{F}_p$.

2.2.4 Exercises

2.2.4.1 A. Check your understanding

Exercise. A1

(a) True or false: $\mathbb{Z}/8\mathbb{Z}$ is a field. Justify your answer.

(b) List the inverses of $1, 2, 3, 4$ in $\mathbb{F}_5$.

(c) Compute $4 \cdot 4 + 3$ in $\mathbb{F}_5$.

(d) True or false: $x^2 = x$ for every $x \in \mathbb{F}_2$.

(e) How many elements does $\mathbb{F}_{13}$ have, and is $13 = 0$ in $\mathbb{F}_{13}$?

Solution.

(a) False. $8 = 2 \cdot 4$ is not prime, so Theorem 2.2.2 applies; concretely $[2][4] = [8] = [0]$ with $[2] \neq [0]$ and $[4] \neq [0]$, which Theorem 2.1.1 (f) forbids in a field.

(b) $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$, as in Example (Elimination over $\mathbb{F}_5$).

(c) $4 \cdot 4 + 3 = 19 = 3 \cdot 5 + 4$, so the answer is 4.

(d) True: $0 \cdot 0 = 0$ and $1 \cdot 1 = 1$ in $\mathbb{F}_2$. (This agrees with Exercise (B1) (c): the solutions of $x^2 = x$ in any field are 0 and 1, and $\mathbb{F}_2$ has no other elements.)

(e) 13 is prime (neither 2 nor 3 divides it, and $4 \cdot 4 = 16 > 13$), so $\mathbb{F}_{13}$ is defined and has 13 elements. And $13 = 0$ in $\mathbb{F}_{13}$, since $13 \mid 13 - 0$.

2.2.4.2 B. Practice

Exercise. B1

(a) Solve $3x + 5 = 2$ in $\mathbb{F}_7$.

(b) Solve the system $x + 2y = 3$, $3x + y = 1$ over $\mathbb{F}_7$.

Solution.

(a) Adding -5 to both sides gives $3x = 2 - 5 = -3 = 4$ in $\mathbb{F}_7$. Since $3 \cdot 5 = 15 = 1$ in $\mathbb{F}_7$, $3^{-1} = 5$, and Proposition 2.1.3 (a) gives $x = 5 \cdot 4 = 20 = 6$. Check: $3 \cdot 6 + 5 = 23 = 3 \cdot 7 + 2$.

(b) Here $a = 1$, $b = 2$, $c = 3$, $d = 1$, $e = 3$, $f = 1$, and $ad - bc = 1 - 6 = -5 = 2 \neq 0$ in $\mathbb{F}_7$. Since $2 \cdot 4 = 8 = 1$, $2^{-1} = 4$. By Proposition 2.1.3 (b),

$$x = (3 \cdot 1 - 2 \cdot 1) \cdot 4 = 4, \qquad y = (1 \cdot 1 - 3 \cdot 3) \cdot 4 = -32 = 3,$$

since $-32 = -5 \cdot 7 + 3$. Check: $4 + 2 \cdot 3 = 10 = 3$ and $3 \cdot 4 + 3 = 15 = 1$ in $\mathbb{F}_7$. Hence $(x, y) = (4, 3)$, and it is the only solution.

Exercise. B2: Which Are Fields?

Determine which of $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{F}_5$, $\mathbb{Z}/1\mathbb{Z}$ and $\mathbb{Z}/91\mathbb{Z}$ are fields. Justify your answer.

Solution. $\mathbb{Z}/9\mathbb{Z}$: **not a field**, since $[3][3] = [9] = [0]$ with $[3] \neq [0]$, against Theorem 2.1.1 (f). $\mathbb{F}_5$: **a field**, by Theorem 2.2.2, since 5 is prime. $\mathbb{Z}/1\mathbb{Z}$: **not a field**, since $[1] = [0]$ there (Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$)), against the condition $1 \neq 0$ of (F7). $\mathbb{Z}/91\mathbb{Z}$: **not a field**, since $91 = 7 \cdot 13$ is not prime (Theorem 2.2.2); concretely $[7][13] = [91] = [0]$.

Exercise. B3

Find all solutions of $x^2 = 2$ in $\mathbb{F}_7$, and all solutions of $x^2 = 2$ in $\mathbb{F}_5$.

Solution. In $\mathbb{F}_7$, $3^2 = 9 = 2$. By Corollary 2.1.2, $x^2 = 2 = 3^2$ holds exactly for $x = 3$ and $x = -3 = 4$. Check: $4^2 = 16 = 2 \cdot 7 + 2$.

In $\mathbb{F}_5$ the squares of $0, 1, 2, 3, 4$ are $0, 1, 4, 9 = 4, 16 = 1$. None is 2, so $x^2 = 2$ has no solution in $\mathbb{F}_5$.

2.2.4.3 C. Going deeper

Exercise. C1: A Field with Four Elements

Let F be the set of formal expressions $a + b\alpha$ with $a, b \in \mathbb{F}_2$: four symbols 0, 1, α and $\beta := 1 + \alpha$, where $a + b\alpha = c + d\alpha$ means $a = c$ and $b = d$. Define

$$(a + b\alpha) + (c + d\alpha) := (a + c) + (b + d)\alpha,$$
$$(a + b\alpha)(c + d\alpha) := (ac + bd) + (ad + bc + bd)\alpha,$$

with all arithmetic of coefficients in $\mathbb{F}_2$. (The product is what multiplying out gives if α^2 is replaced by $1 + \alpha$.)

(a) Write out the addition and multiplication tables of F.

(b) Prove that F is a field.

(c) Show that there is no bijection $\varphi\colon F \to \mathbb{Z}/4\mathbb{Z}$ with $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in F$. So this four-element field is not $\mathbb{Z}/4\mathbb{Z}$ in disguise.

Solution (Hint 1). For (c): where must φ send 0?

Solution (Hint 2). For (c): look for a non-zero element of $\mathbb{Z}/4\mathbb{Z}$ whose square is zero, and ask which element of F is sent to it.

Solution.

(a) Using the formulas, with $1+1=0$ in $\mathbb{F}_2$:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

For instance, $\alpha\alpha = (0+1\alpha)(0+1\alpha) = (0+1)+(0+0+1)\alpha = 1+\alpha = \beta$, and $\alpha\beta = (0+1\alpha)(1+1\alpha) = (0+1)+(0+1+1)\alpha = 1$.

(b) Let $x = a+b\alpha$, $y = c+d\alpha$, $z = e+g\alpha$ with $a,b,c,d,e,g \in \mathbb{F}_2$. Since $\mathbb{F}_2$ is a field (Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$)), the coefficients obey every rule of Section 2.1, and in addition $u+u = (1+1)u = 0$ for every $u \in \mathbb{F}_2$.
Addition works on each coefficient separately, so (F1) and (F2) for F are (F1) and (F2) for $\mathbb{F}_2$, applied twice; the element $0 = 0+0\alpha$ satisfies (F3); and $-x = x$ satisfies (F4), since $a+a=0$ and $b+b=0$.
(F6). Exchanging (a,b) with (c,d) leaves the product formula as it was: $ac+bd = ca+db$ and $ad+bc+bd = cb+da+db$, by (F1) and (F6) in $\mathbb{F}_2$.
(F7). With $1 = 1+0\alpha$, $x\cdot 1 = (a\cdot 1+b\cdot 0)+(a\cdot 0+b\cdot 1+b\cdot 0)\alpha = a+b\alpha = x$. And $1 \neq 0$, because the first coefficients 1 and 0 of $\mathbb{F}_2$ differ.
(F9). Since $y+z = (c+e)+(d+g)\alpha$,

$$\begin{aligned} x(y+z) = {} & \big(a(c+e)+b(d+g)\big) \\ & + \big(a(d+g)+b(c+e)+b(d+g)\big)\alpha, \end{aligned}$$

and multiplying out the coefficients regroups this as $\big((ac+bd)+(ae+bg)\big)+\big((ad+bc+bd)+(ag+be+bg)\big)\alpha = xy+xz$.
(F5). Write $xy = h+k\alpha$ with $h = ac+bd$ and $k = ad+bc+bd$. Then $(xy)z = (he+kg)+(hg+ke+kg)\alpha$, and multiplying out,

$$\begin{aligned} he+kg &= ace+adg+bcg+bde+bdg, \\ hg+ke+kg &= acg+ade+adg+bce+bcg+bde, \end{aligned}$$

where the second line uses $bdg+bdg=0$. On the other side, $yz = l+m\alpha$ with $l = ce+dg$ and $m = cg+de+dg$, and $x(yz) = (al+bm)+(am+bl+bm)\alpha$. Multiplying out gives $al+bm = ace+adg+bcg+bde+bdg$ and $am+bl+bm = acg+ade+adg+bce+bcg+bde$, again using $bdg+bdg=0$. The coefficients agree, so $(xy)z = x(yz)$.
(F8). From the table, $1\cdot 1 = 1$ and $\alpha\beta = \beta\alpha = 1$. So every non-zero element has an inverse: $1^{-1}=1$, $\alpha^{-1}=\beta$, $\beta^{-1}=\alpha$.
This proves that F is a field.

(c) Assume, for a contradiction, that φ is such a bijection. To begin, $\varphi(0) = \varphi(0+0) = \varphi(0)+\varphi(0)$ in $\mathbb{Z}/4\mathbb{Z}$. Adding $-\varphi(0)$ to both sides gives $\varphi(0) = [0]$; this is additive cancellation, whose proof (Theorem 2.1.1 (b), first half) uses only (F1)–(F4), which hold in the commutative ring $\mathbb{Z}/4\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\),

Theorem 3.4.3 (a)). Surjectivity provides $x \in F$ with $\varphi(x) = [2]$; this x is not 0, because $\varphi(0) = [0] \neq [2]$. But

$$\varphi(xx) = \varphi(x)\varphi(x) = [2][2] = [4] = [0] = \varphi(0),$$

and injectivity turns this into $xx = 0$. By (b), F is a field, so Theorem 2.1.1 (f) gives $x = 0$, a contradiction. Hence no such φ exists.

Marking scheme. (10 points)

- 2: (a) both tables correct, with at least one product computed from the formula.
- 1: (b) addition clauses (F1)–(F4), coefficientwise, with $-x = x$.
- 1: (b) (F6) and (F7), including $1 \neq 0$.
- 2: (b) (F5) and (F9) by expanding coefficients, with $u + u = 0$ in $\mathbb{F}_2$ used and named.
- 1: (b) (F8) from the table.
- 1: (c) $\varphi(0) = [0]$, with the cancellation justified in $\mathbb{Z}/4\mathbb{Z}$.
- 2: (c) an $x \neq 0$ with $\varphi(x) = [2]$ by surjectivity, then $xx = 0$ by injectivity, contradicting the absence of zero divisors in F. A solution that instead takes x with $\varphi(x) = [1]$ by surjectivity and uses $x + x = 0$ in F (from the addition table) to get $[0] = \varphi(0) = \varphi(x + x) = [1] + [1] = [2]$ earns these 2 points; $\varphi(0) = [0]$ still earns the line above.

Fatal errors (0 for the step): "F is $\mathbb{Z}/4\mathbb{Z}$ because both have four elements"; using in (c) that $\mathbb{Z}/4\mathbb{Z}$ is a field. A solution of (b) that checks (F5) and (F9) by listing all 64 triples from the tables earns the same points.

By Theorem 2.2.2, $\mathbb{Z}/4\mathbb{Z}$ is not a field, so a field with four elements cannot be found among the rings $\mathbb{Z}/n\mathbb{Z}$; part (c) shows that F is not even a disguised copy of $\mathbb{Z}/4\mathbb{Z}$. Chapter 5 builds this field again, from polynomials over $\mathbb{F}_2$, and explains where the rule $\alpha^2 = 1 + \alpha$ comes from.

Exercise. C2: Find the error

Here is a claim with a proof.

> **Claim.** Let p be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is a field.
>
> **Proof.** (1) By Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$), only (F8) needs checking. (2) Let $[a] \neq [0]$; then $a \neq 0$. (3) Put $[a]^{-1} := [1/a]$. (4) Then $[a][1/a] = [a \cdot (1/a)] = [1]$. (5) So every non-zero class has an inverse, and $\mathbb{Z}/p\mathbb{Z}$ is a field.

Is the claim true? Does the proof prove it? If not, name the line that fails, the error, and give a counterexample to the step.

Solution. The **claim is true**: it is Theorem 2.2.2, direction ($\Leftarrow$).

The **proof is wrong**, at line (3), and line (4) inherits the fault. The classes of $\mathbb{Z}/p\mathbb{Z}$ are classes of **integers**, and "$[1/a]$" names a class only when $1/a$ is an integer, that is, when $a = 1$ or $a = -1$. The rule $[x][y] = [xy]$ of Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2 is stated for integers x, y only; line (4) applies it to the non-integer $1/a$, a general "fact" that no result supplies. This is entry (N9) of Logic and Proof, Example (What is not allowed): citing a line that is not available. The proof also never uses that p is prime, a sign that something is wrong: the same lines would "prove" that $\mathbb{Z}/6\mathbb{Z}$ is a field.

A counterexample to the step: $p = 5$, $a = 2$. Then $1/2 \notin \mathbb{Z}$, so $[1/2]$ is not an element of $\mathbb{Z}/5\mathbb{Z}$. (The inverse of $[2]$ exists, but it is $[3]$, which line (3) does not produce.)

A repair: since p is prime and $p \nmid a$, the only positive common divisor of a and p is 1; Lemma 2.2.1 gives $ax + py = 1$, and then $[a][x] = [ax] = [1]$, because $p \mid ax - 1$.

Exercise. C3

Find all solutions of $x^2 + x + 1 = 0$ in $\mathbb{F}_2$, in $\mathbb{F}_3$ and in $\mathbb{F}_7$.

Solution. Each field is finite, so we can test every element; this finds all solutions.

In $\mathbb{F}_2$: the values at $x = 0, 1$ are 1 and $3 = 1$. **No solution.**

In $\mathbb{F}_3$: the values at $x = 0, 1, 2$ are 1, $3 = 0$ and $7 = 1$. The **only solution is** $x = 1$.

In $\mathbb{F}_7$: the values at $x = 0, 1, \ldots, 6$ are the remainders of $1, 3, 7, 13, 21, 31, 43$ on division by 7, namely $1, 3, 0, 6, 0, 3, 1$. The **solutions are** $x = 2$ **and** $x = 4$, since $7 = 1 \cdot 7$ and $21 = 3 \cdot 7$.

The three answers differ in number (none, one, two), although the equation looks the same. Section 2.5 returns to this equation with completing the square, which needs $1 + 1$ to be invertible: it is in $\mathbb{F}_3$ and $\mathbb{F}_7$, and it is not in $\mathbb{F}_2$.

2.3 Subfields

The fields met so far sit inside one another. $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, and each is a field with the sum and product of the next: $\mathbb{Q}$ inside $\mathbb{R}$ through the identification of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 5.4 (Number Systems: From \(\nN\) to \(\nR\), Definition 5.4.1), and $\mathbb{R}$ inside $\mathbb{C}$ through Proposition 1.1.1. Between $\mathbb{Q}$ and $\mathbb{R}$ lies the set $\mathbb{Q}(\sqrt{2})$ of numbers $a + b\sqrt{2}$ with a, b rational. Sums and products of two such numbers are again of that form, but is $1/(1 + 2\sqrt{2})$? This section gives a short test that settles such questions once, and it finds, inside every field, a smallest field.

Throughout, $a - b := a + (-b)$ and $a/b := ab^{-1}$ for $b \neq 0$, as in Definition 2.1.1, and the rules of Theorem 2.1.1 are used freely, each cited by its letter.

2.3.1 Fields inside fields

A subset K of a field L inherits two operations, but only in a weak sense: $a + b$ and ab are defined for $a, b \in K$, as elements of L. For K to be a field with these operations, the sum and the product must land in K, and the elements that the axioms (F3), (F4), (F7) and (F8) ask for must be found in K. The natural guess is that nothing else needs checking.

A subfield is a subset that a field's own arithmetic never leaves.

Definition 2.3.1. Subfield

Let L be a field. A **subfield** of L is a subset $K \subseteq L$ such that

- $0 \in K$ and $1 \in K$;
- K is **closed under sums and products**: $a + b \in K$ and $ab \in K$ **for all** $a, b \in K$;
- K is **closed under negatives**: $-a \in K$ **for every** $a \in K$;
- K is **closed under inverses**: $a^{-1} \in K$ **for every non-zero** $a \in K$.

Here 0, 1, $+$, $\cdot$, $-a$ and a^{-1} are those of L.

In words: the first clause asks for the two special elements of L; the second says that the operations of L do not leave K; the last two say that the negatives and inverses which L provides already lie in K.

Examples.

- L **itself** is a subfield of L. It is the largest one, and the degenerate case: every clause holds because $K = L$.
- $\mathbb{Q}$ **in** $\mathbb{R}$**.** Under the identification of a rational q with $\kappa(q) \in \mathbb{R}$, the embedding κ sends 0, 1, sums, products, negatives and inverses of rationals to the same things in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.4.1 (a), (c)). So all four clauses hold, and $\mathbb{Q}$ is a subfield of $\mathbb{R}$.
- $\mathbb{R}$ **in** $\mathbb{C}$**.** Chapter 1 checked the four clauses for the copy of $\mathbb{R}$ in $\mathbb{C}$. The zero $0 = (0, 0)$ and the one $1 = (1, 0)$ of $\mathbb{C}$ (Proposition 1.1.2 (d)) are the real numbers 0 and 1 under the identification $a = (a, 0)$ that follows Proposition 1.1.1, and Theorem 1.2.4 gives closure under sums, products, negatives and inverses. So $\mathbb{R}$ is a subfield of $\mathbb{C}$, and so is $\mathbb{Q}$, since a subfield of a subfield is a subfield: each clause of the inner one is a statement about the operations of the outer field.

Non-examples.

- $\{0\} \subseteq \mathbb{Q}$ is closed under sums, products, negatives and inverses (the last vacuously), and does not contain 1, since $1 \neq 0$ in a field.
- $\mathbb{N} \subseteq \mathbb{Q}$ contains 0 and 1 and is closed under sums and products, but not under negatives, since $-1 \notin \mathbb{N}$, nor under inverses, since $2^{-1} = 1/2 \notin \mathbb{N}$ (as for $\mathbb{Z}$ below).
- $\mathbb{Z} \subseteq \mathbb{Q}$ satisfies every clause except closure under inverses: $2^{-1} = 1/2 \notin \mathbb{Z}$, since $2x = 1$ has no solution $x \in \mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a)).

These are the non-examples (i)–(iii) of Example (Four Systems That Are Not Fields), now seen from inside $\mathbb{Q}$ (the fourth, $\mathbb{Z}/6\mathbb{Z}$, is not a subset of $\mathbb{Q}$): each fails as a subfield exactly where it failed as a field.

2.3.2 The subfield test

The guess above is right, and it comes with a converse and a shortcut. The converse says that a subset closed under the operations which happens to be a field cannot have its own zero or one: they must be those of L. The shortcut, part (c), reduces the four clauses to three checks.

Proposition 2.3.1. The Subfield Test

Let L be a field and $K \subseteq L$.

(a) If K is a subfield of L, then K, with the restrictions of $+$ and $\cdot$ to $K \times K$, is a field (Definition 2.1.1). Its zero is 0_L, its one is 1_L, and the negative and the inverse of an element of K are those of L.

(b) Conversely, suppose that $a + b \in K$ and $ab \in K$ for all $a, b \in K$, and that K with the

restricted operations is a field. Then K is a subfield of L: its zero 0_K is 0_L, its one 1_K is 1_L, and its negatives and inverses are those of L.

(c) K is a subfield of L **if and only if** $1 \in K$, $a - b \in K$ for all $a, b \in K$, and $ab^{-1} \in K$ for all $a, b \in K$ with $b \neq 0$.

Idea.

(a) The axioms (F1), (F2), (F5), (F6) and (F9) are identities that hold **for all** elements of L, so in particular for all elements of K; nothing about K needs checking. The other axioms ask for elements, 0, $-a$, 1, a^{-1}, and the four clauses of Definition 2.3.1 put them in K. We call this move **test inside the big field**: the identities come free, and only closure and the special elements cost anything.

(b) runs the other way. An equation true in K is an equation in L, where cancellation and the uniqueness of negatives and inverses are available; so 0_K and 1_K are forced to be 0_L and 1_L.

(c) builds 0, $-b$, b^{-1}, $a+b$ and ab out of 1 and the two operations "subtract" and "divide".

Before reading on: in (b), where is it used that L is a field, and not just a commutative ring?

Proof.

(a) Since K is closed under sums and products, $+$ and $\cdot$ restrict to functions $K \times K \to K$. Axioms (F1), (F2), (F5), (F6) and (F9) hold for all elements of L, hence for all elements of K. (F3): $0 \in K$, and $a + 0 = a$ for $a \in K$. (F4): for $a \in K$, $-a \in K$ by closure under negatives, and $a + (-a) = 0$. (F7): $1 \in K$, $a \cdot 1 = a$ for $a \in K$, and $1 \neq 0$ because this holds in L. (F8): for non-zero $a \in K$, $a^{-1} \in K$ by closure under inverses, and $aa^{-1} = 1$. So K is a field, and 0_L, 1_L, $-a$, a^{-1} witness its axioms; by the uniqueness of these elements in the field K (Theorem 2.1.1 (a), (c), applied in K), they are its zero, its one, its negatives and its inverses.

(b) Write 0_K, 1_K for the zero and one of the field K. In K, $0_K + 0_K = 0_K$ by (F3); in L, $0_K + 0_L = 0_K$. So $0_K + 0_K = 0_K + 0_L$ in L, and additive cancellation in L (Theorem 2.1.1 (b)) gives $0_K = 0_L$. Next, $1_K \cdot 1_K = 1_K$ by (F7) in K, and $1_K \cdot 1_L = 1_K$ by (F7) in L. Since $1_K \neq 0_K = 0_L$, multiplicative cancellation in L (Theorem 2.1.1 (b)) gives $1_K = 1_L$. Now let $a \in K$, and let $x \in K$ be its negative in K: $a + x = 0_K = 0_L$, so $x = -a$ by the uniqueness of negatives in L (Theorem 2.1.1 (c)). Likewise, if $a \neq 0_K$, that is $a \neq 0_L$, its inverse $y \in K$ satisfies $ay = 1_K = 1_L$, so $y = a^{-1}$ by the uniqueness of inverses in L. Hence $0_L, 1_L \in K$, K is closed under the negatives and inverses of L, and with the hypothesis on sums and products, K is a subfield.

(c) ($\Rightarrow$) $1 \in K$ by definition. For $a, b \in K$, $-b \in K$, so $a - b = a + (-b) \in K$, by closure under negatives and sums. For $b \neq 0$, $b^{-1} \in K$, so $ab^{-1} \in K$, by closure under inverses and products.

($\Leftarrow$) First, $0 = 1 - 1 \in K$, since $1 + (-1) = 0$ by (F4). For $b \in K$, $-b = 0 + (-b) = 0 - b \in K$, by (F1) and (F3). For non-zero $b \in K$, $b^{-1} = 1 \cdot b^{-1} \in K$, by (F6) and (F7). For $a, b \in K$, $-b \in K$ and $-(-b) = b$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)), so $a + b = a - (-b) \in K$. For the product, let $a, b \in K$. If $b = 0$, then $ab = 0 \in K$ by Theorem 2.1.1 (d) and (F6). If $b \neq 0$, then $b^{-1} \in K$, and $b^{-1} \neq 0$, since $bb^{-1} = 1 \neq 0$ while $b \cdot 0 = 0$; so $a(b^{-1})^{-1} \in K$, and $(b^{-1})^{-1} = b$ (Theorem 2.1.1 (g)) gives $ab \in K$. So K contains 0 and 1 and is closed under sums, products, negatives and inverses: it is a subfield.

■

The answer to the prompt. Part (b) uses that L is a field in the step $1_K \cdot 1_K = 1_K \cdot 1_L \Rightarrow 1_K = 1_L$: canceling the factor 1_K means multiplying by its inverse in L, which exists because $1_K \neq 0$ and (F8) holds in L. The additive step uses only negatives, which every commutative ring has. The warning below shows the multiplicative step failing in a ring.

So to show that a subset is a field, we rarely check nine axioms: we check (c), three closure statements, and (a) does the rest.

Warning. A subset of a ring can be a field with **another** one. In the ring $\mathbb{Z}/6\mathbb{Z}$, the subset $\{[0],[3]\}$ is closed under $+$ and $\cdot$: $[3]+[3]=[6]=[0]$ and $[3][3]=[9]=[3]$. With these operations it is a field with two elements, a copy of $\mathbb{F}_2$, but its one is $[3]$, not $[1]$. Part (b) has no counterpart here: $[3][3]=[3][1]$, and $[3]$ cannot be canceled, since $\mathbb{Z}/6\mathbb{Z}$ is not a field.

Likewise, a field structure with **other operations** does not make a subset a subfield: the set $\{0,1\} \subseteq \mathbb{Q}$ with the tables of $\mathbb{F}_2$ is a field, but it is not a subfield of $\mathbb{Q}$, because the sum of $\mathbb{Q}$ gives $1+1=2 \notin \{0,1\}$.

2.3.3 Square roots of two and of minus one

The question of the opening is now one application of the test. Recall that $\mathbb{R}$ is a complete ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3), so by Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4 there is exactly one $r \in \mathbb{R}$ with $r \geq 0$ and $r^2 = 2$, and $\sqrt{2} \coloneqq r$. The set $\mathbb{Q}(\sqrt{2})$ is that of Number Systems: From \(\nN\) to \(\nR\), Definition 6.4.2.

Example. The Field Generated by the Square Root of Two

Show that $\mathbb{Q}(\sqrt{2}) \coloneqq \{a+b\sqrt{2} : a,b \in \mathbb{Q}\} \subseteq \mathbb{R}$ is a field, namely a subfield of $\mathbb{R}$, and find the inverse of $1+2\sqrt{2}$.

Solution. We check the three conditions of Proposition 2.3.1 (c). All computations are in the field $\mathbb{R}$, with $(\sqrt{2})^2 = 2$, and they expand brackets by (F5), (F6), (F9) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c).

One. $1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Differences. For $a,b,c,d \in \mathbb{Q}$, $(a+b\sqrt{2})-(c+d\sqrt{2}) = (a-c)+(b-d)\sqrt{2}$, and $a-c, b-d \in \mathbb{Q}$.

Products, used below. $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$, again in $\mathbb{Q}(\sqrt{2})$.

Inverses. Let $y = c+d\sqrt{2} \neq 0$, with $c,d \in \mathbb{Q}$. First, the **conjugate** $c-d\sqrt{2}$ is not 0. If $d \neq 0$ and $c-d\sqrt{2}=0$, then $\sqrt{2} = c/d \in \mathbb{Q}$, and $(c/d)^2 = 2$, against Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1. If $d=0$, then $c-d\sqrt{2} = c = y \neq 0$. Now

$$N \coloneqq (c+d\sqrt{2})(c-d\sqrt{2}) = c^2 - 2d^2,$$

a rational number, and $N \neq 0$ by Theorem 2.1.1 (f) in $\mathbb{R}$, both factors being non-zero. Put $y' \coloneqq c/N-(d/N)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Then $yy' = (c+d\sqrt{2})(c-d\sqrt{2})N^{-1} = NN^{-1} = 1$, so $y' = y^{-1}$

by the uniqueness of inverses (Theorem 2.1.1 (c)). Finally, for $x \in \mathbb{Q}(\sqrt{2})$, $xy^{-1} \in \mathbb{Q}(\sqrt{2})$ by the product formula.

By Proposition 2.3.1 (c), $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$, and by (a) it is a field.

The inverse of $1+2\sqrt{2}$. Here $c=1$, $d=2$ and $N=1-8=-7$, so

$$(1+2\sqrt{2})^{-1} = -\frac{1}{7} + \frac{2}{7}\sqrt{2} = \frac{-1+2\sqrt{2}}{7}.$$

Check: $(1+2\sqrt{2})(-1+2\sqrt{2}) = -1+2\sqrt{2}-2\sqrt{2}+8 = 7$.

The move "multiply by the conjugate" is the one that inverted complex numbers in Proposition 1.2.3. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 6.4, proved the same facts about $\mathbb{Q}(\sqrt{2})$ as part of an ordered field (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.4.5), and showed that it does not contain a square root of 3 (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.4.6).

Quick check. Is $\{a+b\sqrt{2} : a,b \in \mathbb{Z}\}$ a subfield of $\mathbb{R}$?

Solution. No. It contains $2 = 2+0\sqrt{2}$, but not $2^{-1} = 1/2$. If $a+b\sqrt{2} = 1/2$ with $a,b \in \mathbb{Z}$ and $b \neq 0$, then $\sqrt{2} = (1/2-a)/b$ would be rational, against Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1; and if $b=0$, then $a = 1/2 \notin \mathbb{Z}$. So it is not closed under inverses. It satisfies the other three clauses, exactly as $\mathbb{Z} \subseteq \mathbb{Q}$ does.

The same test works inside $\mathbb{C}$, where $i^2 = -1$ plays the part of $(\sqrt{2})^2 = 2$, and $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ as above.

Example. Rational and Integer Complex Numbers

Let $\mathbb{Q}(i) \coloneqq \{a+bi : a,b \in \mathbb{Q}\}$ and $\mathbb{Z}[i] \coloneqq \{a+bi : a,b \in \mathbb{Z}\}$, subsets of $\mathbb{C}$.

(i) Show that $\mathbb{Q}(i)$ is a subfield of $\mathbb{C}$.

(ii) Show that $\mathbb{Z}[i]$ contains 0 and 1 and is closed under differences and products, but is not a subfield of $\mathbb{C}$.

(iii) Summarize the subfields of $\mathbb{C}$ met so far.

Solution. Real and imaginary parts are compared as in Definition 1.1.1: $a+bi = c+di$ with $a,b,c,d \in \mathbb{R}$ holds exactly when $a=c$ and $b=d$.

(i) We use Proposition 2.3.1 (c). $1 = 1+0i \in \mathbb{Q}(i)$. Differences: $(a+bi)-(c+di) = (a-c)+(b-d)i$. Products: $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$, from $i^2=-1$. Inverses: let $y = c+di \neq 0$ with $c,d \in \mathbb{Q}$; then $(c,d) \neq (0,0)$. The rational number $M \coloneqq c^2+d^2$ is positive: $\mathbb{Q}$ is an ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1), a non-zero square is positive (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)) and $0^2 = 0\cdot 0 = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)), so every square is non-negative, and a sum

of a positive and a non-negative element is positive (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (b)). So $M \neq 0$. Since $(c+di)(c-di) = c^2+d^2 = M$, the element $y' \coloneqq c/M - (d/M)i \in \mathbb{Q}(i)$ satisfies $yy' = MM^{-1} = 1$, so $y^{-1} = y' \in \mathbb{Q}(i)$ (Theorem 2.1.1 (c)), and then $xy^{-1} \in \mathbb{Q}(i)$ for $x \in \mathbb{Q}(i)$ by the product formula. So $\mathbb{Q}(i)$ is a subfield of $\mathbb{C}$.

(ii) $0 = 0 + 0i$ and $1 = 1 + 0i$ lie in $\mathbb{Z}[i]$, and the difference and product formulas of (i), with integer a, b, c, d, give integer parts. But $2 \in \mathbb{Z}[i]$ has no inverse in $\mathbb{Z}[i]$. Suppose $u = a + bi \in \mathbb{Z}[i]$ had $2u = 1$. Then $u = 2^{-1} = 1/2$ in $\mathbb{C}$, by the uniqueness of inverses (Theorem 2.1.1 (c)) and because the inverse of 2 in $\mathbb{C}$ is the real number $1/2$ (Theorem 1.2.4), so $a + bi = 1/2 + 0i$, and comparing real parts gives $a = 1/2 \notin \mathbb{Z}$. So $\mathbb{Z}[i]$ is not closed under inverses.

(iii) $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{R}$ and $\mathbb{C}$ are subfields of $\mathbb{C}$, and $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$, hence of $\mathbb{C}$:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} \subseteq \mathbb{C}, \qquad \mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{C}.$$

For $\mathbb{R}$ in $\mathbb{C}$ there is a second way to see it: by Proposition 1.1.1 the copy $\iota(\mathbb{R})$ of $\mathbb{R}$ in $\mathbb{C}$ is closed under $+$ and $\cdot$, since $\iota(a) + \iota(c) = \iota(a+c)$ and $\iota(a)\iota(c) = \iota(ac)$. It is a field with these operations. Every element of $\iota(\mathbb{R})$ is $\iota(a)$ for some $a \in \mathbb{R}$, so each identity among the axioms carries over from $\mathbb{R}$ through these two equations; for instance $\iota(a)(\iota(c) + \iota(e)) = \iota(a(c+e)) = \iota(ac + ae) = \iota(a)\iota(c) + \iota(a)\iota(e)$. In the same way $\iota(0)$, $\iota(-a)$, $\iota(1)$ and, for $a \neq 0$, $\iota(a^{-1})$ serve as the zero, the negatives, the one and the inverses; and $\iota(1) \neq \iota(0)$, and $\iota(a) \neq \iota(0)$ exactly when $a \neq 0$, because ι is injective. Proposition 2.3.1 (b) then says that it is a subfield, with the zero and one of $\mathbb{C}$.

2.3.4 The smallest subfield

Subfields can be intersected, and that gives, for any set S of elements, a smallest field containing them.

Proposition 2.3.2. Intersections of Subfields

Let L be a field.

(a) If $\mathcal{K}$ is a **non-empty** set of subfields of L, then $\bigcap \mathcal{K}$ is a subfield of L.

(b) For every subset $S \subseteq L$ there is a **smallest** subfield of L containing S: a subfield K_S with $S \subseteq K_S$, contained in every subfield of L that contains S. It is $K_S = \bigcap \mathcal{K}_S$, where $\mathcal{K}_S$ is the set of subfields of L that contain S.

Proof.

(a) The intersection $\bigcap \mathcal{K} = \{x \in L : x \in K \text{ for every } K \in \mathcal{K}\}$ is defined because $\mathcal{K}$ is a non-empty set of subsets of L (Sets, Relations, and Cardinality, Definition 1.2.4). We check Proposition 2.3.1 (c). Every $K \in \mathcal{K}$ contains 1, so $1 \in \bigcap \mathcal{K}$. If $a, b \in \bigcap \mathcal{K}$, then $a, b \in K$ for every $K \in \mathcal{K}$, so $a - b \in K$ for every $K \in \mathcal{K}$, by (c) applied to K; hence $a - b \in \bigcap \mathcal{K}$. In the same way, $ab^{-1} \in \bigcap \mathcal{K}$ when $b \neq 0$.

(b) $\mathcal{K}_S$ is a set, by Separation (Z6) from the power set of L, which exists by (Z5) (Number Systems: From \(\nN\) to \(\nR\), Axiom 1.1.1). It is non-empty, since $L \in \mathcal{K}_S$. By (a), $K_S \coloneqq \bigcap \mathcal{K}_S$ is a subfield of L. Every $K \in \mathcal{K}_S$ contains S, so $S \subseteq K_S$. And if K is a subfield containing S, then $K \in \mathcal{K}_S$, so $K_S \subseteq K$. Two smallest subfields containing

S would each contain the other, so K_S is the only one.

■

The case $S = \emptyset$ asks for no element at all, and gives a subfield contained in every subfield. It has a name.

Definition 2.3.2. Prime Subfield

The **prime subfield** of a field L is the smallest subfield of L, that is, $K_\emptyset$ of Proposition 2.3.2 (b): the intersection of the set of **all** subfields of L.

In words: the prime subfield is what every subfield of L contains. Section 2.5 identifies it in every field, as a copy of $\mathbb{Q}$ or of exactly one $\mathbb{F}_p$. One case can be settled now: the prime subfield of $\mathbb{F}_p$ is $\mathbb{F}_p$ itself, because $\mathbb{F}_p$ has no other subfield. Indeed, let K be a subfield of $\mathbb{F}_p$. It contains 1 and is closed under $+$, so it contains every multiple $k \cdot 1$ with $k \in \mathbb{N}$, the multiples of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 2.3 ("Multiples"): $0 \cdot 1 = 0 \in K$, and if $k \cdot 1 \in K$, then $(k+1) \cdot 1 = k \cdot 1 + 1 \in K$, so induction (Logic and Proof, Axiom 4.2.1) covers every k. In $\mathbb{Z}/p\mathbb{Z}$, $k \cdot [1] = [k]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d)), and every element is $[k]$ for some $k \in \{0, \ldots, p-1\}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)). So $K = \mathbb{F}_p$.

The smallest subfield containing a given element is often easy to name. Exercise B2 shows that $\mathbb{Q}(\sqrt{2})$ is the smallest subfield of $\mathbb{R}$ containing $\sqrt{2}$; the reason to expect it is that a subfield containing $\sqrt{2}$ contains 1, hence every rational, and is closed under the sums and products that build $a + b\sqrt{2}$.

2.3.5 Exercises

2.3.5.1 A. Check your understanding

Exercise. A1

These parts are about Proposition 2.3.1 (b).

(a) Why must the one of a field $K \subseteq L$, closed under the operations of the field L, be 1_L? Name the step of the proof.

(b) Run the proof of (b) on $K = \{[0], [3]\}$ inside the ring $\mathbb{Z}/6\mathbb{Z}$ (the warning). Which steps go through, and which step fails?

(c) In Example (The Field Generated by the Square Root of Two), is the commutativity (F6) of $\mathbb{Q}(\sqrt{2})$ checked, or inherited? From where?

(d) State the idea of the subfield test, parts (a) and (b), in two sentences.

Solution.

(a) In L, $1_K \cdot 1_K = 1_K = 1_K \cdot 1_L$, and $1_K \neq 0_K = 0_L$; multiplicative cancellation in L (Theorem 2.1.1 (b)) removes the factor 1_K and gives $1_K = 1_L$.

(b) The zero step goes through: $[0]$ is the zero of both, and $[0] + [0] = [0] + [0]$ cancels in any commutative ring. The negative step also goes through ($[3] + [3] = [0]$, so $-[3] = [3]$ in both). The one step fails: $[3][3] = [3] = [3][1]$, but $[3]$ has no inverse in

$\mathbb{Z}/6\mathbb{Z}$ ($[3][x] \in \{[0],[3]\}$ for every x), so it cannot be canceled, and indeed $[3] \neq [1]$. The inverse step then has nothing to say.

(c) Inherited. (F6) holds for all elements of $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.2.3), hence for all elements of the subset $\mathbb{Q}(\sqrt{2})$; Proposition 2.3.1 (a) records this. The solution of the example checks only the three conditions of (c).

(d) The identities among the field axioms hold for all elements of the big field, hence for the elements of any subset, so only closure and the special elements $0, 1, -a, a^{-1}$ need checking. Conversely, the zero and one of a field sitting inside L with L's operations are forced, by cancellation in L, to be those of L.

2.3.5.2 B. Practice

Exercise. B1: Putting a proof in order

Here are the lines of the proof of Proposition 2.3.1 (c) ($\Leftarrow$), shuffled, together with two lines that do not belong. Put the correct lines in an admissible order, say which other orders are admissible, and say what is wrong with each of the other two lines.

(i) Assume $1 \in K$, $a - b \in K$ for all $a, b \in K$, and $ab^{-1} \in K$ for all $a, b \in K$ with $b \neq 0$.

(ii) $0 = 1 - 1 \in K$.

(iii) For $b \in K$, $-b = 0 - b \in K$.

(iv) For non-zero $b \in K$, $b^{-1} = 1 \cdot b^{-1} \in K$.

(v) For $a, b \in K$, $a + b = a - (-b) \in K$.

(vi) For $a, b \in K$: if $b \neq 0$, then $b^{-1} \in K$ and $b^{-1} \neq 0$ (as $bb^{-1} = 1 \neq 0 = b \cdot 0$), so $ab = a(b^{-1})^{-1} \in K$; if $b = 0$, $ab = 0 \in K$.

(vii) So K is a subfield of L.

The two extra lines: "(ii′) $0 \in K$, since $0 = bb^{-1}$ for any $b \in K$", and "(vi′) $ab \in K$, because K is closed under multiplication".

Solution. An admissible order is (i), (ii), (iii), (iv), (v), (vi), (vii). The constraints are what each line uses: (i) comes first and (vii) last; (ii) comes before (iii), which uses $0 \in K$, and before (vi), whose case $b = 0$ uses $0 \in K$; (iii) comes before (v), which uses $-b \in K$; (iv) comes before (vi), which uses $b^{-1} \in K$ (line (vi) itself checks $b^{-1} \neq 0$ before applying (i) to it). Any order respecting these is admissible; for instance (i), (ii), (iv), (iii), (vi), (v), (vii).

(ii′) is false: $bb^{-1} = 1$, not 0, and b^{-1} exists only for $b \neq 0$.

(vi′) is circular: closure under products is part of what the proof must establish, so the line cites the goal. This is entry (N9) of Logic and Proof, Example (What is not allowed).

Exercise. B2

Show that $\mathbb{Q}(\sqrt{2})$ is the smallest subfield of $\mathbb{R}$ containing $\sqrt{2}$, in the sense of Proposition 2.3.2 (b).

Solution. Let K be a subfield of $\mathbb{R}$ with $\sqrt{2} \in K$. Since $1 \in K$ and K is closed under $+$, $n \cdot 1 \in K$ for every $n \in \mathbb{N}$, by induction (Logic and Proof, Axiom 4.2.1) as for $\mathbb{F}_p$ above; and in $\mathbb{R}$, $n \cdot 1 = n$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.4.1 (d), under the identification). Then $-n \in K$ by closure under negatives, so every integer lies in K (every integer is n or $-n$ with $n \in \mathbb{N}$, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (c)). For $m \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$, $n \neq 0$, so $m/n = mn^{-1} \in K$ by closure under inverses and products; and every rational is of this form (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4 (b)). So $\mathbb{Q} \subseteq K$, and then $a + b\sqrt{2} \in K$ for all $a, b \in \mathbb{Q}$, by closure under sums and products. Hence $\mathbb{Q}(\sqrt{2}) \subseteq K$.

Conversely, $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$ (Example (The Field Generated by the Square Root of Two)) containing $\sqrt{2} = 0 + 1\sqrt{2}$. So it is the smallest such subfield.

Exercise. B3

Inside $\mathbb{C}$ (with $\mathbb{R} \subseteq \mathbb{C}$), show that $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(i) = \mathbb{Q}$.

Solution. ($\supseteq$) A rational a is $a + 0\sqrt{2}$ and $a + 0i$.

($\subseteq$) Let $x = a + b\sqrt{2} = c + di$ with $a, b, c, d \in \mathbb{Q}$. The number $a + b\sqrt{2}$ is real, so its imaginary part is 0; the imaginary part of $c + di$ is d. Comparing parts (Definition 1.1.1), $d = 0$ and $a + b\sqrt{2} = c$. If $b \neq 0$, then $\sqrt{2} = (c - a)/b \in \mathbb{Q}$, against Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1. So $b = 0$, and $x = a \in \mathbb{Q}$.

By Proposition 2.3.2 (a), this also shows again that $\mathbb{Q}$ is a subfield of $\mathbb{C}$.

Exercise. B4

Let $\sqrt{3}$ be the non-negative real number with square 3 (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), and $\mathbb{Q}(\sqrt{3}) := \{a + b\sqrt{3} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$. Show that $\mathbb{Q}(\sqrt{3})$ is a subfield of $\mathbb{R}$, and that $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3})$. Hence deduce that the union of two subfields need not be a subfield.

Hint: the claim stated with Number Systems: From \(\nN\) to \(\nR\), Proposition 6.4.6 says which integers are not squares of rationals.

Solution. The claim stated with Number Systems: From \(\nN\) to \(\nR\), Proposition 6.4.6 says: if $n, k \in \mathbb{N}$ and $k^2 < n < (k+1)^2$, no rational squares to n. We use it for $(n, k) = (3, 1)$ and $(6, 2)$, since $1 < 3 < 4$ and $4 < 6 < 9$.

$\mathbb{Q}(\sqrt{3})$ is a subfield. Exactly as in Example (The Field Generated by the Square Root of Two), with 3 in place of 2: the product is $(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$; for $y = c + d\sqrt{3} \neq 0$, the conjugate $c - d\sqrt{3}$ is non-zero (if $d \neq 0$, it would make $\sqrt{3} = c/d$ rational, against the claim with $(3, 1)$), $N := c^2 - 3d^2 \neq 0$, and $y^{-1} = c/N - (d/N)\sqrt{3}$.

Not in $\mathbb{Q}(\sqrt{2})$. If $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2})$, then $\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$, a square root of 3 in $\mathbb{Q}(\sqrt{2})$, against Number Systems: From \(\nN\) to \(\nR\), Proposition 6.4.6.

Not in $\mathbb{Q}(\sqrt{3})$. If it were, then $\sqrt{2} = (\sqrt{2}+\sqrt{3}) - \sqrt{3} \in \mathbb{Q}(\sqrt{3})$, say $\sqrt{2} = a + b\sqrt{3}$ with $a, b \in \mathbb{Q}$. Squaring,

$$2 = (a^2 + 3b^2) + 2ab\sqrt{3}, \quad \text{that is,} \quad (a^2 + 3b^2 - 2) + 2ab\sqrt{3} = 0.$$

If $ab \neq 0$, then $\sqrt{3} = (2 - a^2 - 3b^2)/(2ab) \in \mathbb{Q}$, against the claim with $(3, 1)$. So $ab = 0$, and then $a^2 + 3b^2 = 2$. If $b = 0$, then $a^2 = 2$, against Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1. If $a = 0$, then $3b^2 = 2$, so $(3b)^2 = 6$, against the claim with $(6, 2)$.

The union. $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and $\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, but their sum is in neither. So $\mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3})$ is not closed under sums, and is not a subfield of $\mathbb{R}$, although both pieces are.

2.3.5.3 C. Going deeper

Exercise. C1: A finite subset closed under the operations

Let L be a field and $K \subseteq L$ a **finite** subset with $1 \in K$, closed under $+$ and $\cdot$. Show that $0 \in K$, that K is closed under negatives and under inverses of non-zero elements, and hence that K is a subfield of L. Then show that the hypothesis "finite" cannot be dropped.

Solution (Hint 1). For $b \in K$, which maps $K \to K$ can you build from b and the two operations?

Solution (Hint 2). The maps $x \mapsto x+b$ and $x \mapsto bx$ go from K to K. Why are they injective, and what does finiteness then give?

Solution. A finite set has no injection onto a proper part. Let $f\colon K \to K$ be injective. If f were not surjective, its image $f(K)$ (Sets, Relations, and Cardinality, Definition 1.6.1) would be a proper subset of K, and f, with codomain $f(K)$, would be a bijection $K \to f(K)$, against Sets, Relations, and Cardinality, Theorem 3.1.9. So every injective map $K \to K$ is surjective.

Zero. Let $t\colon K \to K$, $t(x) := x + 1$, a map into K because K is closed under $+$ and $1 \in K$. It is injective: $x + 1 = x' + 1$ gives $1 + x = 1 + x'$ by (F1), so $x = x'$ by additive cancellation in L (Theorem 2.1.1 (b)). So it is surjective, and some $x \in K$ has $x + 1 = 1 = 0 + 1$, so $1 + x = 1 + 0$ by (F1); canceling, $x = 0$. So $0 \in K$.

Negatives. Let $b \in K$. The map $x \mapsto x + b$ is injective in the same way, hence surjective, and $0 \in K$ is a value: $x + b = 0$ for some $x \in K$. By the uniqueness of negatives in L, $x = -b$.

Inverses. Let $b \in K$, $b \neq 0$. The map $x \mapsto bx$ goes from K to K and is injective by multiplicative cancellation in L, which uses $b \neq 0$. So it is surjective, $bx = 1$ for some $x \in K$, and $x = b^{-1}$ by the uniqueness of inverses in L.

So K is a subfield. Note that $K \neq \emptyset$ need not be assumed: $1 \in K$.

Finiteness is needed. $\mathbb{N} \subseteq \mathbb{Q}$ contains 1 and is closed under $+$ and $\cdot$, and $-1 \notin \mathbb{N}$. The argument breaks at "injective, hence surjective": $x \mapsto x + 1$ is injective on $\mathbb{N}$, and 0 is not a value.

Marking scheme. (10 points) - 2: a finiteness argument with its reason: an injective map from a finite set to itself is surjective (Sets, Relations, and Cardinality, Theorem 3.1.9, or a count), or pigeonhole on a sequence in K (Sets, Relations, and Cardinality, Theorem 3.1.2). - 2: $0 \in K$, from a translation map and cancellation, or from a repetition $m \cdot 1 = n \cdot 1$ with $m < n$ and cancellation in L, **before** 0 is used. - 2: negatives, from surjectivity of $x \mapsto x + b$ and uniqueness of negatives in L, or from a repetition $i \cdot b = j \cdot b$ with $i < j$, giving $-b = (j - i - 1) \cdot b$. - 2: inverses, with the cancellation by b justified by $b \neq 0$ (injectivity of $x \mapsto bx$, or $b^i = b^j$ with $i < j$ giving $b^{j-i} = 1$ and $b^{-1} = b^{j-i-1}$). - 2: a witness that finiteness is needed ($\mathbb{N} \subseteq \mathbb{Q}$, or $\mathbb{Z} \subseteq \mathbb{Q}$ for inverses). Fatal errors (0 for the step): using $0 \in K$ or $-b \in K$ to build the translation before proving it; "injective, hence surjective" (or pigeonhole) without finiteness.

Exercise. C2: Find the error

Here is an argument. Is its conclusion true? Does the argument prove it? If not, name the line that fails and why.

"$\mathbb{Q}(\sqrt{2})$ is closed under inverses. (1) Let $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ be non-zero. (2) Then

$$(a + b\sqrt{2})^{-1} = \frac{1}{a} + \frac{1}{b\sqrt{2}} = \frac{1}{a} + \frac{1}{2b}\sqrt{2}.$$

(3) Both coefficients are rational, so the inverse lies in $\mathbb{Q}(\sqrt{2})$."

Solution. The conclusion is **true** (Example (The Field Generated by the Square Root of Two)). The argument does not prove it.

Line (2) fails. Its first equality uses the general "fact" $1/(x+y) = 1/x+1/y$, which is neither proved nor true; so the line cites nothing, entry (N9) of Logic and Proof, Example (What is not allowed). It also divides by a and by b, either of which may be 0 (for $\sqrt{2} = 0 + 1\sqrt{2}$, $a = 0$). The second equality, $1/(b\sqrt{2}) = (1/(2b))\sqrt{2}$, is correct for $b \neq 0$.

Counterexample to the step. $x = y = 1$ in $\mathbb{Q}$: $1/(1+1) = 1/2$, while $1/1 + 1/1 = 2$. In the case at hand, $a = b = 1$: the formula gives $1 + \frac{1}{2}\sqrt{2}$, and $(1 + \sqrt{2})(1 + \frac{1}{2}\sqrt{2}) = 2 + \frac{3}{2}\sqrt{2} \neq 1$; the true inverse is $-1 + \sqrt{2}$.

Repair. Multiply by the conjugate, as in Example (The Field Generated by the Square Root of Two): $(a + b\sqrt{2})^{-1} = (a - b\sqrt{2})/(a^2 - 2b^2)$.

2.4 Field Homomorphisms

Section 2.3 looked at fields inside fields. This section looks at maps between fields. Two such maps have appeared already. Complex conjugation $z \mapsto \overline{z}$ turns sums into sums and products into products (Theorem 1.2.2 (a), (b)), and so does $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ on $\mathbb{Q}(\sqrt{2})$ (Number Systems: From \(\nN\) to \(\nR\), Example (Conjugation in $\mathbb{Q}(\sqrt{2})$)). A map that respects both operations carries every equation that holds in one field to an equation in the other. That single observation decides where such a map can send an element, shows that it never collapses two elements, and rules out most maps between most pairs of fields.

Throughout, F and L are fields, and $n \cdot a$ for $n \in \mathbb{N}$ is the multiple of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 2.3 ("Multiples"): $0 \cdot a := 0$, $(n+1) \cdot a := n \cdot a + a$. Powers in a field are defined by the same recursion with products: $a^0 := 1$ and $a^{n+1} := a^n a$ for $n \in \mathbb{N}$, as Sets, Relations, and Cardinality, Definition 2.3.2 does for real numbers; the power laws $a^{m+n} = a^m a^n$, $(a^m)^n = a^{mn}$ and $(ab)^n = a^n b^n$ of Sets, Relations, and Cardinality, Proposition 2.3.4 have proofs that use only (F1)–(F7), (F9) and induction, and hold in every field with the same proofs.

2.4.1 Maps that respect both operations

A homomorphism is a map that respects addition, multiplication and the number one.

Definition 2.4.1. Field Homomorphism

Let F and L be fields. A **homomorphism** (of fields) $\varphi\colon F \to L$ is a function such that, **for all** $a, b \in F$,

$$\varphi(a+b) = \varphi(a) + \varphi(b), \qquad \varphi(ab) = \varphi(a)\varphi(b), \qquad \varphi(1) = 1.$$

A **bijective** (Sets, Relations, and Cardinality, Definition 1.4.5) homomorphism is an **isomorphism**; F and L are **isomorphic**, written $F \cong L$, if there is an isomorphism $F \to L$. An isomorphism $F \to F$ is an **automorphism** of F.

In words: the first clause says that adding and then mapping gives the same as mapping and then adding; the second says the same for multiplying; the third pins down the image of 1, where 1 on the left is 1_F and on the right 1_L. An isomorphism is a homomorphism that is also a one-to-one correspondence of elements, so F and L are then "the same field with the elements renamed".

Examples.

- The **identity** $\mathrm{id}_F\colon F \to F$ is an automorphism.
- **Conjugation** $z \mapsto \overline{z}$ on $\mathbb{C}$ is a homomorphism by Theorem 1.2.2 (a), (b), since $\overline{1} = 1$; Example (Conjugation and Other Automorphisms) below shows that it is an automorphism.
- **The conjugation of** $\mathbb{Q}(\sqrt{2})$, $\sigma(a + b\sqrt{2}) := a - b\sqrt{2}$, is an automorphism (Number Systems: From \(\nN\) to \(\nR\), Example (Conjugation in $\mathbb{Q}(\sqrt{2})$)).

Why the clause $\varphi(1) = 1$. The **zero map** $a \mapsto 0$ satisfies the first two clauses, since $0 = 0+0$ and $0 = 0 \cdot 0$, and it carries no information about F at all. The third clause excludes it, and the next proposition shows that the third clause is exactly what forces a homomorphism to remember every element.

Remark. The order-preserving field maps of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 6.1 (Number Systems: From \(\nN\) to \(\nR\), Definition 6.1.1), are the homomorphisms between ordered fields that also preserve $<$. From here on, $F \cong L$ means isomorphic as fields, in the sense above; the relation of that chapter, an isomorphism that also preserves the order, is said in words, "isomorphic as ordered fields". The two differ: the conjugation σ of $\mathbb{Q}(\sqrt{2})$ is an automorphism of the field, and it is not order-preserving, since $0 < \sqrt{2}$ while $\sigma(\sqrt{2}) = -\sqrt{2} < 0 = \sigma(0)$.

2.4.2 What a homomorphism must do

To find where a homomorphism sends an element, we take an equation that the element satisfies and apply φ to both sides. The equation in L that comes out often has only one solution.

Proposition 2.4.1. Properties of Field Homomorphisms

Let $\varphi\colon F \to L$ be a homomorphism of fields, and let $a, b \in F$.

(a) $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$ and $\varphi(a-b) = \varphi(a) - \varphi(b)$.

(b) If $a \neq 0$, then $\varphi(a) \neq 0$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(c) φ is **injective**.

(d) The image $\varphi(F)$ is a subfield of L, and φ, with codomain $\varphi(F)$, is an isomorphism $F \to \varphi(F)$.

(e) If $\psi\colon L \to M$ is a homomorphism of fields, then $\psi \circ \varphi\colon F \to M$ is a homomorphism. If φ is an isomorphism, its inverse function $\varphi^{-1}\colon L \to F$ is an isomorphism. The identity id_F is an automorphism.

(f) $\varphi(n \cdot a) = n \cdot \varphi(a)$ and $\varphi(a^n) = \varphi(a)^n$ for every $n \in \mathbb{N}$.

Idea. For (a) and (b) the equations to push through φ are $0+0=0$, $a+(-a)=0$ and $aa^{-1}=1$; in L the results are equations with a unique solution, by cancellation and the uniqueness of negatives and inverses. For (c): a homomorphism cannot send a non-zero element to 0, because a non-zero element has an inverse, and then $\varphi(a)\varphi(a^{-1}) = \varphi(1) = 1 \neq 0$. Injectivity is that fact applied to $a-b$. The rest is bookkeeping with (a)–(c), and induction for (f).

Before reading on: in the proof of (c), where is $\varphi(1)=1$ used, and which map satisfies the other two clauses of Definition 2.4.1 but is not injective?

Proof.

(a) Since $0+0=0$ in F,

$$\varphi(0) + \varphi(0) = \varphi(0+0) = \varphi(0) = \varphi(0) + 0,$$

and additive cancellation in L (Theorem 2.1.1 (b)) gives $\varphi(0) = 0$. Next, $a+(-a)=0$ gives $\varphi(a) + \varphi(-a) = \varphi(a+(-a)) = \varphi(0) = 0$, so $\varphi(-a)$ is a negative of $\varphi(a)$, and $\varphi(-a) = -\varphi(a)$ by the uniqueness of negatives (Theorem 2.1.1 (c)). Finally, $\varphi(a-b) = \varphi(a+(-b)) = \varphi(a) + \varphi(-b) = \varphi(a) - \varphi(b)$.

(b) Let $a \neq 0$. Since $aa^{-1} = 1$,

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1) = 1.$$

If $\varphi(a) = 0$, the left side would be $0 \cdot \varphi(a^{-1}) = 0$ (Theorem 2.1.1 (d)), and the display would read $0 = 1$, against (F7) in L. So $\varphi(a) \neq 0$, and the display says that $\varphi(a^{-1})$ is an inverse of $\varphi(a)$; by the uniqueness of inverses (Theorem 2.1.1 (c)), $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(c) Let $\varphi(a) = \varphi(b)$. By (a), $\varphi(a-b) = \varphi(a) - \varphi(b) = 0$. By (b), read contrapositively, an element whose image is 0 is 0; so $a - b = 0$, and $a = b$ (add b to both sides, with (F2), (F1), (F4) and (F3)). So φ is injective.

(d) We use Proposition 2.3.1 (c) for $\varphi(F) \subseteq L$. First, $1 = \varphi(1) \in \varphi(F)$. Next, two elements of $\varphi(F)$ are $\varphi(a)$, $\varphi(b)$ with $a, b \in F$ (Sets, Relations, and Cardinality, Definition 1.6.1), and $\varphi(a) - \varphi(b) = \varphi(a - b) \in \varphi(F)$ by (a). If moreover $\varphi(b) \neq 0$, then $b \neq 0$, since $\varphi(0) = 0$; so by (b), $\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(F)$. Hence $\varphi(F)$ is a subfield of L, a field with the operations of L (Proposition 2.3.1 (a)). The map $\varphi\colon F \to \varphi(F)$ still satisfies the three clauses, since the operations of $\varphi(F)$ are those of L and its one is 1_L; it is surjective by the definition of the image, and injective by (c). So it is an isomorphism.

(e) For the composite, $(\psi \circ \varphi)(a + b) = \psi(\varphi(a) + \varphi(b)) = \psi(\varphi(a)) + \psi(\varphi(b))$, likewise for products, and $\psi(\varphi(1)) = \psi(1) = 1$ (Sets, Relations, and Cardinality, Definition 1.4.2). Now let φ be an isomorphism, with inverse function $\varphi^{-1}\colon L \to F$ (Sets, Relations, and Cardinality, Definition 1.5.2, which exists by Sets, Relations, and Cardinality, Theorem 1.5.4). For $x, y \in L$,

$$\varphi(\varphi^{-1}(x) + \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) + \varphi(\varphi^{-1}(y)) = x + y = \varphi(\varphi^{-1}(x + y)),$$

so $\varphi^{-1}(x) + \varphi^{-1}(y) = \varphi^{-1}(x + y)$, because φ is injective. The same computation with products gives $\varphi^{-1}(x)\varphi^{-1}(y) = \varphi^{-1}(xy)$. And $\varphi(1) = 1$ gives $\varphi^{-1}(1) = 1$. The function φ^{-1} is bijective, with inverse φ (Sets, Relations, and Cardinality, Theorem 1.5.4); so it is an isomorphism. The identity satisfies the three clauses trivially and is bijective.

(f) By induction on n (Logic and Proof, Axiom 4.2.1, read on $\mathbb{N} = \omega$ through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3). For $n = 0$: $\varphi(0 \cdot a) = \varphi(0) = 0 = 0 \cdot \varphi(a)$ by (a), and $\varphi(a^0) = \varphi(1) = 1 = \varphi(a)^0$. If the two formulas hold for n, then

$$\varphi((n + 1) \cdot a) = \varphi(n \cdot a + a) = n \cdot \varphi(a) + \varphi(a) = (n + 1) \cdot \varphi(a),$$
$$\varphi(a^{n+1}) = \varphi(a^n a) = \varphi(a)^n \varphi(a) = \varphi(a)^{n+1}.$$

This proves the proposition.

■

The answer to the prompt. In (c), $\varphi(1) = 1$ enters through (b): the display $\varphi(a)\varphi(a^{-1}) = 1$ is what makes $\varphi(a) = 0$ impossible. The zero map $F \to L$ satisfies the two other clauses, sends every element to 0, and is not injective. A map that respected sums and products but sent 1 to 0 would be the zero map: $\varphi(a) = \varphi(a \cdot 1) = \varphi(a)\varphi(1) = \varphi(a) \cdot 0 = 0$, by (F7), the product clause, $\varphi(1) = 0$, and Theorem 2.1.1 (d) with (F6) in L.

We call the move of this proof **push the equation through** φ: to learn $\varphi(x)$, apply φ to an equation that x satisfies, and solve the resulting equation in L. By (c) and (d), a homomorphism $F \to L$ is the same thing as a copy of F inside L: $F \cong \varphi(F)$, a subfield of L. By (e) and Sets, Relations, and Cardinality, Theorem 1.4.4 (c), composing isomorphisms gives isomorphisms, so $\cong$ is reflexive, symmetric and transitive on any set of fields.

Warning. A bijection that respects addition alone is not an isomorphism. The map $f\colon \mathbb{Q} \to \mathbb{Q}$, $f(x) := 2x$, is bijective (its inverse is $x \mapsto x/2$) and satisfies $f(a + b) = f(a) + f(b)$, by (F9). But $f(1 \cdot 1) = 2$, while $f(1)f(1) = 4$; and $f(1) = 2 \neq 1$. All three clauses of Definition 2.4.1 must be checked.

Quick check. Is $a \mapsto -a$ a homomorphism $\mathbb{Q} \to \mathbb{Q}$?

Solution. No. It sends 1 to -1, and $-1 \neq 1$ in $\mathbb{Q}$: if $-1 = 1$, then $1 + 1 = 1 + (-1) = 0$, while $1 + 1 = 2 \cdot 1 > 0$ in the ordered field $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h), Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1). (In $\mathbb{F}_2$, where $-1 = 1$, the same map is the identity.) It also fails the product clause: $1 \cdot 1 = 1$ is sent to -1, while the product of the images is $(-1)(-1) = 1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)). It does respect sums, by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c) and (F9): $-(a + b) = (-1)(a + b) = -a + (-b)$.

2.4.3 Examples, and pairs of fields with no map between them

Example. Conjugation and Other Automorphisms

(i) Show that conjugation $z \mapsto \overline{z}$ is an automorphism of $\mathbb{C}$, that it is not the identity, and that $\overline{z} = z$ if and only if $z \in \mathbb{R}$.

(ii) Let K be a subfield of L. Show that the inclusion $K \to L$, $x \mapsto x$, is a homomorphism, and that it is not surjective when $K \neq L$.

(iii) Recall why $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism of $\mathbb{Q}(\sqrt{2})$.

(iv) Which automorphisms does $\mathbb{R}$ have?

Solution.

(i) By Theorem 1.2.2 (a), (b), $\overline{z + w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\,\overline{w}$; and $\overline{1} = \overline{1 + 0i} = 1 - 0i = 1$ (Definition 1.2.1). So conjugation is a homomorphism. By Theorem 1.2.2 (a), $\overline{\overline{z}} = z$, so conjugation is its own inverse, hence bijective (Sets, Relations, and Cardinality, Theorem 1.5.4): an automorphism. It is not the identity: $\overline{i} = -i$, and $-i \neq i$, since $i - (-i) = 2i = (0, 2) \neq (0, 0)$.
For the fixed elements, let $z = a + bi$ with $a, b \in \mathbb{R}$. Then $\overline{z} = a - bi$ (Definition 1.2.1), and comparing parts (Definition 1.1.1), $\overline{z} = z$ if and only if $-b = b$, that is $2b = 0$, that is $b = 0$ (as $2 = 2 \cdot 1 > 0$ in the ordered field $\mathbb{R}$, Number Systems: From \(\nN\) to \(\nR\), Theorem 5.3.3, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h), so $2 \neq 0$, and by Theorem 2.1.1 (f)). And $b = 0$ says $z = a + 0i = a \in \mathbb{R}$ (Proposition 1.1.1). This fact is not among the parts of Theorem 1.2.2; the two lines above prove it.

(ii) The operations of K are those of L, and $1_K = 1_L$ (Proposition 2.3.1 (a)). So $x \mapsto x$ satisfies the three clauses. If $K \neq L$, some element of L is not in K, and it is not a value of the inclusion.

(iii) This is Number Systems: From \(\nN\) to \(\nR\), Example (Conjugation in $\mathbb{Q}(\sqrt{2})$), recalled and not proved again: unique representation makes the formula a function, the product formula of Example (The Field Generated by the Square Root of Two) with $-b$, $-d$ in place of b, d shows that products go to products, and the map is its own inverse.

(iv) Only the identity. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 6, proved that a map $\sigma\colon \mathbb{R} \to \mathbb{R}$ with $\sigma(a + b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$ and $\sigma(1) = 1$, that is, a homomorphism $\mathbb{R} \to \mathbb{R}$, is the identity, with no order condition assumed (Number Systems: From \(\nN\) to \(\nR\), Theorem 6.3.4, with $\mathbb{R}$ complete by Number

Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3). So $\mathbb{C}$ has a symmetry and $\mathbb{R}$ has none. Section 2.5 shows that $\mathbb{Q}$ and every $\mathbb{F}_p$ have no automorphism other than the identity either.

Pushing an equation through φ also proves that no homomorphism exists: an equation that holds in F and has no counterpart in L leaves φ nowhere to go.

Example. Pairs of Fields with No Homomorphism

Show that there is no homomorphism (i) $\mathbb{C} \to \mathbb{R}$; (ii) $\mathbb{F}_2 \to \mathbb{Q}$; (iii) $\mathbb{Q} \to \mathbb{F}_p$, for any prime p. (iv) Which clause of Definition 2.4.1 does the zero map $\mathbb{Q} \to \mathbb{Q}$ fail?

Solution.

(i) Suppose $\varphi\colon \mathbb{C} \to \mathbb{R}$ is a homomorphism. In $\mathbb{C}$, $i^2 = -1$. Pushing this through φ,

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1,$$

by (f) and (a) of Proposition 2.4.1. But $\mathbb{R}$ is an ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.3.3), in which every square is ≥ 0 and $1 > 0$, so $-1 < 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e), (a)). So $\varphi(i)^2 = -1$ is impossible.

(ii) Suppose $\varphi\colon \mathbb{F}_2 \to \mathbb{Q}$ is a homomorphism. In $\mathbb{F}_2$, $1 + 1 = 0$ (Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$)). Pushing it through φ, $1 + 1 = \varphi(1) + \varphi(1) = \varphi(1 + 1) = \varphi(0) = 0$ in $\mathbb{Q}$, by (a). But $1 + 1 = 2 \cdot 1 > 0$ in the ordered field $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h), Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1). So no such φ exists.

(iii) Suppose $\varphi\colon \mathbb{Q} \to \mathbb{F}_p$ is a homomorphism. In $\mathbb{F}_p$, $p \cdot 1 = 0$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d)). By Proposition 2.4.1 (f), $\varphi(p \cdot 1) = p \cdot \varphi(1) = p \cdot 1 = 0 = \varphi(0)$, and φ is injective by (c), so $p \cdot 1 = 0$ in $\mathbb{Q}$. But $p \cdot 1 > 0$ in $\mathbb{Q}$, as in (ii), since $p \geq 1$. So no such φ exists.

(iv) The zero map $a \mapsto 0$ respects sums and products, since $0 + 0 = 0$ and $0 \cdot 0 = 0$, and it sends 1 to $0 \neq 1$. So it fails only $\varphi(1) = 1$, and is not a homomorphism.

Section 2.5 explains (ii) and (iii) at once: both pairs of fields differ in the number of copies of 1 that add up to 0.

2.4.4 Exercises

2.4.4.1 A. Check your understanding

Exercise. A1

These parts are about Proposition 2.4.1, mainly its part (c).

(a) Where in the proof of (c) is the clause $\varphi(1) = 1$ used?

(b) Let $\zeta\colon \mathbb{Q} \to \mathbb{Q}$ be the zero map. Which clause of Definition 2.4.1 fails? Which of the conclusions (a)–(f) fail for ζ?

(c) Run the proof of (c) with conjugation on $\mathbb{C}$ and the elements $a = 1 + i$, $b = 1 - i$: compute $a - b$, its image, and conclude.

(d) State the idea of the proof of (c) in two sentences.

Solution.

(a) In (b), which (c) cites: $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1) = 1$, and $1 \neq 0$, so $\varphi(a) \neq 0$ for $a \neq 0$.

(b) The clause $\zeta(1) = 1$ fails: $\zeta(1) = 0$. Conclusion (a) holds ($\zeta(0) = 0 = -0$). Conclusion (b) fails: $1 \neq 0$ and $\zeta(1) = 0$. Conclusion (c) fails: $\zeta(1) = \zeta(2)$. Conclusion (d) fails: the image $\{0\}$ does not contain 1, so it is not a subfield. Conclusion (f) holds for multiples (both sides are 0) and fails for powers at $n = 0$: $\zeta(a^0) = \zeta(1) = 0$, while $\zeta(a)^0 = 1$. Conclusion (e) fails in its first clause: for a homomorphism $\psi\colon \mathbb{Q} \to M$ (for example $\psi = \mathrm{id}_{\mathbb{Q}}$), $\psi \circ \zeta$ is the zero map, since $\psi(0) = 0$ by (a) for ψ, and the zero map sends 1 to 0, so it is not a homomorphism. The clause about inverses holds vacuously, since ζ is not bijective, and the clause about id_F does not involve ζ.

(c) $a - b = 2i \neq 0$. Its image is $\overline{2i} = -2i \neq 0$, as (b) predicts; so $\overline{a} - \overline{b} = \overline{a - b} \neq 0$, and $\overline{a} \neq \overline{b}$. Indeed $\overline{a} = 1 - i$ and $\overline{b} = 1 + i$.

(d) A non-zero element has an inverse, so its image times another image is $\varphi(1) = 1 \neq 0$; hence a homomorphism sends no non-zero element to 0. Applied to a difference $a - b$, this says that different elements have different images.

2.4.4.2 B. Practice

Exercise. B1: Images of quotients

Let $\varphi\colon F \to L$ be a homomorphism, and let $a, b \in F$ with $b \neq 0$. Prove that $\varphi(a/b) = \varphi(a)/\varphi(b)$. Here is the start of a proof. *Name the move, then complete it.*

"Since $a = (a/b) \cdot b$, applying φ gives $\varphi(a) = \varphi(a/b)\,\varphi(b)$. . . ."

Solution. *The move* is **push the equation through** φ: the equation $a = (a/b)b$, which holds since $(ab^{-1})b = a(b^{-1}b) = a$ by (F5), (F6), (F8) and (F7), is carried to L and solved there.

Completion. Since $b \neq 0$, $\varphi(b) \neq 0$ by Proposition 2.4.1 (b), so $\varphi(b)^{-1}$ exists. Multiplying $\varphi(a) = \varphi(a/b)\varphi(b)$ by $\varphi(b)^{-1}$, with (F5), (F8) and (F7),

$$\varphi(a)\varphi(b)^{-1} = \varphi(a/b)\,\varphi(b)\varphi(b)^{-1} = \varphi(a/b).$$

That is, $\varphi(a/b) = \varphi(a)/\varphi(b)$.

Exercise. B2: The automorphisms of the rational complex numbers

Show that $\mathbb{Q}(i)$ (Example (Rational and Integer Complex Numbers)) has exactly two automorphisms: the identity and conjugation $a + bi \mapsto a - bi$. Here is the first half of a proof. *Name the move, then complete it.*

"Let σ be an automorphism of $\mathbb{Q}(i)$. It fixes every rational: $\sigma(n) = \sigma(n \cdot 1) = n \cdot \sigma(1) = n$ for $n \in \mathbb{N}$ by Proposition 2.4.1 (f), $\sigma(-n) = -\sigma(n) = -n$ by (a), and $\sigma(m/n) = \sigma(m)/\sigma(n) = m/n$ for $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, by Exercise (B1: Images of quotients). Moreover $i^2 = -1$. ..."

Solution. The move is **push the equation through** σ, applied to $i^2 = -1$.

Completion. Every rational is m/n with $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4 (b)), so $\sigma(q) = q$ for every $q \in \mathbb{Q}$. Applying σ to $i^2 = -1$,

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1 = i^2.$$

By Corollary 2.1.2 in the field $\mathbb{Q}(i)$, $\sigma(i) = i$ or $\sigma(i) = -i$. For $a, b \in \mathbb{Q}$, $\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\,\sigma(i)$. So either $\sigma(a + bi) = a + bi$ for all a, b, and σ is the identity, or $\sigma(a + bi) = a - bi$ for all a, b, and σ is conjugation. There are at most these two.

Both occur. The identity is an automorphism (Proposition 2.4.1 (e)). Conjugation sends $a+bi$ to $a+(-b)i \in \mathbb{Q}(i)$, so it maps $\mathbb{Q}(i)$ into itself; it respects sums and products and sends 1 to 1 because conjugation on $\mathbb{C}$ does (Example (Conjugation and Other Automorphisms) (i)) and the operations of $\mathbb{Q}(i)$ are those of $\mathbb{C}$; and it is its own inverse on $\mathbb{Q}(i)$, hence bijective. The two are different maps, since conjugation sends $i \in \mathbb{Q}(i)$ to $-i \neq i$ (Example (Conjugation and Other Automorphisms) (i)). So $\mathbb{Q}(i)$ has exactly two automorphisms.

Exercise. B3

Let F be the field of Exercise (B3: Which Are Fields?) (a): the set $\mathbb{Q}$ with the usual sum and the product $a \odot b := 2ab$. Show that $f\colon F \to \mathbb{Q}$, $f(x) := 2x$, is an isomorphism of fields, so $F \cong \mathbb{Q}$. Compare with the warning of this section.

Solution. The one of F is $1/2$: $a \odot \frac{1}{2} = 2a \cdot \frac{1}{2} = a$. We check the three clauses, with $\mathbb{Q}$'s usual product on the right. Sums: $f(a + b) = 2a + 2b = f(a) + f(b)$, by (F9). Products: $f(a \odot b) = 2(2ab) = (2a)(2b) = f(a)f(b)$, by (F5) and (F6). One: $f(1/2) = 1$. The map is bijective, with inverse $x \mapsto x/2$: $2(x/2) = x$ and $(2x)/2 = x$ (Sets, Relations, and Cardinality, Theorem 1.5.4). So f is an isomorphism.

The warning used the same formula $x \mapsto 2x$ as a map $\mathbb{Q} \to \mathbb{Q}$, with the usual product on **both** sides, and it is not a homomorphism there. Whether a map is a homomorphism depends on the operations of the source as well as on the formula: on F, the product $\odot$ contains the factor 2 that the formula needs.

Exercise. B4: The fixed field

Let σ be an automorphism of a field F. Show that its **fixed set** $\{a \in F : \sigma(a) = a\}$ is a subfield of F. Find the fixed set of conjugation on $\mathbb{C}$ and of conjugation on $\mathbb{Q}(\sqrt{2})$.

Solution. Write K for the fixed set, and use Proposition 2.3.1 (c). $\sigma(1) = 1$, so $1 \in K$. For $a, b \in K$, $\sigma(a - b) = \sigma(a) - \sigma(b) = a - b$ by Proposition 2.4.1 (a), so $a - b \in K$. If moreover $b \neq 0$, then $\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} = ab^{-1}$ by (b), so $ab^{-1} \in K$. Hence K is a subfield. (Only

the homomorphism property was used.)

For conjugation on $\mathbb{C}$, $K = \mathbb{R}$, by Example (Conjugation and Other Automorphisms) (i).

For conjugation on $\mathbb{Q}(\sqrt{2})$, $a - b\sqrt{2} = a + b\sqrt{2}$ holds if and only if $2b\sqrt{2} = 0$, that is, $b = 0$: in the ordered field $\mathbb{R}$, $2 = 2 \cdot 1 > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h), Number Systems: From \(\nN\) to \(\nR\), Theorem 5.3.3), so $2 \neq 0$, and $\sqrt{2} \neq 0$ (since $0^2 = 0 \neq 2$), and a product of non-zero elements is non-zero (Theorem 2.1.1 (f)). So $K = \{a + 0\sqrt{2} : a \in \mathbb{Q}\} = \mathbb{Q}$.

2.4.4.3 C. Going deeper

Exercise. C1: Isomorphic fields have the same square roots of minus one

(a) Let $F \cong L$. Prove that F has an element x with $x^2 = -1$ if and only if L has one.

(b) Deduce that $\mathbb{Q}(i) \ncong \mathbb{Q}(\sqrt{2})$ and that $\mathbb{C} \ncong \mathbb{R}$.

Solution.

(a) Let $\varphi\colon F \to L$ be an isomorphism. If $x \in F$ has $x^2 = -1$, then by Proposition 2.4.1 (f) and (a),

$$\varphi(x)^2 = \varphi(x^2) = \varphi(-1) = -\varphi(1) = -1,$$

so $\varphi(x) \in L$ is such an element. Conversely, $\varphi^{-1}\colon L \to F$ is an isomorphism (Proposition 2.4.1 (e)), and the same computation carries an element $y \in L$ with $y^2 = -1$ to $\varphi^{-1}(y) \in F$ with $\varphi^{-1}(y)^2 = -1$.

(b) In $\mathbb{Q}(i)$, $i^2 = -1$. In $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, every y has $y^2 \geq 0 > -1$, since $\mathbb{R}$ is an ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.3.3, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e), (a)); so $\mathbb{Q}(\sqrt{2})$ has no such element, and by (a), $\mathbb{Q}(i) \ncong \mathbb{Q}(\sqrt{2})$. Likewise $i \in \mathbb{C}$ and no element of $\mathbb{R}$ squares to -1, so $\mathbb{C} \ncong \mathbb{R}$.

The same argument works for any statement written with $+$, $\cdot$, 0, 1 and elements: an isomorphism carries it in both directions. (For $\mathbb{C}$ and $\mathbb{R}$, Example (Pairs of Fields with No Homomorphism) (i) shows more: there is no homomorphism $\mathbb{C} \to \mathbb{R}$ at all.)

Marking scheme. (10 points) - 3: pushes $x^2 = -1$ through φ, with $\varphi(-1) = -1$ justified (by (a) and $\varphi(1) = 1$). - 3: the converse, by either route: through φ^{-1}, with the fact that it is an isomorphism (or a homomorphism) justified (Proposition 2.4.1 (e)); or directly, writing $y = \varphi(x)$ by surjectivity, getting $\varphi(x^2) = \varphi(-1)$, and concluding $x^2 = -1$ by injectivity. - 2: no element of $\mathbb{Q}(\sqrt{2})$ (or of $\mathbb{R}$) squares to -1, from the order of $\mathbb{R}$. - 2: both conclusions of (b) drawn from (a). Fatal errors (0 for the step): treating $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(i)$ as evident because the sets "look different"; using $\varphi(-1) = -1$ without (a).

Exercise. C2: Find the error

Here is an argument. Is its conclusion true? Does the argument prove it? If not, name the line that fails and why.

"Every homomorphism $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ is the identity. (1) By definition, $\varphi(1) = 1$, and φ respects sums. (2) For $x \in \mathbb{Q}$, $\varphi(x) = \varphi(x \cdot 1) = x\,\varphi(1)$. (3) Hence $\varphi(x) = x \cdot 1 = x$."

Solution. The conclusion is **true**: the repair below proves it, and Section 2.5 proves it again by another route. The argument does not prove it.

Line (2) fails, at the second equality. "$\varphi(x \cdot 1) = x\,\varphi(1)$" pulls the factor x out of φ, as if φ were compatible with multiplication by a scalar x; that is not a clause of Definition 2.4.1, and nothing proved so far supplies it. So the line cites a general "fact" that is not available, entry (N9) of Logic and Proof, Example (What is not allowed). The clause that is available, multiplicativity, gives only $\varphi(x \cdot 1) = \varphi(x)\varphi(1) = \varphi(x)$, which proves nothing.

Counterexample to the step (in its general form, "a homomorphism satisfies $\varphi(x \cdot 1) = x\,\varphi(1)$"): conjugation on $\mathbb{C}$ has $\overline{i \cdot 1} = -i$, while $i \cdot \overline{1} = i$.

Repair. For $n \in \mathbb{N}$, $\varphi(n \cdot 1) = n \cdot \varphi(1) = n \cdot 1$ by Proposition 2.4.1 (f), and $n \cdot 1 = n$ in $\mathbb{Q}$; so $\varphi(n) = n$. For $n \in \mathbb{N}$, $\varphi(-n) = -\varphi(n) = -n$ by (a), so $\varphi(m) = m$ for every $m \in \mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (c)). Every rational is m/n with $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4 (b)), and $\varphi(m/n) = \varphi(m)/\varphi(n) = m/n$ by Exercise (B1: Images of quotients). So $\varphi = \mathrm{id}_{\mathbb{Q}}$.

2.5 Integer Multiples, the Characteristic, and the Prime Subfield

Add 1 to itself in $\mathbb{Q}$ and the sums $1, 1+1, 1+1+1, \ldots$ never return to 0. In $\mathbb{F}_2$ two copies of 1 already give 0, and in $\mathbb{F}_p$ it takes p copies. This one number decides whether "$2x = 0$, so $x = 0$" is a valid step, and Section 2.4 showed that homomorphisms respect it: there is none from $\mathbb{F}_2$ to $\mathbb{Q}$ (Example (Pairs of Fields with No Homomorphism) (ii)). This section names the number, the **characteristic**, proves that it is 0 or a prime, and uses it to find the smallest subfield of every field: a copy of $\mathbb{Q}$ or of exactly one $\mathbb{F}_p$.

Throughout, F and L are fields (Definition 2.1.1), 0 and 1 are the zero and one of the field in play, and we write 1_F when two fields are in play at once.

2.5.1 Integer multiples

The question "can $1+1+\cdots+1$ be 0?" is about the elements $n \cdot 1$. For $n \in \mathbb{N}$ these are already defined in every commutative ring. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Section 2.3 ("Multiples") defines, for a commutative ring R and $a \in R$, by recursion on $\mathbb{N} = \omega$,

$$0 \cdot a := 0, \qquad (n+1) \cdot a := n \cdot a + a \quad (n \in \mathbb{N}).$$

So $1 \cdot a = a$, $2 \cdot a = a + a$, and $n \cdot a$ is the sum of n copies of a. We need negative multiples too, because the divisibility arguments below write $n = qc + r$ with q possibly negative.

Negative multiples. Every integer is m or $-m$ for some $m \in \mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (c)). For $n \in \mathbb{Z}$ with $n < 0$ we have $-n > 0$, so $-n \in \mathbb{N}$ by Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.4 (b), and we define

$$n \cdot a := -\big((-n) \cdot a\big).$$

So $(-3) \cdot a = -(a + a + a)$. Extending the convention of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Section 2.3 (there for natural numbers), a dot with an integer on its left always means this multiple, and the product of two ring elements is written by juxtaposition, ab. When $R = \mathbb{Z}$ the two

readings agree: for $n \in \mathbb{N}$ this is the remark after the definition of multiples in that section, and for $n < 0$, $n \cdot a = -((-n)a) = -(-(na)) = na$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c) and (a).

The lemma below collects the rules for multiples. Parts (a)–(c) are the three identities that the linear-algebra volumes cite; part (d) extends everything to integer multiples.

Lemma 2.5.1. Integer Multiples

Let R be a commutative ring, $a, b \in R$, and $m, k \in \mathbb{N}$.

(a) $(m \cdot 1) + (k \cdot 1) = (m + k) \cdot 1$.

(b) $(m \cdot 1)(k \cdot 1) = (mk) \cdot 1$.

(c) $(m \cdot 1)\, a = m \cdot a$.

(d) The identities (a)–(c) hold for **all** $m, k \in \mathbb{Z}$, and so do

$$(m + k) \cdot a = m \cdot a + k \cdot a, \quad (-m) \cdot a = -(m \cdot a),$$
$$m \cdot (a + b) = m \cdot a + m \cdot b, \quad (m \cdot a)\, b = m \cdot (ab),$$
$$(mk) \cdot a = m \cdot (k \cdot a).$$

In words: integer multiples obey the rules one expects of "m copies of a", with signs behaving as in $\mathbb{Z}$. Since every field is a commutative ring (the remark after Definition 2.1.1), the lemma holds in every field.

Idea. For natural numbers everything is one induction each, on the recursion that defines $m \cdot a$: four rules for natural multiples (a sum law, a distributive law, a product law and a composition law) and then (a)–(c) as special cases with $a = 1$. Negative multiples are reduced to natural ones by writing an integer as a difference $m_1 - m_2$ of natural numbers; that bookkeeping is (d), and its proof is in the fold below.

Proof. All inductions are Logic and Proof, Axiom 4.2.1, read on $\mathbb{N} = \omega$ through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b). We first prove four rules for $m, k \in \mathbb{N}$.

(i) $(m+k)\cdot a = m\cdot a + k\cdot a$. Induction on k. For $k = 0$, $(m+0)\cdot a = m\cdot a = m\cdot a + 0 = m\cdot a + 0\cdot a$ by (F3). If it holds for k, then

$$\begin{aligned}(m + (k+1)) \cdot a &= ((m + k) + 1) \cdot a = (m + k) \cdot a + a \\ &= (m \cdot a + k \cdot a) + a = m \cdot a + (k + 1) \cdot a,\end{aligned}$$

by the recursion, the induction hypothesis, (F2) and the recursion again. (This is the sum law of Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h), whose proof uses no order.)

(ii) $m\cdot(a+b) = m\cdot a + m\cdot b$. Induction on m. For $m = 0$ both sides are 0 (with $0+0=0$ by (F3)). If it holds for m, then $(m+1)\cdot(a+b) = (m\cdot a + m\cdot b) + (a+b) = (m\cdot a + a) + (m\cdot b + b)$ by (F1) and (F2), which is $(m+1)\cdot a + (m+1)\cdot b$.

(iii) $(m\cdot a)b = m\cdot(ab)$. Induction on m. For $m = 0$, $(0\cdot a)b = 0b = 0 = 0\cdot(ab)$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) and (F6). If it holds for m, then

$((m+1)\cdot a)b = (m\cdot a + a)b = (m\cdot a)b + ab = m\cdot(ab) + ab = (m+1)\cdot(ab)$, by (F9) with (F6), and the induction hypothesis.

(iv) $(mk)\cdot a = m\cdot(k\cdot a)$. Induction on m. For $m = 0$ both sides are 0. If it holds for m, then, since $(m+1)k = mk + k$ in $\mathbb{N}$,

$$((m+1)k)\cdot a = (mk+k)\cdot a = (mk)\cdot a + k\cdot a = m\cdot(k\cdot a) + k\cdot a = (m+1)\cdot(k\cdot a),$$

by (i), the induction hypothesis and the recursion.

Now (a) is (i) with $a = 1$. For (c), $(m\cdot 1)a = m\cdot(1a) = m\cdot a$ by (iii), then (F6) and (F7). For (b), $(m\cdot 1)(k\cdot 1) = m\cdot(1(k\cdot 1)) = m\cdot(k\cdot 1) = (mk)\cdot 1$ by (iii), (F6) with (F7), and (iv). Part (d) is proved in the fold below. This proves the lemma.

■

↻ **Second reading** · *Proof of (d): from natural to integer multiples*

Idea. Every integer is a difference $m_1 - m_2$ of natural numbers, and a negative multiple is the negative of a natural one. So each identity of (d) splits into identities for natural multiples, which are rules (i)–(iv), combined with the ring rules for negatives. Only the composition law needs the four sign cases separately, and a table keeps them apart.

Proof. Step 1: $(-m)\cdot a = -(m\cdot a)$ *for every* $m \in \mathbb{Z}$. If $m > 0$, then $-m < 0$ and the definition gives $(-m)\cdot a = -((-(-m))\cdot a) = -(m\cdot a)$. If $m = 0$, both sides are 0, since $-0 = 0$ ($0+0=0$ and uniqueness of negatives, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)). If $m < 0$, the definition gives $m\cdot a = -((-m)\cdot a)$, so $-(m\cdot a) = (-m)\cdot a$ because $-(-x) = x$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)).

Step 2: $(m-k)\cdot a = m\cdot a - k\cdot a$ *for* $m, k \in \mathbb{N}$. If $m \geq k$, then $m-k \in \mathbb{N}$ and $(m-k)+k = m$, so $m\cdot a = (m-k)\cdot a + k\cdot a$ by rule (i) of the proof above; adding $-(k\cdot a)$ to both sides gives the claim. If $m < k$, then by Step 1 and the first case

$$(m-k)\cdot a = -\big((k-m)\cdot a\big) = -\big(k\cdot a - m\cdot a\big) = m\cdot a - k\cdot a,$$

the last step because $(k\cdot a - m\cdot a) + (m\cdot a - k\cdot a) = 0$ by (F1)–(F4), and negatives are unique.

Step 3: the sum, distributive and product rules. By Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (c), every integer is a difference $m_1 - m_2$ of natural numbers ($m = m-0$, $-m = 0-m$). Let $x = m_1 - m_2$ and $y = k_1 - k_2$ with $m_1, m_2, k_1, k_2 \in \mathbb{N}$. Then $x + y = (m_1 + k_1) - (m_2 + k_2)$, and by Step 2 and rule (i),

$$\begin{aligned}(x+y)\cdot a &= (m_1\cdot a + k_1\cdot a) - (m_2\cdot a + k_2\cdot a)\\ &= (m_1\cdot a - m_2\cdot a) + (k_1\cdot a - k_2\cdot a) = x\cdot a + y\cdot a,\end{aligned}$$

using $-(u+v) = (-u)+(-v)$ (both are negatives of $u+v$) and (F1), (F2). In the same way, Step 2 with rules (ii) and (iii) gives $x\cdot(a+b) = x\cdot a + x\cdot b$ and $(x\cdot a)b = (m_1\cdot a)b - (m_2\cdot a)b = x\cdot(ab)$, the middle step by (F9) and $(-u)b = -(ub)$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)). From the distributive rule, $x\cdot c + x\cdot(-c) = x\cdot 0$, and

$x \cdot 0 = (x \cdot 1)0 = 0$ by the product rule just proved (with $a = 1$, $b = 0$) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b); so $x \cdot (-c) = -(x \cdot c)$.

Step 4: $(xy) \cdot a = x \cdot (y \cdot a)$. Write $x = \pm m'$ and $y = \pm k'$ with $m', k' \in \mathbb{N}$. In $\mathbb{Z}$, $(-m')k' = m'(-k') = -(m'k')$ and $(-m')(-k') = m'k'$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)). Each row of the table reduces both sides to rule (iv), using Step 1 and the last line of Step 3.

x, y	$(xy) \cdot a$	$x \cdot (y \cdot a)$
m', k'	$(m'k') \cdot a$	$m' \cdot (k' \cdot a)$
$-m'$, k'	$-((m'k') \cdot a)$	$-(m' \cdot (k' \cdot a))$
m', $-k'$	$-((m'k') \cdot a)$	$m' \cdot (-(k' \cdot a)) = -(m' \cdot (k' \cdot a))$
$-m'$, $-k'$	$(m'k') \cdot a$	$-(m' \cdot (-(k' \cdot a))) = m' \cdot (k' \cdot a)$

Step 5: (a)–(c) for integers. (a) is the sum rule with $a = 1$. (c): $(x \cdot 1)a = x \cdot (1a) = x \cdot a$. (b): $(x \cdot 1)(y \cdot 1) = x \cdot (1(y \cdot 1)) = x \cdot (y \cdot 1) = (xy) \cdot 1$, by the product rule and Step 4. This proves (d).

■

Two readings of the lemma are used constantly. First, by (a) and (b) with (d), the map $\mathbb{Z} \to R$, $n \mapsto n \cdot 1$, turns sums of integers into sums in R and products into products, and sends 1 to $1 \cdot 1 = 1$. Second, by (c) with (d), every multiple $n \cdot a$ is a product in R, namely $(n \cdot 1)a$: to know how multiples behave, it is enough to know the elements $n \cdot 1$.

In $\mathbb{Z}/n\mathbb{Z}$ these elements are the classes themselves: $k \cdot [1] = [k]$ for $k \in \mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d)), and for $k < 0$, $k \cdot [1] = -((-k) \cdot [1]) = -[-k] = [k]$, since $-[u] = [-u]$ in a quotient ring (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (b)).

Quick check. In $\mathbb{Z}/5\mathbb{Z}$, compute $(-3) \cdot [2]$ in two ways: by the definition of a negative multiple, and by (c) of Lemma 2.5.1, extended to integers by (d).

Solution. By the definition, $(-3) \cdot [2] = -(3 \cdot [2]) = -([2]+[2]+[2]) = -[6] = [-6] = [4]$, since $-6-4 = -10$ is divisible by 5. By (c) and (d), $(-3) \cdot [2] = ((-3) \cdot [1])[2] = [-3][2] = [-6] = [4]$, using $k \cdot [1] = [k]$ for $k = -3$.

2.5.2 The characteristic

The elements $1, 2 \cdot 1, 3 \cdot 1, \ldots$ of a field either never reach 0, or reach it for some positive n. In the second case the first time they reach it is the number that matters.

The characteristic counts how many copies of 1 *add up to* 0*, and is* 0 *if no number of copies does.*

Definition 2.5.1. Characteristic

Let F be a field. If **there exists** a positive integer n with $n \cdot 1 = 0$, the **characteristic** of F, written $\operatorname{char} F$, is the **least** such n. If there is none, $\operatorname{char} F := 0$.

In words: test $n = 1, 2, 3, \ldots$ in turn; $\operatorname{char} F$ is the first n with $n \cdot 1 = 0$, and 0 if the test never stops. The same words define the characteristic of a commutative ring.

Well-definedness. If the set $S := \{n \in \mathbb{Z}_{>0} : n \cdot 1 = 0\}$ is non-empty, it is a non-empty set of integers bounded below by 1, so it has a least element by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6. So "the least such n" names exactly one integer.

First examples.

- $\mathbb{F}_2$: $1 \cdot 1 = 1 \neq 0$ and $2 \cdot 1 = 1 + 1 = 0$ by the table of Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$), so $\operatorname{char} \mathbb{F}_2 = 2$.
- $\mathbb{F}_3$: $1 \cdot 1 = 1$, $2 \cdot 1 = 2$, $3 \cdot 1 = 3 = 0$, and $1, 2 \neq 0$ in $\mathbb{F}_3$, so $\operatorname{char} \mathbb{F}_3 = 3$.
- $\mathbb{Q}$: $n \cdot 1 = n \neq 0$ for every $n \geq 1$, so $\operatorname{char} \mathbb{Q} = 0$. The reason is the order of $\mathbb{Q}$; the example at the end of the next subsection gives it.
- The ring $\mathbb{Z}/6\mathbb{Z}$, which is not a field: $k \cdot [1] = [k] \neq [0]$ for $k = 1, \ldots, 5$ and $6 \cdot [1] = [0]$, so it has characteristic 6.

The degenerate case. In the zero ring $\{0\}$ of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 2.3, $1 = 0$, so $1 \cdot 1 = 1 = 0$ and the characteristic is 1. It is the only ring of characteristic 1: characteristic 1 means $1 = 1 \cdot 1 = 0$, and then every $a = a \cdot 1 = a \cdot 0 = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)). It is not a field. For fields, the clause $1 \neq 0$ of (F7) rules out characteristic 1, and that is the first step of the theorem below on which characteristics occur.

Why 0 and not "infinity". The convention $\operatorname{char} F = 0$ makes the next proposition read the same in every case: $n \cdot 1 = 0$ exactly when $\operatorname{char} F$ divides n. For $\operatorname{char} F = 0$ this says $n \cdot 1 = 0$ only for $n = 0$, because $0 \mid n$ only for $n = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (a)).

The proposition is the form in which the characteristic is used. Its proof is the move of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3: take the least positive element, then divide by it.

Proposition 2.5.2. The Characteristic Divides Every Vanishing Multiple

Let F be a field, $c := \operatorname{char} F$, and $n \in \mathbb{Z}$.

(a) $n \cdot 1 = 0$ **if and only if** $c \mid n$.

(b) $n \cdot 1$ is invertible in F if and only if $c \nmid n$. In particular $2 := 1 + 1$ is invertible in F if and only if $\operatorname{char} F \neq 2$.

Idea. For $c > 0$, divide n by c with remainder, $n = qc + r$. The multiple $c \cdot 1$ is 0, so the rules of Lemma 2.5.1 kill the part qc and leave $n \cdot 1 = r \cdot 1$. The remainder is smaller than c, and c was the **least** positive integer with a vanishing multiple, so $r \cdot 1 = 0$ forces $r = 0$. For $c = 0$ there is nothing to divide: no positive multiple vanishes, and negatives follow by a sign.

Proof.

(a) *Case* $c = 0$. We show $n \cdot 1 = 0$ iff $n = 0$, which is the claim since $0 \mid n$ iff $n = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (a)). If $n = 0$, $n \cdot 1 = 0$. If $n > 0$, then $n \cdot 1 \neq 0$ by Definition 2.5.1, since $c = 0$ means no positive multiple vanishes. If $n < 0$, then $n \cdot 1 = -((-n) \cdot 1)$ with $(-n) \cdot 1 \neq 0$; and $-x = 0$ would give $x = -(-x) = -0 = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)), so $n \cdot 1 \neq 0$.
Case $c > 0$. ($\Leftarrow$) If $c \mid n$, say $n = qc$ with $q \in \mathbb{Z}$, then by Lemma 2.5.1 (b), which holds for integers by part (d),

$$n \cdot 1 = (qc) \cdot 1 = (q \cdot 1)(c \cdot 1) = (q \cdot 1)\, 0 = 0,$$

the last step by Theorem 2.1.1 (d) and (F6).
($\Rightarrow$) Suppose $n \cdot 1 = 0$. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2 there are $q, r \in \mathbb{Z}$ with $n = qc + r$ and $0 \leq r < c$. By the sum rule of Lemma 2.5.1 (d) and the computation just made,

$$0 = n \cdot 1 = (qc) \cdot 1 + r \cdot 1 = 0 + r \cdot 1 = r \cdot 1,$$

using (F1) and (F3) at the end. If $r > 0$, then r is a positive integer with $r \cdot 1 = 0$ and $r < c$, against the minimality of c in Definition 2.5.1. So $r = 0$, and $n = qc$, that is, $c \mid n$.

(b) In a field an element is invertible if and only if it is non-zero: a non-zero element has an inverse by (F8), and 0 has none, since $0 \cdot y = 0 \neq 1$ (Theorem 2.1.1 (d), and $1 \neq 0$ by (F7)). So (b) is (a) negated. For $n = 2$: $2 \cdot 1 = (0 \cdot 1 + 1) + 1 = 1 + 1$. The positive divisors of 2 are 1 and 2 (2 is prime), and $0 \nmid 2$; and $c \neq 1$, since $1 \cdot 1 = 1 \neq 0$. So $c \mid 2$ iff $c = 2$, and $1 + 1$ is invertible iff $c \neq 2$. This proves the proposition.

■

This is the form the linear-algebra volumes use, in sentences such as "$\operatorname{char} F \neq 2$, so 2 is invertible" and "$m \cdot 1$ is invertible when $\operatorname{char} F \nmid m$". It also says that the integers n with $n \cdot 1 = 0$ are exactly the multiples of one integer, c, with nothing else vanishing by accident.

Warning. In characteristic 2, $1 + 1 = 0$, so $-1 = 1$ and $x = -x$ for every x. The familiar step "$x = -x$, so $2x = 0$, so $x = 0$" divides by $2 = 1 + 1$, which is 0 there. In $\mathbb{F}_2$, the element 1 satisfies $1 = -1$ and $1 \neq 0$. This is why many later results, for instance about symmetric and alternating bilinear forms in the linear-algebra volumes, assume $\operatorname{char} F \neq 2$: by Proposition 2.5.2 (b), that is exactly the hypothesis that makes the step valid.

Example. Completing the square in $\mathbb{F}_3$

Solve $x^2 + x + 1 = 0$ in $\mathbb{F}_3$ by completing the square.

Solution. Since $\operatorname{char} \mathbb{F}_3 = 3 \neq 2$ (the first examples above), $2 = 1 + 1$ is invertible by Proposition 2.5.2 (b); indeed $2 \cdot 2 = 4 = 1$, so $2^{-1} = 2$. Also $4 = 1 \neq 0$, so $x^2 + x + 1 = 0$ holds if and only if $4(x^2 + x + 1) = 0$ (one direction by Theorem 2.1.1 (d) and (F6), the

other by (f)). By Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d), with the multiples regrouped by Lemma 2.5.1 (b), (F5) and (F6), $(2x+1)^2 = 4x^2 + 4x + 1$, so

$$4(x^2 + x + 1) = (2x+1)^2 + 3 = (2x+1)^2,$$

as $3 = 0$ in $\mathbb{F}_3$. So the equation says $(2x+1)^2 = 0$, that is, $2x + 1 = 0$ by Theorem 2.1.1 (f), and $x = 2^{-1}(-1) = 2 \cdot 2 = 1$ by Proposition 2.1.3 (a), using $-1 = 2$. Testing all three elements agrees: $x = 0, 1, 2$ give 1, $3 = 0$ and $7 = 1$. In $\mathbb{F}_2$ the method stops at the first step: there $2 = 0$ and $4 = 0$, so multiplying by 4 cannot be undone and 2 has no inverse.

The characteristics found so far are 0, 2 and 3, and the ring $\mathbb{Z}/6\mathbb{Z}$ has characteristic 6. A field cannot.

Theorem 2.5.3. The Characteristic Is Zero or a Prime

Let F be a field. Then $\operatorname{char} F$ is 0 or a prime.

Idea. This is the argument that showed $\mathbb{Z}/n\mathbb{Z}$ is not a field for composite n (Theorem 2.2.2), run inside F. If $c = rs$ with smaller factors, then $(r \cdot 1)(s \cdot 1) = c \cdot 1 = 0$. A field has no zero divisors, so one of the two factors is already 0, at a multiple smaller than c.

Proof. Let $c := \operatorname{char} F$ and suppose $c > 0$. Since $1 \cdot 1 = 1 \neq 0$ by (F7), $c \neq 1$, so $c \geq 2$. Suppose c is not prime. By Sets, Relations, and Cardinality, Definition 2.2.2 it has a positive divisor $r \notin \{1, c\}$; write $c = rs$ with $s \in \mathbb{Z}$. Then $s > 0$, as $r, c > 0$, and $s \mid c$; $r \leq c$ and $s \leq c$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e); and $s \neq 1$, $s \neq c$, since $s = 1$ would give $r = c$ and $s = c$ would give $r = 1$ (cancel $c \neq 0$ in $\mathbb{Z}$). So $1 < r < c$ and $1 < s < c$. By Lemma 2.5.1 (b),

$$(r \cdot 1)(s \cdot 1) = (rs) \cdot 1 = c \cdot 1 = 0,$$

so $r \cdot 1 = 0$ or $s \cdot 1 = 0$ by Theorem 2.1.1 (f). Either way a positive integer smaller than c has a vanishing multiple, against the minimality of c. Hence c is prime. This proves the theorem. ∎

So the possible characteristics of fields are $0, 2, 3, 5, 7, 11, \ldots$, and the example at the end of the next subsection shows that each of them occurs. The hypothesis "field" is used twice, at $1 \neq 0$ and at "no zero divisors", and the ring $\mathbb{Z}/6\mathbb{Z}$ shows the second cannot be dropped: there $[2][3] = [0]$.

2.5.3 The characteristic under subfields and homomorphisms

The characteristic is computed from 0, 1 and + alone. A subfield has the same three, and a homomorphism carries them over, so both must preserve it.

Proposition 2.5.4. Subfields and Homomorphisms Preserve the Characteristic

(a) If K is a subfield of L, then $\operatorname{char} K = \operatorname{char} L$.

(b) If $\varphi\colon F \to L$ is a homomorphism, then $\operatorname{char} F = \operatorname{char} L$.

(c) There is no homomorphism between two fields of different characteristic.

Proof.

(a) By Proposition 2.3.1 (a), K has the zero 0_L, the one 1_L, and the restricted addition of L. Hence $n \cdot 1_K = n \cdot 1_L$ for every $n \in \mathbb{N}$, by induction (Logic and Proof, Axiom 4.2.1): both are 0_L at $n = 0$, and both add 1_L at each step. So the sets of positive n with $n \cdot 1 = 0$ are the same in K and in L, and so are their least elements, or both sets are empty.

(b) For $n \in \mathbb{N}$, $\varphi(n \cdot 1_F) = n \cdot \varphi(1_F) = n \cdot 1_L$ by Proposition 2.4.1 (f) and Definition 2.4.1. Since $\varphi(0) = 0$ (Proposition 2.4.1 (a)) and φ is injective (part (c) there), $n \cdot 1_F = 0$ if and only if $\varphi(n \cdot 1_F) = 0$, that is, if and only if $n \cdot 1_L = 0$. As in (a), the two characteristics coincide.

(c) is (b) read contrapositively. This proves the proposition.

■

Part (c) explains two of the obstructions of Section 2.4 at once: there is no homomorphism $\mathbb{F}_2 \to \mathbb{Q}$ and none $\mathbb{Q} \to \mathbb{F}_p$ (Example (Pairs of Fields with No Homomorphism) (ii), (iii)), because the characteristics are 2 and 0, and 0 and p.

Example. The characteristics of the standard fields

Find the characteristic of every ordered field, of $\mathbb{Q}$ and $\mathbb{R}$, of $\mathbb{C}$, of $\mathbb{F}_p$ for a prime p, and of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$.

Solution. Ordered fields. Let F be an ordered field (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.2). Since $1 \neq 0$, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h) gives $n \cdot 1 > 0$ for every $n \in \mathbb{N}$ with $n \geq 1$; in particular $n \cdot 1 \neq 0$. So no positive multiple of 1 vanishes, and $\operatorname{char} F = 0$.

$\mathbb{Q}$ *and* $\mathbb{R}$. Both are ordered fields (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 5.3.3), so both have characteristic 0. For $\mathbb{R}$ one can also use Proposition 2.5.4 (a), as $\mathbb{Q}$ is a subfield of $\mathbb{R}$ (Example (Rational and Integer Complex Numbers) (iii)).

$\mathbb{C}$. The field $\mathbb{R}$ is a subfield of $\mathbb{C}$ (Example (Rational and Integer Complex Numbers) (iii)), so $\operatorname{char} \mathbb{C} = \operatorname{char} \mathbb{R} = 0$ by Proposition 2.5.4 (a). This argument uses no order on $\mathbb{C}$.

$\mathbb{F}_p$. (In this section we keep the brackets on classes of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ wherever integers and their classes appear side by side, as in $n \cdot [1] = [n]$; elsewhere elements of $\mathbb{F}_p$ are written without brackets, as in Section 2.2.) For $n \in \mathbb{N}$, $n \cdot [1] = [n]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d)), and $[n] = [0]$ if and only if $n \in p\mathbb{Z}$, that is, $p \mid n$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (d)). A positive n with $p \mid n$ has $p \leq n$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e)), and $p \mid p$. So the least

positive n with $n \cdot [1] = [0]$ is p, and $\operatorname{char} \mathbb{F}_p = p$.

$\mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(i)$. They are subfields of $\mathbb{R}$ and of $\mathbb{C}$ (Example (The Field Generated by the Square Root of Two), Example (Rational and Integer Complex Numbers) (i)), so both have characteristic 0 by Proposition 2.5.4 (a).

So every prime occurs as a characteristic, and so does 0. The four-element field of Section 2.2's Exercise C1 has characteristic 2; Exercise C3 below checks it, and nothing here depends on it.

Quick check. What are $\operatorname{char} \mathbb{F}_7$ and $\operatorname{char} \mathbb{Q}(\sqrt{2})$? Is $7 \cdot [3] = [1]$ in $\mathbb{F}_5$?

Solution. $\operatorname{char} \mathbb{F}_7 = 7$ and $\operatorname{char} \mathbb{Q}(\sqrt{2}) = 0$ (Example (The characteristics of the standard fields)). Yes: $7 \cdot [3] = (7 \cdot [1])[3] = [7][3] = [21]$ by Lemma 2.5.1 (c), and $[21] = [1]$ since $21 - 1 = 20 = 4 \cdot 5$. Equivalently, $7 \cdot [3] = 2 \cdot [3]$ because $5 \cdot [3] = [0]$, and $2 \cdot [3] = [6] = [1]$.

2.5.4 The prime subfield

Section 2.3 defined the prime subfield of a field F as the smallest subfield, the intersection of all subfields of F (Definition 2.3.2), and promised to identify it. Every subfield contains 1, hence every $n \cdot 1$, hence every quotient $(m \cdot 1)(n \cdot 1)^{-1}$ with $n \cdot 1 \neq 0$. The characteristic decides which of these quotients exist, and so which number system the prime subfield copies.

The identification goes through a homomorphism into F, and the main point is that there is exactly one. For ordered fields this is *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 4's embedding $\iota_F \colon \mathbb{Q} \to F$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 4.2.2). We keep the name ι_F, and, as before, the brackets on the classes of $\mathbb{F}_p$.

Theorem 2.5.5. The Prime Subfield

Let F be a field and P its prime subfield (Definition 2.3.2).

(a) If $\operatorname{char} F = p > 0$, then $\iota_F([n]) := n \cdot 1$ $(n \in \mathbb{Z})$ is a well-defined homomorphism $\iota_F \colon \mathbb{F}_p \to F$. It is the **only** homomorphism $\mathbb{F}_p \to F$, and its image is P. Hence $P \cong \mathbb{F}_p$.

(b) If $\operatorname{char} F = 0$, then $\iota_F(m/n) := (m \cdot 1)(n \cdot 1)^{-1}$ $(m \in \mathbb{Z},\ n \in \mathbb{Z}_{>0})$ is a well-defined homomorphism $\iota_F \colon \mathbb{Q} \to F$. It is the **only** homomorphism $\mathbb{Q} \to F$, and its image is P. Hence $P \cong \mathbb{Q}$.

In (a), p is prime by Theorem 2.5.3, so $\mathbb{F}_p$ is a field (Definition 2.2.1) and "homomorphism $\mathbb{F}_p \to F$" has a meaning.

Try it first (ten minutes): a homomorphism $\psi \colon \mathbb{Q} \to F$ *must send* 1 *to* 1. *Where must it send* 3, -3 *and* $1/3$? *What could go wrong with* $1/3$?

Idea. An attempt runs as follows. $\psi(3) = \psi(1+1+1) = 1+1+1 = 3 \cdot 1$, then $\psi(-3) = -\psi(3) = (-3) \cdot 1$, and $\psi(1/3)$ must be the inverse of $\psi(3)$, so $\psi(1/3) = (3 \cdot 1)^{-1}$. The homomorphism

has no freedom at all: it is determined by $\psi(1) = 1$, through sums, negatives and inverses. That gives **uniqueness**, and it also dictates the only possible formula, $m/n \mapsto (m\cdot 1)(n\cdot 1)^{-1}$.

What can go wrong is $1/3$: if $3 \cdot 1 = 0$ in F, it has no inverse, and no homomorphism exists. The characteristic says exactly when this happens. In characteristic 0 the formula makes sense, and what remains is to check that it does not depend on how a rational is written, which follows from Lemma 2.5.1 (b) and a regrouping by (F5)–(F8), and that it respects $+$ and $\cdot$, which the fraction rules of Theorem 2.1.1 (g) give. In characteristic p, the classes $[n]$ play the role of the rationals, and $p \cdot 1 = 0$ is exactly what makes $[n] \mapsto n \cdot 1$ well defined. The image is then a subfield (Section 2.4) built from 1 alone, so it lies inside every subfield: it is the prime subfield.

Before reading on: where is $\operatorname{char} F = 0$ *used in (b), and why does the same formula fail for* $F = \mathbb{F}_5$*?*

Proof. **Part (a).** Let $\operatorname{char} F = p > 0$.

Well defined. Every element of $\mathbb{F}_p$ is a class $[n]$ with $n \in \mathbb{Z}$ (Sets, Relations, and Cardinality, Definition 2.5.4). If $[n] = [n']$, then $p \mid n - n'$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (a), for the ideal $p\mathbb{Z}$), so $(n - n') \cdot 1 = 0$ by Proposition 2.5.2 (a), and $n\cdot 1 - n'\cdot 1 = (n-n')\cdot 1 = 0$ by Lemma 2.5.1 (d). So $n\cdot 1 = n'\cdot 1$: the value does not depend on the representative. (This is Number Systems: From \(\nN\) to \(\nR\), Theorem 2.2.1 (a) with equality as the relation on F, whose classes are the singletons $\{y\}$, followed by $\{y\} \mapsto y$.)

Homomorphism. For $m, n \in \mathbb{Z}$, by the operations of $\mathbb{Z}/p\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (b)) and Lemma 2.5.1 (d), parts (a) and (b) there,

$$\iota_F([m] + [n]) = \iota_F([m+n]) = (m+n)\cdot 1 = m\cdot 1 + n\cdot 1,$$
$$\iota_F([m][n]) = \iota_F([mn]) = (mn)\cdot 1 = (m\cdot 1)(n\cdot 1),$$

and $\iota_F([1]) = 1 \cdot 1 = 1$. So ι_F is a homomorphism (Definition 2.4.1).

Image $= P$. The image $\iota_F(\mathbb{F}_p)$ is a subfield of F (Proposition 2.4.1 (d)), and P is contained in every subfield (Definition 2.3.2), so $P \subseteq \iota_F(\mathbb{F}_p)$. Conversely, let K be any subfield of F. It contains 0 and 1 and is closed under $+$ (Definition 2.3.1), so $n \cdot 1 \in K$ for every $n \in \mathbb{N}$, by induction on n (Logic and Proof, Axiom 4.2.1): $0 \cdot 1 = 0 \in K$, and $(n+1)\cdot 1 = n\cdot 1 + 1 \in K$. It is closed under negatives, so $n \cdot 1 = -((-n)\cdot 1) \in K$ for $n < 0$ as well. So $\iota_F(\mathbb{F}_p) \subseteq K$ for every subfield K, that is, $\iota_F(\mathbb{F}_p) \subseteq P$.

Uniqueness. Let $\psi\colon \mathbb{F}_p \to F$ be a homomorphism and $n \in \mathbb{Z}$. Then $[n] = n\cdot[1]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d), extended to $n < 0$ after Lemma 2.5.1). For $n \in \mathbb{N}$, $\psi(n \cdot [1]) = n \cdot \psi([1]) = n \cdot 1$ by Proposition 2.4.1 (f); for $n < 0$,

$$\psi(n \cdot [1]) = \psi(-((-n)\cdot[1])) = -((-n)\cdot 1) = n \cdot 1,$$

by the definition of negative multiples at both ends, and in the middle by Proposition 2.4.1 (a) followed by the case $-n \in \mathbb{N}$ just done. So $\psi([n]) = n \cdot 1 = \iota_F([n])$ for every n, and $\psi = \iota_F$.

Finally, ι_F is an isomorphism from $\mathbb{F}_p$ onto its image P by Proposition 2.4.1 (d), so $P \cong \mathbb{F}_p$.

Part (b). Let $\operatorname{char} F = 0$. Recall that $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}_{>0})/\!\sim$ (Number Systems: From \(\nN\) to \(\nR\), Definition 2.4.1), that the class $[(m,n)]$ is the quotient m/n of the integers m and n in $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4 (a)), and that for $n, n' \in \mathbb{Z}_{>0}$, $m/n = m'/n'$ if and only if $mn' = m'n$ (part (b) there).

The formula makes sense. For $n > 0$, $n \cdot 1 \neq 0$ by Proposition 2.5.2 (a), since $0 \nmid n$. So $(n \cdot 1)^{-1}$ exists by (F8). This is the only place where $\operatorname{char} F = 0$ is used.

Well defined. Let $m/n = m'/n'$ with $n, n' > 0$, so $mn' = m'n$. By Lemma 2.5.1 (d), part (b) there,

$$(m \cdot 1)(n' \cdot 1) = (mn') \cdot 1 = (m'n) \cdot 1 = (m' \cdot 1)(n \cdot 1).$$

Multiply both sides by $(n \cdot 1)^{-1}(n' \cdot 1)^{-1}$ and regroup by (F5), (F6), (F8) and (F7): the left side becomes $(m \cdot 1)(n \cdot 1)^{-1}$ and the right side $(m' \cdot 1)(n' \cdot 1)^{-1}$. So the value does not depend on the representative.

Homomorphism. Let $m/n, r/s \in \mathbb{Q}$ with $n, s > 0$, and put $\bar{m} \coloneqq m \cdot 1$, and likewise $\bar{n}$, $\bar{r}$, $\bar{s}$. By Number Systems: From \(\nN\) to \(\nR\), Definition 2.4.2, $m/n + r/s = (ms + rn)/(ns)$ and $(m/n)(r/s) = (mr)/(ns)$, with $ns > 0$. By Lemma 2.5.1 (d), $(ms + rn) \cdot 1 = \bar{m}\bar{s} + \bar{r}\bar{n}$, $(mr) \cdot 1 = \bar{m}\bar{r}$ and $(ns) \cdot 1 = \bar{n}\bar{s}$. So, by the fraction rules Theorem 2.1.1 (g) in F (with $\bar{n}, \bar{s} \neq 0$),

$$\iota_F\Big(\frac{m}{n} + \frac{r}{s}\Big) = \frac{\bar{m}\bar{s} + \bar{n}\bar{r}}{\bar{n}\bar{s}} = \frac{\bar{m}}{\bar{n}} + \frac{\bar{r}}{\bar{s}},$$
$$\iota_F\Big(\frac{m}{n} \cdot \frac{r}{s}\Big) = \frac{\bar{m}\bar{r}}{\bar{n}\bar{s}} = \frac{\bar{m}}{\bar{n}} \cdot \frac{\bar{r}}{\bar{s}},$$

where $x/y \coloneqq xy^{-1}$ in F and $\bar{r}\bar{n} = \bar{n}\bar{r}$ by (F6). Also $\iota_F(1) = \iota_F(1/1) = (1 \cdot 1)(1 \cdot 1)^{-1} = 1 \cdot 1^{-1} = 1$. So ι_F is a homomorphism.

Image $= P$. As in (a), $P \subseteq \iota_F(\mathbb{Q})$ because the image is a subfield. Conversely, every subfield K contains $m \cdot 1$ and $n \cdot 1$ (as in (a)), hence $(n \cdot 1)^{-1}$, as $n \cdot 1 \neq 0$, and the product $(m \cdot 1)(n \cdot 1)^{-1}$ (Definition 2.3.1). So $\iota_F(\mathbb{Q}) \subseteq P$.

Uniqueness. Let $\psi \colon \mathbb{Q} \to F$ be a homomorphism. In $\mathbb{Q}$, the integer $m \in \mathbb{Z} \subseteq \mathbb{Q}$ is the multiple $m \cdot 1_{\mathbb{Q}}$: the embedding j of Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4 has $j(0) = 0$ and $j(k+1) = j(k) + 1$, so $j(k) = k \cdot 1_{\mathbb{Q}}$ for $k \in \mathbb{N}$ by induction, and $j(-k) = -j(k) = (-k) \cdot 1_{\mathbb{Q}}$. As in (a), $\psi(m \cdot 1_{\mathbb{Q}}) = m \cdot 1$ for every $m \in \mathbb{Z}$, by Proposition 2.4.1 (f) and (a). For $n > 0$, $m/n = mn^{-1}$ in $\mathbb{Q}$ with $n \neq 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4 (a)), so by Proposition 2.4.1 (b),

$$\psi\Big(\frac{m}{n}\Big) = \psi(m)\,\psi(n^{-1}) = \psi(m)\,\psi(n)^{-1} = (m \cdot 1)(n \cdot 1)^{-1} = \iota_F\Big(\frac{m}{n}\Big).$$

So $\psi = \iota_F$. As in (a), ι_F is an isomorphism onto P, and $P \cong \mathbb{Q}$. This proves the theorem.

■

Answer to the prompt. In (b), $\operatorname{char} F = 0$ is used only to know that $n \cdot 1 \neq 0$ for $n > 0$, so that $(n \cdot 1)^{-1}$ exists; every other step works in any field. In $F = \mathbb{F}_5$, $5 \cdot 1 = 0$, so "$1/5 \mapsto (1 \cdot 1)(5 \cdot 1)^{-1}$" names no element: the formula has no meaning there, which matches Example (Pairs of Fields with No Homomorphism) (iii), where no homomorphism $\mathbb{Q} \to \mathbb{F}_p$ exists at all.

Second reading · *Two remarks on the formulas*

Two consequences of the formulas are worth recording, though nothing below rests on them. For $F = \mathbb{Q}$, $\iota_{\mathbb{Q}}(m/n) = j(m)j(n)^{-1} = m/n$, so $\iota_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$; for $F = \mathbb{F}_p$, $\iota_{\mathbb{F}_p}([n]) = n \cdot [1] = [n]$, so $\iota_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$. And in (b) the formula also holds for negative denominators: if $n < 0$, then $m/n = (-m)/(-n)$ with $-n > 0$, and $((-m) \cdot 1)((-n) \cdot 1)^{-1} = (-\bar{m})(-\bar{n})^{-1} = \bar{m}\bar{n}^{-1}$, because $(-\bar{n})^{-1} = -\bar{n}^{-1}$ (their product with $-\bar{n}$ is $\bar{n}\bar{n}^{-1} = 1$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)).

Remark. For an ordered field F, part (b) is Number Systems: From \(\nN\) to \(\nR\), Theorem 4.2.2, where order supplied $n \cdot 1 > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.2.1); by uniqueness the two maps called ι_F are the same map. Here the characteristic supplies the weaker fact $n \cdot 1 \neq 0$, which is all the construction needs. The same "no freedom on 1" argument gave *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 6's Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.1.

The uniqueness half of the theorem is a rigidity statement. It says that a homomorphism has no choice on the prime subfield, and the next corollary spells this out.

Corollary 2.5.6. Homomorphisms Respect the Prime Subfield

(a) Let $\varphi\colon F \to L$ be a homomorphism. Then $\varphi \circ \iota_F = \iota_L$, and φ maps the prime subfield of F onto the prime subfield of L.

(b) The identity is the only homomorphism $\mathbb{Q} \to \mathbb{Q}$, and the only homomorphism $\mathbb{F}_p \to \mathbb{F}_p$ for each prime p. In particular the only automorphism of $\mathbb{Q}$, and of $\mathbb{F}_p$, is the identity.

(c) Every automorphism of a field F fixes each element of the prime subfield of F.

Proof.

(a) By Proposition 2.5.4 (b), $\operatorname{char} F = \operatorname{char} L$, so ι_F and ι_L have the same domain D, which is $\mathbb{Q}$ or $\mathbb{F}_p$ by Theorem 2.5.5. The composite $\varphi \circ \iota_F\colon D \to L$ is a homomorphism (Proposition 2.4.1 (e)), so it equals ι_L by the uniqueness clause of Theorem 2.5.5. Hence $\varphi(\iota_F(D)) = \iota_L(D)$, and by Theorem 2.5.5 these images are the prime subfields of F and of L.

(b) The identity $\mathrm{id}_{\mathbb{Q}}$ is a homomorphism (Proposition 2.4.1 (e)), and $\operatorname{char}\mathbb{Q} = 0$ (Example (The characteristics of the standard fields)), so by the uniqueness clause of Theorem 2.5.5 (b) with $F = \mathbb{Q}$, every homomorphism $\mathbb{Q} \to \mathbb{Q}$ equals $\mathrm{id}_{\mathbb{Q}}$. Likewise for $\mathbb{F}_p$, using $\operatorname{char}\mathbb{F}_p = p$ and part (a) of the theorem. An automorphism is a homomorphism, so it is the identity.

(c) Let σ be an automorphism of F. By (a) with $L = F$, $\sigma \circ \iota_F = \iota_F$, so $\sigma(x) = x$ for every $x = \iota_F(d)$ in the image of ι_F, which is the prime subfield. This proves the corollary.

■

For instance, complex conjugation fixes every rational number, and the automorphisms of $\mathbb{Q}(\sqrt{2})$ and of $\mathbb{Q}(i)$ in Section 2.4 had no choice on $\mathbb{Q}$; only the images of $\sqrt{2}$ and of i were free.

Finite fields are the case that matters most for computation, and for them the characteristic cannot be 0.

Corollary 2.5.7. A Finite Field Has Prime Characteristic

Let F be a finite field.

(a) $\operatorname{char} F$ is a prime p.

(b) F contains a subfield isomorphic to $\mathbb{F}_p$, namely its prime subfield.

(c) $p \cdot a = 0$ for every $a \in F$.

Proof.

(a) Say F has N elements (Sets, Relations, and Cardinality, Definition 3.1.2). Suppose $\operatorname{char} F = 0$, and consider $f\colon \{1, \dots, N+1\} \to F$, $f(k) \coloneqq k \cdot 1$. If $k \cdot 1 = k' \cdot 1$, then $(k-k') \cdot 1 = 0$ (Lemma 2.5.1 (d)), so $0 \mid k-k'$ by Proposition 2.5.2 (a), hence $k-k' = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (a)) and $k = k'$. So f is an injection from a set with $N+1$ elements into a set with N elements, which Sets, Relations, and Cardinality, Corollary 3.1.3 (a) forbids. Hence $\operatorname{char} F \neq 0$, and $\operatorname{char} F$ is a prime by Theorem 2.5.3.

(b) is Theorem 2.5.5 (a).

(c) By Lemma 2.5.1 (c), $p \cdot a = (p \cdot 1)a = 0 \cdot a = 0$, using Theorem 2.1.1 (d). This proves the corollary.

■

A finite field therefore contains one of the fields $\mathbb{F}_p$ of Section 2.2. One can show that it has p^n elements for some $n \geq 1$; that needs the vector spaces of the linear-algebra volumes, and nothing in this volume uses it.

Quick check. Can a field with 6 elements contain a copy of $\mathbb{F}_2$ and also a copy of $\mathbb{F}_3$?

Solution. No. A copy of $\mathbb{F}_2$ is a subfield K with $\operatorname{char} K = 2$, and a copy of $\mathbb{F}_3$ a subfield with characteristic 3 (Example (The characteristics of the standard fields), Proposition 2.5.4 (b) for the isomorphisms). By Proposition 2.5.4 (a) both characteristics equal $\operatorname{char} F$, and $2 \neq 3$. (In fact no field has 6 elements, but that is the p^n fact just mentioned, which we do not prove.)

2.5.5 Exercises

2.5.5.1 A. Check your understanding

Exercise. A1

These parts are about the proof of Theorem 2.5.5.

(a) In the proof of part (b), where is the hypothesis $\operatorname{char} F = 0$ used, and where is it not needed?

(b) Try to define $\mathbb{Q} \to \mathbb{F}_5$ by $m/n \mapsto [m][n]^{-1}$ $(n > 0)$. Name a rational number that has no image, and explain why the rule also fails to be well defined.

(c) What are $\iota_{\mathbb{R}}$ and $\iota_{\mathbb{C}}$? Justify your answer from the uniqueness clause.

(d) State the idea of the proof in two sentences.

Solution.

(a) Only in the step "the formula makes sense": $n \cdot 1 \neq 0$ for $n > 0$ (Proposition 2.5.2 (a)), so $(n \cdot 1)^{-1}$ exists. Well-definedness, the homomorphism property, the image and uniqueness are computations in an arbitrary field once these inverses exist.

(b) $1/5$: its image would be $[1][5]^{-1}$, and $[5] = [0]$ has no inverse. The rule is not even well defined on the rationals where it seems to make sense: $1 = 1/1 = 5/5$, and the representative $(5, 5)$ gives $[5][5]^{-1}$, which does not exist, while $(1, 1)$ gives $[1]$.

(c) Both are inclusions. $\mathbb{Q}$ is a subfield of $\mathbb{R}$ and $\mathbb{R}$ of $\mathbb{C}$ (Example (Rational and Integer Complex Numbers) (iii)), so $\mathbb{Q}$ is a subfield of $\mathbb{C}$, and the inclusion of a subfield is a homomorphism (Example (Conjugation and Other Automorphisms) (ii)). By the uniqueness clause of Theorem 2.5.5 (b) (both fields have characteristic 0, Example (The characteristics of the standard fields)), $\iota_{\mathbb{R}}$ and $\iota_{\mathbb{C}}$ are these inclusions, $q \mapsto q$.

(d) A homomorphism out of $\mathbb{Q}$ or $\mathbb{F}_p$ is forced by $1 \mapsto 1$ to send m/n to $(m \cdot 1)(n \cdot 1)^{-1}$ (or $[n]$ to $n \cdot 1$), so there is at most one, and its image lies in every subfield. The characteristic decides whether this forced formula makes sense, and when it does, the fraction rules show it is a homomorphism, whose image is then the prime subfield.

2.5.5.2 B. Practice

Exercise. B1: Reducing multiples

Let F be a field of characteristic $p > 0$ and $a \in F$.

(a) Show that $(p - 1) \cdot a = -a$.

(b) Show that $(kp + r) \cdot a = r \cdot a$ for all $k, r \in \mathbb{Z}$.

(c) In $\mathbb{F}_7$, compute $100 \cdot [3]$ directly, and again using (b).

Solution.

(a) By Lemma 2.5.1 (d) and (c), $(p - 1) \cdot a + a = (p - 1) \cdot a + 1 \cdot a = p \cdot a = (p \cdot 1)a = 0 \cdot a = 0$, using Theorem 2.1.1 (d). By uniqueness of negatives (Theorem 2.1.1 (c)), $(p - 1) \cdot a = -a$.

(b) By Lemma 2.5.1 (d), $(kp + r) \cdot a = (kp) \cdot a + r \cdot a = k \cdot (p \cdot a) + r \cdot a$. Now $p \cdot a = 0$ as in (a), and $k \cdot 0 = (k \cdot 1)0 = 0$ by Lemma 2.5.1 (c) with (d) and Theorem 2.1.1 (d). So $(kp + r) \cdot a = 0 + r \cdot a = r \cdot a$.

(c) Directly: $100 \cdot [3] = (100 \cdot [1])[3] = [100][3] = [300]$ (Lemma 2.5.1 (c), Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d)), and $300 = 42 \cdot 7 + 6$, so $100 \cdot [3] = [6]$. By (b): $100 = 14 \cdot 7 + 2$, so $100 \cdot [3] = 2 \cdot [3] = [6]$. The two agree.

Exercise. B2: Completing the square

Let F be a field with $\operatorname{char} F \neq 2$, and write $2 := 2 \cdot 1$, $4 := 4 \cdot 1$.

(a) Show that $x = -x$ implies $x = 0$, for $x \in F$.

(b) Let $b, c \in F$. Show that the equation $x^2 + bx + c = 0$ has a solution $x \in F$ if and only if $b^2 - 4c = s^2$ for some $s \in F$, and that then its solutions are exactly $x = (-b + s)/2$ and $x = (-b - s)/2$.

(c) Use (b) to solve $x^2 + x + 1 = 0$ in $\mathbb{F}_7$.

(d) Explain why (b) says nothing in $\mathbb{F}_2$, and show that its conclusion is in fact false there.

Solution. By Proposition 2.5.2 (b), $2 \neq 0$, so 2 is invertible; and $4 = (2 \cdot 2) \cdot 1 = 2 \cdot 2 \neq 0$ by Lemma 2.5.1 (b) and Theorem 2.1.1 (f). For $u \in F$, $2u = (2 \cdot 1)u = u + u$ by Lemma 2.5.1 (c).

(a) If $x = -x$, then $2x = x + x = x + (-x) = 0$. Since $2 \neq 0$, $x = 0$ by Theorem 2.1.1 (f).

(b) Since $4 \neq 0$, $x^2 + bx + c = 0$ if and only if $4(x^2 + bx + c) = 0$ (one direction by Theorem 2.1.1 (d) and (F6), the other by (f)). By Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d), $(2x + b)^2 = (2x)^2 + 2(2x)b + b^2 = 4x^2 + 4bx + b^2$, the products of the multiples regrouped by Lemma 2.5.1 (b), (F5) and (F6). Hence, with $D := b^2 - 4c$,

$$4(x^2 + bx + c) = (2x + b)^2 - D,$$

and the equation is equivalent to $(2x+b)^2 = D$. (Multiplying this identity by 4^{-1} gives the familiar $x^2 + bx + c = (x + b/2)^2 - D/4$.) If x is a solution, $s := 2x + b$ has $s^2 = D$. Conversely, if $s^2 = D$, then by Corollary 2.1.2, $(2x + b)^2 = s^2$ if and only if $2x + b = s$ or $2x + b = -s$, and by Proposition 2.1.3 (a) (with $2 \neq 0$) these say $x = (-b + s)/2$ or $x = (-b - s)/2$.

(c) Here $b = c = 1$ and $D = 1 - 4 = -3 = 4 = 2^2$ in $\mathbb{F}_7$, so $s = 2$; and $2^{-1} = 4$, since $2 \cdot 4 = 8 = 1$. The solutions are $x = 4(-1 + 2) = 4$ and $x = 4(-1 - 2) = -12 = 2$. Check: $4^2 + 4 + 1 = 21 = 0$ and $2^2 + 2 + 1 = 7 = 0$ in $\mathbb{F}_7$. This agrees with Exercise (C3), found there by trying all seven elements.

(d) In $\mathbb{F}_2$, $2 = 0$ and $4 = 0$, so the first step, "$x^2 + bx + c = 0$ iff $4(\dots) = 0$", fails, and $/2$ has no meaning. The conclusion of (b) is false there: for $x^2 + x + 1 = 0$, $D = 1 - 0 = 1 = 1^2$ is a square, yet the equation has no solution, since $x = 0$ and $x = 1$ both give 1.

Exercise. B3: When the integers embed

Let F be a field.

(a) Show that for $n, n' \in \mathbb{Z}$, $n \cdot 1 = n' \cdot 1$ if and only if $\operatorname{char} F \mid n - n'$.

(b) Deduce that the map $\mathbb{Z} \to F$, $n \mapsto n \cdot 1$, is injective if $\operatorname{char} F = 0$, and is not injective if $\operatorname{char} F = p > 0$.

Solution.

(a) By Lemma 2.5.1 (d), $n \cdot 1 - n' \cdot 1 = (n - n') \cdot 1$. So $n \cdot 1 = n' \cdot 1$ iff $(n - n') \cdot 1 = 0$, iff $\operatorname{char} F \mid n - n'$ by Proposition 2.5.2 (a).

(b) If $\operatorname{char} F = 0$ and $n \cdot 1 = n' \cdot 1$, then $0 \mid n - n'$ by (a), so $n - n' = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (a)) and $n = n'$. If $\operatorname{char} F = p > 0$, then $p \cdot 1 = 0 = 0 \cdot 1$ with $p \neq 0$, so the map is not injective.

2.5.5.3 C. Going deeper

Exercise. C1: Exit check: the characteristic

Using only Definition 2.5.1, Lemma 2.5.1, division with remainder in $\mathbb{Z}$, Sets, Relations, and Cardinality, Definition 2.2.2 and the rules for divisibility in $\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1), and the field axioms with Theorem 2.1.1, prove:

(a) for a field F and $n \in \mathbb{Z}$, $n \cdot 1 = 0$ if and only if $\operatorname{char} F \mid n$;

(b) $\operatorname{char} F$ is 0 or a prime.

Solution.

(a) Let $c \coloneqq \operatorname{char} F$.
Case $c = 0$. No positive n has $n \cdot 1 = 0$, by Definition 2.5.1. For $n < 0$, $n \cdot 1 = -((-n) \cdot 1)$, and $(-n) \cdot 1 \neq 0$; since $-x = 0$ implies $x = -(-x) = 0$, also $n \cdot 1 \neq 0$. And $0 \cdot 1 = 0$. So $n \cdot 1 = 0$ iff $n = 0$, iff $0 \mid n$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (a)).
Case $c > 0$. Divide: $n = qc + r$ with $q, r \in \mathbb{Z}$, $0 \leq r < c$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2). By Lemma 2.5.1 (d), $(qc) \cdot 1 = (q \cdot 1)(c \cdot 1) = (q \cdot 1)0 = 0$ and $n \cdot 1 = (qc) \cdot 1 + r \cdot 1 = r \cdot 1$. If $c \mid n$, then $r = 0$ by uniqueness of the remainder, so $n \cdot 1 = 0 \cdot 1 = 0$. If $n \cdot 1 = 0$, then $r \cdot 1 = 0$ with $0 \leq r < c$; $r > 0$ would contradict the minimality of c, so $r = 0$ and $c \mid n$.

(b) Let $c > 0$. As $1 \cdot 1 = 1 \neq 0$, $c \geq 2$. If c were not prime, by Sets, Relations, and Cardinality, Definition 2.2.2 it would have a positive divisor $r \notin \{1, c\}$; write $c = rs$. Then $s > 0$, $r, s \leq c$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e), and $s \notin \{1, c\}$, since $s = 1$ gives $r = c$ and $s = c$ gives $r = 1$ (cancel $c \neq 0$). So $1 < r, s < c$, and $(r \cdot 1)(s \cdot 1) = (rs) \cdot 1 = 0$ by Lemma 2.5.1 (b), so $r \cdot 1 = 0$ or $s \cdot 1 = 0$ (Theorem 2.1.1 (f)), contradicting the minimality of c. So c is prime.

Marking scheme. (10 points)

- 2: the case $c = 0$, including negative n (a negative multiple is the negative of a non-zero element, hence non-zero).
- 3: division of n by c with remainder, and $n \cdot 1 = r \cdot 1$ justified by the rules for multiples and $c \cdot 1 = 0$.
- 2: minimality of c forces $r = 0$; the converse $c \mid n \Rightarrow n \cdot 1 = 0$.
- 1: $c \neq 1$ from $1 \neq 0$.
- 2: a factorization $c = rs$ with $1 < r, s < c$, bounds justified, gives $(r \cdot 1)(s \cdot 1) = 0$, and the absence of zero divisors contradicts minimality.

Fatal errors (0 for the step): "$c \cdot 1 = 0$, so $c \mid n$" for every n with $n \cdot 1 = 0$, without the

division step; treating $n \cdot 1$ as the integer n (for instance "$n \cdot 1 = 0$, so $n = 0$" in $\mathbb{F}_p$).

Exercise. C2: Find the error

Here is an argument.

> *Claim.* A finite field F has prime characteristic.
>
> *Proof.* (1) The elements $1 \cdot 1, 2 \cdot 1, 3 \cdot 1, \ldots$ of F cannot all be different, since F is finite. (2) So $m \cdot 1 = k \cdot 1$ for some positive integers $k < m$. (3) Hence $(m-k) \cdot 1 = m \cdot 1 - k \cdot 1 = 0$. (4) So $m - k$ is the characteristic of F, and it is prime by Theorem 2.5.3.

Is the conclusion true? Does the argument prove it? Name the failing step, say what is wrong with it, and give a counterexample to the step.

Solution. The conclusion is true: it is Corollary 2.5.7 (a). Steps (1) and (2) are correct (they are the pigeonhole argument of that proof, Sets, Relations, and Cardinality, Corollary 3.1.3), and so is step (3), by Lemma 2.5.1 (d). Step (4) fails.

Step (4). The argument only produces **some** positive integer with a vanishing multiple. The characteristic is the **least** one (Definition 2.5.1), and $m - k$ need not be least: in $\mathbb{F}_3$, $7 \cdot 1 = 1 = 1 \cdot 1$ gives $m - k = 6$, while $\operatorname{char} \mathbb{F}_3 = 3$. The step cites a property, "is the characteristic", that no line supplies, which is (N9) of Logic and Proof, Example (What is not allowed).

Repair. By (2) and Lemma 2.5.1 (d), $(m-k) \cdot 1 = 0$ with $m - k > 0$, so the set of positive integers with a vanishing multiple is non-empty and $\operatorname{char} F > 0$ (Definition 2.5.1); then Theorem 2.5.3 makes it prime.

Marking scheme. (10 points)

- 2: the conclusion is true, with the reference.
- 2: steps (1)–(3) are correct (including $(m-k) \cdot 1 = 0$ via Lemma 2.5.1 (d)).
- 6: step (4) named: only some positive multiple vanishes, the characteristic is the least one (Definition 2.5.1), with a counterexample to the step.

Exercise. C3: The four-element field

Let $F = \{0, 1, \alpha, \beta\}$ be the four-element field of Exercise (C1: A Field with Four Elements), with $\beta = 1 + \alpha$, $\alpha^2 = \beta$ and $\alpha\beta = 1$.

(a) Show that $\operatorname{char} F = 2$.

(b) Show that the prime subfield of F is $\{0, 1\}$, and that it is isomorphic to $\mathbb{F}_2$.

(c) Show that the map $F \to F$, $x \mapsto x^2$, is an automorphism of F that exchanges α and β.

Solution.

(a) $1 \cdot 1 = 1 \neq 0$, and $2 \cdot 1 = 1 + 1 = (1+1) + (0+0)\alpha = 0$ by the addition rule of Exercise

(C1: A Field with Four Elements), coefficient by coefficient in $\mathbb{F}_2$. So $\operatorname{char} F = 2$.

(b) By Theorem 2.5.5 (a), the prime subfield is the image of $\iota_F \colon \mathbb{F}_2 \to F$, which is $\{0 \cdot 1, 1 \cdot 1\} = \{0, 1\}$, and ι_F is an isomorphism from $\mathbb{F}_2$ onto it.

(c) Let $s(x) := x^2$. For $x, y \in F$, $(x+y)^2 = x^2 + 2xy + y^2$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d), where $2xy = (1+1)(xy) = 0\,(xy) = 0$, since $1+1 = 2 \cdot 1 = 0$ by part (a) and $0\,(xy) = 0$ by Theorem 2.1.1 (d); so $s(x+y) = s(x)+s(y)$. Next $(xy)^2 = (xy)(xy) = (xx)(yy) = x^2y^2$ by (F5) and (F6), and $1^2 = 1$. So s is a homomorphism (Definition 2.4.1). Its values are

$$s(0) = 0, \quad s(1) = 1, \quad s(\alpha) = \alpha^2 = \beta, \quad s(\beta) = (1+\alpha)^2 = 1 + \alpha^2 = 1 + \beta = \alpha,$$

using the additivity just proved and $1 + \beta = 1 + 1 + \alpha = \alpha$. So s permutes the four elements, is bijective, and is an automorphism exchanging α and β. (The next section shows that $x \mapsto x^p$ is a homomorphism in every field of characteristic p, and an automorphism when the field is finite.)

2.6 The Binomial Theorem, the Frobenius Map, and Fermat's Little Theorem

In $\mathbb{F}_5$, compute $(1+2)^5$ and $1^5 + 2^5$. The first is $3^5 = 243$, and $243 = 48 \cdot 5 + 3$, so it is 3. The second is $1 + 32 = 33 = 6 \cdot 5 + 3$, so it is 3 as well. The rule "$(x+y)^n = x^n + y^n$", the classic error of school algebra, is a theorem when n is the characteristic p of the field. This section proves it, and deduces Fermat's little theorem from it with the rigidity of Section 2.5: a homomorphism of $\mathbb{F}_p$ to itself is the identity.

The tool is the binomial theorem. School proves it for numbers; we need it in an arbitrary commutative ring, with the binomial coefficients acting as integer multiples, and so we first set up finite sums in a ring.

2.6.1 Sums and powers in a commutative ring

Sets, Relations, and Cardinality, Chapter 2 defines finite sums, products and powers of real numbers by recursion (Sets, Relations, and Cardinality, Definition 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.2, both from Sets, Relations, and Cardinality, Theorem 2.3.1). The definitions use nothing about $\mathbb{R}$ except an addition with a 0 and a multiplication with a 1. So, read on $\mathbb{N} = \omega$ through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b), with $X = R$, they define in every commutative ring R:

- sums $\sum_{k=m}^{n} a_k$ of elements $a_k \in R$, with the empty sum 0, and the three remarks after Sets, Relations, and Cardinality, Definition 2.3.1: a sum depends only on the terms it adds (finite lists), **shifting the index**, and **splitting off the last term**, $\sum_{k=m}^{n+1} a_k = \sum_{k=m}^{n} a_k + a_{n+1}$ for $m \le n+1$;
- powers $x^0 := 1$, $x^{n+1} := x^n x$ for $x \in R$ and $n \in \mathbb{N}$, with the laws of Sets, Relations, and Cardinality, Proposition 2.3.4 (a)–(c):

$$x^{m+n} = x^m x^n, \qquad (x^m)^n = x^{mn}, \qquad (xy)^n = x^n y^n.$$

The proofs of those laws in *Sets, Relations, and Cardinality* use only (F1)–(F7), (F9) and induction, so they run unchanged in R. We use this paragraph as a template and do not repeat it. (Chapter 1 proves the same power laws for every commutative ring as Proposition 1.1.3; we

compare, and cite the template.) In particular $1^n = 1$ for every n, by induction: $1^0 = 1$ and $1^{n+1} = 1^n \cdot 1 = 1$.

The binomial theorem rearranges sums term by term, and the rules it needs are collected in the next lemma. The sums start at $k = 0$; by the definition, $\sum_{k=0}^{0} a_k = 0 + a_0 = a_0$.

Lemma 2.6.1. Finite Sums in a Commutative Ring

Let R be a commutative ring, $n \in \mathbb{N}$, $c \in R$, and let $(a_k)_{k\in\mathbb{N}}$ and $(b_k)_{k\in\mathbb{N}}$ be sequences in R.

(a) $\sum_{k=0}^{n}(a_k + b_k) = \sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k$.
(b) $c\sum_{k=0}^{n} a_k = \sum_{k=0}^{n} c\,a_k$.
(c) $\sum_{k=0}^{n} m \cdot a_k = m \cdot \sum_{k=0}^{n} a_k$ for every $m \in \mathbb{Z}$.
(d) Let $j \in \mathbb{N}$, and suppose $a_k = 0$ for every $k \neq j$. Then $\sum_{k=0}^{n} a_k = a_j$ if $j \leq n$, and $\sum_{k=0}^{n} a_k = 0$ if $j > n$.
(e) $-\sum_{k=0}^{n} a_k = \sum_{k=0}^{n}(-a_k)$.
(f) *(Splitting off the first term.)* $\sum_{k=0}^{n+1} a_k = a_0 + \sum_{k=0}^{n} a_{k+1}$.

In words: a finite sum may be split termwise, multiplied termwise, and negated termwise; a sum with one non-zero term is that term; and the first term may be split off, the rest being re-indexed from 0. By the finite-lists remark, the lemma applies to finitely many terms $a_0, \ldots, a_n$ as well.

Idea. A sum up to $n+1$ is the sum up to n plus one term, so every rule that holds for one term and survives adding one more term holds for all sums: an induction on n whose step is a single axiom, (F1)–(F2) for (a), (F9) for (b), and associativity for (f). Parts (c) and (e) need no induction, because a multiple is a product, $m \cdot a = (m \cdot 1)a$, so they are (b) in disguise.

Proof. Each part is an induction on n (Logic and Proof, Axiom 4.2.1), splitting off the last term at the step, except (c) and (e), which follow from (b).

(a) For $n = 0$ both sides are $a_0 + b_0$. If (a) holds for n, then splitting off the last term,

$$\sum_{k=0}^{n+1}(a_k + b_k) = \Big(\sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k\Big) + (a_{n+1} + b_{n+1}),$$

which is $(\sum_{k=0}^{n} a_k + a_{n+1}) + (\sum_{k=0}^{n} b_k + b_{n+1})$ by (F1) and (F2), and that is the right side for $n+1$.

(b) For $n = 0$ both sides are ca_0. At the step, $c(\sum_{k=0}^{n} a_k + a_{n+1}) = c\sum_{k=0}^{n} a_k + ca_{n+1}$ by (F9), and the induction hypothesis rewrites the first term.

(c) By Lemma 2.5.1 (c), which holds for $m \in \mathbb{Z}$ by part (d) there, $m \cdot a_k = (m \cdot 1)a_k$ and $m \cdot \sum a_k = (m \cdot 1)\sum a_k$. So (c) is (b) with $c = m \cdot 1$.

(d) For $n = 0$: if $j = 0$ the sum is $a_0 = a_j$; if $j > 0$, then $0 \neq j$, so the sum is $a_0 = 0$. Suppose (d) holds for n, and split off a_{n+1}. If $j \leq n$, the sum up to n is a_j and $a_{n+1} = 0$ (as $n+1 \neq j$), so the total is a_j. If $j = n+1$, the sum up to n is 0 (as $j > n$) and the total is $0 + a_{n+1} = a_j$. If $j > n+1$, both parts are 0.

(e) By (c) with $m = -1$, since $(-1) \cdot x = -(1 \cdot x) = -x$ (Lemma 2.5.1 (d)).

(f) For $n = 0$ both sides are $a_0 + a_1$. If (f) holds for n, then

$$\sum_{k=0}^{n+2} a_k = \Big(a_0 + \sum_{k=0}^{n} a_{k+1}\Big) + a_{n+2} = a_0 + \sum_{k=0}^{n+1} a_{k+1},$$

by splitting off the last term, the induction hypothesis, (F2), and splitting off the last term of the sequence $(a_{k+1})_k$, whose term at $k = n+1$ is a_{n+2}. This proves the lemma.

■

2.6.2 Binomial coefficients

In $(x + y)^n$, each product $x^k y^{n-k}$ appears a certain number of times, and that number is the binomial coefficient. We define it by Pascal's rule, which is how the coefficients arise when $(x + y)^n$ is multiplied by $x + y$, and we never divide.

Definition 2.6.1. Binomial Coefficients

The **binomial coefficients** $\binom{n}{k} \in \mathbb{N}$, for $n, k \in \mathbb{N}$, are defined by recursion on n (Sets, Relations, and Cardinality, Theorem 2.3.1, with X the set of functions $\mathbb{N} \to \mathbb{N}$):

$$\binom{0}{0} := 1, \qquad \binom{0}{k} := 0 \quad (k \geq 1),$$
$$\binom{n+1}{0} := 1, \quad \binom{n+1}{k+1} := \binom{n}{k} + \binom{n}{k+1} \quad (k \in \mathbb{N}).$$

In words: row $n + 1$ starts with 1, and each later entry is the sum of the two entries of row n above it (**Pascal's rule**). Each row is a whole function $\mathbb{N} \to \mathbb{N}$, so the recursion has values for every k, and a coefficient is a natural number, never a quotient.

Three facts follow by one induction on n each.

- $\binom{n}{k} = 0$ for $k > n$. For $n = 0$ this is the definition. If it holds for n and $k > n + 1$, write $k = j + 1$ with $j > n$; then $\binom{n+1}{j+1} = \binom{n}{j} + \binom{n}{j+1} = 0 + 0$.
- $\binom{n}{n} = 1$. Indeed $\binom{0}{0} = 1$, and $\binom{n+1}{n+1} = \binom{n}{n} + \binom{n}{n+1} = 1 + 0$ by the first fact.
- $\binom{n}{1} = n$. Indeed $\binom{0}{1} = 0$, and $\binom{n+1}{1} = \binom{n}{0} + \binom{n}{1} = 1 + n$.

The rows $n = 0, \ldots, 6$, with the zeros for $k > n$ shown:

n	$k = 0$	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0
2	1	2	1	0	0	0	0
3	1	3	3	1	0	0	0
4	1	4	6	4	1	0	0
5	1	5	10	10	5	1	0
6	1	6	15	20	15	6	1

Remark. The formula $\binom{n}{k} \cdot k! \cdot (n-k)! = n!$ for $k \leq n$ is true, but we neither prove nor use it. The route below needs one identity between neighboring coefficients and avoids division altogether, which matters because in $\mathbb{F}_p$ the factorial $p!$ is 0.

The identity we need relates row $n+1$ to row n by a factor. It is what makes a prime divide the middle coefficients of row p.

Proposition 2.6.2. Absorption Identity

For all $n, k \in \mathbb{N}$,

$$(k+1)\binom{n+1}{k+1} = (n+1)\binom{n}{k}.$$

Idea. The definition is a recursion on n, so we induct on n, proving the statement for **all** k at once; the step then needs the hypothesis at two values of k. In the step, expand the left side by Pascal's rule, split the factor $k+2$ as $(k+1)+1$ in front of one of the two terms, apply the hypothesis twice, and recombine with Pascal's rule. For $n = 2$, $k = 0$ it reads $1 \cdot 3 = 3 \cdot 1$; for $n = 3$, $k = 1$, $2 \cdot 6 = 4 \cdot 3$.

Proof. We prove by induction on n (Logic and Proof, Axiom 4.2.1) the statement "for every $k \in \mathbb{N}$, $(k+1)\binom{n+1}{k+1} = (n+1)\binom{n}{k}$".

Base $n = 0$. For $k = 0$: $1 \cdot \binom{1}{1} = 1 = 1 \cdot \binom{0}{0}$. For $k \geq 1$: $\binom{1}{k+1} = 0$ since $k+1 > 1$, and $\binom{0}{k} = 0$; both sides are 0.

Step. Suppose the statement holds for n. For $k = 0$, the claim for $n+1$ reads $\binom{n+2}{1} = (n+2)\binom{n+1}{0}$, and both sides are $n+2$ by the facts above. For $k = j+1$ with $j \in \mathbb{N}$, Pascal's rule gives

$$\begin{aligned}
(j+2)\binom{n+2}{j+2} &= (j+2)\binom{n+1}{j+1} + (j+2)\binom{n+1}{j+2} \\
&= (j+1)\binom{n+1}{j+1} + \binom{n+1}{j+1} + (j+2)\binom{n+1}{j+2} \\
&= (n+1)\binom{n}{j} + \binom{n+1}{j+1} + (n+1)\binom{n}{j+1} \\
&= (n+1)\binom{n+1}{j+1} + \binom{n+1}{j+1} = (n+2)\binom{n+1}{j+1},
\end{aligned}$$

where the third line uses the hypothesis at $k = j$ and at $k = j+1$, and the fourth line Pascal's rule again. This is the claim for $n+1$ at $k = j+1$. This proves the proposition.

■

2.6.3 The binomial theorem

Expanding $(x+y)^n$ multiplies out n factors $x+y$ and collects the products $x^k y^{n-k}$. In a commutative ring this collecting is legitimate, and the counts are the binomial coefficients, acting as integer multiples.

Theorem 2.6.3. The Binomial Theorem in a Commutative Ring

Let R be a commutative ring, $x, y \in R$ and $n \in \mathbb{N}$. Then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot (x^k y^{n-k}).$$

Here $\binom{n}{k} \cdot z$ is the integer multiple of Section 2.5, and $n-k \in \mathbb{N}$ since $k \le n$.

Idea. Induct on n, with $(x+y)^{n+1} = (x+y)^n x + (x+y)^n y$. Multiplying the sum for $(x+y)^n$ by x raises every power of x by one, which shifts the coefficients one place to the right; multiplying by y leaves them in place. Adding the two rows entry by entry is exactly Pascal's rule. The work is in lining the two sums up over the same range $k = 0, \dots, n+1$: the shifted sum gets a zero first term, and the other one a zero last term.

Proof. Induction on n (Logic and Proof, Axiom 4.2.1). For $n = 0$, $(x+y)^0 = 1$ and the right side is $\binom{0}{0} \cdot (x^0 y^0) = 1 \cdot (1 \cdot 1) = 1$.

Suppose the formula holds for n, and put $t_k := \binom{n}{k} \cdot (x^k y^{n-k})$ for $0 \le k \le n$. By the power recursion, (F9) and Lemma 2.6.1 (b) with (F6),

$$(x+y)^{n+1} = (x+y)^n x + (x+y)^n y = \sum_{k=0}^{n} t_k x + \sum_{k=0}^{n} t_k y.$$

By the rule $(m \cdot a)b = m \cdot (ab)$ of Lemma 2.5.1 (d), with (F5), (F6) and the power recursion,

$$t_k x = \binom{n}{k} \cdot (x^{k+1} y^{n-k}), \qquad t_k y = \binom{n}{k} \cdot (x^k y^{n+1-k}).$$

For $0 \le k \le n+1$ let $z_k := x^k y^{n+1-k}$, and define

$$u_0 := 0, \quad u_k := \binom{n}{k-1} \cdot z_k \ (1 \le k \le n+1), \qquad w_k := \binom{n}{k} \cdot z_k \ (0 \le k \le n+1).$$

Then $t_k x = u_{k+1}$ and $t_k y = w_k$ for $0 \le k \le n$, and $w_{n+1} = 0 \cdot z_{n+1} = 0$, since $\binom{n}{n+1} = 0$. By Lemma 2.6.1 (f) and $u_0 = 0$, and by splitting off the last term $w_{n+1} = 0$,

$$\sum_{k=0}^{n} t_k x = \sum_{k=0}^{n+1} u_k, \qquad \sum_{k=0}^{n} t_k y = \sum_{k=0}^{n+1} w_k.$$

So $(x+y)^{n+1} = \sum_{k=0}^{n+1}(u_k + w_k)$ by Lemma 2.6.1 (a). Finally, $u_0 + w_0 = 0 + 1 \cdot z_0 = \binom{n+1}{0} \cdot z_0$, and for $k = j+1$ with $0 \le j \le n$, the sum rule of Lemma 2.5.1 (d) and Pascal's rule give

$$u_k + w_k = \binom{n}{j} \cdot z_k + \binom{n}{j+1} \cdot z_k = \binom{n+1}{j+1} \cdot z_k = \binom{n+1}{k} \cdot z_k.$$

Hence $(x+y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} \cdot (x^k y^{n+1-k})$, which is the formula for $n+1$. This proves the theorem.

■

The proof used (F6) at every regrouping of $x^k y^{n-k} x$, and the theorem needs it: the linear-algebra volumes meet matrices, whose multiplication is not commutative, and there the expansion holds only for pairs that commute. For $R = \mathbb{Z}$ the theorem is the familiar expansion, since there $m \cdot z = mz$ (Section 2.5).

In row 5 of the table, the four middle entries $5, 10, 10, 5$ are all multiples of 5; in row 6 the middle entries 15 and 20 are not multiples of 6. Primes are special.

Lemma 2.6.4. A Prime Divides the Middle Binomial Coefficients

Let p be a prime and $k \in \mathbb{N}$ with $0 < k < p$. Then $p \mid \binom{p}{k}$.

Proof. We read the coefficients in $\mathbb{N} \subseteq \mathbb{Z}$. By Proposition 2.6.2 with $n = p-1$ and $k-1$ in place of k,

$$k\binom{p}{k} = p\binom{p-1}{k-1},$$

so $p \mid k\binom{p}{k}$. Since $0 < k < p$, $p \nmid k$: a positive multiple of p is at least p (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e)). Hence $\gcd(p,k) = 1$ by Number Systems: From \(\nN\) to \(\nR\), Corollary 3.3.2 (a), and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.3.1 gives $p \mid \binom{p}{k}$. This proves the lemma.

■

The hypothesis "prime" is needed: $\binom{4}{2} = 6$, and $4 \nmid 6$. In the proof, $4 \mid 2\binom{4}{2}$, but $\gcd(4,2) = 2$, so Euclid's lemma does not apply.

Quick check. Use Proposition 2.6.2 to compute $\binom{7}{3}$ from $\binom{6}{2} = 15$, and check that 7 divides it.

Solution. With $n = 6$, $k = 2$: $3\binom{7}{3} = 7\binom{6}{2} = 7 \cdot 15 = 105$, so $\binom{7}{3} = 35$, and $35 = 5 \cdot 7$. (By Pascal's rule, $\binom{7}{3} = \binom{6}{2} + \binom{6}{3} = 15 + 20 = 35$, the same.)

2.6.4 The Frobenius map

We can now expand $(x+y)^p$ in a field of characteristic p.

Theorem 2.6.5. The Frobenius Homomorphism

Let F be a field of characteristic $p > 0$.

(a) For all $x, y \in F$,
$$(x+y)^p = x^p + y^p, \qquad (xy)^p = x^p y^p,$$
and $1^p = 1$. So the **Frobenius map** $\mathrm{Fr}\colon F \to F$, $\mathrm{Fr}(x) := x^p$, is a homomorphism, and it is injective.

(b) $(x-y)^p = x^p - y^p$ for all $x, y \in F$.

(c) If F is finite, then Fr is an automorphism of F.

By Theorem 2.5.3, the hypothesis $\operatorname{char} F = p > 0$ already makes p prime.

Try it first (ten minutes): expand $(x+y)^5$ and $(x+y)^6$ in $\mathbb{F}_5$, using the rows $n=5$ and $n=6$ of the table above, and see which coefficients survive.

Idea. For $(x+y)^5$ the coefficients $1,5,10,10,5,1$ become $1,0,0,0,0,1$ in $\mathbb{F}_5$, and $(x+y)^5 = x^5+y^5$. For $(x+y)^6$ the coefficients $1,6,15,20,15,6,1$ become $1,1,0,0,0,1,1$, and $(x+y)^6 = x^6+x^5y+xy^5+y^6$: the extra terms survive because 6 is not the characteristic. So the plan is: expand by the binomial theorem; every middle coefficient $\binom{p}{k}$ is a multiple of p; and a multiple of p acts on F as 0, because $p \cdot 1 = 0$. The product rule and $1^p = 1$ are power laws, and injectivity is free for a homomorphism of fields.

Before reading on: where is it used that p is prime?

Proof.

(a) By Theorem 2.6.3, $(x+y)^p = \sum_{k=0}^{p} t_k$ with $t_k := \binom{p}{k} \cdot (x^k y^{p-k})$. Let $0 < k < p$. By Lemma 2.6.4, $p \mid \binom{p}{k}$, so $\binom{p}{k} \cdot 1 = 0$ by Proposition 2.5.2 (a), and then, by Lemma 2.5.1 (c) and Theorem 2.1.1 (d),
$$t_k = \left(\binom{p}{k} \cdot 1\right)(x^k y^{p-k}) = 0 \cdot (x^k y^{p-k}) = 0.$$
The end terms are $t_0 = 1 \cdot (x^0 y^p) = y^p$ and $t_p = 1 \cdot (x^p y^0) = x^p$. Let $b_k := t_k$ for $k = 0$ and $b_k := 0$ otherwise, and $c_k := t_k$ for $k = p$ and $c_k := 0$ otherwise. Since $p \neq 0$, $t_k = b_k + c_k$ for every $0 \le k \le p$, so by Lemma 2.6.1 (a) and (d),
$$(x+y)^p = \sum_{k=0}^{p} b_k + \sum_{k=0}^{p} c_k = t_0 + t_p = y^p + x^p,$$
which is $x^p + y^p$ by (F1). Next, $(xy)^p = x^p y^p$ is the third power law of this section's opening paragraph (Sets, Relations, and Cardinality, Proposition 2.3.4 (c), read in F), and $1^p = 1$. So Fr is a homomorphism (Definition 2.4.1), and it is injective by Proposition 2.4.1 (c).

(b) By Proposition 2.4.1 (a), $\mathrm{Fr}(x-y) = \mathrm{Fr}(x) - \mathrm{Fr}(y)$.

(c) The image $\mathrm{Fr}(F)$ is a subset of F, and Fr, with codomain $\mathrm{Fr}(F)$, is a bijection $F \to \mathrm{Fr}(F)$ by (a). If $\mathrm{Fr}(F) \neq F$, this would be a bijection from the finite set F onto a proper subset, which Sets, Relations, and Cardinality, Theorem 3.1.9 forbids. So $\mathrm{Fr}(F) = F$, Fr is bijective, and a bijective homomorphism $F \to F$ is an automorphism (Definition 2.4.1). This proves the theorem.

■

Answer to the prompt. Primality is used in one place: Lemma 2.6.4, whose proof needs Euclid's lemma, and so needs p prime. It costs nothing here, since a positive characteristic is always prime (Theorem 2.5.3).

In words: in characteristic p, raising to the p-th power respects sums. The map is not the identity in general; Exercise C3 of Section 2.5 found that on the four-element field it exchanges two elements. On $\mathbb{F}_p$ itself it is the identity, and that is Fermat's little theorem.

Warning. "$(x+y)^n = x^n + y^n$" is not a general rule. In a field of characteristic $p > 0$ it holds for $n = p$ (Theorem 2.6.5 (a)), and so for $n = p^2$ by Exercise B2 (and in the same way for every power of p). With other exponents it can fail: in $\mathbb{F}_3$, $(1+1)^2 = 4 = 1$, while $1^2+1^2 = 2$. In a ring of composite characteristic it can fail even with n equal to the characteristic: in $\mathbb{Z}/4\mathbb{Z}$, which has characteristic 4, $([1]+[1])^4 = [16] = [0]$, while $[1]^4 + [1]^4 = [2]$; the middle coefficient $\binom{4}{2} = 6$ is not a multiple of 4. In $\mathbb{Z}$ the identity fails for every $n \geq 2$: $(1+1)^n = 2^n \neq 2$.

2.6.5 Fermat's little theorem

On $\mathbb{F}_p$, the Frobenius map is a homomorphism $\mathbb{F}_p \to \mathbb{F}_p$, and by Corollary 2.5.6 (b) there is only one such map, the identity. That is the whole proof of the first part below.

Theorem 2.6.6. Fermat's Little Theorem

Let p be a prime.

(a) $a^p = a$ for every $a \in \mathbb{F}_p$.

(b) $a^{p-1} = 1$ for every non-zero $a \in \mathbb{F}_p$; so $a^{-1} = a^{p-2}$.

(c) For every $a \in \mathbb{Z}$, $p \mid a^p - a$; and if $p \nmid a$, then $p \mid a^{p-1} - 1$.

Proof.

(a) $\mathrm{char}\,\mathbb{F}_p = p$ (Example (The characteristics of the standard fields)), so $\mathrm{Fr}\colon \mathbb{F}_p \to \mathbb{F}_p$ is a homomorphism by Theorem 2.6.5 (a). By Corollary 2.5.6 (b), the only homomorphism $\mathbb{F}_p \to \mathbb{F}_p$ is the identity. Hence $a^p = \mathrm{Fr}(a) = a$ for every $a \in \mathbb{F}_p$.

(b) Let $a \neq 0$. Since $p \geq 2$, $p-1 \in \mathbb{N}$ and $a \cdot a^{p-1} = a^{p-1}a = a^p = a = a \cdot 1$, by (F6), the power recursion and (a). Canceling $a \neq 0$ (Theorem 2.1.1 (b)) gives $a^{p-1} = 1$. Likewise $p-2 \in \mathbb{N}$ and $a \cdot a^{p-2} = a^{p-1} = 1$, so $a^{-1} = a^{p-2}$ by uniqueness of inverses (Theorem 2.1.1 (c)).

(c) Write $[a]$ for the class of $a \in \mathbb{Z}$ in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Since $[a][b] = [ab]$ (Number Systems:

From \(\nN\) to \(\nR\), Theorem 3.4.1 (b)), induction on n gives $[a]^n = [a^n]$ for every $n \in \mathbb{N}$: $[a]^0 = [1] = [a^0]$, and $[a]^{n+1} = [a]^n[a] = [a^n][a] = [a^{n+1}]$. By (a), $[a^p] = [a]^p = [a]$, so $p \mid a^p - a$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (a), for the ideal $p\mathbb{Z}$). If $p \nmid a$, then $[a] \neq [0]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (d)), so $[a^{p-1}] = [a]^{p-1} = [1]$ by (b), and $p \mid a^{p-1} - 1$. This proves the theorem.

■

Primality is needed in (c). For the modulus 4 and $a = 2$, $2^4 - 2 = 14$ is not a multiple of 4 (in $\mathbb{Z}/4\mathbb{Z}$ this is $([1] + [1])^4 = [0] \neq [2]$, from the warning above), and although $4 \nmid 2$, $2^3 - 1 = 7$ is not a multiple of 4 either.

Part (b) gives a second way to invert in $\mathbb{F}_p$, besides the Euclidean algorithm of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 3: $a^{-1} = a^{p-2}$. It also reduces large exponents: for non-zero a, only the remainder of the exponent on division by $p - 1$ matters, since $a^{q(p-1)+r} = (a^{p-1})^q a^r = a^r$. Exercise C2 below gives a second proof of (a), by induction, and Chapter 4 gives another proof of (b), from a product of all the non-zero elements.

Example. Powers and inverses in prime fields

(i) Compute 3^{100} in $\mathbb{F}_7$.

(ii) Compute 2^{100} in $\mathbb{F}_{101}$.

(iii) Find the inverse of 7 in $\mathbb{F}_{31}$ twice: by Theorem 2.6.6 (b), and by the Euclidean algorithm.

(iv) What is the Frobenius map of $\mathbb{F}_p$?

Solution.

(i) 7 is prime (the small-primes remark of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Section 3.1) and $3 \neq 0$ in $\mathbb{F}_7$, so $3^6 = 1$ by Theorem 2.6.6 (b). Since $100 = 16 \cdot 6 + 4$, the power laws give $3^{100} = (3^6)^{16}\, 3^4 = 1 \cdot 81$, and $81 = 11 \cdot 7 + 4$. So $3^{100} = 4$ in $\mathbb{F}_7$.

(ii) 101 is prime: by the remark after Number Systems: From \(\nN\) to \(\nR\), Lemma 3.3.4 it suffices that no d with $2 \leq d$ and $d \cdot d \leq 101$, that is $2 \leq d \leq 10$, divides 101, and the remainders of 101 on division by $2, 3, \ldots, 10$ are $1, 2, 1, 1, 5, 3, 5, 2, 1$. Since $2 \neq 0$ in $\mathbb{F}_{101}$, Theorem 2.6.6 (b) gives $2^{100} = 2^{101-1} = 1$. No multiplication was needed.

(iii) 31 is prime by the same test ($d = 2, 3, 4, 5$ leave remainders $1, 1, 3, 1$). *By Fermat:* since $7 \neq 0$ in $\mathbb{F}_{31}$, Theorem 2.6.6 (b) gives $7^{-1} = 7^{29}$. Square repeatedly in $\mathbb{F}_{31}$: $7^2 = 49 = 18$, $7^4 = 18^2 = 324 = 14$, $7^8 = 14^2 = 196 = 10$, $7^{16} = 10^2 = 100 = 7$. With $29 = 16 + 8 + 4 + 1$,

$$7^{29} = 7^{16}\, 7^8\, 7^4\, 7 = 7 \cdot 10 \cdot 14 \cdot 7 = 70 \cdot 98 = 8 \cdot 5 = 40 = 9.$$

By Euclid: $31 = 4 \cdot 7 + 3$ and $7 = 2 \cdot 3 + 1$, so

$$1 = 7 - 2 \cdot 3 = 7 - 2(31 - 4 \cdot 7) = 9 \cdot 7 - 2 \cdot 31,$$

and $7^{-1} = 9$ by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1. Both

routes give 9. Check: $7 \cdot 9 = 63 = 2 \cdot 31 + 1$. For small p the Euclidean algorithm is shorter; Fermat's route needs no back-substitution, only squaring.

(iv) The identity, by Theorem 2.6.6 (a): $\mathrm{Fr}(a) = a^p = a$ for every $a \in \mathbb{F}_p$.

Quick check. Compute 2^6 in $\mathbb{F}_7$ and 3^{10} in $\mathbb{F}_{11}$, with and without Theorem 2.6.6.

Solution. Both are 1. Without it: $2^6 = 64 = 9 \cdot 7 + 1$; and $3^5 = 243 = 22 \cdot 11 + 1$, so $3^{10} = (3^5)^2 = 1$. With it: 7 and 11 are prime, $2 \neq 0$ in $\mathbb{F}_7$ and $3 \neq 0$ in $\mathbb{F}_{11}$, and the exponents are $7 - 1$ and $11 - 1$.

2.6.6 Exercises

2.6.6.1 A. Check your understanding

Exercise. A1

These parts are about Theorem 2.6.5 and its proof.

(a) Where in the proof of (a) is it used that p is prime, and why does the theorem not need "p prime" as a separate hypothesis?

(b) List $\binom{5}{k}$ for $0 \leq k \leq 5$ and $\binom{6}{k}$ for $0 \leq k \leq 6$. Which are divisible by 5, and which by 6?

(c) Why is Fr injective? Does the proof use that F is finite?

(d) State the idea of the proof of (a) in two sentences.

Solution.

(a) In Lemma 2.6.4, through Euclid's lemma: $p \mid k\binom{p}{k}$ gives $p \mid \binom{p}{k}$ only because $\gcd(p, k) = 1$, which needs p prime. A positive characteristic is always prime (Theorem 2.5.3), so "$\mathrm{char}\, F = p > 0$" already includes it.

(b) Row 5: $1, 5, 10, 10, 5, 1$; the four middle ones are divisible by 5, the end ones are not. Row 6: $1, 6, 15, 20, 15, 6, 1$; only the two 6's are divisible by 6, and 15, 20 are not. This is why $(x + y)^6 \neq x^6 + y^6$ in a ring of characteristic 6 such as $\mathbb{Z}/6\mathbb{Z}$.

(c) Every homomorphism of fields is injective (Proposition 2.4.1 (c)): $\mathrm{Fr}(a) = 0$ only for $a = 0$. The proof of injectivity does not use finiteness; finiteness is used only for surjectivity in (c).

(d) Expand $(x + y)^p$ by the binomial theorem; every middle coefficient $\binom{p}{k}$ is a multiple of p. In characteristic p, $p \cdot 1 = 0$, so every middle term vanishes and only $x^p + y^p$ remains.

2.6.6.2 B. Practice

Exercise. B1

Compute 5^{38} in $\mathbb{F}_{13}$, and find the inverse of 5 in $\mathbb{F}_{13}$ by Theorem 2.6.6.

Solution. 13 is prime (no d with $2 \le d \le 3$ divides it, and $4 \cdot 4 > 13$; the remark after Number Systems: From \(\nN\) to \(\nR\), Lemma 3.3.4), and $5 \neq 0$ in $\mathbb{F}_{13}$. By Theorem 2.6.6 (b), $5^{12} = 1$. Since $38 = 3 \cdot 12 + 2$, $5^{38} = (5^{12})^3 5^2 = 25 = 12$ in $\mathbb{F}_{13}$. For the inverse, $5^{-1} = 5^{11}$. Now $5^2 = 12 = -1$, so $5^{10} = (5^2)^5 = (-1)^5 = -1$ and $5^{11} = -5 = 8$. Check: $5 \cdot 8 = 40 = 3 \cdot 13 + 1$. Hence $5^{38} = 12$ and $5^{-1} = 8$.

Exercise. B2

Let F be a field of characteristic $p > 0$.

(a) Show that $(x + y)^{p^2} = x^{p^2} + y^{p^2}$ for all $x, y \in F$.

(b) Show that $\left(\sum_{i=1}^{m} x_i\right)^p = \sum_{i=1}^{m} x_i^p$ for all $m \in \mathbb{N}$ and $x_1, \ldots, x_m \in F$.

Solution.

(a) $\mathrm{Fr} \circ \mathrm{Fr}$ is a homomorphism, as a composite of homomorphisms (Proposition 2.4.1 (e)), and $(\mathrm{Fr} \circ \mathrm{Fr})(x) = (x^p)^p = x^{p^2}$ by the power law $(x^m)^n = x^{mn}$. Applying its additivity to $x + y$ gives the claim.

(b) Induction on m. For $m = 0$ both sides are 0: the empty sum is 0, and $0^p = 0^{p-1} \cdot 0 = 0$ as $p \ge 1$. If the claim holds for m, split off the last term and use Theorem 2.6.5 (a):

$$\Big(\sum_{i=1}^{m+1} x_i\Big)^p = \Big(\sum_{i=1}^{m} x_i + x_{m+1}\Big)^p = \Big(\sum_{i=1}^{m} x_i\Big)^p + x_{m+1}^p = \sum_{i=1}^{m+1} x_i^p.$$

Exercise. B3

Let p be a prime. Show that the solutions $x \in \mathbb{F}_p$ of $x^{p-1} = 1$ are exactly the non-zero elements, and that every $a \in \mathbb{F}_p$ satisfies $a^p - a = 0$.

Solution. Every non-zero a satisfies $a^{p-1} = 1$ by Theorem 2.6.6 (b). The element 0 does not: since $p - 1 \ge 1$, $0^{p-1} = 0^{p-2} \cdot 0 = 0 \neq 1$. So the solutions are exactly the non-zero elements. And $a^p - a = a - a = 0$ for every a by Theorem 2.6.6 (a).

2.6.6.3 C. Going deeper

Exercise. C1: Exit check: the Frobenius identity

Let F be a field of characteristic $p > 0$. Using Theorem 2.6.3 and Lemma 2.6.4, prove that $\mathrm{Fr}\colon F \to F$, $x \mapsto x^p$, is an injective homomorphism.

Solution. Sums. By Theorem 2.6.3, $(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot (x^k y^{p-k})$. For $0 < k < p$, $\binom{p}{k} \cdot (x^k y^{p-k}) = (\binom{p}{k} \cdot 1)(x^k y^{p-k})$ by Lemma 2.5.1 (c). By Lemma 2.6.4, $p \mid \binom{p}{k}$, and since $\operatorname{char} F = p$, $\binom{p}{k} \cdot 1 = 0$ (Proposition 2.5.2 (a)); so the term is 0 (Theorem 2.1.1 (d)). The terms $k = 0$ and $k = p$ are $1 \cdot y^p = y^p$ and $1 \cdot x^p = x^p$, since $\binom{p}{0} = \binom{p}{p} = 1$ and $x^0 = y^0 = 1$.

A sum whose terms vanish except at two places is the sum of those two terms (Lemma 2.6.1 (a), (d)), so $(x+y)^p = x^p + y^p$.

Products and one. $(xy)^p = x^p y^p$ by the power law $(xy)^n = x^n y^n$, and $1^p = 1$. So Fr is a homomorphism (Definition 2.4.1).

Injective. Every homomorphism of fields is injective (Proposition 2.4.1 (c)).

Marking scheme. (10 points)

- 2: the binomial expansion written with integer multiples $\binom{p}{k} \cdot (x^k y^{p-k})$.
- 2: each middle term reduced to a multiple that vanishes, with the rule named (for example $(\binom{p}{k} \cdot 1)(x^k y^{p-k})$ by $(m \cdot 1)a = m \cdot a$, or $\binom{p}{k} \cdot z = q \cdot (p \cdot z)$ where $\binom{p}{k} = qp$).
- 2: that multiple is 0 from $p \mid \binom{p}{k}$ and $\operatorname{char} F = p$, with both reasons named.
- 1: the end terms y^p and x^p.
- 1: $(xy)^p = x^p y^p$ and $1^p = 1$.
- 2: injectivity, by Proposition 2.4.1 (c) or by any correct direct argument.

Second route for injectivity: $x^p = y^p \Rightarrow (x-y)^p = 0 \Rightarrow x = y$ earns the 2 points, 1 for $(x-y)^p = x^p - y^p$ with its reason (Proposition 2.4.1 (a), or $(-y)^p = -y^p$ for every prime p, the even one included), and 1 for $x - y = 0$ because a field has no zero divisors.

Fatal errors (0 for the step): "$\binom{p}{k} = 0$" as an integer; using $(x+y)^p = x^p + y^p$ in its own proof.

Exercise. C2: Fermat by induction

Let p be a prime. Give another proof of Theorem 2.6.6 (a) and of the first claim of Theorem 2.6.6 (c), without Corollary 2.5.6. In (a) use only Theorem 2.6.5 (a) (with $\operatorname{char} \mathbb{F}_p = p$, Example (The characteristics of the standard fields)) and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b), (d); in (b) you may also use Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1.

(a) prove by induction on $r \in \mathbb{N}$ that $(r \cdot 1)^p = r \cdot 1$ in $\mathbb{F}_p$, and deduce $a^p = a$ for every $a \in \mathbb{F}_p$;

(b) deduce that $p \mid a^p - a$ for every integer a.

Solution.

(a) For $r = 0$: $(0 \cdot 1)^p = 0^p = 0^{p-1} \cdot 0 = 0 = 0 \cdot 1$, as $p \geq 1$. If $(r \cdot 1)^p = r \cdot 1$, then by Theorem 2.6.5 (a) ($\operatorname{char} \mathbb{F}_p = p$, Example (The characteristics of the standard fields)),

$$((r+1) \cdot 1)^p = (r \cdot 1 + 1)^p = (r \cdot 1)^p + 1^p = r \cdot 1 + 1 = (r+1) \cdot 1.$$

Every element of $\mathbb{F}_p$ is $[r]$ for some $r \in \{0, \ldots, p-1\}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)), and $[r] = r \cdot [1]$ (part (d) there). So $a^p = a$ for every $a \in \mathbb{F}_p$.

(b) Let $a \in \mathbb{Z}$. Then $[a] \in \mathbb{F}_p$, so $[a]^p = [a]$ by (a). By induction on n, $[a]^n = [a^n]$, using $[a][b] = [ab]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (b)), as in the proof of Theorem 2.6.6 (c). So $[a^p] = [a]$, and $p \mid a^p - a$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (a), for the ideal $p\mathbb{Z}$). (This proves only what

Theorem 2.6.6 already gives; it is practice with the Frobenius identity, and nothing cites it.)

Exercise. C3: Roots of order p

Let F be a finite field of characteristic p. Show that for every $a \in F$ the equation $x^p = a$ has **exactly one** solution $x \in F$. Deduce that in $\mathbb{F}_p$, the only solution of $x^p = a$ is $x = a$.

Solution. By Corollary 2.5.7 (a), p is a prime, so $p > 0$, and by Theorem 2.6.5 (c), Fr is a bijection $F \to F$. Surjectivity gives a solution of $\mathrm{Fr}(x) = a$, and injectivity says there is at most one. In $\mathbb{F}_p$, $x = a$ is a solution by Theorem 2.6.6 (a), $a^p = a$, so it is the only one. The uniqueness half needs only that Fr is injective, so it holds in every field of characteristic $p > 0$ (Theorem 2.6.5 (a)); existence used the finiteness of F.

2.6.6.4 R. Review

Exercise. R1

Find all $z \in \mathbb{C}$ with $z^2 = -3 + 4i$, and explain why there are exactly two.

Solution. By the square-root formula of Proposition 1.4.1, with $a = -3$, $b = 4$: $r = |-3 + 4i| = 5$ (since $9 + 16 = 25$), $(r + a)/2 = 1$, $(r - a)/2 = 4$, and $b > 0$, so $w = 1 + 2i$. Check: $(1 + 2i)^2 = 1 + 4i + 4i^2 = -3 + 4i$. By Corollary 2.1.2 in the field $\mathbb{C}$ (Example (The Fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$)), $z^2 = w^2$ if and only if $z = w$ or $z = -w$. So the solutions are $1 + 2i$ and $-1 - 2i$. They are two, not one: $w = -w$ would give $2w = 0$, hence $w = 0$, since $2 \neq 0$ in $\mathbb{C}$ ($\mathrm{char}\,\mathbb{C} = 0$, Example (The characteristics of the standard fields), with Proposition 2.5.2 (b)).

Exercise. R2

Show that 7 has no square root in $\mathbb{Q}(\sqrt{2})$.

Solution. Suppose $(a + b\sqrt{2})^2 = 7$ with $a, b \in \mathbb{Q}$. Expanding, $(a^2 + 2b^2) + 2ab\sqrt{2} = 7 + 0\sqrt{2}$, so by unique representation (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.4.5 (a)), $2ab = 0$ and $a^2 + 2b^2 = 7$. Since $2 \neq 0$ in $\mathbb{Q}$ ($\mathrm{char}\,\mathbb{Q} = 0$, Example (The characteristics of the standard fields), with Proposition 2.5.2 (b)), Theorem 2.1.1 (f) applied twice (to $2 \cdot (ab) = 0$, then to $ab = 0$) gives $a = 0$ or $b = 0$. If $b = 0$, then $a^2 = 7$. If $a = 0$, then $2b^2 = 7$, so $(2b)^2 = 14$. Both are excluded by the claim stated with Number Systems: From \(\nN\) to \(\nR\), Proposition 6.4.6: no natural number n with $k^2 < n < (k + 1)^2$ for some $k \in \mathbb{N}$ is the square of a rational; take $(n, k) = (7, 2)$, as $4 < 7 < 9$, and $(n, k) = (14, 3)$, as $9 < 14 < 16$. So 7 has no square root in $\mathbb{Q}(\sqrt{2})$. This is the method of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 6, which showed the same for 3.

Exercise. R3

Show that no relation $<$ makes $\mathbb{Q}(i)$ (Example (Rational and Integer Complex Numbers)) an ordered field, and none makes the four-element field F of Exercise C1 of Section 2.2 an ordered field.

Solution. F. In F, $1+1=(1+1)+(0+0)\alpha=0$, by the definition of the sum, with coefficients in $\mathbb{F}_2$. So $2\cdot 1=0$ and $\operatorname{char} F\neq 0$, while every ordered field has characteristic 0 (Example (The characteristics of the standard fields)). This is the method of Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (e) and Number Systems: From \(\nN\) to \(\nR\), Example (A field with two elements that cannot be ordered): in an ordered field $n\cdot 1>0$ for $n\geq 1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h)), while here $2\cdot 1=0$.

$\mathbb{Q}(i)$. This is the method of Proposition 1.4.3; the proposition itself does not apply, since an order on the subfield $\mathbb{Q}(i)$ need not extend to $\mathbb{C}$. Suppose $<$ made $\mathbb{Q}(i)$ an ordered field. Then $i\neq 0$ gives $i^2>0$, and $1\neq 0$ gives $1>0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)). But $i^2=-1$ (Proposition 1.1.1; the operations of $\mathbb{Q}(i)$ are those of $\mathbb{C}$), and $1>0$ gives $-1<0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (a)). So $0<-1<0$, and $0<0$ by transitivity, which is impossible for the strict part of an order. The characteristic does not help here, since $\operatorname{char}\mathbb{Q}(i)=0$ (Example (The characteristics of the standard fields)): the obstruction for $\mathbb{Q}(i)$ is a square, not a multiple of 1.

Exercise. R4

Find all homomorphisms $\mathbb{Q}(\sqrt{2})\to\mathbb{R}$.

Solution. There are exactly two: the inclusion $a+b\sqrt{2}\mapsto a+b\sqrt{2}$, and $a+b\sqrt{2}\mapsto a-b\sqrt{2}$.

Every homomorphism is one of them. Let $\sigma\colon\mathbb{Q}(\sqrt{2})\to\mathbb{R}$ be a homomorphism. The inclusions $\mathbb{Q}\to\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}\to\mathbb{R}$ are homomorphisms (Example (Conjugation and Other Automorphisms) (ii); $\mathbb{Q}$ is a subfield of both), so they are $\iota_{\mathbb{Q}(\sqrt{2})}$ and $\iota_{\mathbb{R}}$ by the uniqueness clause of Theorem 2.5.5 (b) (both fields have characteristic 0, Example (The characteristics of the standard fields)). By Corollary 2.5.6 (a), $\sigma\circ\iota_{\mathbb{Q}(\sqrt{2})}=\iota_{\mathbb{R}}$: $\sigma(q)=q$ for every $q\in\mathbb{Q}$. Then

$$\sigma(\sqrt{2})^2=\sigma((\sqrt{2})^2)=\sigma(2)=2=(\sqrt{2})^2,$$

so $\sigma(\sqrt{2})=\sqrt{2}$ or $\sigma(\sqrt{2})=-\sqrt{2}$ by Corollary 2.1.2 in $\mathbb{R}$. Hence $\sigma(a+b\sqrt{2})=\sigma(a)+\sigma(b)\sigma(\sqrt{2})=a\pm b\sqrt{2}$.

Both occur. The inclusion is a homomorphism (Example (Conjugation and Other Automorphisms) (ii)), and so is conjugation $a+b\sqrt{2}\mapsto a-b\sqrt{2}$ of $\mathbb{Q}(\sqrt{2})$ followed by the inclusion (Example (Conjugation and Other Automorphisms) (iii) and Proposition 2.4.1 (e)). They differ at $\sqrt{2}$, since $\sqrt{2}>0>-\sqrt{2}$.

The tool, and the look-alikes. The tool is rigidity on the prime subfield (Corollary 2.5.6) followed by "push the equation $x^2=2$ through σ". The uniqueness theorem for complete ordered fields of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 6 (Number Systems: From \(\nN\) to \(\nR\), Theorem 6.3.4) does not apply: it concerns maps of a complete ordered field to

itself, and $\mathbb{Q}(\sqrt{2})$ is not complete. Nor does "a homomorphism into an ordered field preserves order": the second homomorphism sends $\sqrt{2} > 0$ to $-\sqrt{2} < 0$.

Chapter 3

Groups, Subgroups, and Homomorphisms

The same four rules keep turning up. Add integers, multiply non-zero rationals, multiply the units of $\mathbb{Z}/12\mathbb{Z}$, compose the bijections of a set: in each case two elements combine to give an element of the same set, the combining is associative, one element changes nothing, and every element can be undone. This chapter names that pattern a **group** and proves its basic laws once, from three axioms, so that they hold in all four cases and in every later one. It then makes two habits honest that school algebra uses without comment: dropping the brackets from a product of many factors, and writing powers g^n for every integer n, negative ones included. One warning runs through the whole chapter: a group need not be abelian, so no factor may be moved past another unless a hypothesis allows it.

After the structure come its substructures, the subgroups, and its maps, the homomorphisms. The subgroups of $(\mathbb{Z}, +)$ turn out to be exactly the sets $n\mathbb{Z}$, by the move that gave greatest common divisors in *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3. A homomorphism sends products to products, and its kernel, the set of elements it sends to the identity, measures how much it forgets. The chapter ends with one group studied in detail, the permutations of $\{1, \dots, n\}$, on which every determinant in linear algebra is built. Every permutation breaks into disjoint cycles, and every one, for $n \geq 2$, is a product of swaps of two points. Different words for the same permutation can use different numbers of swaps; that the parity of the number never changes is the theorem on the sign of a permutation, which later volumes prove.

A language more than a subject. Linear algebra and algebra both speak of groups, and this chapter supplies the vocabulary and the few facts they use constantly. Much of group theory is deliberately left out, and each omission is named once, where it would come up, as a pointer and never as a claim. Cyclic groups and the least $m \geq 1$ with $g^m = e$ are studied in *Groups*, the chapter "Cyclic Groups" (Section 3.2 points there). Cosets and Lagrange's theorem are in its chapter "Cosets and Lagrange's Theorem" (Section 3.3, Exercise C2, and review exercise R4 of Section 3.5). The uniqueness of the disjoint cycle decomposition, conjugacy in S_n and the sign of a permutation are in its chapter "Symmetric Groups and the Sign of a Permutation" (Sections 3.4 and 3.5), and the sign is also proved in *Determinants and the Structure of Operators*, the chapter "Determinants". Quotient groups and the isomorphism theorems are in the chapter "Normal Subgroups, Quotient Groups, and the Isomorphism Theorems" of *Groups* (the closing remark of Section 3.3). Nothing in this chapter depends on any of them.

What you need. *Sets, Relations, and Cardinality*, Chapter 1 (functions, composition, bijections and inverses), Chapter 2 (induction from any base and the recursion theorem, with

equivalence relations for one exercise) and Section 3.1 (finite sets); *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2 (commutative rings and $\mathbb{Z}$) and Chapter 3 (division with remainder, $\mathbb{Z}/n\mathbb{Z}$ and units); induction from *Logic and Proof*, Chapter 3. Throughout, $\mathbb{N}$ is ω and $\mathbb{Z}$, $\mathbb{Q}$ are the integers and rationals of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2, and results of the first two volumes about $\mathbb{N}$ are read on ω through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3, from its Chapter 1, as that volume does.

- From *Sets, Relations, and Cardinality*, Chapter 1: functions, Cartesian products, composition and its associativity, equality of functions, the empty function, and the theorem that a composite of bijections is a bijection (Sets, Relations, and Cardinality, Definition 1.4.1, Sets, Relations, and Cardinality, Definition 1.3.2, Sets, Relations, and Cardinality, Definition 1.4.2, Sets, Relations, and Cardinality, Proposition 1.4.3, Sets, Relations, and Cardinality, Proposition 1.4.1, Sets, Relations, and Cardinality, Proposition 1.4.2, Sets, Relations, and Cardinality, Theorem 1.4.4), which make the bijections of a set a group and S_0 the trivial group; inverse functions, the uniqueness of inverses, and bijections as the invertible functions (Sets, Relations, and Cardinality, Definition 1.5.2, Sets, Relations, and Cardinality, Proposition 1.5.3, Sets, Relations, and Cardinality, Theorem 1.5.4), whose argument Section 3.1 repeats with functions erased; images (Sets, Relations, and Cardinality, Definition 1.6.1), for the image of a homomorphism; intersections of families (Sets, Relations, and Cardinality, Definition 1.2.4), for intersections of subgroups.
- From *Sets, Relations, and Cardinality*, Chapter 2: induction from a base other than 0 (Sets, Relations, and Cardinality, Theorem 2.2.1), in Section 3.5; the recursion theorem, with its finite sums and products as the pattern for products of lists in a group and for $n!$ (Sets, Relations, and Cardinality, Theorem 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.1), in Sections 3.1 and 3.4; equivalence relations and their classes (Sets, Relations, and Cardinality, Definition 2.5.1, Sets, Relations, and Cardinality, Theorem 2.5.1), in review exercise R4 of Section 3.5. From its Chapter 3: finite sets, subsets and disjoint unions of finite sets, the pigeonhole principle, and the uniqueness of size (Sets, Relations, and Cardinality, Definition 3.1.2, Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations, and Cardinality, Proposition 3.1.5, Sets, Relations, and Cardinality, Corollary 3.1.3, Sets, Relations, and Cardinality, Corollary 3.1.4), for counting S_n, for the decomposition into cycles, and in exercises; a finite set has no proper subset of the same size (Sets, Relations, and Cardinality, Theorem 3.1.9), in review exercise R3.
- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2: commutative rings and fields and their algebra (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2), whose additive clauses are the group axioms for $(R, +)$; $\mathbb{Z}$ as an ordered commutative ring with a least element in every non-empty set bounded below (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.4, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6); every integer as n or $-n$ with $n \in \mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3), which defines negative powers; the multiples $n \cdot a$ of the "Multiples" paragraph of its Section 2.3, which Section 3.1 shows to be the multiples of the group $(R, +)$; and $\mathbb{Q}$ as an ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3, Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1), with the rule that the reciprocal of a positive element of an ordered field is positive (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.5.2), used for $\mathbb{Q}_{>0}$ in Sections 3.1 and 3.2 and for $\mathbb{R}_{>0}$ in Section 3.3.
- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3: division with remainder, the rules for divisibility, and parity (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1, Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3); integer linear combinations and Bézout's identity (Number

Systems: From \(\nN\) to \(\nR\), Definition 3.2.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.2.1, Number Systems: From \(\nN\) to \(\nR\), Corollary 3.2.2), whose proof is the model for the subgroups of $\mathbb{Z}$ and which Section 3.2's Exercise B3 recovers; ideals, quotient rings and the rings $\mathbb{Z}/n\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1, Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3, Number Systems: From \(\nN\) to \(\nR\), Example (Multiplication modulo six and modulo five)), the first finite groups of the chapter; the principal ideals of $\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.2), compared with in Section 3.2; and units, the units of $\mathbb{Z}/n\mathbb{Z}$, the field $\mathbb{Z}/p\mathbb{Z}$ and the Chinese remainder map (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3). Section 3.1 also uses the prime factorization (Number Systems: From \(\nN\) to \(\nR\), Definition 3.3.1) as a second instance of the recursion pattern, and Section 3.2's Exercise C3 recovers Number Systems: From \(\nN\) to \(\nR\), Exercise (B2: The least common multiple).

- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 5, in examples only: $\mathbb{R}$ as an ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.3.3), for the groups $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$.
- From *Logic and Proof*: induction and strong induction (Logic and Proof, Axiom 4.2.1, Logic and Proof, Theorem 4.2.2), from Section 3.2; and, for the two find-the-error exercises (Exercise C2 of Sections 3.1 and 3.5), the catalogue of moves that are not allowed (Logic and Proof, Example (What is not allowed)), from Section 5.6.
- From Chapter 1, in examples only: the complex numbers as a field, $i^2 = -1$ with $\mathbb{R}$ identified inside $\mathbb{C}$, the modulus and its product rule, the unit circle $\mathbb{T}$ and the roots of unity μ_n (Definition 1.1.1, Proposition 1.1.1, Theorem 1.2.4, Definition 1.2.1, Theorem 1.2.2, Proposition 1.5.1, Example (Roots of Unity)), for the subgroups $\mathbb{T}$ and μ_n of $\mathbb{C} \setminus \{0\}$ in Section 3.2 and the modulus as a homomorphism in Section 3.3.
- From Chapter 2, in examples, remarks and review exercise R1 only: fields (Definition 2.1.1) and the rule that a product of non-zero elements is non-zero (Theorem 2.1.1); integer multiples in a commutative ring (Lemma 2.5.1), compared with the group multiples in a second-reading fold of Section 3.1; field homomorphisms (Definition 2.4.1, Proposition 2.4.1), in the closing remark of Section 3.3; and the characteristic (Definition 2.5.1, Theorem 2.5.3), which review exercise R1 of Section 3.5 reaches again through the subgroups of $\mathbb{Z}$.

No proof of a result of this chapter uses $\mathbb{R}$, $\mathbb{C}$ or Chapter 2. The chapter also pays two debts of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3: its Exercise C2 of Section 3.4 becomes a theorem here (Theorem 3.2.4), and its remark that the units of a commutative ring form a group is proved in Section 3.1 (Proposition 3.1.4). Chapter 4 returns to groups and homomorphisms in its review exercise R1.

Time. About 25 hours on the core track (all of A, one B and one C per section, the exit checks); about 35 hours for everything.

3.0.1 Roadmap

- **Groups.** Four familiar situations with the same three rules; groups, abelian groups and additive notation; $(R, +)$ for a commutative ring, $F \setminus \{0\}$ for a field, the bijections of a set, the trivial group and the rotations of a square, with non-examples and the warning to check closure first; the basic laws, the uniqueness of the identity and of inverses, $(ab)^{-1} = b^{-1}a^{-1}$, cancellation and the unique solution of $ax = b$, proved once; products of lists by

recursion and the laws that let us drop brackets; integer powers and the power laws, with $(gh)^n = g^n h^n$ only when $gh = hg$; and the units $R^\times$ of a commutative ring as an abelian group, with $\mathbb{Z}^\times$, $(\mathbb{Z}/n\mathbb{Z})^\times$ and $F^\times$.

- **Subgroups and the Subgroups of the Integers.** Subgroups and the one-condition subgroup test; examples from $\mathbb{Z}$, $\mathbb{Q}\setminus\{0\}$, $\mathbb{Z}/6\mathbb{Z}$, $(\mathbb{Z}/8\mathbb{Z})^\times$, the bijections fixing a point, and $\mathbb{T}$ and μ_n inside $\mathbb{C}\setminus\{0\}$, with minimal-change non-examples; intersections of subgroups, and a union that is not one; the subgroup $\langle g\rangle$ generated by one element, the smallest subgroup containing g, listed explicitly when some $g^m = e$; and the theorem that the subgroups of $(\mathbb{Z}, +)$ are exactly the sets $n\mathbb{Z}$, each for exactly one $n \in \mathbb{N}$, with exercises recovering Bézout's identity and the least common multiple.
- **Homomorphisms and Isomorphisms.** Two tables that differ only in names; homomorphisms, isomorphisms and kernels, with no clause for the identity, which follows; the product of two groups; examples $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto g^k$, conjugation, squaring in an abelian group, the Chinese remainder map and the modulus, and the non-example $x \mapsto x + 1$; identities, inverses and powers preserved, kernels and images subgroups; composites and inverses of homomorphisms, so that $\cong$ behaves like equality; injective exactly when the kernel is trivial; isomorphic and non-isomorphic small groups, with the warning that the same number of elements decides nothing; and a remark on where homomorphisms go next.
- **Permutations and Cycle Notation.** The symmetric groups S_X and S_n, the support, two-line notation and products read right to left; cycles and transpositions, computing with them, S_n not abelian for $n \geq 3$, and two warnings, on the order of reading and on $(\sigma\tau)^2 \neq \sigma^2\tau^2$; the permutations of $n + 1$ points fixing the last one as a copy of S_n, and $|S_n| = n!$; disjoint permutations commute; and every permutation a product of disjoint cycles, by following the orbit of a moved point and peeling off the cycle found, with a worked run and exercises on the table of S_3, the number of k-cycles, the rotations of a square and powers of disjoint cycles.
- **Transpositions Generate the Symmetric Group.** A k-cycle as a product of $k - 1$ transpositions; every permutation of $n \geq 2$ points a product of transpositions, proved by fixing the last point and inducting, with the route through the cycle decomposition as a remark; the word is not unique, and the parity of its length, the sign, is left to later volumes; 3-cycles do not generate S_3; adjacent transpositions suffice; and review exercises on the kernel of $k \mapsto k \cdot 1_F$ and the characteristic of a field, on $\mathbb{Z}/6\mathbb{Z}$, $(\mathbb{Z}/7\mathbb{Z})^\times$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, on the permutations of a set with finite support, and on an element $g \neq e$ with $g^2 = e$ in a group with an even number of elements.

3.0.2 Named moves

- **Multiply by the inverse.** To remove a factor from one side of an equation in a group, multiply both sides **on the same side** by its inverse, then regroup with (G1); there is no "dividing", and the side matters because a group need not be abelian. Named in Section 3.1, where it proves the uniqueness of inverses and cancellation (Theorem 3.1.1 (2), (4)). Section 3.3 uses it to show that a homomorphism sends the identity to the identity and that a trivial kernel forces injectivity. Exercise B2 of Section 3.1 leaves its last step to you, and Exercise C1 of Section 3.2 its last half.
- **Check closure first.** Before checking (G1)–(G3), check that combining two elements of the set gives an element of the set: closure is not a fourth axiom but is built into "binary operation". The warning of Section 3.1 names it, with $\mathbb{Z}_{>0}$ under subtraction, and Example (Not Groups) and Exercise B1 of Section 3.1 show sets that fail at closure before any axiom is in question. In Section 3.2 the subgroup test packs closure under products and inverses into the one condition $ab^{-1} \in H$, and Exercise C1 there shows that for a finite

subset closure under products is enough.

- **Least positive element, then divide.** In a subgroup of $\mathbb{Z}$ other than $\{0\}$, take the least positive element n and divide any element by it: the remainder lies in the subgroup and is smaller than n, so it is 0. It is the move of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Section 3.2, now with only subtraction available. It proves Theorem 3.2.4 in Section 3.2, which turns Exercises B3 and C3 there into one-line consequences and reaches the characteristic of a field in review exercise R1 of Section 3.5.
- **Follow the orbit, then peel it off.** Start at a point the permutation moves and apply it until the point returns; record the cycle found, remove it, and induct on what is left, which moves fewer points. Named in Section 3.4, it proves Theorem 3.4.4 there, and Exercise A1 of Section 3.4 runs it by hand. Its one-transposition version, **fix one point, then induct**, proves Theorem 3.5.2 in Section 3.5: one swap makes the permutation fix the last point, and a permutation fixing the last point is a permutation of one point fewer (Lemma 3.4.1). Exercise A1 of Section 3.5 runs it, and its Exercise C1 asks for the proof as an exit check.

3.1 Groups

Several structures met so far behave alike: the integers under addition, the non-zero rationals under multiplication, the units of $\mathbb{Z}/n\mathbb{Z}$ (*Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Section 3.5), and the bijections of a set under composition (*Sets, Relations, and Cardinality*, Chapter 1). This section names their common structure, a group, and proves its basic laws once, from three axioms, so that they hold in all of these at once. It then makes two habits honest: dropping brackets from a product of many factors, and writing powers g^n with $n \in \mathbb{Z}$.

Throughout the chapter $\mathbb{N}$ is ω, and $\mathbb{Z}$, $\mathbb{Q}$ are the integers and rationals built in *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 2. Induction and recursion on $\mathbb{N}$ are Logic and Proof, Axiom 4.2.1 and Sets, Relations, and Cardinality, Theorem 2.3.1, read on ω through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b). Strong induction, Logic and Proof, Theorem 4.2.2, holds on ω too, since its proof uses only Logic and Proof, Axiom 4.2.1 and the order facts Number Systems: From \(\nN\) to \(\nR\), Theorem 1.6.1 (a), (b), (d).

3.1.1 Four situations side by side

Look at four situations in which two things are combined into a third.

- In $(\mathbb{Z}, +)$ we add integers. The integer 0 does nothing, $a + 0 = a$, and $-a$ undoes a, $a + (-a) = 0$.
- In $\mathbb{Q} \setminus \{0\}$ we multiply. The rational 1 does nothing, and a^{-1} undoes a.
- Among the units of $\mathbb{Z}/12\mathbb{Z}$, which are $[1], [5], [7], [11]$ by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1 (the classes of the integers coprime to 12), we multiply classes. The class $[1]$ does nothing, and each unit undoes itself: $[5][5] = [25] = [1]$, $[7][7] = [49] = [1]$ and $[11][11] = [121] = [1]$, since $25 = 2 \cdot 12 + 1$, $49 = 4 \cdot 12 + 1$ and $121 = 10 \cdot 12 + 1$.
- Among the bijections $X \to X$ of a set we compose. The identity map id_X does nothing, and each bijection f is undone by its inverse f^{-1} (Sets, Relations, and Cardinality, Definition 1.5.2).

The objects differ, and so do the ways of combining them, but the rules used are the same three: the combining is associative, one element changes nothing, and every element can be undone. So we give the pattern a name.

A group is a set with one way of combining two elements into a third, in which combining is associative, some element does nothing, and every element can be undone.

Definition 3.1.1. Group

A **group** is a set G together with a **binary operation** on G, that is, a function $G \times G \to G$, $(a, b) \mapsto ab$ (Sets, Relations, and Cardinality, Definition 1.4.1, with $G \times G$ the Cartesian product of Sets, Relations, and Cardinality, Definition 1.3.2), such that:

(G1) **(Associativity)** $(ab)c = a(bc)$ **for all** $a, b, c \in G$;

(G2) **(Identity) there is** an element $e \in G$ with $ea = ae = a$ **for every** $a \in G$;

(G3) **(Inverses) for every** $a \in G$ **there is** $b \in G$ with $ab = ba = e$, where e is the element of (G2).

The group is **abelian** if moreover $ab = ba$ **for all** $a, b \in G$.

In words: the operation is a function on pairs, so the combination of two elements of G **lies in** G again. This "closure" is not a fourth axiom; it is built into the phrase "binary operation $G \times G \to G$". (G1) says that the two ways of combining three elements in a fixed order agree. (G2) asks for an element that changes nothing, from **both** sides. (G3) asks that each element can be undone, again from both sides, back to that same e.

We write a group as $(G, \cdot)$, or simply G when the operation is clear, and call ab the **product** of a and b, whatever the operation is. When the operation is an addition we write $a + b$, 0 and $-a$ in place of ab, e and the inverse of a. This **additive notation** is used only for abelian groups.

Example. Groups

Check that each of (a)–(d) is a group, and decide which are abelian.

(a) $(R, +)$ for a commutative ring R (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1); in particular $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$ for $n \in \mathbb{Z}_{>0}$.

(b) $(\mathbb{Q} \setminus \{0\}, \cdot)$, and $(F \setminus \{0\}, \cdot)$ for any field F; in particular $(\mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}, \cdot)$ for a prime p.

(c) The set of bijections $X \to X$ of a set X, under composition $\circ$.

(d) A one-element set $\{e\}$ with $ee := e$.

(e) (A fifth situation, described here and checked in Section 3.4.) The four rotations of a square about its center, by no turn, a quarter turn, a half turn and three quarter turns. Label the corners $1, 2, 3, 4$ in order around the square; the quarter turn moves each label to the next corner, which is the bijection $i \mapsto i + 1$ for $i < 4$, $4 \mapsto 1$ of $\{1, 2, 3, 4\}$. Two rotations in a row make a rotation, the rotation by no turn changes nothing, and each rotation is undone by turning back.

Solution. (a) Recall the clauses (F1)–(F4) of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1: addition is commutative (F1) and associative (F2), $a + 0 = a$ (F3), and $a + (-a) = 0$ (F4). Addition is a function $R \times R \to R$ by the definition, so it is a binary operation. (G1) is (F2). For (G2), $a+0 = a$ is (F3), and $0+a = a+0 = a$ by (F1). For (G3), $a+(-a) = 0$ is (F4), and $(-a)+a = 0$ by (F1). The group is abelian by (F1). The instances: $\mathbb{Z}$ is a commutative ring by Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1, $\mathbb{Q}$ by Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3, $\mathbb{R}$ by Number Systems: From \(\nN\) to \(\nR\), Theorem 5.3.3, and $\mathbb{Z}/n\mathbb{Z}$ by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (a).

(b) Let F be a field (in the form of Number Systems: From \(\nN\) to \(\nR\), Defini-

tion 2.3.1; Chapter 2 restates the definition as Definition 2.1.1), for instance $F = \mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3). The first thing to check is that multiplication lands in $F \setminus \{0\}$. If $x \neq 0$ and $y \neq 0$, then x is a unit by (F8), and a unit is not a zero divisor (the paragraph after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1), so $xy \neq 0$. So a product of two non-zero elements is non-zero, and multiplication restricts to a binary operation on $F \setminus \{0\}$. (G1) is (F5). For (G2), $1 \neq 0$ in a field, so $1 \in F \setminus \{0\}$, and $a \cdot 1 = 1 \cdot a = a$ by (F7) and (F6). For (G3), let $a \neq 0$; then $aa^{-1} = a^{-1}a = 1$ by (F8) and (F6), and $a^{-1} \neq 0$, since $a^{-1} = 0$ would give $1 = a \cdot 0 = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)). The group is abelian by (F6). For a prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2, so $\mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}$ is a group under multiplication.

(c) Composition of two bijections $X \to X$ is a bijection $X \to X$ by Sets, Relations, and Cardinality, Theorem 1.4.4 (c), so $\circ$ is a binary operation on the set of bijections. (G1) holds by Sets, Relations, and Cardinality, Proposition 1.4.3, and the same result gives $f \circ \mathrm{id}_X = f = \mathrm{id}_X \circ f$, so id_X, a bijection, satisfies (G2). For (G3), a bijection f has a two-sided inverse f^{-1} by Sets, Relations, and Cardinality, Theorem 1.5.4, with $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_X$ (Sets, Relations, and Cardinality, Definition 1.5.2). These two equations also say that f is a two-sided inverse of f^{-1}, so f^{-1} is a bijection, again by Sets, Relations, and Cardinality, Theorem 1.5.4.

Whether it is abelian depends on X; the fold below decides it.

Second reading · *When is the group of bijections abelian?*

If X has three distinct elements x, y, z, let f swap x and y and fix every other point, and let g swap y and z and fix every other point. Each is its own inverse ($f \circ f = \mathrm{id}_X$), so each is a bijection. Then $(f \circ g)(x) = f(x) = y$, while $(g \circ f)(x) = g(y) = z \neq y$. So $f \circ g \neq g \circ f$, and the group is **not** abelian. If X has at most two elements, there are at most two bijections, id_X and the swap, and any two of them commute, since each commutes with id_X and with itself. Section 3.4 meets this group again for $X = \{1, \ldots, n\}$ and computes in it.

(d) All three axioms reduce to $ee = e$: $(ee)e = e = e(ee)$, e is an identity, and e is its own inverse. This **trivial group** is the degenerate case. It is abelian, and it reappears in Section 3.2 as the smallest subgroup of every group.

(e) is not checked here. Section 3.4 writes the four rotations as permutations of $\{1, 2, 3, 4\}$, and its Exercise B3 shows that they behave exactly like $\mathbb{Z}/4\mathbb{Z}$ under addition.

Remark. The invertible $n \times n$ matrices over a field form a group under matrix multiplication; *Spaces and Maps*, the chapter "Matrices", proves it. Nothing in this volume uses it.

Now non-examples, each a minimal change of an example above.

Example. Not Groups

For each of the following, say which of (G1)–(G3), or the binary operation itself, fails: $(\mathbb{Z}, \cdot)$; $(\mathbb{N}, +)$; $\mathbb{Z}$ with $a * b \coloneqq a - b$; $\mathbb{Z}/6\mathbb{Z} \setminus \{[0]\}$ under multiplication.

Solution. $(\mathbb{Z}, \cdot)$. Replace addition by multiplication in (a). Multiplication is a binary operation on $\mathbb{Z}$, it is associative by (F5), and 1 is an identity by (F7) and (F6) (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1). But (G3) fails at $a = 2$: if $2b = 1$ for some $b \in \mathbb{Z}$, then $2 \mid 1$, and Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (g) gives $2 = 1$ or $2 = -1$, which is false.

$(\mathbb{N}, +)$. Keep addition but shrink $\mathbb{Z}$ to $\mathbb{N}$. Addition still lands in $\mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (a)), it is associative, and 0 is an identity, by (F1)–(F3) in $\mathbb{Z}$. But (G3) fails at $a = 1$: in $\mathbb{Z}$ the only b with $1 + b = 0$ is -1 (uniqueness of negatives, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)), and $-1 < 0$, so $-1 \notin \mathbb{N}$ by Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.4 (b).

$a * b \coloneqq a - b$ *on* $\mathbb{Z}$. It is a binary operation, but (G1) fails: $(1 * 1) * 1 = 0 - 1 = -1$, while $1 * (1 * 1) = 1 - 0 = 1$.

$\mathbb{Z}/6\mathbb{Z} \setminus \{[0]\}$ *under multiplication.* Replace the prime p of (b) by 6. Here the operation itself fails: $[2]$ and $[3]$ lie in the set, but $[2][3] = [6] = [0]$ does not (Number Systems: From \(\nN\) to \(\nR\), Example (Multiplication modulo six and modulo five)), so (G1)–(G3) are not even in question.

Warning. **Check closure first.** "$\mathbb{Z}_{>0}$ under subtraction" is not a group, and not because an axiom fails: 1 and 2 are positive integers, but $1 - 2 = -1$ is not, so subtraction is not a binary operation on $\mathbb{Z}_{>0}$ at all. Before checking (G1)–(G3), check that combining two elements of the set gives an element of the set.

3.1.2 The basic laws, proved once

The rules we proved separately for functions (uniqueness of inverses) and for rings (uniqueness of 0, of $-a$, of u^{-1}) follow from the three axioms alone. We prove them once:

Theorem 3.1.1. Basic Properties of Groups

Let G be a group and $a, b, c \in G$.

(1) The identity element of G is unique.
(2) The inverse of a is unique. We denote it by a^{-1}.
(3) $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.
(4) **(Cancellation)** If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.
(5) The equations $ax = b$ and $ya = b$ have **exactly one** solution $x \in G$ and **exactly one** solution $y \in G$: $x = a^{-1}b$ and $y = ba^{-1}$.

Idea. Uniqueness is proved by taking two candidates and showing they are equal. For the identity, play the two identity properties against each other. For inverses, the only tools are

(G1)–(G3), so insert e in a clever form and regroup. The candidate $b^{-1}a^{-1}$ for the inverse of ab is found by undoing the last step first, as with putting on socks and then shoes.

Proof. For (1), suppose e and e' both satisfy (G2). Then $e = ee'$, using that e' is an identity, and $ee' = e'$, using that e is one. Hence $e = e'$.

For (2), suppose b and b' both satisfy (G3) for a: $ab = ba = e$ and $ab' = b'a = e$. Multiply the equation $ab' = e$ on the left by b, and regroup by (G1):

$$b = be = b(ab') = (ba)b' = eb' = b',$$

where the first and last equalities are (G2), and $ba = e$ is used in the fourth.

For (3), the equations $aa^{-1} = a^{-1}a = e$ say that a is an inverse of a^{-1}, so $(a^{-1})^{-1} = a$ by (2). Next, by (G1) twice, then (G3), (G2) and (G3),

$$(ab)(b^{-1}a^{-1}) = \big((ab)b^{-1}\big)a^{-1} = \big(a(bb^{-1})\big)a^{-1} = (ae)a^{-1} = aa^{-1} = e,$$

and in the same way $(b^{-1}a^{-1})(ab) = \big((b^{-1}a^{-1})a\big)b = \big(b^{-1}(a^{-1}a)\big)b = (b^{-1}e)b = b^{-1}b = e$. By (2), $(ab)^{-1} = b^{-1}a^{-1}$.

For (4), suppose $ab = ac$. Multiplying on the left by a^{-1} and using (G1),

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c.$$

The second statement follows by multiplying on the right by a^{-1}.

For (5), $x = a^{-1}b$ is a solution, since $a(a^{-1}b) = (aa^{-1})b = eb = b$ by (G1), (G3) and (G2). If $ax = b$ and $ax' = b$, then $ax = ax'$, so $x = x'$ by (4). In the same way $y = ba^{-1}$ solves $ya = b$, since $(ba^{-1})a = b(a^{-1}a) = b$, and it is the only solution by the second half of (4). This proves the theorem.

■

Parts (2) and (4) use one move, and we give it a name: **multiply by the inverse**. To remove a factor from one side of an equation in a group, multiply both sides **on the same side** by its inverse, then regroup with (G1). The side matters, since a group need not be abelian; there is no "dividing by a".

Part (2) is the argument of Sets, Relations, and Cardinality, Proposition 1.5.3, that a left inverse and a right inverse of a function agree, with functions erased; the uniqueness of the inverse of a unit in Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1 is the same argument once more. Part (1) is the argument for the uniqueness of 0 and 1 in Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a). That is the point of the definition: a proof that uses only (G1)–(G3) holds in every group at once.

3.1.3 Products of many factors

Part (3) had to write every bracket out. To write $g_1 g_2 \cdots g_r$ with no brackets at all, we must say which product it means, and then check that the brackets do not matter. The definition uses the recursion that defined finite sums and products of reals.

Definition 3.1.2. Product of a List

Let G be a group and $r \in \mathbb{N}$. A **list** of length r in G is a function $\{1, \dots, r\} \to G$, written $(g_1, \dots, g_r)$; for $r = 0$ it is the **empty list**. Its **product** $g_1 g_2 \cdots g_r \in G$ is given by recursion: the product of the empty list is e, and

$$g_1 \cdots g_{j+1} \coloneqq (g_1 \cdots g_j)\, g_{j+1} \quad \text{for } 0 \le j < r,$$

where $g_1 \cdots g_j$ is the product of the shortened list $(g_1, \dots, g_j)$.

In words: start with e, and multiply on the right by one more entry at each stage. The product of a list of length 1 is $eg_1 = g_1$, the product of (g_1, g_2) is $g_1 g_2$, and $g_1 g_2 g_3$ means $(g_1 g_2) g_3$: **the brackets are nested to the left** by definition.

This is the recursion of Sets, Relations, and Cardinality, Definition 2.3.1, stated there for products of real numbers and used here as a pattern with the group G in place of $\mathbb{R}$ and e in place of 1, as *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Section 3.3 used it for products of integers (Number Systems: From \(\nN\) to \(\nR\), Definition 3.3.1). The recursion runs on $\mathbb{N}$ by Sets, Relations, and Cardinality, Theorem 2.3.1, after extending the list by $g_k \coloneqq e$ for $k > r$; the "Finite lists" remark after Sets, Relations, and Cardinality, Definition 2.3.1 shows that the products up to r do not depend on the extension. That remark only multiplies on the right; it never reorders factors, so it holds in a group that is not abelian.

Proposition 3.1.2. Laws for Products of Lists

Let G be a group, and let $(g_1, \dots, g_r)$ and $(h_1, \dots, h_s)$ be lists in G.

(a) **(Concatenation)** $(g_1 \cdots g_r)(h_1 \cdots h_s) = g_1 \cdots g_r h_1 \cdots h_s$, the product of the list $(g_1, \dots, g_r, h_1, \dots, h_s)$ of length $r + s$.

(b) **(Brackets)** If $r \ge 1$, every bracketing of $g_1, \dots, g_r$, in this order, has the value $g_1 \cdots g_r$.

(c) **(Inverses)** $(g_1 \cdots g_r)^{-1} = g_r^{-1} \cdots g_1^{-1}$.

Here a **bracketing** of a list of length $r \ge 1$ is a way of inserting brackets, built by one rule: a single entry g_1 is a bracketing of (g_1), with value g_1; and for $r \ge 2$, a bracketing is $(B)(B')$, where B is a bracketing of a first part $(g_1, \dots, g_k)$ with $1 \le k < r$ and B' is a bracketing of the rest $(g_{k+1}, \dots, g_r)$, with value the product of their values. For instance, $(g_1 g_2)(g_3 g_4)$ and $g_1(g_2(g_3 g_4))$ are bracketings of a list of length 4.

Idea. Each part is an induction that follows the recursion. For (a), induct on the length s of the second list: adding one entry to it multiplies both sides on the right by that entry, and (G1) moves the bracket. For (b), the outermost product of a bracketing joins two shorter bracketings, which the induction hypothesis turns into list products, and (a) joins those. For (c), part (3) of Theorem 3.1.1 reverses two factors at a time.

Proof.

(a) Fix the list $(g_1, \dots, g_r)$ and write $P \coloneqq g_1 \cdots g_r$. We prove the statement for every list $(h_1, \dots, h_s)$ by Logic and Proof, Axiom 4.2.1 on s. For $s = 0$, the right side is the product of $(g_1, \dots, g_r)$ itself, and the left side is $Pe = P$ by (G2). Suppose the

statement holds for lists of length s, and let $(h_1, \dots, h_{s+1})$ be a list. Then

$$\begin{aligned} P(h_1 \cdots h_{s+1}) &= P((h_1 \cdots h_s)h_{s+1}) = (P(h_1 \cdots h_s))h_{s+1} \\ &= (g_1 \cdots g_r h_1 \cdots h_s)\, h_{s+1} = g_1 \cdots g_r h_1 \cdots h_{s+1}, \end{aligned}$$

by the recursion of Definition 3.1.2, then (G1), then the induction hypothesis for the shortened list $(h_1, \dots, h_s)$, and finally the recursion for the concatenated list at its last entry, h_{s+1}.

Parts (b) and (c) are proved in the fold below. This proves (a).

■

Second reading · *Proofs of (b) and (c): brackets and inverses*

Proof.

(b) We use Logic and Proof, Theorem 4.2.2 on r, for the property "if $r \geq 1$, every bracketing of every list of length r has the value $g_1 \cdots g_r$"; for $r = 0$ there is nothing to prove. Let $r \geq 1$, and suppose the property holds for every smaller length. If $r = 1$, the only bracketing is g_1, and $g_1 = eg_1$ is the product of (g_1) by (G2) and the recursion. If $r \geq 2$, a bracketing is $(B)(B')$ with B a bracketing of $(g_1, \dots, g_k)$ and B' a bracketing of $(g_{k+1}, \dots, g_r)$, where $1 \leq k < r$. Both lengths, k and $r-k$, are at least 1 and smaller than r, so by the hypothesis the value of B is $g_1 \cdots g_k$ and the value of B' is $g_{k+1} \cdots g_r$. By (a), their product is the product of the concatenated list, which is $(g_1, \dots, g_r)$. So the value of $(B)(B')$ is $g_1 \cdots g_r$. This completes the induction.

(c) By Logic and Proof, Axiom 4.2.1 on r. For $r = 0$, both sides are e, since $ee = e$ makes e its own inverse (Theorem 3.1.1 (2)). Suppose the statement holds for lists of length r, and let $(g_1, \dots, g_{r+1})$ be a list. Then

$$\begin{aligned} (g_1 \cdots g_{r+1})^{-1} &= ((g_1 \cdots g_r)\, g_{r+1})^{-1} = g_{r+1}^{-1} (g_1 \cdots g_r)^{-1} \\ &= g_{r+1}^{-1} (g_r^{-1} \cdots g_1^{-1}) = g_{r+1}^{-1} g_r^{-1} \cdots g_1^{-1}, \end{aligned}$$

by the recursion, Theorem 3.1.1 (3), the induction hypothesis, and (a) with the list (g_{r+1}^{-1}) of length 1, whose product is g_{r+1}^{-1}. This proves the proposition.

■

By part (b), **from now on we drop brackets** from products in a group, regrouping in any way that keeps the order of the factors. The order itself may not change, unless the group is abelian (Exercise C3).

3.1.4 Integer powers

The commonest list is a constant one. A product of n copies of g is the power g^n, and the inverse of g^n deserves to be a power too.

Definition 3.1.3. Integer Powers

Let G be a group and $g \in G$. For $n \in \mathbb{N}$, the **power** g^n is the product of the constant list $(g, \dots, g)$ of length n; so

$$g^0 = e, \qquad g^{n+1} = g^n g \quad \text{for } n \in \mathbb{N}.$$

For $n \in \mathbb{Z}$ with $n < 0$, write $n = -m$ with $m \in \mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (c)), and set $g^n := (g^{-1})^m$. In additive notation the power is the **multiple** $n \cdot g$: $0 \cdot g = 0$, $(n+1) \cdot g = n \cdot g + g$, and $(-m) \cdot g = m \cdot (-g)$.

The two clauses do not overlap, since $n < 0$ and $n \in \mathbb{N}$ exclude each other (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.4 (b)), and for $n < 0$ the m is $-n$, so g^n is well defined. The new notation agrees with the old one: $g^1 = eg = g$, and $g^{-1} = (g^{-1})^1$ is the inverse of g. So $g^2 = gg$ and $g^{-2} = g^{-1}g^{-1}$.

The power laws look like school algebra, but the school proofs commute factors; here only (d) may, and it says so:

Proposition 3.1.3. Power Laws in a Group

Let G be a group, $g, h \in G$ and $m, n \in \mathbb{Z}$.

(a) $g^m g^n = g^{m+n}$.
(b) $(g^m)^{-1} = g^{-m} = (g^{-1})^m$.
(c) $(g^m)^n = g^{mn}$.
(d) If $gh = hg$, then $(gh)^n = g^n h^n$.
(e) Let R be a commutative ring. In the group $(R, +)$, for $a \in R$ and $n \in \mathbb{N}$, the multiple $n \cdot a$ of Definition 3.1.3 is the multiple $n \cdot a$ of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Section 2.3. In $(\mathbb{Z}, +)$, $n \cdot a = na$, the product in the ring $\mathbb{Z}$, for all $n, a \in \mathbb{Z}$.

Idea. For exponents in $\mathbb{N}$, a power is a list product, and (a) is concatenation. Negative exponents are reduced to natural ones by one fact: g^m and $(g^{-1})^m$ are inverse to each other, because the factors cancel in pairs from the middle out, $g \cdots g\, g^{-1} \cdots g^{-1} = e$. With that, each sign case of (a) is a natural-number case for g or for g^{-1}. Parts (c) and (d) are inductions on $n \in \mathbb{N}$, extended to $n < 0$ by (b).

↻ **Second reading** · *Proof of the power laws*

Proof. (a) for $m, n \in \mathbb{N}$. The left side is the product of the constant list of length m times that of length n. By Proposition 3.1.2 (a) it is the product of the concatenated list, the constant list of length $m + n$, which is g^{m+n}.

(b). First let $m \in \mathbb{N}$. We show $g^m (g^{-1})^m = e$ by Logic and Proof, Axiom 4.2.1 on m. For $m = 0$, $ee = e$. For the step, $g^{m+1} = g^1 g^m = gg^m$ by (a) on $\mathbb{N}$, and $(g^{-1})^{m+1} = (g^{-1})^m g^{-1}$

by the definition, so, dropping brackets (Proposition 3.1.2 (b)),

$$g^{m+1}(g^{-1})^{m+1} = g(g^m(g^{-1})^m)g^{-1} = geg^{-1} = e.$$

So $x = (g^{-1})^m$ solves $g^m x = e$. By Theorem 3.1.1 (5) the only solution is $(g^m)^{-1}e = (g^m)^{-1}$; hence $(g^m)^{-1} = (g^{-1})^m$. This is also g^{-m}: for $m > 0$ by the definition of negative powers, and for $m = 0$ because $g^0 = e = (g^{-1})^0$.

Now let $m < 0$, and write $m = -k$ with $k \in \mathbb{N}$. By the definition, $g^m = (g^{-1})^k$. The case just proved, applied to the element g^{-1} and the exponent k, gives $\left((g^{-1})^k\right)^{-1} = \left((g^{-1})^{-1}\right)^k = g^k$, by Theorem 3.1.1 (3). So $(g^m)^{-1} = g^k = g^{-m}$. Finally $(g^{-1})^m = \left((g^{-1})^{-1}\right)^k = g^k$ by the definition of negative powers, applied to the element g^{-1}. This proves (b). In particular,

$$(g^{-1})^p = g^{-p} \quad \text{for every } p \in \mathbb{Z}. \tag{$*$}$$

(a) in general. We first show, for $m, k \in \mathbb{N}$,

$$g^m g^{-k} = g^{m-k}. \tag{$**$}$$

By (b), $g^{-k} = (g^{-1})^k$, and $g^k(g^{-1})^k = e$ (shown in (b)). If $m \geq k$, then $m - k \in \mathbb{N}$ and $g^m = g^{m-k}g^k$ by (a) on $\mathbb{N}$, so $g^m(g^{-1})^k = g^{m-k}g^k(g^{-1})^k = g^{m-k}$. If $m < k$, then $k - m \in \mathbb{N}$, and $(g^{-1})^k = (g^{-1})^m(g^{-1})^{k-m}$ by (a) on $\mathbb{N}$ for the element g^{-1}; since $g^m(g^{-1})^m = e$, we get $g^m(g^{-1})^k = (g^{-1})^{k-m} = g^{-(k-m)} = g^{m-k}$, by $(*)$.

Now let $m, n \in \mathbb{Z}$, and write $u := g^{-1}$, so that $g^p = u^{-p}$ for every $p \in \mathbb{Z}$ by $(*)$ and $(g^{-1})^{-1} = g$. There are four cases. If $m, n \geq 0$, this is (a) on $\mathbb{N}$. If $m \geq 0 > n$, write $n = -k$; this is $(**)$. If $m < 0 \leq n$, write $m = -j$; then $g^m g^n = u^j u^{-n} = u^{j-n} = g^{n-j} = g^{m+n}$, by $(**)$ for u and then $(*)$. If $m, n < 0$, write $m = -j$, $n = -k$; then $g^m g^n = u^j u^k = u^{j+k} = g^{-(j+k)} = g^{m+n}$, by (a) on $\mathbb{N}$ for u and $(*)$. The identities between exponents used here, such as $n - j = m + n$, are ring arithmetic in $\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1).

(c). For $n \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1 on n: $(g^m)^0 = e = g^0$, and $(g^m)^{n+1} = (g^m)^n g^m = g^{mn}g^m = g^{mn+m} = g^{m(n+1)}$, by the definition, the hypothesis, (a), and (F9) in $\mathbb{Z}$. For $n < 0$, write $n = -k$; then

$$(g^m)^n = \left((g^m)^{-1}\right)^k = (g^{-m})^k = g^{(-m)k} = g^{m(-k)} = g^{mn},$$

by the definition, (b), the case $k \in \mathbb{N}$ for the exponent $-m$, and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c).

(d). Suppose $gh = hg$. First, $gh^n = h^n g$ for $n \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1: for $n = 0$ both sides are g, and $gh^{n+1} = (gh^n)h = h^n gh = h^n hg = h^{n+1}g$. Next, $(gh)^n = g^n h^n$ for $n \in \mathbb{N}$, again by induction: for $n = 0$ both sides are e, and

$$(gh)^{n+1} = (gh)^n\, gh = g^n h^n gh = g^n gh^n h = g^{n+1}h^{n+1},$$

using $h^n g = gh^n$ and (a). For $n < 0$, write $n = -k$. Taking inverses in $gh = hg$ gives $h^{-1}g^{-1} = g^{-1}h^{-1}$ (Theorem 3.1.1 (3)), so g^{-1} and h^{-1} commute too. Hence

$$(gh)^n = \left((gh)^{-1}\right)^k = (h^{-1}g^{-1})^k = (g^{-1}h^{-1})^k = (g^{-1})^k(h^{-1})^k = g^n h^n,$$

by the definition, Theorem 3.1.1 (3), the commuting just shown, the case $k \in \mathbb{N}$ for the commuting pair g^{-1}, h^{-1}, and the definition again.

(e). For $n \in \mathbb{N}$, both multiples are given by the same two clauses, $0 \cdot a = 0$ and $(n+1) \cdot a = n \cdot a + a$, so they are the same function $\mathbb{N} \to R$ by the uniqueness in Sets, Relations, and Cardinality, Theorem 2.3.1. In $\mathbb{Z}$, *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 2.3 shows $n \cdot a = na$ for $n \in \mathbb{N}$ (the paragraph "Multiples", before Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5). For $n = -m$ with $m \in \mathbb{N}$, $(-m) \cdot a = m \cdot (-a) = m(-a) = (-m)a$, by Definition 3.1.3, the case $n \in \mathbb{N}$, and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c). This proves the proposition.

■

Part (d) needs $gh = hg$: without it the law fails, and Section 3.4 exhibits a failure with two permutations of $\{1, 2, 3\}$.

↻ **Second reading** · *Multiples in Chapters 2 and 3 agree*

Remark. For $n = -m < 0$, part (b) in additive notation reads $m \cdot (-a) = -(m \cdot a)$, so the multiple $(-m) \cdot a = m \cdot (-a)$ of Definition 3.1.3 equals $-(m \cdot a)$. That is how Section 2.5 defines $n \cdot a$ for $n < 0$ in a commutative ring. So "$n \cdot a$" means the same thing in Chapters 2 and 3 for every $n \in \mathbb{Z}$, and the identities of Lemma 2.5.1 apply to the multiples of the group $(R, +)$. No proof in this chapter rests on this comparison; Exercise R1 of Section 3.5 needs only part (e).

3.1.5 The units of a commutative ring form a group

Number Systems: From $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.5 found the units of a commutative ring R, the elements u with $uv = 1$ for some $v \in R$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1), and showed in the paragraph after the definition that 1 is a unit, that products and inverses of units are units, and that the inverse u^{-1} is unique. In the language of this section:

Proposition 3.1.4. The Units Form a Group

Let R be a commutative ring. Then $R^\times$, the set of units of R, is an abelian group under the multiplication of R, with identity 1, and the inverse of u in this group is u^{-1}.

Proof. By the paragraph after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1, a product of two units is a unit, so multiplication restricts to a binary operation on $R^\times$. (G1) holds by (F5) of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1. For (G2), 1 is a unit since $1 \cdot 1 = 1$, and $u \cdot 1 = 1 \cdot u = u$ by (F7) and (F6). For (G3), let $u \in R^\times$. Then $uu^{-1} = u^{-1}u = 1$ by Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1 and (F6), and u^{-1} is itself a unit, by the same paragraph. The group is abelian by (F6). This proves the proposition.

■

So the third situation at the start of the section was the group $(\mathbb{Z}/12\mathbb{Z})^\times$. More examples:

- $\mathbb{Z}^\times = \{1, -1\}$ (the examples after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1), a group with two elements.
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] : \gcd(a, n) = 1\}$ for $n \in \mathbb{Z}_{>0}$, by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1. For $n = 8$ it is $\{[1], [3], [5], [7]\}$, and every element is its own inverse: $[3][3] = [9] = [1]$, $[5][5] = [25] = [1]$, $[7][7] = [49] = [1]$.
- $F^\times = F \setminus \{0\}$ for a field F: every non-zero element is a unit by (F8), and 0 is not, since $0 \cdot v = 0 \neq 1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)). So the group of Example (Groups) (b) is $F^\times$.

Quick check. In $(\mathbb{Z}/7\mathbb{Z})^\times$, find $[3]^{-1}$ and $[3]^{-2}$.

Solution. $[3]^{-1} = [5]$, since $3 \cdot 5 = 15 = 2 \cdot 7 + 1$, so $[3][5] = [1]$. By Definition 3.1.3, $[3]^{-2} = ([3]^{-1})^2 = [5][5] = [25] = [4]$, since $25 = 3 \cdot 7 + 4$. Check: $[3]^2[4] = [9][4] = [36] = [1]$, as $36 = 5 \cdot 7 + 1$.

3.1.6 Exercises

3.1.6.1 A. Check your understanding

Exercise. A1

(a) State the axioms (G1)–(G3), and say where in the definition of a group closure is required.

(b) Is $\mathbb{Z}$ with $a * b \coloneqq a + b + 1$ a group? Justify your answer.

(c) True or false: in every group, $(ab)^{-1} = a^{-1}b^{-1}$. Justify your answer.

(d) Compute $3 \cdot [5]$ and $(-2) \cdot [5]$ in the group $(\mathbb{Z}/7\mathbb{Z}, +)$.

Solution.

(a) (G1) $(ab)c = a(bc)$ for all $a, b, c \in G$; (G2) there is $e \in G$ with $ea = ae = a$ for every $a \in G$; (G3) for every $a \in G$ there is $b \in G$ with $ab = ba = e$. Closure is not an axiom of its own: it is required by "binary operation", a function $G \times G \to G$, whose values lie in G.

(b) Yes. The rule is a function $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. (G1): both $(a * b) * c = (a + b + 1) + c + 1$ and $a * (b * c) = a + (b + c + 1) + 1$ equal $a + b + c + 2$, by (F1) and (F2). (G2): $e = -1$ works, since $a * (-1) = a + (-1) + 1 = a$ and $(-1) * a = a$ likewise. (G3): the inverse of a is $-a - 2$, since $a * (-a - 2) = a - a - 2 + 1 = -1$, and the other order gives the same by (F1). It is abelian, since $a + b + 1 = b + a + 1$.

(c) False. Let f and g be the bijections of $\{1, 2, 3\}$ with f swapping $1, 2$ and g swapping $2, 3$, each fixing the third point; each is its own inverse. Then $f \circ g$ sends $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$ (for instance $(f \circ g)(2) = f(3) = 3$), so its inverse sends $1 \mapsto 3$.

But $f^{-1} \circ g^{-1} = f \circ g$ sends $1 \mapsto 2$. So $(f \circ g)^{-1} \neq f^{-1} \circ g^{-1}$. The correct rule is $(ab)^{-1} = b^{-1}a^{-1}$ (Theorem 3.1.1 (3)); in an abelian group $b^{-1}a^{-1} = a^{-1}b^{-1}$, so there the statement is true.

(d) By Definition 3.1.3, $3 \cdot [5] = [5] + [5] + [5] = [15] = [1]$, since $15 = 2 \cdot 7 + 1$. Next $-[5] = [-5] = [2]$, so $(-2) \cdot [5] = 2 \cdot [2] = [4]$.

3.1.6.2 B. Practice

Exercise. B1: Groups or not

Determine which of the following are groups. Justify your answer.

(a) $\mathbb{Q}_{>0}$ under multiplication.

(b) $\{1, -1\} \subseteq \mathbb{Z}$ under multiplication.

(c) The odd integers under addition.

(d) $\{[1], [3], [5], [7]\} \subseteq \mathbb{Z}/8\mathbb{Z}$ under multiplication.

(e) $\mathbb{Z}/6\mathbb{Z} \setminus \{[0]\}$ under multiplication.

Solution.

(a) A group. $\mathbb{Q}$ is an ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1), so a product of positive rationals is positive by (O4), and multiplication is a binary operation on $\mathbb{Q}_{>0}$. Associativity is (F5), and $1 > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)) is an identity. For $x > 0$, x^{-1} exists since $x \neq 0$, and $x^{-1} > 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.5.2 (a). So the inverse stays in $\mathbb{Q}_{>0}$.

(b) A group: it is $\mathbb{Z}^\times$, a group by Proposition 3.1.4.

(c) Not a group: addition is not a binary operation on the odd integers, since $1 + 1 = 2$ is even and so not odd (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a)).

(d) A group: it is $(\mathbb{Z}/8\mathbb{Z})^\times$ (the examples after Proposition 3.1.4), and every element is its own inverse.

(e) Not a group: $[2][3] = [0]$, so multiplication is not a binary operation on the set (Example (Not Groups)).

Exercise. B2: An element equal to its square

Let G be a group and $g \in G$ with $gg = g$. Prove that $g = e$.

The first step is given: by (G2), $gg = g = ge$.

The last step is blank. *Name the move, then complete it.*

Solution. The move is **multiply by the inverse**: g appears on the left of both sides, so multiply both sides on the left by g^{-1} and regroup.

Completion: from $gg = ge$, cancellation (Theorem 3.1.1 (4)) gives $g = e$. Written out,

$g = (g^{-1}g)g = g^{-1}(gg) = g^{-1}(ge) = (g^{-1}g)e = e.$

Exercise. B3: Powers of a conjugate

Let G be a group and $g, h \in G$. Prove that $(ghg^{-1})^n = gh^n g^{-1}$ for every $n \in \mathbb{Z}$.

Solution. *For $n \in \mathbb{N}$,* by Logic and Proof, Axiom 4.2.1 on n. For $n = 0$, both sides are e, since $geg^{-1} = gg^{-1} = e$. Suppose $(ghg^{-1})^n = gh^n g^{-1}$. Then, dropping brackets (Proposition 3.1.2 (b)),

$$(ghg^{-1})^{n+1} = (ghg^{-1})^n\, ghg^{-1} = gh^n g^{-1} ghg^{-1} = gh^n hg^{-1} = gh^{n+1}g^{-1},$$

by Definition 3.1.3, the hypothesis, $g^{-1}g = e$, and Definition 3.1.3 again.

For $n < 0$, write $n = -k$ with $k \in \mathbb{N}$. By Proposition 3.1.3 (b), the case just proved, and Proposition 3.1.2 (c),

$$(ghg^{-1})^n = \left((ghg^{-1})^k\right)^{-1} = (gh^k g^{-1})^{-1} = (g^{-1})^{-1}(h^k)^{-1}g^{-1} = gh^{-k}g^{-1},$$

where the last step uses Theorem 3.1.1 (3) and Proposition 3.1.3 (b). This proves the identity for every $n \in \mathbb{Z}$.

3.1.6.3 C. Going deeper

Exercise. C1: Exit check: the basic laws of a group

Prove parts (1)–(3) of Theorem 3.1.1 from (G1)–(G3) only: the identity is unique; the inverse of each element is unique; and $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$.

Solution (Hint 1). For uniqueness, take two candidates and compute one expression in two ways.

Solution (Hint 2). For inverses, let b and b' both be inverses of a, and start from $b = be$.

Solution. The proof of (1)–(3) in Theorem 3.1.1 is a complete answer. In outline: two identities e, e' give $e = ee' = e'$; two inverses b, b' of a give $b = be = b(ab') = (ba)b' = eb' = b'$; a is an inverse of a^{-1}, so $(a^{-1})^{-1} = a$ by uniqueness; and $(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = e$ and $(b^{-1}a^{-1})(ab) = ((b^{-1}a^{-1})a)b = (b^{-1}(a^{-1}a))b = e$, so $(ab)^{-1} = b^{-1}a^{-1}$ by uniqueness.

Marking scheme. (10 points) - 2: uniqueness of the identity, with each of the two identity properties named where it is used. - 3: uniqueness of inverses, by inserting $e = ab'$ (or an equivalent use of (G2) and (G3)) and regrouping, with each step named. - 1: $(a^{-1})^{-1} = a$, by reading $aa^{-1} = a^{-1}a = e$ as "a is an inverse of a^{-1}" and citing uniqueness. - 3: $(ab)(b^{-1}a^{-1}) = e$, with (G1) named, **and** $(b^{-1}a^{-1})(ab) = e$. - 1: the conclusion $(ab)^{-1} = b^{-1}a^{-1}$, citing uniqueness of inverses. Fatal errors (0 for the step): using commutativity;

"dividing" by an element. Checking only one product earns 1 of those 3 points (not fatal), or all 4 points for $(ab)^{-1}$ with a proof from (G1)–(G3) that a one-sided inverse is the inverse ($xy = e$ or $yx = e$ implies $y = x^{-1}$). A proof of uniqueness of inverses through cancellation earns the 3 points only if cancellation is itself proved from (G1)–(G3).

Exercise. C2: Find the error

Here is a statement and an argument for it.

> **Claim.** In every group, $(ab)^{-1} = b^{-1}a^{-1}$.
>
> **Argument.** (1) By (G1)–(G3), $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$. (2) Since $xy = yx$ for all x, y in a group, also $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$. (3) So $b^{-1}a^{-1}$ is a two-sided inverse of ab, and $(ab)^{-1} = b^{-1}a^{-1}$ by uniqueness of inverses.

Is the claim true? Does the argument prove it? If not, name the line that fails, explain why, and give a counterexample to the step.

Solution. The claim is **true**: it is Theorem 3.1.1 (3). The argument does **not** prove it.

Lines (1) and (3) are correct. The failing line is (2), and only (2). It rests on the general "fact" that any two elements of a group commute. That is not an axiom, it has not been proved, and it is false, so the line cites nothing: entry (N9) of Logic and Proof, Example (What is not allowed). A counterexample to the step: the bijections f, g of $\{1, 2, 3\}$ in A1 (c), with $(f \circ g)(1) = 2$ and $(g \circ f)(1) = g(2) = 3$, so $f \circ g \neq g \circ f$. There is no counterexample to the conclusion, which is true.

The repair is to compute the second product as the first one was computed, with (G1): $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Alternatively, line (1) alone suffices: it says that $b^{-1}a^{-1}$ solves $y(ab) = e$, whose only solution is $e(ab)^{-1} = (ab)^{-1}$ by Theorem 3.1.1 (5).

Exercise. C3: Rearranging in an abelian group

Let G be an abelian group and $(g_1, \ldots, g_r)$ a list in G with $r \geq 2$.

(a) Prove that swapping two adjacent entries g_i, g_{i+1} $(1 \leq i < r)$ does not change the product of the list.

(b) Deduce that the product does not change under any rearrangement obtained by finitely many such adjacent swaps.

Solution.

(a) By Proposition 3.1.2 (a) and (b), the product of the list is the bracketing

$$(g_1 \cdots g_{i-1})(g_i g_{i+1})(g_{i+2} \cdots g_r),$$

where an empty product is e. The list with g_i and g_{i+1} swapped has, in the same way,

the product $(g_1 \cdots g_{i-1})(g_{i+1}g_i)(g_{i+2} \cdots g_r)$. Since G is abelian, $g_i g_{i+1} = g_{i+1} g_i$, so the two products are equal.

(b) By Logic and Proof, Axiom 4.2.1 on the number k of swaps: for $k = 0$ the list is unchanged, and a rearrangement by $k+1$ swaps is one swap applied to a rearrangement by k swaps, whose product equals the original product by the hypothesis; the last swap does not change the product, by (a).

Section 3.5 proves that every permutation of $\{1, \ldots, r\}$ is a product of adjacent transpositions; read for lists, every rearrangement is obtained by adjacent swaps, and so the product of a list in an abelian group does not depend on the order of the factors.

Marking scheme. (10 points) - 3: (a) brackets both products as $(g_1 \cdots g_{i-1})(\,\cdot\,)(g_{i+2} \cdots g_r)$, citing Proposition 3.1.2, with the empty product read as e when $i = 1$ or $i + 1 = r$. - 2: (a) uses $g_i g_{i+1} = g_{i+1} g_i$ (abelian) to conclude that the products agree. - 1: (b) names the induction and its variable, the number of swaps. - 2: (b) base case: zero swaps leave the list unchanged. - 2: (b) step: writes a rearrangement by $k + 1$ swaps as one swap after k swaps and applies (a) to the intermediate list. Fatal errors (0 for the step): (a) swaps the two entries inside a product written without brackets, with no appeal to the list-product laws; (b) "and so on" in place of an induction.

3.2 Subgroups and the Subgroups of the Integers

Section 3.1 defined groups and proved their basic laws. After a structure comes the substructure. The even integers sit inside $(\mathbb{Z}, +)$ and form a group on their own, with the same addition; so do the multiples of 7, of 12, and of 0, which is just $\{0\}$. Are there any other subgroups of $\mathbb{Z}$? *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.4 answered the same question for ideals, which are closed under multiplication by every integer (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.2). Here the multiplication is gone, and the answer is the same: this section proves that the subgroups of $(\mathbb{Z}, +)$ are exactly the sets $n\mathbb{Z}$ with $n \in \mathbb{N}$.

3.2.1 Subgroups

A subset of a group can fail to be a group with the inherited operation in three ways: a product can leave it, the identity can be missing, or an inverse can be missing. The definition rules out all three.

A subgroup is a subset that contains the identity and is closed under products and inverses.

Definition 3.2.1. Subgroup

Let G be a group. A subset $H \subseteq G$ is a **subgroup** of G if $e \in H$, and $ab \in H$ and $a^{-1} \in H$ **for all** $a, b \in H$.

In words: the identity of G is in H; multiplying two elements of H never leaves H; and the inverse in G of an element of H lies in H. We say "H is a subgroup of G" in words and use no symbol for it; in this chapter $\leq$ always means the order of $\mathbb{Z}$.

Then the operation of G restricts to a binary operation $H \times H \to H$, and H is a group with it:

(G1) holds in H because it holds in G, and (G2), (G3) hold because e and the inverses lie in H. The identity of the group H is the identity e of G, and the inverse of a in H is its inverse in G, by the uniqueness in Theorem 3.1.1 (1) and (2). Three conditions are a lot to check; in practice one checks that H is non-empty and a single combined condition.

Theorem 3.2.1. Subgroup Test

Let G be a group and $H \subseteq G$. Then H is a subgroup of G if and only if $H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$.

Proof. ($\Rightarrow$) If H is a subgroup, then $e \in H$, so $H \neq \emptyset$. For $a, b \in H$ we have $b^{-1} \in H$, and then $ab^{-1} \in H$, since H is closed under products.

($\Leftarrow$) Suppose $H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$. Pick $h \in H$. Taking $a = b = h$ gives $e = hh^{-1} \in H$. For $b \in H$, taking $a = e$ gives $b^{-1} = eb^{-1} \in H$. For $a, b \in H$, we now know $b^{-1} \in H$, so $ab = a(b^{-1})^{-1} \in H$ by Theorem 3.1.1 (3). Hence H is a subgroup. This proves the theorem.

■

In additive notation the test reads: $H \neq \emptyset$ and $a - b \in H$ for all $a, b \in H$, where $a - b := a + (-b)$.

Example. Subgroups

Check that each of the following is a subgroup.

(a) $\{e\}$ and G, in any group G.

(b) $n\mathbb{Z}$ in $(\mathbb{Z}, +)$, for $n \in \mathbb{Z}$; more generally $a\mathbb{Z} + b\mathbb{Z}$, for $a, b \in \mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.2.1).

(c) $\{1, -1\}$ and $\mathbb{Q}_{>0}$ in $(\mathbb{Q} \setminus \{0\}, \cdot)$.

(d) $\{[0], [2], [4]\}$ in $(\mathbb{Z}/6\mathbb{Z}, +)$; $\{[1], [3]\}$ in $(\mathbb{Z}/8\mathbb{Z})^\times$.

(e) In the group of bijections of a set X (Example (Groups) (c)), the bijections σ that fix a chosen point $x_0 \in X$, that is, $\sigma(x_0) = x_0$.

(f) $\{1, i, -1, -i\}$, the unit circle $\mathbb{T}$, and, for $n \geq 1$, the set μ_n of n-th roots of unity, in $(\mathbb{C} \setminus \{0\}, \cdot)$ (Chapter 1).

Solution. In each case we use Theorem 3.2.1, or Definition 3.2.1 directly.

(a) $\{e\}$ is non-empty, and $ee^{-1} = e$. G is non-empty, since $e \in G$, and $ab^{-1} \in G$ because the operation is a binary operation. The **trivial subgroup** $\{e\}$ is the smallest subgroup of every group: by the definition, every subgroup contains e.

(b) $0 = 0n \in n\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), with (F6)). For $kn, ln \in n\mathbb{Z}$,

$$kn - ln = kn + (-l)n = (k - l)n \in n\mathbb{Z},$$

by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c), then (F9) with (F6). In the same way $0 = a0 + b0 \in a\mathbb{Z} + b\mathbb{Z}$, and $(ax + by) - (ax' + by') = a(x - x') + b(y - y')$.

So both are subgroups, by the additive form of the test. For instance $2\mathbb{Z}$ is the set of even integers, and $0\mathbb{Z} = \{0\}$.

(c) For $\{1, -1\}$: $(-1)(-1) = 1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)), so each of $1, -1$ is its own inverse, and the products $1 \cdot 1 = 1$, $1 \cdot (-1) = -1$, $(-1)(-1) = 1$ lie in the set; so it is a subgroup by the definition. For $\mathbb{Q}_{>0}$: it contains 1, which is positive (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)). Let $a, b > 0$. Then $b^{-1} > 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.5.2 (a). So $ab^{-1} > 0$ by (O4), $\mathbb{Q}$ being an ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1).

(d) For classes, $[a]-[b] = [a-b]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (b)). For $a, b \in \{0, 2, 4\}$, the difference $a - b$ is one of $0, \pm 2, \pm 4$, and $[-2] = [4]$, $[-4] = [2]$ in $\mathbb{Z}/6\mathbb{Z}$ (since $6 \mid -2-4$ and $6 \mid -4-2$). So every difference lies in $\{[0], [2], [4]\}$. For $\{[1], [3]\}$: $[3]^{-1} = [3]$, since $[3][3] = [9] = [1]$, so the four quotients $[1][1]^{-1} = [1]$, $[1][3]^{-1} = [3]$, $[3][1]^{-1} = [3]$, $[3][3]^{-1} = [1]$ lie in the set.

(e) The identity map fixes x_0, so the set is non-empty. Let σ and τ fix x_0. Applying τ^{-1} to $\tau(x_0) = x_0$ gives $x_0 = \tau^{-1}(x_0)$, so $(\sigma \circ \tau^{-1})(x_0) = \sigma(x_0) = x_0$. Section 3.4 uses this subgroup for $X = \{1, \ldots, n+1\}$ and $x_0 = n + 1$.

(f) $\mathbb{C}$ is a field (Theorem 1.2.4), so $(\mathbb{C} \setminus \{0\}, \cdot)$ is a group by Example (Groups) (b). Recall that $i^2 = -1$ (Proposition 1.1.1, with the identification of $\mathbb{R}$ inside $\mathbb{C}$ made after it).

For $\{1, i, -1, -i\}$: products of two of ± 1 are ± 1, products of ± 1 with $\pm i$ are $\pm i$, and products of two of $\pm i$ are $\pm i^2 = \mp 1$ (signs by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)). So the set is closed under products, and it contains 1. Each of $1, -1$ is its own inverse, and $i(-i) = -i^2 = 1$, so $i^{-1} = -i$ and $(-i)^{-1} = i$. It is a subgroup by the definition.

For $\mathbb{T} = \{u \in \mathbb{C} : |u| = 1\}$: by Proposition 1.5.1 (a), which rests on the modulus rule $|zw| = |z||w|$ of Theorem 1.2.2 (d), $1 \in \mathbb{T}$, $uv \in \mathbb{T}$ for $u, v \in \mathbb{T}$, and each $u \in \mathbb{T}$ is non-zero with $u^{-1} = \overline{u} \in \mathbb{T}$. So $\mathbb{T} \subseteq \mathbb{C} \setminus \{0\}$, and $\mathbb{T}$ is a subgroup by the definition.

For μ_n, the set of $z \in \mathbb{C}$ with $z^n = 1$ (Chapter 1's notation, after Example (Roots of Unity)): $0 \notin \mu_n$, since $0^n = 0^{n-1} \cdot 0 = 0 \neq 1$ for $n \geq 1$; so $\mu_n \subseteq \mathbb{C} \setminus \{0\}$, and there z^n is the power of Definition 3.1.3, defined by the same recursion. Also $1 \in \mu_n$. For $\zeta, \eta \in \mu_n$, since $\mathbb{C} \setminus \{0\}$ is abelian,

$$(\zeta\eta^{-1})^n = \zeta^n(\eta^{-1})^n = \zeta^n(\eta^n)^{-1} = 1 \cdot 1^{-1} = 1,$$

by Proposition 3.1.3 (d) and (b). So $\zeta\eta^{-1} \in \mu_n$, and μ_n is a subgroup by the test. Chapter 1 also notes that $\mu_n \subseteq \mathbb{T}$. Its Section 1.6, Exercise R2 builds a bijection $\mathbb{Z}/n\mathbb{Z} \to \mu_n$ that sends sums to products; in the words of Section 3.3 this is an isomorphism of groups. That exercise rests on the facts about cosine and sine that Chapter 1 borrows, and nothing in this chapter cites it.

Now non-examples, each a minimal change of an example. The set $\mathbb{N} \subseteq \mathbb{Z}$ contains 0 and is closed under $+$, but $0 - 1 = -1 \notin \mathbb{N}$: the inverses are missing. The odd integers fail more badly: they do not contain 0, which is even ($0 = 2 \cdot 0$) and so not odd (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a)). And $\mathbb{Z}_{>0} \subseteq \mathbb{Q}_{>0}$ is non-empty and closed under multiplication, but $2^{-1} = 1/2 \notin \mathbb{Z}$: an integer m with $2m = 1$ would make 1 even, and $1 = 2 \cdot 0 + 1$ is odd. Each fails the test at one clause, and each is an infinite set; for a **finite** non-empty subset, closure under products alone suffices (Exercise C1).

Subgroups can be combined. If two subgroups are given, the elements they share form a subgroup again, and so do the elements shared by any family of subgroups:

Proposition 3.2.2. Intersections of Subgroups

Let G be a group and $(H_i)_{i\in I}$ a family of subgroups of G. Then $\bigcap_{i\in I} H_i$, taken inside G (Sets, Relations, and Cardinality, Definition 1.2.4 (b)), is a subgroup of G.

Proof. Write $H \coloneqq \bigcap_{i\in I} H_i$. Since $e \in G$ and $e \in H_i$ for every $i \in I$, $e \in H$, so $H \neq \emptyset$. Let $a, b \in H$. Then $ab^{-1} \in G$, and for each $i \in I$, $a, b \in H_i$, so $ab^{-1} \in H_i$ by Theorem 3.2.1 applied to the subgroup H_i. Hence $ab^{-1} \in H$, and H is a subgroup by Theorem 3.2.1. This proves the proposition.

■

For the empty family the intersection is G itself, which is a subgroup.

Warning. A union of two subgroups need not be a subgroup. $2\mathbb{Z} \cup 3\mathbb{Z}$ contains 3 and 2, but not $3 - 2 = 1$: $1 \notin 2\mathbb{Z}$ and $1 \notin 3\mathbb{Z}$, since neither 2 nor 3 divides 1 (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (g)). Intersections are safe; unions are not.

3.2.2 The subgroup generated by one element

Fix $g \in G$. Which subgroups contain g? Each of them contains gg, ggg, ..., and their inverses, so it contains every power g^n. The powers themselves form a subgroup, and so they are the smallest possible answer.

Definition 3.2.2. Subgroup Generated by an Element

Let G be a group and $g \in G$. The **subgroup generated by** g is

$$\langle g \rangle \coloneqq \{g^n : n \in \mathbb{Z}\},$$

with the powers of Definition 3.1.3. In additive notation, $\langle a \rangle = \{n \cdot a : n \in \mathbb{Z}\}$.

In $(\mathbb{Z}, +)$, $\langle n \rangle = \{k \cdot n : k \in \mathbb{Z}\} = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$, since the group multiple $k \cdot n$ is the product kn (Proposition 3.1.3 (e)). The name is justified by the next result.

Proposition 3.2.3. The Subgroup Generated by an Element

Let G be a group and $g \in G$. Then $\langle g \rangle$ is an abelian subgroup of G that contains g, and every subgroup of G that contains g contains $\langle g \rangle$.

Idea. Both halves are the power laws at work. The test asks for $g^m(g^n)^{-1}$, which the laws turn into the single power g^{m-n}. Conversely, a subgroup containing g is closed under products and inverses, and every power is built from g by those two operations.

Proof. First, $g = g^1 \in \langle g \rangle$, so $\langle g \rangle \neq \emptyset$. For $g^m, g^n \in \langle g \rangle$,

$$g^m (g^n)^{-1} = g^m g^{-n} = g^{m-n} \in \langle g \rangle,$$

by Proposition 3.1.3 (b) and (a); so $\langle g \rangle$ is a subgroup by Theorem 3.2.1. It is abelian: $g^m g^n = g^{m+n} = g^{n+m} = g^n g^m$, by Proposition 3.1.3 (a) and (F1) in $\mathbb{Z}$.

Now let H be a subgroup of G with $g \in H$. By Logic and Proof, Axiom 4.2.1, $g^n \in H$ for every $n \in \mathbb{N}$: $g^0 = e \in H$, and if $g^n \in H$, then $g^{n+1} = g^n g \in H$, since H is closed under products. For $n \in \mathbb{N}$, also $g^{-n} = (g^n)^{-1} \in H$ (Proposition 3.1.3 (b)), since H is closed under inverses. Every integer is n or $-n$ for some $n \in \mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 (c)), so $\langle g \rangle \subseteq H$. This proves the proposition.

■

So $\langle g \rangle$ is the smallest subgroup containing g. A group that equals $\langle g \rangle$ for one of its elements g is called cyclic; *Groups*, the chapter "Cyclic Groups", studies these groups and the least $m \geq 1$ with $g^m = e$.

Examples. If $g^m = e$ for some $m \geq 1$, the subgroup $\langle g \rangle$ is finite and easy to list. Indeed, divide any $n \in \mathbb{Z}$ by m: $n = qm + r$ with $0 \leq r < m$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2 (a)). Then

$$g^n = g^{mq} g^r = (g^m)^q g^r = e^q g^r = g^r,$$

by Proposition 3.1.3 (a) and (c), and $e^q = (g^0)^q = g^0 = e$ by (c) again. So $\langle g \rangle = \{g^0, g^1, \ldots, g^{m-1}\}$.

- In $(\mathbb{Z}/6\mathbb{Z}, +)$, $k \cdot [2] = [2k]$ for $k \in \mathbb{N}$, by Proposition 3.1.3 (c) and (e) and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d), where (e) identifies the group multiples with the ring multiples to which (d) applies: $k \cdot (2 \cdot [1]) = (2k) \cdot [1] = [2k]$. So the multiples are $[0], [2], [4]$, and $3 \cdot [2] = [6] = [0]$. By the paragraph above (with $m = 3$), $\langle [2] \rangle = \{[0], [2], [4]\}$, the subgroup of Example (Subgroups) (d).
- In $(\mathbb{Z}/7\mathbb{Z})^\times$, the powers of $[2]$ are $[1], [2], [4]$, and $[2]^3 = [8] = [1]$. So $\langle [2] \rangle = \{[1], [2], [4]\}$.
- In $(\mathbb{Z}/7\mathbb{Z})^\times$, the powers $[3]^1, \ldots, [3]^6$ are $[3], [2], [6], [4], [5], [1]$, each obtained from the one before by multiplying by $[3]$ (for instance $[6][3] = [18] = [4]$). Since $\mathbb{Z}/7\mathbb{Z}$ is a field (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2), $(\mathbb{Z}/7\mathbb{Z})^\times = (\mathbb{Z}/7\mathbb{Z}) \setminus \{[0]\}$, as in any field (the paragraph "Why this definition" after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1), so it has the six elements $[1], \ldots, [6]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)), and all of them are powers of $[3]$: $\langle [3] \rangle = (\mathbb{Z}/7\mathbb{Z})^\times$.

3.2.3 The subgroups of the integers

Every set $n\mathbb{Z} = \langle n \rangle$ is a subgroup of $(\mathbb{Z}, +)$. The theorem says that there are no others, and that n is determined by the subgroup.

Theorem 3.2.4. Subgroups of the Integers

Let H be a subgroup of $(\mathbb{Z}, +)$. Then $H = n\mathbb{Z}$ for **exactly one** $n \in \mathbb{N}$: $n = 0$ if $H = \{0\}$, and otherwise n is the least positive element of H.

Try it first (ten minutes): find the smallest subgroup of $\mathbb{Z}$ containing 6 and 15. List a few of its

elements, guess what it is, and say why its least positive element should divide 6.

Idea. The attempt finds elements by subtracting: $15-6=9$, $9-6=3$, and then every multiple of 3. That suggests "the multiples of 3", but listing gives no reason why nothing else can be in the subgroup. The guess also points at the right candidate for n: the **least positive** element, 3 here. Why should every element be a multiple of it? Divide an element a by n. The remainder is a minus a multiple of n, so it lies in the subgroup, and it is smaller than n. It cannot be positive, so it is 0. This is the move of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.2, **least positive element, then divide**, now with nothing but subtraction available.

Before reading on: where is $H \neq \{0\}$ *used, and why is the least* ***positive*** *element taken, not the least element?*

Proof. If $H=\{0\}$, then $H=0\mathbb{Z}$. Suppose $H\neq\{0\}$, and pick $a\in H$ with $a\neq 0$. Then $-a\in H$, and one of a, $-a$ is positive (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (h)). So $H\cap\mathbb{Z}_{>0}$ is non-empty, and it has the lower bound 0; by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6 it has a least element n, the least positive element of H.

($\supseteq$) Since $n\in H$ and $n\mathbb{Z}=\langle n\rangle$ (Proposition 3.1.3 (e)), Proposition 3.2.3 gives $n\mathbb{Z}\subseteq H$.

($\subseteq$) Let $a\in H$. Since $n>0$, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2 (a) gives $q,r\in\mathbb{Z}$ with $a=qn+r$ and $0\leq r<n$. Here $qn\in n\mathbb{Z}\subseteq H$, so $r=a-qn\in H$, since H is a subgroup. If $r>0$, then r is a positive element of H smaller than n, against the choice of n. So $r=0$, and $a=qn\in n\mathbb{Z}$.

Hence $H=n\mathbb{Z}$. For uniqueness, let $n\mathbb{Z}=m\mathbb{Z}$ with $n,m\in\mathbb{N}$. Then $n=1\cdot n\in m\mathbb{Z}$, so $m\mid n$, and in the same way $n\mid m$; hence $n=m$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (f). This proves the theorem.

■

The answer to the prompt. The hypothesis $H\neq\{0\}$ is used once, in the first paragraph: it supplies a non-zero element, hence a positive one, so that the set of positive elements of H is non-empty and has a least element. The least element of H itself does not exist when $H\neq\{0\}$: if m were least, then $m-n\in H$ and $m-n<m$. And $0\in H$ is useless as a divisor, since division with remainder needs a positive divisor; the minimality of n among the **positive** elements is exactly what forces $r=0$.

Remark. This is the statement of Number Systems: From \(\nN\) to \(\nR\), Exercise (C2: Closed under subtraction), an exercise in *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.4, promoted to a theorem, and it is the additive half of Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.2 (b). In $\mathbb{Z}$, being an ideal comes free: every subgroup $H=n\mathbb{Z}$ of $\mathbb{Z}$ is an ideal (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.1), since for $jn\in H$ and $k\in\mathbb{Z}$, $k(jn)=(kj)n\in n\mathbb{Z}$ by (F5).

The theorem turns questions about subgroups of $\mathbb{Z}$ into questions about one number: the least positive element.

Quick check. Which $n \in \mathbb{N}$ has $n\mathbb{Z} = 6\mathbb{Z} \cap 15\mathbb{Z}$?

Solution. $n = 30$. The intersection is a subgroup (Proposition 3.2.2), and it contains $30 = 5 \cdot 6 = 2 \cdot 15 \neq 0$, so by Theorem 3.2.4 it is $n\mathbb{Z}$ with n its least positive element, the least positive common multiple of 6 and 15. The positive multiples of 15 below 30 are 15 alone, and $15 = 2 \cdot 6 + 3$ is not a multiple of 6 (by the uniqueness of the remainder in Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2 (a)), while 30 is. So $n = 30$.

3.2.4 Exercises

3.2.4.1 A. Check your understanding

Exercise. A1

These parts are about the proof of Theorem 3.2.4.

(a) Where is the minimality of n used?

(b) Run the proof on $H = 4\mathbb{Z} + 6\mathbb{Z}$: find n, and the division of 6 by n.

(c) The conclusion fails for the subset $\mathbb{N}$ of $\mathbb{Z}$. Which condition of Definition 3.2.1 does $\mathbb{N}$ lack, and which step of the proof breaks?

(d) State the idea of the proof in two sentences.

Solution.

(a) In the step ($\subseteq$): the remainder r lies in H and $0 \leq r < n$, and minimality forbids $r > 0$, so $r = 0$.

(b) H is a subgroup (Example (Subgroups) (b)). Its least positive element is $n = 2$: $2 = 6 - 4 \in H$, and $1 \notin H$, since every element $4x + 6y = 2(2x + 3y)$ is even and 1 is odd (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a)). Dividing 6 by 2 gives $6 = 3 \cdot 2 + 0$, with remainder 0, as the proof predicts. So $H = 2\mathbb{Z}$.

(c) $\mathbb{N}$ lacks inverses: $1 \in \mathbb{N}$, but $-1 \notin \mathbb{N}$. The step ($\supseteq$) breaks: there $n = 1$, and $n\mathbb{Z} \subseteq H$ went through $n\mathbb{Z} = \langle n \rangle$ and Proposition 3.2.3, which needs a subgroup; indeed $-1 = (-1) \cdot 1 \notin \mathbb{N}$. The first paragraph's step $-a \in H$ also fails for $\mathbb{N}$ (take $a = 1$), but harmlessly: a non-zero $a \in \mathbb{N}$ is already positive, so $n = 1$ still exists. The step whose failure breaks the conclusion is ($\supseteq$). The other inclusion still holds for $\mathbb{N}$: each $a \in \mathbb{N}$ is $a = a \cdot 1 + 0$, so $\mathbb{N} \subseteq 1\mathbb{Z} = \mathbb{Z}$.

(d) The least positive element n of H is the only candidate. Division by n leaves a remainder in H smaller than n, so the remainder is 0 and every element is a multiple of n.

3.2.4.2 B. Practice

Exercise. B1: Put the proof in order

The following lines contain the proof of the direction ($\Leftarrow$) of Theorem 3.2.1, shuffled, together

with two lines that do not belong. Write the seven correct lines in an order that makes a proof, say which other orders are also admissible, and say why each of the other two lines fails.

(i) For $a, b \in H$, we know $b^{-1} \in H$.
(ii) Hence H is a subgroup of G.
(iii) Choose $h \in H$.
(iv) Taking $a = e$ and $b = h$: $h^{-1} = eh^{-1} \in H$; so $e = hh^{-1} \in H$.
(v) Suppose $H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$.
(vi) So $ab = a(b^{-1})^{-1} \in H$, by Theorem 3.1.1 (3).
(vii) For $b \in H$, taking $a = e$: $b^{-1} = eb^{-1} \in H$.
(viii) $ab \in H$, because H is closed under products.
(ix) Taking $a = b = h$: $e = hh^{-1} \in H$.

Solution. The admissible order is (v), (iii), (ix), (vii), (i), (vi), (ii). Each line uses the one before it: (iii) uses $H \neq \emptyset$ from (v); (ix) uses the h of (iii); (vii) takes $a = e$, which needs $e \in H$ from (ix); (i) is (vii) applied to an arbitrary b; (vi) needs $b^{-1} \in H$ from (i); and (ii) collects $e \in H$, inverses and products. So no other order is admissible: the dependencies form a single chain.

The distractor (iv) is circular. It takes $a = e$ in the hypothesis, which is allowed only once $e \in H$ is known, and then concludes $e \in H$. Placed before (ix), it uses what it is meant to prove; placed after (ix), its first half is a special case of (vii) and its second half repeats (ix).

The distractor (viii) assumes what is being proved: closure under products is one of the three conditions of Definition 3.2.1 that the direction ($\Leftarrow$) must establish, and the hypothesis (v) does not state it.

Exercise. B2: Subgroups of the integers modulo twelve

Determine which of the following subsets of $(\mathbb{Z}/12\mathbb{Z}, +)$ are subgroups. Justify your answer.

(a) $\{[0], [4], [8]\}$.
(b) $\{[0], [3], [6], [9]\}$.
(c) $\{[0], [5]\}$.
(d) $\{[0], [6]\}$.

Then show that every subgroup of $\mathbb{Z}/12\mathbb{Z}$ that contains $[5]$ is all of $\mathbb{Z}/12\mathbb{Z}$.

Solution. We use the additive form of Theorem 3.2.1, with $[a] - [b] = [a - b]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (b)).

(a) A subgroup. For $a, b \in \{0, 4, 8\}$, $a - b \in \{0, \pm 4, \pm 8\}$, and $[-4] = [8]$, $[-8] = [4]$, since 12 divides $-4 - 8$ and $-8 - 4$.
(b) A subgroup. For $a, b \in \{0, 3, 6, 9\}$, $a - b \in \{0, \pm 3, \pm 6, \pm 9\}$, and $[-3] = [9]$, $[-6] = [6]$, $[-9] = [3]$.
(c) Not a subgroup: $[0] - [5] = [-5] = [7]$, which is not in the set (the remainders 7, 0, 5

are distinct, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)). Equally, $[5]+[5]=[10]$ is not in the set.

(d) A subgroup: $[6]-[6]=[0]$, $[0]-[6]=[-6]=[6]$, and the other differences are $[0]$ and $[6]$.

Now let H be a subgroup with $[5]\in H$. By Proposition 3.2.3, $\langle[5]\rangle\subseteq H$, so $5\cdot[5]\in H$. By Proposition 3.1.3 (c) and (e) and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d), $5\cdot[5]=5\cdot(5\cdot[1])=25\cdot[1]=[25]=[1]$, since $25=2\cdot 12+1$. So $[1]\in H$, and then $k\cdot[1]=[k]\in H$ for every $k\in\mathbb{N}$ (Proposition 3.2.3, Proposition 3.1.3 (e) and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d) again). Taking $k=0,1,\dots,11$ gives every class of $\mathbb{Z}/12\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)). Hence $H=\mathbb{Z}/12\mathbb{Z}$.

Exercise. B3: Integer combinations, once more

Let $a,b\in\mathbb{Z}$, not both 0. Use Theorem 3.2.4 to prove that $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$, where d is the least positive element of $a\mathbb{Z}+b\mathbb{Z}$. Compare the proof with the one in *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.2.

Solution. $a\mathbb{Z}+b\mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$ (Example (Subgroups) (b)). It is not $\{0\}$: it contains $a=a\cdot 1+b\cdot 0$ and $b=a\cdot 0+b\cdot 1$, and one of them is non-zero. So by Theorem 3.2.4, $a\mathbb{Z}+b\mathbb{Z}=n\mathbb{Z}$ with n its least positive element, which is d.

This is Number Systems: From \(\nN\) to \(\nR\), Theorem 3.2.1 (e), whose d is the same least positive combination. The two proofs are one argument. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$ divided a and b by d and used that the remainder is again a combination; the proof of Theorem 3.2.4 divides an arbitrary element of the subgroup by n and uses only that a subgroup is closed under subtraction. The second form applies to every subgroup of $\mathbb{Z}$, not only to sets of combinations.

3.2.4.3 C. Going deeper

Exercise. C1: Finite subsets closed under products

Let G be a group, and let $H\subseteq G$ be finite, non-empty and closed under products ($ab\in H$ for all $a,b\in H$). Prove that H is a subgroup of G. Then explain why $\mathbb{N}\subseteq\mathbb{Z}$, which is non-empty and closed under $+$ but not a subgroup, does not contradict this.

The first half of a proof is given.

> Let $h\in H$, and let $k:=|H|$ (Sets, Relations, and Cardinality, Definition 3.1.2). The powers $h,h^2,\dots,h^{k+1}$ all lie in H, by induction on the exponent, since $h^{j+1}=h^jh$.

The last half is blank. *Name the move, then complete it.*

Solution. The move is **multiply by the inverse**: two equal powers $h^i=h^j$ become $e=h^{j-i}$ once h^i is removed from both sides.

Completion. The map $\{1, \ldots, k+1\} \to H$, $j \mapsto h^j$, goes from a set with $k+1$ elements to a set with k elements, so it is not injective (Sets, Relations, and Cardinality, Corollary 3.1.3 (a)): $h^i = h^j$ for some $1 \leq i < j \leq k+1$. Multiplying both sides on the left by $(h^i)^{-1} = h^{-i}$ gives

$$e = h^{-i}h^i = h^{-i}h^j = h^{j-i}$$

(Proposition 3.1.3 (b), (a)). Since $1 \leq j - i \leq k$, h^{j-i} is one of the listed powers, so $e \in H$. Next, if $j - i \geq 2$, then $h\,h^{j-i-1} = h^{j-i-1}h = h^{j-i} = e$ (Proposition 3.1.3 (a)), so $h^{-1} = h^{j-i-1}$ by Theorem 3.1.1 (2), and $h^{j-i-1} \in H$ since $1 \leq j - i - 1 \leq k$. If $j - i = 1$, then $h = h^1 = e$, and $h^{-1} = e \in H$. As $h \in H$ was arbitrary, H is closed under inverses; it contains e and is closed under products, so it is a subgroup by Definition 3.2.1.

The set $\mathbb{N}$ is not finite, so the result does not apply to it. Read backwards, the result even proves this: if $\mathbb{N}$ were finite, it would be a subgroup of $\mathbb{Z}$, and it is not, since $-1 \notin \mathbb{N}$.

Marking scheme. (10 points) - 1: names the move (multiply by the inverse, or cancel h^i). - 2: gets $h^i = h^j$ with $1 \leq i < j \leq k+1$ from the pigeonhole principle, cited. - 2: derives $h^{j-i} = e$ with the power laws named, and concludes $e \in H$ from $1 \leq j - i \leq k$. - 3: shows $h^{-1} \in H$: $h^{-1} = h^{j-i-1}$ when $j - i \geq 2$, and $h = e$ when $j - i = 1$. - 1: concludes that H is a subgroup, by Definition 3.2.1 or Theorem 3.2.1. - 1: explains that $\mathbb{N}$ is infinite, so the result does not apply. Fatal errors (0 for the step): $h^0 = e$ taken as one of the listed powers (the list starts at h^1); $h^{-1} \in H$ asserted without exhibiting it as a positive power; the case $j - i = 1$ mishandled so that h^0 is claimed to lie in the list.

Exercise. C2: Exit check: subgroups of the integers

State and prove Theorem 3.2.4.

Solution (Hint 1). Look at the positive elements of H, and take the least one.

Solution (Hint 2). To show that an element $a \in H$ is a multiple of that least positive element n, divide a by n.

Solution. The statement and proof of Theorem 3.2.4 are a complete answer. In outline: $H = \{0\} = 0\mathbb{Z}$, or H has a non-zero element a, and then a or $-a$, both in H, is positive; the least positive element n exists by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6; $n\mathbb{Z} \subseteq H$ because H is a subgroup containing n (all multiples kn, negative k included); for $a \in H$, $a = qn + r$ with $0 \leq r < n$ and $r = a - qn \in H$, so $r = 0$ by minimality; and $n\mathbb{Z} = m\mathbb{Z}$ with $n, m \in \mathbb{N}$ forces $n = m$.

Marking scheme. (10 points) - 3: the case $H = \{0\}$; otherwise the existence of a positive element, with the reason when the chosen element is negative (its inverse lies in H). - 1: the least positive element, by a cited well-ordering result for sets of integers bounded below. - 2: $n\mathbb{Z} \subseteq H$ by closure, with the negative multiples included. - 2: division of $a \in H$ by n, with the remainder shown to lie in H. - 1: minimality of n forces $r = 0$. - 1: uniqueness of $n \in \mathbb{N}$. Fatal errors (0 for the step): assuming that H is an ideal, or citing Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.2 for H (closure under multiplication by integers is not

given; that it comes free is a consequence of the theorem); "the least element of H" without positivity. A proof by induction showing $kn \in H$ for $k \in \mathbb{N}$, followed by inverses for $k < 0$, earns the 2 points for $n\mathbb{Z} \subseteq H$. A descent proof (for $a \in H$ with $a \geq 0$, strong induction on a: if $a \geq n$, then $a - n \in H$ and $0 \leq a - n < a$; negative a handled through $-a \in H$) earns the 2 points for division when it shows $a - n \in H$ and treats negative a, and the 1 point for minimality when it rules out $0 < a < n$.

Exercise. C3: Inclusions and intersections

Let $m, n \in \mathbb{Z}_{>0}$.

(a) Prove that $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if $n \mid m$.

(b) Prove that $m\mathbb{Z} \cap n\mathbb{Z} = L\mathbb{Z}$, where L is the least positive common multiple of m and n. Deduce that L divides every common multiple of m and n.

Solution (Hint 1). For (a), ask where m itself lies. For (b), ask what kind of set the intersection is.

Solution (Hint 2). For (b): $m\mathbb{Z} \cap n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ by Proposition 3.2.2, and mn lies in it.

Solution.

(a) ($\Rightarrow$) $m = 1 \cdot m \in m\mathbb{Z} \subseteq n\mathbb{Z}$, so $m = kn$ for some $k \in \mathbb{Z}$, that is, $n \mid m$. ($\Leftarrow$) If $m = kn$, then every $jm = (jk)n$ lies in $n\mathbb{Z}$, by (F5).

(b) By Proposition 3.2.2, $m\mathbb{Z} \cap n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. It contains $mn = n \cdot m = m \cdot n$, which is positive by (O4), so it is not $\{0\}$. By Theorem 3.2.4 it equals $L\mathbb{Z}$, with L its least positive element. Its elements are exactly the common multiples of m and n, so L is the least positive common multiple. A common multiple c lies in $m\mathbb{Z} \cap n\mathbb{Z} = L\mathbb{Z}$, so $L \mid c$.

This is Number Systems: From \(\nN\) to \(\nR\), Exercise (B2: The least common multiple), there proved by dividing c by L directly; here the division is done once and for all inside Theorem 3.2.4.

Marking scheme. (10 points) - 2: (a) ($\Rightarrow$) uses $m \in m\mathbb{Z}$ to get $m = kn$. - 1: (a) ($\Leftarrow$) shows $jm = (jk)n \in n\mathbb{Z}$. - 2: (b) the intersection is a subgroup of $(\mathbb{Z}, +)$, by Proposition 3.2.2. - 2: (b) it is not $\{0\}$ (mn is a positive element), so Theorem 3.2.4 gives $L\mathbb{Z}$ with L its least positive element. - 2: (b) identifies the intersection with the set of common multiples, so L is the least positive common multiple. - 1: (b) deduces $L \mid c$ for every common multiple c. Fatal errors (0 for the step): (b) applies Theorem 3.2.4 without checking that the intersection is a subgroup; (b) assumes $L = mn$ or $L = mn/\gcd(m, n)$ without proof.

3.3 Homomorphisms and Isomorphisms

Section 3.1 named the pattern shared by $(\mathbb{Z}, +)$, the units of a ring and the bijections of a set, and Section 3.2 looked inside one group at a time, at its subgroups. This section compares two groups. A map between groups that respects the two operations is a homomorphism; a bijective one is an isomorphism, and it says that two groups differ only in the names of their elements. The elements a homomorphism sends to the identity form its kernel, a subgroup that measures how much the map forgets.

3.3.1 Maps that respect the operation

Write out the addition table of $\mathbb{Z}/2\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2) and the multiplication table of $\{1, -1\} \subseteq \mathbb{Z}$, the group $\mathbb{Z}^\times$ of Proposition 3.1.4:

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	1	-1
1	1	-1
-1	-1	1

Rename $[0]$ as 1 and $[1]$ as -1, and the first table becomes the second, entry for entry. The two groups are the same table with different names. The renaming is a function φ with $\varphi([0]) = 1$ and $\varphi([1]) = -1$, and "entry for entry" says that the entry for a, b is sent to the entry for $\varphi(a), \varphi(b)$: $\varphi(a+b) = \varphi(a)\varphi(b)$. Maps with this property are worth having even when they are not bijections. The map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $a \mapsto [a]$, keeps only the parity of an integer, and it still turns sums into sums.

A homomorphism is a map between groups that sends products to products; an isomorphism is a bijective one, a renaming of the elements.

Definition 3.3.1. Group Homomorphism

Let G and H be groups. A function $\varphi\colon G \to H$ is a **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$ **for all** $a, b \in G$. A **bijective** homomorphism is an **isomorphism**. The groups G and H are **isomorphic**, written $G \cong H$, if **there exists** an isomorphism $G \to H$. The **kernel** of φ is

$$\ker \varphi := \{g \in G : \varphi(g) = e_H\},$$

where e_H is the identity of H.

In words: the product ab on the left is taken in G, and the product $\varphi(a)\varphi(b)$ on the right is taken in H. So "φ respects the operation" compares two different operations, and either group may be written additively. For $\varphi\colon (\mathbb{Z}/2\mathbb{Z}, +) \to (\{1, -1\}, \cdot)$ above, the condition reads $\varphi(a+b) = \varphi(a)\varphi(b)$. The kernel is a subset of the **source** G; the identity it is measured against is that of the **target** H. We write e_G and e_H whenever both groups are in play.

The definition asks for one equation and nothing else. It does not ask that $\varphi(e_G) = e_H$ or that φ respect inverses: both follow, by Theorem 3.3.1 below. This differs from the field homomorphisms of Chapter 2, which must send 1 to 1 by a clause of their own: the map sending every element of a field to 0 respects $+$ and $\cdot$, yet $1 \mapsto 0$. In a group, every element can be canceled, and that is what makes the clause redundant.

Two homomorphisms exist between any two groups, or from any group to itself:

- the **trivial homomorphism** $G \to H$, $g \mapsto e_H$: since $e_H e_H = e_H$ by (G2), $\varphi(ab) = e_H = \varphi(a)\varphi(b)$. Its kernel is all of G. It forgets everything.
- the **identity** $\mathrm{id}_G \colon G \to G$: $\mathrm{id}_G(ab) = ab = \mathrm{id}_G(a)\,\mathrm{id}_G(b)$. It is bijective (Sets, Relations, and Cardinality, Theorem 1.5.4, with inverse id_G), so it is an isomorphism, and its kernel is $\{e_G\}$. It forgets nothing.

These two extremes are why we say that the kernel measures what φ forgets: the larger $\ker\varphi$, the more elements φ sends to the same place. Proposition 3.3.3 below makes the slogan exact at the end where nothing is forgotten.

The product of two groups. Several examples below have a pair of groups as their target. For groups G and H, take the set $G \times H$ of pairs (Sets, Relations, and Cardinality, Definition 1.3.2) with the operation in each coordinate:

$$(g, h)(g', h') \coloneqq (gg', hh').$$

This is a binary operation on $G \times H$, since $gg' \in G$ and $hh' \in H$. It makes $G \times H$ a group, the **product** of G and H:

- (G1) For $(g, h), (g', h'), (g'', h'') \in G \times H$, both bracketings give $(gg'g'', hh'h'')$, because (G1) holds in G in the first coordinate and in H in the second.
- (G2) $(e_G, e_H)(g, h) = (e_G g, e_H h) = (g, h)$, and $(g, h)(e_G, e_H) = (g, h)$ in the same way.
- (G3) $(g, h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H)$, and $(g^{-1}, h^{-1})(g, h) = (e_G, e_H)$ in the same way.

If G and H are abelian, so is $G \times H$, coordinate by coordinate. For abelian groups written additively, the product is written additively too, $(g, h) + (g', h') = (g + g', h + h')$; this is the componentwise sum on $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ of Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3 (b).

Example. Homomorphisms

Check that each map is a homomorphism, and find its kernel.

(a) For $n \in \mathbb{Z}_{>0}$, the map $(\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$, $a \mapsto [a]$.

(b) For a group G and $g \in G$, the map $(\mathbb{Z}, +) \to G$, $k \mapsto g^k$. Find its image as well.

(c) For a group G and $g \in G$, **conjugation by** g, $c_g \colon G \to G$, $c_g(x) \coloneqq gxg^{-1}$. Show that it is an isomorphism, and that it is the identity map exactly when g commutes with every element of G.

(d) For an **abelian** group G, the map $G \to G$, $x \mapsto x^2$.

(e) For $m, n \in \mathbb{Z}_{>0}$ with $\gcd(m, n) = 1$, the map $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $[x]_{mn} \mapsto ([x]_m, [x]_n)$, of additive groups. Show that it is an isomorphism.

(f) The modulus $(\mathbb{C} \setminus \{0\}, \cdot) \to (\mathbb{R}_{>0}, \cdot)$, $z \mapsto |z|$, where $\mathbb{R}_{>0} \coloneqq \{x \in \mathbb{R} : x > 0\}$.

Then show that $x \mapsto x + 1$ is **not** a homomorphism $(\mathbb{Z}, +) \to (\mathbb{Z}, +)$.

Solution.

(a) $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group by Example (Groups) (a). By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (c), applied to the ideal $n\mathbb{Z}$ of $\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2), $[a+b] = [a]+[b]$: a homomorphism. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (d), $[a] = [0]$ exactly when $a \in n\mathbb{Z}$, so the kernel is $n\mathbb{Z}$. Every element of $\mathbb{Z}/n\mathbb{Z}$ is a class $[a]$, so the map is surjective.

(b) By Proposition 3.1.3 (a), $g^{k+l} = g^k g^l$ for all $k, l \in \mathbb{Z}$, which is the homomorphism property with $+$ in the source and the product of G in the target. The kernel is $\{k \in \mathbb{Z} : g^k = e_G\}$. The image is $\{g^k : k \in \mathbb{Z}\} = \langle g \rangle$, by Definition 3.2.2. For instance, for the group $G = (\mathbb{Z}/7\mathbb{Z})^\times$ (Proposition 3.1.4) and $g = [3]$, the image is all of $(\mathbb{Z}/7\mathbb{Z})^\times$: the powers $[3]^0, \ldots, [3]^5$ are $[1], [3], [2], [6], [4], [5]$, and $[3]^6 = [1]$, so 6 lies in the kernel.

(c) For $x, y \in G$, inserting $e = g^{-1}g$ between x and y and dropping brackets (Proposition 3.1.2 (b)),

$$c_g(x)c_g(y) = gxg^{-1}gyg^{-1} = gxeyg^{-1} = gxyg^{-1} = c_g(xy).$$

So c_g is a homomorphism. Next, since $(g^{-1})^{-1} = g$ (Theorem 3.1.1 (3)),

$$c_{g^{-1}}(c_g(x)) = g^{-1}gxg^{-1}g = x,$$

and in the same way $c_g(c_{g^{-1}}(x)) = gg^{-1}xgg^{-1} = x$. So $c_{g^{-1}}$ is a two-sided inverse of c_g (Sets, Relations, and Cardinality, Definition 1.5.2), and c_g is bijective (Sets, Relations, and Cardinality, Theorem 1.5.4): an isomorphism. Finally, $c_g = \mathrm{id}_G$ means $gxg^{-1} = x$ for every x (Sets, Relations, and Cardinality, Proposition 1.4.1). Multiplying on the right by g turns $gxg^{-1} = x$ into $gx = xg$, and multiplying $gx = xg$ on the right by g^{-1} turns it back. So $c_g = \mathrm{id}_G$ exactly when $gx = xg$ for every $x \in G$. In an abelian group every conjugation is the identity. The kernel of c_g is $\{e\}$: if $gxg^{-1} = e$, then $x = c_{g^{-1}}(e) = g^{-1}eg = e$.

(d) Since G is abelian, $xy = yx$, and Proposition 3.1.3 (d) gives $(xy)^2 = x^2y^2$. The kernel is $\{x \in G : x^2 = e\}$. In $(\mathbb{Z}/7\mathbb{Z})^\times$ the squares of $[1], \ldots, [6]$ are $[1], [4], [2], [2], [4], [1]$, so the kernel is $\{[1], [6]\}$. In $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1], [3], [5], [7]\}$ the squares are $[1], [9], [25], [49]$, all equal to $[1]$, so the kernel is the whole group.

(e) The target is the product of the groups $(\mathbb{Z}/m\mathbb{Z}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$, written additively. The rule is the map Φ of Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3 (b), a well-defined bijection, and it satisfies $\Phi([x]_{mn}+[y]_{mn}) = \Phi([x]_{mn})+\Phi([y]_{mn})$ with the componentwise sum, which is the product operation above. So it is an isomorphism of additive groups, and its kernel is $\{[0]_{mn}\}$. For example, $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, since $1 = 4 - 3$ shows $\gcd(3, 4) = 1$ (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.2.2).

(f) $\mathbb{C}$ is a field (Theorem 1.2.4), so $(\mathbb{C}\setminus\{0\}, \cdot)$ is a group by Example (Groups) (b). $(\mathbb{R}_{>0}, \cdot)$ is a group by the rules of the ordered field $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.3.3): a product of positive reals is positive by (O4), associativity and the identity law are (F5)–(F7), and $1 > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)). For $x > 0$ we have $x \neq 0$ by (O1), so x^{-1} exists by (F8), and it is positive by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.5.2 (a). For $z \neq 0$, $|z| \geq 0$ by its definition as a non-negative square root (Definition 1.2.1) and $|z| \neq 0$ by Theorem 1.2.2 (e), so $|z| \in \mathbb{R}_{>0}$. The homomorphism property is $|zw| = |z||w|$, Theorem 1.2.2 (d). The kernel is $\{z \in \mathbb{C} : |z| = 1\} = \mathbb{T}$, the unit circle of Proposition 1.5.1.

The non-example. Let $\varphi(x) := x + 1$. Then $\varphi(0 + 0) = 1$, while $\varphi(0) + \varphi(0) = 2$. So $\varphi(0+0) \neq \varphi(0)+\varphi(0)$, and φ is not a homomorphism. It is a minimal change of the identity map $x \mapsto x$, which is one: the shift keeps the map bijective and destroys only the equation.

Part (b) says that every element g of every group is the image of 1 under a homomorphism out of $\mathbb{Z}$. Part (c) gives the first isomorphisms of a group with itself that can differ from the identity: $c_g \neq \mathrm{id}_G$ exactly when g fails to commute with some element of G, as for the two swaps of the fold after Example (Groups) (c), there called f, g: writing h for the second, $c_f(h) = f \circ h \circ f^{-1} \neq h$ because $f \circ h \neq h \circ f$. Part (f) shows a kernel that is not a set of integers.

3.3.2 Basic properties of homomorphisms

The definition asks only for products. Identities, inverses and powers come with them, and kernels and images are subgroups.

Theorem 3.3.1. Basic Properties of Homomorphisms

Let $\varphi\colon G \to H$ be a homomorphism of groups, and let $a \in G$.

(a) $\varphi(e_G) = e_H$.
(b) $\varphi(a^{-1}) = \varphi(a)^{-1}$.
(c) $\ker\varphi$ is a subgroup of G.
(d) $\varphi(a^n) = \varphi(a)^n$ for every $n \in \mathbb{Z}$.
(e) The image $\varphi(G)$ is a subgroup of H.

Idea. For (a), apply φ to $e_G e_G = e_G$: the equation $\varphi(e_G)\varphi(e_G) = \varphi(e_G)$ has the shape $gg = g$, and **multiply by the inverse** of $\varphi(e_G)$ leaves $\varphi(e_G) = e_H$. For (b), $\varphi(a^{-1})$ undoes $\varphi(a)$, and inverses are unique. Then (c) and (e) are the subgroup test, and (d) is induction along the definition of powers.

Proof.

(a) Since $e_G e_G = e_G$ by (G2) in G, and $\varphi(e_G) = \varphi(e_G)e_H$ by (G2) in H,

$$\varphi(e_G)\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G) = \varphi(e_G)e_H.$$

Canceling $\varphi(e_G)$ on the left (Theorem 3.1.1 (4)) gives $\varphi(e_G) = e_H$.

(b) By the homomorphism property, (G3) in G and (a),

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_G) = e_H,$$

and in the same way $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = e_H$. So $\varphi(a^{-1})$ is an inverse of $\varphi(a)$, and since inverses are unique (Theorem 3.1.1 (2)), $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(c) By (a), $e_G \in \ker\varphi$, so $\ker\varphi \neq \emptyset$. Let $x, y \in \ker\varphi$. By the homomorphism property and (b),

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1} = e_H,$$

where $e_H^{-1} = e_H$ because $e_H e_H = e_H$ and inverses are unique. So $xy^{-1} \in \ker\varphi$, and $\ker\varphi$ is a subgroup by the subgroup test (Theorem 3.2.1).

(d) First let $n \in \mathbb{N}$; we use induction on n (Logic and Proof, Axiom 4.2.1). For $n = 0$, $\varphi(a^0) = \varphi(e_G) = e_H = \varphi(a)^0$ by Definition 3.1.3 and (a). If $\varphi(a^n) = \varphi(a)^n$, then by the recursion $a^{n+1} = a^n a$ of Definition 3.1.3, in G and in H,

$$\varphi(a^{n+1}) = \varphi(a^n a) = \varphi(a^n)\varphi(a) = \varphi(a)^n\varphi(a) = \varphi(a)^{n+1}.$$

Now let $n < 0$, and write $n = -m$ with $m \in \mathbb{N}$. By Definition 3.1.3, $a^n = (a^{-1})^m$ and $\varphi(a)^n = (\varphi(a)^{-1})^m$. By the case just proved, applied to a^{-1}, and by (b),

$$\varphi(a^n) = \varphi((a^{-1})^m) = \varphi(a^{-1})^m = (\varphi(a)^{-1})^m = \varphi(a)^n.$$

(e) By Sets, Relations, and Cardinality, Definition 1.6.1, $\varphi(G) = \{\varphi(x) : x \in G\} \subseteq H$. It contains $\varphi(e_G)$, so it is non-empty. For two of its elements $\varphi(x)$ and $\varphi(y)$, with $x, y \in G$, the homomorphism property and (b) give

$$\varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}) \in \varphi(G).$$

So $\varphi(G)$ is a subgroup by Theorem 3.2.1. This proves the theorem.

■

So a homomorphism carries the whole structure of Section 3.1, identity, inverses and powers, and not just the products it was defined by. In additive notation, (a), (b) and (d) read $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$ and $\varphi(n \cdot a) = n \cdot \varphi(a)$. Conversely to Example (Homomorphisms) (b), every homomorphism $\varphi\colon (\mathbb{Z}, +) \to G$ is $k \mapsto \varphi(1)^k$: $k = k \cdot 1$ (Proposition 3.1.3 (e)), so $\varphi(k) = \varphi(1)^k$ by (d). Part (c) gives a supply of subgroups: the unit circle $\mathbb{T}$ is a subgroup of $\mathbb{C} \setminus \{0\}$ because it is the kernel of the modulus (Example (Homomorphisms) (f)), and $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ because it is the kernel of $a \mapsto [a]$.

Quick check. Is $a \mapsto 3a$ a homomorphism $(\mathbb{Z}, +) \to (\mathbb{Z}, +)$? What is its kernel? Is it an isomorphism?

Solution. Yes: $3(a + b) = 3a + 3b$ by distributivity in $\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1). The kernel is $\{0\}$, since $3a = 0$ with $3 \neq 0$ forces $a = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (f)). It is injective, since $3a = 3b$ gives $3(a - b) = 0$ and so $a = b$ by the same rule, but **not** surjective: 1 is not of the form $3a$, since $3 \nmid 1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (g)). So it is not an isomorphism.

Homomorphisms compose, and the inverse of an isomorphism is again one. These are the facts that let "isomorphic" behave like "equal up to renaming".

Proposition 3.3.2. Composites and Inverses of Homomorphisms

Let G, H and K be groups.

(a) If $\varphi\colon G \to H$ and $\psi\colon H \to K$ are homomorphisms, then so is $\psi \circ \varphi\colon G \to K$.

(b) If $\varphi\colon G \to H$ is an isomorphism, then its inverse function $\varphi^{-1}\colon H \to G$ is an isomorphism.

(c) id_G is an isomorphism. Consequently $G \cong G$; if $G \cong H$, then $H \cong G$; and if $G \cong H$ and $H \cong K$, then $G \cong K$.

Idea. Part (a) is the homomorphism property applied twice. For (b), we cannot compute φ^{-1} directly, but we can compare $\varphi^{-1}(xy)$ with $\varphi^{-1}(x)\varphi^{-1}(y)$ after applying φ, which is injective.

Proof.

(a) For $a, b \in G$, by Sets, Relations, and Cardinality, Definition 1.4.2 and the homomorphism property of φ and then of ψ,

$$(\psi \circ \varphi)(ab) = \psi(\varphi(a)\varphi(b)) = \psi(\varphi(a))\,\psi(\varphi(b)) = (\psi \circ \varphi)(a)\,(\psi \circ \varphi)(b).$$

(b) Since φ is bijective, it has a two-sided inverse φ^{-1} (Sets, Relations, and Cardinality, Theorem 1.5.4), which is bijective by the same theorem, with inverse φ. Let $x, y \in H$. Then, since φ is a homomorphism and $\varphi \circ \varphi^{-1} = \mathrm{id}_H$,

$$\varphi(\varphi^{-1}(x)\,\varphi^{-1}(y)) = \varphi(\varphi^{-1}(x))\,\varphi(\varphi^{-1}(y)) = xy = \varphi(\varphi^{-1}(xy)).$$

Since φ is injective, $\varphi^{-1}(x)\varphi^{-1}(y) = \varphi^{-1}(xy)$. So φ^{-1} is a homomorphism, and being bijective, an isomorphism.

(c) id_G is an isomorphism (the second of the two homomorphisms listed after Definition 3.3.1), so $G \cong G$. If $\varphi\colon G \to H$ is an isomorphism, so is $\varphi^{-1}\colon H \to G$ by (b). If $\varphi\colon G \to H$ and $\psi\colon H \to K$ are isomorphisms, then $\psi \circ \varphi$ is a homomorphism by (a) and bijective by Sets, Relations, and Cardinality, Theorem 1.4.4 (c). This proves the proposition.

■

The kernel was introduced to measure what a homomorphism forgets. At the end where it forgets nothing, the measurement is exact:

Proposition 3.3.3. Injective Exactly When the Kernel Is Trivial

A homomorphism $\varphi\colon G \to H$ is injective **if and only if** $\ker\varphi = \{e_G\}$.

Idea. Injectivity compares two elements a, b with the same image; the kernel looks at one element with the image e_H. The quotient ab^{-1} turns the first question into the second: $\varphi(a) = \varphi(b)$ says exactly that ab^{-1} lies in the kernel.

Proof. ($\Rightarrow$) Suppose φ is injective. By Theorem 3.3.1 (a), $e_G \in \ker\varphi$. If $g \in \ker\varphi$, then $\varphi(g) = e_H = \varphi(e_G)$, so $g = e_G$ by injectivity. Hence $\ker\varphi = \{e_G\}$.

($\Leftarrow$) Suppose $\ker\varphi = \{e_G\}$, and let $a, b \in G$ with $\varphi(a) = \varphi(b)$. By the homomorphism property and Theorem 3.3.1 (b),

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = \varphi(b)\varphi(b)^{-1} = e_H.$$

So $ab^{-1} \in \ker\varphi$, that is, $ab^{-1} = e_G$. **Multiply by the inverse:** multiplying on the right by b and using (G1)–(G3), $a = ab^{-1}b = e_Gb = b$. So φ is injective. This proves the proposition.

■

To decide injectivity we now check one equation, $\varphi(g) = e_H$, instead of all pairs a, b. Linear maps in linear algebra satisfy the same statement, with the same proof read additively: *Spaces and Maps*, the chapter "Linear Maps", proves that a linear map is injective exactly when its kernel is $\{0\}$.

Quick check. Use the proposition to show that $k \mapsto [3]^k$, from $(\mathbb{Z}, +)$ to $(\mathbb{Z}/7\mathbb{Z})^\times$, is not injective.

Solution. It is a homomorphism by Example (Homomorphisms) (b). Its kernel contains 6, since $[3]^6 = [729] = [1]$ ($729 = 104 \cdot 7 + 1$). So the kernel is not $\{0\}$, and by Proposition 3.3.3 the map is not injective; indeed $[3]^0 = [3]^6$.

3.3.3 Isomorphic and non-isomorphic groups

An isomorphism is a renaming, so we expect two isomorphic groups to agree on every property that is stated with the operation alone. For the three properties used here this is a one-line check; let $\varphi\colon G \to H$ be an isomorphism. A bijection preserves the number of elements. If G is abelian, then any two elements of H are $\varphi(a), \varphi(b)$, and $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a)$. And $x^2 = e_G$ exactly when $\varphi(x)^2 = e_H$, by the homomorphism property, Theorem 3.3.1 (a) and injectivity, so φ maps the solutions of $x^2 = e$ in G bijectively onto those in H. This gives a method in both directions. To show $G \cong H$, write down a bijection and check the homomorphism property. To show $G \ncong H$, find such a property that one group has and the other lacks.

Example. Isomorphic and Non-Isomorphic Small Groups

(a) Show that $(\mathbb{Z}/2\mathbb{Z}, +) \cong (\{1, -1\}, \cdot)$.

(b) Show that $(\mathbb{Z}/4\mathbb{Z}, +) \cong ((\mathbb{Z}/5\mathbb{Z})^\times, \cdot)$, by $[k] \mapsto [2]^k$.

(c) Show that $(\mathbb{Z}/4\mathbb{Z}, +)$ and $((\mathbb{Z}/8\mathbb{Z})^\times, \cdot)$ are **not** isomorphic.

(d) Show that $(\mathbb{Z}, +) \cong (2\mathbb{Z}, +)$, by $x \mapsto 2x$.

Solution.

(a) By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b), each element of $\mathbb{Z}/2\mathbb{Z}$ is $[r]$ for exactly one $r \in \{0, 1\}$, so $\varphi([0]) := 1$, $\varphi([1]) := -1$ defines a function. It is bijective, since it pairs off the two elements. The homomorphism property is the

comparison of the two tables at the start of the section, four equations:

$$\varphi([0]+[0]) = \varphi([0]) = 1 = 1\cdot 1, \qquad \varphi([0]+[1]) = \varphi([1]) = -1 = 1\cdot(-1),$$
$$\varphi([1]+[0]) = \varphi([1]) = -1 = (-1)\cdot 1, \quad \varphi([1]+[1]) = \varphi([0]) = 1 = (-1)(-1),$$

using $[1]+[1] = [2] = [0]$ and $(-1)(-1) = 1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c)).

(b) The target is a group by Proposition 3.1.4. Its elements are the four non-zero classes $[1], [2], [3], [4]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b), (c)): each is a unit, since $[1][1] = [1]$, $[2][3] = [6] = [1]$ and $[4][4] = [16] = [1]$, while $[0]$ is not, since $[0][v] = [0] \neq [1]$.
Well defined. The rule must not depend on the representative k. The powers $[2]^0, [2]^1, [2]^2, [2]^3, [2]^4$ are $[1], [2], [4], [8] = [3], [16] = [1]$. If $[k] = [k']$ in $\mathbb{Z}/4\mathbb{Z}$, then $k' - k \in 4\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (a)), so $k' = k + 4q$ for some $q \in \mathbb{Z}$, and by Proposition 3.1.3 (a) and (c),

$$[2]^{k'} = [2]^k([2]^4)^q = [2]^k[1]^q = [2]^k,$$

where $[1]^q = ([2]^0)^q = [2]^{0\cdot q} = [1]$, again by (c).
Homomorphism. $[k]+[l] = [k+l] \mapsto [2]^{k+l} = [2]^k[2]^l$, by Proposition 3.1.3 (a).
Bijective. The four distinct classes $[0], [1], [2], [3]$, which are all of $\mathbb{Z}/4\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)), go to $[1], [2], [4], [3]$: four different elements, which are all of $(\mathbb{Z}/5\mathbb{Z})^\times$. So the map is injective and surjective.

(c) Both groups have four elements (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)). In $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1], [3], [5], [7]\}$ (the even classes are not units: $[0]$, and $[2][4] = [4][2] = [6][4] = [0]$ with $[4], [2] \neq [0]$, and a unit is not a zero divisor, the paragraph after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1), every element y has $y^2 = [1]$: the squares are $[1]$, $[9] = [1]$, $[25] = [1]$, $[49] = [1]$. Suppose $\varphi\colon \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/8\mathbb{Z})^\times$ were an isomorphism. Then, by the homomorphism property and Theorem 3.3.1 (a),

$$\varphi([2]) = \varphi([1]+[1]) = \varphi([1])^2 = [1] = \varphi([0]).$$

Since $[2] \neq [0]$ in $\mathbb{Z}/4\mathbb{Z}$, this contradicts injectivity. So no isomorphism exists.

(d) $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ (Example (Subgroups) (b)), so a group. The map $x \mapsto 2x$ is a homomorphism by distributivity, $2(x+y) = 2x + 2y$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1). It is surjective onto $2\mathbb{Z}$ by the definition of $2\mathbb{Z}$, and injective because its kernel is $\{0\}$: $2x = 0$ forces $x = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (f)), and Proposition 3.3.3 applies. So $\mathbb{Z} \cong 2\mathbb{Z}$: a group can be isomorphic to a subgroup of itself other than itself.

The square of Section 3.1, turned by quarter turns, gives another group with four elements; once its rotations are written as permutations, Exercise B3 of Section 3.4 matches them with $\mathbb{Z}/4\mathbb{Z}$.

Warning. Two groups with the same number of elements need not be isomorphic. $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/8\mathbb{Z})^\times$ both have four elements, yet part (c) shows that no isomorphism exists between them. Equal counts decide nothing by themselves: different counts prove $G \ncong H$, but equal counts never prove $G \cong H$. To prove $G \ncong H$, find a property that an isomorphism would carry over and that one group has and the other lacks; in (c) it was "some element x has $x^2 \neq e$", which holds in $\mathbb{Z}/4\mathbb{Z}$ (in additive form, $[1]+[1] \neq [0]$) and fails in $(\mathbb{Z}/8\mathbb{Z})^\times$.

Remark (Where homomorphisms go next). In linear algebra, a linear map is in particular a homomorphism of the additive groups, and its kernel is the kernel of this section (*Spaces and Maps*, the chapter "Linear Maps"). The determinant will be a homomorphism from the invertible matrices to $F^\times$ (*Determinants and the Structure of Operators*, the chapter "Determinants"). Quotient groups and the isomorphism theorems are in *Groups*, the chapter "Normal Subgroups, Quotient Groups, and the Isomorphism Theorems".

Remark (Field homomorphisms as group homomorphisms). In the terms of Chapter 2 (no proof in this chapter rests on this remark): a field homomorphism $\varphi\colon F \to L$ (Definition 2.4.1) is a homomorphism of the additive groups $(F,+) \to (L,+)$; it sends $F^\times$ into $L^\times$, and is a homomorphism of these multiplicative groups (Proposition 2.4.1 (a)–(c)). The automorphisms of F form a group under composition (Proposition 2.4.1 (e)), a subgroup of the group of bijections of F (Example (Groups) (c)). And the multiplicative group $\mathbb{F}_p^\times$ of the field with p elements is the group $(\mathbb{Z}/p\mathbb{Z})^\times$ of Proposition 3.1.4.

3.3.4 Exercises

3.3.4.1 A. Check your understanding

Exercise. A1

(a) In the proof of ($\Leftarrow$) of Proposition 3.3.3, where is it used that φ is a homomorphism?

(b) The map $\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $a \mapsto ([a],[a])$, is a homomorphism of additive groups. Find its kernel.

(c) True or false: a homomorphism $\varphi\colon G \to H$ sends every subgroup K of G onto a subgroup $\varphi(K)$ of H. Justify your answer.

(d) The map $x \mapsto x+1$ on $(\mathbb{Z},+)$ sends 0 to 1. Could it become a homomorphism $(\mathbb{Z},+) \to (\mathbb{Z},+)$ if 1 were declared the identity of the target, keeping its operation $+$? Explain.

Solution.

(a) In the first displayed step, $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}$: the homomorphism property gives $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1})$, and Theorem 3.3.1 (b), itself a consequence of the homomorphism property, gives $\varphi(b^{-1}) = \varphi(b)^{-1}$. Without it, $\varphi(a) = \varphi(b)$ says nothing about ab^{-1}.

(b) The map is a homomorphism into the product group, coordinate by coordinate (Example (Homomorphisms) (a) in each coordinate). Its kernel is $\{a : [a]_6 = [0]_6 \text{ and } [a]_4 = [0]_4\} = 6\mathbb{Z} \cap 4\mathbb{Z}$, by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (d). This is a subgroup of $\mathbb{Z}$ (Proposition 3.2.2), so it is $d\mathbb{Z}$ with d its least positive element (Theorem 3.2.4). The positive multiples of 6 are $6, 12, \ldots$, and $4 \nmid 6$, $4 \mid 12$; so $d = 12$ and the kernel is $12\mathbb{Z}$.

(c) True. A subgroup K is a group with the operation of G (the paragraph after Definition 3.2.1), and the restriction of φ to K is a homomorphism $K \to H$, since the homomorphism property for $a, b \in K$ is a special case of that for $a, b \in G$. Its image is $\varphi(K)$, a subgroup of H by Theorem 3.3.1 (e).

(d) No. The identity of a group is not chosen; it is the element with (G2), and it is unique (Theorem 3.1.1 (1)). In $(\mathbb{Z},+)$ it is 0, since $1+1\neq 1$. Every homomorphism into $(\mathbb{Z},+)$ must send 0 to 0 (Theorem 3.3.1 (a)), and $x\mapsto x+1$ does not. Changing the operation does change the identity: with $a*b\coloneqq a+b-1$, the check of Exercise (A1) (b) with -1 in place of $+1$ shows that $(\mathbb{Z},*)$ is a group: both bracketings of $a*b*c$ equal $a+b+c-2$, the identity is 1, and the inverse of a is $2-a$. The map $x\mapsto x+1$ is a bijection $\mathbb{Z}\to\mathbb{Z}$ (its inverse is $x\mapsto x-1$), and $(a+1)*(b+1)=(a+b)+1$, so it is an isomorphism $(\mathbb{Z},+)\to(\mathbb{Z},*)$. But that is a different group.

3.3.4.2 B. Practice

Exercise. B1

Find all homomorphisms $(\mathbb{Z},+)\to(\mathbb{Z}/6\mathbb{Z},+)$, and the kernel of each.

Hint: Theorem 3.3.1 (d), applied to $k=k\cdot 1$.

Solution. Let φ be a homomorphism and write $\varphi(1)=[c]$ with $c\in\{0,\dots,5\}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)). For $k\in\mathbb{Z}$, $k=k\cdot 1$ in $(\mathbb{Z},+)$ (Proposition 3.1.3 (e)), so Theorem 3.3.1 (d), in additive notation, gives

$$\varphi(k)=\varphi(k\cdot 1)=k\cdot\varphi(1)=k\cdot[c].$$

So φ is determined by c. Conversely, for each c, the map $k\mapsto k\cdot[c]$ is a homomorphism by Example (Homomorphisms) (b) with $g=[c]$. So there are exactly six homomorphisms, one for each class $[c]$.

Kernels. The quotient map $a\mapsto[a]$ is a homomorphism (Example (Homomorphisms) (a)), so Theorem 3.3.1 (d) and Proposition 3.1.3 (e) give $k\cdot[c]=[k\cdot c]=[kc]$. Hence, since $[kc]=[0]$ exactly when $kc\in 6\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (d)), the kernel is $\{k\in\mathbb{Z}:6\mid kc\}$, a subgroup of $\mathbb{Z}$, so it is $d\mathbb{Z}$ with d the least positive k with $6\mid kc$ (Theorem 3.2.4). Running through $k=1,2,\dots$:

c	0	1	2	3	4	5
least k with $6\mid kc$	1	6	3	2	3	6
kernel	$\mathbb{Z}$	$6\mathbb{Z}$	$3\mathbb{Z}$	$2\mathbb{Z}$	$3\mathbb{Z}$	$6\mathbb{Z}$

For instance, for $c=4$: 4, 8 are not multiples of 6, and 12 is. For $c=5$: $5,10,15,20,25$ are not, and 30 is.

Exercise. B2

(a) Let G and H be groups. Show that $G\to G\times H$, $g\mapsto(g,e_H)$, is an injective homomorphism into the product group.

(b) Show that $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ (additive groups) are not isomorphic.

Solution.

(a) For $g, g' \in G$, $(gg', e_H) = (gg', e_H e_H) = (g, e_H)(g', e_H)$, by (G2) in H and the definition of the product operation. The kernel is $\{g : (g, e_H) = (e_G, e_H)\} = \{e_G\}$, since two pairs are equal exactly when their coordinates are. By Proposition 3.3.3 the map is injective.

(b) The invariant is that of Example (Isomorphic and Non-Isomorphic Small Groups) (c). In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, every element satisfies $x + x = 0$: $([a], [b]) + ([a], [b]) = ([2a], [2b]) = ([0], [0])$. Suppose $\varphi\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ were an isomorphism. Then

$$\varphi([2]) = \varphi([1] + [1]) = \varphi([1]) + \varphi([1]) = ([0], [0]) = \varphi([0])$$

by Theorem 3.3.1 (a), against injectivity, since $[2] \neq [0]$ in $\mathbb{Z}/4\mathbb{Z}$. An isomorphism in the other direction would have an inverse that is an isomorphism (Proposition 3.3.2 (b)), so it cannot exist either.

Exercise. B3

Give an example of a homomorphism from $(\mathbb{Q} \setminus \{0\}, \cdot)$ **onto** $(\{1, -1\}, \cdot)$, and find its kernel.

Solution. What any answer must have. A function $\varphi\colon \mathbb{Q} \setminus \{0\} \to \{1, -1\}$ with $\varphi(xy) = \varphi(x)\varphi(y)$ for all non-zero x, y, taking **both** values 1 and -1. Its kernel is then a subgroup (Theorem 3.3.1 (c)) that is not the whole group.

One answer: the sign. Let $\varphi(x) := 1$ if $x > 0$ and $\varphi(x) := -1$ if $x < 0$. This defines a function on $\mathbb{Q}\setminus\{0\}$, since the order of $\mathbb{Q}$ is total (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1; Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (i)). By the rules of the ordered field $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (c), (d)), the product of two positives is positive, of a positive and a negative is negative, and of two negatives is positive. In each of the four cases $\varphi(xy) = \varphi(x)\varphi(y)$: for example, if $x > 0 > y$, then $xy < 0$ and $\varphi(xy) = -1 = 1 \cdot (-1)$. Both values are taken, at 1 and -1. The kernel is $\mathbb{Q}_{>0}$.

Other answers exist. For instance, writing a non-zero rational as $\pm 2^k a/b$ with a, b odd, the parity of k gives another one; we do not prove that this is well defined here.

3.3.4.3 C. Going deeper

Exercise. C1

(a) Let $\varphi\colon G \to H$ be a homomorphism, with G abelian. Prove that the subgroup $\varphi(G)$ of H is abelian.

(b) Deduce that there is no homomorphism from $\mathbb{Z}/6\mathbb{Z}$ **onto** the group of bijections of $\{1, 2, 3\}$.

Solution.

(a) Let $u, v \in \varphi(G)$, say $u = \varphi(a)$ and $v = \varphi(b)$ with $a, b \in G$ (Sets, Relations, and

Cardinality, Definition 1.6.1). Then

$$uv = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = vu,$$

using that G is abelian in the middle step.

(b) $\mathbb{Z}/6\mathbb{Z}$ is abelian (Example (Groups) (a)). If φ were a homomorphism from it onto the group of bijections of $\{1,2,3\}$, then that group would be $\varphi(\mathbb{Z}/6\mathbb{Z})$, abelian by (a). It is not: the bijections f swapping $1,2$ and g swapping $2,3$ satisfy $(f \circ g)(1) = f(1) = 2$ and $(g \circ f)(1) = g(2) = 3$, as in the fold after Example (Groups) (c). So no such homomorphism exists. (Size alone could not decide this: Section 3.4 shows that both groups have six elements.)

Marking scheme. (10 points) - 2: (a) writes arbitrary $u, v \in \varphi(G)$ as $\varphi(a), \varphi(b)$. - 3: (a) the chain $uv = \varphi(ab) = \varphi(ba) = vu$, with the homomorphism property and commutativity of G named. - 1: (b) notes that $\mathbb{Z}/6\mathbb{Z}$ is abelian. - 1: (b) "onto" makes the target equal to $\varphi(\mathbb{Z}/6\mathbb{Z})$, so (a) applies. - 3: (b) exhibits two bijections of $\{1,2,3\}$ that do not commute, with a point where the two composites differ. Fatal errors (0 for the step): (a) takes u, v in all of H rather than in the image; (b) argues from the number of elements alone.

Exercise. C2

Let $\varphi\colon G \to H$ be a homomorphism and $a, b \in G$.

(a) Prove that the following are equivalent: (i) $\varphi(a) = \varphi(b)$; (ii) $ab^{-1} \in \ker\varphi$; (iii) $a^{-1}b \in \ker\varphi$.

(b) Deduce that the set of elements with the same image as a, the **fiber** $\varphi^{-1}(\{\varphi(a)\})$, equals $\{ak : k \in \ker\varphi\}$.

(c) For the quotient map $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$, $x \mapsto [x]$, write out the fiber of 7.

Solution.

(a) (i) $\Rightarrow$ (ii): as in the proof of Proposition 3.3.3, $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = \varphi(b)\varphi(b)^{-1} = e_H$.

(ii) $\Rightarrow$ (i): if $\varphi(ab^{-1}) = e_H$, then $\varphi(a)\varphi(b)^{-1} = e_H$; multiplying on the right by $\varphi(b)$, $\varphi(a) = \varphi(b)$.

(iii) $\Leftrightarrow$ (iii): the same two arguments with $a^{-1}b$: $\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b)$ (Theorem 3.3.1 (b)), which is e_H exactly when $\varphi(b) = \varphi(a)$, multiplying on the left by $\varphi(a)$ or by $\varphi(a)^{-1}$.

(b) ($\subseteq$) Let b lie in the fiber, so $\varphi(b) = \varphi(a)$. By (a), $k := a^{-1}b \in \ker\varphi$, and $b = a(a^{-1}b) = ak$. ($\supseteq$) If $k \in \ker\varphi$, then $\varphi(ak) = \varphi(a)e_H = \varphi(a)$.

(c) The kernel is $5\mathbb{Z}$ (Example (Homomorphisms) (a)), so by (b) the fiber of 7 is $\{7 + 5j : j \in \mathbb{Z}\} = \{\ldots, -3, 2, 7, 12, \ldots\}$, the class $[7] = [2]$ itself. The sets $\{ak : k \in \ker\varphi\}$ are the **cosets** of the kernel, which *Groups*, the chapter "Cosets and Lagrange's Theorem", studies for every subgroup.

Marking scheme. (10 points) - 2: (a) (i) $\Rightarrow$ (ii), using $\varphi(b^{-1}) = \varphi(b)^{-1}$, cited. - 2: (a) (ii) $\Rightarrow$ (i), multiplying by $\varphi(b)$ on the right. - 2: (a) (i) $\Leftrightarrow$ (iii), both directions, by the mirror argument. - 2: (b) both inclusions, with $k := a^{-1}b$ for ($\subseteq$). - 2: (c) kernel $5\mathbb{Z}$, and the fiber

$\{7 + 5j : j \in \mathbb{Z}\}$. Fatal errors (0 for the step): (a) "divides" by $\varphi(b)$, or uses commutativity of H; (b) proves one inclusion and calls it equality.

3.4 Permutations and Cycle Notation

Shuffle three cards, then shuffle them again. Two shuffles in a row are a shuffle, every shuffle can be undone, and the order of the two shuffles matters. This is the group of bijections of a finite set (Example (Groups) (c)), and it is the one group of this chapter studied in detail, because every determinant in linear algebra is built from it. This section gives it a compact notation, cycle notation, learns to multiply in it, counts its elements, and proves that every permutation breaks into independent loops: **follow the orbit, then peel it off**.

3.4.1 Permutations and two-line notation

Section 3.1 showed that the bijections of a set form a group under composition. On the set $\{1, \dots, n\}$ they are the rearrangements of n objects, and they get a name of their own.

A permutation is a rearrangement: a bijection of a set to itself.

Definition 3.4.1. Permutations and the Symmetric Group

Let X be a set. A **permutation** of X is a bijection $X \to X$. The permutations of X, with the operation $\sigma\tau := \sigma \circ \tau$, form the group S_X of Example (Groups) (c). For $n \in \mathbb{N}$, the **symmetric group** is

$$S_n := S_{\{1,\dots,n\}},$$

where $\{1, \dots, n\}$ is empty for $n = 0$. The **support** of $\sigma \in S_X$ is the set of points it moves,

$$\operatorname{supp}\sigma := \{x \in X : \sigma(x) \neq x\}.$$

In words: S_X is not a new group. It is the group of bijections of X, with the product written as juxtaposition. Its identity is id_X, written id when X is clear, and the inverse of σ is the inverse function σ^{-1} (Sets, Relations, and Cardinality, Definition 1.5.2). The support of id is empty, and the support is empty only for id: if $\sigma(x) = x$ for every x, then $\sigma = \mathrm{id}_X$ (Sets, Relations, and Cardinality, Proposition 1.4.1).

The product is read right to left. In S_X the product $\sigma\tau$ is the composite $\sigma \circ \tau$: **first apply τ, then** σ, exactly as $g \circ f$ applies f first (Sets, Relations, and Cardinality, Definition 1.4.2). So $(\sigma\tau)(x) = \sigma(\tau(x))$, and a longer product $\sigma_1\sigma_2 \cdots \sigma_r$ applies σ_r first and σ_1 last.

Two-line notation. A permutation $\sigma \in S_n$ is given by its values, and we write them under the points:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

This array is a **table** of values, not a matrix. For example, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \in S_4$ sends $1 \mapsto 3$, $2 \mapsto 1$, $3 \mapsto 2$ and fixes 4; its support is $\{1, 2, 3\}$. The bottom row of a permutation lists each of $1, \dots, n$ exactly once: once at least, because σ is surjective, and at most once, because it is injective.

The smallest symmetric groups. S_0 has one element, the empty function $\emptyset \to \emptyset$ (Sets,

Relations, and Cardinality, Proposition 1.4.2 (a)), which is a bijection because there is nothing to check; it is the trivial group. S_1 has one element, id, since the only function $\{1\} \to \{1\}$ sends $1 \mapsto 1$. S_2 has two elements, id and the permutation swapping 1 and 2: a bijection of $\{1, 2\}$ either fixes 1, and then also 2, or sends $1 \mapsto 2$, and then $2 \mapsto 1$. These degenerate cases are where inductions on n start, here and in Section 3.5.

3.4.2 Cycles

Two-line notation lists every value, even the values of points that do not move. Most permutations met in practice move a few points around a loop and leave the rest alone, and a notation that records only the loop is shorter and shows more.

A cycle moves a list of distinct points one step along the list, the last back to the first, and fixes everything else.

Definition 3.4.2. Cycle, Transposition

Let $n \in \mathbb{N}$ and $k \geq 2$, and let $i_1, \ldots, i_k \in \{1, \ldots, n\}$ be **distinct**. The **k-cycle** $(i_1\ i_2\ \cdots\ i_k) \in S_n$ is the permutation γ with

$$\gamma(i_j) \coloneqq i_{j+1} \quad \text{for } 1 \leq j < k, \qquad \gamma(i_k) \coloneqq i_1,$$

and $\gamma(x) \coloneqq x$ for every $x \in \{1, \ldots, n\}$ not among $i_1, \ldots, i_k$. A 2-cycle $(i\ j)$ is a **transposition**. Two cycles are **disjoint** if their supports are disjoint.

In words: $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$, and the points off the list stay put. A transposition $(i\ j)$ swaps i and j.

Well-definedness. Because the entries are distinct, each point of $\{1, \ldots, n\}$ receives exactly one value from the rule, so γ is a function. It is a bijection: the cycle $(i_k\ \cdots\ i_2\ i_1)$, the list read backwards, undoes it point by point ($i_{j+1} \mapsto i_j$ and $i_1 \mapsto i_k$, and the other points are fixed by both), so it is a two-sided inverse and Sets, Relations, and Cardinality, Theorem 1.5.4 applies. Hence

$$(i_1\ i_2\ \cdots\ i_k)^{-1} = (i_k\ \cdots\ i_2\ i_1).$$

Every entry is moved, since $i_{j+1} \neq i_j$ and $i_1 \neq i_k$ by distinctness and $k \geq 2$; so $\operatorname{supp}(i_1\ \cdots\ i_k) = \{i_1, \ldots, i_k\}$. A transposition is its own inverse: $(i\ j)(i\ j) = \mathrm{id}$.

Examples. In S_4, (1 2 3) sends $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$ and fixes 4; in two-line notation it is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$. The same cycle may be written starting at any of its entries: $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$, since all three describe the loop $1 \mapsto 2 \mapsto 3 \mapsto 1$. But $(1\ 3\ 2)$ is a different permutation: it sends $1 \mapsto 3$. The cycles (1 2) and (3 4) are disjoint; (1 2) and (2 3) are not.

↻ **Second reading** · *Why a cycle has at least two entries*

The identity is not a cycle. The definition asks for $k \geq 2$: a "1-cycle" (i) would be the identity, and so would every one of them, so the notation would not be telling us anything. The identity is instead the empty product of cycles (Definition 3.1.2), and that is how it will appear in the decomposition theorem below.

Quick check. Which of these are equal in S_4: (2 4 1), (1 2 4), (1 4 2)? Write the one that differs in two-line notation.

Solution. (2 4 1) is the loop $2 \mapsto 4 \mapsto 1 \mapsto 2$, and (1 2 4) is the same loop started at 1: both send $1 \mapsto 2$, $2 \mapsto 4$, $4 \mapsto 1$ and fix 3. So they are equal. (1 4 2) runs the loop backwards: it sends $1 \mapsto 4$, $4 \mapsto 2$, $2 \mapsto 1$, so it differs from the other two at 1. In two-line notation it is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$; it is the inverse of the other two.

Products of cycles are computed by following each point through the factors, **from right to left**.

Example. Computing with Cycles

In S_3, compute (1 3)(1 2) and (1 2)(1 3). In S_5, write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

as a product of cycles.

Solution. For (1 3)(1 2), follow each point through (1 2) first, then (1 3): $1 \mapsto 2 \mapsto 2$, $2 \mapsto 1 \mapsto 3$, $3 \mapsto 3 \mapsto 1$. So (1 3)(1 2) = (1 2 3). For (1 2)(1 3): $1 \mapsto 3 \mapsto 3$, $3 \mapsto 1 \mapsto 2$, $2 \mapsto 2 \mapsto 1$. So (1 2)(1 3) = (1 3 2). The two products differ, so S_3 is not abelian. For every $n \geq 3$, the same two transpositions lie in S_n, the same computation applies at $1, 2, 3$, and both products fix every point ≥ 4; so S_n is not abelian for every $n \geq 3$.

For σ, start at 1 and follow: $1 \mapsto 3 \mapsto 1$, a loop (1 3). The smallest point not yet used is 2: $2 \mapsto 5 \mapsto 4 \mapsto 2$, a loop (2 5 4). Every point is now used, so σ = (1 3)(2 5 4). To check, follow each point through (2 5 4) first, then (1 3): $1 \mapsto 1 \mapsto 3$, $2 \mapsto 5 \mapsto 5$, $3 \mapsto 3 \mapsto 1$, $4 \mapsto 2 \mapsto 2$, $5 \mapsto 4 \mapsto 4$, which is the bottom row $3, 5, 1, 2, 4$. The two cycles move disjoint sets of points, and the product in the other order, (2 5 4)(1 3), is also σ, as the same check shows.

↻ **Second reading** · *The small symmetric groups are abelian*

For S_n with $n \leq 2$ the situation is different: S_0, S_1 and S_2 have at most two elements, and any two of their elements commute, since one of them is id or both are equal. So S_n is abelian exactly when $n \leq 2$.

Warning. **Mind the order.** $\sigma\tau$ applies τ first, as $g \circ f$ applies f first. Reading a product of cycles from left to right gives a wrong answer: read that way, (1 3)(1 2) would send $1 \mapsto 3 \mapsto 3$, $3 \mapsto 1 \mapsto 2$, $2 \mapsto 2 \mapsto 1$, that is, "(1 3 2)"; but the example computed

$(1\ 3)(1\ 2) = (1\ 2\ 3)$. The left-to-right reading computes the product in the other order.

Section 3.1 noted that the power law $(gh)^n = g^n h^n$ of Proposition 3.1.3 (d) needs $gh = hg$. In S_3 it fails without that hypothesis.

Warning. $(\sigma\tau)^2 = \sigma^2\tau^2$ is false in general. Take $\sigma = (1\ 2)$ and $\tau = (1\ 3)$. By the example, $\sigma\tau = (1\ 3\ 2)$, and $(1\ 3\ 2)(1\ 3\ 2)$ sends $1 \mapsto 3 \mapsto 2$, $2 \mapsto 1 \mapsto 3$, $3 \mapsto 2 \mapsto 1$, so $(\sigma\tau)^2 = (1\ 2\ 3)$. But transpositions are their own inverses, so $\sigma^2\tau^2 = \mathrm{id} \cdot \mathrm{id} = \mathrm{id}$. Here $\sigma\tau \neq \tau\sigma$, and the law fails.

Quick check. Compute $(1\ 2\ 3)(1\ 2)$ in S_3.

Solution. Apply $(1\ 2)$ first: $1 \mapsto 2 \mapsto 3$, $2 \mapsto 1 \mapsto 2$, $3 \mapsto 3 \mapsto 1$. So 1 and 3 are swapped and 2 is fixed: $(1\ 2\ 3)(1\ 2) = (1\ 3)$.

3.4.3 Counting permutations

How many permutations does S_n have? There are n choices for $\sigma(1)$, then $n-1$ for $\sigma(2)$, and so on, which suggests $n!$. We make this precise by induction on n, and the induction needs one structural fact: the permutations of $\{1, \dots, n+1\}$ that fix the last point are, in effect, the permutations of $\{1, \dots, n\}$. Section 3.5 uses the same fact for a different induction.

Lemma 3.4.1. Permutations Fixing the Last Point

Let $n \in \mathbb{N}$, and let $S' := \{\sigma \in S_{n+1} : \sigma(n+1) = n+1\}$, a subgroup of S_{n+1}.

(a) For $\sigma \in S'$, the restriction σ' of σ to $\{1, \dots, n\}$, with codomain $\{1, \dots, n\}$, is a permutation of $\{1, \dots, n\}$.

(b) The map $S' \to S_n$, $\sigma \mapsto \sigma'$, is an isomorphism. Its inverse sends $\rho \in S_n$ to its **extension** $\bar{\rho} \in S'$, defined by $\bar{\rho}(i) := \rho(i)$ for $i \leq n$ and $\bar{\rho}(n+1) := n+1$.

That S' is a subgroup is Example (Subgroups) (e), with $X = \{1, \dots, n+1\}$ and the chosen point $n+1$.

Idea. A permutation fixing $n+1$ cannot send any other point to $n+1$, since that value is taken; so it maps $\{1, \dots, n\}$ into itself. It also reaches every point there, because whatever reaches $j \leq n$ cannot be $n+1$. Restricting and extending undo each other, and restriction respects composition.

Proof.

(a) Let $\sigma \in S'$ and $i \in \{1, \dots, n\}$. If $\sigma(i) = n+1 = \sigma(n+1)$, then $i = n+1$ by injectivity, which is false; so $\sigma(i) \in \{1, \dots, n\}$, and $\sigma' \colon \{1, \dots, n\} \to \{1, \dots, n\}$, $\sigma'(i) := \sigma(i)$, is

a function. It is injective because σ is. It is surjective: for $j \in \{1, \dots, n\}$ there is $i \in \{1, \dots, n+1\}$ with $\sigma(i) = j$, since σ is surjective, and $i \neq n+1$, since $\sigma(n+1) = n+1 \neq j$. So $\sigma' \in S_n$.

(b) Write $R(\sigma) \coloneqq \sigma'$ and $E(\rho) \coloneqq \bar{\rho}$.

E maps into S'. The extension $\bar{\rho}$ is a function on $\{1, \dots, n+1\}$ with values in that set, and $\overline{\rho^{-1}}$ undoes it point by point: for $i \leq n$, $\overline{\rho^{-1}}(\bar{\rho}(i)) = \rho^{-1}(\rho(i)) = i$, and both fix $n+1$; the other composite is the same with ρ and ρ^{-1} exchanged. So $\bar{\rho}$ is a bijection (Sets, Relations, and Cardinality, Theorem 1.5.4) fixing $n+1$.

R and E are mutually inverse. For $\sigma \in S'$, $\overline{\sigma'}$ agrees with σ at every $i \leq n$ and at $n+1$, so $E(R(\sigma)) = \sigma$ (Sets, Relations, and Cardinality, Proposition 1.4.1). For $\rho \in S_n$, $(\bar{\rho})'$ agrees with ρ at every $i \leq n$, so $R(E(\rho)) = \rho$. Hence R is a bijection with inverse E (Sets, Relations, and Cardinality, Definition 1.5.2, Sets, Relations, and Cardinality, Theorem 1.5.4).

R is a homomorphism. Let $\sigma, \tau \in S'$ and $i \leq n$. By (a), $\tau(i) \leq n$, so

$$(\sigma\tau)'(i) = \sigma(\tau(i)) = \sigma'(\tau'(i)) = (\sigma'\tau')(i).$$

So $(\sigma\tau)' = \sigma'\tau'$, and R is an isomorphism. Its inverse E is an isomorphism by Proposition 3.3.2 (b). This proves the lemma.

■

So inside S_{n+1} sits a copy of S_n, the permutations that leave the last point alone. The factorial $n!$ is that of Sets, Relations, and Cardinality, Definition 2.3.1, read in $\mathbb{N}$: $0! = 1$ and $(n+1)! = n!\,(n+1)$.

Proposition 3.4.2. The Symmetric Group Has n! Elements

For every $n \in \mathbb{N}$, S_n is finite and has $n!$ elements: $|S_n| = n!$.

Idea. Sort the permutations of $\{1, \dots, n+1\}$ by where they send the last point. Those sending it to $n+1$ are a copy of S_n, by the lemma. Those sending it to $k \leq n$ are matched with the first kind by composing with the swap $(k \;\; n{+}1)$. So there are $n+1$ classes of $n!$ permutations each.

Proof. We use induction on n (Logic and Proof, Axiom 4.2.1). For $n = 0$, S_0 has exactly one element, the empty function (Sets, Relations, and Cardinality, Proposition 1.4.2 (a)), and $0! = 1$.

Suppose S_n has $n!$ elements. For $k \in \{1, \dots, n+1\}$ let

$$A_k \coloneqq \{\sigma \in S_{n+1} : \sigma(n+1) = k\}.$$

Every $\sigma \in S_{n+1}$ lies in exactly one A_k, namely for $k = \sigma(n+1)$. So the sets $A_1, \dots, A_{n+1}$ are pairwise disjoint and their union is S_{n+1}.

The class A_{n+1}. A_{n+1} is the subgroup S' of Lemma 3.4.1. By the induction hypothesis there is a bijection $\{1, \dots, n!\} \to S_n$ (Sets, Relations, and Cardinality, Definition 3.1.2);

composing it with the bijection $S_n \to S'$ of the lemma gives a bijection $\{1, \dots, n!\} \to A_{n+1}$ (Sets, Relations, and Cardinality, Theorem 1.4.4 (c)). So A_{n+1} has $n!$ elements.

The classes A_k, $k \leq n$. Let $\tau := (k \;\; n{+}1)$, a transposition with $\tau\tau = \mathrm{id}$. If $\sigma \in A_k$, then $(\tau\sigma)(n+1) = \tau(k) = n+1$, so $\tau\sigma \in A_{n+1}$; if $\rho \in A_{n+1}$, then $(\tau\rho)(n+1) = \tau(n+1) = k$, so $\tau\rho \in A_k$. The maps $A_k \to A_{n+1}$, $\sigma \mapsto \tau\sigma$, and $A_{n+1} \to A_k$, $\rho \mapsto \tau\rho$, are mutually inverse, since $\tau(\tau\sigma) = (\tau\tau)\sigma = \sigma$ by (G1), $\tau\tau = \mathrm{id}$ and (G2), and likewise for ρ. So $\sigma \mapsto \tau\sigma$ is a bijection $A_k \to A_{n+1}$ (Sets, Relations, and Cardinality, Theorem 1.5.4), and composing as before, A_k has $n!$ elements.

Adding up. We prove, by Sets, Relations, and Cardinality, Theorem 2.2.1 with base 1 (read on ω by Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)), the statement $P(j)$: "if $j \leq n+1$, the union $A_1 \cup \dots \cup A_j$ has $j\,n!$ elements". For $j = 1$ this is the count of A_1, and the step adds the $n!$ elements of A_{j+1}, disjoint from $A_1 \cup \dots \cup A_j$, by Sets, Relations, and Cardinality, Proposition 3.1.5, with $j\,n! + n! = (j+1)\,n!$. For $j = n+1$, S_{n+1} has $(n+1)\,n! = (n+1)!$ elements. This completes the induction and proves the proposition.

■

So S_3 has 6 elements, S_4 has 24, and S_{10} already has 3628800. For S_3 all six can be listed: id, the three transpositions (1 2), (1 3), (2 3), and the two 3-cycles (1 2 3), (1 3 2). These are six different permutations, so by the proposition they are all of S_3: a proper subset of a 6-element set has fewer elements (Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations, and Cardinality, Corollary 3.1.4).

3.4.4 Disjoint cycles and the decomposition theorem

In Example (Computing with Cycles), σ came apart into the loops (1 3) and (2 5 4), which move disjoint sets of points, and the order of the two factors did not matter. Both observations hold in general. We start with the second: permutations moving disjoint sets of points do not interfere with each other.

Proposition 3.4.3. Disjoint Permutations Commute

Let $n \in \mathbb{N}$ and $\sigma, \tau \in S_n$ with $\operatorname{supp}\sigma \cap \operatorname{supp}\tau = \emptyset$. Then $\sigma\tau = \tau\sigma$. Moreover, every permutation σ maps $\operatorname{supp}\sigma$ onto itself: $\sigma(\operatorname{supp}\sigma) = \operatorname{supp}\sigma$.

In particular, disjoint cycles commute.

Idea. A point moved by σ is fixed by τ, and so is its image under σ, because σ keeps its moved points among its moved points. So on $\operatorname{supp}\sigma$ only σ acts, on $\operatorname{supp}\tau$ only τ, and elsewhere neither: the order of application cannot matter.

Proof. σ maps its support onto itself. Let $i \in \operatorname{supp}\sigma$. If $\sigma(i) \notin \operatorname{supp}\sigma$, then $\sigma(\sigma(i)) = \sigma(i)$, and injectivity gives $\sigma(i) = i$, against $i \in \operatorname{supp}\sigma$. So $\sigma(\operatorname{supp}\sigma) \subseteq \operatorname{supp}\sigma$. Conversely, let $j \in \operatorname{supp}\sigma$ and $i := \sigma^{-1}(j)$. If $i \notin \operatorname{supp}\sigma$, then $j = \sigma(i) = i \notin \operatorname{supp}\sigma$, a contradiction; so $i \in \operatorname{supp}\sigma$ and $j = \sigma(i) \in \sigma(\operatorname{supp}\sigma)$. Hence $\sigma(\operatorname{supp}\sigma) = \operatorname{supp}\sigma$.

Commuting. Let $i \in \{1, \dots, n\}$. There are three cases, since i lies in at most one of the disjoint supports.

Case 1: $i \in \operatorname{supp}\sigma$. Then $i \notin \operatorname{supp}\tau$, so $\tau(i) = i$. Also $\sigma(i) \in \operatorname{supp}\sigma$ by the first part, so $\sigma(i) \notin \operatorname{supp}\tau$ and $\tau(\sigma(i)) = \sigma(i)$. Hence $(\sigma\tau)(i) = \sigma(i) = (\tau\sigma)(i)$.

Case 2: $i \in \operatorname{supp}\tau$. The same argument with σ and τ exchanged gives $(\tau\sigma)(i) = \tau(i) = (\sigma\tau)(i)$.

Case 3: i lies in neither support. Then $\sigma(i) = i = \tau(i)$, and both products send i to i.

So $\sigma\tau$ and $\tau\sigma$ agree at every point, and $\sigma\tau = \tau\sigma$ (Sets, Relations, and Cardinality, Proposition 1.4.1). This proves the proposition.

■

The hypothesis "disjoint" cannot be dropped: (1 2) and (1 3) share the point 1, and Example (Computing with Cycles) shows that they do not commute. Exercise C1 looks at the dropped hypothesis more closely.

Now the main theorem. To break a permutation into loops, start at a point it moves and follow it until it comes back. The loop found is a cycle; remove it, and fewer points are moved, so induction finishes the job.

Theorem 3.4.4. Disjoint Cycle Decomposition

Let $n \in \mathbb{N}$. Every $\sigma \in S_n$ is a product $\sigma = \gamma_1\gamma_2\cdots\gamma_s$, $s \in \mathbb{N}$, of pairwise disjoint cycles, each with support contained in $\operatorname{supp}\sigma$. For $\sigma = \mathrm{id}$ the product is empty ($s = 0$).

The clause about supports is part of the statement because the induction needs it: it is what makes the new cycle disjoint from the old ones. The theorem says nothing about uniqueness; that the decomposition is unique up to the order of the factors is proved in *Groups*, the chapter "Symmetric Groups and the Sign of a Permutation".

Idea. Induction on the number m of points that σ moves. ① Pick a moved point i and follow its orbit $i, \sigma(i), \sigma^2(i), \dots$. There are only n points, so the orbit repeats, and it repeats first at i itself. ② The points before the return form a cycle γ on which σ acts exactly as γ does. ③ Peel it off: $\rho \coloneqq \gamma^{-1}\sigma$ fixes the orbit and everything σ fixes, so it moves fewer points, and the induction hypothesis decomposes it. Then $\sigma = \gamma\rho$.

Before reading on: why must the orbit of i return to i itself, and not to some later point?

Proof. We use strong induction (Logic and Proof, Theorem 4.2.2) on $m \in \mathbb{N}$, for the statement: every $\sigma \in S_n$ whose support has m elements is a product of pairwise disjoint cycles with supports in $\operatorname{supp}\sigma$. Every support is a subset of $\{1, \dots, n\}$, which has n elements, so it is finite (Sets, Relations, and Cardinality, Proposition 3.1.6), and every σ is covered by the statement for some m.

Let $\sigma \in S_n$, let $\operatorname{supp}\sigma$ have m elements, and suppose the statement holds for every smaller number. If $m = 0$, then $\operatorname{supp}\sigma = \emptyset$, so $\sigma = \mathrm{id}$, the empty product (Definition 3.1.2). Let $m \geq 1$ and choose $i \in \operatorname{supp}\sigma$.

Follow the orbit. Powers are taken in the group S_n (Definition 3.1.3). The map $\{0,1,\dots,n\} \to \{1,\dots,n\}$, $c \mapsto \sigma^c(i)$, goes from a set of $n+1$ elements to a set of n elements, so it is not injective (Sets, Relations, and Cardinality, Corollary 3.1.3 (a)): $\sigma^a(i) = \sigma^b(i)$ for some $0 \le a < b \le n$. Apply σ^{-a} to both sides. By Proposition 3.1.3 (a), $\sigma^{-a}\sigma^a = \sigma^0 = \mathrm{id}$ and $\sigma^{-a}\sigma^b = \sigma^{b-a}$, so

$$i = \sigma^{b-a}(i), \qquad b - a \ge 1.$$

So the set of $c \in \mathbb{Z}_{>0}$ with $\sigma^c(i) = i$ is non-empty and bounded below by 0, and it has a least element r (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6). Since $\sigma(i) \ne i$, $r \ge 2$.

The points $i, \sigma(i), \dots, \sigma^{r-1}(i)$ are distinct. Indeed, if $\sigma^c(i) = \sigma^d(i)$ with $0 \le c < d \le r-1$, the argument just given yields $\sigma^{d-c}(i) = i$ with $0 < d - c < r$, against the minimality of r. Let

$$O \coloneqq \{\sigma^c(i) : 0 \le c \le r-1\}, \qquad \gamma \coloneqq (i \;\; \sigma(i) \;\; \cdots \;\; \sigma^{r-1}(i)),$$

an r-cycle (Definition 3.4.2) with $\operatorname{supp}\gamma = O$.

σ acts on O as γ does. For $0 \le c < r-1$, $\gamma(\sigma^c(i)) = \sigma^{c+1}(i) = \sigma(\sigma^c(i))$, where $\sigma^{c+1} = \sigma\sigma^c$ by Proposition 3.1.3 (a). For $c = r-1$, $\gamma(\sigma^{r-1}(i)) = i = \sigma^r(i) = \sigma(\sigma^{r-1}(i))$. So $\sigma(x) = \gamma(x)$ for every $x \in O$. In particular σ moves every point of O, since γ does, and $O \subseteq \operatorname{supp}\sigma$.

Peel it off. Let $\rho \coloneqq \gamma^{-1}\sigma$. For $x \in O$, $\rho(x) = \gamma^{-1}(\sigma(x)) = \gamma^{-1}(\gamma(x)) = x$. For $x \notin \operatorname{supp}\sigma$, we have $x \notin O$, so $\gamma(x) = x$ and hence $\gamma^{-1}(x) = x$; then $\rho(x) = \gamma^{-1}(x) = x$. So ρ fixes every point of O and every point outside $\operatorname{supp}\sigma$:

$$\operatorname{supp}\rho \subseteq \operatorname{supp}\sigma \setminus O.$$

Since $i \in O$, the set $\operatorname{supp}\sigma \setminus O$ is a proper subset of $\operatorname{supp}\sigma$, so it has fewer than m elements, and so does its subset $\operatorname{supp}\rho$ (Sets, Relations, and Cardinality, Proposition 3.1.6, twice). By the induction hypothesis, $\rho = \gamma_1 \cdots \gamma_s$ with pairwise disjoint cycles γ_j and $\operatorname{supp}\gamma_j \subseteq \operatorname{supp}\rho \subseteq \operatorname{supp}\sigma \setminus O$. Each γ_j is therefore disjoint from γ, whose support is O.

Finally, $\gamma\rho = \gamma\gamma^{-1}\sigma = \sigma$, so by Proposition 3.1.2 (a)

$$\sigma = \gamma\gamma_1 \cdots \gamma_s,$$

a product of pairwise disjoint cycles, with $\operatorname{supp}\gamma = O \subseteq \operatorname{supp}\sigma$ and $\operatorname{supp}\gamma_j \subseteq \operatorname{supp}\sigma$. This completes the induction and proves the theorem.

■

The answer to the prompt. The orbit returns to i itself because σ is injective; in the proof, that is the step "apply σ^{-a}". If the first repetition were $\sigma^b(i) = \sigma^a(i)$ with $a \ge 1$, applying σ^{-1} would give the earlier repetition $\sigma^{b-1}(i) = \sigma^{a-1}(i)$. For a function that is not injective this fails: $f\colon \{1,2\} \to \{1,2\}$ with $f(1) = f(2) = 2$ has the orbit $1, 2, 2, 2, \dots$, which never comes back to 1.

The proof is an algorithm. Here it is run on one permutation.

A worked run. Let $\sigma \in S_6$ send $1 \mapsto 4$, $2 \mapsto 6$, $3 \mapsto 3$, $4 \mapsto 1$, $5 \mapsto 2$, $6 \mapsto 5$. Its support is $\{1,2,4,5,6\}$. Start at 1: $1 \mapsto 4 \mapsto 1$, so $r = 2$ and $\gamma = (1\ 4)$. Peel it off: $\rho = (1\ 4)^{-1}\sigma = (1\ 4)\sigma$ fixes 1 and 4 and agrees with σ elsewhere, with support $\{2,5,6\}$. Start again at 2: $2 \mapsto 6 \mapsto 5 \mapsto 2$, so $r = 3$ and the next cycle is $(2\ 6\ 5)$. Peeling it off leaves the identity, and the point 3, fixed by σ, never enters. So

$$\sigma = (1\ 4)(2\ 6\ 5).$$

Quick check. Decompose $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_6$ into disjoint cycles.

Solution. Start at 1: $1 \mapsto 3 \mapsto 5 \mapsto 1$, the cycle $(1\ 3\ 5)$. The next moved point is 2: $2 \mapsto 6 \mapsto 2$, the cycle $(2\ 6)$. The point 4 is fixed. So the permutation is $(1\ 3\ 5)(2\ 6)$, and by Proposition 3.4.3 also $(2\ 6)(1\ 3\ 5)$.

By Proposition 3.4.3, two neighboring factors of a disjoint cycle decomposition may be exchanged; for instance $(1\ 3\ 5)(2\ 6) = (2\ 6)(1\ 3\ 5)$. The next section breaks each cycle further, into transpositions.

3.4.5 Exercises

3.4.5.1 A. Check your understanding

Exercise. A1

(a) Compute $(1\ 2\ 3\ 4)(2\ 4)$ and $(2\ 4)(1\ 2\ 3\ 4)$ in S_4, as products of disjoint cycles.

(b) Find the inverse of $(1\ 5\ 2\ 7)$ in S_7, written as a cycle starting at 1.

(c) Run the proof of Theorem 3.4.4 on

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \in S_5,$$

starting at $i = 1$: give the orbit of 1, the number r, the cycle γ, and $\rho = \gamma^{-1}\sigma$; then finish the run. Which step of the proof uses that σ is injective?

(d) Compute $((1\ 2)(2\ 3))^2$ and $(1\ 2)^2(2\ 3)^2$ in S_3.

Solution.

(a) For $(1\ 2\ 3\ 4)(2\ 4)$, apply $(2\ 4)$ first: $1 \mapsto 1 \mapsto 2$, $2 \mapsto 4 \mapsto 1$, $3 \mapsto 3 \mapsto 4$, $4 \mapsto 2 \mapsto 3$. So the product is $(1\ 2)(3\ 4)$. For $(2\ 4)(1\ 2\ 3\ 4)$, apply $(1\ 2\ 3\ 4)$ first: $1 \mapsto 2 \mapsto 4$, $4 \mapsto 1 \mapsto 1$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 4 \mapsto 2$. So the product is $(1\ 4)(2\ 3)$. The two orders give different permutations.

(b) By the inverse formula after Definition 3.4.2, $(1\ 5\ 2\ 7)^{-1} = (7\ 2\ 5\ 1)$, which, started at 1, is $(1\ 7\ 2\ 5)$.

(c) The orbit of 1 is $1 \mapsto 2 \mapsto 5 \mapsto 1$, so $r = 3$ and $\gamma = (1\ 2\ 5)$, with $\gamma^{-1} = (5\ 2\ 1) = (1\ 5\ 2)$. Then $\rho = \gamma^{-1}\sigma$ sends $1 \mapsto 2 \mapsto 1$, $2 \mapsto 5 \mapsto 2$, $5 \mapsto 1 \mapsto 5$, $3 \mapsto 4 \mapsto 4$, $4 \mapsto 3 \mapsto 3$: $\rho = (3\ 4)$. Running the proof on ρ, starting at 3: $3 \mapsto 4 \mapsto 3$, so the cycle is $(3\ 4)$, and peeling it off leaves id. Hence $\sigma = (1\ 2\ 5)(3\ 4)$. Injectivity is used where the orbit is shown to return to i itself: the step that applies σ^{-a} to $\sigma^a(i) = \sigma^b(i)$.

(d) $(1\ 2)(2\ 3)$: $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 2 \mapsto 1$, so it is $(1\ 2\ 3)$, and its square sends $1 \mapsto 2 \mapsto 3$, $3 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 1$: $((1\ 2)(2\ 3))^2 = (1\ 3\ 2)$. On the other hand $(1\ 2)^2(2\ 3)^2 = \mathrm{id}$, since transpositions are their own inverses. A second instance of the warning on $(\sigma\tau)^2$.

3.4.5.2 B. Practice

Exercise. B1: The table of S_3

List the six elements of S_3 in cycle notation and write out the table whose entry in row x and column y is xy. Hence find all $x \in S_3$ with $x^2 = \mathrm{id}$, and all x that commute with every element of S_3.

Solution. By the list after Proposition 3.4.2, the elements are $\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$. Computing each product right to left, as in Example (Computing with Cycles), the entry in row x, column y is xy:

xy	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

For example, the entry in row (1 2), column (2 3) is (1 2)(2 3): $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 2 \mapsto 1$, which is (1 2 3).

Reading the diagonal, $x^2 = \mathrm{id}$ exactly for $x = \mathrm{id}, (1\ 2), (1\ 3), (2\ 3)$. An element x commutes with every element exactly when row x equals column x. This holds for id. It fails for every other element: $(1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3)(1\ 2)$ handles (1 2) and (1 3); $(2\ 3)(1\ 2) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 2)(2\ 3)$ handles (2 3); and $(1\ 2\ 3)(1\ 2) = (1\ 3) \neq (2\ 3) = (1\ 2)(1\ 2\ 3)$ handles (1 2 3), while $(1\ 3\ 2)(1\ 2) = (2\ 3) \neq (1\ 3) = (1\ 2)(1\ 3\ 2)$ handles (1 3 2). Hence only id commutes with everything.

Exercise. B2: Counting cycles

Let $n \in \mathbb{N}$ and $2 \leq k \leq n$. Show that S_n contains exactly

$$\frac{n!}{(n-k)!\,k}$$

k-cycles. Check the formula for $n = 4$ by listing the cycles of S_4.

Solution. We use one counting fact: *if a finite set is the union of N pairwise disjoint subsets with q elements each, it has Nq elements.* This is Sets, Relations, and Cardinality, Proposition 3.1.5 applied $N-1$ times, by induction on N, as in the proof of Proposition 3.4.2.

Lists. Let T_k be the set of lists $(i_1, \ldots, i_k)$ of **distinct** elements of $\{1, \ldots, n\}$. Then T_k has $n(n-1)\cdots(n-k+1)$ elements, by induction on k: T_0 has one element, the empty list, and T_{j+1} is the disjoint union, over the lists $t \in T_j$, of the sets of lists extending t by a point x of the complement C of its entry set E. Here E has j elements, since the entries are distinct, so $j + |C| = n$ (Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations,

and Cardinality, Proposition 3.1.5, Sets, Relations, and Cardinality, Corollary 3.1.4) and C has $n-j$ elements. By the counting fact, T_{j+1} has $(n-j)$ times as many elements as T_j. Since $n(n-1)\cdots(n-k+1)\cdot(n-k)! = n!$, this number is $n!/(n-k)!$.

Lists to cycles. Each list in T_k defines the k-cycle $(i_1\ \cdots\ i_k)$, and every k-cycle arises this way. Two lists give the same cycle exactly when one is a rotation of the other. Indeed, rotations give the same cycle (the remark after Definition 3.4.2). Conversely, if $(i_1\ \cdots\ i_k) = (j_1\ \cdots\ j_k) = \gamma$, then j_1 lies in the support $\{i_1,\dots,i_k\}$, say $j_1 = i_c$, and then $j_2 = \gamma(j_1) = i_{c+1}$, and so on around the loop: the second list is the first rotated to start at i_c. The k rotations of a list are k different lists, since their first entries differ. So the lists fall into pairwise disjoint classes of k elements, one class per k-cycle, and by the counting fact, with N_k the number of k-cycles,

$$k\,N_k = \frac{n!}{(n-k)!}.$$

Dividing by k gives the formula.

Check, $n = 4$. Transpositions: $4!/(2!\cdot 2) = 6$, namely $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$. 3-cycles: $4!/(1!\cdot 3) = 8$, two for each of the four sets of three points: $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2$ 4-cycles: $4!/(0!\cdot 4) = 6$, starting at 1 with the other three points in any of their $3! = 6$ orders: $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$.

Exercise. B3: The rotations of a square

Label the corners of a square $1, 2, 3, 4$ in order around it. The quarter turn moves each label to the next corner, which is the permutation $\rho = (1\ 2\ 3\ 4) \in S_4$ (Example (Groups) (e)).

(a) Compute ρ^2 and ρ^3 as products of disjoint cycles, and show $\rho^4 = \mathrm{id}$.

(b) Show that $\langle\rho\rangle = \{\mathrm{id}, \rho, \rho^2, \rho^3\}$.

(c) Show that $[k] \mapsto \rho^k$ is a well-defined isomorphism $(\mathbb{Z}/4\mathbb{Z}, +) \to \langle\rho\rangle$.

Solution.

(a) $\rho^2 = \rho\rho$ sends $1 \mapsto 2 \mapsto 3$, $3 \mapsto 4 \mapsto 1$, $2 \mapsto 3 \mapsto 4$, $4 \mapsto 1 \mapsto 2$: $\rho^2 = (1\ 3)(2\ 4)$. Then $\rho^3 = \rho^2\rho$ sends $1 \mapsto 2 \mapsto 4$, $4 \mapsto 1 \mapsto 3$, $3 \mapsto 4 \mapsto 2$, $2 \mapsto 3 \mapsto 1$: $\rho^3 = (1\ 4\ 3\ 2)$. Finally $\rho^4 = \rho^3\rho$ sends $1 \mapsto 2 \mapsto 1$, $2 \mapsto 3 \mapsto 2$, $3 \mapsto 4 \mapsto 3$, $4 \mapsto 1 \mapsto 4$: $\rho^4 = \mathrm{id}$.

(b) By Definition 3.2.2, $\langle\rho\rangle = \{\rho^k : k \in \mathbb{Z}\}$. For $k \in \mathbb{Z}$, divide by 4: $k = 4q + r$ with $0 \le r < 4$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2 (a)). By Proposition 3.1.3 (a) and (c),

$$\rho^k = (\rho^4)^q\rho^r = \mathrm{id}^q\,\rho^r = \rho^r,$$

where $\mathrm{id}^q = (\rho^0)^q = \rho^0 = \mathrm{id}$, again by (c). So every ρ^k is one of $\rho^0 = \mathrm{id}, \rho, \rho^2, \rho^3$, and all four lie in $\langle\rho\rangle$.

(c) *Well defined.* If $[k] = [k']$ in $\mathbb{Z}/4\mathbb{Z}$, then $k' - k \in 4\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2), so $k' = k + 4q$ for some $q \in \mathbb{Z}$, and $\rho^{k'} = \rho^k(\rho^4)^q = \rho^k$ as in (b). *Homomorphism.* $[k] + [l] = [k + l] \mapsto \rho^{k+l} = \rho^k\rho^l$ by Proposition 3.1.3 (a). *Bijective.* The four distinct classes $[0], [1], [2], [3]$, which are all of $\mathbb{Z}/4\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)), go to $\mathrm{id}, \rho, \rho^2, \rho^3$, which are four different permutations by (a) (they differ at the point 1: $1, 2, 3, 4$) and are all of

$\langle\rho\rangle$ by (b). So the map is a bijection, hence an isomorphism, and the four rotations of the square form a copy of $\mathbb{Z}/4\mathbb{Z}$, as Section 3.1 announced.

3.4.5.3 C. Going deeper

Exercise. C1: Dropping "disjoint"

Proposition 3.4.3 assumes that the supports are disjoint.

(a) Find two transpositions that share exactly one point and do not commute.

(b) Find two cycles in S_3 with the **same** support that do commute.

(c) In the proof of Proposition 3.4.3, which step fails for the pair of (a)?

Solution.

(a) (1 2) and (2 3) share only the point 2. By the table of Exercise B1, (1 2)(2 3) = (1 2 3) and (2 3)(1 2) = (1 3 2), which differ (at 1: 2 versus 3).

(b) (1 2 3) and (1 3 2) both have support $\{1,2,3\}$. They are inverse to each other (the inverse formula after Definition 3.4.2), so both products are id: (1 2 3)(1 3 2) = id = (1 3 2)(1 2 3). More generally every permutation commutes with its inverse and with its own powers (Proposition 3.1.3 (a)). So disjointness is sufficient for commuting, not necessary.

(c) Case 1 at the point $i = 1 \in \operatorname{supp}(1\ 2)$: the proof needs $\sigma(i) = 2 \notin \operatorname{supp}\tau$, so that τ fixes it. Here $\tau = (2\ 3)$ moves 2, so $(\tau\sigma)(1) = \tau(2) = 3$, while $(\sigma\tau)(1) = \sigma(1) = 2$.

Exercise. C2: Powers of disjoint cycles

(a) Let $\sigma = (i_1\ \cdots\ i_k) \in S_n$ be a k-cycle and $m \in \mathbb{Z}_{>0}$. Prove that $\sigma^m = \mathrm{id}$ if and only if $k \mid m$.

(b) Let σ be a k-cycle and τ an l-cycle in S_n, disjoint. Prove that, for every $m \in \mathbb{Z}_{>0}$, $(\sigma\tau)^m = \mathrm{id}$ if and only if $k \mid m$ and $l \mid m$.

(c) Deduce that the least $m \geq 1$ with $(\sigma\tau)^m = \mathrm{id}$ is the least positive common multiple of k and l.

(d) Find the least $m \geq 1$ with $\big((1\ 2)(3\ 4\ 5)\big)^m = \mathrm{id}$ in S_5.

Solution (Hint 1). For (b): a power of τ fixes every point that τ fixes.

Solution (Hint 2). Converse of (b): evaluate $\sigma^m\tau^m = \mathrm{id}$ at a point of $\operatorname{supp}\sigma$.

Solution.

(a) Read the indices of the entries modulo k: for $j \in \mathbb{Z}$ let $i_j := i_t$, where $t \in \{1,\dots,k\}$ and $j \equiv t \pmod{k}$. Write $j - 1 = kq + s$ with $0 \leq s < k$ (Number Systems: From

\(\nN\) to \(\nR\), Theorem 3.1.2 (a)) and take $t := s + 1$; t is unique because s is. Then $\sigma(i_j) = i_{j+1}$ for every j, which is Definition 3.4.2. By induction on $m \in \mathbb{N}$ (Logic and Proof, Axiom 4.2.1), $\sigma^m(i_j) = i_{j+m}$ for every j: for $m = 0$ both sides are i_j, and $\sigma^{m+1}(i_j) = \sigma(\sigma^m(i_j)) = \sigma(i_{j+m}) = i_{j+m+1}$, using $\sigma^{m+1} = \sigma\sigma^m$ (Proposition 3.1.3 (a)). Every point off the cycle is fixed by σ, hence by σ^m. So $\sigma^m = \mathrm{id}$ if and only if $i_{j+m} = i_j$ for every j. Since the entries $i_1, \ldots, i_k$ are distinct, $i_{j+m} = i_j$ holds exactly when $j + m \equiv j \pmod{k}$, that is, when $k \mid m$.

(b) The supports are disjoint, so $\sigma\tau = \tau\sigma$ (Proposition 3.4.3), and $(\sigma\tau)^m = \sigma^m\tau^m$ by Proposition 3.1.3 (d). If $k \mid m$ and $l \mid m$, then $\sigma^m = \tau^m = \mathrm{id}$ by (a), so $(\sigma\tau)^m = \mathrm{id}$. Conversely, suppose $\sigma^m\tau^m = \mathrm{id}$. Let $x \in \operatorname{supp}\sigma$. Then $x \notin \operatorname{supp}\tau$, so $\tau(x) = x$, and by induction on m (Logic and Proof, Axiom 4.2.1) $\tau^m(x) = x$ (Hint 1). Hence $\sigma^m(x) = \sigma^m(\tau^m(x)) = x$. Also σ^m fixes every $x \notin \operatorname{supp}\sigma$, since σ does. So $\sigma^m = \mathrm{id}$, and then $\tau^m = \sigma^m\tau^m = \mathrm{id}$. By (a), $k \mid m$ and $l \mid m$.

(c) By (b), the $m \geq 1$ with $(\sigma\tau)^m = \mathrm{id}$ are exactly the positive common multiples of k and l. This set contains kl, and so it has a least element (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6), the least positive common multiple of k and l. By Exercise (C3: Inclusions and intersections), the common multiples of k and l are exactly the multiples of that number.

(d) (1 2) and (3 4 5) are disjoint, of lengths 2 and 3. The positive common multiples of 2 and 3 start $6, 12, \ldots$ (a common multiple of 2 is even, and $3 \nmid 2, 4$), so the least m is 6.

Marking scheme. (10 points) - 3: (a) the formula $\sigma^m(i_j) = i_{j+m}$ with indices modulo k, proved by induction, and the points off the cycle fixed. - 1: (a) from distinctness of the entries to $k \mid m$, in both directions. - 2: (b) commuting from disjointness, cited, and $(\sigma\tau)^m = \sigma^m\tau^m$ with the reason. - 3: (b) the converse: from $\sigma^m\tau^m = \mathrm{id}$, uses disjointness of the supports to get $\sigma^m = \mathrm{id}$ and $\tau^m = \mathrm{id}$. - 1: (c) and (d), the least element named.

Second route: $\sigma^m = \tau^{-m}$, with $\operatorname{supp}\sigma^m \subseteq \operatorname{supp}\sigma$ and $\operatorname{supp}\tau^{-m} \subseteq \operatorname{supp}\tau$, and these are disjoint, so both are id; this earns the same 3 points if both inclusions are justified.

Fatal errors (0 for the step): $(\sigma\tau)^m = \sigma^m\tau^m$ without using that the cycles commute; "$\sigma^m\tau^m = \mathrm{id}$ so $\sigma^m = \tau^{-m}$, hence both are id" with no use of disjointness.

3.5 Transpositions Generate the Symmetric Group

Section 3.4 wrote permutations in cycle notation and showed that every permutation breaks into disjoint cycles (Theorem 3.4.4). One small computation there, (1 3)(1 2) = (1 2 3) in Example (Computing with Cycles), says more than it seems to: a 3-cycle is two swaps. This section shows that every permutation of $\{1, \ldots, n\}$, for $n \geq 2$, is a product of swaps of two points. The determinant of linear algebra is built on exactly this fact, and so is the sign of a permutation, which later volumes define.

Throughout, $n \in \mathbb{N}$, products of permutations are read **right to left** (Definition 3.4.1: $\sigma\tau = \sigma \circ \tau$ applies τ first), and a product $\tau_1\tau_2 \cdots \tau_r$ is the product of a list in the group S_n (Definition 3.1.2), so brackets may be dropped (Proposition 3.1.2 (b)).

3.5.1 Cycles as products of transpositions

Recall from Definition 3.4.2 that a **transposition** is a 2-cycle $(a\ b)$, with $a \neq b$: it swaps a and b and fixes every other point. Two facts about it are used constantly below.

- $(a\ b) = (b\ a)$, since both swap a and b and fix the rest (Sets, Relations, and Cardinality, Proposition 1.4.1).
- A transposition is its own inverse: $(a\ b)(a\ b) = \mathrm{id}$. Indeed $a \mapsto b \mapsto a$, $b \mapsto a \mapsto b$, and every other point is fixed twice. Equivalently, the inverse of $(a\ b)$ is $(b\ a) = (a\ b)$ (Definition 3.4.2).

The computation $(1\ 3)(1\ 2) = (1\ 2\ 3)$ has a pattern: both transpositions contain the first entry 1 of the cycle, and the one applied **first** is $(1\ 2)$, which sends 1 to the next entry. Longer cycles follow the same pattern.

Proposition 3.5.1. A Cycle Is a Product of Transpositions

Let $k \geq 2$, and let $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$ be **distinct**. Then

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2),$$

a product of $k - 1$ transpositions.

Read right to left, the factors are $(i_1\ i_2)$, then $(i_1\ i_3)$, and so on up to $(i_1\ i_k)$. For $k = 4$: $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$. Follow 2: the first factor $(1\ 2)$ sends it to 1, the second sends 1 to 3, and the third fixes 3; so $2 \mapsto 3$, as the cycle requires.

Idea. Induct on the length. To pass from $(i_1\ \cdots\ i_k)$ to $(i_1\ \cdots\ i_k\ i_{k+1})$, the only change is that i_k must now go to i_{k+1} instead of back to i_1, and i_{k+1} must go to i_1. One more swap of i_1 and i_{k+1}, applied **after** the shorter cycle, makes exactly this change.

Proof. We prove, by Sets, Relations, and Cardinality, Theorem 2.2.1 with base 2 (read on ω by Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)), the statement $P(k)$: "for every list $(i_1, \ldots, i_k)$ of distinct points of $\{1, \ldots, n\}$, the displayed equation holds".

Base, $k = 2$. The right-hand side is the list of one factor $(i_1\ i_2)$, whose product is $(i_1\ i_2)$ (Definition 3.1.2), and this is the left-hand side.

Step. Let $k \geq 2$, suppose $P(k)$, and let $i_1, \ldots, i_{k+1}$ be distinct. Put $\gamma := (i_1\ \cdots\ i_k)$ and $\tau := (i_1\ i_{k+1})$. We claim $\tau\gamma = (i_1\ \cdots\ i_{k+1})$, and check it point by point (Sets, Relations, and Cardinality, Proposition 1.4.1).

- For $1 \leq j < k$: $\gamma(i_j) = i_{j+1}$, which is neither i_1 (as $j + 1 \geq 2$) nor i_{k+1} (as $j + 1 \leq k$), the entries being distinct; so τ fixes it: $\tau\gamma(i_j) = i_{j+1}$.
- $\gamma(i_k) = i_1$ and $\tau(i_1) = i_{k+1}$: so $\tau\gamma(i_k) = i_{k+1}$.
- i_{k+1} is not among $i_1, \ldots, i_k$, so γ fixes it, and $\tau(i_{k+1}) = i_1$: so $\tau\gamma(i_{k+1}) = i_1$.
- Every other point x is fixed by γ and by τ.

These are the values of the $(k + 1)$-cycle (Definition 3.4.2), which proves the claim. By $P(k)$ and the concatenation law Proposition 3.1.2 (a), applied to the list (τ) and the list

$((i_1\ i_k), \dots, (i_1\ i_2))$,

$$(i_1\ \cdots\ i_{k+1}) = \tau\gamma = (i_1\ i_{k+1})(i_1\ i_k)\cdots(i_1\ i_2),$$

which is $P(k+1)$. This proves the proposition.

■

The proof never used that the cycle starts at its smallest entry, so the formula may be applied to any way of writing the cycle. Writing (1 2 3) as (2 3 1) gives (2 1)(2 3) = (1 2)(2 3), a second word for the same permutation; we return to this below.

Quick check. Write (2 5 3) as a product of transpositions, and check your answer point by point.

Solution. By Proposition 3.5.1 with $i_1 = 2$, $i_2 = 5$, $i_3 = 3$: (2 5 3) = (2 3)(2 5). Check, applying (2 5) first: $2 \mapsto 5 \mapsto 5$, $5 \mapsto 2 \mapsto 3$, $3 \mapsto 3 \mapsto 2$, and every other point is fixed. So $2 \mapsto 5$, $5 \mapsto 3$, $3 \mapsto 2$, which is (2 5 3).

3.5.2 Every permutation is a product of transpositions

We say that $\sigma \in S_n$ is a **product of transpositions** if $\sigma = \tau_1\tau_2\cdots\tau_r$ for some $r \geq 1$ and transpositions $\tau_1, \dots, \tau_r \in S_n$. The words "$r \geq 1$" matter for one permutation only: the identity is always the empty product (Definition 3.1.2), but it is a product of **at least one** transposition only when a transposition exists, that is, when $n \geq 2$. Then id = (1 2)(1 2). More generally, for a set $T \subseteq S_n$, σ is a **product of elements of** T if $\sigma = t_1t_2\cdots t_r$ for some $r \geq 1$ and $t_1, \dots, t_r \in T$, and T **generates** S_n if every $\sigma \in S_n$ is a product of elements of T. The theorem below says that the transpositions generate S_n for $n \geq 2$, and its corollary says the same for the adjacent transpositions.

Theorem 3.5.2. Transpositions Generate S_n

Let $n \geq 2$. Every $\sigma \in S_n$ is a product of transpositions.

Try it first (ten minutes): write (1 2 3 4) *and* (1 3)(2 4) *as products of transpositions. Then let* $\sigma \in S_4$ *with* $\sigma(4) \neq 4$*: which single transposition* τ *makes* $\tau\sigma$ *fix* 4*?*

Idea. The two examples are easy: the first is (1 4)(1 3)(1 2) by Proposition 3.5.1, and the second is already a product of two transpositions. They suggest a route through Theorem 3.4.4, and that route works (the remark after the proof). But it hides where the transpositions come from. The second question points to a route that needs no cycles at all: induction on n. What is the smaller object inside a permutation of $n+1$ points? If σ fixes $n+1$, it is really a permutation of $\{1, \dots, n\}$, and Lemma 3.4.1 makes that precise. If not, say $\sigma(n+1) = k$, one swap repairs it: $\tau \coloneqq (k\ \ n{+}1)$ sends k back to $n+1$, so $\tau\sigma$ fixes $n+1$. Apply the first case to $\tau\sigma$, then undo the swap. In one phrase: **fix one point, then induct**.

Before reading on: why does $\tau\sigma$ fix $n+1$, and why is that the right thing to aim for?

Proof. We use Sets, Relations, and Cardinality, Theorem 2.2.1 with base 2 (read on ω by Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) on $n \geq 2$.

Base, $n = 2$. Let $\sigma \in S_2$. If $\sigma(1) = 1$, then $\sigma(2) \neq 1$ since σ is injective, so $\sigma(2) = 2$ and $\sigma = \mathrm{id}$ (Sets, Relations, and Cardinality, Proposition 1.4.1). If $\sigma(1) = 2$, then $\sigma(2) = 1$ in the same way, and $\sigma = (1\ 2)$. So $S_2 = \{\mathrm{id}, (1\ 2)\}$. Here $(1\ 2)$ is one transposition and $\mathrm{id} = (1\ 2)(1\ 2)$ is two.

Step. Let $n \geq 2$, suppose that every element of S_n is a product of transpositions, and let $\sigma \in S_{n+1}$. For $\rho \in S_n$, write $\overline{\rho} \in S_{n+1}$ for its extension, $\overline{\rho}(i) = \rho(i)$ for $i \leq n$ and $\overline{\rho}(n+1) = n+1$. By Lemma 3.4.1, $\rho \mapsto \overline{\rho}$ is the inverse of the isomorphism $\sigma \mapsto \sigma'$ from $S' := \{\sigma \in S_{n+1} : \sigma(n+1) = n+1\}$ onto S_n; so it is an isomorphism $S_n \to S'$ (Proposition 3.3.2 (b)), and $\overline{\rho\pi} = \overline{\rho}\,\overline{\pi}$ for all $\rho, \pi \in S_n$, the product on the right being taken in S', that is, in S_{n+1}.

We record two facts about the extension.

1. *It carries list products to list products:* $\overline{\tau_1 \cdots \tau_r} = \overline{\tau_1} \cdots \overline{\tau_r}$ for every $r \geq 1$ and $\tau_1, \ldots, \tau_r \in S_n$. For $r = 1$ both sides are $\overline{\tau_1}$. If it holds for r, then by the recursion of Definition 3.1.2 and the homomorphism property,
$$\overline{\tau_1 \cdots \tau_{r+1}} = \overline{(\tau_1 \cdots \tau_r)\tau_{r+1}} = \overline{\tau_1 \cdots \tau_r}\ \overline{\tau_{r+1}} = \overline{\tau_1} \cdots \overline{\tau_{r+1}},$$
so it holds for $r+1$ (Sets, Relations, and Cardinality, Theorem 2.2.1 with base 1).
2. *It carries transpositions to transpositions:* for distinct $a, b \leq n$, $\overline{(a\ b)}$ swaps a and b and fixes every other point of $\{1, \ldots, n+1\}$, including $n+1$; so it is the transposition $(a\ b)$ of S_{n+1}.

Case 1: $\sigma(n+1) = n+1$. Then $\sigma \in S'$, and its restriction σ' lies in S_n (Lemma 3.4.1). By the induction hypothesis, $\sigma' = \tau_1 \cdots \tau_r$ with $r \geq 1$ and transpositions $\tau_j \in S_n$. Since the two maps of the lemma are mutually inverse, $\sigma = \overline{\sigma'}$, and by facts 1 and 2,
$$\sigma = \overline{\sigma'} = \overline{\tau_1 \cdots \tau_r} = \overline{\tau_1} \cdots \overline{\tau_r},$$
a product of r transpositions of S_{n+1}.

Case 2: $\sigma(n+1) = k \neq n+1$. Then $k \in \{1, \ldots, n\}$, and $\tau := (k\ \ n{+}1)$ is a transposition of S_{n+1}. Now
$$(\tau\sigma)(n+1) = \tau(\sigma(n+1)) = \tau(k) = n+1,$$
so Case 1 applies to $\tau\sigma$: $\tau\sigma = \tau_1 \cdots \tau_r$ with $r \geq 1$ and transpositions $\tau_j \in S_{n+1}$. Multiply on the left by τ, using $\tau\tau = \mathrm{id}$, (G1), (G2) and the concatenation law Proposition 3.1.2 (a):
$$\sigma = (\tau\tau)\sigma = \tau(\tau\sigma) = \tau(\tau_1 \cdots \tau_r) = \tau\tau_1 \cdots \tau_r,$$
a product of $r+1$ transpositions.

In both cases σ is a product of transpositions. This completes the induction and proves the theorem.

■

The answer to the prompt. The transposition $\tau = (k \quad n{+}1)$ was chosen so that it sends $k = \sigma(n+1)$ back to $n+1$; that is the whole computation in Case 2. Fixing $n+1$ is the right aim because it is exactly the hypothesis of Lemma 3.4.1: a permutation of $n+1$ points that fixes the last one **is** a permutation of n points, and only there does the induction hypothesis speak. Case 1 also needs the restriction σ' to be **onto** $\{1, \dots, n\}$, and the lemma proves this directly from $\sigma(n+1) = n+1$, with no counting.

Remark. Alternatively, Theorem 3.4.4 writes $\sigma = \gamma_1 \cdots \gamma_s$ with disjoint cycles γ_j. If $s = 0$, then $\sigma = \mathrm{id} = (1\ 2)(1\ 2)$, using $n \geq 2$. Otherwise Proposition 3.5.1 writes each γ_j as a product of transpositions, and the concatenation law Proposition 3.1.2 (a) joins the words. For $\sigma = (1\ 3)(2\ 5\ 4)$ of Example (Computing with Cycles) this gives $(1\ 3)(2\ 4)(2\ 5)$.

3.5.3 The word is not unique

A product $\tau_1 \cdots \tau_r$ equal to σ is a **word** for σ. A permutation has many words. For the 3-cycle of the opening,

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (1\ 3)(1\ 2)(1\ 2)(1\ 2).$$

The first word is Example (Computing with Cycles). The second is Proposition 3.5.1 applied to $(2\ 3\ 1)$, as above; directly, applying $(2\ 3)$ first, $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 2 \mapsto 1$. The third inserts $(1\ 2)(1\ 2) = \mathrm{id}$ after the first word.

Warning. "The transpositions of σ" means nothing, and neither does "σ is a product of r transpositions, so r is determined by σ". The three words for $(1\ 2\ 3)$ above have lengths 2, 2 and 4, and the first two consist of different transpositions. A word must also be read **right to left**, like every product of permutations: reversing the word $(1\ 3)(1\ 2)$ gives $(1\ 2)(1\ 3) = (1\ 3\ 2)$ (Example (Computing with Cycles)), a different permutation.

Something does survive. The three lengths 2, 2, 4 above are all even. That every word for a given permutation has a length of the same parity is true, but it is not proved here: it is the theorem on the **sign** of a permutation, proved in the chapter "Determinants" of the linear algebra volume *Determinants and the Structure of Operators* and in the chapter "Symmetric Groups and the Sign of a Permutation" of *Groups*. Nothing in this chapter uses it.

Second reading · *A minimal change: 3-cycles do not generate*

Not every kind of cycle generates S_n. Change "transpositions" to "3-cycles" in the theorem, with $n = 3$. By Definition 3.4.2, a 3-cycle of S_3 is $(i_1\ i_2\ i_3)$ with $\{i_1, i_2, i_3\} = \{1, 2, 3\}$, and rotating the written cycle shows that there are only two of them: $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$ and $(1\ 3\ 2) = (3\ 2\ 1) = (2\ 1\ 3)$. Let $H := \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. Computing right to left as in Example (Computing with Cycles),

$$\begin{aligned} (1\ 2\ 3)(1\ 2\ 3) &= (1\ 3\ 2), & (1\ 3\ 2)(1\ 3\ 2) &= (1\ 2\ 3), \\ (1\ 2\ 3)(1\ 3\ 2) &= \mathrm{id}, & (1\ 3\ 2)(1\ 2\ 3) &= \mathrm{id}, \end{aligned}$$

and id times anything is that thing; so H is closed under products. By induction on the length $r \geq 1$, using the recursion of Definition 3.1.2, every product of r 3-cycles lies in H. But $(1\ 2) \notin H$.

So the 3-cycles do **not** generate S_3, and the theorem depends on the kind of cycle it names.

3.5.4 Adjacent transpositions

Linear algebra often sorts a list by swapping **neighbors**, positions i and $i{+}1$. The transpositions $(i\ \ i{+}1)$, $1 \le i < n$, are the **adjacent** transpositions, and they are enough.

Corollary 3.5.3. Adjacent Transpositions Generate S_n

Let $n \ge 2$. Every $\sigma \in S_n$ is a product of adjacent transpositions $(i\ \ i{+}1)$, $1 \le i < n$.

Idea. By Theorem 3.5.2 it is enough to write one transposition $(i\ j)$, $i < j$, with adjacent ones. Conjugating by a neighbor swap moves an endpoint one step: $(i\ \ i{+}1)(i{+}1\ \ j)(i\ \ i{+}1) = (i\ j)$. So the gap $j - i$ shrinks by one, and an induction on the gap finishes.

Proof. First let $1 \le i < j \le n$ with $j - i \ge 2$, and put $s := (i\ \ i{+}1)$, $t := (i{+}1\ \ j)$; here $i{+}1 < j$, so t is a transposition. We check $sts = (i\ j)$ point by point, applying the right-hand s first:

$$i \mapsto i+1 \mapsto j \mapsto j, \quad j \mapsto j \mapsto i+1 \mapsto i,$$
$$i+1 \mapsto i \mapsto i \mapsto i+1,$$

and every other point is fixed by s, t and s. So

$$(i\ j) = (i\ \ i{+}1)(i{+}1\ \ j)(i\ \ i{+}1). \tag{$*$}$$

Next we prove, by Sets, Relations, and Cardinality, Theorem 2.2.1 with base 1 on d, the statement $Q(d)$: "for every $i \ge 1$ with $i + d \le n$, $(i\ \ i{+}d)$ is a product of adjacent transpositions". $Q(1)$ holds, since $(i\ \ i{+}1)$ is one. Suppose $Q(d)$, and let $i + d + 1 \le n$. By $(*)$ with $j = i + d + 1$, $(i\ \ i{+}d{+}1) = (i\ \ i{+}1)(i{+}1\ \ i{+}1{+}d)(i\ \ i{+}1)$, and the middle factor is a product of adjacent transpositions by $Q(d)$, applied at $i + 1$. Joining the three words by Proposition 3.1.2 (a) gives $Q(d + 1)$.

Finally let $\sigma \in S_n$. By Theorem 3.5.2, $\sigma = \tau_1 \cdots \tau_r$ with $r \ge 1$. Each τ_j is $(a\ b) = (b\ a)$ with $a \ne b$, so it can be written as $(i\ \ i{+}d)$ with i the smaller entry and $d \ge 1$ the difference; by $Q(d)$ it is a product of adjacent transpositions. Joining these r words by Proposition 3.1.2 (a) proves the corollary. ∎

The words this proof produces are long. Unwinding $(*)$ twice, $(1\ 4) = (1\ 2)(2\ 4)(1\ 2)$ and $(2\ 4) = (2\ 3)(3\ 4)(2\ 3)$, so

$$(1\ 4) = (1\ 2)(2\ 3)(3\ 4)(2\ 3)(1\ 2).$$

The corollary only promises that some word exists; it says nothing about the shortest one.

Quick check. Find a second word of adjacent transpositions for $(1\ 4)$ in S_4, different from the one above, and check it point by point.

Solution. Shrink the gap from the other end: $(1\ 4) = (3\ 4)(1\ 3)(3\ 4)$ and $(1\ 3) = (2\ 3)(1\ 2)(2\ 3)$, so $(1\ 4) = (3\ 4)(2\ 3)(1\ 2)(2\ 3)(3\ 4)$. Check, applying the right-most factor first: $1 \mapsto 1 \mapsto 1 \mapsto 2 \mapsto 3 \mapsto 4$; $4 \mapsto 3 \mapsto 2 \mapsto 1 \mapsto 1 \mapsto 1$; $2 \mapsto 2 \mapsto 3 \mapsto 3 \mapsto 2 \mapsto 2$; $3 \mapsto 4 \mapsto 4 \mapsto 4 \mapsto 4 \mapsto 3$. So $1 \leftrightarrow 4$ with 2, 3 fixed, which is $(1\ 4)$. (The first step is the mirror image of $(*)$: $(i\ j) = (j{-}1\ \ j)(i\ \ j{-}1)(j{-}1\ \ j)$ for $j - i \geq 2$, checked in the same way.)

3.5.5 Exercises

3.5.5.1 A. Check your understanding

Exercise. A1

(a) Where in Theorem 3.5.2 is the hypothesis $n \geq 2$ used? What goes wrong for $n = 1$?

(b) Run the proof of Theorem 3.5.2 on $\sigma := (1\ 3\ 4\ 2) \in S_4$: at each stage name the case, the transposition τ chosen, and the permutation passed down to the smaller symmetric group. Write down the word for σ the run produces, and check it.

(c) Where does the proof use Lemma 3.4.1, and for what?

(d) State the idea of the proof in two sentences.

Solution.

(a) In the base case. The induction starts at $n = 2$, where $\mathrm{id} = (1\ 2)(1\ 2)$ needs a transposition to exist. For $n = 1$, $S_1 = \{\mathrm{id}\}$ has no transposition at all (a transposition needs two distinct points), so id is a product of transpositions only as the empty product, which the definition of "product of transpositions" ($r \geq 1$) excludes.

(b) *First stage, in S_4.* $\sigma(4) = 2 \neq 4$: Case 2, with $k = 2$ and $\tau = (2\ 4)$. Then $\tau\sigma$, applying σ first: $1 \mapsto 3 \mapsto 3$, $3 \mapsto 4 \mapsto 2$, $2 \mapsto 1 \mapsto 1$, $4 \mapsto 2 \mapsto 4$. So $\tau\sigma = (1\ 3\ 2)$, which fixes 4, and Case 1 passes its restriction, the permutation $(1\ 3\ 2)$ of $\{1, 2, 3\}$, down to S_3.
Second stage, in S_3. $\sigma' := (1\ 3\ 2)$ has $\sigma'(3) = 2 \neq 3$: Case 2 again, with $\tau' = (2\ 3)$. Then $\tau'\sigma'$: $1 \mapsto 3 \mapsto 2$, $2 \mapsto 1 \mapsto 1$, $3 \mapsto 2 \mapsto 3$. So $\tau'\sigma' = (1\ 2)$, which fixes 3; Case 1 passes $(1\ 2) \in S_2$ down.
Base, in S_2. $(1\ 2)$ is one transposition.
Back up. $\tau'\sigma' = (1\ 2)$ gives $\sigma' = \tau'(1\ 2) = (2\ 3)(1\ 2)$, and then $\sigma = \tau(\tau\sigma) = (2\ 4)(2\ 3)(1\ 2)$, each transposition read in S_4 by fact 2 of the proof. Check, applying $(1\ 2)$ first: $1 \mapsto 2 \mapsto 3 \mapsto 3$, $3 \mapsto 3 \mapsto 2 \mapsto 4$, $4 \mapsto 4 \mapsto 4 \mapsto 2$, $2 \mapsto 1 \mapsto 1 \mapsto 1$. So $1 \mapsto 3 \mapsto 4 \mapsto 2 \mapsto 1$, which is $(1\ 3\ 4\ 2)$.
The second route of the remark after the theorem gives another word: by Proposition 3.5.1, $(1\ 3\ 4\ 2) = (1\ 2)(1\ 4)(1\ 3)$ (check: $1 \mapsto 3 \mapsto 3 \mapsto 3$, $3 \mapsto 1 \mapsto 4 \mapsto 4$, $4 \mapsto 4 \mapsto 1 \mapsto 2$, $2 \mapsto 2 \mapsto 2 \mapsto 1$). That is a correct word, but it is not the run asked for. Neither is $(2\ 4)(1\ 2)(1\ 3)$, which applies one Case-2 step and then the cycle formula to $\tau\sigma = (1\ 3\ 2)$; it is a third valid word.

(c) In two places. In the paragraph opening the Step, part (b) of the lemma says that $\rho \mapsto \overline{\rho}$ is the inverse of the isomorphism $\sigma \mapsto \sigma'$ from S' onto S_n; so, by Proposition 3.3.2 (b),

the extension is a homomorphism, the product of extensions being taken in S_{n+1}. Fact 1 rests on this. In Case 1, part (a) says that a permutation σ of $\{1,\dots,n+1\}$ fixing $n+1$ restricts to a permutation σ' of $\{1,\dots,n\}$, to which the induction hypothesis applies, and part (b) says that extending σ' back gives σ, so that the extension carries the word for σ' to a word for σ.

(d) Induct on n: a permutation that fixes the last point is a permutation of one point fewer, so the induction hypothesis writes it as transpositions. A permutation that moves the last point is brought to that case by one transposition, which is then undone.

3.5.5.2 B. Practice

Exercise. B1

Write $(1\ 2\ 3\ 4\ 5)$ and $(1\ 5)(2\ 4)$ as products of transpositions, and then as products of adjacent transpositions. Check one of your adjacent words point by point.

Solution. Transpositions. By Proposition 3.5.1, $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$. The permutation $(1\ 5)(2\ 4)$ is already a product of two transpositions.

Adjacent transpositions. A word of neighbor swaps for the 5-cycle can be checked directly:

$$(1\ 2\ 3\ 4\ 5) = (1\ 2)(2\ 3)(3\ 4)(4\ 5).$$

Check, applying $(4\ 5)$ first: $1 \mapsto 1 \mapsto 1 \mapsto 1 \mapsto 2$; $2 \mapsto 2 \mapsto 2 \mapsto 3 \mapsto 3$; $3 \mapsto 3 \mapsto 4 \mapsto 4 \mapsto 4$; $4 \mapsto 5 \mapsto 5 \mapsto 5 \mapsto 5$; $5 \mapsto 4 \mapsto 3 \mapsto 2 \mapsto 1$. So $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 1$, as required.

For $(1\ 5)(2\ 4)$, use $(*)$ of the corollary's proof repeatedly: $(1\ 5) = (1\ 2)(2\ 5)(1\ 2)$, $(2\ 5) = (2\ 3)(3\ 5)(2\ 3)$, $(3\ 5) = (3\ 4)(4\ 5)(3\ 4)$, and $(2\ 4) = (2\ 3)(3\ 4)(2\ 3)$. Joining the words (Proposition 3.1.2 (a)),

$$\begin{aligned}(1\ 5)(2\ 4) = (1\ 2)(2\ 3)(3\ 4)(4\ 5)(3\ 4)(2\ 3)(1\ 2)\\ \cdot (2\ 3)(3\ 4)(2\ 3),\end{aligned}$$

a word of ten adjacent transpositions.

Exercise. B2

Let $n \geq 2$ and $\rho := (1\ 2\ \cdots\ n) \in S_n$ (for $n = 2$, $\rho = (1\ 2)$).

(a) Prove that $\sigma(a\ b)\sigma^{-1} = (\sigma(a)\ \sigma(b))$ for every $\sigma \in S_n$ and every transposition $(a\ b) \in S_n$.

(b) Prove that $\rho^{i-1}(1\ 2)\rho^{-(i-1)} = (i\ \ i{+}1)$ for $1 \leq i \leq n-1$.

(c) Deduce that every $\sigma \in S_n$ is a product of factors each equal to $(1\ 2)$, ρ or ρ^{-1}.

Solution.

(a) The points $\sigma(a)$, $\sigma(b)$ are distinct, since σ is injective, so the right-hand side is a transposition. Check point by point, applying σ^{-1} first. For $x = \sigma(a)$: $\sigma^{-1}(x) = a \mapsto b \mapsto \sigma(b)$. For $x = \sigma(b)$: $\sigma^{-1}(x) = b \mapsto a \mapsto \sigma(a)$. For any other x: $\sigma^{-1}(x) \notin \{a, b\}$ (otherwise $x = \sigma(\sigma^{-1}(x))$ would be $\sigma(a)$ or $\sigma(b)$), so $(a\ b)$ fixes it, and $\sigma(\sigma^{-1}(x)) = x$.

These are the values of $(\sigma(a)\ \sigma(b))$ (Sets, Relations, and Cardinality, Proposition 1.4.1).

(b) First, $\rho^m(j) = j + m$ whenever $m \in \mathbb{N}$, $j \geq 1$ and $j + m \leq n$. By induction on m: $\rho^0 = \mathrm{id}$; and if it holds for m and $j+m+1 \leq n$, then $\rho^{m+1} = \rho^m\rho$ (Definition 3.1.3), so $\rho^{m+1}(j) = \rho^m(j+1) = j+1+m$, using $\rho(j) = j+1$ for $j < n$ (Definition 3.4.2). Now let $1 \leq i \leq n-1$ and $\sigma := \rho^{i-1}$. Then $\sigma(1) = i$ and $\sigma(2) = i+1$, since $2+(i-1) \leq n$, and $\sigma^{-1} = \rho^{-(i-1)}$ by Proposition 3.1.3 (b). By (a), $\rho^{i-1}(1\ 2)\rho^{-(i-1)} = (i\ \ i{+}1)$.

(c) By Corollary 3.5.3, σ is a product of adjacent transpositions. By (b), each $(i\ \ i{+}1)$ equals $\rho^{i-1}(1\ 2)\rho^{-(i-1)}$, where ρ^{i-1} is the product of $i-1$ factors ρ and $\rho^{-(i-1)} = (\rho^{-1})^{i-1}$ the product of $i-1$ factors ρ^{-1} (Definition 3.1.3, Proposition 3.1.3 (b)). Joining all these words by Proposition 3.1.2 (a) writes σ as required.

3.5.5.3 C. Going deeper

Exercise. C1: Exit check: transpositions generate

Let $n \geq 2$. State and prove that every $\sigma \in S_n$ is a product of transpositions.

Solution. Statement. For $n \geq 2$, every $\sigma \in S_n$ is $\tau_1 \cdots \tau_r$ for some $r \geq 1$ and transpositions $\tau_j \in S_n$ (Theorem 3.5.2).

Proof. Induction on $n \geq 2$ (Sets, Relations, and Cardinality, Theorem 2.2.1 with base 2). For $n = 2$, a bijection σ of $\{1,2\}$ has $\sigma(1) = 1$, and then $\sigma(2) = 2$ by injectivity, or $\sigma(1) = 2$ and $\sigma(2) = 1$; so $S_2 = \{\mathrm{id}, (1\ 2)\}$, and $\mathrm{id} = (1\ 2)(1\ 2)$.

Suppose the statement for $n \geq 2$, and let $\sigma \in S_{n+1}$.

If $\sigma(n+1) = n+1$, then $\sigma(i) \neq n+1$ for $i \leq n$ by injectivity, so σ restricts to an injective map $\sigma' \colon \{1,\ldots,n\} \to \{1,\ldots,n\}$. It is onto: for $j \leq n$, $j = \sigma(i)$ for some i, and $i \neq n+1$ because $\sigma(n+1) = n+1 \neq j$. So $\sigma' \in S_n$ (Lemma 3.4.1), and $\sigma' = \tau_1 \cdots \tau_r$ by the hypothesis. Extending each permutation of $\{1,\ldots,n\}$ by $n+1 \mapsto n+1$ is the inverse of the restriction isomorphism of Lemma 3.4.1 (b), so it is a homomorphism (Proposition 3.3.2 (b)). By induction on r, using the recursion of Definition 3.1.2 (fact 1 in the proof of Theorem 3.5.2), it carries this word to the word $\overline{\tau_1} \cdots \overline{\tau_r}$ in S_{n+1}, each $\overline{\tau_j}$ the transposition of the same two points; and it carries σ' to σ. Hence $\sigma = \overline{\tau_1} \cdots \overline{\tau_r}$.

If $\sigma(n+1) = k \neq n+1$, let $\tau := (k\ \ n{+}1)$. Then $(\tau\sigma)(n+1) = \tau(k) = n+1$, so by the first case $\tau\sigma = \tau_1 \cdots \tau_r$ with transpositions in S_{n+1}. Since $\tau\tau = \mathrm{id}$, $\sigma = \tau(\tau\sigma) = \tau\tau_1 \cdots \tau_r$. This completes the induction.

Marking scheme. (10 points)

- 2: sets up induction on n with base $n = 2$, and handles S_2, including id as a product of transpositions.
- 3: Case $\sigma(n+1) = n+1$: reduces to S_n, with the restriction shown to be a permutation of $\{1,\ldots,n\}$ (surjectivity justified, or Lemma 3.4.1 cited).
- 3: Case $\sigma(n+1) = k \neq n+1$: chooses a transposition τ with $\tau\sigma$ fixing $n+1$, and computes $(\tau\sigma)(n+1) = n+1$.
- 1: undoes τ, using $\tau^{-1} = \tau$.
- 1: says why transpositions of S_n, extended, are transpositions of S_{n+1} and the extended word still equals σ.

Fatal errors (0 for the step): using "σ is a product of transpositions in S_{n+1}" inside its own

proof (circular); assuming the cycle decomposition or the cycle formula without citing it as proved.

Second route (accepted, 10 points).

- 3: cites Theorem 3.4.4 as proved, writing σ as a product of disjoint cycles.
- 3: writes each cycle as transpositions by Proposition 3.5.1, cited or proved, with the factors in the right (right-to-left) order.
- 2: handles $\sigma = \mathrm{id}$ as $(1\ 2)(1\ 2)$, using $n \geq 2$.
- 2: joins the words into one product of transpositions (Proposition 3.1.2 (a)).

Third route (accepted, 10 points): strong induction on $|\operatorname{supp}\sigma|$ (finite, as a subset of $\{1, \ldots, n\}$).

- 2: sets up the induction and handles the base $\operatorname{supp}\sigma = \emptyset$, that is, $\sigma = \mathrm{id} = (1\ 2)(1\ 2)$, using $n \geq 2$.
- 3: for $\sigma \neq \mathrm{id}$, picks i with $j := \sigma(i) \neq i$ and $\tau := (i\ j)$, and shows that $\tau\sigma$ fixes i and every point that σ fixes (such a point is neither i nor j, by injectivity).
- 3: concludes $\operatorname{supp}(\tau\sigma) \subseteq \operatorname{supp}\sigma \setminus \{i\}$, so the hypothesis applies to $\tau\sigma$ (or $\tau\sigma = \mathrm{id}$, and $\sigma = \tau$).
- 1: undoes τ, using $\tau^{-1} = \tau$.
- 1: joins the words (Proposition 3.1.2 (a)).

Exercise. C2: Find the error

Here is an argument.

> **Claim.** Every cycle is a product of transpositions.
>
> **Proof.** (1) Let $\gamma = (i_1\ i_2\ \cdots\ i_k)$ with $k \geq 2$ and distinct entries. (2) The cycle sends i_1 to i_2, then i_2 to i_3, and so on, up to i_k, which it sends back to i_1. (3) The swap $(i_1\ i_2)$ takes i_1 to i_2; the swap $(i_1\ i_3)$ is next; and so on. (4) Hence $\gamma = (i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_k)$. (5) So γ is a product of $k-1$ transpositions.

Is the claim true? Does the argument prove it? Name the line that fails and the reason, give a counterexample to the illegal step, and repair the argument.

Solution. **The claim is true:** it is Proposition 3.5.1. **The argument does not prove it.**

Line (4) fails, on the strength of line (3). Line (3) lists the transpositions in the order in which they should **act**, and line (4) writes them left to right in that order. But a product of permutations acts right to left (Definition 3.4.1): in $(i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_k)$ the factor $(i_1\ i_k)$ acts first. The equation of line (4) is an unproved "fact", and a false one: entry (N9) of Logic and Proof, Example (What is not allowed). Lines (1), (2) and (5) are correct.

Counterexample to the step. For $k = 3$ and $\gamma = (1\ 2\ 3)$, line (4) claims $(1\ 2\ 3) = (1\ 2)(1\ 3)$. But $(1\ 2)(1\ 3) = (1\ 3\ 2)$ (Example (Computing with Cycles)), and $(1\ 3\ 2) \neq (1\ 2\ 3)$, since the first sends 1 to 3 and the second sends 1 to 2. There is no counterexample to the conclusion.

In fact the product in line (4) is γ^{-1}: by Proposition 3.1.2 (c), the inverse of $(i_1\ i_k)\cdots(i_1\ i_2) = \gamma$ is the reversed product of the inverses, and each transposition is its own inverse.

Repair. Reverse the order of the factors: $\gamma = (i_1\ i_k)(i_1\ i_{k-1})\cdots(i_1\ i_2)$, and prove it as in

Proposition 3.5.1, by induction on k with a point-by-point check of $(i_1\ i_{k+1})(i_1\ \cdots\ i_k) = (i_1\ \cdots\ i_{k+1})$.

Marking scheme. (10 points)

- 2: says the claim is true and the argument does not prove it.
- 3: names line (4) (or lines (3)–(4) together) and the reason: the factors are written in the order they should act, but products act right to left.
- 2: a counterexample to the step, such as $(1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3)$.
- 3: gives a correct formula for γ as a product of transpositions and justifies it. For the reversed product $(i_1\ i_k)\cdots(i_1\ i_2)$, the induction or a citation of Proposition 3.5.1 is enough. For another word, such as $(i_1\ i_2)(i_2\ i_3)\cdots(i_{k-1}\ i_k)$, the reader must prove it, by induction on k or by a point-by-point check for general k.

Fatal errors (0 for the step): a counterexample to the conclusion (there is none); a "repair" that keeps line (4)'s product and silently replaces γ by another cycle (such as γ^{-1}).

Exercise. C3

(a) Let $\sigma \in S_n$ and let $(i_1\ \cdots\ i_k) \in S_n$ be a cycle. Prove that $\sigma(i_1\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \cdots\ \sigma(i_k))$.

(b) Deduce that any two transpositions of S_n are conjugate: for transpositions τ, τ' there is $\pi \in S_n$ with $\tau' = \pi\tau\pi^{-1}$.

Solution.

(a) Write $\gamma := (i_1\ \cdots\ i_k)$, and read indices so that i_{k+1} means i_1. The points $\sigma(i_1), \ldots, \sigma(i_k)$ are distinct, since σ is injective, so the right-hand side is a k-cycle. For $x = \sigma(i_j)$: $\sigma^{-1}(x) = i_j \mapsto i_{j+1} \mapsto \sigma(i_{j+1})$. For x not among the $\sigma(i_j)$: $\sigma^{-1}(x)$ is not among the i_j, so γ fixes it, and $\sigma\gamma\sigma^{-1}(x) = x$. These are the values of $(\sigma(i_1)\ \cdots\ \sigma(i_k))$.

(b) Here $n \geq 2$, since a transposition exists. First, every transposition $(a\ b)$, written with $a < b$, is conjugate to $(1\ 2)$: by (a) it suffices to find π with $\pi(1) = a$, $\pi(2) = b$. If $(a, b) = (1, 2)$, take $\pi = \mathrm{id}$. If $a = 1$ and $b \geq 3$, take $\pi = (2\ b)$. If $a \geq 2$, then $b \geq 3$; take $\pi = (1\ a)(2\ b)$: applying $(2\ b)$ first, $1 \mapsto 1 \mapsto a$, and $2 \mapsto b \mapsto b$, since $b \neq 1$ and $b \neq a$. Now let $\tau = \pi(1\ 2)\pi^{-1}$ and $\tau' = \pi'(1\ 2)\pi'^{-1}$. Then $(1\ 2) = \pi^{-1}\tau\pi$, and

$$\tau' = \pi'\pi^{-1}\tau\pi\pi'^{-1} = (\pi'\pi^{-1})\tau(\pi'\pi^{-1})^{-1},$$

by Proposition 3.1.2 (c) and Theorem 3.1.1 (3). Conjugacy in S_n is studied in the chapter "Symmetric Groups and the Sign of a Permutation" of *Groups*.

Marking scheme. (10 points)

- 2: notes that the $\sigma(i_j)$ are distinct (σ injective), so the right side of (a) is a k-cycle.
- 2: checks $\sigma\gamma\sigma^{-1}(\sigma(i_j)) = \sigma(i_{j+1})$, including the wrap-around $j = k$.
- 2: checks that every x outside $\{\sigma(i_1), \ldots, \sigma(i_k)\}$ is fixed.
- 3: for transpositions $(a\ b)$, $(c\ d)$, exhibits a permutation π with $\{\pi(a), \pi(b)\} = \{c, d\}$, covering every case of overlap between $\{a, b\}$ and $\{c, d\}$; directly or through $(1\ 2)$.
- 1: applies (a) with $k = 2$ to conclude $\tau' = \pi\tau\pi^{-1}$, or composes the two conjugations by $(1\ 2)$ using $(\pi'\pi^{-1})^{-1} = \pi\pi'^{-1}$.

Fatal errors (0 for the step): a proof of (a) that only asserts the formula (0 for the three (a) items); π is not a bijection, or is built only for disjoint (or only for overlapping) pairs. Part (b) may use (a) even where (a) was not proved.

3.5.5.4 R. Review

Exercise. R1

Let F be a field. Show that $\varphi(k) \coloneqq k \cdot 1_F$ defines a homomorphism $(\mathbb{Z}, +) \to (F, +)$, that $\ker \varphi = m\mathbb{Z}$ for exactly one $m \in \mathbb{N}$, and that this m is 0 or a prime.

Solution. Homomorphism. In additive notation, Proposition 3.1.3 (a) says $(k + l) \cdot 1_F = k \cdot 1_F + l \cdot 1_F$ for all $k, l \in \mathbb{Z}$, the multiples being those of the group $(F, +)$ (Definition 3.1.3). That is $\varphi(k + l) = \varphi(k) + \varphi(l)$. By Proposition 3.1.3 (e), for $k \in \mathbb{N}$ these group multiples are the multiples of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 2.3, which are the multiples of Lemma 2.5.1; that lemma is applied below only to natural numbers.

Kernel. $\ker \varphi$ is a subgroup of $\mathbb{Z}$ (Theorem 3.3.1 (c)), so $\ker \varphi = m\mathbb{Z}$ for exactly one $m \in \mathbb{N}$ (Theorem 3.2.4): $m = 0$ if the kernel is $\{0\}$, and otherwise m is its least positive element.

m is 0 or prime. $m \neq 1$: $1 \cdot 1_F = 1_F$ (Definition 3.1.3), and $1_F \neq 0_F$ in a field (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1), so $1 \notin \ker \varphi$. Suppose $m \geq 2$ were not prime. By Sets, Relations, and Cardinality, Definition 2.2.2 it has a positive divisor $a \notin \{1, m\}$; write $m = ab$ with $b \in \mathbb{Z}$. Then $b > 0$, as $a, m > 0$; $a \leq m$ and $b \leq m$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e); and $b \neq m$, since $b = m$ would give $a = 1$ (cancel $m \neq 0$ in $\mathbb{Z}$). So $0 < a < m$ and $0 < b < m$. By Lemma 2.5.1 (b),

$$(a \cdot 1_F)(b \cdot 1_F) = (ab) \cdot 1_F = m \cdot 1_F = 0_F.$$

But $a \notin m\mathbb{Z}$: if $m \mid a$ with $a > 0$, then $m \leq a$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e), against $a < m$. So $a \cdot 1_F \neq 0_F$, and in the same way $b \cdot 1_F \neq 0_F$. A field has no zero divisors (Theorem 2.1.1 (f)): a contradiction. So m is 0 or prime.

This is a group-theoretic route to Chapter 2's characteristic. The number m is $\operatorname{char} F$ (Definition 2.5.1): if $m > 0$ it is the least positive n with $n \cdot 1_F = 0_F$, and $m = 0$ exactly when there is none. The result is Theorem 2.5.3, whose proof there runs the same argument without the language of kernels.

Exercise. R2

Show that $(\mathbb{Z}/6\mathbb{Z}, +) \cong ((\mathbb{Z}/7\mathbb{Z})^\times, \cdot)$, and that $(\mathbb{Z}/6\mathbb{Z}, +) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Solution. The first isomorphism. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2, $\mathbb{Z}/7\mathbb{Z}$ is a field, so every non-zero class is a unit, while $[0]$ is not ($[0][x] = [0] \neq [1]$). So the units are the six classes $[1], \ldots, [6]$, distinct by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b), and they form a group by Proposition 3.1.4. Compute the powers of $[3]$:

$$[3]^0, [3]^1, \ldots, [3]^5 = [1], [3], [2], [6], [4], [5],$$

from $3 \cdot 3 = 9 = 7 + 2$, $2 \cdot 3 = 6$, $6 \cdot 3 = 18 = 14 + 4$, $4 \cdot 3 = 12 = 7 + 5$, and then $[3]^6 = [5][3] = [15] = [1]$.

Define $f([k]) \coloneqq [3]^k$. *Well defined:* if $[k] = [k']$ in $\mathbb{Z}/6\mathbb{Z}$, then $k' = k + 6q$ with $q \in \mathbb{Z}$, and by Proposition 3.1.3 (a), (c),

$$[3]^{k'} = [3]^k([3]^6)^q = [3]^k[1]^q = [3]^k,$$

since every power of the identity is the identity (Definition 3.1.3, by induction on $q \in \mathbb{N}$, and for $q < 0$ because $[1]^{-1} = [1]$). *A homomorphism:* $f([k] + [l]) = f([k + l]) = [3]^{k+l} = [3]^k[3]^l = f([k])f([l])$, by Proposition 3.1.3 (a). *Bijective:* the six classes $[0], \ldots, [5]$ of $\mathbb{Z}/6\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)) go to the six distinct units listed above, which are all of $(\mathbb{Z}/7\mathbb{Z})^\times$. So f is an isomorphism (Definition 3.3.1).

The second isomorphism. $1 = 3 \cdot 1 + 2 \cdot (-1)$, so 2 and 3 are coprime (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.2.2). By Example (Homomorphisms) (e), which rests on Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3 (b), $[x]_6 \mapsto ([x]_2, [x]_3)$ is an isomorphism of additive groups $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

The method is that of Example (Isomorphic and Non-Isomorphic Small Groups) (b), where [2] played the role of [3] modulo 5.

Exercise. R3

Let X be a set. Show that the permutations $\sigma \in S_X$ with $\operatorname{supp}\sigma$ finite form a subgroup of S_X.

Solution. Let $H \coloneqq \{\sigma \in S_X : \operatorname{supp}\sigma \text{ is finite}\}$. We use Theorem 3.2.1. $H \neq \emptyset$: $\operatorname{supp}\mathrm{id}_X = \emptyset$, which has 0 elements (Sets, Relations, and Cardinality, Definition 3.1.2).

Let $\sigma, \tau \in H$. If $x \notin \operatorname{supp}\sigma \cup \operatorname{supp}\tau$, then $\tau(x) = x$, so $\tau^{-1}(x) = x$, and $\sigma(x) = x$; hence $\sigma\tau^{-1}(x) = x$. So

$$\operatorname{supp}(\sigma\tau^{-1}) \subseteq \operatorname{supp}\sigma \cup \operatorname{supp}\tau = \operatorname{supp}\sigma \cup (\operatorname{supp}\tau \setminus \operatorname{supp}\sigma).$$

The set $\operatorname{supp}\tau \setminus \operatorname{supp}\sigma$ is finite, as a subset of the finite set $\operatorname{supp}\tau$ (Sets, Relations, and Cardinality, Proposition 3.1.6); it is disjoint from $\operatorname{supp}\sigma$, so the union is finite (Sets, Relations, and Cardinality, Proposition 3.1.5); and $\operatorname{supp}(\sigma\tau^{-1})$, a subset of it, is finite (Sets, Relations, and Cardinality, Proposition 3.1.6). So $\sigma\tau^{-1} \in H$, and H is a subgroup.

For an infinite X the subgroup can be proper. On $X = \mathbb{Z}$, the translation $\sigma(x) \coloneqq x + 1$ is a bijection (its inverse is $x \mapsto x - 1$) that moves every point, since $x + 1 \neq x$. Its support $\mathbb{Z}$ is not finite: $x \mapsto 2x$ is a bijection from $\mathbb{Z}$ onto $2\mathbb{Z}$ (injective by cancellation, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (f)), and $2\mathbb{Z} \neq \mathbb{Z}$ since $1 \notin 2\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (g)), which a finite set does not allow (Sets, Relations, and Cardinality, Theorem 3.1.9).

Exercise. R4

Let G be a finite group with an even number of elements. Prove that some $g \in G$ with $g \neq e$

has $g^2 = e$.

Solution. The tool is to pair each element with its inverse. Define $g \sim h$ on G by $h \in \{g, g^{-1}\}$. It is an equivalence relation (Sets, Relations, and Cardinality, Definition 2.5.1): reflexive since $g \in \{g, g^{-1}\}$; symmetric since $h = g^{-1}$ gives $g = h^{-1}$ (Theorem 3.1.1 (3)); transitive since $h \in \{g, g^{-1}\}$ and $k \in \{h, h^{-1}\}$ give $k \in \{g, g^{-1}, (g^{-1})^{-1}\} = \{g, g^{-1}\}$. The class of g is $\{g, g^{-1}\}$, and the classes partition G (Sets, Relations, and Cardinality, Theorem 2.5.1).

A class has one element exactly when $g = g^{-1}$, that is, when $g^2 = e$: if $g = g^{-1}$, then $g^2 = gg^{-1} = e$; if $g^2 = e$, then g is an inverse of g, so $g = g^{-1}$ by uniqueness of inverses (Theorem 3.1.1 (2)). Let $T := \{g \in G : g^2 = e\}$, the union of the one-element classes, and $U := G \setminus T$, the union of the two-element classes; both are finite, as subsets of G (Sets, Relations, and Cardinality, Proposition 3.1.6).

$|U|$ is even. We show, by Logic and Proof, Theorem 4.2.2 on j, that every subset $V \subseteq U$ with j elements that contains g^{-1} whenever it contains g has an even number of elements. If $j = 0$, this holds. If $j \geq 1$, pick $g \in V$; then $g^{-1} \in V$ and $g^{-1} \neq g$ (as $g \notin T$), so $\{g, g^{-1}\}$ has 2 elements, and $V' := V \setminus \{g, g^{-1}\}$ again contains the inverse of each of its elements: if $h \in V'$, then $h^{-1} \in V$, and $h^{-1} \notin \{g, g^{-1}\}$, since otherwise $h = (h^{-1})^{-1} \in \{g^{-1}, g\}$ by Theorem 3.1.1 (3). As V is the disjoint union of V' and $\{g, g^{-1}\}$, $j = |V'| + 2$ (Sets, Relations, and Cardinality, Proposition 3.1.5 with Sets, Relations, and Cardinality, Corollary 3.1.4), so V' has $j - 2 < j$ elements; that number is even by the hypothesis, so j is even. Apply this to $V = U$.

Conclusion. $G = T \cup U$ is a disjoint union, so $|G| = |T| + |U|$ (Sets, Relations, and Cardinality, Proposition 3.1.5). With $|G|$ and $|U|$ even, $|T| = |G| - |U|$ is even. Since $e \in T$, $|T| \geq 1$, so $|T| \geq 2$: an even number cannot be 1, as $2 \nmid 1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (g)). So T contains some $g \neq e$, and $g^2 = e$.

Look-alikes. Lagrange's theorem (the chapter "Cosets and Lagrange's Theorem" of *Groups*) and Cauchy's theorem (the chapter "Group Actions, the Orbit–Stabilizer Theorem, and the Class Equation" of *Groups*) would give this, but neither is available here. "Pick $g \neq e$ and square it" does not work: in $(\mathbb{Z}/6\mathbb{Z}, +)$, where the condition reads $2 \cdot g = [0]$, the element $g = [1]$ has $2 \cdot [1] = [2] \neq [0]$; the element that works there is $[3]$, and the pairing argument shows that such an element exists without searching for it.

Chapter 4

Formal Polynomials

At school a polynomial is "an expression in x", and x is a number not yet chosen. Over the field $\mathbb{F}_2$ of Chapter 2 this picture breaks at once: $x^2 + x$ takes the value 0 at both elements, so as a function it is the zero function, yet we want it to have degree 2. This chapter therefore decides that a polynomial **is** its list of coefficients, a sequence with only finitely many non-zero entries, and that x is the name of a position, never a number. From that one decision it builds the polynomial ring $R[x]$ over any commutative ring R of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2, and proves its laws with one device, **check on monomials, extend by additivity**, so that no double sum is ever reordered. It then attaches the degree and the leading coefficient, recovers "plugging in" as a ring homomorphism, and defines the derivative by its coefficients, with no limit in sight.

Which school rules survive depends on R, and the chapter keeps count. Over $\mathbb{Z}/6\mathbb{Z}$ the degree of a product can drop, because $[2][3] = [0]$. Over $\mathbb{Z}/4\mathbb{Z}$ the polynomial $1 + [2]x$ is its own inverse. Over every finite ring with $1 \neq 0$ some non-zero polynomial vanishes at every element, so a polynomial is not its function. Over $\mathbb{F}_p$ the derivative of x^p is 0. Each result says what it needs from R: nothing at all, no zero divisors, a unit leading coefficient, finiteness with $1 \neq 0$, or, for the derivative, the characteristic of a field. The chapter ends where Chapter 5 begins, with $R = F$ a field and division with remainder still to come.

One construction, many rings. The linear-algebra companion defines polynomials over a field F, and its later chapters cite this chapter's results with F a field. Every such statement is the case $R = F$ of the statement proved here for a commutative ring, since a field is a commutative ring. Where a result really needs more than a commutative ring, the hypothesis is named at the point of use: no zero divisors (Theorem 4.3.2 (b), Corollary 4.3.3, Proposition 4.3.4), a unit leading coefficient (Theorem 4.3.2 (b)), R finite with $1 \neq 0$ (Proposition 4.4.4 (d)), or the characteristic of a field (Proposition 4.5.2).

What you need. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapters 2 and 3 above all, with index arithmetic in $\mathbb{N}$ from its Chapter 1; Chapter 2 of this volume; *Sets, Relations, and Cardinality*, Chapters 1 and 3 and Section 2.3 (and Section 2.5 for R3); and induction from *Logic and Proof*, Chapter 3.

- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2: commutative rings, with $1 = 0$ allowed, and their algebra (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2); the multiples $n \cdot a$ of the "Multiples" paragraph of its Section 2.3; $\mathbb{Z}$ as an ordered commutative ring with a greatest element in every non-empty set bounded above (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.4,

Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6); the field $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3); and the copies $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4). From its Chapter 1, the laws and the order of $\mathbb{N} = \omega$ (Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3, Number Systems: From \(\nN\) to \(\nR\), Theorem 1.5.3, Number Systems: From \(\nN\) to \(\nR\), Theorem 1.6.1).

- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3: division with remainder and the rules for divisibility (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1); ideals and quotient rings (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1); the rings $\mathbb{Z}/n\mathbb{Z}$ and the example $\mathbb{Z}/6\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3, Number Systems: From \(\nN\) to \(\nR\), Example (Multiplication modulo six and modulo five)); units, the field $\mathbb{Z}/p\mathbb{Z}$ and the Chinese remainder map (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3). Section 4.3 also pays a debt to its Chapter 4: the polynomial algebra that the field $\mathbb{Q}(t)$ of Number Systems: From \(\nN\) to \(\nR\), Example (A Non-Archimedean Ordered Field) took on school credit.
- From Chapter 2: fields and the rule that a product of non-zero elements is non-zero (Definition 2.1.1, Theorem 2.1.1); $\mathbb{F}_p$ and the tables of $\mathbb{F}_2$ (Definition 2.2.1, Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$)); finite sums and integer multiples in a commutative ring (Lemma 2.6.1, Lemma 2.5.1); the characteristic, 0 or a prime (Definition 2.5.1, Theorem 2.5.3); and, for Section 4.4's Exercise C4, Fermat's little theorem (Theorem 2.6.6).
- From *Sets, Relations, and Cardinality*: functions and their equality, products and bijections (Sets, Relations, and Cardinality, Definition 1.4.1, Sets, Relations, and Cardinality, Proposition 1.4.1, Sets, Relations, and Cardinality, Definition 1.3.2, Sets, Relations, and Cardinality, Definition 1.4.5), from Chapter 1; the recursion theorem, with its sums, products and powers used as patterns (Sets, Relations, and Cardinality, Theorem 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.2), from Section 2.3; finite sets (Sets, Relations, and Cardinality, Definition 3.1.2, Sets, Relations, and Cardinality, Proposition 3.1.6), from Chapter 3.
- From *Logic and Proof*: induction (Logic and Proof, Axiom 4.2.1), from Section 3.2, and, for the two find-the-error exercises, the catalogue of moves that are not allowed (Logic and Proof, Example (What is not allowed)), from Section 5.6.

Chapters 1 and 3 enter only through the review exercises of Section 4.5: the complex numbers and their conjugate in R2, groups and their homomorphisms in R1. The countability results of *Sets, Relations, and Cardinality*, Chapter 3, and its quotient sets (Sets, Relations, and Cardinality, Definition 2.5.4, Section 2.5) enter only through R3. Sections 4.1 and 4.4 also compare two results with Chapter 1 (Proposition 1.1.3, Lemma 1.1.4) without using them. Outside R2, no proof in the chapter uses $\mathbb{R}$ or $\mathbb{C}$.

Time. About 25 hours on the core track (all of A, one B and one C per section, the exit checks); about 35 hours for everything.

4.0.1 Roadmap

- **Polynomials as Coefficient Sequences.** Why "an expression in x" fails over $\mathbb{F}_2$; a polynomial over a commutative ring as a sequence $\mathbb{N} \to R$ with only finitely many non-zero entries, with monomials, $x = (0, 1, 0, \dots)$, equality by comparing coefficients, the

display $\sum_k p_k x^k$ as notation only, the zero ring, and the non-example $(1, 1, 1, \dots)$; and a lemma collecting finite sums (which need only an addition), products of lists, powers and multiples, with the proofs of its new parts in a second-reading fold.

- **The Polynomial Ring.** The sum taken position by position and the product as a convolution, closed in $R[x]$ and computed over $\mathbb{Q}$, $\mathbb{F}_3$ and $\mathbb{Z}/6\mathbb{Z}$; every polynomial an honest sum of its monomials; multiplication by a monomial as a shift and a scaling; the lemma that two maps additive in each argument and equal on monomials are equal; and the theorem that $R[x]$ is a commutative ring containing R as its constants, with associativity proved on monomials instead of by reordering double sums.
- **Degree, Leading Coefficients, and Integral Domains.** Degree with $\deg 0 = -\infty$, the leading coefficient and monic polynomials; the degree of a sum; the degree of a product, whose top coefficient is $\operatorname{lc}(p)\operatorname{lc}(q)$ in every commutative ring, so that degrees add exactly when that product is non-zero, as over a ring with no zero divisors or for a unit leading coefficient; integral domains, with $R[x]$ an integral domain exactly when R is; the units of $R[x]$ over an integral domain, and the non-constant unit $1 + [2]x$ over $\mathbb{Z}/4\mathbb{Z}$; and the sets $R[x]_{\leq n}$ and $R[x]_{=n}$.
- **Evaluation, Substitution, and Polynomial Functions.** The value $p(c)$, roots, and evaluation respecting sums and products; ring homomorphisms and two impostors; the substitution principle, that one ring homomorphism $R[x] \to S$ extends a given $\varphi\colon R \to S$ and sends x to a given s, and only one; changing coefficients along φ, with reduction modulo n and the exact condition for the degree to drop, and the composition $p \circ q$; and the ring R^R of functions, with polynomial composition matching composition of functions and, over every finite ring with $1 \neq 0$, a non-zero polynomial whose function is 0.
- **The Formal Derivative.** The derivative defined by $(f')_k = (k+1) \cdot f_{k+1}$, the role of the element $n \cdot 1$, and examples in five rings; the sum, product and power rules in every commutative ring, the product rule by checking on monomials; over a field, $f' = 0$ exactly for the constants in characteristic 0 and exactly for the polynomials in x^p in characteristic p; and review exercises that return to groups (Chapter 3), complex conjugation (Chapter 1) and countability (*Sets, Relations, and Cardinality*, Chapter 3).

4.0.2 Named moves

- **Compare coefficients.** Two polynomials are equal if and only if their coefficients agree in every position, so an identity in $R[x]$ is proved by computing the k-th coefficient of both sides for an arbitrary k. It is *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2's "reduce to the level below", now with sequences. Named in Section 4.1, it proves the additive laws and both distributive laws of $R[x]$ in Section 4.2 and the linearity of the derivative in Section 4.5.
- **Check on monomials, extend by additivity.** Two maps of up to three polynomial arguments that are additive in each argument, and agree when every argument is a monomial, agree everywhere (Lemma 4.2.3). It proves commutativity and associativity of the product in Section 4.2, evaluation and substitution respecting products in Section 4.4, and the product rule in Section 4.5. Exercise B2 of Section 4.2 leaves its last step to you, and Exercise C2 of Section 4.4 its second half.
- **Look at the top coefficient.** The coefficient of $x^{\deg p + \deg q}$ in pq is $\operatorname{lc}(p)\operatorname{lc}(q)$, and nothing sits above it; every question about the degree of a product becomes the question whether that one element of R is 0. It proves the degree formula in Section 4.3 and, through it, the absence of zero divisors and the units of $R[x]$; in Section 4.4 it shows that the product of the factors $x - c$ over a finite ring is monic, and Exercise B1 there uses it for the degree of a composition.
- **A homomorphism out of $R[x]$ is fixed by the constants and x.** To show that two

ring homomorphisms out of $R[x]$ agree, check that they agree on the constants and on x (Theorem 4.4.2 (b)). Named in Section 4.4, it proves there that composing polynomials matches composing their functions, and Exercise B3 of Section 4.4 uses it to invert the shift $p \mapsto p \circ (x + c)$.

4.1 Polynomials as Coefficient Sequences

At school a polynomial is an expression such as $3x^2 - x + 2$, and x is a number that has not been chosen yet. This chapter replaces that picture by a definition that works over every commutative ring of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2 (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1): over $\mathbb{Q}$, over the fields $\mathbb{F}_p$ of Chapter 2, and over rings such as $\mathbb{Z}/6\mathbb{Z}$, where a product of two non-zero elements can be zero. This section makes the one decision the whole chapter rests on: a polynomial **is** its list of coefficients. It then collects the finite sums, powers and multiples that the next sections compute with.

Throughout, R is a commutative ring, with $a - b \coloneqq a + (-b)$.

4.1.1 What goes wrong with "an expression in x"

Take the field $\mathbb{F}_2 = \{0, 1\}$ of Definition 2.2.1, in which $1 + 1 = 0$. Read $x^2 + x$ the school way, as a rule: replace x by an element c and compute $cc + c$. The tables of Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$) give

$$0 \cdot 0 + 0 = 0, \qquad 1 \cdot 1 + 1 = 1 + 1 = 0.$$

So the rule $c \mapsto cc + c$ and the rule $c \mapsto 0$ give the same output at both elements of $\mathbb{F}_2$. As functions $\mathbb{F}_2 \to \mathbb{F}_2$ they are equal, by Sets, Relations, and Cardinality, Proposition 1.4.1: same domain, same codomain, same values.

If a polynomial were the function it defines, then $x^2 + x$ would be the zero polynomial over $\mathbb{F}_2$. So would $x^3 + x$ and $x^4 + x^2$, which also give 0 at 0 and $1 + 1 = 0$ at 1. None of them would have a highest power of x, and the rule "the degree of a product is the sum of the degrees", which we want over every field, would fail for $x \cdot (x + 1) = x^2 + x$: degrees 1 and 1, product "zero". Over $\mathbb{Q}$ the problem never shows (Section 5.4 proves that over an infinite field a non-zero polynomial never gives the zero function), which is why school algebra can afford the picture. Over a finite ring with $1 \neq 0$ it cannot.

So we decide the other way. Two polynomials are the same when their coefficients are the same, and the letter x is not a number at all.

A polynomial is its list of coefficients; the letter x only marks the positions.

4.1.2 Polynomials over a commutative ring

A list of coefficients that goes on forever is a sequence, that is, a function on $\mathbb{N}$. We keep only the sequences that stop being non-zero.

Definition 4.1.1. Polynomial

Let R be a commutative ring. A **polynomial over** R (in the indeterminate x) is a function $p\colon \mathbb{N} \to R$, written $p = (p_0, p_1, p_2, \dots)$, such that **only finitely many** p_k are non-zero: **there exists** $N \in \mathbb{N}$ with $p_k = 0$ **for every** $k > N$. Such an N is called **admissible** for p.

The element p_k is the **coefficient of** x^k in p.

For $a \in R$ and $n \in \mathbb{N}$, the **monomial** $a\,x^n$ is the polynomial with a in position n and 0 in every other position. We set $x \coloneqq 1\,x^1$, and for $a \in R$ the **constant** a is the monomial $a\,x^0$. The **zero polynomial** is $0 \coloneqq (0, 0, 0, \dots)$. The set of all polynomials over R is written $R[x]$.

In words: the first clause says that a polynomial is an infinite list of elements of R, indexed from 0; the second says that from some position on, every entry is 0. The quantifiers are in the order "there is one N that works for every later k": a sequence with infinitely many non-zero entries, however sparse, is excluded. A monomial has at most one non-zero entry, so n is admissible for it, and it is a polynomial. The symbol x is the particular sequence $(0, 1, 0, 0, \dots)$: an element of $R[x]$, never an element of R, and never a variable that takes values.

Equality. Two polynomials $p, q \in R[x]$ are functions with the same domain $\mathbb{N}$ and the same codomain R. By Sets, Relations, and Cardinality, Proposition 1.4.1,

$$p = q \quad \iff \quad p_k = q_k \ \text{ for every } k \in \mathbb{N}.$$

To prove an identity between polynomials we therefore compute the k-th coefficient of both sides, for an arbitrary k. We call this move **compare coefficients**. It is *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2's "reduce to the level below" once more: a statement about polynomials becomes a statement about elements of R, one position at a time.

The display. If N is admissible for p, we write

$$p = \sum_{k=0}^{N} p_k x^k = p_0 + p_1 x + p_2 x^2 + \cdots + p_N x^N.$$

For now this is **notation only**. No addition of polynomials has been defined yet, so the plus signs are not an operation: the display names the sequence by listing its entries, each with a marker x^k for its position. We drop terms whose coefficient is 0, write ax for ax^1, a for ax^0, x^k for $1x^k$, and $-ax^k$ for $(-a)x^k$. So $3x^2 - x + 2$ over $\mathbb{Q}$ names the sequence with $p_0 = 2$, $p_1 = -1$, $p_2 = 3$ and $p_k = 0$ for $k \geq 3$. Section 4.2 defines the sum of two polynomials and proves that the display is then an honest sum of monomials.

There is one thing to check about the display. The admissible N is not unique: if N is admissible, so is every $M \geq N$, since $k > M$ implies $k > N$. Passing from N to M only adds the terms $0x^k$ for $N < k \leq M$, which the convention drops. So every admissible N names the same sequence, and the display is well defined.

Why "only finitely many". Two later uses need it. In Section 4.4 we put an element $c \in R$ in place of x and form $\sum_k p_k c^k$; in a ring only finite sums are defined, and finiteness is what makes the sum finite. In Section 4.3 every non-zero polynomial gets a degree, the highest position holding a non-zero coefficient; without finiteness there may be no highest position.

The degenerate cases. The zero polynomial has every N admissible, including $N = 0$, and it is the monomial $0\,x^n$ for every n. It is the one polynomial with no non-zero coefficient at all, and Section 4.3 will need a convention for its degree. At the other extreme, let R be the zero ring $\{0\}$ of the examples after Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1, where $1 = 0$. There is exactly one function $\mathbb{N} \to \{0\}$, so $R[x]$ has exactly one element, the zero polynomial, and $x = 1\,x^1 = 0\,x^1 = 0$. This is why some results below assume $1 \neq 0$ in R.

Example. Reading off coefficient sequences

Write the coefficient sequence of each polynomial, and check it against Definition 4.1.1. In a ring $\mathbb{Z}/n\mathbb{Z}$, a natural number m written as an element stands for $m \cdot [1] = [m]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d)), just as Definition 2.2.1 does for $\mathbb{F}_p$.

(a) $3x^2 - x + 2 \in \mathbb{Q}[x]$.
(b) $x^2 + x \in \mathbb{F}_2[x]$.
(c) $[3]x + [4] \in (\mathbb{Z}/6\mathbb{Z})[x]$.
(d) The constant 7, over $\mathbb{Z}$, over $\mathbb{Z}/5\mathbb{Z}$ and over $\mathbb{F}_2$.
(e) $0 \in R[x]$, for any R.

Solution.

(a) $(2, -1, 3, 0, 0, \dots)$. The entries lie in $\mathbb{Q}$, and $N = 2$ is admissible, so it is a polynomial over $\mathbb{Q}$.
(b) $(0, 1, 1, 0, 0, \dots)$, with entries in $\mathbb{F}_2$ and $N = 2$ admissible. It is **not** the zero sequence, since its entry in position 1 is $1 \neq 0$. So $x^2 + x \neq 0$ in $\mathbb{F}_2[x]$, although the rule $c \mapsto cc + c$ is the zero function on $\mathbb{F}_2$, as computed above.
(c) $([4], [3], [0], [0], \dots)$: the constant term comes first. The entries lie in $\mathbb{Z}/6\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2) and $N = 1$ is admissible.
(d) Over $\mathbb{Z}$: $(7, 0, 0, \dots)$. Over $\mathbb{Z}/5\mathbb{Z}$: $([7], [0], [0], \dots)$, and $[7] = [2]$ because $7 - 2 = 5$ is a multiple of 5; so this is the constant $[2]$. Over $\mathbb{F}_2$: $(1, 0, 0, \dots)$, because $7 = 1$ in $\mathbb{F}_2$ ($7 - 1 = 6 = 3 \cdot 2$). The same symbol 7 names three different polynomials, one in each ring, and in each ring $N = 0$ is admissible.
(e) $(0, 0, 0, \dots)$, with every N admissible: the degenerate case.

Now a non-example, by a minimal change. Start from $1 + x + x^2 \in \mathbb{Q}[x]$, the sequence $(1, 1, 1, 0, 0, \dots)$, and change every later 0 to 1. The result $(1, 1, 1, 1, \dots)$, informally "$1 + x + x^2 + \cdots$", is still a function $\mathbb{N} \to \mathbb{Q}$. The one clause that fails is **only finitely many**: for every N, the entry in position $N + 1$ is $1 \neq 0$, so no N is admissible. It is a *formal power series*, met again in the exercises of Section 4.2, but not a polynomial. An expression such as $x^{-1} + 1$ fails for a more basic reason: it would need an entry in position -1, and a polynomial is a function on $\mathbb{N}$.

$\mathbb{R}$ and $\mathbb{C}$ are commutative rings too (for $\mathbb{R}$, *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 5; for $\mathbb{C}$, Chapter 1), so $\mathbb{R}[x]$ and $\mathbb{C}[x]$ are defined, and they are the main examples of the linear-algebra companion. No proof in this chapter needs them; our examples come from $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{F}_p$, the rings this series has built.

Where R matters. Nothing in Definition 4.1.1 mentions inverses, an order, or size. It makes sense word for word over $\mathbb{Z}/6\mathbb{Z}$, where $[2][3] = [0]$ (Number Systems: From \(\nN\) to \(\nR\), Example (Multiplication modulo six and modulo five)), and over the zero ring. The price is that school rules about polynomials cannot be assumed: each one that survives is proved, here or (division with remainder, counting roots) in Chapter 5, and each result says what it needs from R (nothing at all, no zero divisors, a unit leading coefficient, finiteness with $1 \neq 0$, or, for the derivative, the characteristic of a field).

Warning. p_2 **is a coefficient;** $p(2)$ **will be a value.** Section 4.4 writes $p(c)$ for the result of putting $c \in R$ in place of x. For $p = x^2 + 1 \in \mathbb{Z}[x]$, the coefficient p_2 is 1, while the value at 2 will be $2 \cdot 2 + 1 = 5$. Both are integers, so a reader who writes $p(k)$ for "the k-th coefficient" gets $1 = 5$. This book never writes $p(k)$ for a coefficient: the coefficient of x^k is p_k, always with a subscript.

Quick check. Is $6x^2$ equal to the zero polynomial in $(\mathbb{Z}/6\mathbb{Z})[x]$? In $\mathbb{Z}[x]$?

Solution. In $(\mathbb{Z}/6\mathbb{Z})[x]$, yes: $6x^2$ is the monomial $[6]\,x^2$, and $[6] = [0]$, so every entry is $[0]$ and the two sequences agree in every position. In $\mathbb{Z}[x]$, no: the entry in position 2 is $6 \neq 0$, while the zero polynomial has 0 there. Same display, two rings, two answers.

4.1.3 Sums, powers and multiples

The next section defines the product of two polynomials by a formula whose k-th coefficient is a finite sum $\sum_{i=0}^{k} p_i q_{k-i}$ of products in R. Later sections raise elements of R, and polynomials, to powers, and use multiples $k \cdot a$. This subsection collects what we use about all three. Most of it is already proved: finite sums and multiples in a commutative ring are Chapter 2's (Lemma 2.6.1, Lemma 2.5.1), and the recursions follow the patterns that *Sets, Relations, and Cardinality*, Section 2.3 set up for real numbers (Sets, Relations, and Cardinality, Definition 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.2). The patterns are reused; no fact about $\mathbb{R}$ is.

One point deserves care before we start. The sums of polynomials in Section 4.2 must be formed **before** we know that $R[x]$ is a commutative ring, because they are used to prove it. So part (a) below asks for an addition and a left-neutral element 0, and nothing more.

Lemma 4.1.1. Finite Sums, Powers and Multiples

Let R be a commutative ring.

(a) *(Sums.)* Let T be a set with a function $+\colon T \times T \to T$ and an element $0 \in T$ with $0 + u = u$ for every $u \in T$. For a sequence $(u_i)_{i \in \mathbb{N}}$ in T there is exactly one way to define $\sum_{i=0}^{k} u_i \in T$, for $k \in \mathbb{N}$, such that

$$\sum_{i=0}^{0} u_i = u_0, \qquad \sum_{i=0}^{k+1} u_i = \sum_{i=0}^{k} u_i + u_{k+1},$$

starting from the empty sum 0. The sum $\sum_{i=0}^{k} u_i$ depends only on $u_0, \ldots, u_k$; so a finite list $u_0, \ldots, u_k$ has a sum, computed from any extension of the list to a sequence. Likewise, a finite list $s_1, \ldots, s_r$ in R has a **product** $\prod_{j=1}^{r} s_j$, with $\prod_{j=1}^{0} s_j = 1$ and $\prod_{j=1}^{r+1} s_j = (\prod_{j=1}^{r} s_j) s_{r+1}$.

(b) *(Rules for sums in R.)* For $k \in \mathbb{N}$, $c \in R$ and elements $u_i, v_i \in R$:
(Σ1) $\sum_{i=0}^{k}(u_i + v_i) = \sum_{i=0}^{k} u_i + \sum_{i=0}^{k} v_i$;
(Σ2) $c \sum_{i=0}^{k} u_i = \sum_{i=0}^{k} c\,u_i$;
(Σ3) for $j \in \mathbb{N}$: if $u_i = 0$ for every $i \leq k$ with $i \neq j$, then $\sum_{i=0}^{k} u_i = u_j$ when $j \leq k$, and $\sum_{i=0}^{k} u_i = 0$ when $j > k$;

($\Sigma 4$) $-\sum_{i=0}^{k} u_i = \sum_{i=0}^{k}(-u_i)$.

(c) *(Powers.)* For $s \in R$ and $n \in \mathbb{N}$, $s^0 := 1$ and $s^{n+1} := s^n s$ define s^n for every n, and for all $s, t \in R$ and $m, n \in \mathbb{N}$,

$$s^{m+n} = s^m s^n, \qquad (s^m)^n = s^{mn}, \qquad (st)^n = s^n t^n.$$

(d) *(Multiples.)* For all $a, b \in R$ and $m, n \in \mathbb{Z}$,

$$\begin{aligned} (m+n)\cdot a &= m\cdot a + n\cdot a, & m\cdot(a+b) &= m\cdot a + m\cdot b,\\ (m\cdot a)b &= m\cdot(ab), & (m\cdot 1)a &= m\cdot a,\\ (mn)\cdot a &= m\cdot(n\cdot a). \end{aligned}$$

In words: (a) says that a finite list in a set with an addition has a sum, built one term at a time, and that terms beyond the list do not matter; it needs no law of addition beyond $0 + u = u$. (b) says that a finite sum of ring elements can be split into two sums, multiplied through by a constant, collapsed to its one non-zero term, or negated term by term. (c) is the three laws of exponents in a commutative ring. (d) is the arithmetic of the multiples $m \cdot a$ of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Section 2.3 ("Multiples"), extended to $m \in \mathbb{Z}$ in Chapter 2: a dot with an integer on its left is always a multiple, and the product of two ring elements is written by juxtaposition.

Parts (b) and (d) are cited from Chapter 2: ($\Sigma 1$)–($\Sigma 4$) are Lemma 2.6.1 (a), (b), (d), (e) (for ($\Sigma 3$), apply Lemma 2.6.1 (d) to the sequence that agrees with $u_0, \ldots, u_k$ and is 0 beyond k; by the finite-lists clause of part (a) above it has the same sum), and the five rules of part (d) above are Lemma 2.5.1 (c), (d). Parts (a) and (c) are the recursions of *Sets, Relations, and Cardinality*, Section 2.3, read in T and in R; each is built by Sets, Relations, and Cardinality, Theorem 2.3.1, and each of its laws is one short induction. Chapter 1 proves the same three power laws for every commutative ring (Proposition 1.1.3); we only compare with it, and prove (c) again from the template, so that this chapter's main line rests on Chapter 2 and not on Chapter 1.

↻ **Second reading** · *Proofs of (a) and (c)*

Idea. Each statement comes from Sets, Relations, and Cardinality, Theorem 2.3.1, and each law is one induction on one index, following the clauses of the recursion: the base case uses the starting value, and the step peels off the last term or factor. Only the laws of R named at each step are used.

Proof. (a) Apply Sets, Relations, and Cardinality, Theorem 2.3.1 (read on $\mathbb{N} = \omega$ through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) with $X = T$, starting value 0 and step $(j, y) \mapsto y + u_j$, a function $\mathbb{N} \times T \to T$ because $+$ maps $T \times T$ into T. It gives exactly one sequence $(S_j)_{j \in \mathbb{N}}$ in T with $S_0 = 0$ and $S_{j+1} = S_j + u_j$. Set $\sum_{i=0}^{k} u_i := S_{k+1}$. Then $\sum_{i=0}^{0} u_i = 0 + u_0 = u_0$ by the hypothesis on 0, and $\sum_{i=0}^{k+1} u_i = S_{k+1} + u_{k+1} = \sum_{i=0}^{k} u_i + u_{k+1}$. Any assignment obeying the two displayed equations agrees with this one at every k, by Logic and Proof, Axiom 4.2.1 on k.

For the dependence on $u_0, \ldots, u_k$, let (v_i) be a second sequence with $v_i = u_i$ for $i \le k$, and let (S'_j) be its sequence of partial sums. We prove by Logic and Proof, Axiom 4.2.1 on j the statement "if $j \le k+1$, then $S_j = S'_j$". For $j = 0$ both are 0. If $j + 1 \le k + 1$, then $j \le k + 1$

and $j \le k$, so $S_j = S'_j$ by the hypothesis and $u_j = v_j$; hence $S_{j+1} = S_j + u_j = S'_j + v_j = S'_{j+1}$. At $j = k+1$ this gives $\sum_{i=0}^{k} u_i = \sum_{i=0}^{k} v_i$. The argument used only that $+$ is a function on T. The product of a list is Sets, Relations, and Cardinality, Theorem 2.3.1 with $X = R$, starting value 1 and step $(j, y) \mapsto y\, s_{j+1}$ (with $s_j := 1$, say, for $j > r$), the pattern of the product in Sets, Relations, and Cardinality, Definition 2.3.1; its dependence on $s_1, \dots, s_r$ only is the same induction.

(c) The powers are Sets, Relations, and Cardinality, Theorem 2.3.1 with $X = R$, starting value 1 and step $(n, y) \mapsto ys$, the pattern of Sets, Relations, and Cardinality, Definition 2.3.2. For the first law fix m and induct on n (Logic and Proof, Axiom 4.2.1). For $n = 0$: $s^{m+0} = s^m = s^m \cdot 1 = s^m s^0$, by (F7). If $s^{m+n} = s^m s^n$, then

$$s^{m+(n+1)} = s^{(m+n)+1} = s^{m+n} s = (s^m s^n) s = s^m (s^n s) = s^m s^{n+1},$$

using $m+(n+1) = (m+n)+1$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 1.5.3 (c)), the recursion, the hypothesis and (F5). For the second law fix m: $(s^m)^0 = 1 = s^0 = s^{m \cdot 0}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 1.5.1 (b)), and if $(s^m)^n = s^{mn}$, then $(s^m)^{n+1} = (s^m)^n s^m = s^{mn} s^m = s^{mn+m} = s^{m(n+1)}$, by the first law and $m(n+1) = mn + m$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 1.5.3 (d), (e)). For the third: $(st)^0 = 1 = 1 \cdot 1 = s^0 t^0$, by (F7), and if $(st)^n = s^n t^n$, then $(st)^{n+1} = (st)^n (st) = (s^n t^n)(st) = (s^n s)(t^n t) = s^{n+1} t^{n+1}$, regrouping by (F5) and (F6). This proves (a) and (c).

■

We will use (a) twice over: for sums of ring elements, as in the product formula of Section 4.2, and for sums in $R[x]$ of finitely many monomials, which Section 4.2 forms with its coefficientwise addition before any ring law of $R[x]$ is known. In both cases $0 + u = u$ holds, in R by (F1) and (F3), and in $R[x]$ position by position.

4.1.4 Exercises

4.1.4.1 A. Check your understanding

Exercise. A1

(a) Write the coefficient sequences of $x^3 - 2x \in \mathbb{Z}[x]$ and of $[2]x^2 + [4]x \in (\mathbb{Z}/4\mathbb{Z})[x]$. Is the second one a monomial?

(b) Is "$1 + x + x^2 + \cdots$", the sequence $(1, 1, 1, \dots)$ of rationals, a polynomial over $\mathbb{Q}$? Name the clause of Definition 4.1.1 that decides it.

(c) True or false: two polynomials p, q over $\mathbb{F}_2$ whose rules $c \mapsto \sum_{k=0}^{N} p_k c^k$ and $c \mapsto \sum_{k=0}^{N} q_k c^k$, for an N admissible for both, agree at 0 and at 1 are equal. Justify your answer.

(d) Which N are admissible for $3x^2 - x + 2 \in \mathbb{Q}[x]$?

Solution.

(a) $x^3 - 2x$ is $(0, -2, 0, 1, 0, 0, \dots)$: the constant term is 0, the coefficient of x is -2, and that of x^3 is 1. The second is $([0], [4], [2], [0], \dots)$, and $[4] = [0]$ in $\mathbb{Z}/4\mathbb{Z}$, since $4 - 0 = 4$. So it is $([0], [0], [2], [0], \dots)$, the monomial $[2]x^2$.

(b) No. The clause **only finitely many** fails: for every $N \in \mathbb{N}$ the entry in position $N+1$ is $1 \neq 0$, so no N is admissible.

(c) False. The polynomials $x^2 + x$ and 0 over $\mathbb{F}_2$ give the rules $c \mapsto cc + c$ and $c \mapsto 0$, which agree at 0 and at 1 (the computation at the start of the section). But $x^2 + x = (0, 1, 1, 0, \dots)$ differs from 0 in position 1, so the polynomials are not equal.

(d) Every $N \geq 2$. The coefficient of x^2 is $3 \neq 0$, so $N = 0$ and $N = 1$ fail (position $2 > N$ holds a non-zero entry); and every $N \geq 2$ works, since all positions $k \geq 3$ hold 0.

4.1.4.2 B. Practice

Exercise. B1: Polynomials of bounded length as tuples

Let $N \in \mathbb{N}$ and $P_N \coloneqq \{p \in R[x] : p_k = 0 \text{ for every } k > N\}$. Prove that

$$\Theta \colon P_N \to R^{N+1}, \qquad p \mapsto (p_0, p_1, \dots, p_N),$$

is a bijection (Sets, Relations, and Cardinality, Definition 1.4.5), where R^{N+1} is the set of $(N+1)$-tuples of elements of R, indexed here from 0 (Sets, Relations, and Cardinality, Definition 1.3.2; for $N = 0$, where the book has no 1-tuples, we read R^1 as R, with (a_0) standing for a_0, and Θ as $p \mapsto p_0$). Hence list the elements of P_2 for $R = \mathbb{F}_2$.

Solution. Injective. Let $p, q \in P_N$ with $\Theta(p) = \Theta(q)$. Then $p_k = q_k$ for $k \leq N$, and $p_k = 0 = q_k$ for $k > N$ by the definition of P_N. So $p_k = q_k$ for every k, and $p = q$ by Sets, Relations, and Cardinality, Proposition 1.4.1.

Surjective. Let $(a_0, \dots, a_N) \in R^{N+1}$. Define $p \colon \mathbb{N} \to R$ by $p_k \coloneqq a_k$ for $k \leq N$ and $p_k \coloneqq 0$ for $k > N$: extend by zeros. Then N is admissible for p, so $p \in R[x]$ and $p \in P_N$, and $\Theta(p) = (a_0, \dots, a_N)$.

So Θ is a bijection; its inverse is "extend by zeros". For $R = \mathbb{F}_2$ and $N = 2$, each a_i is 0 or 1, and the eight triples (a_0, a_1, a_2) give the eight polynomials

$$0, \quad 1, \quad x, \quad x+1, \quad x^2, \quad x^2+1, \quad x^2+x, \quad x^2+x+1.$$

Section 4.4 returns to this list and asks which functions $\mathbb{F}_2 \to \mathbb{F}_2$ they define.

Exercise. B2: Determine which

Each formula below defines a sequence $\mathbb{N} \to \mathbb{Z}/4\mathbb{Z}$. Determine which of them are polynomials over $\mathbb{Z}/4\mathbb{Z}$. Justify your answer, and for each polynomial give the least admissible N and the polynomial in the notation of the display.

(a) $p_k \coloneqq [2^k]$.

(b) $p_k \coloneqq [k^2]$.

(c) $p_k \coloneqq [k(k-1)(k-2)(k-3)]$.

(d) $p_k \coloneqq [2k]$.

Solution. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b), $[0], [1], [2], [3]$ are four different classes; in particular $[1] \neq [0]$ and $[2] \neq [0]$.

(a) A polynomial. The first entries are $[1], [2], [4], [8], \ldots$, and for $k \geq 2$, $2^k = 4 \cdot 2^{k-2}$ (Lemma 4.1.1 (c)), so $[2^k] = [0]$. The least admissible N is 1: $N = 1$ works, and $N = 0$ does not, since $p_1 = [2] \neq [0]$. The polynomial is $1 + [2]x$.

(b) Not a polynomial. For odd $k = 2j + 1$, $k^2 = 4(j^2 + j) + 1$, so $p_k = [1] \neq [0]$. Given any N, the odd number $k = 2N + 1 > N$ has $p_k \neq [0]$, so no N is admissible.

(c) A polynomial: the zero polynomial. Let $k \in \mathbb{N}$. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2 (a), $k = 4q + r$ with $0 \leq r \leq 3$, so $k - r = 4q$ is one of the four factors $k, k-1, k-2, k-3$. Hence the product is a multiple of 4, and $p_k = [0]$ for every k (for $k \leq 3$ the multiple is 0, since then $q = 0$). Every N is admissible; the least is 0, and the display is 0.

(d) Not a polynomial. For odd $k = 2j + 1$, $2k = 4j + 2$, so $p_k = [2] \neq [0]$, and as in (b) no N is admissible.

The sequences in (b) and (d) have infinitely many non-zero entries even though their values repeat; (c) shows that a formula in k can describe the zero polynomial.

4.1.4.3 C. Going deeper

Exercise. C1: Finitely many, in the sense of finite sets

For a sequence $p\colon \mathbb{N} \to R$, let $S \coloneqq \{k \in \mathbb{N} : p_k \neq 0\}$, the set of positions that hold a non-zero entry. Prove that some $N \in \mathbb{N}$ is admissible for p if and only if S is finite (Sets, Relations, and Cardinality, Definition 3.1.2). So "only finitely many p_k are non-zero" in Definition 4.1.1 means exactly what it says.

Solution. ($\Rightarrow$) Let N be admissible. If $k \in S$, then $p_k \neq 0$, so $k \leq N$; hence $S \subseteq \{0, \ldots, N\}$. The set $\{0, \ldots, N\}$ has $N + 1$ elements (the third example after Sets, Relations, and Cardinality, Definition 3.1.2), so its subset S is finite by Sets, Relations, and Cardinality, Proposition 3.1.6.

($\Leftarrow$) We prove by Logic and Proof, Axiom 4.2.1 on $n \in \mathbb{N}$: *every subset $A \subseteq \mathbb{N}$ with n elements has an upper bound $b \in \mathbb{N}$*, that is, $a \leq b$ for every $a \in A$. For $n = 0$, $A = \emptyset$ (the first example after Sets, Relations, and Cardinality, Definition 3.1.2), and $b = 0$ works vacuously. Suppose the statement holds for n, and let $\varphi\colon \{1, \ldots, n+1\} \to A$ be a bijection. Put $z \coloneqq \varphi(n+1)$ and $A' \coloneqq A \setminus \{z\}$. The restriction of φ to $\{1, \ldots, n\}$ maps into A' (if $\varphi(j) = z$ then $j = n+1$, by injectivity), is injective, and is onto A' (an element of A' is $\varphi(j)$ with $j \neq n+1$, so $j \leq n$). So A' has n elements and an upper bound b'. By trichotomy (Number Systems: From \(\nN\) to \(\nR\), Theorem 1.6.1 (a)), the larger b of b' and z is defined, and it bounds every element of $A = A' \cup \{z\}$.

Now let S be finite, with an upper bound N. If $k > N$, then $k \notin S$, that is, $p_k = 0$. So N is admissible.

The proof of ($\Leftarrow$) never needed a greatest element of S, only an upper bound. The greatest element exists when S is non-empty and finite (an upper bound in $\mathbb{N} \subseteq \mathbb{Z}$ gives one by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6), and Section 4.3 calls it the degree.

Marking scheme. (10 points) - 3: ($\Rightarrow$) shows $S \subseteq \{0, \dots, N\}$ and concludes that S is finite, citing that $\{0, \dots, N\}$ is finite and that a subset of a finite set is finite (Sets, Relations, and Cardinality, Proposition 3.1.6). - 2: ($\Leftarrow$) sets up an induction on the number of elements of a finite $A \subseteq \mathbb{N}$, with the claim that A has an upper bound, and handles $A = \emptyset$. - 2: in the step, removes one element z and shows that the rest A' has n elements (by restricting the bijection, or by Sets, Relations, and Cardinality, Corollary 3.1.7). - 1: takes the larger of b' and z, by trichotomy, as a bound for $A = A' \cup \{z\}$. - 2: concludes that an upper bound N of S is admissible: $k > N$ implies $k \notin S$, so $p_k = 0$.

Fatal errors (0 for the step): using a greatest element of S without justification; overlooking $S = \emptyset$ in ($\Leftarrow$).

4.2 The Polynomial Ring

Section 4.1 made a polynomial a coefficient sequence, and the display $\sum_k p_k x^k$ only a way of writing it down. This section gives the sequences their sum and product, read off from what school algebra does with expressions, and proves that the result obeys every law of a commutative ring (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1). The obvious proof of associativity needs a theorem about reordering double sums that we have not proved. We avoid it with one device, **check on monomials, extend by additivity**, which returns in Sections 4.4 and 4.5.

Throughout, R is a commutative ring and $R[x]$ is the set of polynomials over R (Definition 4.1.1).

4.2.1 Adding and multiplying coefficient sequences

At school, $(3x^2 - x + 2)(x + 1)$ is computed by multiplying every term of the first factor by every term of the second, using $a_i x^i \cdot b_j x^j = a_i b_j x^{i+j}$, and then collecting the terms with the same power. The coefficient of x^k in the result collects the products $a_i b_j$ over all pairs with $i + j = k$, that is, over $i = 0, \dots, k$ with $j = k - i$. Addition collects like powers too, so it adds coefficients position by position. We turn these two recipes into definitions.

Add position by position; multiply by collecting, in position k, every product of a coefficient from position i with one from position $k - i$.

Definition 4.2.1. The Polynomial Ring

Let R be a commutative ring. For $p, q \in R[x]$ and $k \in \mathbb{N}$ define

$$(p + q)_k := p_k + q_k, \qquad (-p)_k := -p_k, \qquad (pq)_k := \sum_{i=0}^{k} p_i \, q_{k-i}.$$

The set $R[x]$ with this addition and this multiplication is the **polynomial ring** over R.

In words: the sum and the negative act on each position separately. The product is the **convolution** of the two sequences: its entry in position k is a sum of $k + 1$ products in R, and the two positions in each product add up to k. For $i \leq k$, the index $k - i$ lies in $\mathbb{N}$, computed in $\mathbb{Z} \supseteq \mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3); the sum is a finite sum in R

(Lemma 4.1.1 (a)). The name "ring" is a promise: the theorem at the end of this section keeps it.

The operations stay inside $R[x]$. There is something to check: the three formulas produce sequences $\mathbb{N} \to R$, and we must see that only finitely many of their entries are non-zero. Let m be admissible for p and n admissible for q.

- For $k > \max(m, n)$, $(p+q)_k = 0 + 0 = 0$ by (F3). So $\max(m, n)$ is admissible for $p + q$.
- For $k > m$, $(-p)_k = -0 = 0$, since $0 + 0 = 0$ and negatives are unique (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)). So m is admissible for $-p$.
- Let $k > m + n$ and $0 \leq i \leq k$. If $i > m$, then $p_i = 0$. If $i \leq m$, then $k - i \geq k - m > n$, so $q_{k-i} = 0$. Either way the term $p_i q_{k-i}$ is 0, by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) with (F6). A sum whose terms are all 0 is 0 (Lemma 4.1.1 (b), (Σ3) with $j = k + 1$), so $(pq)_k = 0$, and $m + n$ is admissible for pq.

So $+$ and $\cdot$ are functions $R[x] \times R[x] \to R[x]$, and $p \mapsto -p$ is a function $R[x] \to R[x]$. The bound $m + n$ is the first hint of the degree of a product, the subject of Section 4.3.

Example. A product, coefficient by coefficient

Compute $(3x^2 - x + 2)(x + 1)$ from Definition 4.2.1 in $\mathbb{Q}[x]$, in $\mathbb{F}_3[x]$ and in $(\mathbb{Z}/6\mathbb{Z})[x]$.

Solution. In $\mathbb{Q}[x]$, let $p = 3x^2 - x + 2$ and $q = x + 1$, so $(p_0, p_1, p_2) = (2, -1, 3)$ and $(q_0, q_1) = (1, 1)$, all other coefficients 0. Then 2 is admissible for p and 1 for q, so $(pq)_k = 0$ for $k \geq 4$ by the closure argument, and

$$\begin{aligned}(pq)_0 &= p_0 q_0 = 2,\\ (pq)_1 &= p_0 q_1 + p_1 q_0 = 2 - 1 = 1,\\ (pq)_2 &= p_0 q_2 + p_1 q_1 + p_2 q_0 = 0 - 1 + 3 = 2,\\ (pq)_3 &= p_0 q_3 + p_1 q_2 + p_2 q_1 + p_3 q_0 = 0 + 0 + 3 + 0 = 3.\end{aligned}$$

Hence $pq = 3x^3 + 2x^2 + x + 2$, as expanding by hand gives.

In $\mathbb{F}_3[x]$ the same display names other coefficients: $3 = 0$ and $-1 = 2$ in $\mathbb{F}_3$, so $(p_0, p_1, p_2) = (2, 2, 0)$, and $p = 2x + 2$. The formula gives $(pq)_0 = 2$, $(pq)_1 = 2 + 2 = 4 = 1$, $(pq)_2 = 0 + 2 + 0 = 2$, and $(pq)_3 = 0$. So $pq = 2x^2 + x + 2$ in $\mathbb{F}_3[x]$.

In $(\mathbb{Z}/6\mathbb{Z})[x]$, $(p_0, p_1, p_2) = ([2], [5], [3])$, since $[-1] = [5]$. The formula gives $[2]$, $[2] + [5] = [7] = [1]$, $[5] + [3] = [8] = [2]$ and $[3]$. So $pq = [3]x^3 + [2]x^2 + x + [2]$.

Each answer over $\mathbb{F}_3$ and $\mathbb{Z}/6\mathbb{Z}$ is the answer over $\mathbb{Q}$ with every integer coefficient replaced by its class. Section 4.4 explains why this always happens.

Warning. **The product is not taken position by position.** The rule $(pq)_k = p_k q_k$ looks like the natural partner of the sum, but it is not the product of school algebra. For $p = q = x = (0, 1, 0, \dots)$ it would give $(0, 1, 0, \dots)$, that is, $x \cdot x = x$. The convolution gives $(x \cdot x)_2 = x_0 x_2 + x_1 x_1 + x_2 x_0 = 0 + 1 + 0 = 1$ and $(x \cdot x)_k = 0$ for $k \neq 2$, so $x \cdot x = x^2$, as it should be. Only the sum is coefficientwise.

4.2.2 Monomials do the work

The display $\sum_k p_k x^k$ of Section 4.1 can now be read as a genuine sum in $R[x]$. The sum is formed with the addition just defined, by Lemma 4.1.1 (a) with $T = R[x]$. That part of the lemma asks only for a function $+\colon T \times T \to T$ and an element 0 with $0 + u = u$; in $R[x]$ the zero polynomial is such an element, since $(0+u)_k = 0 + u_k = u_k$ by (F1) and (F3). We do not yet know any other law of $R[x]$, and the next proposition needs none.

Proposition 4.2.1. A Polynomial Is the Sum of Its Monomials

Let $p \in R[x]$ and $N \in \mathbb{N}$. The sum $\sum_{k=0}^{N} p_k x^k$ of the monomials $p_k x^k$, formed in $(R[x], +)$, has coefficient p_j in position j for every $j \le N$, and 0 in every position $j > N$. In particular, if N is admissible for p, then

$$p = \sum_{k=0}^{N} p_k x^k.$$

Proof. Write $s_N := \sum_{k=0}^{N} p_k x^k$. We use Logic and Proof, Axiom 4.2.1 on N. For $N = 0$, $s_0 = p_0 x^0$, which has p_0 in position 0 and 0 elsewhere (Definition 4.1.1). Suppose s_N has the stated coefficients. By the recursion of Lemma 4.1.1 (a), $s_{N+1} = s_N + p_{N+1} x^{N+1}$, so by Definition 4.2.1 its j-th coefficient is $(s_N)_j + (p_{N+1}x^{N+1})_j$. This is $p_j + 0 = p_j$ for $j \le N$; it is $0 + p_{N+1} = p_{N+1}$ for $j = N+1$; and it is $0 + 0 = 0$ for $j > N+1$, by (F1) and (F3). These are the stated coefficients for $N+1$.

If N is admissible for p, then $p_j = 0$ for $j > N$, so p and s_N agree in every position, and $p = s_N$ by Sets, Relations, and Cardinality, Proposition 1.4.1. This proves the proposition. ∎

So the display of Definition 4.1.1 is now an honest sum: $3x^2 - x + 2$ is the sum, in $(R[x], +)$, of the monomials $2x^0$, $(-1)x^1$ and $3x^2$. Every polynomial is a finite sum of monomials.

Next we multiply by a monomial. Multiplying by ax^m should move every coefficient m places up and multiply it by a.

Lemma 4.2.2. Multiplying by a Monomial

Let $a, b \in R$, $m, n \in \mathbb{N}$ and $q \in R[x]$.

(a) $\big((ax^m)q\big)_k = a\, q_{k-m}$ for $k \ge m$, and $\big((ax^m)q\big)_k = 0$ for $k < m$.
(b) $(ax^m)(bx^n) = (ab)\, x^{m+n}$.

Proof.

(a) By Definition 4.2.1, $\big((ax^m)q\big)_k = \sum_{i=0}^{k} (ax^m)_i\, q_{k-i}$. For $i \ne m$, $(ax^m)_i = 0$, so the i-th term is $0 \cdot q_{k-i} = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) with (F6)). By (Σ3) of Lemma 4.1.1 (b) with $j = m$, the sum is the term with $i = m$, namely $a\, q_{k-m}$, when $m \le k$, and 0 when $m > k$.

(b) Apply (a) with $q = bx^n$. For $k < m$ the coefficient is 0. For $k \ge m$ it is $a\,(bx^n)_{k-m}$, which is ab when $k - m = n$, that is, when $k = m + n$, and $a \cdot 0 = 0$ otherwise

(Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)). Since $k < m$ implies $k \neq m+n$, the product has ab in position $m+n$ and 0 elsewhere: it is the monomial $(ab)x^{m+n}$.

■

Part (b) is the school rule $ax^m \cdot bx^n = ab\,x^{m+n}$, now a theorem about sequences. It contains everything multiplication does: the next lemma shows that a law which holds on monomials, and which survives sums in each argument, holds everywhere.

Additivity in each argument. For all $p, p', q, q' \in R[x]$,

$$(p+p')q = pq + p'q \tag{$*$}$$

$$p(q+q') = pq + pq'. \tag{$**$}$$

For $(*)$, the k-th coefficient of the left side is

$$\sum_{i=0}^{k} (p_i + p'_i)\, q_{k-i} = \sum_{i=0}^{k} (p_i q_{k-i} + p'_i q_{k-i}) = \sum_{i=0}^{k} p_i q_{k-i} + \sum_{i=0}^{k} p'_i q_{k-i},$$

where the first equality applies (F6), (F9) and (F6) again inside each term, and the second is (Σ1). The right side is the k-th coefficient of $pq + p'q$. For $(**)$ the same computation runs with $p_i(q_{k-i} + q'_{k-i}) = p_i q_{k-i} + p_i q'_{k-i}$, which is (F9) itself. Each sum has a single index i, and no term is moved past another. So each distributive law is one line of algebra in R, with compare coefficients doing the rest.

A map of several polynomial arguments is **additive in each argument** if, whenever one argument is replaced by a sum $u + u'$ and the others are held fixed, the value is the sum of the two values. By $(*)$ and $(**)$, the product $(p, q) \mapsto pq$ is additive in each argument. Here is what that buys.

Lemma 4.2.3. Check on Monomials

Let R be a commutative ring, and let T be a set with a function $+\colon T \times T \to T$. Let Φ, Ψ be maps of one, two or three polynomial arguments to T, that is, both maps $R[x] \to T$, both $R[x]^2 \to T$ or both $R[x]^3 \to T$, that are **additive in each argument**: for each argument position and **all** fixed values of the other arguments,

$$\Phi(\dots, u+u', \dots) = \Phi(\dots, u, \dots) + \Phi(\dots, u', \dots)$$

with u, u' in that position, and the same for Ψ. If Φ and Ψ take the same value whenever **every** argument is a monomial, then $\Phi = \Psi$.

Here $R[x]^2$ and $R[x]^3$ are the sets of pairs and triples. The proof uses no law of T at all, not even associativity of its addition, and no product on T. That is why it may be applied with $T = R[x]$ inside the proof that $R[x]$ is a ring.

Idea. Every polynomial is a finite sum of monomials (Proposition 4.2.1), so a map that is additive is fixed by what it does to monomials: peel off the top monomial and induct. With several arguments, unlock them one at a time: first let the last argument be arbitrary while the others stay monomials, then the one before, and so on.

Before reading on: why is additivity in ***each*** *argument separately enough, and where would*

"additive in the pair", $\Phi(p+p', q+q') = \Phi(p,q) + \Phi(p',q')$, *fail?*

Proof. One argument. We prove by Logic and Proof, Axiom 4.2.1 on N: *for every* $p \in R[x]$ *for which* N *is admissible,* $\Phi(p) = \Psi(p)$. Every polynomial has an admissible N (Definition 4.1.1), so this gives $\Phi = \Psi$ (Sets, Relations, and Cardinality, Proposition 1.4.1). For $N = 0$, p agrees in every position with the monomial p_0x^0, so $p = p_0x^0$ and $\Phi(p) = \Psi(p)$ by hypothesis. Suppose the statement holds for N, and let $N+1$ be admissible for p. Put $p' := \sum_{k=0}^{N} p_k x^k$. By Proposition 4.2.1, N is admissible for p', and by the recursion of Lemma 4.1.1 (a) and the same proposition,

$$p = \sum_{k=0}^{N+1} p_k x^k = p' + p_{N+1}x^{N+1}.$$

Hence

$$\Phi(p) = \Phi(p') + \Phi(p_{N+1}x^{N+1}) = \Psi(p') + \Psi(p_{N+1}x^{N+1}) = \Psi(p),$$

by additivity of Φ, the induction hypothesis for p' together with the hypothesis on monomials, and additivity of Ψ.

Two arguments. Fix a monomial u. The maps $v \mapsto \Phi(u,v)$ and $v \mapsto \Psi(u,v)$ are additive and agree on monomials, so by the case of one argument they agree everywhere: $\Phi(u,q) = \Psi(u,q)$ for every monomial u and **every** $q \in R[x]$. Now fix any q. The maps $u \mapsto \Phi(u,q)$ and $u \mapsto \Psi(u,q)$ are additive and, by what was just shown, agree on monomials; so they agree everywhere.

Three arguments. The same, one argument at a time. For monomials u_1, u_2, the case of one argument, applied to the third argument, gives $\Phi(u_1,u_2,r) = \Psi(u_1,u_2,r)$ for every r. For a monomial u_1 and any r, the same case, applied to the second argument, then gives agreement for every q in the middle. Finally, for any q, r, the same case, applied to the first argument, gives $\Phi(p,q,r) = \Psi(p,q,r)$ for every p. This proves the lemma.

■

The answer to the prompt. Each step of the proof changes **one** argument from "a monomial" to "arbitrary" while the other arguments are held fixed, and it only ever splits that one argument into a sum. Additivity in each argument separately is exactly that. "Additive in the pair" is a different condition, and the product does not satisfy it: with $p = q' = 1$ and $p' = q = 0$, $(p+p')(q+q') = 1 \cdot 1 = 1$, while $pq + p'q' = 0 + 0 = 0$ whenever $1 \neq 0$ in R. A proof that split both arguments at once would lose the cross terms pq' and $p'q$.

We call this move **check on monomials, extend by additivity**. To prove that two expressions in polynomials agree, check that both are additive in each argument, and check the identity when every argument is a monomial. The second check is a computation with a single coefficient in each argument.

4.2.3 The ring laws

Now the payoff: every law of a commutative ring holds in $R[x]$. The theorem also records how R sits inside $R[x]$ and why the school notation ax^n means what it seems to mean.

Theorem 4.2.4. The Polynomial Ring Is a Commutative Ring

Let R be a commutative ring.

(a) $R[x]$, with the operations of Definition 4.2.1, is a commutative ring (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1), with zero the zero polynomial, negative $-p$ as defined there, and one $1 := 1\,x^0$. Spelled out, for all $p, q, r \in R[x]$: (1) $p+q = q+p$ and $(p+q)+r = p+(q+r)$; (2) $p+0 = p$ and $p+(-p) = 0$; (3) $pq = qp$ and $(pq)r = p(qr)$; (4) $1 \cdot p = p$; (5) $p(q+r) = pq+pr$.

(b) The map $R \to R[x]$, $a \mapsto a\,x^0$, is injective and satisfies $(a+b)x^0 = ax^0 + bx^0$, $(ab)x^0 = (ax^0)(bx^0)$ and $1x^0 = 1$. If $1 \neq 0$ in R, then $1 \neq 0$ in $R[x]$.

(c) For $n \in \mathbb{N}$, the n-th power of x in the ring $R[x]$ (Lemma 4.1.1 (c)) is the monomial $1\,x^n$, and the product of the constant a with it is the monomial $a\,x^n$. Hence $p = \sum_{k=0}^{N} p_k x^k$, for admissible N, is a sum of products of constants and powers of x.

(d) For a constant a and $p \in R[x]$, $(ap)_k = a\,p_k$ for every k.

In words: (a) says we may compute in $R[x]$ by every rule of a commutative ring; (b) says that computing with constant polynomials is computing in R, which justifies calling $a\,x^0$ "the constant a"; (c) says that the monomial ax^n of Section 4.1, a sequence, is the product $a \cdot x \cdot x \cdots x$ of school algebra; and (d) says that multiplying by a constant multiplies every coefficient.

Try it first (ten minutes): for $p = a_0 + a_1 x$, $q = b_0 + b_1 x$ and $r = c_0 + c_1 x$, write the coefficient of x^2 in $(pq)r$ and in $p(qr)$ from Definition 4.2.1. Which laws of R did you need to see that they are equal, and how would your argument scale to polynomials of degree 10?

Idea. The attempt gives $pq = a_0b_0 + (a_0b_1 + a_1b_0)x + a_1b_1x^2$, and the coefficient of x^2 in $(pq)r$ is $(a_0b_1 + a_1b_0)c_1 + (a_1b_1)c_0$, while in $p(qr)$ it is $a_0(b_1c_1) + a_1(b_0c_1 + b_1c_0)$. Both expand, by (F9), to the three products $a_0b_1c_1$, $a_1b_0c_1$, $a_1b_1c_0$, grouped and ordered differently, so (F1), (F2), (F5), (F6) and (F9) all enter. In degree 10 the two coefficients of x^k are double sums, $\sum_s (\sum_i a_i b_{s-i}) c_{k-s}$ and $\sum_i a_i (\sum_j b_j c_{k-i-j})$, and the plan "both are the sum of all $a_i b_j c_l$ with $i+j+l = k$" needs a theorem on reordering finite double sums, which we have not proved.

Monomials avoid that theorem. When each of p, q, r has a single non-zero coefficient, every double sum collapses to one product, and the law becomes a law of R together with a law of $\mathbb{N}$ for the exponents. Both sides are additive in each argument, by $(*)$ and $(**)$, so Lemma 4.2.3 carries the monomial case to all polynomials. The additive laws need nothing new: they are the laws of R, position by position.

Before reading on: self-explain the monomial line for (F5) in the proof below. Which law of R does it use, and which law of $\mathbb{N}$?

Proof. (a) By Definition 4.2.1 and the closure paragraph after it, $+$ and $\cdot$ are functions $R[x] \times R[x] \to R[x]$. We check the clauses of Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1.

(F1)–(F4), position by position. For every k, $(p+q)_k = p_k + q_k = q_k + p_k = (q+p)_k$ by (F1) in R; $((p+q)+r)_k = (p_k+q_k)+r_k = p_k+(q_k+r_k) = (p+(q+r))_k$ by (F2); $(p+0)_k = p_k+0 = p_k$ by (F3); and $(p+(-p))_k = p_k + (-p_k) = 0$ by (F4). So (F1)–(F4) hold in $R[x]$, by **compare coefficients** (Sets, Relations, and Cardinality, Proposition 1.4.1), with the zero polynomial as 0 and $-p$ as the negative of p.

(F9). This is $(**)$.

(F6). Let $\Phi(p,q) \coloneqq pq$ and $\Psi(p,q) \coloneqq qp$. Both are additive in each argument: for Φ this is $(*)$ and $(**)$, and for Ψ it is the same two laws with the roles of the factors exchanged, $q(p+p') = qp + qp'$ and $(q+q')p = qp + q'p$. On monomials,

$$(ax^m)(bx^n) = (ab)\,x^{m+n} = (ba)\,x^{n+m} = (bx^n)(ax^m),$$

by Lemma 4.2.2 (b), (F6) in R with $m+n = n+m$ in $\mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 1.5.3 (b)), and Lemma 4.2.2 (b) again. By Lemma 4.2.3 with two arguments and $T = R[x]$, whose addition is a function by the closure paragraph, $pq = qp$ for all p, q.

(F7). By Lemma 4.2.2 (a) with $a = 1$ and $m = 0$, $(1 \cdot p)_k = 1\,p_k = p_k$ for every k, by (F7) and (F6) in R. So $1 \cdot p = p$, and $p \cdot 1 = 1 \cdot p = p$ by (F6) in $R[x]$.

(F5). Let $\Phi(p,q,r) \coloneqq (pq)r$ and $\Psi(p,q,r) \coloneqq p(qr)$. Each is additive in each argument, by two applications of $(*)$ and $(**)$; for instance, in the middle argument,

$$(p(q+q'))r = (pq + pq')r = (pq)r + (pq')r, \qquad p((q+q')r) = p(qr + q'r) = p(qr) + p(q'r),$$

and in the first and third arguments in the same way. On monomials ax^m, bx^n, cx^l, two applications of Lemma 4.2.2 (b) on each side give

$$\big((ax^m)(bx^n)\big)(cx^l) = \big((ab)c\big)x^{(m+n)+l} = \big(a(bc)\big)x^{m+(n+l)} = (ax^m)\big((bx^n)(cx^l)\big),$$

where the middle equality is (F5) in R and $(m+n)+l = m+(n+l)$ in $\mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 1.5.3 (c)). By Lemma 4.2.3 with three arguments and $T = R[x]$, $(pq)r = p(qr)$ for all p, q, r. This proves (a); the rules (1)–(5) are (F1) with (F2), (F3) with (F4), (F6) with (F5), (F7) in the form $1 \cdot p = p$, and (F9).

(b) If $ax^0 = bx^0$, the entries in position 0 give $a = b$. The sum $ax^0 + bx^0$ has $a + b$ in position 0 and $0 + 0 = 0$ elsewhere, so it is $(a+b)x^0$. The product is $(ab)x^{0+0} = (ab)x^0$ by Lemma 4.2.2 (b), and $1x^0 = 1$ by the definition of 1 in (a). If $1 \neq 0$ in R, then by injectivity $1x^0 \neq 0x^0$, and $0x^0$ is the zero polynomial.

(c) By Lemma 4.1.1 (c) in the commutative ring $R[x]$, $x^0 = 1 = 1x^0$ and $x^{n+1} = x^n x$. By Logic and Proof, Axiom 4.2.1 on n: if $x^n = 1x^n$, then $x^{n+1} = (1x^n)(1x^1) = (1 \cdot 1)x^{n+1} = 1x^{n+1}$, by Lemma 4.2.2 (b) and (F7) in R. For a constant a, $(ax^0)(1x^n) = (a \cdot 1)x^{0+n} = ax^n$, by the same lemma. With Proposition 4.2.1, $p = \sum_{k=0}^{N} p_k x^k$ is the sum of the products of the constants p_k with the powers x^k.

(d) Lemma 4.2.2 (a) with $m = 0$: $(ax^0\,p)_k = a\,p_{k-0} = a\,p_k$. This proves the theorem.

■

The answer to the prompt. The monomial line for (F5) uses associativity of multiplication in R, $(ab)c = a(bc)$, for the coefficient, and associativity of addition in $\mathbb{N}$, $(m+n)+l = m+(n+l)$, for the exponent. Apart from Lemma 4.2.2, which it cites, nothing else: the regrouping that the direct route needed has been absorbed into Lemma 4.2.3, whose proof only peels off one monomial at a time.

The proof never reordered a double sum. Each of its sums has a single index: a coefficient sum of Definition 4.2.1 (in the closure paragraph, $(*)$, $(**)$ and Lemma 4.2.2), or a sum of monomials of Proposition 4.2.1 (inside Lemma 4.2.3 and in part (c)).

Remark. Part (a) makes the name "polynomial ring" honest, and everything proved for commutative rings now applies to $R[x]$. In particular, ideals and quotient rings (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1) are available in $R[x]$; Chapter 5 builds quotients of $F[x]$ for a field F this way. Also, $(R[x], +)$ is an abelian group in the sense of Chapter 3, by (F1)–(F4).

From now on we compute in $R[x]$ as at school: expand brackets, collect terms, and move terms across equations, citing (a) and (c). The two things school algebra does **not** give us are any rule that needs division, and any rule about the degree of a product; the second depends on R, and Section 4.3 finds out how.

Quick check. In $\mathbb{Q}[x]$ and in $\mathbb{F}_2[x]$: is $(x+1)^2$ equal to x^2+2x+1? Is it equal to x^2+1?

Solution. By Lemma 4.1.1 (c) and Theorem 4.2.4 (a), rule (4), $(x+1)^2 = (1\cdot(x+1))(x+1) = (x+1)(x+1)$, and by Definition 4.2.1 this product has coefficients $1\cdot 1 = 1$, $1\cdot 1+1\cdot 1 = 2$ and $1\cdot 1 = 1$ in positions $0, 1, 2$, and 0 beyond, where $2 = 1+1$. Over $\mathbb{Q}$, $(x+1)^2 = x^2+2x+1$, and it is **not** x^2+1, since $2 \neq 0$ in position 1. Over $\mathbb{F}_2$, $2 = 1+1 = 0$, so the sequence is $(1, 0, 1, 0, \dots)$: $(x+1)^2 = x^2+1$, and also $(x+1)^2 = x^2+2x+1$, because over $\mathbb{F}_2$ the display x^2+2x+1 names the same sequence. The same three-term display means different things over different rings.

4.2.4 Exercises

4.2.4.1 A. Check your understanding

Exercise. A1

These questions are about the proof of Theorem 4.2.4.

(a) Where is the commutativity of R, $ab = ba$, used?

(b) Run the monomial check of (F5) on $(2x)(3x^2)(x)$ in $\mathbb{Z}[x]$: compute both groupings.

(c) In the proof of (F5), which additivity does Lemma 4.2.3 need for the third argument? Write out both identities.

(d) Give the idea of the proof of (F5) in two sentences.

Solution.

(a) In the monomial line of (F6), where $ab = ba$ in R gives $(ab)x^{m+n} = (ba)x^{n+m}$. In the additivity law $(*)$, where $(p_i + p_i')q_{k-i} = p_iq_{k-i} + p_i'q_{k-i}$ is (F9) only after (F6) has moved q_{k-i} to the left. And in small ways, wherever $0 \cdot b = 0$ is obtained from $b \cdot 0 = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)), as in Lemma 4.2.2 (a), and in (F7), where $1\,p_k = p_k \cdot 1$. The monomial line of (F5) uses it only through Lemma 4.2.2 (a); its own coefficient step $(ab)c = a(bc)$ does **not**.

(b) With $a = 2, m = 1$, $b = 3, n = 2$, $c = 1, l = 1$: $((2x)(3x^2))x = (6x^3)x = 6x^4$, using $2 \cdot 3 = 6$, $1 + 2 = 3$, then $6 \cdot 1 = 6$, $3 + 1 = 4$; and $(2x)((3x^2)x) = (2x)(3x^3) = 6x^4$,

using $3 \cdot 1 = 3$, $2 + 1 = 3$, then $2 \cdot 3 = 6$, $1 + 3 = 4$. Both are $6x^4$.

(c) For Φ: $(pq)(r + r') = (pq)r + (pq)r'$, which is $(**)$ with pq in place of p. For Ψ: $p(q(r + r')) = p(qr + qr') = p(qr) + p(qr')$, which is $(**)$ twice.

(d) On monomials, associativity is a single product: $(ab)c = a(bc)$ in R and $(m + n) + l = m + (n + l)$ in $\mathbb{N}$. Both sides of $(pq)r = p(qr)$ are additive in each argument and every polynomial is a finite sum of monomials, so the monomial case extends to all polynomials, one argument at a time.

4.2.4.2 B. Practice

Exercise. B1: A product over two rings

Compute $(2x^3 - x + 4)(-2x^3 + x^2 + 3)$ in $\mathbb{Z}[x]$ and in $\mathbb{F}_2[x]$, from Definition 4.2.1.

Solution. In $\mathbb{Z}[x]$, $(p_0, p_1, p_2, p_3) = (4, -1, 0, 2)$ and $(q_0, q_1, q_2, q_3) = (3, 0, 1, -2)$, with 3 admissible for both; so $(pq)_k = 0$ for $k > 6$, and

$$\begin{aligned}
(pq)_0 &= 4 \cdot 3 = 12,\\
(pq)_1 &= 4 \cdot 0 + (-1) \cdot 3 = -3,\\
(pq)_2 &= 4 \cdot 1 + (-1) \cdot 0 + 0 \cdot 3 = 4,\\
(pq)_3 &= 4 \cdot (-2) + (-1) \cdot 1 + 0 \cdot 0 + 2 \cdot 3 = -3,\\
(pq)_4 &= (-1)(-2) + 0 \cdot 1 + 2 \cdot 0 = 2,\\
(pq)_5 &= 0 \cdot (-2) + 2 \cdot 1 = 2,\\
(pq)_6 &= 2 \cdot (-2) = -4,
\end{aligned}$$

where in positions $4, 5, 6$ the terms with an index above 3 are 0 and have been left out. Hence

$$pq = -4x^6 + 2x^5 + 2x^4 - 3x^3 + 4x^2 - 3x + 12.$$

In $\mathbb{F}_2[x]$ the displays name other sequences: $2 = 0$, $4 = 0$, $-1 = 1$, $-2 = 0$ and $3 = 1$ in $\mathbb{F}_2$, so the first factor is x and the second is $x^2 + 1$. By Lemma 4.2.2 (a) with $a = 1$, $m = 1$, the product shifts $(1, 0, 1, 0, \dots)$ one place up: $x(x^2 + 1) = x^3 + x$. This agrees with reducing the integer coefficients $12, -3, 4, -3, 2, 2, -4$ modulo 2, which gives $0, 1, 0, 1, 0, 0, 0$.

Exercise. B2: Changing the sign of x

Define $\sigma\colon R[x] \to R[x]$ by $\sigma(p)_k := (-1)^k p_k$, where $(-1)^k$ is the power in R (Lemma 4.1.1 (c)). Then $\sigma(p)$ is a polynomial, since $(-1)^k \cdot 0 = 0$. We want to prove that $\sigma(pq) = \sigma(p)\sigma(q)$ for all $p, q \in R[x]$.

You may use the following, without proof. The map σ is additive: $\sigma(p + q) = \sigma(p) + \sigma(q)$, position by position by (F9). Hence, with $(*)$ and $(**)$, the maps $\Phi(p, q) := \sigma(pq)$ and $\Psi(p, q) := \sigma(p)\sigma(q)$ are additive in each argument.

The last step is blank. *Name the move, then complete it.*

Solution. The move is **check on monomials, extend by additivity**.

Let $a, b \in R$ and $m, n \in \mathbb{N}$. The monomial ax^m has only position m possibly non-zero, so $\sigma(ax^m) = ((-1)^m a)x^m$. By Lemma 4.2.2 (b),

$$\Phi(ax^m, bx^n) = \sigma((ab)x^{m+n}) = ((-1)^{m+n}ab)x^{m+n},$$

$$\Psi(ax^m, bx^n) = ((-1)^m a)x^m \cdot ((-1)^n b)x^n = ((-1)^m a\,(-1)^n b)x^{m+n}.$$

The two coefficients agree: $(-1)^m a\,(-1)^n b = ((-1)^m(-1)^n)(ab) = (-1)^{m+n}ab$, by (F5) and (F6) in R and the first power law of Lemma 4.1.1 (c). So Φ and Ψ agree on monomials, and by Lemma 4.2.3 with two arguments and $T = R[x]$, $\sigma(pq) = \sigma(p)\sigma(q)$ for all p, q.

Also $\sigma(1) = 1$, since $(-1)^0 = 1$. Section 4.4 writes $\sigma(p)$ as $p(-x)$.

4.2.4.3 C. Going deeper

Exercise. C1: Exit check: the ring laws

Let R be a commutative ring. Prove, from Definition 4.2.1, that the multiplication of $R[x]$ is commutative and associative. You may use the laws of R, Lemma 4.1.1, Logic and Proof, Axiom 4.2.1 and Sets, Relations, and Cardinality, Proposition 1.4.1, but no result of this section after Definition 4.2.1.

Solution. Distributivity. For $p, p', q, q' \in R[x]$, the k-th coefficient of $(p + p')q$ is $\sum_{i=0}^{k}(p_i + p'_i)q_{k-i}$. Inside each term, (F6), (F9), (F6) give $p_i q_{k-i} + p'_i q_{k-i}$, and ($\Sigma$1) splits the sum into $(pq)_k + (p'q)_k$. So $(p + p')q = pq + p'q$, and in the same way, with (F9) directly, $p(q + q') = pq + pq'$. Hence $(p, q) \mapsto pq$ and $(p, q) \mapsto qp$ are additive in each argument, and so are $(p, q, r) \mapsto (pq)r$ and $(p, q, r) \mapsto p(qr)$, by applying the two laws twice.

Monomials. For $a, b \in R$ and $m, n \in \mathbb{N}$, the k-th coefficient of $(ax^m)(bx^n)$ is $\sum_{i=0}^{k}(ax^m)_i(bx^n)_{k-i}$. Every term with $i \neq m$ is 0, and the term with $i = m$ (present when $m \leq k$) is $a\,(bx^n)_{k-m}$, which is ab if $k = m + n$ and 0 otherwise. By (Σ3), $(ax^m)(bx^n) = (ab)x^{m+n}$.

Reduction. (i) For $p \in R[x]$, the sum $s_N := \sum_{k=0}^{N} p_k x^k$ in $(R[x], +)$ (Lemma 4.1.1 (a)) has p_j in position $j \leq N$ and 0 beyond, by Logic and Proof, Axiom 4.2.1 on N: $s_0 = p_0 x^0$, and $s_{N+1} = s_N + p_{N+1}x^{N+1}$ has coefficients $p_j + 0$, $0 + p_{N+1}$ and $0 + 0$ for $j \leq N$, $j = N + 1$ and $j > N + 1$, by (F1) and (F3). So $p = s_N$ for admissible N (Sets, Relations, and Cardinality, Proposition 1.4.1).

(ii) Let $\Phi, \Psi\colon R[x] \to R[x]$ be additive and agree on monomials. By Logic and Proof, Axiom 4.2.1 on N, $\Phi(p) = \Psi(p)$ for every p for which N is admissible: for $N = 0$, $p = p_0 x^0$ by (i); if $N + 1$ is admissible for p, then $p = s_N + p_{N+1}x^{N+1}$ with N admissible for s_N, by (i), and

$$\Phi(p) = \Phi(s_N) + \Phi(p_{N+1}x^{N+1}) = \Psi(s_N) + \Psi(p_{N+1}x^{N+1}) = \Psi(p)$$

by additivity, the induction hypothesis with the monomial case, and additivity. Every polynomial has an admissible N, so $\Phi = \Psi$.

(iii) With two arguments, fix a monomial u and apply (ii) to $v \mapsto \Phi(u, v)$ and $v \mapsto \Psi(u, v)$; then fix any q and apply (ii) to the first argument. With three, treat the third, the second and the first argument in turn.

Commutativity. $(ax^m)(bx^n) = (ab)x^{m+n} = (ba)x^{n+m} = (bx^n)(ax^m)$, by (F6) in R and $m+n = n+m$ in $\mathbb{N}$; the reduction gives $pq = qp$.

Associativity. $((ax^m)(bx^n))(cx^l) = ((ab)c)x^{(m+n)+l}$ and $(ax^m)((bx^n)(cx^l)) = (a(bc))x^{m+(n+l)}$, equal by (F5) in R and associativity of $+$ in $\mathbb{N}$; the reduction with three arguments gives $(pq)r = p(qr)$.

Marking scheme. (10 points) - 2: both distributive laws from the coefficient formula, naming the rule for a single-index sum ((Σ1)) and the law of R used inside each term. - 2: the product of two monomials, $(ax^m)(bx^n) = (ab)x^{m+n}$, with the vanishing of the other terms shown. - 3: the reduction to monomials, with additivity in each argument stated and used one argument at a time (both inductions proved in the answer; citing Lemma 4.2.3 earns none of these points). - 1: commutativity on monomials, naming (F6) in R. - 2: associativity on monomials, naming (F5) in R and the law of $\mathbb{N}$ used for the exponents.

Fatal errors (0 for the step): treating polynomials as functions on R and citing the laws of R "pointwise"; checking only on x^m and x^n, with no account of the coefficients (the coefficients are where (F5) and (F6) of R are needed).

A direct route works with coefficients throughout: commutativity by (F6) and the reversal $i \mapsto k - i$ of a finite sum, associativity by rewriting both triple products as one sum over all (i, j, l) with $i + j + l = k$. Each needs a lemma that (Σ1)–(Σ4) do not contain, proved by induction. Commutativity with the reversal proved earns 3 points (the monomial product and commutativity on monomials); associativity with the reindexing proved earns the other 7. An unproved reversal or reindexing earns 0 for that step.

Exercise. C2: Formal power series

Let $R^{\mathbb{N}}$ be the set of **all** sequences $\mathbb{N} \to R$, with sum and product given by the formulas of Definition 4.2.1.

(a) Show that the formulas define functions $R^{\mathbb{N}} \times R^{\mathbb{N}} \to R^{\mathbb{N}}$.

(b) Show that $R[x] \subseteq R^{\mathbb{N}}$ is closed under the sum and the product.

(c) Let $s \coloneqq (1, 1, 1, \dots)$. Show that $(1 - x)s = 1$.

(d) Which step of the proof of Lemma 4.2.3 (with one argument) does not reach the elements of $R^{\mathbb{N}}$?

Solution.

(a) For $p, q \in R^{\mathbb{N}}$ and $k \in \mathbb{N}$, $p_k + q_k \in R$, and $\sum_{i=0}^{k} p_i q_{k-i}$ is a sum of $k+1$ elements of R, defined by Lemma 4.1.1 (a). No finiteness of p or q is needed: each coefficient of the product only looks at positions $0, \dots, k$. So both formulas give sequences $\mathbb{N} \to R$.

(b) This is the closure paragraph after Definition 4.2.1: if m and n are admissible for p and q, then $\max(m, n)$ is admissible for $p + q$ and $m + n$ for pq.

(c) $1 - x = (1, -1, 0, 0, \dots)$. In position 0, $((1 - x)s)_0 = 1 \cdot 1 = 1$. In position $k \geq 1$, write the i-th term as $v_i + w_i$ (by (F1) and (F3)), with $v_0 = 1 \cdot 1$, $w_1 = (-1) \cdot 1$ and every other v_i, w_i equal to 0, since for $i \geq 2$ the term is $0 \cdot 1 = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) with (F6)). By (Σ1) and (Σ3), the sum is $1 \cdot 1 + (-1) \cdot 1 = 1 + (-1) = 0$, by (F7) and (F4). So $(1 - x)s = (1, 0, 0, \dots) = 1$.

(d) The induction proves $\Phi(p) = \Psi(p)$ only for sequences p that have an admissible N; the step from it to $\Phi = \Psi$ uses that every polynomial has one. The sequence s has none, and it is not a finite sum of monomials either, since by (b) such a sum is a polynomial. So Lemma 4.2.3 says nothing about s, and the proof of Theorem 4.2.4 does not apply to $R^{\mathbb{N}}$. The ring laws do hold in $R^{\mathbb{N}}$, the ring of **formal power series**, though we do not prove this here; nothing in this book depends on it.

So $(1 - x)s = 1$ among all sequences, while Section 4.3 shows that over $\mathbb{Z}$, $1 - x$ is not a unit of $\mathbb{Z}[x]$.

4.3 Degree, Leading Coefficients, and Integral Domains

Section 4.2 made $R[x]$ a commutative ring for every commutative ring R (Theorem 4.2.4). This section attaches to each non-zero polynomial its **degree**, the position of its last non-zero coefficient, and asks the school question: is the degree of a product the sum of the degrees? Over $\mathbb{Z}$ it is. Over $\mathbb{Z}/6\mathbb{Z}$ it is not, and the reason is a single product of two elements of R. Sorting out which rings behave like $\mathbb{Z}$ leads to the integral domains, and to the two facts later chapters use most: a polynomial ring over an integral domain has no zero divisors, and its units are the units of R.

Throughout, R is a commutative ring (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1), and polynomials are coefficient sequences (Definition 4.1.1), with the sum and product of Definition 4.2.1.

4.3.1 Degree and leading coefficient

Here is the computation that drives the section. Multiply $p = 2x + 1$ by $q = 3x^2 + x$ by the product formula of Definition 4.2.1, once in $\mathbb{Z}[x]$ and once in $(\mathbb{Z}/6\mathbb{Z})[x]$. The coefficients of p are $1, 2, 0, 0, \ldots$ and those of q are $0, 1, 3, 0, \ldots$, so

$$\begin{aligned}(pq)_0 &= p_0q_0 = 0,\\ (pq)_1 &= p_0q_1 + p_1q_0 = 1,\\ (pq)_2 &= p_0q_2 + p_1q_1 + p_2q_0 = 3 + 2 = 5,\\ (pq)_3 &= p_0q_3 + p_1q_2 + p_2q_1 + p_3q_0 = 2 \cdot 3 = 6,\end{aligned}$$

and $(pq)_k = 0$ for $k \geq 4$. Over $\mathbb{Z}$ the product is $6x^3 + 5x^2 + x$, with its last non-zero coefficient in position $3 = 1 + 2$. Over $\mathbb{Z}/6\mathbb{Z}$ the same sums are read modulo 6: $(pq)_3 = [6] = [0]$, and the product is $[5]x^2 + x$, whose last non-zero coefficient sits in position 2. The top coefficient of the product was $2 \cdot 3$, the product of the top coefficients of the factors, and in $\mathbb{Z}/6\mathbb{Z}$ that product is $[0]$ (Number Systems: From \(\nN\) to \(\nR\), Example (Multiplication modulo six and modulo five)).

To state any of this we need a name for "the position of the last non-zero coefficient". A non-zero polynomial has one, because only finitely many of its coefficients are non-zero.

The degree of a polynomial is the position of its last non-zero coefficient; the leading coefficient is the coefficient sitting there.

Definition 4.3.1. Degree, Leading Coefficient, Monic

Let R be a commutative ring and $p \in R[x]$.

(a) If $p \neq 0$, the **degree** $\deg p$ is the **largest** $n \in \mathbb{N}$ with $p_n \neq 0$. The **leading coefficient** of p is $\mathrm{lc}(p) := p_{\deg p}$, and p is **monic** if $\mathrm{lc}(p) = 1$.

(b) The zero polynomial has degree $\deg 0 := -\infty$, and **no** leading coefficient.

Here $-\infty$ is a symbol not in $\mathbb{N}$, with the conventions $-\infty < n$ and $-\infty + n = n + (-\infty) = -\infty$ for every $n \in \mathbb{N}$, and $-\infty + (-\infty) = -\infty$.

In words: (a) looks along the coefficient sequence and stops at the last place where it is non-zero; that place is the degree, and the entry there is the leading coefficient. A polynomial is monic when that entry is 1. Clause (b) gives the zero polynomial, which has no non-zero coefficient at all, a degree below every natural number.

Well-definedness. Let $p \neq 0$, and let N be admissible for p: $p_k = 0$ for every $k > N$ (Definition 4.1.1). The set $S := \{n \in \mathbb{N} : p_n \neq 0\}$ is non-empty, since p is not the zero sequence, and every element of S is at most N. Read in $\mathbb{Z} \supseteq \mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3), S is a non-empty set of integers bounded above, so it has a greatest element (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6). That element is $\deg p$. Two facts come with it, and every proof below uses them:

$$p_{\deg p} \neq 0, \qquad p_k = 0 \ \text{ for every } k > \deg p.$$

The second says that $\deg p$ is itself admissible for p, and the least admissible N: any smaller N would leave the non-zero coefficient $p_{\deg p}$ beyond it.

Examples.

- In $\mathbb{Q}[x]$, $\deg(3x^2 - x + 2) = 2$ with leading coefficient 3; $x^2 + 1$ is monic of degree 2. The monomial ax^n with $a \neq 0$ has degree n and leading coefficient a.
- A non-zero constant $a = ax^0$ has degree 0. The constant 0 has degree $-\infty$, not 0: degree 0 means "a constant, and not the zero one".
- Degree depends on the ring. The integer polynomial $6x^3 + 5x^2 + x$ has degree 3 in $\mathbb{Z}[x]$; its coefficients read in $\mathbb{Z}/6\mathbb{Z}$ give $[5]x^2 + x$, of degree 2. Read in $\mathbb{Z}/5\mathbb{Z}$ they give $x^3 + x$ ($[6] = [1]$, $[5] = [0]$), monic of degree 3.
- **The degenerate ring.** If $1 = 0$ in R, then every $a \in R$ is $a = a \cdot 1 = a \cdot 0 = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)), so $R = \{0\}$, and the only polynomial over R is the zero sequence. Every polynomial over the zero ring has degree $-\infty$, and no polynomial over it is monic. This is why "monic" will never need the hypothesis $1 \neq 0$: a monic polynomial is non-zero, so its ring has $1 = \mathrm{lc}(p) \neq 0$.

Non-example by minimal change. The sequence $(1, 1, 1, \dots)$ has no degree: the set S of its non-zero positions is all of $\mathbb{N}$, which has no greatest element. It fails exactly the clause "only finitely many" of Definition 4.1.1, which is what made S bounded above.

↻ **Second reading** · *Why the degree of the zero polynomial is minus infinity*

Any value given to $\deg 0$ is a convention, and the choice is made so that the rule "degrees add under products" survives the zero polynomial. For every q, $0 \cdot q = 0$, so the rule asks for $\deg 0 = \deg 0 + \deg q$. If $\deg 0$ were an integer d, then in any ring with $1 \neq 0$ the case $q = x$, of

degree 1, would give $d = d+1$. No integer works; a symbol $-\infty$ with $-\infty + n = -\infty$ does. The order $-\infty < n$ then lets "$\deg p \leq n$" include the zero polynomial, which is what the sets $R[x]_{\leq n}$ at the end of this section need.

Warning. The leading coefficient is the coefficient of the **highest** power, not the first one written. In $2 + x - 5x^3 \in \mathbb{Q}[x]$, the leading coefficient is -5, and the polynomial is not monic although its x has coefficient 1. And the zero polynomial has no leading coefficient at all: "$\mathrm{lc}(p)$" silently assumes $p \neq 0$.

4.3.2 The degree of a sum

A sum cannot raise the degree, because adding coefficients position by position creates no non-zero coefficient beyond the last non-zero ones of the summands.

Theorem 4.3.1. Degree of a Sum

Let R be a commutative ring and $p, q \in R[x]$. Then

$$\deg(p+q) \leq \max(\deg p, \deg q),$$

with **equality** when $\deg p \neq \deg q$.

Idea. Beyond the larger of the two degrees both summands have only zero coefficients, so the sum does too. When one degree is strictly larger, the other summand contributes 0 at that top position, and the top coefficient survives.

Proof. Let $M := \max(\deg p, \deg q)$. If $M = -\infty$, then $p = q = 0$, so $p+q = 0$ and both sides are $-\infty$. Otherwise $M \in \mathbb{N}$, and for $k > M$ we have $k > \deg p$ and $k > \deg q$, so $p_k = 0$ and $q_k = 0$ (by the two facts after Definition 4.3.1 when the polynomial is non-zero, and trivially when it is 0). Hence $(p+q)_k = p_k + q_k = 0 + 0 = 0$ for every $k > M$, by Definition 4.2.1 and (F3). So either $p+q = 0$, with degree $-\infty < M$, or $p+q \neq 0$ and its last non-zero coefficient is at a position $\leq M$. In both cases $\deg(p+q) \leq M$.

Now let $\deg p \neq \deg q$; by symmetry $\deg q < \deg p$, so $p \neq 0$ and $M = \deg p$. Then $q_M = 0$, and

$$(p+q)_M = p_M + q_M = p_M + 0 = p_M \neq 0,$$

so $p + q \neq 0$ and $\deg(p+q) \geq M$. With the first part, $\deg(p+q) = M$.

■

Remark. The inequality is strict exactly when $\deg p = \deg q = M \in \mathbb{N}$ and the leading coefficients cancel, $p_M + q_M = 0$: for example $(x^2 + x) + (-x^2 + 1) = x + 1$, of degree $1 < 2$, and $x + (-x) = 0$, of degree $-\infty < 1$.

4.3.3 The degree of a product

The opening computation suggests how a product behaves at the top. In $(pq)_k = \sum_{i=0}^{k} p_i q_{k-i}$, a term can be non-zero only if $i \le \deg p$ **and** $k - i \le \deg q$; for $k = \deg p + \deg q$ that leaves exactly one term. We call this move **look at the top coefficient**.

Theorem 4.3.2. Degree of a Product

Let R be a commutative ring, let $p, q \in R[x]$ be non-zero, and let $m := \deg p$, $n := \deg q$.

(a) $(pq)_k = 0$ for every $k > m+n$, and $(pq)_{m+n} = \operatorname{lc}(p)\operatorname{lc}(q)$. Hence $\deg(pq) \le \deg p + \deg q$ for **all** $p, q \in R[x]$, zero or not; and if $p = 0$ or $q = 0$, then $pq = 0$ and $\deg(pq) = -\infty = \deg p + \deg q$.

(b) $\deg(pq) = m + n$ **if and only if** $\operatorname{lc}(p)\operatorname{lc}(q) \neq 0$, and then $\operatorname{lc}(pq) = \operatorname{lc}(p)\operatorname{lc}(q)$. This holds in particular

- when R has **no zero divisors** ($ab = 0$ implies $a = 0$ or $b = 0$), for example when R is a field (Theorem 2.1.1 (f)); together with the last clause of (a), $\deg(pq) = \deg p + \deg q$ then holds for **all** $p, q \in R[x]$, zero or not;
- when $\operatorname{lc}(p)$ is a unit of R (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1), in particular when p is monic.

In words: (a) says that the product has nothing above position $m + n$, and that what sits at $m + n$ is the product of the two leading coefficients, in every commutative ring; (b) says that the degree formula holds precisely when that one product is non-zero, and names two common situations where it is.

Idea. The top of a product comes from the tops of the factors alone. Above $m + n$ every term $p_i q_{k-i}$ has a factor beyond the top of p or beyond the top of q; at $m + n$ exactly one term escapes, $p_m q_n$. So the only question is whether $p_m q_n$ can be 0, and that is a question about R, not about polynomials.

Before reading on: which line needs R to have no zero divisors, and which works in every ring?

Proof. *(a)* Let $k \ge m + n$ and $0 \le i \le k$, and consider the term $p_i q_{k-i}$ of $(pq)_k$ (Definition 4.2.1). If $i > m$, then $p_i = 0$. If $i \le m$, then $k - i \ge k - m \ge n$, and $k - i > n$ (so $q_{k-i} = 0$) unless $k = m + n$ and $i = m$. So every term with $i \neq m$, or with $k > m + n$, has a factor 0, and is 0 by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) with (F6).

For $k > m + n$, all terms of $(pq)_k$ are 0, so $(pq)_k = 0$ by (Σ3) of Lemma 4.1.1 (b) (with $j = 0$). For $k = m + n$, every term with $i \neq m$ is 0, and $m \le m + n$, so (Σ3) with $j = m$ leaves

$$(pq)_{m+n} = p_m q_n = \operatorname{lc}(p)\operatorname{lc}(q).$$

For the inequality, let $p, q \in R[x]$ be arbitrary. If $p = 0$, every coefficient of pq is a sum of terms $0 \cdot q_{k-i} = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), (F6)), so $pq = 0$, and both sides of the inequality are $-\infty$ by the conventions of Definition 4.3.1, which is also the last clause of (a); likewise if $q = 0$. If $p, q \neq 0$ and $pq = 0$, the left side is

$-\infty < m+n$. Otherwise $pq \neq 0$, and since $(pq)_k = 0$ for every $k > m+n$, its last non-zero coefficient is at a position $\leq m+n$: $\deg(pq) \leq m+n$.

(b) By (a), $m+n$ is admissible for pq, and $(pq)_{m+n} = \operatorname{lc}(p)\operatorname{lc}(q)$. If this element is non-zero, then $pq \neq 0$, its last non-zero coefficient is at $m+n$, and so $\deg(pq) = m+n$ and $\operatorname{lc}(pq) = (pq)_{m+n} = \operatorname{lc}(p)\operatorname{lc}(q)$. If it is 0, then $(pq)_k = 0$ for every $k \geq m+n$, so $\deg(pq) < m+n$.

For the two situations: $p_m \neq 0$ and $q_n \neq 0$ by Definition 4.3.1, so if R has no zero divisors, $p_m q_n \neq 0$. If $u := p_m$ is a unit and $uq_n = 0$, then $q_n = (u^{-1}u)q_n = u^{-1}(uq_n) = u^{-1} \cdot 0 = 0$, by (F6), (F7), (F5) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), against $q_n \neq 0$; so $p_m q_n \neq 0$. A monic p has $p_m = 1$, a unit since $1 \cdot 1 = 1$. This proves the theorem.

■

The answer to the prompt. Part (a), including the inequality, uses only (F1)–(F7), (F9), Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), (Σ3) of Lemma 4.1.1 (b), and the two facts after Definition 4.3.1 and its conventions, all valid in every commutative ring: it holds over $\mathbb{Z}/6\mathbb{Z}$ as over $\mathbb{Q}$. Part (b) as an equivalence also holds in every ring. "No zero divisors" enters in one line, the first sentence of the last paragraph, and only to decide that $p_m q_n \neq 0$; the unit hypothesis is a second, different way to decide the same thing.

Warning. **The degree formula is not automatic.** In $(\mathbb{Z}/6\mathbb{Z})[x]$, the opening computation gives

$$([2]x + [1])([3]x^2 + x) = [5]x^2 + x,$$

a product of polynomials of degrees 1 and 2 that has degree 2, not 3. The coefficient $(pq)_3$ is $\operatorname{lc}(p)\operatorname{lc}(q) = [2][3] = [6] = [0]$ (Number Systems: From \(\nN\) to \(\nR\), Example (Multiplication modulo six and modulo five)). Part (a) of Theorem 4.3.2 holds here; the hypothesis of (b) fails.

Quick check. Let $p, q \in \mathbb{Q}[x]$ with $\deg p = 3$ and $\deg q = 2$. What are $\deg(pq)$, $\deg(p+q)$ and $\deg(p^2)$, where $p^2 := pp$? Can you say what $\deg(p - x^3)$ is?

Solution. $\deg(pq) = 5$ and $\deg(p^2) = 6$, by Theorem 4.3.2 (b): $\mathbb{Q}$ is a field (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3), so it has no zero divisors. $\deg(p+q) = 3$, by the equality case of Theorem 4.3.1, since $3 \neq 2$. The degree of $p - x^3$ is not determined: it is 3 if $\operatorname{lc}(p) \neq 1$, at most 2 if p is monic, and $-\infty$ if $p = x^3$. The difference has coefficient $\operatorname{lc}(p) - 1$ at position 3, and that coefficient decides.

4.3.4 Integral domains

Theorem 4.3.2 (b) asks for one property of R: a product of two non-zero elements is non-zero. The integers have it, every field has it, $\mathbb{Z}/6\mathbb{Z}$ lacks it. A ring that has it, and is not the zero ring, gets a name.

An integral domain is a commutative ring in which a product is zero only when a factor is zero.

Definition 4.3.2. Integral Domain

An **integral domain** is a commutative ring R with $1 \neq 0$ and **no zero divisors**: **for all** $a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$.

In words: the zero ring is excluded, and the rule "a product vanishes only if a factor vanishes", the rule used to solve $(x-1)(x-2) = 0$ at school, holds in R. Equivalently, by contraposition: the product of two non-zero elements is non-zero.

Example. Which Rings Are Integral Domains

Decide which of the following are integral domains: $\mathbb{Z}$; a field, and in particular $\mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z}$ for a prime p; $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$ not prime (Sets, Relations, and Cardinality, Definition 2.2.2); $\mathbb{Z}/1\mathbb{Z}$; and $\mathbb{Z} \times \mathbb{Z}$ with componentwise operations, $(a, b) + (c, d) := (a + c, b + d)$ and $(a, b)(c, d) := (ac, bd)$.

Solution. *$\mathbb{Z}$: yes.* It is a commutative ring with $1 \neq 0$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.1), and an ordered commutative ring (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.3.4), so $ab = 0$ implies $a = 0$ or $b = 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (f).

A field: yes. A field has $1 \neq 0$ (Definition 2.1.1) and no zero divisors (Theorem 2.1.1 (f)). So $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3) and $\mathbb{Z}/p\mathbb{Z}$ for p prime (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2) are integral domains.

$\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$ not prime: no. By Sets, Relations, and Cardinality, Definition 2.2.2, n has a positive divisor $r \notin \{1, n\}$; write $n = rs$. As in the proof of Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2 ($\Rightarrow$), $1 < r < n$ and $0 < s < n$. Then $[r] \neq [0]$: otherwise $n \mid r$ with $n, r > 0$, and Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e) would give $n \leq r$, against $r < n$. Likewise $[s] \neq [0]$. But $[r][s] = [rs] = [n] = [0]$, by the multiplication of Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2 (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (b)).

$\mathbb{Z}/1\mathbb{Z}$: no. It has $[1] = [0]$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (c)); it is the zero ring.

$\mathbb{Z} \times \mathbb{Z}$: no. Each ring axiom holds componentwise, because it holds in each coordinate in $\mathbb{Z}$, with zero $(0, 0)$ and one $(1, 1) \neq (0, 0)$. But $(1, 0)(0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$, with both factors non-zero.

Putting the second and third answers together with Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2: for $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if it is a field, if and only if n is prime.

Now the payoff. Over an integral domain the degree formula holds without exception, and the polynomial ring inherits the property it was built from.

Corollary 4.3.3. Polynomial Rings over Integral Domains

Let R be a commutative ring.

(a) If R is an integral domain, $p, q \in R[x]$ and $pq = 0$, then $p = 0$ or $q = 0$. So $R[x]$ is an integral domain.

(b) (Cancellation) If R is an integral domain, $p, q, r \in R[x]$, $pq = pr$ and $p \neq 0$, then $q = r$.

(c) Conversely, if $R[x]$ is an integral domain, then so is R.

Proof. *(a)* Let $p \neq 0$ and $q \neq 0$. Since R has no zero divisors, Theorem 4.3.2 (b) gives $\deg(pq) = \deg p + \deg q \in \mathbb{N}$, so $\deg(pq) \neq -\infty$ and $pq \neq 0$. By contraposition, $pq = 0$ implies $p = 0$ or $q = 0$. Moreover $R[x]$ is a commutative ring (Theorem 4.2.4 (a)), and $1 \neq 0$ in $R[x]$ because $1 \neq 0$ in R (Theorem 4.2.4 (b)). So $R[x]$ is an integral domain.

(b) By (F9) of $R[x]$ and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (c), $p(q - r) = pq - pr = 0$. By (a) and $p \neq 0$, $q - r = 0$, so $q = r$ (add r to both sides, with (F2), (F1), (F4), (F3)).

(c) The map $a \mapsto ax^0$ from R to $R[x]$ is injective and preserves sums, products and 1 (Theorem 4.2.4 (b)). If $1 = 0$ in R, then the one of $R[x]$, which is $1x^0$, equals $0x^0$, the zero polynomial, against $1 \neq 0$ in $R[x]$. If $ab = 0$ in R, then $(ax^0)(bx^0) = (ab)x^0 = 0x^0$ is the zero polynomial, so $ax^0 = 0x^0$ or $bx^0 = 0x^0$, and by injectivity $a = 0$ or $b = 0$.

■

With $R = \mathbb{Q}$, Definition 4.3.1, Theorem 4.3.2 (b) and part (a) are the polynomial algebra that the ordered field $\mathbb{Q}(t)$ of Number Systems: From \(\nN\) to \(\nR\), Example (A Non-Archimedean Ordered Field) took on school credit: the degree and the leading coefficient of a polynomial, the rule $\operatorname{lc}(pq) = \operatorname{lc}(p)\operatorname{lc}(q)$, and the absence of zero divisors in $\mathbb{Q}[t]$ (the letter t there plays the part of our x). Building fractions p/q of polynomials is a further step, which this volume does not take.

The cancellation law (b) is what makes it legitimate to "divide both sides by p" in an identity of polynomials over $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{F}_p$. Over $\mathbb{Z}/6\mathbb{Z}$ it fails: $[2] \cdot [3]x = [0] = [2] \cdot [0]$ with $[2] \neq [0]$ and $[3]x \neq [0]$.

4.3.5 Units of a polynomial ring

The degree also tells us which polynomials can be inverted. If $pq = 1$ and degrees add, then $\deg p + \deg q = 0$, so both are constants.

Proposition 4.3.4. Units of a Polynomial Ring

Let R be an integral domain. Then the units of $R[x]$ are exactly the constants a with $a \in R^\times$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1): identifying a with ax^0, $(R[x])^\times = R^\times$.

Proof. Let p be a unit of $R[x]$, with $pq = 1$. Since $1 \neq 0$ in $R[x]$ (Corollary 4.3.3 (a)) and $0 \cdot q = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) in the commutative ring $R[x]$, Theorem 4.2.4 (a)), we have $p \neq 0$, and likewise $q \neq 0$. By Theorem 4.3.2 (b), $\deg p + \deg q = \deg 1 = 0$. Two natural numbers with sum 0 are both 0, so $\deg p = \deg q = 0$: $p = ax^0$ and $q = bx^0$ with $a = p_0$, $b = q_0 \in R$ (0 is admissible for p and q by the facts after Definition 4.3.1, so Proposition 4.2.1 with $N = 0$ applies). Then $(ab)x^0 = (ax^0)(bx^0) = 1x^0$

(Theorem 4.2.4 (b)), so $ab = 1$ by injectivity of $a \mapsto ax^0$, and $a \in R^\times$.

Conversely, if $a \in R^\times$ with $ab = 1$, then $(ax^0)(bx^0) = (ab)x^0 = 1x^0$, so the constant a is a unit of $R[x]$.

■

For a field F, $F^\times$ consists of the non-zero elements (by (F8), and 0 is not a unit since $0 \cdot b = 0 \neq 1$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) and (F6)). So the units of $F[x]$ are the non-zero constants. Over $\mathbb{Z}$, an integral domain (Example (Which Rings Are Integral Domains)), the units of $\mathbb{Z}[x]$ are the constants 1 and -1, since $\mathbb{Z}^\times = \{1, -1\}$ (the examples after Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1): 2 is a unit of $\mathbb{Q}[x]$ and not of $\mathbb{Z}[x]$.

Warning. **Without "integral domain", non-constant units exist.** In $(\mathbb{Z}/4\mathbb{Z})[x]$,

$$(1 + [2]x)^2 = 1 + [4]x + [4]x^2 = 1,$$

by the product formula: the coefficients are $1 \cdot 1$, $1 \cdot [2] + [2] \cdot 1$ and $[2][2]$. So $1 + [2]x$ is a unit of degree 1, its own inverse. The proof above breaks at Theorem 4.3.2 (b): $\operatorname{lc}(p) \operatorname{lc}(p) = [2][2] = [0]$, so degrees do not add.

4.3.6 Polynomials of bounded degree

Many later arguments fix a bound on the degree: interpolation through $n+1$ points looks for a polynomial of degree at most n, and the linear-algebra companion treats such polynomials as a vector space. Two sets get names.

Definition 4.3.3. Polynomials of Degree at Most n

Let R be a commutative ring and $n \in \mathbb{N}$. The set of **polynomials of degree at most** n is

$$R[x]_{\leq n} \coloneqq \{p \in R[x] : \deg p \leq n\}.$$

There are two ways to describe this set, and it is worth seeing that they agree. A polynomial has $\deg p \leq n$ exactly when $p_k = 0$ for every $k > n$: for $p \neq 0$ by the two facts after Definition 4.3.1, and for $p = 0$ both hold. By Proposition 4.2.1, such a p is the sum $p_0 + p_1 x + \cdots + p_n x^n$ of its first $n+1$ monomials, and every such sum, with $a_0, \ldots, a_n \in R$ arbitrary, has its coefficients beyond n equal to 0. So

$$R[x]_{\leq n} = \{a_0 + a_1 x + \cdots + a_n x^n : a_0, \ldots, a_n \in R\}.$$

The first description is about degrees; the second is the one used for computing. Some of the a_i, including a_n, may be 0, and $0 \in R[x]_{\leq n}$ (all $a_i = 0$; $-\infty \leq n$).

The set is closed under the operations that do not raise the degree. If $p, q \in R[x]_{\leq n}$, then $p + q \in R[x]_{\leq n}$ by Theorem 4.3.1; $-p \in R[x]_{\leq n}$, since $(-p)_k = -p_k = -0 = 0$ for $k > n$; and $ap \in R[x]_{\leq n}$ for every constant a, since $(ap)_k = ap_k = a \cdot 0 = 0$ for $k > n$ (Theorem 4.2.4 (d), Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)). It is not closed under products: $x^n \cdot x \notin R[x]_{\leq n}$ when $1 \neq 0$.

Example. Membership in Polynomials of Bounded Degree

Which of $3x^2 - 2x + 1$, $5x + 7$, -4, 0 and $x^3 - x^3 + x$ lie in $\mathbb{Q}[x]_{\leq 2}$? Which lie in $\mathbb{Q}[x]_{\leq 0}$?

Solution. The degrees are 2, 1, 0, $-\infty$ and 1: the last expression is the polynomial x, since its coefficient in position 3 is $1 + (-1) = 0$. An expression containing x^3 can still have degree below 3; the degree belongs to the polynomial, not to the way it is written. So all five lie in $\mathbb{Q}[x]_{\leq 2}$, and exactly -4 and 0 lie in $\mathbb{Q}[x]_{\leq 0}$, the set of constants.

Definition 4.3.4. Polynomials of Degree Exactly n

Let R be a commutative ring and $n \in \mathbb{N}$. The set of **polynomials of degree exactly** n is $R[x]_{=n} \coloneqq \{p \in R[x] : \deg p = n\}$.

The second description also counts these sets over a finite ring. Over $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$, whose elements are $0, 1, 2$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)), $\mathbb{F}_3[x]_{\leq 1}$ consists of the polynomials $a_0 + a_1 x$, and distinct pairs (a_0, a_1) give distinct polynomials, since a_0 and a_1 are the coefficients (Proposition 4.2.1). So it has $3 \cdot 3 = 9$ elements, one for each pair. Those in $\mathbb{F}_3[x]_{=1}$ are the ones with $a_1 \neq 0$: $x, x+1, x+2, 2x, 2x+1, 2x+2$, that is $3 \cdot 2 = 6$ of them. The remaining 3 are the constants $0, 1, 2$.

Example. Comparing the Two Sets

Decide whether each of $x^2 + 1$, $3x - 2$ and 0 lies in $\mathbb{Q}[x]_{\leq 2}$ and in $\mathbb{Q}[x]_{=2}$. Then express $R[x]_{\leq n}$ through $R[x]_{=n}$ and $R[x]_{\leq n-1}$ for $n \geq 1$, and decide whether $\mathbb{Q}[x]_{=2}$ is closed under addition.

Solution. $x^2 + 1$ has degree 2, so it lies in both sets. $3x - 2$ has degree 1: it lies in $\mathbb{Q}[x]_{\leq 2}$ but not in $\mathbb{Q}[x]_{=2}$. The zero polynomial has degree $-\infty$: it lies in $\mathbb{Q}[x]_{\leq 2}$ and not in $\mathbb{Q}[x]_{=2}$.

For $n \geq 1$, a polynomial of degree at most n has degree exactly n or degree at most $n - 1$, and not both, so

$$R[x]_{\leq n} = R[x]_{=n} \cup R[x]_{\leq n-1}, \qquad R[x]_{=n} \cap R[x]_{\leq n-1} = \emptyset.$$

$\mathbb{Q}[x]_{=2}$ is **not** closed under addition: $x^2 + x$ and $-x^2 + 1$ both have degree 2, and their sum $x + 1$ has degree 1. It does not contain 0 either. In the linear-algebra companion, the first of the two sets is a subspace of the space of polynomials and the second is not, for exactly these two reasons.

4.3.7 Exercises

4.3.7.1 A. Check your understanding

Exercise. A1

(a) In the proof of Theorem 4.3.2, where is the hypothesis "R has no zero divisors" used?

(b) Run the proof of Theorem 4.3.2 (a) on $p = 2x + 1$ and $q = 3x^2 + x$, once over $\mathbb{Z}$ and once over $\mathbb{Z}/6\mathbb{Z}$: what is $m + n$, and which element is $(pq)_{m+n}$?

(c) True or false: $\deg(p + q) = \max(\deg p, \deg q)$ for all $p, q \in \mathbb{Q}[x]$. Justify your answer.

(d) Give the idea of the proof of Theorem 4.3.2 in two sentences.

(e) For which $n \geq 2$ is $(\mathbb{Z}/n\mathbb{Z})[x]$ an integral domain?

Solution.

(a) Only in (b), to conclude that $\operatorname{lc}(p)\operatorname{lc}(q) \neq 0$ from $\operatorname{lc}(p) \neq 0$ and $\operatorname{lc}(q) \neq 0$. Part (a), the vanishing above $m + n$ and the value at $m + n$, holds in every commutative ring.

(b) $m = 1$, $n = 2$, $m+n = 3$, and $(pq)_3 = p_1q_2 = 2 \cdot 3$: over $\mathbb{Z}$ this is $6 \neq 0$, so $\deg(pq) = 3$; over $\mathbb{Z}/6\mathbb{Z}$ it is $[6] = [0]$, so $\deg(pq) < 3$ (in fact 2, by the warning after the theorem).

(c) False: $p = x$, $q = -x$ give $p + q = 0$, of degree $-\infty$, while $\max(\deg p, \deg q) = 1$. Equality is only guaranteed when $\deg p \neq \deg q$ (Theorem 4.3.1).

(d) In the k-th coefficient of pq with $k \geq m + n$, every term but p_mq_n has a factor beyond the top of p or of q, hence vanishes. So the product's top is the product of the tops, and the degree formula holds exactly when that one product in R is non-zero.

(e) Exactly for n prime. If n is prime, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain (Example (Which Rings Are Integral Domains)), so $(\mathbb{Z}/n\mathbb{Z})[x]$ is one by Corollary 4.3.3 (a). If n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain (Example (Which Rings Are Integral Domains)), so $(\mathbb{Z}/n\mathbb{Z})[x]$ is not one by Corollary 4.3.3 (c).

4.3.7.2 B. Practice

Exercise. B1: Put the proof in order

Below are eight lines. Six of them, in a suitable order, form a proof of Corollary 4.3.3 (a), "if R is an integral domain and $pq = 0$ in $R[x]$, then $p = 0$ or $q = 0$"; two are distractors. Write an admissible order, say which other orders are admissible, and say why each distractor fails.

(i) R has no zero divisors, so $p_mq_n \neq 0$.

(ii) By contraposition, $pq = 0$ implies $p = 0$ or $q = 0$.

(iii) Let $m := \deg p$ and $n := \deg q$, so $p_m \neq 0$ and $q_n \neq 0$.

(iv) $(pq)_{m+n} = \sum_{i=0}^{m+n} p_iq_{m+n-i}$, and this is non-zero because each of its terms is non-zero.

(v) Hence pq has a non-zero coefficient, so $pq \neq 0$.

(vi) Suppose $p \neq 0$ and $q \neq 0$.

(vii) By Theorem 4.3.2 (a), $(pq)_{m+n} = p_mq_n$.

(viii) $p_mq_n \neq 0$ because R is a commutative ring.

Solution. An admissible order is (vi), (iii), (vii), (i), (v), (ii). Line (vi) must come first: it introduces the assumptions that m and n need (the degree of the zero polynomial is $-\infty$, not a position). Line (iii) must come before (vii) and (i), which use m, n, p_m, q_n. Lines (vii) and (i) do not use each other, so they may come in either order; both must precede (v), which combines them. Line (ii) closes the contrapositive and comes last. So the admissible

orders are exactly

(vi), (iii), (vii), (i), (v), (ii) and
(vi), (iii), (i), (vii), (v), (ii).

Line (iv) fails twice: the terms $p_i q_{m+n-i}$ with $i \neq m$ are 0, not non-zero, and even a sum of non-zero terms can be 0 ($1 + (-1) = 0$). Line (viii) gives a false reason: in the commutative ring $\mathbb{Z}/6\mathbb{Z}$, $[2] \neq [0]$ and $[3] \neq [0]$ but $[2][3] = [0]$. The hypothesis that does the work is "no zero divisors", which is line (i).

Exercise. B2: Units in polynomial rings

(a) Show that for **every** commutative ring R, each unit of R is a unit of $R[x]$: $R^\times \subseteq (R[x])^\times$.

(b) Find the inverse of $1 + [3]x$ in $(\mathbb{Z}/9\mathbb{Z})[x]$.

(c) Show that $1 + [2]x + [2]x^2$ is a unit of $(\mathbb{Z}/4\mathbb{Z})[x]$.

Hint: in (b), what is $[3]^2$ *in* $\mathbb{Z}/9\mathbb{Z}$*?*

Solution.

(a) The second paragraph of the proof of Proposition 4.3.4 uses nothing about R beyond Theorem 4.2.4 (b): if $ab = 1$ in R, then $(ax^0)(bx^0) = (ab)x^0 = 1x^0$, which is the one of $R[x]$.

(b) By the product formula, $(1 + [3]x)(1 - [3]x)$ has coefficients 1, $[3] - [3] = [0]$ and $-[3][3] = -[9] = [0]$, so it equals 1. Since $-[3] = [6]$, the inverse is $1 + [6]x$. (It is unique by Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1.)

(c) Let $p := 1 + [2]x + [2]x^2$, with coefficients $1, [2], [2]$. The coefficients of $p^2 = pp$ are, by the product formula,

$$(p^2)_0 = 1, \qquad (p^2)_1 = [2] + [2] = [4],$$
$$(p^2)_2 = [2] + [4] + [2] = [8], \qquad (p^2)_3 = [4] + [4] = [8],$$

and $(p^2)_4 = [2][2] = [4]$. In $\mathbb{Z}/4\mathbb{Z}$, $[4] = [8] = [0]$, so $p^2 = 1$, and p is a unit, its own inverse. Again $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, and Proposition 4.3.4 does not apply.

Exercise. B3: Counting polynomials over a finite field

Let p be a prime and $n \in \mathbb{N}$. How many elements do $\mathbb{F}_p[x]_{\leq n}$ and $\mathbb{F}_p[x]_{=n}$ have?

Hint: Exercise (B1: Polynomials of bounded length as tuples).

Solution. Since $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has the p elements $0, 1, \ldots, p-1$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)), the non-zero elements $1, \ldots, p-1$ form a set with $p-1$ elements.

At most n. By the description after Definition 4.3.3, $\mathbb{F}_p[x]_{\leq n}$ is the set of polynomials q with $q_k = 0$ for every $k > n$. By Exercise (B1: Polynomials of bounded length as tuples) with

$N = n$, $q \mapsto (q_0, \ldots, q_n)$ is a bijection from this set onto $\mathbb{F}_p^{n+1}$ (for $n = 0$, with $\mathbb{F}_p^1$ read as $\mathbb{F}_p$, as there). A tuple $(a_0, \ldots, a_n)$ is the same as the function $\{1, \ldots, n+1\} \to \mathbb{F}_p$, $i \mapsto a_{i-1}$, so by Sets, Relations, and Cardinality, Exercise (C2: Counting products and functions) (b) there are p^{n+1} of them. So $\mathbb{F}_p[x]_{\leq n}$ has p^{n+1} elements.

Exactly n. The same bijection maps $\mathbb{F}_p[x]_{=n}$ onto the tuples $(a_0, \ldots, a_n)$ with $a_n \neq 0$: such a tuple is a pair of an arbitrary $(a_0, \ldots, a_{n-1})$, p^n choices as before, and a non-zero a_n, $p-1$ choices. By Sets, Relations, and Cardinality, Exercise (C2: Counting products and functions) (a), there are $(p-1)p^n$ of them. (For $n = 0$ these are the $p-1$ non-zero constants, and $(p-1)p^0 = p-1$.) For example, over $\mathbb{F}_2$ there are $2^3 = 8$ polynomials of degree at most 2 and $1 \cdot 2^2 = 4$ of degree exactly 2.

4.3.7.3 C. Going deeper

Exercise. C1: Exit check: polynomial rings over integral domains

Let R be a commutative ring. Prove Theorem 4.3.2 (a) and (b) (for (b), the equivalence, the leading coefficient, and the case of no zero divisors), and then prove Corollary 4.3.3 (a) and (c).

Solution. Degree of a product. Let $p, q \neq 0$, $m = \deg p$, $n = \deg q$, so $p_m \neq 0$, $q_n \neq 0$, and $p_i = 0$ for $i > m$, $q_j = 0$ for $j > n$. Let $k \geq m + n$ and $0 \leq i \leq k$. If $i > m$, then $p_i = 0$. If $i \leq m$, then $k - i \geq n$, with equality only when $k = m+n$ and $i = m$; otherwise $q_{k-i} = 0$. So for $k > m + n$ every term $p_i q_{k-i}$ of $(pq)_k$ is 0 (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) with (F6)), and $(pq)_k = 0$; for $k = m + n$, every term with $i \neq m$ is 0, and the sum is $p_m q_n$ by (Σ3) of Lemma 4.1.1. Hence $\deg(pq) \leq m + n$ when $pq \neq 0$, and trivially when $pq = 0$; if $p = 0$ or $q = 0$, then $pq = 0$ and both sides are $-\infty$.

If $p_m q_n \neq 0$, then pq has a non-zero coefficient at $m+n$ and none beyond, so $\deg(pq) = m+n$ and $\operatorname{lc}(pq) = p_m q_n$. If $p_m q_n = 0$, all coefficients from $m + n$ on vanish, and $\deg(pq) < m + n$.

No zero divisors. Let R be an integral domain and $p, q \neq 0$. Then $p_m q_n \neq 0$, since R has no zero divisors, so pq has a non-zero coefficient and $pq \neq 0$. Contraposition gives (a); with $R[x]$ a commutative ring (Theorem 4.2.4 (a)) and $1x^0 \neq 0x^0$ because $1 \neq 0$ in R, $R[x]$ is an integral domain.

The converse. Let $R[x]$ be an integral domain. If $1 = 0$ in R, the one $1x^0$ of $R[x]$ is the zero polynomial, a contradiction. If $ab = 0$ in R, then $(ax^0)(bx^0) = (ab)x^0 = 0$ (Lemma 4.2.2 (b)), so one factor is the zero polynomial, and its only possibly non-zero coefficient, a or b, is 0.

Marking scheme. (10 points)

- 3: shows that every coefficient of pq above $m + n$ vanishes, treating both cases $i > m$ and $i \leq m$ of the index argument, and the case $p = 0$ or $q = 0$ of the inequality.
- 2: shows that $(pq)_{m+n} = \operatorname{lc}(p) \operatorname{lc}(q)$, with the other terms of that coefficient shown to be 0.
- 1: derives $\deg(pq) = \deg p + \deg q$ and $\operatorname{lc}(pq) = \operatorname{lc}(p) \operatorname{lc}(q)$ from $\operatorname{lc}(p) \operatorname{lc}(q) \neq 0$, and that this holds when R has no zero divisors.
- 1: shows the converse direction of the equivalence: $\operatorname{lc}(p) \operatorname{lc}(q) = 0$ gives $\deg(pq) < m+n$.
- 2: concludes that $R[x]$ has no zero divisors and $1 \neq 0$ in $R[x]$.
- 1: proves the converse through the constants.

Fatal errors (0 for the step): "the leading term of pq is $\mathrm{lc}(p)\,\mathrm{lc}(q)x^{m+n}$" without showing that the other terms of the $(m+n)$-th coefficient vanish; using $\deg(pq) = \deg p + \deg q$ in an arbitrary commutative ring. A proof through the **lowest** non-zero coefficients (as in the repair of Exercise (C2: Find the error)) earns the same points for (a) of the corollary, with the index argument mirrored.

Exercise. C2: Find the error

Here is an argument.

> **Claim.** If R is an integral domain, then $R[x]$ has no zero divisors.
>
> **Proof.** Let $p, q \in R[x]$ be non-zero. (1) Then $p_0 \neq 0$ and $q_0 \neq 0$. (2) The constant term of pq is $(pq)_0 = p_0 q_0$. (3) Since R has no zero divisors, $p_0 q_0 \neq 0$. (4) So $pq \neq 0$.

Is the claim true? Does the argument prove it? If not, name the first line that fails, say why, give a counterexample to that step, and repair the proof.

Solution. The claim is true: it is Corollary 4.3.3 (a). The argument does not prove it.

The failing line is (1). A non-zero polynomial may have constant term 0: $p = x$ is non-zero, with $p_0 = 0$. That is a counterexample to the step from "$p \neq 0$" to "$p_0 \neq 0$". The step generalizes from the constants, where it is true, to all polynomials, where no result supports it: it cites a general "fact" that is neither proved nor true, entry (N9) of Logic and Proof, Example (What is not allowed). Lines (2), (3) and (4) are correct: (2) is the product formula at $k = 0$, and (3), (4) follow once (1) is granted.

Two repairs. The book's repair looks at the **top** coefficients: with $m = \deg p$, $n = \deg q$, Theorem 4.3.2 (a) gives $(pq)_{m+n} = p_m q_n \neq 0$.

The argument can also be repaired at the **bottom**. Let i_0 and j_0 be the least indices with $p_{i_0} \neq 0$ and $q_{j_0} \neq 0$; they exist because the sets of non-zero positions are non-empty subsets of $\mathbb{N}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6, bounded below by 0). In $(pq)_{i_0+j_0} = \sum_{i=0}^{i_0+j_0} p_i q_{i_0+j_0-i}$, a term with $i < i_0$ has $p_i = 0$, and a term with $i > i_0$ has $i_0 + j_0 - i < j_0$, so $q_{i_0+j_0-i} = 0$. By (Σ3), $(pq)_{i_0+j_0} = p_{i_0} q_{j_0}$, which is non-zero since R has no zero divisors. So $pq \neq 0$. This is the index argument of Theorem 4.3.2, mirrored.

4.4 Evaluation, Substitution, and Polynomial Functions

A polynomial, in this chapter, is a sequence of coefficients (Definition 4.1.1), not a function. But every polynomial **defines** a function: put an element c of the ring in place of x and add up. More generally we can put in place of x a class modulo n, or another polynomial, after first moving the coefficients into the ring where the substitution happens. This section proves one theorem, the substitution principle, that covers all of these at once, because each is a ring homomorphism out of $R[x]$ determined by where it sends the constants and x. Then it compares a polynomial with its function, and shows that over every finite ring other than the zero ring

the passage from polynomials to functions loses information.

Throughout, R and S are commutative rings (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1), and powers s^n and finite sums are those of Lemma 4.1.1.

4.4.1 Evaluating a polynomial

To evaluate a polynomial at c, replace each monomial ax^k by the element ac^k and add.

Definition 4.4.1. Evaluation, Root, Polynomial Function

Let R be a commutative ring, $p \in R[x]$ and $c \in R$. The **value** of p at c is

$$p(c) := \sum_{k=0}^{N} p_k c^k \in R,$$

for **any** $N \in \mathbb{N}$ with $p_k = 0$ for every $k > N$. The element c is a **root** of p if $p(c) = 0$. The **polynomial function** of p is the function $R \to R$, $c \mapsto p(c)$.

In words: the value is the finite sum of the coefficients times the powers of c, with $c^0 = 1$, so the constant coefficient enters as itself. The sum runs far enough to include every non-zero coefficient, and how far beyond that is our choice. Only finitely many coefficients are non-zero, and this is what makes the sum finite; a sequence such as $(1, 1, 1, \dots)$ would ask for an infinite sum, which a ring does not provide.

Well-definedness. The definition allows many N, and they all give the same element: enlarging N only adds terms $0 \cdot c^k = 0$. The fold below writes this out.

Second reading · *Why the value does not depend on the bound*

Let N be admissible for p. We show by Logic and Proof, Axiom 4.2.1 on j (through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) that $\sum_{k=0}^{N+j} p_k c^k = \sum_{k=0}^{N} p_k c^k$. The case $j = 0$ is trivial, and the sum recursion of Lemma 4.1.1 (a) gives

$$\begin{aligned} \sum_{k=0}^{N+j+1} p_k c^k &= \sum_{k=0}^{N+j} p_k c^k + p_{N+j+1} c^{N+j+1} \\ &= \sum_{k=0}^{N+j} p_k c^k + 0, \end{aligned}$$

since $p_{N+j+1} = 0$ and $0 \cdot c^{N+j+1} = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) with (F6)); then (F3) and the hypothesis finish. Any two admissible N and N' differ in this way, the larger being the smaller plus some $j \in \mathbb{N}$. So $p(c)$ depends only on p and c.

Examples.

- In $\mathbb{Q}[x]$, let $p = x^2 - 3x + 2$, with coefficients $2, -3, 1$. Then $p(0) = 2$, $p(1) = 1 - 3 + 2 = 0$ and $p(2) = 4 - 6 + 2 = 0$: 1 and 2 are roots.

- In $\mathbb{F}_3[x]$, let $p = x^3 + 2$. Its values at $0, 1, 2$ are 2, $1 + 2 = 3 = 0$ and $8 + 2 = 10 = 1$ (in $\mathbb{F}_3$). Its only root in $\mathbb{F}_3$ is 1.
- **A monomial.** For ax^m, take $N = m$: every term with $k \neq m$ is $0 \cdot c^k = 0$, so (Σ3) of Lemma 4.1.1 gives $(ax^m)(c) = ac^m$. In particular a constant $a = ax^0$ has value $ac^0 = a \cdot 1 = a$ at every c, and $x = 1x^1$ has value $1 \cdot c^1 = c$.

Warning. $p(2)$ **is a value;** p_2 **is a coefficient.** For $p = x^2 - 3x + 2 \in \mathbb{Z}[x]$, $p_2 = 1$ but $p(2) = 0$. At 0 the two always agree, $p(0) = p_0$, because $0^k = 0$ for $k \geq 1$; at any other position they differ in general. Over $\mathbb{Z}$ both are integers, which is why this book never writes $p(k)$ for a coefficient.

4.4.2 Evaluation respects the operations

At school, "substitute $x = c$" is done after or before multiplying out, with the same answer. In our setting that is a theorem: evaluation at c turns sums and products of polynomials into sums and products in R.

Theorem 4.4.1. Evaluation Respects the Operations

Let R be a commutative ring, $p, q \in R[x]$ and $c \in R$. Then

$$(p + q)(c) = p(c) + q(c), \qquad (pq)(c) = p(c)\, q(c),$$

and $a(c) = a$ for every constant a, and $x(c) = c$.

Idea. Sums are coefficientwise, and the sum rule (Σ1) splits the defining sum. For products, the move is **check on monomials, extend by additivity** (Lemma 4.2.3): both sides are additive in p and in q, and on monomials the product rule is the power law $c^{m+n} = c^m c^n$ together with one reordering of factors in R.

Proof. Sums. Let N be admissible for both p and q (the larger of an admissible N for each). Then N is admissible for $p + q$, and

$$\begin{aligned}(p + q)(c) &= \sum_{k=0}^{N} (p_k + q_k)c^k \\ &= \sum_{k=0}^{N} (p_k c^k + q_k c^k) = p(c) + q(c),\end{aligned}$$

by Definition 4.2.1, then (F6) and (F9) in each term, then (Σ1) of Lemma 4.1.1.

Constants and x. These are the monomial example after Definition 4.4.1: $a(c) = ac^0 = a$ and $x(c) = 1 \cdot c^1 = c$.

Products. Define $\Phi, \Psi \colon R[x] \times R[x] \to R$ by $\Phi(p, q) := (pq)(c)$ and $\Psi(p, q) := p(c)\, q(c)$. Both are additive in each argument. For Φ in the first argument,

$$\Phi(p + p', q) = (pq + p'q)(c) = (pq)(c) + (p'q)(c) = \Phi(p, q) + \Phi(p', q),$$

by the distributive law of the ring $R[x]$ (Theorem 4.2.4 (a)) and the sum rule just proved. For Ψ, $(p(c)+p'(c))q(c) = p(c)q(c)+p'(c)q(c)$ by the sum rule, (F6) and (F9). The second argument is the same with $p(q+q') = pq+pq'$.

On monomials ax^m and bx^n, Lemma 4.2.2 (b) gives $(ax^m)(bx^n) = (ab)x^{m+n}$, so

$$\Phi(ax^m, bx^n) = (ab)c^{m+n} = (ab)(c^m c^n) = (ac^m)(bc^n) = \Psi(ax^m, bx^n),$$

by the value of a monomial, the power law $c^{m+n} = c^m c^n$ (Lemma 4.1.1 (c)), and (F5) and (F6) to move b past c^m. By Lemma 4.2.3 with two arguments and $T = R$, $\Phi = \Psi$. This proves the theorem.

■

Remark. The monomial line moves the coefficient b past the power c^m; that is the one step that needs two elements of R to commute. Elsewhere (F6) is used only to get the mirror forms of (F7), (F9) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), namely $1\cdot c = c$, $(a+b)c = ac+bc$ and $0\cdot c = 0$. The same proof works for substituting a square matrix into a polynomial with coefficients in a field, as in the linear-algebra companion, Chapter 0, because there the mirror laws hold for matrices too, b is a scalar, and scalars commute with every matrix; two matrices need not commute, and nothing in the proof asks them to.

Two consequences are used constantly. First, a root of a factor is a root of the product: if $q(c) = 0$, then $(pq)(c) = p(c)\cdot 0 = 0$. Second, if R has no zero divisors, the converse holds: $(pq)(c) = p(c)q(c) = 0$ forces $p(c) = 0$ or $q(c) = 0$. This is the school method for solving $(x-1)(x-2) = 0$. In $\mathbb{Q}[x]$, $(x-1)(x-2) = x^2-3x+2$ by the product formula, so, since $\mathbb{Q}$ is an integral domain (Example (Which Rings Are Integral Domains)) and $(x-a)(c) = c-a$ by the sum rule and the value of a constant, the roots of x^2-3x+2 in $\mathbb{Q}$ are exactly the c with $c-1 = 0$ or $c-2 = 0$: the numbers 1 and 2 found above, and no others.

4.4.3 Ring homomorphisms

Evaluation at c is a map $R[x] \to R$ that respects $+$, $\cdot$ and 1. The quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ of Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (c) does the same, and so does the map of the Chinese remainder theorem. Maps of this kind recur in every chapter from here on.

A ring homomorphism is a map between rings that turns sums into sums, products into products, and the one into the one.

Definition 4.4.2. Ring Homomorphism

Let R and S be commutative rings. A **ring homomorphism** $\varphi\colon R \to S$ is a function such that, **for all** $a, b \in R$,

$$\varphi(a+b) = \varphi(a)+\varphi(b), \qquad \varphi(ab) = \varphi(a)\varphi(b),$$

and $\varphi(1) = 1$.

In words: computing in R and then applying φ gives the same result as applying φ and then computing in S. The sum and product on the left are those of R, on the right those of S. The

condition on 1 is not a consequence of the other two, as the zero map below shows.

Between two fields this is exactly a homomorphism of fields (Definition 2.4.1). The consequences below are the ring versions of Proposition 2.4.1 (a), the composites in (e) and the powers in (f), with the same proofs. Parts (b)–(d) of that proposition do not carry over: the quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ of Example (Ring Homomorphisms and Two Impostors) (i) is not injective.

Consequences. Let $\varphi\colon R \to S$ be a ring homomorphism.

- $\varphi(0) = 0$. Let $z \coloneqq \varphi(0)$. Then $z+z = \varphi(0+0) = z$, by (F3) in R. Adding $-z$ to both sides and using (F2), (F4) and (F3) in S gives $z = 0$. (This is cancellation, not the uniqueness of 0 in Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a): uniqueness concerns an element that is neutral for **every** element, and we only know $z + z = z$.)
- $\varphi(-a) = -\varphi(a)$: $\varphi(a) + \varphi(-a) = \varphi(a + (-a)) = \varphi(0) = 0$, and negatives are unique (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a)). Hence also $\varphi(a-b) = \varphi(a) - \varphi(b)$.
- $\varphi(s^n) = \varphi(s)^n$ for $s \in R$ and $n \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1 on n: $\varphi(s^0) = \varphi(1) = 1 = \varphi(s)^0$, and $\varphi(s^{n+1}) = \varphi(s^n s) = \varphi(s)^n\varphi(s) = \varphi(s)^{n+1}$.
- If $\psi\colon S \to T$ is another ring homomorphism, then so is $\psi \circ \varphi\colon R \to T$: $\psi(\varphi(a + b)) = \psi(\varphi(a) + \varphi(b)) = \psi(\varphi(a)) + \psi(\varphi(b))$, the same for products, and $\psi(\varphi(1)) = \psi(1) = 1$.

Example. Ring Homomorphisms and Two Impostors

Which of the following are ring homomorphisms? (i) The quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto [a]$, for $n \in \mathbb{Z}_{>0}$. (ii) The constants $R \to R[x]$, $a \mapsto ax^0$. (iii) The map $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $[a]_{mn} \mapsto ([a]_m, [a]_n)$, for coprime $m, n \in \mathbb{Z}_{>0}$. (iv) $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto 2a$. (v) The zero map $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto 0$.

Solution.

(i) Yes, by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (c) with the ideal $n\mathbb{Z}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.2); more generally, the quotient map $R \to R/I$ is one for every ideal I.

(ii) Yes, by Theorem 4.2.4 (b).

(iii) Yes, by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3 (b), where the target carries componentwise operations; it is a commutative ring because each axiom holds in each component, and its one is $([1]_m, [1]_n)$.

(iv) No. It is additive, $2(a + b) = 2a + 2b$, but not multiplicative: $2(1 \cdot 1) = 2$, while $(2 \cdot 1)(2 \cdot 1) = 4$. It also sends 1 to 2.

(v) No. It is additive and multiplicative ($0 = 0 + 0 = 0 \cdot 0$), but it sends 1 to $0 \neq 1$.

Complex conjugation $z \mapsto \overline{z}$ on $\mathbb{C}$, whose rules are proved in Chapter 1, is another example; we use it only in a review exercise of the next section.

4.4.4 The substitution principle

Evaluation puts an element of R in place of x. Reduction modulo n changes the coefficients from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ and keeps x. Composition puts a polynomial in place of x. The next theorem does all three: it moves the coefficients along a ring homomorphism φ and puts an element s in place of x, and it says that there is exactly one way to do so that respects the operations.

Theorem 4.4.2. Substitution Principle

Let R and S be commutative rings, $\varphi\colon R \to S$ a ring homomorphism, and $s \in S$. Define $\Phi\colon R[x] \to S$ by

$$\Phi(p) := \sum_{k=0}^{N} \varphi(p_k)\, s^k,$$

for any N admissible for p.

(a) Φ is well defined, and it is a ring homomorphism with $\Phi(a) = \varphi(a)$ for every constant $a \in R$ and $\Phi(x) = s$.

(b) Φ is the **only** ring homomorphism $R[x] \to S$ with these two properties.

In words: (a) says that substituting s for x, after moving each coefficient to S by φ, respects sums, products and 1; (b) says that a ring homomorphism out of $R[x]$ is pinned down by what it does to the constants and to x.

Try it first (ten minutes): take $R = \mathbb{Z}$, $S = \mathbb{Z}/5\mathbb{Z}$, φ the quotient map, and $s = [2]$. Which value must a ring homomorphism Φ with $\Phi(a) = [a]$ for constants and $\Phi(x) = [2]$ give to $3x^2 + 1$? Why is there no choice?

Idea. The attempt finds the value at once: $3x^2+1$ is the constant 3 times x times x, plus the constant 1 (Theorem 4.2.4 (c)), so a homomorphism must send it to $[3][2][2]+[1] = [13] = [3]$. The same reasoning applies to every polynomial: a homomorphism has no freedom, because it must send ax^n to $\varphi(a)s^n$, and then the sum of the monomials to the sum of their images. That proves (b) and shows that the formula for Φ is forced. The only work is (a), showing that the forced formula respects products, and that is again a check on monomials, with the coefficients now computed in S.

Before reading on: where is S commutative used, and where $\varphi(1) = 1$?

Proof. (a) Well defined. If N is admissible, then so is $N + j$, and each added term is $\varphi(0)s^k = 0 \cdot s^k = 0$, by $\varphi(0) = 0$ (after Definition 4.4.2) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) with (F6); as for Definition 4.4.1, the value does not depend on N. Taking $N = m$ for a monomial, (Σ3) of Lemma 4.1.1 gives

$$\Phi(ax^m) = \varphi(a)\, s^m.$$

Additive. Let N be admissible for p and q. Then

$$\begin{aligned}\Phi(p+q) &= \sum_{k=0}^{N} \varphi(p_k + q_k)s^k \\ &= \sum_{k=0}^{N} (\varphi(p_k)s^k + \varphi(q_k)s^k) = \Phi(p) + \Phi(q),\end{aligned}$$

by additivity of φ, (F6) and (F9) in S, and (Σ1).

Multiplicative. The maps $(p, q) \mapsto \Phi(pq)$ and $(p, q) \mapsto \Phi(p)\Phi(q)$, from $R[x] \times R[x]$ to S, are additive in each argument: the first by the distributive laws of $R[x]$ (Theorem 4.2.4 (a))

and additivity of Φ, the second by additivity of Φ and (F9), (F6) in S. On monomials, by Lemma 4.2.2 (b), multiplicativity of φ, the power law of Lemma 4.1.1 (c), and (F5), (F6) **in** S,

$$\begin{aligned}\Phi\big((ax^m)(bx^n)\big) &= \Phi\big((ab)x^{m+n}\big) = \varphi(ab)\, s^{m+n} \\ &= \varphi(a)\varphi(b)\, s^m s^n = \big(\varphi(a)s^m\big)\big(\varphi(b)s^n\big) \\ &= \Phi(ax^m)\,\Phi(bx^n).\end{aligned}$$

By Lemma 4.2.3 with two arguments and $T = S$, $\Phi(pq) = \Phi(p)\Phi(q)$ for all p, q.

The one, the constants, x. $\Phi(1) = \Phi(1x^0) = \varphi(1)s^0 = 1 \cdot 1 = 1$. For a constant, $\Phi(ax^0) = \varphi(a)s^0 = \varphi(a)$. And $\Phi(x) = \Phi(1x^1) = \varphi(1)s^1 = s$. So Φ is a ring homomorphism with the two properties.

(b) Let $\Psi\colon R[x] \to S$ be a ring homomorphism with $\Psi(ax^0) = \varphi(a)$ for every $a \in R$ and $\Psi(x) = s$. By Theorem 4.2.4 (c), the monomial ax^n is the product of the constant a and the n-th power of x, so

$$\Psi(ax^n) = \Psi(ax^0)\,\Psi(x)^n = \varphi(a)\, s^n = \Phi(ax^n),$$

by multiplicativity and the power property of ring homomorphisms (after Definition 4.4.2). Both Ψ and Φ are additive maps $R[x] \to S$ that agree on monomials, so $\Psi = \Phi$ by Lemma 4.2.3 with one argument. This proves the theorem.

■

The answer to the prompt. Commutativity of S does real work in one place, the middle line of the monomial computation, where it moves $\varphi(b)$ past s^m. Its other uses ($0 \cdot s^k = 0$, the right distributive law $(u+v)w = uw + vw$ in the additivity steps, and $1 \cdot s = s$) only supply the mirror forms of Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b), (F9) and (F7), which a two-sided list of ring axioms gives directly. The condition $\varphi(1) = 1$ is used twice, for $\Phi(1) = 1$ and for $\Phi(x) = s$. If S is not commutative but satisfies those two-sided laws, the same proof goes through provided s commutes with every $\varphi(b)$, since that is all the monomial line asks; this is the case of a square matrix and scalar coefficients, from the remark after Theorem 4.4.1.

Remark. With $S = R$, $\varphi = \mathrm{id}_R$ and $s = c$, the map Φ is $p \mapsto p(c)$, and part (a) contains Theorem 4.4.1. We proved evaluation first because it is the case used most, and its proof is the substitution proof with φ invisible.

We call the move of (b) **a homomorphism out of $R[x]$ is fixed by the constants and x**: to show that two ring homomorphisms out of $R[x]$ agree, check that they agree on constants and on x.

4.4.5 Changing coefficients and composing

Two special cases of the substitution principle get names: the change of coefficients, which the algebra volumes of the series use for reduction modulo a prime, and composition, which Section 4.5 uses.

The first moves the coefficients and keeps x: take the target $S[x]$, the homomorphism "φ, then a constant of $S[x]$", and $s = x$.

Corollary 4.4.3. Changing the Coefficient Ring

Let $\varphi\colon R \to S$ be a ring homomorphism. For $p \in R[x]$, let $\varphi_*(p)$ be the sequence with $(\varphi_*(p))_k \coloneqq \varphi(p_k)$. Then $\varphi_*(p) \in S[x]$, and $\varphi_*\colon R[x] \to S[x]$ is a ring homomorphism with $\varphi_*(ax^n) = \varphi(a)x^n$. Moreover $\deg \varphi_*(p) \leq \deg p$ for every p, and for $p \neq 0$, equality holds **if and only if** $\varphi(\mathrm{lc}(p)) \neq 0$.

Idea. Substitute x for x, after moving each coefficient to S: the substitution principle then hands us a ring homomorphism, and its formula is the coefficientwise image. The degree can only drop, and it drops exactly when the leading coefficient is sent to 0.

Proof. If $p_k = 0$ for $k > N$, then $\varphi(p_k) = \varphi(0) = 0$ for $k > N$, so $\varphi_*(p)$ is a polynomial over S. Let $\gamma\colon R \to S[x]$, $\gamma(a) \coloneqq \varphi(a)x^0$: the composite of φ and the constants of $S[x]$, a ring homomorphism (Example (Ring Homomorphisms and Two Impostors) (ii) and the composite rule after Definition 4.4.2). Theorem 4.4.2 with target $S[x]$, γ and $s = x$ gives a ring homomorphism $\Phi\colon R[x] \to S[x]$ with

$$\begin{aligned}\Phi(p) &= \sum_{k=0}^{N} (\varphi(p_k)x^0)x^k \\ &= \sum_{k=0}^{N} \varphi(p_k)x^k = \varphi_*(p),\end{aligned}$$

where the middle equality is Theorem 4.2.4 (c) in $S[x]$, and the last is Proposition 4.2.1 applied to $\varphi_*(p) \in S[x]$. So $\varphi_* = \Phi$ is a ring homomorphism, and $\varphi_*(ax^n) = \varphi(a)x^n$ by definition.

For the degree: if $p = 0$, then $\varphi_*(p) = 0$. Otherwise let $d \coloneqq \deg p$. For $k > d$, $\varphi(p_k) = \varphi(0) = 0$, so $\deg \varphi_*(p) \leq d$; and the coefficient of $\varphi_*(p)$ at d is $\varphi(\mathrm{lc}(p))$, so the degree is exactly d if and only if this element is non-zero.

■

The main example is **reduction modulo** n: the quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ gives $\mathbb{Z}[x] \to (\mathbb{Z}/n\mathbb{Z})[x]$, which reads every coefficient modulo n and respects sums and products. For $n = 2$,

$$2x^2 + 3x - 1 \longmapsto 0x^2 + 1x + 1 = x + 1 \in \mathbb{F}_2[x],$$

since $2 = 0$, $3 = 1$ and $-1 = 1$ in $\mathbb{F}_2$: the degree drops from 2 to 1, because the leading coefficient 2 reduces to 0. The opening computation of Section 4.3 is another instance: modulo 6, $6x^3 + 5x^2 + x$ reduces to $[5]x^2 + x$, of lower degree because its leading coefficient 6 reduces to $[0]$. The algebra volumes of the series test integer polynomials for factorization by reducing them modulo a prime in exactly this way.

The second special case substitutes a polynomial for x: take $S = R[x]$, φ the constants (Example (Ring Homomorphisms and Two Impostors) (ii)) and $s = q$.

Definition 4.4.3. Composition of Polynomials

Let R be a commutative ring and $p, q \in R[x]$. The **composition** $p \circ q \in R[x]$ is $\Phi(p)$ for the

homomorphism Φ of Theorem 4.4.2 with $S = R[x]$, $\varphi\colon a \mapsto ax^0$ and $s = q$:

$$p \circ q = \sum_{k=0}^{N} p_k\, q^k \qquad (N \text{ admissible for } p).$$

By Theorem 4.4.2 (a), $p \mapsto p \circ q$ is a ring homomorphism $R[x] \to R[x]$ that fixes every constant, $a \circ q = a$, and sends x to $x \circ q = q$. Substituting x itself changes nothing: $p \circ x = \sum_k p_k x^k = p$, by Theorem 4.2.4 (c) and Proposition 4.2.1. For example, in $\mathbb{Z}[x]$,

$$(x^2 + 1) \circ (x + 1) = (x + 1)^2 + 1 = x^2 + 2x + 2,$$

where $(x + 1)^2 = x^2 + 2x + 1$ by the product formula. The polynomial $p(-x) \coloneqq p \circ (-x)$ has coefficients $(-1)^k p_k$, since $(-x)^k = (-1)^k x^k$: it is the sign-change map σ of Exercise (B2: Changing the sign of x), which the substitution principle shows once more to be multiplicative.

Quick check. In $(\mathbb{Z}/8\mathbb{Z})[x]$, evaluate $x^2 - 1$ at $[3]$. Which ring homomorphism of Theorem 4.4.2 is "evaluate at $[3]$"?

Solution. $[3]^2 - [1] = [9 - 1] = [8] = [0]$, so $[3]$ is a root. Evaluation at $[3]$ is the Φ of Theorem 4.4.2 with $R = S = \mathbb{Z}/8\mathbb{Z}$, $\varphi = \mathrm{id}_{\mathbb{Z}/8\mathbb{Z}}$ and $s = [3]$.

4.4.6 Polynomials and polynomial functions

Every polynomial $p \in R[x]$ has a polynomial function $R \to R$. The functions $R \to R$ form a ring of their own, and passing from a polynomial to its function respects the operations. The question is whether anything is lost on the way.

Proposition 4.4.4. Polynomials and Their Functions

Let R be a commutative ring.

(a) The set R^R of functions $R \to R$ (Sets, Relations, and Cardinality, Definition 1.4.1), with the pointwise operations $(f + g)(c) \coloneqq f(c) + g(c)$ and $(fg)(c) \coloneqq f(c)g(c)$, is a commutative ring, whose zero and one are the constant functions with values 0 and 1.

(b) The map $\varepsilon\colon R[x] \to R^R$, $\varepsilon(p) \coloneqq (c \mapsto p(c))$, is a ring homomorphism.

(c) For all $p, q \in R[x]$ and $c \in R$, $(p \circ q)(c) = p(q(c))$: composition of polynomials matches composition of their functions.

(d) If R is **finite** with $1 \neq 0$, then ε is **not** injective. Explicitly, if $c_1, \ldots, c_r$ lists the elements of R without repetition, then

$$P \coloneqq \prod_{j=1}^{r} (x - c_j)$$

is monic of degree r, so $P \neq 0$, yet $P(c) = 0$ for every $c \in R$.

Idea. Parts (a) and (b) are bookkeeping: every ring law holds value by value, and evaluation respects the operations value by value. Part (c) compares two ring homomorphisms $R[x] \to R$ and uses the move just named: they agree on constants and on x. Part (d) builds a polynomial with a factor vanishing at each element of R, and the degree, computed by multiplying monic factors, shows it is not the zero polynomial.

Proof. *(a)* The two rules define functions $R \to R$, so $+$ and $\cdot$ are operations on R^R. Each of (F1)–(F7) and (F9) is an equation between functions with domain and codomain R, so by Sets, Relations, and Cardinality, Proposition 1.4.1 it suffices that the two sides agree at every $c \in R$, and there it is the same law in R: for example $(f(g+h))(c) = f(c)(g(c)+h(c)) = f(c)g(c) + f(c)h(c) = (fg+fh)(c)$. The zero is the constant function 0 by (F3) in R, the negative of f is $c \mapsto -f(c)$ by (F4), and the one is the constant function 1 by (F7).

(b) For $p, q \in R[x]$ and $c \in R$, Theorem 4.4.1 gives $\varepsilon(p+q)(c) = p(c) + q(c) = (\varepsilon(p) + \varepsilon(q))(c)$ and likewise for products; and $\varepsilon(1)(c) = 1$. By Sets, Relations, and Cardinality, Proposition 1.4.1, $\varepsilon(p+q) = \varepsilon(p) + \varepsilon(q)$, $\varepsilon(pq) = \varepsilon(p)\varepsilon(q)$, and $\varepsilon(1)$ is the one of R^R.

(c) Fix q and c, and consider $\alpha, \beta\colon R[x] \to R$, $\alpha(p) \coloneqq (p \circ q)(c)$, $\beta(p) \coloneqq p(q(c))$. The map α is the composite of $p \mapsto p \circ q$ (a ring homomorphism, after Definition 4.4.3) and evaluation at c (a ring homomorphism, Theorem 4.4.1), so it is one; β is evaluation at $q(c)$, a ring homomorphism. On a constant a, $\alpha(a) = a(c) = a$ and $\beta(a) = a$. On x, $\alpha(x) = q(c)$ and $\beta(x) = x(q(c)) = q(c)$. By the uniqueness in Theorem 4.4.2 (b), with $S = R$, $\varphi = \mathrm{id}_R$ and $s = q(c)$, $\alpha = \beta$.

(d) Since R is finite, there is a bijection $j \mapsto c_j$ from $\{1, \dots, r\}$ to R (Sets, Relations, and Cardinality, Definition 3.1.2), and $r \geq 1$ because R contains 0. The product P is the product of a finite list in the commutative ring $R[x]$ (Lemma 4.1.1 (a)). Write $P_j \coloneqq \prod_{i=1}^{j}(x - c_i)$, so $P_0 = 1$ and $P_{j+1} = P_j\,(x - c_{j+1})$. We show by induction on $j \leq r$ that P_j is monic of degree j. The base: $P_0 = 1$ is monic of degree 0, as $1 \neq 0$. The step: $x - c_{j+1}$ has coefficients $-c_{j+1}, 1, 0, \dots$, so it is monic of degree 1; by Theorem 4.3.2 (b) in its monic case, P_{j+1} has degree $j+1$ and leading coefficient $1 \cdot 1 = 1$. So $P = P_r$ has degree $r \in \mathbb{N}$, and $P \neq 0$.

Now let $c \in R$; then $c = c_l$ for some l, by surjectivity. By Theorem 4.4.1, $P_{j+1}(c) = P_j(c)\,(c - c_{j+1})$, using $(x - c_{j+1})(c) = c - c_{j+1}$ (the sum rule, with $(-a)(c) = -a$ for a constant). At $j + 1 = l$ the second factor is $c_l - c_l = 0$, so $P_l(c) = 0$, and each later step multiplies 0 by an element, so $P_r(c) = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) with (F6)). Hence $\varepsilon(P) = \varepsilon(0)$ with $P \neq 0$, and ε is not injective.

■

The smallest instance is the one this chapter opened with.

Example. Different Polynomials, Equal Functions

Over $\mathbb{F}_2$, compare $x^2 + x$ with 0, and x^2 with x, first as polynomials, then as functions $\mathbb{F}_2 \to \mathbb{F}_2$.

Solution. *As polynomials.* $x^2 + x$ has coefficient $1 \neq 0$ in position 1, so it is not the zero polynomial; it has degree 2. And $x^2 \neq x$, since their coefficients differ in position 2 (and in

position 1).

As functions. At 0: $0^2 + 0 = 0$ and $0^2 = 0$. At 1: $1^2 + 1 = 1 + 1 = 0$ in $\mathbb{F}_2$ (Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$)), and $1^2 = 1$. So the function of $x^2 + x$ is the zero function, and x^2 and x have the same function, the identity of $\mathbb{F}_2$.

This is Proposition 4.4.4 (d) with $R = \mathbb{F}_2$, $c_1 = 0$, $c_2 = 1$: $P = (x - 0)(x - 1) = x(x + 1) = x^2 + x$, since $-1 = 1$ in $\mathbb{F}_2$.

Warning. **A polynomial is not its function.** "$p(c) = 0$ for every $c \in R$" does not give $p = 0$: over every finite ring with $1 \neq 0$ the polynomial P of Proposition 4.4.4 (d) is a counterexample, and over $\mathbb{F}_2$ it is $x^2 + x$. Over $\mathbb{Q}$ the implication does hold: Chapter 5 proves it for every infinite field, by bounding the number of roots of a non-zero polynomial. Over $\mathbb{Z}$ it follows, though we do not prove it here: read $p \in \mathbb{Z}[x]$ as a polynomial with the same coefficients in $\mathbb{Q}[x]$, where it vanishes at infinitely many points. In this chapter, two polynomials are equal only when their coefficients are equal.

4.4.7 Exercises

4.4.7.1 A. Check your understanding

Exercise. A1

These questions are about Theorem 4.4.2 and its proof, except the last.

(a) Where in the proof is $\varphi(1) = 1$ used?

(b) Where is the commutativity of S used?

(c) Run the theorem with $R = \mathbb{Z}$, $S = \mathbb{Z}/5\mathbb{Z}$, φ the quotient map, $s = [2]$ and $p = x^2 + 3x + 1$: compute $\Phi(p)$. For the uniqueness half, explain why **any** ring homomorphism Ψ with $\Psi(a) = [a]$ on constants and $\Psi(x) = [2]$ must send $3x^2$ to $[2]$.

(d) Give the idea of the proof in two sentences.

(e) In $\mathbb{F}_3[x]$, compute the values of $(x + 2)(x^2 + x + 1)$ at 0, 1, 2, and find all its roots in $\mathbb{F}_3$.

Solution.

(a) Twice: for $\Phi(1) = \varphi(1)s^0 = 1$, and for $\Phi(x) = \varphi(1)s^1 = s$.

(b) Essentially once: in the monomial computation, to rewrite $\varphi(a)\varphi(b)s^m s^n$ as $(\varphi(a)s^m)(\varphi(b)s^n)$, which moves $\varphi(b)$ past s^m by (F6) in S. The proof also uses (F6) in S for $0 \cdot s^k = 0$, for the right distributive law in the additivity steps, and for $1 \cdot s = s$; these uses only give the mirror forms of $a \cdot 0 = 0$, (F9) and (F7). An answer that lists them too, with this distinction, is correct.

(c) The coefficients of p are $1, 3, 1$, so $\Phi(p) = [1] + [3][2] + [1][2]^2 = [1 + 6 + 4] = [11] = [1]$. For the uniqueness half: $3x^2$ is the product of the constant 3 and x^2 (Theorem 4.2.4 (c)), so $\Psi(3x^2) = \Psi(3)\Psi(x)^2 = [3][2]^2 = [12] = [2]$. No other value is possible, because Ψ respects products.

(d) A ring homomorphism out of $R[x]$ has no freedom: it must send ax^n to $\varphi(a)s^n$, so

the formula is forced and uniqueness follows by additivity. The only work is to show that the forced formula respects products, and that is a check on monomials, where it becomes the power law and one reordering of factors in the commutative ring S.

(e) Evaluation respects products (Theorem 4.4.1), so the value is the product of the values of the factors. At 0: $2 \cdot 1 = 2$. At 1: $(1+2)(1+1+1) = 0 \cdot 0 = 0$. At 2: $(2+2)(4+2+1) = 1 \cdot 1 = 1$ (in $\mathbb{F}_3$, $4 = 7 = 1$). So the only root is 1. Multiplied out by the product formula, the polynomial is $x^3 + 3x^2 + 3x + 2 = x^3 + 2$ in $\mathbb{F}_3[x]$, the second example after Definition 4.4.1, whose values $2, 0, 1$ agree.

4.4.7.2 B. Practice

Exercise. B1: The degree of a composition

Let R be an integral domain, $p, q \in R[x]$, $p \neq 0$, and $\deg q \geq 1$. Prove that $\deg(p \circ q) = \deg p \cdot \deg q$. Show by an example that the hypothesis $\deg q \geq 1$ cannot be dropped.

Solution. Let $d := \deg p$ and $e := \deg q \geq 1$.

Powers of q. By Logic and Proof, Axiom 4.2.1 on k, $q^k \neq 0$, $\deg q^k = ke$ and $\operatorname{lc}(q^k) = \operatorname{lc}(q)^k$. For $k = 0$, $q^0 = 1$ has degree 0 and leading coefficient 1 (as $1 \neq 0$). For the step, $q^{k+1} = q^k q$, and since R has no zero divisors, Theorem 4.3.2 (b) gives degree $ke + e = (k+1)e$ and leading coefficient $\operatorname{lc}(q)^k \operatorname{lc}(q)$.

The top term. By Definition 4.4.3 with $N = d$, $p \circ q = \sum_{k=0}^{d} p_k q^k$. The term $p_d q^d$ is the product of the non-zero constant p_d (degree 0) and q^d, so by Theorem 4.3.2 (b) it has degree de. Every other term $p_k q^k$ with $k < d$ is 0 or has degree $ke < de$, since $e \geq 1$ (Theorem 4.3.2 (a)). By Theorem 4.3.1 and induction along the sum recursion, $r := \sum_{k=0}^{d-1} p_k q^k$ has $\deg r < de$ (for $d = 0$, r is the empty sum 0). Then $p \circ q = r + p_d q^d$, and the equality case of Theorem 4.3.1 gives $\deg(p \circ q) = de$.

The hypothesis on q. Take $R = \mathbb{Z}$, $p = x - 1$ and $q = 1$, of degree 0. Then $p \circ q = 1 - 1 = 0$, of degree $-\infty$, while $\deg p \cdot \deg q = 1 \cdot 0 = 0$. A constant q can make the top terms cancel.

Exercise. B2: All polynomials of degree at most two over the field with two elements

List the elements of $\mathbb{F}_2[x]_{\leq 2}$ with their degrees and their functions $\mathbb{F}_2 \to \mathbb{F}_2$ (given by the values at 0 and 1). How many functions $\mathbb{F}_2 \to \mathbb{F}_2$ are there, and how many of the eight polynomials give each one?

Solution. By Definition 4.3.3, the elements are $a_0 + a_1 x + a_2 x^2$ with $a_i \in \{0, 1\}$; there are eight (Exercise (B3: Counting polynomials over a finite field) for $\mathbb{F}_2$, $n = 2$). The value at 0

is a_0, and the value at 1 is $a_0 + a_1 + a_2$ in $\mathbb{F}_2$.

p	$\deg p$	$p(0)$	$p(1)$
0	$-\infty$	0	0
1	0	1	1
x	1	0	1
$x+1$	1	1	0
x^2	2	0	1
x^2+1	2	1	0
x^2+x	2	0	0
x^2+x+1	2	1	1

A function $\mathbb{F}_2 \to \mathbb{F}_2$ is determined by its two values, so there are $2 \cdot 2 = 4$ of them, and each occurs for exactly **two** polynomials in the table: $(0,0)$ for 0 and x^2+x; $(1,1)$ for 1 and x^2+x+1; $(0,1)$ for x and x^2; $(1,0)$ for $x+1$ and x^2+1. In each pair the two polynomials differ by x^2+x, the polynomial of Example (Different Polynomials, Equal Functions).

Exercise. B3: Shifting the variable

Let R be a commutative ring and $c \in R$. Define $T_c \colon R[x] \to R[x]$ by $T_c(p) \coloneqq p \circ (x+c)$. Prove that T_c is a bijective ring homomorphism with inverse T_{-c}.

Solution. By Definition 4.4.3, T_c is a ring homomorphism that fixes every constant and sends x to $x+c$; likewise T_{-c} fixes constants and sends x to $x-c$. The composite $T_{-c} \circ T_c$ is a ring homomorphism (after Definition 4.4.2) that fixes constants, and

$$T_{-c}(T_c(x)) = T_{-c}(x+c) = T_{-c}(x) + T_{-c}(c) = (x-c) + c = x.$$

The identity map of $R[x]$ is also a ring homomorphism that fixes constants and sends x to x. By the uniqueness in Theorem 4.4.2 (b), with $S = R[x]$, φ the constants and $s = x$, $T_{-c} \circ T_c = \mathrm{id}_{R[x]}$. Exchanging c and $-c$ (and $-(-c) = c$), $T_c \circ T_{-c} = \mathrm{id}_{R[x]}$. So T_c has the inverse T_{-c}, and is a bijection (Sets, Relations, and Cardinality, Definition 1.4.5).

4.4.7.3 C. Going deeper

Exercise. C1: Exit check: the substitution principle

State and prove Theorem 4.4.2.

Solution. Statement. Let R and S be commutative rings, $\varphi \colon R \to S$ a ring homomorphism and $s \in S$, and let $\Phi(p) \coloneqq \sum_{k=0}^{N} \varphi(p_k) s^k$ for N admissible for p. Then $\Phi \colon R[x] \to S$ is a well-defined ring homomorphism with $\Phi(a) = \varphi(a)$ for constants and $\Phi(x) = s$, and it is the only ring homomorphism $R[x] \to S$ with these two properties.

Well defined. Enlarging N by one adds the term $\varphi(0)s^k = 0 \cdot s^k = 0$, since $\varphi(0) + \varphi(0) = \varphi(0)$ gives $\varphi(0) = 0$; by induction any two admissible N give the same sum. In particular $\Phi(ax^m) = \varphi(a)s^m$, the other terms being 0.

Additive. With N admissible for p and q, $\Phi(p+q) = \sum_k \varphi(p_k + q_k)s^k = \sum_k (\varphi(p_k)s^k + \varphi(q_k)s^k) = \Phi(p) + \Phi(q)$, by additivity of φ, (F9) and (F6) in S, and (Σ1).

Multiplicative. The maps $(p, q) \mapsto \Phi(pq)$ and $(p, q) \mapsto \Phi(p)\Phi(q)$ are additive in p for fixed q, and in q for fixed p: the first because multiplication in $R[x]$ distributes over addition and Φ is additive, the second because Φ is additive and multiplication in S distributes. On monomials,

$$\Phi\big((ab)x^{m+n}\big) = \varphi(a)\varphi(b)s^m s^n = \big(\varphi(a)s^m\big)\big(\varphi(b)s^n\big),$$

by multiplicativity of φ, $s^{m+n} = s^m s^n$, and (F5), (F6) in S to move $\varphi(b)$ past s^m. Since $(ax^m)(bx^n) = (ab)x^{m+n}$, the two maps agree on pairs of monomials, so they agree everywhere by Lemma 4.2.3.

The one, constants and x. $\Phi(1) = \varphi(1)s^0 = 1$, $\Phi(ax^0) = \varphi(a)$, and $\Phi(x) = \varphi(1)s = s$.

Uniqueness. If Ψ is a ring homomorphism with $\Psi(ax^0) = \varphi(a)$ and $\Psi(x) = s$, then, as ax^n is the constant a times the n-th power of x, $\Psi(ax^n) = \varphi(a)s^n = \Phi(ax^n)$. Both maps are additive and agree on monomials, so $\Psi = \Phi$ by Lemma 4.2.3 with one argument.

Marking scheme. (10 points)

- 1: gives the formula for Φ and proves it does not depend on N, from $\varphi(0) = 0$.
- 1: proves Φ additive.
- 3: reduces multiplicativity to monomials (in one argument or in both), justifying the additivity it uses.
- 2: computes the monomial case correctly, justifying the reordering of factors in S (commutativity).
- 1: shows $\Phi(1) = 1$ and $\Phi(x) = s$ (and $\Phi(a) = \varphi(a)$).
- 2: proves uniqueness: the values on monomials are forced, then additivity.

Fatal errors (0 for the step): proving multiplicativity only for p, q of degree at most 1; assuming that a homomorphism is determined by its value at x alone, without using $\Psi(a) = \varphi(a)$ on constants. A proof of multiplicativity by expanding $\Phi(p)\Phi(q)$ as a double sum and regrouping by $i + j = k$ earns the 3 points of the reduction step only if the regrouping is proved.

Exercise. C2: Composition is associative

Let R be a commutative ring and $p, q, r \in R[x]$. Prove that $(p \circ q) \circ r = p \circ (q \circ r)$.

The first half of a proof is given.

> Fix q and r. Both sides are additive in p: the left side is $p \mapsto p \circ q$ followed by $u \mapsto u \circ r$, two ring homomorphisms (Definition 4.4.3), and the right side is $p \mapsto p \circ (q \circ r)$, a ring homomorphism.

The second half is blank. *Name the move, then complete it.*

Solution. One move is **check on monomials, extend by additivity**.

Let $p = ax^n$. Since $u \mapsto u \circ q$ is a ring homomorphism fixing the constant a and sending x

to q, and ax^n is the product of a and x^n (Theorem 4.2.4 (c)),

$$(ax^n) \circ q = (a \circ q)(x \circ q)^n = aq^n,$$

by the power property of ring homomorphisms (after Definition 4.4.2). Applying the ring homomorphism $u \mapsto u \circ r$ in the same way,

$$(aq^n) \circ r = (a \circ r)(q \circ r)^n = a\,(q \circ r)^n.$$

On the other side, the same computation with $q \circ r$ in place of q gives $(ax^n) \circ (q \circ r) = a\,(q \circ r)^n$. So the two sides agree on every monomial. Both are additive in p, so by Lemma 4.2.3 (with one argument and $T = R[x]$) they agree for every p.

Also correct: the move **a homomorphism out of $R[x]$ is fixed by the constants and x.** Both sides are ring homomorphisms $R[x] \to R[x]$ (composites of ring homomorphisms, after Definition 4.4.2), both fix every constant ($(a \circ q) \circ r = a \circ r = a$ and $a \circ (q \circ r) = a$), and both send x to $q \circ r$: $(x \circ q) \circ r = q \circ r$ and $x \circ (q \circ r) = q \circ r$. So they are equal by the uniqueness in Theorem 4.4.2 (b), with $S = R[x]$, $\varphi\colon a \mapsto ax^0$ and $s = q \circ r$.

Exercise. C3: The factor theorem over any commutative ring

Let R be a commutative ring and $c \in R$.

(a) Prove that for every $n \geq 1$,

$$x^n - c^n = (x - c) \sum_{j=0}^{n-1} c^{n-1-j} x^j.$$

(b) Prove that for $p \in R[x]$, $p(c) = 0$ if and only if $p = (x - c)q$ for some $q \in R[x]$.

(c) In $\mathbb{Z}/8\mathbb{Z}$, find all roots of $x^2 - 1$. The usual argument that a quadratic polynomial cannot have more than two roots goes: "if c_1 is a root, then $p = (x - c_1)q$ with $\deg q = 1$; a second root $c_2 \neq c_1$ has $(c_2 - c_1)q(c_2) = 0$, so $q(c_2) = 0$". Which step fails in $\mathbb{Z}/8\mathbb{Z}$?

Solution (Hint 1). For (a), compare coefficients: multiplying a polynomial by x shifts its coefficients up by one place (Lemma 4.2.2 (a)). For (b) ($\Rightarrow$), reduce to (a).

Solution (Hint 2). For (b), let N be admissible for p and start from $p - p(c) = \sum_{k=0}^{N} p_k x^k - \sum_{k=0}^{N} p_k c^k$, with $p(c)$ read as a constant.

Solution.

(a) Let $u := \sum_{j=0}^{n-1} c^{n-1-j} x^j$, so $u_j = c^{n-1-j}$ for $0 \leq j \leq n-1$ and $u_j = 0$ for $j \geq n$. By Lemma 4.2.2 (a) and Theorem 4.2.4 (d), $(x - c)u = xu - cu$ has coefficient $-cu_0$ at 0 and $u_{k-1} - cu_k$ at $k \geq 1$. So:

- at $k = 0$: $-c \cdot c^{n-1} = -c^n$;
- at $1 \leq k \leq n-1$: $c^{n-k} - c \cdot c^{n-1-k} = 0$, by the power law;

- at $k = n$: $u_{n-1} - cu_n = c^0 - 0 = 1$;
- at $k > n$: $0 - 0 = 0$.

These are the coefficients of $x^n - c^n$. This is Chapter 1's difference-of-powers identity (Lemma 1.1.4), read in the commutative ring $R[x]$ with $z = x$ and $w = c$; the proof above does not use it.

(b) ($\Leftarrow$) By Theorem 4.4.1, $p(c) = (c - c)\, q(c) = 0 \cdot q(c) = 0$.
($\Rightarrow$) Let N be admissible for p. By Proposition 4.2.1 and Theorem 4.2.4 (b), (c), and since the constants respect sums,

$$\begin{aligned} p - p(c) &= \sum_{k=0}^{N} p_k x^k - \sum_{k=0}^{N} p_k c^k \\ &= \sum_{k=1}^{N} p_k (x^k - c^k), \end{aligned}$$

where the term $k = 0$ is $p_0(1 - 1) = 0$. By (a), each $x^k - c^k$ with $k \geq 1$ is $(x - c)u^{(k)}$ for a polynomial $u^{(k)}$, so by the distributive law $p - p(c) = (x - c)q$ with $q := \sum_{k=1}^{N} p_k u^{(k)}$. If $p(c) = 0$, then $p = (x - c)q$.

(c) The squares in $\mathbb{Z}/8\mathbb{Z}$ of $[0], \ldots, [7]$ are $[0], [1], [4], [1], [0], [1], [4], [1]$ (for instance $[5]^2 = [25] = [1]$, $[7]^2 = [49] = [1]$). So $x^2 - 1$ has the four roots $[1], [3], [5], [7]$. The failing step is "$(c_2 - c_1)q(c_2) = 0$, so $q(c_2) = 0$": it needs $\mathbb{Z}/8\mathbb{Z}$ to have no zero divisors. With $c_1 = [1]$, $q = x + 1$ and $c_2 = [3]$, $(c_2 - c_1)q(c_2) = [2][4] = [8] = [0]$, with both factors non-zero.

Chapter 5 proves the factor theorem over a field again, by division with remainder.

Exercise. C4: A second proof of Fermat's little theorem

Let p be a prime. Give another proof that $a^{p-1} = 1$ for every non-zero $a \in \mathbb{F}_p$, along the following steps, and then compare $x^p - x$ with its function.

(a) Let $a \in \mathbb{F}_p$ be non-zero. Show that $b \mapsto ab$ is a bijection from $\mathbb{F}_p \setminus \{0\}$ to itself.

(b) Deduce that $a^{p-1} = 1$, by computing the product of all non-zero elements of $\mathbb{F}_p$ in two ways.

(c) Show that $x^p - x \neq 0$ in $\mathbb{F}_p[x]$, but $\varepsilon(x^p - x) = 0$.

Solution. Write $F := \mathbb{F}_p$, a field (Definition 2.2.1); then $F \setminus \{0\}$ has the $p - 1$ elements $1, \ldots, p - 1$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)).

(a) For $b \in F \setminus \{0\}$, $ab \neq 0$, since F has no zero divisors (Theorem 2.1.1 (f)); so $b \mapsto ab$ maps $F \setminus \{0\}$ to $F \setminus \{0\}$. It is injective: $ab = ab'$ gives $a(b - b') = 0$, so $b = b'$. Its image is a subset of the finite set $F \setminus \{0\}$ in bijection with $F \setminus \{0\}$; if the image were a proper subset, this would contradict Sets, Relations, and Cardinality, Theorem 3.1.9. So the map is surjective, hence a bijection.

(b) *A rearranged product is the same product.* For a list $t_1, \ldots, t_r$ in a commutative ring and a bijection σ of $\{1, \ldots, r\}$, we show $\prod_{j=1}^{r} t_{\sigma(j)} = \prod_{j=1}^{r} t_j$, by Logic and Proof, Axiom 4.2.1 on r. For $r = 0$ both sides are the empty product 1. For the step, first a deletion rule: for a list $u_1, \ldots, u_{r+1}$ and a position k, the product equals u_k times the product of the list with position k deleted. For $k = r + 1$ this is the product recursion;

for $k \le r$, it follows from the rule for the first r entries (induction on the length) and (F5), (F6):

$$\prod_{j=1}^{r+1} u_j = \Big(\prod_{j=1}^{r} u_j\Big)u_{r+1} = \Big((\textstyle\prod_{j\le r,\, j\ne k} u_j)u_k\Big)u_{r+1}$$
$$= \Big((\textstyle\prod_{j\le r,\, j\ne k} u_j)u_{r+1}\Big)u_k,$$

and the bracket in the last line is the product of the list with position k deleted, by the product recursion, since that list ends with u_{r+1}. Now let $u_j := t_{\sigma(j)}$ and $k := \sigma^{-1}(r+1)$. Deleting position k leaves the list $t_{\sigma'(1)}, \dots, t_{\sigma'(r)}$, where $\sigma'(i) := \sigma(i)$ for $i < k$ and $\sigma'(i) := \sigma(i+1)$ for $i \ge k$, a bijection of $\{1, \dots, r\}$: its values lie in $\{1, \dots, r\}$, since $\sigma(m) = r+1$ only for $m = k$ and the index used (i for $i < k$, $i+1$ for $i \ge k$) is never k; it is injective because σ and this index map are; and every $j \le r$ is $\sigma(m)$ for some $m \ne k$, so $j = \sigma'(m)$ if $m < k$ and $j = \sigma'(m-1)$ if $m > k$. By the deletion rule and the hypothesis for r, $\prod_{j=1}^{r+1} t_{\sigma(j)} = (\prod_{i=1}^{r} t_i)t_{r+1} = \prod_{j=1}^{r+1} t_j$.

The two computations. List $F \setminus \{0\}$ as $b_1, \dots, b_{p-1}$, and let $Q := \prod_{j=1}^{p-1} b_j$. By (a), $ab_j = b_{\sigma(j)}$ for a bijection σ of $\{1, \dots, p-1\}$, so the list $ab_1, \dots, ab_{p-1}$ is a rearrangement of $b_1, \dots, b_{p-1}$, and its product is Q. By (F5), (F6) and induction on the length, the same product is $a^{p-1}Q$. So $a^{p-1}Q = Q = 1 \cdot Q$. Since Q is a product of non-zero elements of a field, $Q \ne 0$ (Theorem 2.1.1 (f), by induction), and canceling Q (Theorem 2.1.1 (b)) gives $a^{p-1} = 1$.

(c) The polynomial $x^p - x$ has coefficient 1 at position p (since $p \ge 2$, the positions p and 1 differ), and $1 \ne 0$ in F; so it is not the zero polynomial. For every $c \in F$, $c^p - c = 0$: if $c \ne 0$, $c^p = c^{p-1}c = c$ by (b); and $0^p = 0$ since $p \ge 1$. So $\varepsilon(x^p - x)$ is the zero function. This gives a second proof, by Fermat rather than by the factors $x - c$, that ε is not injective over $\mathbb{F}_p$. The two witnesses are in fact the same polynomial: Chapter 5 shows that $x^p - x = \prod_{c \in \mathbb{F}_p}(x - c)$, the P of Proposition 4.4.4 (d) with $R = \mathbb{F}_p$ (Example (Polynomial Functions over a Finite Field) (b)).

This is the second proof of Theorem 2.6.6 (b); the first, in Chapter 2, went through the Frobenius map. Part (c) also follows directly from Theorem 2.6.6 (a).

4.5 The Formal Derivative

The polynomials of this chapter are coefficient sequences, and Theorem 4.4.2 showed how to evaluate them and how to substitute into them. One more operation from school survives the passage to an arbitrary commutative ring: the derivative. This section defines it by its coefficients, proves the sum, product and power rules with the move of Lemma 4.2.3, and asks when a derivative can be 0. Over a field the answer depends on the characteristic of Chapter 2, and over $\mathbb{F}_p$ it is not the answer of calculus.

At school a double root shows itself in the graph. The parabola $y = (x-1)^2$ touches the axis at 1 instead of crossing it, and its slope there is 0: the derivative $2(x-1)$ vanishes at 1 as well. Over $\mathbb{F}_p$ there is no graph and no slope; the field has p elements and no limits. What survives is the formula: the derivative of ax^n is nax^{n-1}. We keep the formula and drop the limit. Chapter 5 uses the result to detect repeated roots; this section builds the tool.

Throughout, R is a commutative ring (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1). Polynomials are written f, g, h, with coefficients f_k, g_k, h_k, because the letter p is kept for a prime. A dot with an integer on its left is a **multiple**, $n \cdot a = a + \cdots + a$ with n terms (the "Multiples" paragraph of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 2.3, collected in

Lemma 4.1.1 (d)); the product of two ring elements is written by juxtaposition.

4.5.1 The derivative by coefficients

At school, $(3x^4 + 5x^2)' = 12x^3 + 10x$. Each term moves down one place, and its coefficient is multiplied by the exponent it had. In $R[x]$ "multiplied by the exponent" has a meaning without any division or limit: the exponent n is a natural number, and $n \cdot a$ is the n-th multiple of a. That recurring computation deserves a name.

The formal derivative moves every coefficient down one place and takes it as many times as its old exponent.

Definition 4.5.1. Formal Derivative

Let R be a commutative ring and $f \in R[x]$. The **formal derivative** of f is the sequence $f' \colon \mathbb{N} \to R$ given by

$$(f')_k := (k+1) \cdot f_{k+1} \qquad \text{for every } k \in \mathbb{N},$$

where $(k+1) \cdot f_{k+1}$ is the $(k+1)$-th multiple of f_{k+1}. The **higher derivatives** are defined by

$$f^{(0)} := f, \qquad f^{(k+1)} := (f^{(k)})' \quad (k \in \mathbb{N}),$$

and we write f'' for $f^{(2)}$.

In words: the coefficient of x^k in f' is read off from the coefficient of x^{k+1} in f, added to itself $k+1$ times. The definition uses only the addition of R, so it makes sense, word for word, over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{F}_p$.

Well-definedness. Two things need checking: that f' is again a polynomial, and that the higher derivatives exist.

- $f' \in R[x]$**.** First, $m \cdot 0 = 0$ for every $m \in \mathbb{N}$: by Lemma 4.1.1 (d), $m \cdot 0 = (m \cdot 1)0$, and this is 0 by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b). Now choose $N \in \mathbb{N}$ with $f_k = 0$ for every $k > N$ (Definition 4.1.1). For $k \geq N$ we have $k+1 > N$, so $f_{k+1} = 0$ and $(f')_k = (k+1) \cdot 0 = 0$. So f' has only finitely many non-zero terms, and $f' \in R[x]$. Moreover $(f')_k = 0$ for $k > N-1$, so for $N \geq 1$, Proposition 4.2.1 writes f' as an honest sum:

$$f' = \sum_{k=0}^{N-1} ((k+1) \cdot f_{k+1}) x^k = 1 \cdot f_1 + (2 \cdot f_2)x + \cdots + (N \cdot f_N)x^{N-1}.$$

- **Higher derivatives.** Since $u \mapsto u'$ is a function $R[x] \to R[x]$, Sets, Relations, and Cardinality, Theorem 2.3.1, with $X = R[x]$, starting value f and step $(k, u) \mapsto u'$, gives exactly one sequence $k \mapsto f^{(k)}$ with the two displayed properties.

Monomials. Let $a \in R$ and $n \in \mathbb{N}$. The monomial ax^n has a in position n and 0 elsewhere (Definition 4.1.1), so $(ax^n)_{k+1}$ is a when $k+1 = n$ and 0 otherwise. Hence $((ax^n)')_k$ is $n \cdot a$ when $k = n-1$, and $(k+1) \cdot 0 = 0$ otherwise:

$$(ax^n)' = (n \cdot a)\, x^{n-1} \quad (n \geq 1), \qquad (ax^0)' = 0. \tag{M}$$

The case $n = 0$ is separate because x^{n-1} has no meaning there: $-1 \notin \mathbb{N}$. Every constant has derivative 0.

The element $n \cdot 1$. By Lemma 4.1.1 (d), $n \cdot a = (n \cdot 1)a$. So the exponent enters the derivative only through one element of R, the multiple $n \cdot 1$, and **that element can be** 0. In $\mathbb{F}_2$,

$2 \cdot 1 = 1 + 1 = 0$, so $(x^2)' = (2 \cdot 1)x = 0$. This is the whole difference between the derivative here and the derivative of calculus, and the rest of the section keeps track of it.

Why this definition. The formula is the school formula with the limit removed. Exercise C1 asks you to show that it is the only additive map $R[x] \to R[x]$ that sends constants to 0, sends x to 1 and obeys the product rule. A definition by limits is not available, since $\mathbb{F}_p$ and $\mathbb{Z}/6\mathbb{Z}$ have no distances.

Warning. The coefficient of x^k in f' is $(k+1) \cdot f_{k+1}$, not $k \cdot f_k$: the derivative shifts before it multiplies. For $f = x^2$ over $\mathbb{Q}$, the coefficient of x^1 in $f' = 2x$ is $2 \cdot f_2 = 2$, while $1 \cdot f_1 = 0$. Reading the formula without the shift gives $\sum_k (k \cdot f_k)x^k$, which is xf', not f'.

Example. Formal derivatives in five rings

Compute the following derivatives.

(i) $(x^4 - 2x^3 + 2x - 1)'$ over $\mathbb{Q}$.

(ii) a', x' and $(x - c)'$ over any commutative ring R, for $a, c \in R$.

(iii) $(x^3 + x)'$ over $\mathbb{F}_3$, and $(x^2)'$ over $\mathbb{F}_2$.

(iv) $([2]x^3 + x)'$ over $\mathbb{Z}/6\mathbb{Z}$.

(v) $(x^n)'$ over $\mathbb{Z}$, for $n \geq 1$.

(vi) The higher derivatives $(x^4)'$, $(x^4)''$ and $(x^4)'''$ over $\mathbb{Q}$ and over $\mathbb{F}_3$.

Solution. In each case, by (M) and Lemma 4.1.1 (d), the derivative of ax^n with $n \geq 1$ is $((n \cdot 1)a)x^{n-1}$, and the derivative of a sum is computed coefficient by coefficient from Definition 4.5.1.

(i) The coefficients are $f_0 = -1$, $f_1 = 2$, $f_2 = 0$, $f_3 = -2$, $f_4 = 1$, and $f_k = 0$ for $k \geq 5$. So $(f')_0 = 1 \cdot 2 = 2$, $(f')_1 = 2 \cdot 0 = 0$, $(f')_2 = 3 \cdot (-2) = -6$, $(f')_3 = 4 \cdot 1 = 4$, and $(f')_k = 0$ for $k \geq 4$. In $\mathbb{Q}$ the multiple $n \cdot a$ is the product na: $n \cdot a = (n \cdot 1)a$ by Lemma 4.1.1 (d), and $n \cdot 1$ is the rational number n, by induction on n from $(n+1) \cdot 1 = n \cdot 1 + 1$, since the embeddings $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$ preserve sums and 1 (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4). Hence

$$(x^4 - 2x^3 + 2x - 1)' = 4x^3 - 6x^2 + 2,$$

as at school.

(ii) $a = ax^0$, so $a' = 0$ by (M). $x = 1x^1$ (Definition 4.1.1), so $x' = (1 \cdot 1)x^0 = 1$, since $1 \cdot 1 = 0 \cdot 1 + 1 = 1$ by the recursion of multiples. The polynomial $x - c$ has $-c$ in position 0, 1 in position 1 and 0 elsewhere, so $((x-c)')_0 = 1 \cdot 1 = 1$, and $((x-c)')_k = (k+1) \cdot 0 = 0$ for $k \geq 1$: $(x - c)' = 1$.

(iii) Over $\mathbb{F}_3$, $(x^3 + x)' = (3 \cdot 1)x^2 + 1 = 1$, since $3 \cdot 1 = 1 + 1 + 1 = 0$ in $\mathbb{F}_3$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d): $p \cdot [1] = [p] = [0]$ in $\mathbb{Z}/p\mathbb{Z}$). Over $\mathbb{F}_2$, $(x^2)' = (2 \cdot 1)x = 0$, since $1 + 1 = 0$ in $\mathbb{F}_2$ (Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$)).

(iv) $([2]x^3 + x)' = (3 \cdot [2])x^2 + 1 = [6]x^2 + 1 = 1$, since $3 \cdot [2] = (3 \cdot [1])[2] = [3][2] = [6] = [0]$, by Lemma 4.1.1 (d), Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d), and

the product of classes computed on representatives (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (b)). The polynomial has degree 3 and its derivative has degree 0: the degree dropped by 3, not by 1.

(v) $(x^n)' = (n{\cdot}1)x^{n-1} = nx^{n-1}$, since in $\mathbb{Z}$ the multiple $n{\cdot}1$ is the integer n (the "Multiples" paragraph cited above).

(vi) Apply (M) three times, with the rule $m \cdot (j \cdot 1) = (mj) \cdot 1$ of Lemma 4.1.1 (d). Over any commutative ring,

$$(x^4)' = (4{\cdot}1)x^3, \qquad (x^4)'' = \big(3{\cdot}(4{\cdot}1)\big)x^2 = (12{\cdot}1)x^2, \qquad (x^4)''' = \big(2{\cdot}(12{\cdot}1)\big)x = (24{\cdot}1)x.$$

Over $\mathbb{Q}$, as in (i), these are $4x^3$, $12x^2$ and $24x$. Over $\mathbb{F}_3$, $3{\cdot}1 = 0$, so $4{\cdot}1 = 3{\cdot}1+1{\cdot}1 = 1$ and $12 \cdot 1 = 4 \cdot (3 \cdot 1) = 4 \cdot 0 = 0$, by Lemma 4.1.1 (d) and $m \cdot 0 = 0$. So $(x^4)' = x^3$, but already $(x^4)'' = 0$, and then $(x^4)''' = 0' = 0$ by (M).

Examples (iii) and (iv) are the new phenomena. Over $\mathbb{F}_2$ a non-constant polynomial has derivative 0; over $\mathbb{Z}/6\mathbb{Z}$ the coefficient of x^2 in the derivative, $3 \cdot [2]$, is $[0]$ although neither $3 \cdot [1] = [3]$ nor $[2]$ is. Both come from the element $n \cdot 1$ above.

Quick check. Compute $(x^3 + x^2 + x + 1)'$ over $\mathbb{F}_2$.

Solution. $(3 \cdot 1)x^2 + (2 \cdot 1)x + 1 = x^2 + 1$, since $3 \cdot 1 = 1 + 1 + 1 = 1$ and $2 \cdot 1 = 0$ in $\mathbb{F}_2$.

4.5.2 The rules of differentiation

Calculus proves the sum, product and power rules with limits. Here they must come from the coefficients. The sum rule is one line per coefficient. The product rule is where a direct attack hurts: the k-th coefficient of $(fg)'$ is $(k+1)\cdot\sum_{i=0}^{k+1} f_i g_{k+1-i}$, and matching it with $f'g+fg'$ means splitting each term between two sums with shifted indices. The move of Section 4.2, **check on monomials, extend by additivity**, avoids that: both sides of the product rule are additive in f and in g, so it is enough to compare them on monomials, where (M) does the work.

Theorem 4.5.1. Rules for the Formal Derivative

Let R be a commutative ring, $f, g \in R[x]$, $a, c \in R$ and $m \in \mathbb{Z}_{>0}$.

(a) (Linearity) $(f + g)' = f' + g'$, and $(af)' = af'$ for the constant a; moreover $a' = 0$.

(b) (Product rule) $(fg)' = f'g + fg'$.

(c) (Power rule) $(g^m)' = (m \cdot 1)\, g^{m-1}g'$. In particular $\big((x - c)^m\big)' = (m \cdot 1)(x - c)^{m-1}$.

Idea. ① Linearity is one coefficient at a time: the multiple $(k + 1) \cdot b$ is additive in b and commutes with multiplication by a constant. ② For the product rule, both $(fg)'$ and $f'g+fg'$ are additive in each argument, by ①; so Lemma 4.2.3 reduces the rule to $f = ax^i$, $g = bx^j$. There (M) and Lemma 4.2.2 (b) turn both sides into one monomial, and the coefficients agree because $(i + j) \cdot (ab) = i \cdot (ab) + j \cdot (ab)$. ③ The power rule is the product rule applied $m - 1$ times, by induction.

Proof. Equality of polynomials is equality of all coefficients (Definition 4.1.1), so it is enough to compare coefficients in (a); (b) and (c) are then built on (a).

(a) Let $k \in \mathbb{N}$. Since addition in $R[x]$ is coefficientwise (Definition 4.2.1),

$$\begin{aligned}((f+g)')_k &= (k+1)\cdot(f_{k+1}+g_{k+1})\\ &= (k+1)\cdot f_{k+1} + (k+1)\cdot g_{k+1} = (f'+g')_k,\end{aligned}$$

where the second equality is the rule $n\cdot(b+d) = n\cdot b + n\cdot d$ of Lemma 4.1.1 (d). For the constant a, $(af)_{k+1} = af_{k+1}$ by Theorem 4.2.4 (d), so

$$\begin{aligned}((af)')_k &= (k+1)\cdot(f_{k+1}a)\\ &= ((k+1)\cdot f_{k+1})a = a(f')_k = (af')_k,\end{aligned}$$

using (F6) of R in the first and third equalities, the rule $(n\cdot b)d = n\cdot(bd)$ of Lemma 4.1.1 (d) in the second, and Theorem 4.2.4 (d) in the last. Finally $a' = 0$ is (M) with $n = 0$.

(b) Define $\Phi, \Psi\colon R[x]\times R[x] \to R[x]$ by

$$\Phi(f,g) \coloneqq (fg)', \qquad \Psi(f,g) \coloneqq f'g + fg'.$$

By Theorem 4.2.4 (a), $R[x]$ is a commutative ring, so (F1)–(F7), (F9) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 hold in it.
Additivity. Let $f, h, g \in R[x]$. By the distributive law (F9) of $R[x]$ and (a),

$$\Phi(f+h,g) = (fg+hg)' = (fg)' + (hg)' = \Phi(f,g) + \Phi(h,g).$$

By (a), (F9) and a regrouping of four terms by (F1) and (F2),

$$\begin{aligned}\Psi(f+h,g) &= (f'+h')g + (f+h)g'\\ &= (f'g+fg') + (h'g+hg') = \Psi(f,g) + \Psi(h,g).\end{aligned}$$

Both maps are symmetric: $\Phi(f,g) = \Phi(g,f)$ because $fg = gf$, and $\Psi(f,g) = \Psi(g,f)$ because $f'g + fg' = gf' + g'f = g'f + gf'$, by (F6) and (F2) of $R[x]$. So each is additive in its second argument as well.
Monomials. Let $u = ax^i$ and $v = bx^j$, with $a, b \in R$ and $i, j \in \mathbb{N}$. By Lemma 4.2.2 (b), $uv = (ab)x^{i+j}$.
Case $i \geq 1$ and $j \geq 1$. Then $i + j \geq 1$, and (M) gives

$$\Phi(u,v) = ((i+j)\cdot(ab))x^{i+j-1}.$$

On the other side, (M) gives $u' = (i\cdot a)x^{i-1}$ and $v' = (j\cdot b)x^{j-1}$, and Lemma 4.2.2 (b), with $(i-1)+j = i+(j-1) = i+j-1$ in $\mathbb{N}$, gives

$$\Psi(u,v) = ((i\cdot a)b)x^{i+j-1} + (a(j\cdot b))x^{i+j-1}.$$

Now $(i\cdot a)b = i\cdot(ab)$, and $a(j\cdot b) = (j\cdot b)a = j\cdot(ba) = j\cdot(ab)$, by Lemma 4.1.1 (d) and (F6) of R. Two monomials in the same position add coefficientwise (Definition 4.2.1), and $i\cdot(ab) + j\cdot(ab) = (i+j)\cdot(ab)$ (Lemma 4.1.1 (d)). So $\Psi(u,v) = \Phi(u,v)$.
Case $i = 0$. Then $u = a$ is a constant, $u' = 0$ by (a), and $uv = (ab)x^j$. So $\Psi(u,v) = 0\cdot v + av' = av'$, by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) and (F3) of $R[x]$. If $j = 0$, then $v' = 0$ and uv is a constant, so both sides are 0 (by

(a) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)). If $j \geq 1$, then by (M) and Lemma 4.2.2 (b) with $m = 0$,

$$av' = (a(j \cdot b))x^{j-1} = (j \cdot (ab))x^{j-1} = ((ab)x^j)' = \Phi(u, v),$$

where the middle step is the computation of the previous case.
Case $j = 0$, $i \geq 1$. By the symmetry of Φ and Ψ this is the case $i = 0$ with u and v exchanged.
So Φ and Ψ agree whenever both arguments are monomials, and both are additive in each argument. By Lemma 4.2.3, with two arguments and $T = R[x]$, $\Phi = \Psi$. This is the product rule.

(c) First, $(f-g)' = f'-g'$: by (a), $(f-g)'+g' = ((f-g)+g)' = f'$, and adding $-g'$ to both sides gives the claim, by (F2)–(F4) of $R[x]$. We prove the power rule by induction on $m \geq 1$ (Logic and Proof, Axiom 4.2.1, with base 1). For $m = 1$: $g^0 = 1$ (Lemma 4.1.1 (c)) and $1 \cdot 1 = 1$, so the right side is $1 \cdot 1 \cdot g' = g'$. Suppose $(g^m)' = (m \cdot 1)g^{m-1}g'$ for some $m \geq 1$. Since $g^{m+1} = g^m g$, the product rule (b) gives

$$\begin{aligned}(g^{m+1})' &= (g^m)'g + g^m g' = (m \cdot 1)g^{m-1}g'g + g^m g' \\ &= (m \cdot 1)g^m g' + 1 \cdot g^m g' = ((m+1) \cdot 1)g^m g'.\end{aligned}$$

The third equality uses (F5), (F6), $g^{m-1}g = g^m$ (the power recursion, since $(m-1)+1 = m$) and (F7); the last uses (F9), the fact that constants add as in R (Theorem 4.2.4 (b)), and the recursion $(m+1)\cdot 1 = m\cdot 1+1$ of multiples. This completes the induction.

For the particular case, $(x - c)' = x' - c' = 1 - 0 = 1$, by the difference rule and Example (Formal derivatives in five rings) (ii). The power rule with $g = x - c$ gives $((x - c)^m)' = (m \cdot 1)(x - c)^{m-1} \cdot 1$, and $\cdot 1$ may be dropped by (F7). This proves the theorem.

■

The theorem is the calculus toolkit with every limit removed, and it holds over every commutative ring. The power rule shows the element $m \cdot 1$ once more: the derivative of $(x - c)^m$ is $(x - c)^{m-1}$ times the constant $m \cdot 1$, and over $\mathbb{F}_p$ that constant is 0 for $m = p$. So over $\mathbb{F}_p$ the polynomial $(x - c)^p$ has derivative 0, although it is not constant; the next subsection says exactly when this happens.

Remark. Over $\mathbb{Q}$, and over the real numbers, f' is the derivative of the polynomial function $c \mapsto f(c)$ in the sense of calculus. This book never uses the agreement, and nothing in it depends on it; it explains only why the formulas look familiar.

Quick check. Over $\mathbb{F}_3$, compute $((x + 1)^3)'$ twice: by the power rule, and by expanding $(x + 1)^3$ first.

Solution. By Theorem 4.5.1 (c), $((x + 1)^3)' = (3 \cdot 1)(x + 1)^2 = 0$, since $3 \cdot 1 = 0$ in $\mathbb{F}_3$. Expanding, $(x + 1)^3 = x^3 + 3x^2 + 3x + 1 = x^3 + 1$ in $\mathbb{F}_3[x]$, and $(x^3 + 1)' = (3 \cdot 1)x^2 = 0$. The two answers agree.

4.5.3 When the derivative vanishes

In calculus, a function with derivative 0 on an interval is constant. Over $\mathbb{F}_2$ the polynomial x^2 is not constant, yet $(x^2)' = 0$ (Example (Formal derivatives in five rings) (iii)). Which polynomials have derivative 0? Over a field the answer depends only on the characteristic. Recall Definition 2.5.1: $\operatorname{char} F$ is the least positive integer n with $n \cdot 1 = 0$ in F, and 0 if there is none; by Theorem 2.5.3 it is 0 or a prime.

Proposition 4.5.2. When the Formal Derivative Is Zero

Let F be a field (Definition 2.1.1) and $f \in F[x]$.

(a) If $\operatorname{char} F = 0$, then $f' = 0$ **if and only if** f is constant. Moreover, $\deg f' = \deg f - 1$ whenever $\deg f \geq 1$.

(b) If $\operatorname{char} F = p > 0$, then p is prime, and the following are equivalent: (i) $f' = 0$; (ii) $f_k = 0$ for every $k \in \mathbb{N}$ **not** divisible by p; (iii) $f = g \circ x^p$ for some $g \in F[x]$ (Definition 4.4.3).

Idea. Everything rests on one identity: for $k \geq 1$, the coefficient of x^{k-1} in f' is $k \cdot f_k = (k \cdot 1) f_k$. In a field a product is 0 only when a factor is. So $f' = 0$ forces $f_k = 0$ exactly at the k with $k \cdot 1 \neq 0$: in characteristic 0 that is every $k \geq 1$, and in characteristic p it is every k not divisible by p. A polynomial whose only non-zero coefficients sit at multiples of p is a polynomial in x^p.

Proof. For every $k \geq 1$, Definition 4.5.1 at the index $k-1$ and Lemma 4.1.1 (d) give

$$(f')_{k-1} = k \cdot f_k = (k \cdot 1) f_k. \tag{$*$}$$

As k runs through the integers ≥ 1, the index $k-1$ runs through $\mathbb{N}$, so $f' = 0$ **if and only if** $(k \cdot 1) f_k = 0$ for every $k \geq 1$.

(a) Let $\operatorname{char} F = 0$. Then $k \cdot 1 \neq 0$ for every $k \geq 1$, by Definition 2.5.1. Suppose $f' = 0$, and let $k \geq 1$. By $(*)$, $(k \cdot 1) f_k = 0$ with $k \cdot 1 \neq 0$, so $f_k = 0$ by Theorem 2.1.1 (f). Thus f and the constant f_0 agree in every position, and $f = f_0$ (Definition 4.1.1). Conversely, a constant has derivative 0 by Theorem 4.5.1 (a).
Now let $n := \deg f \geq 1$, so that $f_n \neq 0$ and $f_k = 0$ for every $k > n$ (Definition 4.3.1). By $(*)$, $(f')_{n-1} = (n \cdot 1) f_n$, a product of two non-zero elements of F, which is non-zero by Theorem 2.1.1 (f). For $k \geq n$, $(f')_k = (k+1) \cdot f_{k+1} = (k+1) \cdot 0 = 0$, as in the well-definedness paragraph after Definition 4.5.1. So $n-1$ is the largest index of a non-zero coefficient of f': $\deg f' = n - 1$.

(b) Let $\operatorname{char} F = p > 0$. Then p is prime by Theorem 2.5.3.

By Proposition 2.5.2 (a), with $c = p$: for $k \in \mathbb{N}$, $k \cdot 1 = 0$ **if and only if** $p \mid k$.

(i) $\Rightarrow$ (ii). Let $f' = 0$ and let $k \in \mathbb{N}$ with $p \nmid k$. Then $k \neq 0$, since $p \mid 0$; so $k \geq 1$, and $(k \cdot 1) f_k = 0$ by $(*)$. By Proposition 2.5.2 (a), $k \cdot 1 \neq 0$, so $f_k = 0$ by Theorem 2.1.1 (f).

(ii) $\Rightarrow$ (i). Let $k \geq 1$. If $p \nmid k$, then $f_k = 0$ by (ii); if $p \mid k$, then $k \cdot 1 = 0$ by Proposition 2.5.2 (a). Either way $(k \cdot 1) f_k = 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b)), so $f' = 0$ by $(*)$.

(ii) $\Rightarrow$ (iii). Choose $N \in \mathbb{N}$ with $f_k = 0$ for every $k > N$, and define $g\colon \mathbb{N} \to F$ by $g_j := f_{pj}$. For $j > N$ we have $pj \geq j > N$, so $g_j = 0$, and $g \in F[x]$. By Definition 4.4.3, then the power law $(x^p)^j = x^{pj}$ in the commutative ring $F[x]$ (Lemma 4.1.1 (c)) and Theorem 4.2.4 (c),

$$g \circ x^p = \sum_{j=0}^{N} g_j \, (x^p)^j = \sum_{j=0}^{N} f_{pj} \, x^{pj}.$$

We compare the coefficients of both sides with those of f at an index $k \in \mathbb{N}$. Addition in $F[x]$ is coefficientwise (Definition 4.2.1), so the k-th coefficient of a finite sum of polynomials is the finite sum of their k-th coefficients (induction on the number of terms, through the sum recursion of Lemma 4.1.1 (a)). The monomial $f_{pj}x^{pj}$ has k-th coefficient f_k if $pj = k$, and 0 otherwise.

- If $p \nmid k$, no j has $pj = k$, so every term is 0 at k, and $f_k = 0$ by (ii).
- If $p \mid k$, then $k = pj_0$ for some $j_0 \in \mathbb{Z}$, and $j_0 \geq 0$: if $j_0 < 0$, then $pj_0 < 0 \cdot p = 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (c), since $p > 0$, against $k \geq 0$. This j_0 is unique (if $pj = pj'$, then $j = j'$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (f), since $p \neq 0$). If $j_0 \leq N$, the sum of the k-th coefficients has the single possibly non-zero term $f_{pj_0} = f_k$, so it equals f_k by (Σ3) of Lemma 4.1.1 (b). If $j_0 > N$, every term is 0 at k, and $f_k = 0$ because $k = pj_0 \geq j_0 > N$.

In every case the k-th coefficients agree, so $g \circ x^p = f$.

(iii) $\Rightarrow$ (ii). Let $f = g \circ x^p$, and choose N with $g_j = 0$ for $j > N$. The computation above gives $f = \sum_{j=0}^{N} g_j \, x^{pj}$, and by the first bullet, the coefficient of this sum at any k with $p \nmid k$ is 0. This proves the proposition.

■

So in characteristic p the polynomials with derivative 0 are exactly the polynomials in x^p. Over $\mathbb{F}_2$, $x^2 + 1 = (x + 1) \circ x^2$; over $\mathbb{F}_3$, $x^6 + 2x^3 + 1 = (x^2 + 2x + 1) \circ x^3$, and indeed its derivative is $(6 \cdot 1)x^5 + (6 \cdot 1)x^2 = 0$, since $6 \cdot 1 = 0$ in $\mathbb{F}_3$. Part (a) is the case where the school statement survives, and its proof spends the hypothesis at exactly one place: $k \cdot 1 \neq 0$.

Warning. "$f' = 0$ means f is constant" and "differentiating lowers the degree by one" both fail in characteristic p. Over $\mathbb{F}_p$, $(x^p)' = (p \cdot 1)x^{p-1} = 0$, although x^p has degree p; and $(x^p - x)' = (p \cdot 1)x^{p-1} - 1 = -1$ has degree 0, not $p - 1$. Tests for repeated roots that use the derivative must therefore say which characteristic they assume. Chapter 5 concludes from $(x^p - x)' = -1$ that $x^p - x$ has no repeated roots in $\mathbb{F}_p$.

Quick check. Compute $(x^5 + x)'$ over $\mathbb{F}_5$.

Solution. $(x^5 + x)' = (5 \cdot 1)x^4 + 1 = 1$, since $5 \cdot 1 = 0$ in $\mathbb{F}_5$.

4.5.4 Exercises

4.5.4.1 A. Check your understanding

Exercise. A1

(a) Compute $(x^5 - x)'$ over $\mathbb{Q}$ and over $\mathbb{F}_5$.

(b) True or false: if $f' = 0$, then f is constant. Answer over $\mathbb{Q}$ and over $\mathbb{F}_2$, with a reason or a witness.

(c) Let $f \in (\mathbb{Z}/6\mathbb{Z})[x]$ have degree 3 and leading coefficient $[2]$. What can $\deg f'$ be? Give a witness for each possibility.

(d) In the proof of the product rule (Theorem 4.5.1 (b)), why is the case $i = 0$ treated separately?

Solution.

(a) Over $\mathbb{Q}$: $(x^5-x)' = 5x^4-1$, by (M), with $5\cdot 1 = 5$. Over $\mathbb{F}_5$: $(x^5-x)' = (5\cdot 1)x^4-1 = -1$, since $5 \cdot 1 = 0$ in $\mathbb{F}_5$; in the elements $0, \dots, 4$ of $\mathbb{F}_5$, $-1 = 4$.

(b) Over $\mathbb{Q}$: **true**. $\mathbb{Q}$ is a field (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3) of characteristic 0 (Example (The characteristics of the standard fields)); so Proposition 4.5.2 (a) applies. Over $\mathbb{F}_2$: **false**. The witness is x^2, which is not constant, with $(x^2)' = (2 \cdot 1)x = 0$ (Example (Formal derivatives in five rings) (iii)).

(c) $\deg f' \in \{1, 0, -\infty\}$, and each occurs. Write $f = [2]x^3 + f_2x^2 + f_1x + f_0$. Then

$$f' = (3 \cdot [2])x^2 + (2 \cdot f_2)x + f_1 = (2 \cdot f_2)x + f_1,$$

since $3 \cdot [2] = [6] = [0]$. So $\deg f' \leq 1$ (Definition 4.3.1). Witnesses: $[2]x^3 + x^2$ has derivative $[2]x$, of degree 1; $[2]x^3 + x$ has derivative 1, of degree 0; $[2]x^3$ has derivative 0, of degree $-\infty$. The school rule "degree drops by one" fails because $3 \cdot [2] = [0]$: the leading coefficient of f' would be $(3 \cdot 1)\operatorname{lc}(f)$, and here that product is 0.

(d) For $i = 0$ the monomial $u = ax^0$ is a constant, and (M) gives $u' = 0$, not $(0 \cdot a)x^{-1}$: the exponent $i - 1 = -1$ is not in $\mathbb{N}$, so x^{i-1} has no meaning. The general computation, which writes $u' = (i \cdot a)x^{i-1}$, therefore cannot be used, and the case is checked directly.

4.5.4.2 B. Practice

Exercise. B1: The chain rule

Let R be a commutative ring and $f, g \in R[x]$. Prove that

$$(f \circ g)' = (f' \circ g)\, g'.$$

Check the formula on $f = x^2$, $g = x^2 + 1$ over $\mathbb{Z}$.

Solution. Fix g, and define $\Phi, \Psi \colon R[x] \to R[x]$ by

$$\Phi(f) := (f \circ g)', \qquad \Psi(f) := (f' \circ g)\, g'.$$

The move is the one of the product rule: check on monomials, extend by additivity.

Additivity. By Definition 4.4.3 and Theorem 4.4.2 (a), $u \mapsto u \circ g$ is a ring homomorphism $R[x] \to R[x]$ that fixes the constants and sends x to g; in particular $(f+h)\circ g = f\circ g + h\circ g$. With Theorem 4.5.1 (a),

$$\Phi(f+h) = (f\circ g + h\circ g)' = \Phi(f) + \Phi(h),$$

and, using also (F9) of $R[x]$,

$$\Psi(f+h) = (f'\circ g + h'\circ g)\, g' = \Psi(f) + \Psi(h).$$

Monomials. Let $f = ax^n$ with $a \in R$, $n \in \mathbb{N}$. By Theorem 4.2.4 (c), ax^n is the product of the constant a and the n-th power of x; a ring homomorphism preserves products and powers (Definition 4.4.2), so $(ax^n)\circ g = ag^n$.

If $n = 0$, then $f = a$ and $f \circ g = a$, so $\Phi(f) = 0$ by Theorem 4.5.1 (a). Also $f' = 0$, and $0 \circ g = 0$ because a ring homomorphism sends 0 to 0 (Definition 4.4.2); so $\Psi(f) = 0 \cdot g' = 0$.

If $n \geq 1$, then by Theorem 4.5.1 (a) and (c),

$$\Phi(f) = (ag^n)' = a\,(g^n)' = a\,(n\cdot 1)\, g^{n-1} g'.$$

On the other side $f' = (n\cdot a)x^{n-1}$ by (M), so $f'\circ g = (n\cdot a)g^{n-1}$ and $\Psi(f) = (n\cdot a)g^{n-1}g'$. The constants agree: $a(n\cdot 1) = (n\cdot 1)a = n\cdot a$, by (F6) and Lemma 4.1.1 (d), and constants multiply as in R (Theorem 4.2.4 (b)). So $\Phi(f) = \Psi(f)$.

By Lemma 4.2.3 with one argument and $T = R[x]$, $\Phi = \Psi$, which is the chain rule.

Check. Over $\mathbb{Z}$, $f\circ g = (x^2+1)^2 = x^4 + 2x^2 + 1$, whose derivative is $4x^3 + 4x$. On the other side, $f' = 2x$, $f'\circ g = 2(x^2+1)$ and $g' = 2x$, so $(f'\circ g)g' = 4x^3 + 4x$.

Exercise. B2: Higher derivatives

For $n, k \in \mathbb{N}$ write $P(n,k)$ for the product $n(n-1)\cdots(n-k+1)$ of k factors, defined by $P(n,0) := 1$ and $P(n,k+1) := P(n,k)\,(n-k)$; it is a natural number for $k \leq n$.

(a) Let R be a commutative ring. Show that $(x^n)^{(k)} = (P(n,k)\cdot 1)x^{n-k}$ for $k \leq n$, and $(x^n)^{(k)} = 0$ for $k > n$.

(b) Let p be a prime. Show that $f^{(p)} = 0$ for every $f \in \mathbb{F}_p[x]$.

Solution.

(a) Induction on $k \leq n$. For $k = 0$, $(x^n)^{(0)} = x^n = (1\cdot 1)x^n$. Let $k < n$ and suppose $(x^n)^{(k)} = (P(n,k)\cdot 1)x^{n-k}$. Since $n - k \geq 1$, (M) gives

$$\begin{aligned}(x^n)^{(k+1)} &= ((n-k)\cdot(P(n,k)\cdot 1))x^{n-k-1}\\ &= (P(n,k+1)\cdot 1)x^{n-(k+1)},\end{aligned}$$

by the rule $m\cdot(j\cdot b) = (mj)\cdot b$ of Lemma 4.1.1 (d) and $(n-k)P(n,k) = P(n,k+1)$ in $\mathbb{N}$. This proves the formula for $k \leq n$. At $k = n$ the polynomial $(x^n)^{(n)}$ is a constant, so $(x^n)^{(n+1)} = 0$ by (M), and the derivative of 0 is 0; by induction, $(x^n)^{(k)} = 0$ for every $k > n$.

(b) *The coefficients of $f^{(k)}$.* Let R be any commutative ring and $f \in R[x]$. We show by induction on k that

$$\left(f^{(k)}\right)_j = P(j+k,k)\cdot f_{j+k} \qquad \text{for every } j \in \mathbb{N}.$$

For $k = 0$ both sides are f_j. If it holds for k, then by Definition 4.5.1 and Lemma 4.1.1 (d),

$$\begin{aligned}\left(f^{(k+1)}\right)_j &= (j+1)\cdot\left(P(j+k+1,k)\cdot f_{j+k+1}\right)\\ &= \left(P(j+k+1,k)(j+1)\right)\cdot f_{j+k+1} = P(j+k+1,k+1)\cdot f_{j+k+1},\end{aligned}$$

since the factor added by the recursion is $(j+k+1)-k = j+1$.

The case $k = p$ over $\mathbb{F}_p$. The number $P(j+p,p) = (j+p)(j+p-1)\cdots(j+1)$ is a product of the p consecutive integers $j+1,\ldots,j+p$. Divide $j = qp+r$ with $0 \le r < p$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2); then $j+(p-r) = (q+1)p$, and $1 \le p-r \le p$, so one of the factors is divisible by p. A product with a factor divisible by p is divisible by p (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (c), one factor at a time). So $P(j+p,p) = Mp$ with $M \in \mathbb{Z}$, and

$$P(j+p,p)\cdot f_{j+p} = M\cdot(p\cdot f_{j+p}) = M\cdot((p\cdot 1)f_{j+p}) = M\cdot 0 = 0,$$

by Lemma 4.1.1 (d), which allows integer multiples, $p\cdot 1 = 0$ in $\mathbb{F}_p$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (d)), Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (b) and $M\cdot 0 = 0$. So every coefficient of $f^{(p)}$ is 0. For instance, over $\mathbb{F}_3$, $(x^4)''' = (P(4,3)\cdot 1)x = (24\cdot 1)x = 0$.

4.5.4.3 C. Going deeper

Exercise. C1: Derivations

Let R be a commutative ring, and let $\delta\colon R[x] \to R[x]$ be a map such that, for all $f, g \in R[x]$ and every constant a,

$$\delta(f+g) = \delta(f)+\delta(g), \qquad \delta(a) = 0, \qquad \delta(fg) = \delta(f)g + f\delta(g).$$

Prove that $\delta(f) = f'\,\delta(x)$ for every $f \in R[x]$. Deduce that $f \mapsto f'$ is the only such map with $\delta(x) = 1$.

Solution. Both sides are additive in f. δ is additive by hypothesis, and $f \mapsto f'\delta(x)$ is additive by Theorem 4.5.1 (a) and (F9) of $R[x]$ (Theorem 4.2.4 (a)).

Powers of x. We show $\delta(x^n) = (n\cdot 1)x^{n-1}\delta(x)$ for every $n \ge 1$, by induction. For $n = 1$, $(1\cdot 1)x^0\delta(x) = \delta(x)$. If it holds for n, then, since $x^{n+1} = x^n x$,

$$\begin{aligned}\delta(x^{n+1}) &= \delta(x^n)x + x^n\delta(x) = (n\cdot 1)x^{n-1}\delta(x)\,x + x^n\delta(x)\\ &= (n\cdot 1+1)x^n\delta(x) = ((n+1)\cdot 1)x^n\delta(x),\end{aligned}$$

by (F5), (F6), (F7), (F9) of $R[x]$, $x^{n-1}x = x^n$, and the recursion of multiples. Also $\delta(x^0) = \delta(1) = 0$, since 1 is a constant.

Monomials. Let $a \in R$ and $n \in \mathbb{N}$. By Theorem 4.2.4 (c), ax^n is the product of the constant

a and x^n, so

$$\delta(ax^n) = \delta(a)x^n + a\,\delta(x^n) = a\,\delta(x^n).$$

If $n = 0$, this is $0 = (ax^0)'\delta(x)$, by (M). If $n \geq 1$, it is $a(n \cdot 1)x^{n-1}\delta(x) = (n \cdot a)x^{n-1}\delta(x) = (ax^n)'\delta(x)$, by (F6), Lemma 4.1.1 (d) and (M).

Conclusion. The two additive maps δ and $f \mapsto f'\delta(x)$ agree on every monomial, so they are equal by Lemma 4.2.3 (one argument, $T = R[x]$).

Uniqueness. The formal derivative satisfies the three conditions, by Theorem 4.5.1 (a) and (b), and $x' = 1$ (Example (Formal derivatives in five rings) (ii)). If δ satisfies them with $\delta(x) = 1$, then $\delta(f) = f' \cdot 1 = f'$ for every f.

Marking scheme. (10 points) - 2: both sides additive in f, with the additivity of $f \mapsto f'\delta(x)$ justified. - 2: $\delta(ax^n) = a\,\delta(x^n)$ from the product condition and $\delta(a) = 0$. - 3: $\delta(x^n) = (n \cdot 1)x^{n-1}\delta(x)$ by induction, with the case $n = 0$ handled separately. - 2: comparison with $(ax^n)'$, using $a(n \cdot 1) = n \cdot a$. - 1: conclusion by extending from monomials, and the uniqueness statement.

A solution that shows instead that $K := \{f \in R[x] : \delta(f) = f'\delta(x)\}$ is all of $R[x]$ is marked on the same points: closure of K under $+$ earns the first 2; the constants and x in K earn the next 2; closure of K under products, by Theorem 4.5.1 (b), earns the 3; $K = R[x]$ earns the 2; the uniqueness statement earns the last 1.

Fatal errors (0 for the step): checking only on x^n, with no account of the coefficient a (that is where $\delta(a) = 0$ is needed); writing x^{-1} in the case $n = 0$.

Exercise. C2: Find the error

Here is an argument.

> **Claim.** If $f \in \mathbb{Q}[x]$ and $f' = 0$, then f is constant.
>
> **Proof.** (1) For $k \geq 1$, the coefficient of x^{k-1} in f' is $k \cdot f_k = (k \cdot 1)f_k$, by the definition of f' and the rules for multiples. (2) Since $f' = 0$, $(k \cdot 1)f_k = 0$ for every $k \geq 1$. (3) For $k \geq 1$ we have $k \neq 0$, so $k \cdot 1 \neq 0$; since $\mathbb{Q}$ has no zero divisors, $f_k = 0$ for every $k \geq 1$. (4) So $f = f_0x^0$ is constant.

Is the claim true? Does the argument prove it? Name the line that fails and the reason, give a counterexample to the illegal step, and repair the argument.

Solution. **The claim is true:** it is Proposition 4.5.2 (a) for $F = \mathbb{Q}$. **The argument, as written, does not prove it.**

Lines (1), (2) and (4) are correct: (1) is Definition 4.5.1 with Lemma 4.1.1 (d), (2) reads $f' = 0$ coefficient by coefficient, and (4) compares coefficients (Definition 4.1.1). The second half of line (3) is correct too: $\mathbb{Q}$ is a field (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.4.3), so it has no zero divisors (Theorem 2.1.1 (f)).

Line (3) fails, in its first half. "$k \neq 0$ in $\mathbb{Z}$, so $k \cdot 1 \neq 0$ in the ring" is a general "fact" that is neither proved nor true, and the line uses nothing about $\mathbb{Q}$ to support it: entry (N9) of Logic and Proof, Example (What is not allowed). *Counterexample to the step:* in $\mathbb{F}_2$, $k = 2$ gives $2 \cdot 1 = 1 + 1 = 0$. The same four lines, read over $\mathbb{F}_2$, would "prove" that x^2 is constant,

since $(x^2)' = 0$ (Example (Formal derivatives in five rings) (iii)). There is no counterexample to the conclusion, which is true.

Repair. What line (3) needs is that $\mathbb{Q}$ has characteristic 0 (Definition 2.5.1): for $k \geq 1$, $k \cdot 1$ is the rational number k (induction on k, since the embeddings $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$ preserve sums and 1, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.2.3 and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.4.4), and $k \neq 0$. With that sentence in place of "so", the argument is the proof of Proposition 4.5.2 (a), whose hypothesis is exactly the characteristic.

Marking scheme. (10 points) - 2: says the claim is true and that the argument, as written, does not prove it. - 3: names the first half of line (3) and the reason: $k \neq 0$ does not give $k \cdot 1 \neq 0$ in a general ring, (N9), or an equivalent statement. - 2: a counterexample to the step, such as $2 \cdot 1 = 0$ in $\mathbb{F}_2$, or the "proof" that x^2 is constant over $\mathbb{F}_2$. - 3: repairs the step by proving $k \cdot 1 \neq 0$ in $\mathbb{Q}$ for every $k \geq 1$, that is, $\operatorname{char} \mathbb{Q} = 0$. Two routes earn full marks: $k \cdot 1 = k$ via the embeddings, as in the solution; or $k \cdot 1 > 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h), since $\mathbb{Q}$ is an ordered field (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.5.1) with $1 \neq 0$. Fatal errors (0 for the step): a counterexample to the conclusion (there is none); blaming the no-zero-divisors half of line (3), which is correct.

4.5.4.4 R. Review

Exercise. R1

Let R be a commutative ring and $E\colon R[x] \to R[x]$, $E(f) \coloneqq f + f'$. Show that E is an injective homomorphism of the group $(R[x], +)$ to itself. If $1 \neq 0$ in R, show that $E(fg) = E(f)E(g)$ fails for some f, g.

Solution. The tools are the notion of a group homomorphism and its kernel, Definition 3.3.1, written additively (Definition 3.1.1), and Proposition 3.3.3.

The group. By Theorem 4.2.4 (a), $R[x]$ satisfies (F1)–(F4), so $(R[x], +)$ is an abelian group, with identity the zero polynomial and inverse $-f$.

A homomorphism. By Theorem 4.5.1 (a) and (F1), (F2) of $R[x]$,

$$E(f+g) = (f+g) + (f'+g') = (f+f') + (g+g') = E(f) + E(g),$$

which is the homomorphism condition in additive notation.

The kernel is $\{0\}$. Let $f \neq 0$, with $n \coloneqq \deg f$, so $f_n \neq 0$ and $f_{n+1} = 0$ (Definition 4.3.1). By Definition 4.5.1, $(f')_n = (n+1) \cdot f_{n+1} = (n+1) \cdot 0 = 0$, as in the well-definedness paragraph after it. Addition is coefficientwise (Definition 4.2.1), so $E(f)_n = f_n + 0 = f_n \neq 0$, and $E(f) \neq 0$. Also $0 = 0x^0$, so $0' = 0$ by (M), and $E(0) = 0 + 0 = 0$ by (F3) of $R[x]$. So $\ker E = \{0\}$, and E is injective by Proposition 3.3.3.

Not multiplicative. Take $f = g = x$. By Example (Formal derivatives in five rings) (ii), $x' = 1$, so $E(x) = x + 1$, and $E(x)E(x) = (x+1)^2 = x^2 + 2x + 1$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d). On the other side, (M) gives $(x^2)' = (2 \cdot 1)x = 2x$, so $E(x^2) = x^2 + 2x$. The two differ in position 0, where they have 1 and 0; since $1 \neq 0$, $E(x \cdot x) \neq E(x)E(x)$. So only the group structure of $R[x]$ is respected, and E is not a ring

homomorphism.

Exercise. R2

For $f \in \mathbb{R}[x]$ and $z \in \mathbb{C}$, let $f(z)$ denote the value obtained by substituting z for x, where a real coefficient a is read as the complex number a. Show that $f(\overline{z}) = \overline{f(z)}$. Deduce that if $z_0 \in \mathbb{C}$ is a root of f that is not real, then $\overline{z_0}$ is a different root of f.

Solution. The tool is the uniqueness in Theorem 4.4.2 (b), applied to the field $\mathbb{C}$ of Chapter 1.

The setting. $\mathbb{C}$ is a field, and $\mathbb{R} \subseteq \mathbb{C}$ is closed under its operations (Theorem 1.2.4); so $\mathbb{C}$ and $\mathbb{R}$ are commutative rings and $\mathbb{R}[x]$ is defined. Let $\iota\colon \mathbb{R} \to \mathbb{C}$ be the map of Proposition 1.1.1; it preserves $+$, $\cdot$ and 1, so it is a ring homomorphism (Definition 4.4.2). For $s \in \mathbb{C}$, let $\Phi_s\colon \mathbb{R}[x] \to \mathbb{C}$ be the homomorphism of Theorem 4.4.2 with $\varphi = \iota$ and this s; then $f(z)$ means $\Phi_z(f)$.

Conjugation is a ring homomorphism. By Theorem 1.2.2 (a) and (b), $\overline{u+v} = \overline{u} + \overline{v}$ and $\overline{uv} = \overline{u}\,\overline{v}$, and $\overline{1} = 1$, since $1 = 1 + 0i$ and $\overline{1} = 1 - 0i = 1$ (Definition 1.2.1).

Two homomorphisms. Let $A(f) \coloneqq \overline{\Phi_z(f)}$ and $B(f) \coloneqq \Phi_{\overline{z}}(f)$. Then A is a composite of ring homomorphisms, hence one (Definition 4.4.2), and B is one by Theorem 4.4.2 (a). On a constant $a \in \mathbb{R}$, $A(a) = \overline{\iota(a)} = \iota(a)$, since $a = a + 0i$ has conjugate $a - 0i = a$; and $B(a) = \iota(a)$. On x, $A(x) = \overline{z} = B(x)$. By the uniqueness in Theorem 4.4.2 (b), $A = B$: $\overline{f(z)} = f(\overline{z})$ for every $f \in \mathbb{R}[x]$.

Roots. If $f(z_0) = 0$, then $f(\overline{z_0}) = \overline{0} = 0$. If $z_0 = a + bi$ is not real, then $b \neq 0$, so $\overline{z_0} = a - bi \neq a + bi$: equality would give $-b = b$ by comparing imaginary parts (Definition 1.1.1), so $2b = 0$, and $b = 0$ because $2 = 2 \cdot 1 \neq 0$ in the ordered field $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h)) and $\mathbb{R}$ has no zero divisors (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (f)). So the non-real roots of a real polynomial come in pairs $z_0 \neq \overline{z_0}$.

The identity and the first deduction are the statement of Proposition 1.6.4, and the distinctness of $\overline{z_0}$ is the paragraph after it; Chapter 1 proved both by a direct computation with the sum $\sum_k a_k z^k$. Here the computation is replaced by the uniqueness of a substitution homomorphism. Polynomials with rational coefficients are a special case, since $\mathbb{Q}$ sits inside $\mathbb{R}$.

Exercise. R3

Show that $\mathbb{Z}[x]$ and $\mathbb{F}_2[x]$ are countable, and that the set of all sequences $\mathbb{N} \to \mathbb{F}_2$ is uncountable. Which clause of the definition of a polynomial does the difference rest on?

Solution. The tools are the countability results of *Sets, Relations, and Cardinality*, Chapter 3, read on $\mathbb{N} = \omega$ through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3.

$\mathbb{Z}$ and $\mathbb{F}_2$ are countable. $\mathbb{N} \times \mathbb{N}$ is countable (Sets, Relations, and Cardinality, Theorem 3.2.6). The class map $\mathbb{N} \times \mathbb{N} \to \mathbb{Z} = (\mathbb{N} \times \mathbb{N})/{\sim}$ is surjective (Sets, Relations, and Cardinality,

Definition 2.5.4), so $\mathbb{Z}$ is countable by Sets, Relations, and Cardinality, Proposition 3.2.4; this is the count of Number Systems: From \(\nN\) to \(\nR\), Exercise (R2). The map $\mathbb{N} \to \mathbb{F}_2$, $n \mapsto [n]$, is surjective, since every class is [0] or [1] (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b)); so $\mathbb{F}_2$ is countable (Sets, Relations, and Cardinality, Definition 3.2.1).

Polynomials of bounded length. Let R be $\mathbb{Z}$ or $\mathbb{F}_2$, and for $N \in \mathbb{N}$ let $A_N \coloneqq \{f \in R[x] : f_k = 0 \text{ for every } k > N\}$. By Exercise (B1: Polynomials of bounded length as tuples), A_N is in bijection with R^{N+1}. For $N \geq 1$, R^{N+1} is countable by Sets, Relations, and Cardinality, Corollary 3.2.7 (b); for $N = 0$ it is R itself. So each A_N is countable, as the image of a countable set under a bijection (Sets, Relations, and Cardinality, Proposition 3.2.4).

The union. Every polynomial lies in some A_N (Definition 4.1.1), so $R[x] = \bigcup_{N \in \mathbb{N}} A_N$, a countable union of countable sets, which is countable by Sets, Relations, and Cardinality, Theorem 3.3.3 (a). (That theorem uses the axiom of countable choice to pick a list of each A_N.)

All sequences. The set $\{0,1\}^{\mathbb{N}}$ is uncountable (Sets, Relations, and Cardinality, Theorem 3.4.1). The map $\{0,1\} \to \mathbb{F}_2$, $0 \mapsto [0]$, $1 \mapsto [1]$, is a bijection; composing a sequence with its inverse turns every sequence $\mathbb{N} \to \mathbb{F}_2$ into a sequence of zeros and ones, and this is a surjection onto $\{0,1\}^{\mathbb{N}}$. If the sequences $\mathbb{N} \to \mathbb{F}_2$ were countable, so would be $\{0,1\}^{\mathbb{N}}$, by Sets, Relations, and Cardinality, Proposition 3.2.4. So they are uncountable.

The clause. The difference is the clause **only finitely many** of Definition 4.1.1: a polynomial is a sequence that is 0 from some point on, so it is determined by a finite tuple, and there are countably many finite tuples. A general sequence carries infinitely many independent choices. The same count, with the polynomials written as integer tuples, is the proof of Sets, Relations, and Cardinality, Theorem 3.3.4.

Exercise. R4

Find all $f \in \mathbb{Q}[x]$ with $f \circ x^2 = f^2$.

Solution. **Answer:** $f = 0$, and $f = x^n$ for $n \in \mathbb{N}$.

They work. $0 \circ x^2 = 0 = 0^2$, and $x^n \circ x^2 = (x^2)^n = x^{2n} = (x^n)^2$ by Definition 4.4.3 and the power laws (Lemma 4.1.1 (c)).

The tool is **look at the top coefficient**, then at the next non-zero one. Let $f \neq 0$ satisfy $f \circ x^2 = f^2$, with $n \coloneqq \deg f$ and $a \coloneqq \operatorname{lc}(f)$. As in the proof of Proposition 4.5.2 (b), $f \circ x^2 = \sum_{j=0}^{n} f_j x^{2j}$, whose coefficient at $2j$ is f_j and whose coefficients at odd positions are 0. So its coefficient at $2n$ is a, and none beyond $2n$ is non-zero. By Theorem 4.3.2 (b), since $\mathbb{Q}$ has no zero divisors, f^2 has degree $2n$ and leading coefficient a^2. Hence $a^2 = a$, so $a(a-1) = 0$, and $a = 1$ since $a \neq 0$ (Theorem 2.1.1 (f)).

Now let $r \coloneqq f - x^n$, so $f = x^n + r$ and $\deg r < n$ (Theorem 4.3.1, since the coefficients at n cancel). Suppose $r \neq 0$, and let $k \coloneqq \deg r < n$. By Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (d) in the commutative ring $\mathbb{Q}[x]$ (Theorem 4.2.4 (a)),

$$f^2 = x^{2n} + 2x^n r + r^2.$$

Its coefficient at $n+k$ is $2r_k$: x^{2n} contributes 0, since $n+k < 2n$; $2x^n r$ contributes $2r_k$, since

multiplying by x^n shifts by n (Lemma 4.2.2 (a)); and r^2 contributes 0, since $\deg r^2 \leq 2k < n+k$ (Theorem 4.3.2 (a)). On the other side, the coefficient of $f \circ x^2$ at $n+k$ is 0: if $n+k$ is odd, it is an odd position; if $n+k = 2j$, then $k < j < n$, so $f_j = r_j = 0$, because $j < n$ and $j > \deg r$. Hence $2r_k = 0$ in $\mathbb{Q}$, and $r_k = 0$ since $2 \neq 0$: a contradiction with $r_k = \operatorname{lc}(r) \neq 0$. So $r = 0$ and $f = x^n$.

Why the look-alikes fail. Evaluating at points gives $f(c^2) = f(c)^2$ for every $c \in \mathbb{Q}$, a statement about polynomial functions; turning it back into a statement about coefficients needs the fact that a polynomial over an infinite field is determined by its values, which this chapter does not prove (Proposition 4.4.4 (d) shows that over a finite ring with $1 \neq 0$ it is false). Differentiating with the chain rule of Exercise B1 gives $2x\,(f' \circ x^2) = 2ff'$, an equation of the same kind and no easier.

Over $\mathbb{F}_2$ every f works. There $(u+v)^2 = u^2 + v^2$, since $2uv = 0$, and $c^2 = c$ for $c \in \mathbb{F}_2$; so $f^2 = \sum_k f_k^2 x^{2k} = \sum_k f_k x^{2k} = f \circ x^2$. The step that fails is "$2r_k = 0$ implies $r_k = 0$": in $\mathbb{F}_2$, $2 = 0$.

Chapter 5

Polynomials over a Field

Number Systems: From $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3 did arithmetic in $\mathbb{Z}$: divide with a remainder, take the least positive element of a set closed under combinations, and the greatest common divisor, Bézout's identity, Euclid's lemma and unique factorization follow. Chapter 4 built the ring $F[x]$ and its degree, but it did not divide one polynomial by another with a remainder. This chapter shows that over a field F the polynomials have the same arithmetic, with the degree in the part of the size and "monic" in the part of "positive". It also proves what $\mathbb{Z}$ has no analogue for. A polynomial can be **evaluated**, so it has roots, and roots occupy the second half of the chapter. A root c is a factor $x - c$; a non-zero polynomial has no more distinct roots than its degree; a repeated root shows up in the formal derivative of Section 4.5; and values at enough points determine a polynomial, which is interpolation. Interpolation turns out to be the Chinese remainder theorem for the moduli $x - c$, and the ring $F[x]/\langle m \rangle$, built by *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3's quotient construction, is a field exactly when m is irreducible.

The chapter ends with the question that algebra courses usually leave to analysis: does every non-constant complex polynomial have a root? It does, and Section 5.6 proves it with no convergent sequences, no compactness, no continuity theorem and no polar form. The one analytic input is the supremum property of $\mathbb{R}$. It is used directly twice, to find a point where $|p|$ is smallest, and indirectly through the real square roots behind the modulus and behind the complex square roots. The factorization of real polynomials into linear factors and quadratics without real roots follows.

Two rings, one arithmetic. The first half of the chapter runs *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3 again, with these substitutions.

In $\mathbb{Z}$	In $F[x]$
the size of an integer	the degree
the units ± 1	the units, the non-zero constants
positive	monic
division with remainder	Theorem 5.1.2
Bézout's theorem, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.2.1	Theorem 5.2.2
primes	monic irreducible polynomials
unique factorization, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.3.5	Theorem 5.3.6
the ring $\mathbb{Z}/n\mathbb{Z}$	the ring $F[x]/\langle m \rangle$, Theorem 5.5.2

In $\mathbb{Z}$	In $F[x]$
$\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2	$F[x]/\langle m\rangle$ is a field iff m is irreducible, Theorem 5.5.3
the Chinese remainder theorem, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3	Theorem 5.5.5, for any number of moduli

Each polynomial proof is written out in full. The integer twins are compared with, never cited as a reason for a polynomial statement. The general facts about ideals, quotient rings and units are cited, not proved again. Integers enter only as integers: as coefficients, in the rational root test of Section 5.3 and the integer polynomials of Section 5.1, and as degrees and exponents.

What you need. Chapter 4 above all, and Chapter 2; Chapter 1 for Section 5.6 and a few examples; *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3 for comparison and for the general theorems it proved once, and its $\mathbb{R}$ for Section 5.6; *Sets, Relations, and Cardinality*, Chapters 1–3; and induction from *Logic and Proof*, Chapter 3.

- From Chapter 4: the ring $F[x]$ and its laws (Definition 4.1.1, Definition 4.2.1, Theorem 4.2.4, Lemma 4.1.1, Lemma 4.2.2); the degree and the leading coefficient, with the degree of a sum and of a product, the absence of zero divisors and the units (Definition 4.3.1, Theorem 4.3.1, Theorem 4.3.2, Example (Which Rings Are Integral Domains), Corollary 4.3.3, Proposition 4.3.4); evaluation, substitution and ring homomorphisms (Definition 4.4.1, Theorem 4.4.1, Theorem 4.4.2, Definition 4.4.2), with the polynomial over $\mathbb{F}_2$ that vanishes everywhere (Example (Different Polynomials, Equal Functions)); and, for Sections 5.4 and 5.5, the formal derivative and its rules (Definition 4.5.1, Theorem 4.5.1, Proposition 4.5.2).
- From Chapter 2: fields and the rule that a product of non-zero elements is non-zero (Definition 2.1.1, Theorem 2.1.1); the fields $\mathbb{F}_p$ (Definition 2.2.1); subfields (Definition 2.3.1, Proposition 2.3.1), for Section 5.2; the characteristic, integer multiples and Fermat's little theorem (Definition 2.5.1, Example (The characteristics of the standard fields), Lemma 2.5.1, Theorem 2.6.6), for Sections 5.4 and 5.5; and, in Section 5.6, the field $\mathbb{Q}(i)$ and complex conjugation (Example (Rational and Integer Complex Numbers), Example (Conjugation and Other Automorphisms)). Section 5.5 meets the four-element field of Exercise (C1: A Field with Four Elements) again, and Exercise R2 of Section 5.6 returns to Example (The Field Generated by the Square Root of Two).
- From Chapter 1, for Section 5.6 (and the difference of powers also for Exercises B2 and B3 of Section 5.1): the complex numbers as a field containing $\mathbb{R}$ (Definition 1.1.1, Theorem 1.2.4, Proposition 1.1.1); the conjugate and the modulus and their rules (Definition 1.2.1, Theorem 1.2.2, Proposition 1.2.1, Lemma 1.3.1); the triangle inequality and its variants (Theorem 1.3.2, Corollary 1.3.3); powers (Proposition 1.1.3, Lemma 1.1.4); complex square roots (Proposition 1.4.1); and conjugate roots (Proposition 1.6.4). Sections 5.2 and 5.5 use $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ in examples, and Exercise B3 of Section 5.5 compares $\mathbb{R}[x]/\langle x^2+1\rangle$ with $\mathbb{C}$. Chapter 1's polar form and k-th roots are not used, and Chapter 3 is not used.
- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3: ideals, quotient rings and units (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1, Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1), cited for $F[x]$; the rules for divisibility, Euclid's lemma and fractions in lowest terms (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1, Number Systems: From

\(\nN\) to \(\nR\), Theorem 3.3.1, Number Systems: From \(\nN\) to \(\nR\), Proposition 3.3.6), for the rational root test; even and odd integers (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3); the integer gcd and its Euclidean step (Number Systems: From \(\nN\) to \(\nR\), Definition 3.2.2, Number Systems: From \(\nN\) to \(\nR\), Lemma 3.2.3), in two exercises; and the integer twins compared with in Sections 5.1–5.5: those in the table above and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.2, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.2.4, Number Systems: From \(\nN\) to \(\nR\), Exercise (C2: Scaling the gcd), Number Systems: From \(\nN\) to \(\nR\), Lemma 3.3.4, Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1.

- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapters 1 and 2: $\mathbb{N} = \omega$, its order and well-ordering, and even and odd exponents (Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3, Number Systems: From \(\nN\) to \(\nR\), Theorem 1.6.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 1.6.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 1.6.4); commutative rings and the rules of an ordered ring (Number Systems: From \(\nN\) to \(\nR\), Definition 2.3.1, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5); greatest elements of bounded sets of integers (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6), for multiplicities; the irrationality of $\sqrt{2}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1), and the gap at $\sqrt{2}$ in $\mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.2), in Exercise C1 of Section 5.6; and maps on classes (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.2.1), for the Chinese remainder theorem.
- From *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapters 4–6, for Section 5.6: absolute values and powers in an ordered field (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3, Number Systems: From \(\nN\) to \(\nR\), Definition 4.2.1), from Chapter 4; $\mathbb{R}$ as a complete ordered field, its Archimedean property and the bound on powers of 2 (Number Systems: From \(\nN\) to \(\nR\), Definition 5.6.1, Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3, Number Systems: From \(\nN\) to \(\nR\), Theorem 5.4.2, Number Systems: From \(\nN\) to \(\nR\), Lemma 5.6.1), with Number Systems: From \(\nN\) to \(\nR\), Example (Picking Representatives Is a Use of Choice) compared with, from Chapter 5; and non-negative square roots in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), from Chapter 6, which also supply $\sqrt{2}$ for examples in Sections 5.2–5.5.
- From *Sets, Relations, and Cardinality*: bijections (Sets, Relations, and Cardinality, Definition 1.4.5), from Chapter 1; the well-ordering of $\mathbb{N}$, the recursion theorem with its finite sums and products, equivalence classes and quotient sets, and suprema and infima (Sets, Relations, and Cardinality, Theorem 2.1.3, Sets, Relations, and Cardinality, Theorem 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.1, Sets, Relations, and Cardinality, Theorem 2.5.1, Sets, Relations, and Cardinality, Definition 2.5.4, Sets, Relations, and Cardinality, Definition 2.6.5), from Chapter 2; and finite and infinite sets (Sets, Relations, and Cardinality, Definition 3.1.2, Sets, Relations, and Cardinality, Definition 3.1.3, Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations, and Cardinality, Proposition 3.1.5), from Chapter 3, for Section 5.4 and Exercise C3 of Section 5.3.
- From *Logic and Proof*: induction and strong induction (Logic and Proof, Axiom 4.2.1, Logic and Proof, Theorem 4.2.2), from Section 3.2, and, for the two find-the-error exercises, the catalogue of moves that are not allowed (Logic and Proof, Example (What is not allowed)), from Section 5.6.

Time. About 30 hours on the core track (all of A, one B and one C per section, the exit checks); about 45 hours for everything.

5.0.1 Roadmap

- **Division with Remainder.** Divisibility over a field, associates and the one monic associate of a non-zero polynomial; division with remainder, with existence by an element of least degree and uniqueness by comparing degrees, and long division over $\mathbb{Q}$ and $\mathbb{F}_3$; and the remainder and factor theorems, which make a root c the same thing as a factor $x - c$.
- **Ideals, the Greatest Common Divisor, and the Euclidean Algorithm.** The ideal generated by finitely many polynomials; every ideal of $F[x]$ generated by exactly one monic polynomial; the gcd defined as the monic common divisor that every common divisor divides, with Bézout's theorem and coprimality; the Euclidean algorithm as a recursively defined sequence, with back-substitution; and division and the gcd unchanged when the field is enlarged.
- **Irreducible Polynomials and Unique Factorization.** Irreducibility over a field, decided by roots in degrees 2 and 3 and not beyond, as $x^4 + 4$ shows; Euclid's lemma and its consequences for irreducibles; an irreducible factor of least degree; unique factorization into monic irreducibles, with uniqueness stated by a bijection of indices; the factorizations of $x^4 - 1$ over five fields; and the rational root test.
- **Roots, Multiplicity, and the Formal Derivative.** At most n roots for a non-zero polynomial of degree n; a polynomial fixed by its values at $n + 1$ points, and over an infinite field by its function, but not over $\mathbb{F}_p$; the expansion in powers of $x - c$; multiplicity, splitting off all roots, and splitting over a field; and repeated roots and repeated factors detected by the formal derivative and by $\gcd(f, f')$.
- **Interpolation, Quotient Rings, and the Chinese Remainder Theorem.** Lagrange polynomials and the unique interpolating polynomial of degree at most n; congruence modulo a polynomial and the ring $F[x]/\langle m \rangle$, named by the remainders and a field exactly when m is irreducible, with a field of four elements and a copy of $\mathbb{C}$; the Chinese remainder theorem for any number of pairwise coprime moduli; interpolation as its case of linear moduli; and values and derivatives prescribed at once.
- **The Fundamental Theorem of Algebra.** Why the field axioms cannot suffice; a growth bound and a Lipschitz bound in place of continuity; the minimum of $|p|$, found by nested squares and two uses of the supremum property; d'Alembert's lemma, with its direction found by square roots instead of polar form; the theorem and the splitting of complex polynomials; and real polynomials, whose irreducible factors are linear or quadratic without real root, so that one of odd degree has a real root. Review exercises return to Chapters 2 and 4 and to *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3.

5.0.2 Named moves

- **Least degree, then divide.** In a set of polynomials closed under the right operations, take a non-zero element d of least degree and divide any element of the set by d; the remainder lies in the set and has smaller degree, so it is 0. It is *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3's "least positive element, then divide", with degree in place of size. Named in Section 5.2, it proves there that every ideal of $F[x]$ has one monic generator (Theorem 5.2.1), and Bézout's theorem with it; its first, unnamed use is the existence half of division with remainder in Section 5.1. Exercise C1 of Section 5.2 asks for the whole proof, Exercise B2 of Section 5.3 leaves its last step to you, and Exercise C2 of Section 5.6 asks you to name it and carry it out.
- **Evaluate at a root.** In $f = qg + r$, evaluate at a root of g: the term qg vanishes, and the value of r is read off. Named in Section 5.1, it proves the remainder theorem and finds remainders without dividing (Example (Remainders without dividing), Exercise C2). In Section 5.5 it makes each Lagrange polynomial vanish at the other nodes, turns

a congruence modulo $x - c$ into a value at c (Proposition 5.5.6), and reads a value and a derivative off a congruence modulo $(x - c)^2$ (Example (Values and derivatives at once)).

- **Compare degrees.** To show that two polynomials are equal, show that their difference has smaller degree than any non-zero polynomial of its kind can have: a non-zero multiple of g has degree at least $\deg g$, and a non-zero polynomial with $n + 1$ distinct roots has degree at least $n + 1$. Named in Section 5.1, it gives the uniqueness of the quotient and the remainder in Section 5.1, of the expansion in powers of $x - c$ in Section 5.4, of the representative of degree less than $\deg m$ in each class and of the solution of the Chinese remainder theorem in Section 5.5, and, with the root count, of the polynomial through given points in Sections 5.4 and 5.5.
- **Keep the quarter that keeps the infimum.** To find a point where a quantity bounded below attains its infimum, halve a square, keep the first quarter in a fixed order whose infimum is the same, and take the point common to all the squares, which completeness supplies. It is *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 5's bisection, now in the plane, and the fixed order makes each step a rule, so no choice is made. Named in Section 5.6, it proves there that $|p|$ attains its minimum (Theorem 5.6.3); Exercise A1 there runs it for $x^2 + 1$, and Exercise C3 uses it to repair a flawed proof.
- **Multiply the Bézout identity**, reused from *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3. From $af + bg = 1$, multiply by h and read off what divides h. It proves Euclid's lemma for polynomials (Theorem 5.3.2) and the rule for coprime divisors (Proposition 5.3.4) in Section 5.3. In Section 5.5 two such identities multiplied together show that coprimality survives products (Lemma 5.5.4), the identity read modulo m gives inverses in $F[x]/\langle m \rangle$, and one identity per modulus builds the solution of the Chinese remainder theorem. That chapter's third move, computing on representatives, is not repeated: Section 5.5 cites its quotient-ring theorem.

5.1 Division with Remainder

Number Systems: From $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.1 divided -17 by 5 and kept the remainder 3: a quotient times the divisor, plus something **smaller** than the divisor. Chapter 4 built the ring $F[x]$ of polynomials over a field and gave every non-zero polynomial a degree. For polynomials, "smaller" will mean "of smaller degree". For instance, in $\mathbb{Q}[x]$,

$$x^4 + 2x^3 - x + 3 = (x^2 + x)(x^2 + x - 1) + 3,$$

and the leftover 3 has degree 0, below the degree 2 of $x^2 + x - 1$. Three questions are open. Why can one always go on until the degree drops below that of the divisor? Why is the answer unique? And where does it matter that the coefficients lie in a **field**? This section answers all three, and then uses the answer to connect a root of a polynomial with a factor of degree 1.

Throughout the chapter, F is a field (Definition 2.1.1), and $F[x]$ is the ring of polynomials over F (Definition 4.2.1), a commutative ring by Theorem 4.2.4 (a). A field is an integral domain (Example (Which Rings Are Integral Domains)), so the results of Chapter 4 stated for integral domains apply to $F[x]$. We use the degree $\deg p$ and the leading coefficient $\mathrm{lc}(p)$ of Definition 4.3.1, with $\deg 0 = -\infty$, and the conventions $-\infty < n$ and $-\infty + n = -\infty$ for $n \in \mathbb{N}$ that come with it. A constant $a \in F$ is identified with the polynomial ax^0 (Theorem 4.2.4 (b)), and $(ap)_k = ap_k$ for a constant a (Theorem 4.2.4 (d)). Numerals in F are multiples of 1: $2 := 1 + 1$, $3 := 2 + 1$, and so on, so that $2 = 0$ in $\mathbb{F}_2$ and $3 = 0$ in $\mathbb{F}_3$ (Definition 2.2.1).

5.1.1 Divisibility over a field

In $\mathbb{Z}$, "a divides b" asked whether b is some integer times a. The same question makes sense in any commutative ring, and in $F[x]$ it is the question this chapter is built on. The one new feature is that the answer can depend on the field.

A polynomial g divides f when f is g times some polynomial over the same field.

Definition 5.1.1. Divisibility of Polynomials

Let F be a field and $f, g \in F[x]$.

(a) g **divides** f **over** F, written $g \mid f$, if **there exists** $h \in F[x]$ with $f = gh$. Then g is a **divisor** (or **factor**) of f, and f is a **multiple** of g. We write $g \nmid f$ when g does not divide f.

(b) f and g are **associates** if $f = cg$ for some **non-zero** constant $c \in F$.

In words: (a) asks for a cofactor h, and the cofactor must have its coefficients in F; (b) says that two polynomials are associates when they differ by a non-zero constant factor. When two fields are in play, "$g \mid f$ in $F[x]$" names the field.

Four instances, chosen so that the same symbols give different answers:

- $x - 1 \mid x^2 - 1$ in $\mathbb{Q}[x]$, since $x^2 - 1 = (x - 1)(x + 1)$.
- $2x - 2 \mid x^2 - 1$ in $\mathbb{Q}[x]$, since $x^2 - 1 = (2x - 2)(\frac{1}{2}x + \frac{1}{2})$. The polynomials $x - 1$ and $2x - 2 = 2(x - 1)$ are associates, and the cofactor $\frac{1}{2}x + \frac{1}{2}$ needs the inverse of 2.
- $x + 1 \mid x^2 + 1$ in $\mathbb{F}_2[x]$, since $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ there: $2 = 0$ in $\mathbb{F}_2$.
- $x + 1 \nmid x^2 + 1$ in $\mathbb{Q}[x]$. Suppose $x^2 + 1 = (x + 1)h$ with $h \in \mathbb{Q}[x]$. Evaluating at -1 respects sums and products (Theorem 4.4.1), so $(-1)^2 + 1 = (-1 + 1) \cdot h(-1)$, that is, $2 = 0 \cdot h(-1) = 0$ in $\mathbb{Q}$, which is false.

Non-example by minimal change. The last two lines use the same symbols, $x + 1$ and $x^2 + 1$. Only the field changed, from $\mathbb{F}_2$ to $\mathbb{Q}$, and with it the value of 2: the evaluation argument gives $2 = 0$, which is true in $\mathbb{F}_2$ and false in $\mathbb{Q}$. So "$g \mid f$" is a statement about g, f **and** F, which is why the definition says "over F".

Degenerate cases. Every g divides 0, since $0 = g \cdot 0$. The zero polynomial divides only 0. And a non-zero constant c divides every f, since $f = c(c^{-1}f)$; this is (F8), inverses of non-zero elements, at work in general (the cofactor of $2x - 2$ above was one instance), and it means that non-zero constants are as invisible to divisibility as ± 1 were in $\mathbb{Z}$.

Quick check. In $\mathbb{F}_3[x]$, does $x + 1$ divide $x^2 + 1$? Evaluate at $-1 = 2$.

Solution. No. If $x^2 + 1 = (x + 1)h$, evaluating at 2 (Theorem 4.4.1) gives $2^2 + 1 = (2 + 1)h(2)$, that is, $5 = 0 \cdot h(2) = 0$. In $\mathbb{F}_3$, $5 = 2 \neq 0$. So $x + 1 \nmid x^2 + 1$ in $\mathbb{F}_3[x]$.

The rules below are the ones the chapter uses. Parts (a)–(d) are identities in the commutative ring $F[x]$, plus the inverse of a non-zero constant (F8) for the last clause of (a) and one degree count; parts (e) and (f) say exactly what "invisible" means.

Proposition 5.1.1. Rules for Divisibility of Polynomials

Let F be a field and $f, g, h \in F[x]$.

(a) $g \mid 0$. $0 \mid f$ if and only if $f = 0$. Every non-zero constant divides every polynomial.

(b) If $f \mid g$ and $g \mid h$, then $f \mid h$.

(c) If $h \mid f$ and $h \mid g$, then $h \mid af + bg$ for **all** $a, b \in F[x]$.

(d) If $g \mid f$ and $f \neq 0$, then $\deg g \leq \deg f$.

(e) The units of $F[x]$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1) are exactly the non-zero constants.

(f) $f \mid g$ and $g \mid f$ if and only if f and g are associates (this includes $f = g = 0$). Every non-zero f has **exactly one** monic associate, namely $\mathrm{lc}(f)^{-1} f$. Two monic polynomials that divide each other are equal.

Idea. Parts (a)–(c) are rearrangements of equations $f = gh$ by the ring laws, except that the last clause of (a) also uses c^{-1}, from (F8). Part (d) is the degree of a product: a non-zero multiple of g has degree $\deg g$ plus something in $\mathbb{N}$. Part (e) is Chapter 4's description of the units of $R[x]$, read with $R = F$. For (f), mutual divisibility gives $f = f \cdot uv$, and canceling f makes u a unit, which (e) identifies as a non-zero constant.

Proof. We use the ring laws of $F[x]$ (Theorem 4.2.4 (a)) and Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 without further mention.

(a) $0 = g \cdot 0$, so $g \mid 0$. If $0 \mid f$, then $f = 0 \cdot k = 0$ for some k; conversely $0 \mid 0$ by the first claim. If $c \in F$ is a non-zero constant, then c^{-1} exists by (F8) of Definition 2.1.1, and $f = (cc^{-1})f = c(c^{-1}f)$, so $c \mid f$.

(b) Let $g = fu$ and $h = gv$. Then $h = (fu)v = f(uv)$, so $f \mid h$.

(c) Let $f = hu$ and $g = hv$. Then $af + bg = a(hu) + b(hv) = h(au + bv)$, so $h \mid af + bg$.

(d) Let $f = gu$ with $u \in F[x]$. Since $f \neq 0$, neither g nor u is 0. The field F has no zero divisors (Theorem 2.1.1 (f)), so Theorem 4.3.2 (b) gives $\deg f = \deg g + \deg u$. Here $\deg u \in \mathbb{N}$, so $\deg g \leq \deg f$.

(e) By Proposition 4.3.4, applied to the integral domain F (Example (Which Rings Are Integral Domains)), the units of $F[x]$ are the constants that are units of F. In a field every non-zero a is a unit, by (F8), and 0 is not, since $0 \cdot v = 0 \neq 1$ for every v (Theorem 2.1.1 (d) and (F7) of Definition 2.1.1). So the units of $F[x]$ are the non-zero constants.

(f) ($\Leftarrow$) Let $f = cg$ with $c \neq 0$ a constant. Then $g \mid f$, and $g = c^{-1}f$, so $f \mid g$.

($\Rightarrow$) Let $f \mid g$ and $g \mid f$. If $f = 0$, then $0 \mid g$, so $g = 0$ by (a), and $f = 1 \cdot g$. Otherwise write $g = fu$ and $f = gv$. Then $f = fuv$, so $f(1 - uv) = 0$. Since $f \neq 0$, Corollary 4.3.3 (a) gives $1 - uv = 0$, that is, $uv = 1$. So v is a unit of $F[x]$, hence a non-zero constant by (e), and $f = vg$: f and g are associates.

The monic associate. Let $f \neq 0$ and $a \coloneqq \mathrm{lc}(f) \neq 0$. The polynomial $a^{-1}f$ has the coefficients $a^{-1}f_k$ (Theorem 4.2.4 (d)). These vanish exactly where the f_k do, since $a^{-1} \neq 0$ (as $a \cdot 0 = 0 \neq 1 = aa^{-1}$, by Theorem 2.1.1 (d), (F7), (F8)) and F has no zero divisors, so $\deg(a^{-1}f) = \deg f$ and $\mathrm{lc}(a^{-1}f) = a^{-1}a = 1$. If also cf is monic for a constant $c \neq 0$, the same computation

gives $\operatorname{lc}(cf) = ca = 1$, so $c = a^{-1}$ (uniqueness of inverses, Theorem 2.1.1 (c)). So $a^{-1}f$ is the only monic associate of f.

Monic and mutually dividing. Let f, g be monic with $f \mid g$ and $g \mid f$. By what we proved, $f = cg$ with a non-zero constant c, and comparing leading coefficients, $1 = \operatorname{lc}(f) = c \operatorname{lc}(g) = c$. So $f = g$. This proves the proposition.

■

Parts (e) and (f) are the polynomial form of a fact about $\mathbb{Z}$: in Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (f) and (g), the units of $\mathbb{Z}$ were ± 1, and two **positive** integers that divide each other are equal. In $F[x]$ the units are the non-zero constants, and the role of "positive" is played by "monic": among the associates of a non-zero polynomial, exactly one is monic. So whenever a polynomial is to be singled out from its associates, it is made monic.

The hypothesis $f \neq 0$ in (d) cannot be dropped: $x^5 \mid 0$, and $\deg x^5 = 5 > -\infty = \deg 0$.

Quick check. In $\mathbb{Q}[x]$, list the associates of $3x + 6$ that have integer coefficients and leading coefficient between -3 and 3. Which one is monic?

Solution. The associates are $c(3x+6)$ with $c \in \mathbb{Q}$, $c \neq 0$; the leading coefficient is $3c$. Leading coefficients $\pm 1, \pm 2, \pm 3$ give $\pm(x+2)$, $\pm(2x+4)$, $\pm(3x+6)$, all with integer coefficients. The monic one is $x + 2 = \frac{1}{3}(3x + 6)$.

5.1.2 Division with remainder

Now the theorem. The tool is the one *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.1 used for integers, with degree in place of size: among all $f - hg$, take one of **least degree**, and show that its degree is below $\deg g$.

Theorem 5.1.2. Division with Remainder in $F[x]$

Let F be a field, and let $f, g \in F[x]$ with $g \neq 0$.

(a) There are **unique** $q, r \in F[x]$ with

$$f = qg + r \quad \text{and} \quad \deg r < \deg g.$$

(b) $g \mid f$ if and only if $r = 0$.

The polynomials q and r are the **quotient** and the **remainder** of f on division by g.

Since $\deg 0 = -\infty < \deg g$, the remainder $r = 0$ is allowed.

Idea. Look at all polynomials $f - hg$, $h \in F[x]$. If 0 is among them, f is a multiple of g and we are done. Otherwise their degrees are natural numbers, and well-ordering gives one, r, of least degree n. If $n \geq \deg g$, we can kill the leading term of r by subtracting a constant times a power of x times g: the constant is $\operatorname{lc}(r) \operatorname{lc}(g)^{-1}$, and that inverse is where the field

is needed. The result is again of the form $f - hg$ and has smaller degree, against the choice of r. Uniqueness: two answers give $(q - q')g = r' - r$, and a non-zero multiple of g cannot have degree below $\deg g$. We call this move **compare degrees**.

Proof.

(a) *Existence.* Let $m := \deg g \in \mathbb{N}$ and $b := \mathrm{lc}(g) \neq 0$, and let

$$S := \{f - hg : h \in F[x]\}.$$

If $0 \in S$, say $0 = f - qg$, then $r := 0$ and this q satisfy $f = qg + r$ and $\deg r = -\infty < m$. Suppose $0 \notin S$. Then every element of S has a degree in $\mathbb{N}$, and $D := \{\deg s : s \in S\} \subseteq \mathbb{N}$ is non-empty, since $f = f - 0 \cdot g \in S$. By the well-ordering of $\mathbb{N}$ (Sets, Relations, and Cardinality, Theorem 2.1.3; on $\mathbb{N} = \omega$ it is Number Systems: From \(\nN\) to \(\nR\), Theorem 1.6.2), D has a least element n. Choose $q \in F[x]$ with $r := f - qg$ of degree n, and let $a := \mathrm{lc}(r) \neq 0$.
Suppose $n \geq m$. Let $t := (ab^{-1})x^{n-m}$, a monomial with $n - m \in \mathbb{N}$ and non-zero coefficient ab^{-1}: $b^{-1} \neq 0$, since $b \cdot 0 = 0 \neq 1 = bb^{-1}$ (Theorem 2.1.1 (d), (F7), (F8)), so $ab^{-1} \neq 0$ by Theorem 2.1.1 (f). Then $\deg t = n - m$ and $\mathrm{lc}(t) = ab^{-1}$, so by Theorem 4.3.2 (b), tg has degree $(n - m) + m = n$ and leading coefficient $ab^{-1}b = a$. Let

$$r_1 := r - tg = f - (q + t)g,$$

an element of S. By Theorem 4.3.1 (with $\deg(-p) = \deg p$ for every p, since $(-p)_k = -p_k$), $\deg r_1 \leq \max(\deg r, \deg tg) = n$, and the coefficient of x^n in r_1 is $a - a = 0$. So $\deg r_1 < n$ (or $r_1 = 0$). But $r_1 \neq 0$, since $0 \notin S$, and then $\deg r_1 \in D$ is smaller than the least element n of D. This contradiction shows $n < m$. So $f = qg + r$ with $\deg r < \deg g$.
Uniqueness. Let $f = qg + r = q'g + r'$ with $\deg r < m$ and $\deg r' < m$. Then

$$(q - q')g = r' - r,$$

and $\deg(r' - r) \leq \max(\deg r', \deg r) < m$ by Theorem 4.3.1 (using $\deg(-r) = \deg r$ as above). If $q \neq q'$, then Theorem 4.3.2 (b) gives $\deg((q - q')g) = \deg(q - q') + m \geq m$, a contradiction. So $q = q'$, hence $r' - r = 0 \cdot g = 0$ and $r = r'$.

(b) ($\Leftarrow$) If $r = 0$, then $f = qg$, so $g \mid f$. ($\Rightarrow$) If $f = hg$, then $f = hg + 0$ with $\deg 0 < \deg g$ is a division with remainder; by the uniqueness in (a), $r = 0$. This proves the theorem.

■

The field is used in two places. The first is the inverse b^{-1} of the leading coefficient of g, which builds the monomial t. The second is the degree of a product, in $\deg(tg) = n$ and in the uniqueness: Theorem 4.3.2 (b) needs the product of the leading coefficients to be non-zero, and a field has no zero divisors. The hypothesis $g \neq 0$ is needed as well: for $g = 0$ no r has $\deg r < -\infty$.

The existence proof is also a procedure. Each pass replaces r by $r - tg$, which removes the leading term of r, and the degree drops by at least one. Starting from f, at most $\deg f - \deg g + 1$ passes are needed when $\deg f \geq \deg g$, and none when $\deg f < \deg g$: then $q = 0$ and $r = f$. This is the long division of school algebra, now with a proof that it stops and that its answer is the only one. Chapter 4 did not divide polynomials with remainder, so this is where the volume

first does it. Its integer twin is Number Systems: From \(\nN\) to \(\nR\), Theorem 3.1.2, whose least-element proof the one above follows.

Example. Long division in two fields

(i) In $\mathbb{Q}[x]$, divide $f = 2x^4 - 3x^3 + x^2 + 4x - 1$ by $g = 2x^2 - x + 3$.

(ii) In $\mathbb{F}_3[x]$, divide $f = x^4 + x + 2$ by $g = 2x^2 + 1$.

Solution.

(i) Here $\mathrm{lc}(g) = 2$, with inverse $\frac{1}{2}$. Each pass subtracts tg, where t is the leading term of the current remainder divided by $2x^2$:

$$\begin{aligned} f - x^2 g &= -2x^3 - 2x^2 + 4x - 1, \\ (-2x^3 - 2x^2 + 4x - 1) - (-x)g &= -3x^2 + 7x - 1, \\ (-3x^2 + 7x - 1) - (-\tfrac{3}{2})g &= \tfrac{11}{2}x + \tfrac{7}{2}. \end{aligned}$$

The last line has degree $1 < 2$, so we stop. Adding up the t's,

$$2x^4 - 3x^3 + x^2 + 4x - 1 = (x^2 - x - \tfrac{3}{2})(2x^2 - x + 3) + \tfrac{11}{2}x + \tfrac{7}{2}.$$

Check: $(x^2 - x - \frac{3}{2})(2x^2 - x + 3) = 2x^4 - 3x^3 + x^2 - \frac{3}{2}x - \frac{9}{2}$, and adding $\frac{11}{2}x + \frac{7}{2}$ gives f.

(ii) In $\mathbb{F}_3$, $2 \cdot 2 = 4 = 1$, so $\mathrm{lc}(g)^{-1} = 2^{-1} = 2$. The first t is $1 \cdot 2 \cdot x^2 = 2x^2$, and $2x^2 \cdot g = 4x^4 + 2x^2 = x^4 + 2x^2$. The second t is 2, and $2g = 4x^2 + 2 = x^2 + 2$:

$$\begin{aligned} f - 2x^2 g &= -2x^2 + x + 2 = x^2 + x + 2, \\ (x^2 + x + 2) - 2g &= x. \end{aligned}$$

So $x^4 + x + 2 = (2x^2 + 2)(2x^2 + 1) + x$ in $\mathbb{F}_3[x]$. Check: $(2x^2 + 2)(2x^2 + 1) = 4x^4 + 6x^2 + 2 = x^4 + 2$ in $\mathbb{F}_3$, and adding x gives f.

Quick check. Find two different pairs (q, r) with $x^2 = q(x^2 + 1) + r$ in $\mathbb{Q}[x]$ and $\deg r \leq 2$. Which condition in part (a) of the theorem does the second one fail?

Solution. $(q, r) = (1, -1)$: $1 \cdot (x^2 + 1) - 1 = x^2$, with $\deg(-1) = 0 < 2$. And $(q, r) = (0, x^2)$: $0 \cdot (x^2 + 1) + x^2 = x^2$, with $\deg r = 2$. The second fails $\deg r < \deg g = 2$. Uniqueness holds only among remainders of degree **strictly** below that of the divisor; $(1, -1)$ is the quotient and remainder.

Warning. Division with remainder needs the leading coefficient of the divisor to be invertible. Take the polynomials in $\mathbb{Q}[x]$ all of whose coefficients lie in $\mathbb{Z}$, and try to divide x^2 by $2x$ **among them**: $x^2 = q \cdot 2x + r$ with $\deg r < 1$. Comparing the coefficients of x^2 gives $1 = 2q_1$ (Lemma 4.2.2 (a)), and no integer q_1 satisfies it, since 1 is odd (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a)). In $\mathbb{Q}[x]$ there is no problem: $x^2 = \frac{1}{2}x \cdot 2x + 0$.

Exercise C1 shows that integer coefficients are kept when the divisor is monic.

5.1.3 Roots and factors of degree one

Division by a polynomial of degree 1 has a remainder of degree at most 0, that is, a constant. Which constant? Evaluate: the divisor $x - c$ vanishes at c, so the quotient term disappears and the remainder is read off. We call this move **evaluate at a root**.

Theorem 5.1.3. Remainder Theorem and Factor Theorem

Let F be a field, $f \in F[x]$ and $c \in F$.

(a) The remainder of f on division by $x - c$ is the constant $f(c)$.

(b) c is a root of f if and only if $x - c \mid f$.

(c) f has a factor of degree 1 in $F[x]$ if and only if f has a root in F.

Idea. Divide by $x - c$ and evaluate at c: the term with the quotient vanishes, and what is left is the remainder. Part (b) is then the divisibility test of Theorem 5.1.2 (b), and for (c) a factor $ax + b$ of degree 1 is made monic, which turns it into some $x - c$.

Proof.

(a) The polynomial $x - c$ is non-zero, of degree 1 and monic. By Theorem 5.1.2 (a), $f = q \cdot (x - c) + r$ with $\deg r < 1$, so r is a constant (possibly 0). Evaluation at c respects sums and products, sends x to c and a constant to itself (Theorem 4.4.1), so

$$f(c) = q(c) \cdot (c - c) + r = q(c) \cdot 0 + r = r.$$

(b) By (a), $f = q \cdot (x - c) + f(c)$ is the division of f by $x - c$. By Theorem 5.1.2 (b), $x - c \mid f$ if and only if this remainder is 0, that is, $f(c) = 0$.

(c) ($\Leftarrow$) If $f(c) = 0$, then $x - c \mid f$ by (b), and $x - c$ has degree 1. ($\Rightarrow$) Let $ax + b \mid f$ with $a, b \in F$, $a \neq 0$. Then $ax + b = a\big(x - (-a^{-1}b)\big)$, so $x - (-a^{-1}b) \mid ax + b$, and by Proposition 5.1.1 (b), $x - (-a^{-1}b) \mid f$. By (b), $-a^{-1}b$ is a root of f.

■

Part (b) is the **factor theorem**, and it turns a question about values (is $f(c) = 0$?) into a question about divisibility. Part (c) turns the search for factors of degree 1 into a search for roots.

Example. Remainders without dividing

(a) In $\mathbb{Q}[x]$, find the remainder of $f = x^5 - 3x^3 + 2x + 7$ on division by $x - 2$.

(b) In $\mathbb{Q}[x]$, find the remainder of x^5 on division by $x^2 - x$.

Solution.

(a) By Theorem 5.1.3 (a), the remainder is

$$f(2) = 32 - 24 + 4 + 7 = 19.$$

(b) The divisor $x^2 - x$ has degree 2, so the remainder has degree at most 1: $x^5 = q \cdot (x^2 - x) + ax + b$ with $a, b \in \mathbb{Q}$ (Theorem 5.1.2 (a)). The divisor vanishes at 0 and at 1. Evaluating at both (Theorem 4.4.1),

$$0 = q(0) \cdot 0 + b, \qquad 1 = q(1) \cdot 0 + a + b,$$

so $b = 0$ and $a = 1$. The remainder is x. Check: $x^5 - x = (x^2 - x)(x^3 + x^2 + x + 1)$.

Quick check. Without dividing, decide whether $x + 1$ divides $x^7 + 1$ in $\mathbb{Q}[x]$, and whether $x - 1$ does.

Solution. $x + 1 = x - (-1)$, and $(-1)^7 + 1 = -1 + 1 = 0$, so $x + 1 \mid x^7 + 1$ by Theorem 5.1.3 (b). For $x - 1$, the remainder is $1^7 + 1 = 2 \neq 0$ in $\mathbb{Q}$, so $x - 1 \nmid x^7 + 1$. (Over $\mathbb{F}_2$, $2 = 0$ and both divide.)

Remark (Looking ahead). Section 5.5 builds, for any finite list of distinct points of F, the polynomial of least degree that takes prescribed values there. Exercise C2 below is the case of two points: the remainder of f on division by $(x - a)(x - b)$.

5.1.4 Exercises

5.1.4.1 A. Check your understanding

Exercise. A1

(a) State Theorem 5.1.2 with every hypothesis.

(b) Name the two places in its proof where "F is a field" is used.

(c) Let $f \in F[x]$, and let $c \in F$ be a non-zero constant. What are the quotient and the remainder of f on division by c?

(d) True or false, with a reason: for $f, g \in \mathbb{Q}[x]$, if $f \mid g$ and $g \mid f$, then $f = g$. The same question in $\mathbb{F}_2[x]$.

Solution.

(a) Let F be a field and $f, g \in F[x]$ with $g \neq 0$. Then there are unique $q, r \in F[x]$ with $f = qg + r$ and $\deg r < \deg g$; and $g \mid f$ if and only if $r = 0$.

(b) The inverse $\mathrm{lc}(g)^{-1}$, which builds the monomial $t = \mathrm{lc}(r)\,\mathrm{lc}(g)^{-1}x^{n-m}$; and the absence of zero divisors in F, through Theorem 4.3.2 (b), which gives $\deg(tg) = n$ and, in the

uniqueness, $\deg((q-q')g) \geq \deg g$.

(c) $q = c^{-1}f$ and $r = 0$: indeed $f = (c^{-1}f)c + 0$, and $\deg 0 = -\infty < 0 = \deg c$. By uniqueness this is the division.

(d) In $\mathbb{Q}[x]$: false. $x \mid 2x$ and $2x \mid x$ ($x = \frac{1}{2} \cdot 2x$), but $x \neq 2x$. By Proposition 5.1.1 (f), mutual divisibility only makes f and g associates. In $\mathbb{F}_2[x]$: true. By (f), $f = cg$ with c a non-zero constant, and the only non-zero element of $\mathbb{F}_2$ is 1; so $f = g$.

5.1.4.2 B. Practice

Exercise. B1: Two long divisions

(a) In $\mathbb{Q}[x]$, divide $x^4 - 3x^3 + 2x - 5$ by $3x^2 - 1$.

(b) In $\mathbb{F}_5[x]$, divide $x^4 + 2x^3 + 3x + 1$ by $2x^2 + 3$, and decide whether $2x^2 + 3$ divides $x^4 + 2x^3 + 3x + 1$ in $\mathbb{F}_5[x]$.

Solution.

(a) $\mathrm{lc}(3x^2 - 1)^{-1} = \frac{1}{3}$. The passes subtract $\frac{1}{3}x^2$, $-x$ and $\frac{1}{9}$ times the divisor:

$$\begin{aligned}(x^4 - 3x^3 + 2x - 5) - \tfrac{1}{3}x^2(3x^2 - 1) &= -3x^3 + \tfrac{1}{3}x^2 + 2x - 5,\\ (-3x^3 + \tfrac{1}{3}x^2 + 2x - 5) + x(3x^2 - 1) &= \tfrac{1}{3}x^2 + x - 5,\\ (\tfrac{1}{3}x^2 + x - 5) - \tfrac{1}{9}(3x^2 - 1) &= x - \tfrac{44}{9}.\end{aligned}$$

So the quotient is $\frac{1}{3}x^2 - x + \frac{1}{9}$ and the remainder is $x - \frac{44}{9}$, of degree $1 < 2$. Check: $(3x^2 - 1)(\frac{1}{3}x^2 - x + \frac{1}{9}) = x^4 - 3x^3 + x - \frac{1}{9}$, and adding $x - \frac{44}{9}$ gives $x^4 - 3x^3 + 2x - 5$.

(b) In $\mathbb{F}_5$, $2 \cdot 3 = 6 = 1$, so $2^{-1} = 3$. The passes subtract $3x^2$, x and 3 times the divisor, with $3x^2(2x^2 + 3) = x^4 + 4x^2$, $x(2x^2 + 3) = 2x^3 + 3x$ and $3(2x^2 + 3) = x^2 + 4$:

$$\begin{aligned}(x^4 + 2x^3 + 3x + 1) - (x^4 + 4x^2) &= 2x^3 + x^2 + 3x + 1,\\ (2x^3 + x^2 + 3x + 1) - (2x^3 + 3x) &= x^2 + 1,\\ (x^2 + 1) - (x^2 + 4) &= 2,\end{aligned}$$

using $-4 = 1$ and $-3 = 2$ in $\mathbb{F}_5$. So the quotient is $3x^2 + x + 3$ and the remainder is the constant 2. Since $2 \neq 0$ in $\mathbb{F}_5$, Theorem 5.1.2 (b) gives $2x^2 + 3 \nmid x^4 + 2x^3 + 3x + 1$ in $\mathbb{F}_5[x]$.

Exercise. B2: A factor of a difference of powers

Let F be a field, $c \in F$ and $n \in \mathbb{Z}_{>0}$. Deduce from Lemma 1.1.4 that

$$x^n - c^n = (x - c)\sum_{j=0}^{n-1} c^j x^{n-1-j},$$

and hence that $x - c \mid x^n - c^n$. Then give a second proof of the divisibility with Theorem 5.1.3.

Solution. $F[x]$ is a commutative ring (Theorem 4.2.4 (a)), so Lemma 1.1.4 applies in it. Take $z = c$ and $w = x$:

$$c^n - x^n = (c - x) \sum_{j=0}^{n-1} c^j x^{n-1-j}.$$

Negate both sides: $-(c^n - x^n) = x^n - c^n$ and $-((c-x)s) = (x-c)s$ for every $s \in F[x]$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.2 (a), (c)). This is the displayed identity, and it shows $x - c \mid x^n - c^n$. Taking $z = c$, $w = x$ rather than $z = x$, $w = c$ gives the sum in the stated order, with no re-indexing.

Second proof. By Theorem 4.2.4 (c), x^n is the monomial $1x^n$, whose value at c is $1 \cdot c^n = c^n$ (Definition 4.4.1, the monomial example after it). So the value of $x^n - c^n$ at c is $c^n - c^n = 0$ (Theorem 4.4.1, for the sum and the constant $-c^n$), so c is a root and $x - c \mid x^n - c^n$ by Theorem 5.1.3 (b). This proof gives the divisibility at once but not the quotient.

Exercise. B3: One remainder over every field

Let F be any field. Show that the remainder of x^{100} on division by $x^2 - 1$ in $F[x]$ is 1. Then explain why, over $\mathbb{Q}$, evaluating at the roots 1 and -1 also finds it, and why that method alone does not settle the question over $\mathbb{F}_2$.

Solution. By Lemma 1.1.4 in $F[x]$ with $z = x^2$, $w = 1$ and $n = 50$, since $(x^2)^k = x^{2k}$ and $1^k = 1$ (Lemma 4.1.1 (c)),

$$(x^2 - 1) \sum_{j=0}^{49} x^{2j} = x^{100} - 1.$$

So $x^{100} = (\sum_{j=0}^{49} x^{2j})(x^2 - 1) + 1$, and $\deg 1 = 0 < 2 = \deg(x^2 - 1)$. By the uniqueness in Theorem 5.1.2 (a), the remainder is 1, over every field.

Over $\mathbb{Q}$ by evaluation. Write $x^{100} = q(x^2-1)+ax+b$. Evaluating at 1 and -1 gives $1 = a+b$ and $1 = -a + b$; subtracting, $2a = 0$, so $a = 0$ since $2 \neq 0$ in $\mathbb{Q}$; then $b = 1$.

Over $\mathbb{F}_2$. There $-1 = 1$, so the two roots coincide and evaluation gives the single equation $1 = a + b$. It does not determine a and b (both $(0, 1)$ and $(1, 0)$ satisfy it), so the uniqueness argument above is needed.

5.1.4.3 C. Going deeper

Exercise. C1: Monic divisors keep integer coefficients

Call $p \in \mathbb{Q}[x]$ an **integer polynomial** if every coefficient of p lies in $\mathbb{Z}$.

(a) Let f, g be integer polynomials with g monic. Prove that the quotient and the remainder of f on division by g in $\mathbb{Q}[x]$ are integer polynomials.

(b) Prove the same if $\mathrm{lc}(g) = -1$.

(c) Explain why the least-degree argument of Theorem 5.1.2 still works when S is replaced by $\{f - hg : h \text{ an integer polynomial}\}$, for g monic.

Solution (Hint 1). Rerun the existence proof of Theorem 5.1.2, but only with integer polynomials h.

Solution (Hint 2). Let $S_{\mathbb{Z}} \coloneqq \{f - hg : h \text{ an integer polynomial}\}$. If $0 \notin S_{\mathbb{Z}}$, take $r = f - qg \in S_{\mathbb{Z}}$ of least degree n (Sets, Relations, and Cardinality, Theorem 2.1.3) and suppose $n \geq \deg g$.

Solution. Sums, negatives and products of integer polynomials are integer polynomials: their coefficients are sums of products of coefficients (Definition 4.2.1), and $\mathbb{Z}$ is closed under $+$, $-$, $\cdot$.

(c) and (a). Let $m \coloneqq \deg g$ and

$$S_{\mathbb{Z}} \coloneqq \{f - hg : h \text{ an integer polynomial}\} \subseteq \mathbb{Q}[x],$$

whose elements are integer polynomials. Run the existence proof with $S_{\mathbb{Z}}$ in place of S. If $0 \in S_{\mathbb{Z}}$, then $f = qg$ with q an integer polynomial and $r = 0$. Otherwise take $r = f - qg \in S_{\mathbb{Z}}$ of least degree n (Sets, Relations, and Cardinality, Theorem 2.1.3), and suppose $n \geq m$. With $a \coloneqq \operatorname{lc}(r) \in \mathbb{Z}$ and $b = 1$, the monomial $t = ax^{n-m}$ is an integer polynomial, so $r - tg = f - (q + t)g \in S_{\mathbb{Z}}$, and it has degree $< n$ or is 0, exactly as in the proof. Both contradict the choice of r. So $\deg r < m$, and $f = qg + r$ with q, r integer polynomials. This is a division with remainder in $\mathbb{Q}[x]$, so by uniqueness (Theorem 5.1.2 (a)) these q, r are **the** quotient and remainder. The argument works because the step $r \mapsto r - tg$ never leaves $S_{\mathbb{Z}}$: it needs $b^{-1} \in \mathbb{Z}$, and $b = 1$ gives $b^{-1} = 1$. That answers (c).

(d) If $\operatorname{lc}(g) = -1$, then $b^{-1} = -1 \in \mathbb{Z}$, and the same proof runs with $t = -ax^{n-m}$. (Alternatively, divide f by the monic $-g$: $f = q(-g) + r = (-q)g + r$.)

Exercise. C2: The remainder modulo a quadratic with known roots

Let F be a field, $f \in F[x]$ and $a, b \in F$.

(a) If $a \neq b$, prove that the remainder of f on division by $(x - a)(x - b)$ is

$$f(a)(a - b)^{-1}(x - b) + f(b)(b - a)^{-1}(x - a).$$

(b) If $a = b$, write $f = (x - a)h + f(a)$ (Theorem 5.1.3 (a)) and prove that the remainder of f on division by $(x - a)^2$ is $h(a)(x - a) + f(a)$.

(c) Hence find the remainder of x^{100} on division by $x^2 - 3x + 2$ in $\mathbb{Q}[x]$.

Solution (Hint 1). The remainder has degree at most 1. Which values does it take at a and at b?

Solution (Hint 2). Write $f = q(x - a)(x - b) + r$ with $\deg r \leq 1$, and let s be the displayed polynomial.

Solution.

(a) The divisor $(x-a)(x-b)$ is monic of degree 2 (Theorem 4.3.2 (b)), so Theorem 5.1.2 (a) gives $f = q(x-a)(x-b)+r$ with $\deg r \leq 1$. Evaluating at a and at b (Theorem 4.4.1) kills the first term: $r(a) = f(a)$ and $r(b) = f(b)$. Let s be the displayed polynomial; it has degree at most 1, and $s(a) = f(a)\cdot 1 + f(b)\cdot 0 = f(a)$, $s(b) = f(b)$. So $r-s$ has degree at most 1 and the two roots $a \neq b$. If $r-s \neq 0$, then $x-a \mid r-s$ (Theorem 5.1.3 (b)), say $r-s = (x-a)k$, and $\deg k \leq 0$ by Theorem 4.3.2 (b), so k is a constant; evaluating at b gives $0 = (b-a)k$, so $k = 0$ because $b-a \neq 0$, and then $r-s = 0$ after all. Hence $r = s$.

(b) Divide h by $x-a$: $h = (x-a)h_2 + h(a)$ (Theorem 5.1.3 (a)). Then

$$f = (x-a)^2 h_2 + h(a)(x-a) + f(a),$$

and $h(a)(x-a)+f(a)$ has degree at most $1 < 2$. By uniqueness, it is the remainder.

(c) $x^2 - 3x + 2 = (x-1)(x-2)$. By (a) with $a = 1$, $b = 2$, $f(1) = 1$ and $f(2) = 2^{100}$, the remainder is

$$1\cdot(-1)^{-1}(x-2) + 2^{100}\cdot 1^{-1}(x-1) = (2^{100}-1)x + (2-2^{100}).$$

5.2 Ideals, the Greatest Common Divisor, and the Euclidean Algorithm

Section 5.1 gave $F[x]$ a division with remainder (Theorem 5.1.2). This section asks what two polynomials have in common. Here is a concrete version of the question. Which polynomials over $\mathbb{Q}$ can be written as

$$a\cdot(x^2-1) + b\cdot(x^2+x-2) \qquad \text{with } a, b \in \mathbb{Q}[x]\,?$$

Taking $a = -1$ and $b = 1$ gives $x-1$, and hence, multiplying a and b by any h, every multiple $h\cdot(x-1)$. Nothing else can occur: $x^2-1 = (x-1)(x+1)$ and $x^2+x-2 = (x-1)(x+2)$, so $x-1$ divides every such combination (Proposition 5.1.1 (c)). So the answer is "all multiples of $x-1$, and nothing else". Why $x-1$, and why should the answer be the set of multiples of a single polynomial? The integer version of this question, in *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Section 3.2, was answered by a least element; here the answer is a polynomial of least degree.

As in Section 5.1, F is a field and $F[x]$ is a commutative ring (Theorem 4.2.4 (a)). So the general notions of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 3 apply to it without change: ideals (Number Systems: From \(\nN\) to \(\nR\), Definition 3.4.1, clauses (I1)–(I3)), quotient rings (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1) and units (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1). We recall the clauses: a subset $I \subseteq F[x]$ is an **ideal** if (I1) $0 \in I$, (I2) $a+b \in I$ for all $a, b \in I$, and (I3) $ra \in I$ for all $a \in I$ and **all** $r \in F[x]$.

5.2.1 The ideal generated by finitely many polynomials

The combinations in the opening question form a set that deserves a name and a symbol.

Definition 5.2.1. Ideal Generated by Polynomials

Let F be a field, $k \in \mathbb{Z}_{>0}$ and $f_1, \dots, f_k \in F[x]$. The set

$$\langle f_1, \dots, f_k \rangle \coloneqq \{a_1 f_1 + \cdots + a_k f_k : a_1, \dots, a_k \in F[x]\}$$

is the **ideal generated by** $f_1, \dots, f_k$. For one polynomial, $\langle f \rangle = \{af : a \in F[x]\}$ is the set of multiples of f.

In words: $\langle f_1, \dots, f_k \rangle$ collects every way of multiplying each f_i by a polynomial and adding up. The coefficients a_i range over **all** of $F[x]$, not over F. The name is earned by two facts.

It is an ideal, and it contains every f_i. (I1): $0 = 0 \cdot f_1 + \cdots + 0 \cdot f_k$. (I2): $\sum_i a_i f_i + \sum_i b_i f_i = \sum_i (a_i + b_i) f_i$. (I3): $r \sum_i a_i f_i = \sum_i (r a_i) f_i$. These are the ring laws of $F[x]$ applied to finite sums (Lemma 4.1.1 (b)). Taking $a_i = 1$ and the other coefficients 0 shows $f_i \in \langle f_1, \dots, f_k \rangle$.

It lies inside every ideal that contains every f_i. If J is an ideal with $f_1, \dots, f_k \in J$, then each $a_i f_i \in J$ by (I3), and their sum lies in J by (I2), applied $k - 1$ times. So $\langle f_1, \dots, f_k \rangle \subseteq J$.

So $\langle f_1, \dots, f_k \rangle$ is the smallest ideal containing $f_1, \dots, f_k$. This "smallest" clause is how we will compare two such ideals: to show $\langle g_1, \dots, g_l \rangle \subseteq \langle f_1, \dots, f_k \rangle$, it is enough to show that each g_j lies in $\langle f_1, \dots, f_k \rangle$.

Examples:

- $\langle 0 \rangle = \{a \cdot 0\} = \{0\}$, the degenerate case. It is the only ideal generated by one polynomial that contains no non-zero element, and the main theorem below treats it separately.
- $\langle c \rangle = F[x]$ for a non-zero constant c: every f equals $(c^{-1} f) \cdot c$.
- For $c \in F$, let $I_c \coloneqq \{f \in F[x] : f(c) = 0\}$, the polynomials with root c. It is an ideal: $0(c) = 0$, $(f + g)(c) = f(c) + g(c) = 0$, and $(rf)(c) = r(c) f(c) = 0$, by Theorem 4.4.1. Moreover $I_c = \langle x - c \rangle$: by the factor theorem (Theorem 5.1.3 (b)), $f(c) = 0$ if and only if $x - c \mid f$, that is, $f \in \langle x - c \rangle$.
- In the opening question, $\langle x^2 - 1, x^2 + x - 2 \rangle = \langle x - 1 \rangle$.

↻ **Second reading** · *A non-example: large degree*

The set $T \coloneqq \{f \in F[x] : \deg f \geq 3\} \cup \{0\}$ satisfies (I1) and (I3) (a non-zero multiple of a polynomial of degree at least 3 has degree at least 3, by Theorem 4.3.2 (b)). But (I2) fails: x^3 and $-x^3 + x$ lie in T, and their sum x has degree 1. So T is not an ideal. "Large degree" is not a property that sums keep, because leading terms can cancel.

Quick check. Is $\{f \in \mathbb{Q}[x] : f(0) = 1\}$ an ideal of $\mathbb{Q}[x]$? Name the first clause that fails.

Solution. No. (I1) fails already: the zero polynomial has $0(0) = 0 \neq 1$. (So do (I2), since $(1 + 1)(0) = 2$, and (I3), with $r = 0$.) Compare $I_0 = \{f : f(0) = 0\} = \langle x \rangle$, which is an ideal.

5.2.2 Every ideal has one generator

Every example above turned out to be the set of multiples of a single polynomial. That is no accident.

Theorem 5.2.1. Ideals of $F[x]$ Are Principal

Let F be a field and I an ideal of $F[x]$.

(a) If $I = \{0\}$, then $I = \langle 0 \rangle$.

(b) If $I \neq \{0\}$, there is **exactly one monic** $d \in F[x]$ with $I = \langle d \rangle$. Moreover d is the only monic element of I of least degree among the non-zero elements of I.

Idea. Take a non-zero element of I of least degree, and scale it to be monic; call it d. Its multiples lie in I by absorption. Conversely, divide any $f \in I$ by d: the remainder $f - qd$ lies in I and has smaller degree than d, so it cannot be a non-zero element of I. It is 0, and f is a multiple of d. Uniqueness comes from Proposition 5.1.1 (f): two monic generators divide each other.

Before reading on: where is "least degree" used, and why is d made monic?

Proof.

(a) If $I = \{0\}$, then $I = \{0\} = \langle 0 \rangle$.

(b) *Existence.* Let $I \neq \{0\}$. The set $D := \{\deg e : e \in I,\ e \neq 0\}$ is a non-empty subset of $\mathbb{N}$, so it has a least element n (Sets, Relations, and Cardinality, Theorem 2.1.3; on $\mathbb{N} = \omega$ it is Number Systems: From \(\nN\) to \(\nR\), Theorem 1.6.2). Choose a non-zero $e \in I$ with $\deg e = n$, let $a := \mathrm{lc}(e) \neq 0$, and let $d := a^{-1}e$. Then $d \in I$ by (I3), and d is monic of degree n (Proposition 5.1.1 (f), Theorem 4.3.2 (b)).

($\supseteq$) For $h \in F[x]$, $hd \in I$ by (I3). So $\langle d \rangle \subseteq I$.

($\subseteq$) Let $f \in I$. Since $d \neq 0$, Theorem 5.1.2 (a) gives $q, r \in F[x]$ with $f = qd + r$ and $\deg r < \deg d = n$. Then $r = f + (-q)d \in I$, by (I3) and (I2). If $r \neq 0$, then $\deg r \in D$ and $\deg r < n$, against the choice of n as least. So $r = 0$, and $f = qd \in \langle d \rangle$. Hence $I = \langle d \rangle$.

Uniqueness. Let d' be monic with $I = \langle d' \rangle$. Then $d \in \langle d' \rangle$ and $d' \in \langle d \rangle$ (each generator lies in its own ideal), so $d' \mid d$ and $d \mid d'$. Both are monic, so $d = d'$ by Proposition 5.1.1 (f).

The least-degree description. Let d'' be any monic element of I with $\deg d'' = n$. The argument of ($\supseteq$) and ($\subseteq$) used only that d is a non-zero element of I of degree n; run with d'' in place of d, it gives $I = \langle d'' \rangle$, and uniqueness gives $d'' = d$. This proves the theorem.

■

The answer to the prompt. "Least degree" is used once, in ($\subseteq$): the remainder r lies in I and has degree below n, so minimality forces $r = 0$. The minimality is about **non-zero** elements, which is why $r = 0$ is the conclusion and not a contradiction. Making d monic plays no part in the existence of a generator: e itself generates I, and so does $2e$ when $2 \neq 0$ in F. It is what makes the generator **unique**, because among the associates of e, all of which generate I, exactly

one is monic.

An ideal of the form $\langle d \rangle$ is called **principal**, hence the name of the theorem. The proof's move is the one this chapter is built on, and we name it: **least degree, then divide**. In a set of polynomials closed under the right operations, take a non-zero element d of least degree; divide any element of the set by d; the remainder lies in the set and has smaller degree, so it is 0. It is the polynomial form of "least positive element, then divide" from *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.2.

↻ **Second reading** · *Comparison with the integers, and two indeterminates*

The integer twin is Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.2: every ideal of $\mathbb{Z}$ is $n\mathbb{Z}$ for exactly one $n \in \mathbb{N}$. There "$n \geq 0$" picked the generator; here "monic" does. In polynomials in **two** indeterminates the theorem fails (the polynomials with zero constant term are an example, which we state without proof; Exercise A1 asks which step of the proof breaks there, without proving the failure).

5.2.3 The greatest common divisor

A **common divisor** of f and g is a polynomial h with $h \mid f$ and $h \mid g$. Every non-zero constant is one (Proposition 5.1.1 (a)). For integers, *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.2 took the **largest** common divisor. For polynomials, "largest" can only refer to the degree, and associates have the same degree: $x - 1$ and $2x - 2$ are both common divisors of $x^2 - 1$ and $x^2 + x - 2$ in $\mathbb{Q}[x]$, of the same degree. So the definition asks instead for the property that Bézout's theorem gave the integer gcd, and fixes one associate by asking it to be monic.

The greatest common divisor is the monic common divisor that every common divisor divides.

Definition 5.2.2. Greatest Common Divisor of Polynomials

Let F be a field and $f, g \in F[x]$, **not both** 0. A **greatest common divisor** of f and g is a **monic** $d \in F[x]$ such that $d \mid f$, $d \mid g$, and $h \mid d$ for **every** common divisor h of f and g. We set $\gcd(0, 0) := 0$.

In words: d is a common divisor, it is "on top" of all common divisors for the relation $\mid$, and it is monic.

At most one. If d and d' are both greatest common divisors of f and g, each is a common divisor, so each divides the other; both are monic, so $d = d'$ (Proposition 5.1.1 (f)). We write $\gcd(f, g)$ for it once it is known to exist, and the next theorem shows it always does. The condition is symmetric in f and g, so $\gcd(f, g) = \gcd(g, f)$.

↻ **Second reading** · *Why* $\gcd(0, 0)$ *is* 0

Every polynomial divides 0, so the common divisors of 0 and 0 are all polynomials, and the only polynomial that every polynomial divides is 0 (Proposition 5.1.1 (a) and (d)); but 0 is not monic. The value 0 keeps "every common divisor divides the gcd" true, and it keeps $\langle f, g \rangle = \langle \gcd(f, g) \rangle$

true, since $\langle 0,0\rangle = \{0\} = \langle 0\rangle$. The gcd clause of Lemma 5.2.4 uses the value $\gcd(0,0) = 0$ in the case $f = g = 0$.

Theorem 5.2.2. Bézout's Theorem for Polynomials

Let F be a field, let $f, g \in F[x]$ be not both 0, and let d be the monic polynomial with $\langle f, g\rangle = \langle d\rangle$ (Theorem 5.2.1).

(a) $d \mid f$ and $d \mid g$.

(b) Every common divisor of f and g divides d.

(c) $d = \gcd(f, g)$. So $\gcd(f, g)$ exists, and $\langle f, g\rangle = \langle \gcd(f, g)\rangle$.

(d) $\gcd(f, g) = af + bg$ for some $a, b \in F[x]$.

(e) $\gcd(f, g)$ has the largest degree among the common divisors of f and g, and a common divisor of that degree is an associate of $\gcd(f, g)$.

The ideal $\langle f, g\rangle$ contains f and g, one of which is non-zero, so $\langle f, g\rangle \neq \{0\}$ and the monic d exists and is unique by Theorem 5.2.1 (b).

Idea. Everything is read off from $\langle f, g\rangle = \langle d\rangle$, used in both directions. Since f and g lie in the ideal, they are multiples of d. Since d lies in the ideal, it is a combination of f and g, and a combination is divisible by every common divisor.

Proof.

(a) $f, g \in \langle f, g\rangle = \langle d\rangle$, so f and g are multiples of d.

(b) Since $d \in \langle d\rangle = \langle f, g\rangle$, there are $a_0, b_0 \in F[x]$ with $d = a_0 f + b_0 g$. If $h \mid f$ and $h \mid g$, then $h \mid a_0 f + b_0 g = d$ by Proposition 5.1.1 (c).

(c) By (a) and (b), d is a monic common divisor that every common divisor divides; so $d = \gcd(f, g)$ by Definition 5.2.2. Then $\langle f, g\rangle = \langle d\rangle = \langle \gcd(f, g)\rangle$.

(d) This is $d = a_0 f + b_0 g$ from (b).

(e) Let h be a common divisor. By (b), $h \mid d$, and $d \neq 0$, so $\deg h \leq \deg d$ by Proposition 5.1.1 (d). If $\deg h = \deg d$, write $d = hu$; then $\deg u = 0$ by Theorem 4.3.2 (b), so u is a non-zero constant and d and h are associates. This proves the theorem. ∎

For the opening question: $\langle x^2-1, x^2+x-2\rangle = \langle d\rangle$ with d monic, and $d = \gcd(x^2-1, x^2+x-2) = x - 1$, because $x - 1$ is a monic common divisor and a combination, so every common divisor divides it.

↻ **Second reading** · *Why the definition is not the integer one*

Number Systems: From $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.2 defined the integer gcd as the **largest** common divisor (Number Systems: From \(\nN\) to \(\nR\), Definition 3.2.2) and then proved Bézout's

theorem (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.2.1). Here the order is reversed: the definition uses the divisibility property, which for integers was a consequence, and part (e) recovers "largest" as a consequence, up to associates.

Pairs with no common divisor of positive degree get a name.

Definition 5.2.3. Coprime Polynomials

Let F be a field. Polynomials $f, g \in F[x]$ are **coprime over** F if $\gcd(f, g) = 1$.

For example, x and $x+1$ are coprime over every field, since $(x+1)-x = 1$ and the next corollary applies; 0 and 0 are not, since $\gcd(0, 0) = 0$.

Corollary 5.2.3. Coprime Means 1 Is a Combination

Let F be a field and $f, g \in F[x]$. Then f and g are coprime if and only if $af + bg = 1$ for some $a, b \in F[x]$.

Proof. ($\Rightarrow$) If $\gcd(f, g) = 1$, then f, g are not both 0, since $\gcd(0, 0) = 0 \neq 1$, and Theorem 5.2.2 (d) gives a, b with $af + bg = 1$.

($\Leftarrow$) Let $af + bg = 1$. Then f, g are not both 0, since otherwise $af + bg = 0 \neq 1$. Since $1 \in \langle f, g\rangle$, every $h = h \cdot 1$ lies in $\langle f, g\rangle$ by (I3), so $\langle f, g\rangle = F[x] = \langle 1\rangle$. The polynomial 1 is monic, so by the uniqueness in Theorem 5.2.1 (b) it is the monic generator of $\langle f, g\rangle$, and Theorem 5.2.2 (c) gives $\gcd(f, g) = 1$. ■

Quick check. Find $\gcd(2x - 2,\ 4x^2 - 4)$ in $\mathbb{Q}[x]$.

Solution. $4x^2 - 4 = (2x - 2)(2x + 2)$, so $2x - 2$ divides both, and every common divisor divides $2x - 2$. But $2x - 2$ is not monic. Its monic associate $x - 1$ has the same divisors and multiples (Proposition 5.1.1 (f), (b)), so $\gcd(2x - 2, 4x^2 - 4) = x - 1$, not $2x - 2$.

5.2.4 The Euclidean algorithm

Bézout's theorem finds $\gcd(f, g)$ as an element of least degree, which is no way to compute it. A computation needs a step that lowers degrees without changing the ideal. Division with remainder is that step.

Lemma 5.2.4. One Step of the Euclidean Algorithm

Let F be a field and $f, g, q, r \in F[x]$ with $f = qg + r$. Then $\langle f, g\rangle = \langle g, r\rangle$, and hence $\gcd(f, g) = \gcd(g, r)$.

Proof. ($\supseteq$) $g \in \langle f, g\rangle$, and $r = f + (-q)g \in \langle f, g\rangle$; by the smallest-ideal property of Definition 5.2.1, $\langle g, r\rangle \subseteq \langle f, g\rangle$. ($\subseteq$) $f = qg + 1 \cdot r \in \langle g, r\rangle$ and $g \in \langle g, r\rangle$, so $\langle f, g\rangle \subseteq \langle g, r\rangle$ in the same way.

For the gcds: if $f = g = 0$, then $r = 0$, and both gcds are $\gcd(0, 0) = 0$. Otherwise $\langle f, g\rangle \neq \{0\}$, so $\langle g, r\rangle \neq \{0\}$ and g, r are not both 0. By Theorem 5.2.2 (c), $\gcd(f, g)$ and $\gcd(g, r)$ are monic generators of the same ideal, so they are equal by the uniqueness in Theorem 5.2.1 (b). ∎

The lemma does not ask r to be the remainder. Choosing the remainder makes the degree drop, and repeating the step gives a sequence. To define "repeat" without "and so on", we use the recursion theorem, as in Number Systems: From \(\nN\) to \(\nR\), Theorem 3.2.4.

Theorem 5.2.5. The Euclidean Algorithm for Polynomials

Let F be a field and $f, g \in F[x]$ with $g \neq 0$. Define pairs $(u_k, v_k) \in F[x] \times F[x]$ for $k \in \mathbb{N}$ by $(u_0, v_0) := (f, g)$ and

$$(u_{k+1}, v_{k+1}) := \begin{cases} (v_k, r_k) & \text{if } v_k \neq 0, \\ (u_k, v_k) & \text{if } v_k = 0, \end{cases}$$

where, when $v_k \neq 0$, r_k is the remainder of u_k on division by v_k. Then:

(a) $\langle u_k, v_k\rangle = \langle f, g\rangle$ for every $k \in \mathbb{N}$;

(b) there is a least $K \in \mathbb{N}$ with $v_K = 0$; moreover $1 \leq K \leq \deg g + 1$, and $\deg v_{k+1} < \deg v_k$ for every $k < K$;

(c) $u_K \neq 0$, and $\gcd(f, g)$ is the monic associate of u_K.

In practice the sequence is written as a chain of divisions $u_k = q_k v_k + r_k$, $k = 0, \ldots, K - 1$, each dividing the previous divisor by the previous remainder, until a remainder is 0. The degrees of the remainders fall, and $u_K = v_{K-1}$ is the last non-zero remainder r_{K-2} if $K \geq 2$, and g itself if $K = 1$ (then $g \mid f$).

Second reading · *Why the sequence exists*

The sequence is well defined. Let $G\colon F[x] \times F[x] \to F[x] \times F[x]$ send (u, v) to (v, r), where r is the remainder of u on division by v, if $v \neq 0$, and to (u, v) if $v = 0$. This is a function, since the remainder exists and is unique (Theorem 5.1.2 (a)). The recursion theorem (Sets, Relations, and Cardinality, Theorem 2.3.1, read on $\mathbb{N} = \omega$ by Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)), with $X = F[x] \times F[x]$, starting value (f, g) and step $(k, P) \mapsto G(P)$, gives exactly one sequence of pairs with the displayed properties.

Idea. Part (a) is Lemma 5.2.4 once per step, carried along by induction. For (b), the degrees of the second entries are natural numbers that drop by at least one per step while the entries are non-zero, so a zero entry must come within $\deg g + 1$ steps. For (c), at the first zero, (a) reads $\langle f, g\rangle = \langle u_K, 0\rangle = \langle u_K\rangle$, and the monic generator of this ideal is the gcd.

Proof.

(a) We use Logic and Proof, Axiom 4.2.1 (through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) on k, for $P(k)$: "$\langle u_k, v_k\rangle = \langle f, g\rangle$". $P(0)$ holds since $(u_0, v_0) = (f, g)$. Suppose $P(k)$. If $v_k \neq 0$, then $u_k = q_k v_k + r_k$ for some q_k, and Lemma 5.2.4 gives $\langle u_{k+1}, v_{k+1}\rangle = \langle v_k, r_k\rangle = \langle u_k, v_k\rangle = \langle f, g\rangle$. If $v_k = 0$, the pair does not change, and $P(k+1)$ is $P(k)$.

(b) *A bound.* We show by Logic and Proof, Axiom 4.2.1 on k the statement $Q(k)$: "if $v_0, \ldots, v_k$ are all non-zero, then $\deg v_k + k \leq \deg g$". $Q(0)$ holds since $v_0 = g$. Suppose $Q(k)$, and let $v_0, \ldots, v_{k+1}$ be non-zero. Then $v_k \neq 0$, so $v_{k+1} = r_k$ has $\deg v_{k+1} < \deg v_k$, and as both degrees lie in $\mathbb{N}$, $\deg v_{k+1} + 1 \leq \deg v_k$. With $Q(k)$, $\deg v_{k+1} + (k+1) \leq \deg v_k + k \leq \deg g$, which is $Q(k+1)$.
The first zero. If $v_0, \ldots, v_k$ were all non-zero for $k := \deg g + 1$, then $Q(k)$ would give $\deg v_k \leq -1$, impossible for a non-zero polynomial. So $\{k \in \mathbb{N} : v_k = 0\}$ is non-empty, and it has a least element K (Sets, Relations, and Cardinality, Theorem 2.1.3). Since $v_0 = g \neq 0$, $K \geq 1$. By the choice of K, $v_0, \ldots, v_{K-1}$ are non-zero, so $Q(K-1)$ gives $0 \leq \deg v_{K-1} \leq \deg g - (K-1)$, that is, $K \leq \deg g + 1$. For $k < K$, $v_k \neq 0$, so $v_{k+1} = r_k$ and $\deg v_{k+1} < \deg v_k$ by Theorem 5.1.2 (a).

(c) Since $K - 1 < K$, $v_{K-1} \neq 0$, so the step gives $u_K = v_{K-1} \neq 0$. By (a) with $k = K$, and since $v_K = 0$,

$$\langle f, g\rangle = \langle u_K, 0\rangle = \langle u_K\rangle,$$

where $\langle u_K, 0\rangle = \{a u_K + b \cdot 0\} = \langle u_K\rangle$. Let $c := \operatorname{lc}(u_K)^{-1}$. The monic associate $c u_K$ generates the same ideal as u_K, because each is a multiple of the other ($u_K = c^{-1} \cdot c u_K$). So $c u_K$ is a monic generator of $\langle f, g\rangle$, and since $g \neq 0$, Theorem 5.2.2 (c) and the uniqueness in Theorem 5.2.1 (b) give $\gcd(f, g) = c u_K$.

■

To find a, b with $\gcd(f, g) = af + bg$, run the step of Lemma 5.2.4 backwards.

Algorithm. **Back-substitution.** Write out the divisions $u_k = q_k v_k + r_k$ for $k = 0, \ldots, K-1$, so that $u_{k+1} = v_k$ and $v_{k+1} = r_k$. Start from $u_K = 1 \cdot u_K + 0 \cdot v_K$. Then, for $k = K-1, K-2, \ldots, 0$ in turn, rewrite a combination $s u_{k+1} + t v_{k+1} = s v_k + t r_k$ as one of u_k and v_k, by substituting $r_k = u_k - q_k v_k$:

$$s v_k + t(u_k - q_k v_k) = t u_k + (s - t q_k) v_k.$$

After $k = 0$ the combination is one of $u_0 = f$ and $v_0 = g$; multiply it by $\operatorname{lc}(u_K)^{-1}$ to get $\gcd(f, g)$, and multiply out to check. (By hand one starts from the last division with a non-zero remainder, as in the example below.)

Nothing rests on the procedure: existence is Theorem 5.2.2 (d), and multiplying out checks the

a, b found.

Example. A run of the Euclidean algorithm

In $\mathbb{Q}[x]$, compute $\gcd(f, g)$ for $f = x^4 - x^3 - 3x^2 + x + 2$ and $g = x^3 - 2x - 1$, and write it as $af + bg$.

Solution. The chain of divisions (each by Theorem 5.1.2, the remainder of degree below the divisor's) is

$$x^4 - x^3 - 3x^2 + x + 2 = (x - 1)(x^3 - 2x - 1) + (1 - x^2),$$
$$x^3 - 2x - 1 = (-x)(1 - x^2) + (-x - 1),$$
$$1 - x^2 = (x - 1)(-x - 1) + 0.$$

So (u_k, v_k) runs through (f, g), $(g, 1-x^2)$, $(1-x^2, -x-1)$, $(-x-1, 0)$: $K = 3$ and $u_3 = -x-1$. Its monic associate is $x + 1$, so $\gcd(f, g) = x + 1$ by Theorem 5.2.5 (c).

Back-substitution, from the second division up:

$$-x - 1 = g + x(1 - x^2) = g + x(f - (x - 1)g)$$
$$= xf + (1 - x^2 + x)g.$$

Multiplying by -1:

$$x + 1 = (-x) \cdot f + (x^2 - x - 1) \cdot g.$$

Check: $(-x)f = -x^5 + x^4 + 3x^3 - x^2 - 2x$ and $(x^2 - x - 1)g = x^5 - x^4 - 3x^3 + x^2 + 3x + 1$; the sum is $x + 1$.

Warning. Bézout coefficients are **not** unique. Since $gf - fg = 0$,

$$x + 1 = (-x + g) \cdot f + (x^2 - x - 1 - f) \cdot g$$

as well, with coefficients of degrees 3 and 4. So "the" coefficients mean nothing by themselves; back-substitution produces one pair, and any other pair works as well.

Quick check. Run the algorithm on $f = x^3$ and $g = x^2 + 1$ in $\mathbb{Q}[x]$. Are they coprime?

Solution. $x^3 = x \cdot (x^2 + 1) + (-x)$, then $x^2 + 1 = (-x)(-x) + 1$, then $-x = (-x) \cdot 1 + 0$. The last non-zero remainder is 1, already monic, so $\gcd(x^3, x^2 + 1) = 1$: they are coprime. Back-substitution gives $1 = (x^2+1) - x^2 = (x^2+1) + x \cdot (-x) = (x^2+1) + x(x^3 - x(x^2+1)) = x \cdot x^3 + (1 - x^2)(x^2 + 1)$.

5.2.5 Changing the field

The same pair of polynomials can be read over a bigger field: $x^2 - 2 \in \mathbb{Q}[x]$ is also an element of $\mathbb{R}[x]$, where it factors as $(x - \sqrt{2})(x + \sqrt{2})$. Factorizations depend on the field; division and

the gcd do not, because the Euclidean algorithm never leaves the smaller field.

Recall that a **subfield** of a field L is a subset $K \subseteq L$ containing 0 and 1 and closed under $+$, $\cdot$, negatives and inverses of non-zero elements (Definition 2.3.1; Proposition 2.3.1 is the practical check). Then K is a field with the operations of L, and $K[x] \subseteq L[x]$: a polynomial with coefficients in K is one with coefficients in L, and sums, products, degrees and leading coefficients are computed by the same formulas in both rings. The examples are $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, with $\mathbb{R} \subseteq \mathbb{C}$ by Proposition 1.1.1 and Theorem 1.2.4.

Proposition 5.2.6. Division and gcd Do Not Depend on the Field

Let L be a field, $K \subseteq L$ a subfield, and $f, g \in K[x]$.

(a) If $g \neq 0$, the quotient and the remainder of f on division by g are the same in $K[x]$ and in $L[x]$.

(b) If $g \neq 0$, then $g \mid f$ in $L[x]$ if and only if $g \mid f$ in $K[x]$.

(c) $\gcd(f, g)$ is the same computed in $K[x]$ or in $L[x]$. In particular, f and g are coprime over K if and only if they are coprime over L.

In words: computing a quotient, a remainder or a gcd never needs an element outside the smaller field.

Second reading · *The proof: the algorithm never leaves the smaller field*

Proof.

(a) Let $f = qg + r$ with $q, r \in K[x]$ and $\deg r < \deg g$ be the division in $K[x]$ (Theorem 5.1.2 (a)). The same equation holds in $L[x]$, and the degrees are the same there, so it is a division with remainder in $L[x]$. By the uniqueness in $L[x]$, it is **the** division there.

(b) By (a), the remainder r is the same in both rings, and by Theorem 5.1.2 (b), applied in each ring, $g \mid f$ holds in that ring if and only if $r = 0$.

(c) If $f = g = 0$, both gcds are 0. If $g = 0 \neq f$, then $\langle f, 0\rangle = \langle f\rangle$ in either ring, generated by the monic associate $\mathrm{lc}(f)^{-1} f$, so $\gcd(f, 0) = \mathrm{lc}(f)^{-1} f$ in either ring (Theorem 5.2.2 (c) and the uniqueness in Theorem 5.2.1 (b)). The inverse $\mathrm{lc}(f)^{-1}$ is the same in K and in L, since K is closed under inverses and inverses in L are unique (Theorem 2.1.1 (c)). If $g \neq 0$, run Theorem 5.2.5 in $K[x]$ and in $L[x]$. By Logic and Proof, Axiom 4.2.1 (through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) on k, the pairs (u_k, v_k) agree: they agree for $k = 0$, and if they agree at k, the next pair is (v_k, r_k) with the same remainder r_k by (a), or the same pair. So the first index with $v_k = 0$ is the same in both runs, the polynomial u at that index is the same, and so is its monic associate, by the remark on inverses. By Theorem 5.2.5 (c), the two gcds are equal. In particular one is 1 if and only if the other is.

■

For example, x^2+1 and $x-1$ are coprime over $\mathbb{Q}$ ($x^2+1 = (x+1)(x-1)+2$ and $0\cdot(x-1)+\frac{1}{2}\cdot 2 = 1$; apply Lemma 5.2.4 and Corollary 5.2.3), so they are coprime over $\mathbb{C}$ as well, although $x^2 + 1 =$

$(x-i)(x+i)$ has factors of degree 1 only over $\mathbb{C}$.

Quick check. Compute $\gcd(x^2-2,\, x^3-2x)$ in $\mathbb{Q}[x]$. Over $\mathbb{R}$, $x-\sqrt{2}$ divides both. Why is the gcd over $\mathbb{R}$ still not $x-\sqrt{2}$?

Solution. The divisions are $x^2-2 = 0\cdot(x^3-2x)+(x^2-2)$ and $x^3-2x = x\cdot(x^2-2)+0$, so $K=2$ and $u_2 = x^2-2$, which is monic: $\gcd = x^2-2$ in $\mathbb{Q}[x]$. By Proposition 5.2.6 (c) it is x^2-2 in $\mathbb{R}[x]$ too. The common divisor $x-\sqrt{2}$ is not the gcd because the gcd must be divisible by **every** common divisor, and $x+\sqrt{2}$ is another one; both divide $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$.

Remark (Looking ahead). Section 5.6 uses part (b) of the last proposition with $\mathbb{R}\subseteq\mathbb{C}$, to bring a divisibility found in $\mathbb{C}[x]$ back to $\mathbb{R}[x]$.

5.2.6 Exercises

5.2.6.1 A. Check your understanding

Exercise. A1

These questions are about the proof of Theorem 5.2.1.

(a) Where is "least degree" used?

(b) Why is d made monic, and what would fail without it?

(c) Run the proof on $I := \{f\in\mathbb{Q}[x] : f(1)=0 \text{ and } f(-1)=0\}$: show that I is an ideal, and find d.

(d) The polynomials in two indeterminates x, y over $\mathbb{Q}$ with zero constant term (such as x, y, x^2y-3y) are closed under sums and under multiplication by any polynomial in x, y. Name the step of the proof that has no analogue there. (A prose answer; no proof that the theorem fails is asked for.)

(e) State the idea of the proof in two sentences.

Solution.

(a) Once, in ($\subseteq$): the remainder $r = f-qd$ lies in I and has degree below $n = \deg d$; since n is least among the degrees of non-zero elements of I, r cannot be non-zero, so $r=0$.

(b) For uniqueness. Every associate of d generates I (for instance $2d$ when $2\neq 0$ in F: $d = \frac{1}{2}\cdot 2d$), so without a normalization "the generator" would not be one polynomial. Exactly one associate is monic (Proposition 5.1.1 (f)).

(c) $I = I_1\cap I_{-1}$ in the notation after Definition 5.2.1. Each clause (I1)–(I3) holds in I_1 and in I_{-1}, hence in the intersection. The polynomial x^2-1 lies in I, since $1-1=0$ and $(-1)^2-1=0$. No non-zero element of I has degree at most 1: if $f=ax+b$ with $f(1)=a+b=0$ and $f(-1)=-a+b=0$, adding gives $2b=0$, so $b=0$ (as $2\neq 0$ in $\mathbb{Q}$), and then $a=0$. So the least degree is 2, and the proof's d is the monic element x^2-1 (any element of degree 2, scaled to be monic, is x^2-1 by the uniqueness clause).

Hence $I = \langle x^2 - 1 \rangle$.

(d) The division step, $f = qd + r$ with $\deg r < \deg d$, which the proof applies to an arbitrary $f \in I$ and the element d of least degree. Two indeterminates have no division with remainder of that kind. In this ideal, x and y both have the least possible degree, 1, and dividing y by x would need a leftover in the ideal of degree below 1, that is, 0; so x would have to divide y, and it does not. (That this ideal is generated by no single polynomial is true, but not proved here.)

(e) Take a non-zero element d of I of least degree, made monic. Dividing any element of I by d leaves a remainder that lies in I and has smaller degree, so it is 0, and I consists of the multiples of d.

5.2.6.2 B. Practice

Exercise. B1: A gcd and its common root

In $\mathbb{Q}[x]$, let $f = x^3 + x^2 + x + 1$ and $g = x^3 + x + 2$. Compute $\gcd(f, g)$ with the Euclidean algorithm, and write it as $af + bg$. Hence show that -1 is the only common root of f and g in $\mathbb{Q}$.

Solution. The divisions are

$$x^3 + x^2 + x + 1 = 1 \cdot (x^3 + x + 2) + (x^2 - 1),$$
$$x^3 + x + 2 = x \cdot (x^2 - 1) + (2x + 2),$$
$$x^2 - 1 = (\tfrac{1}{2}x - \tfrac{1}{2})(2x + 2) + 0.$$

So $K = 3$, $u_3 = 2x + 2$, and $\gcd(f, g) = x + 1$ (Theorem 5.2.5 (c)). Back-substitution:

$$2x + 2 = g - x(x^2 - 1) = g - x(f - g) = (-x)f + (x + 1)g,$$

so

$$x + 1 = (-\tfrac{1}{2}x)f + \tfrac{1}{2}(x + 1)g.$$

Check: $-\frac{1}{2}xf = -\frac{1}{2}(x^4 + x^3 + x^2 + x)$ and $\frac{1}{2}(x + 1)g = \frac{1}{2}(x^4 + x^3 + x^2 + 3x + 2)$; the sum is $\frac{1}{2}(2x + 2) = x + 1$.

Common roots. $f(-1) = -1 + 1 - 1 + 1 = 0$ and $g(-1) = -1 - 1 + 2 = 0$, so -1 is a common root. Let $c \in \mathbb{Q}$ be any common root. By Theorem 5.1.3 (b), $x - c$ divides f and g, so it divides $x + 1$ by Theorem 5.2.2 (b). Both are monic of degree 1, so they are associates by Theorem 5.2.2 (e) (equal degree), hence equal (Proposition 5.1.1 (f)). So $x - c = x + 1$, and $c = -1$.

Exercise. B2: A gcd over the field with two elements

In $\mathbb{F}_2[x]$, let $f = x^4 + x^3 + x + 1$ and $g = x^3 + x^2 + x + 1$. Show that $\gcd(f, g) = x^2 + 1$ and that $x^2 + 1 = 1 \cdot f + x \cdot g$.

Solution. In $\mathbb{F}_2$, $-1 = 1$ and $1 + 1 = 0$. First, $xg = x^4 + x^3 + x^2 + x$, so

$$f - xg = -x^2 + 1 = x^2 + 1,$$

that is, $f = x \cdot g + (x^2+1)$, a division with remainder. Next, $(x+1)(x^2+1) = x^3+x^2+x+1 = g$, so $g = (x + 1)(x^2 + 1) + 0$. The algorithm stops with $u_2 = x^2 + 1$, which is monic, so $\gcd(f, g) = x^2 + 1$. Finally $x^2 + 1 = f - xg = 1 \cdot f + x \cdot g$, since $-x = x$ in $\mathbb{F}_2[x]$.

5.2.6.3 C. Going deeper

Exercise. C1: Exit check: ideals of $F[x]$ and Bézout

Let F be a field.

(a) Prove that for every ideal $I \neq \{0\}$ of $F[x]$ there is exactly one monic d with $I = \langle d \rangle$.

(b) Let $f, g \in F[x]$, not both 0, and let d be the monic generator of $\langle f, g \rangle$. Prove that $d \mid f$, $d \mid g$, that every common divisor of f and g divides d, that $d = \gcd(f, g)$, and that $d = af + bg$ for some $a, b \in F[x]$.

Solution.

(a) *A generator.* The degrees of the non-zero elements of I form a non-empty subset of $\mathbb{N}$, which has a least element n (Sets, Relations, and Cardinality, Theorem 2.1.3). Let $e \in I$ be non-zero of degree n, and $d := \mathrm{lc}(e)^{-1}e$. Then $d \in I$ by (I3), and d is monic of degree n. Every multiple hd lies in I by (I3), so $\langle d \rangle \subseteq I$. Conversely, let $f \in I$, and divide: $f = qd + r$ with $\deg r < n$ (Theorem 5.1.2 (a)). Then $r = f + (-q)d \in I$ by (I3) and (I2). If $r \neq 0$, it is a non-zero element of I of degree less than n, against the choice of n; so $r = 0$ and $f \in \langle d \rangle$. Hence $I = \langle d \rangle$.
Uniqueness. If also $I = \langle d' \rangle$ with d' monic, then $d \in \langle d' \rangle$ and $d' \in \langle d \rangle$, so d and d' divide each other. Then $d' = cd$ for a non-zero constant c (Proposition 5.1.1 (f)), and comparing leading coefficients gives $c = 1$.

(b) The ideal $\langle f, g \rangle$ is not $\{0\}$, since it contains f and g; let d be its monic generator, from (a). Since $f, g \in \langle d \rangle$, $d \mid f$ and $d \mid g$. Since $d \in \langle f, g \rangle$, $d = af + bg$ for some $a, b \in F[x]$. If $h \mid f$ and $h \mid g$, then $h \mid af + bg = d$ (Proposition 5.1.1 (c)). So d is a monic common divisor that every common divisor divides: $d = \gcd(f, g)$ by Definition 5.2.2.

Marking scheme. (10 points) - 1: a non-zero element of least degree exists, with the well-ordering of $\mathbb{N}$ cited. - 1: it is made monic, and the monic element is shown to lie in I (absorption). - 3: an arbitrary element of I is divided by d, and the remainder is shown to lie in I. - 2: minimality of the degree forces the remainder to be 0. - 1: uniqueness of the monic generator (by any route: mutual divisibility, or minimality of the degree applied to the difference). - 2: $d \mid f$, $d \mid g$, $d = af + bg$, and "every common divisor divides d" are read off from $\langle f, g \rangle = \langle d \rangle$, and $d = \gcd(f, g)$ is concluded from the definition.

Fatal errors (0 for the step): assuming that the gcd is a combination of f and g (circular); "d divides f because d has least degree", with no division step; citing Theorem 5.2.5 (c) or the gcd clause of Lemma 5.2.4 for (b) (both are proved from Bézout's theorem). A second route for (b), the Euclidean algorithm with back-substitution by induction on the number of steps, may use the ideal equality of Lemma 5.2.4; it earns the 2 points of (b) when it shows that the monic associate of the last non-zero remainder divides f and g, is a combination of

them, and is divisible by every common divisor. Existence in (a) has no second route here.

Exercise. C2: Scaling the gcd

Let F be a field, $f, g \in F[x]$, and $h \in F[x]$ monic. Prove that $\gcd(hf, hg) = h \gcd(f, g)$.

Solution (Hint 1). Compare the ideals $\langle hf, hg\rangle$ and $\langle f, g\rangle$.

Solution (Hint 2). Show first that $\langle hf, hg\rangle = \{hu : u \in \langle f, g\rangle\}$.

Solution. If $f = g = 0$, then $hf = hg = 0$, and both sides are 0: $\gcd(0, 0) = 0 = h \cdot 0$.

Otherwise let $d := \gcd(f, g)$, monic, with $\langle f, g\rangle = \langle d\rangle$ (Theorem 5.2.2 (c)). Since h is monic, $h \neq 0$, and one of hf, hg is non-zero (Corollary 4.3.3 (a)); so Theorem 5.2.2 applies to (hf, hg) as well.

The ideals. For $a, b \in F[x]$, $a(hf) + b(hg) = h(af + bg)$. As a, b range over $F[x]$, $af + bg$ ranges over $\langle f, g\rangle = \langle d\rangle$, so

$$\langle hf, hg\rangle = \{h \cdot cd : c \in F[x]\} = \{c \cdot hd : c \in F[x]\} = \langle hd\rangle.$$

The generator. hd is monic, since $\mathrm{lc}(hd) = \mathrm{lc}(h)\,\mathrm{lc}(d) = 1$ (Theorem 4.3.2 (b)). By Theorem 5.2.2 (c), $\langle hf, hg\rangle = \langle \gcd(hf, hg)\rangle$ with $\gcd(hf, hg)$ monic; by the uniqueness in Theorem 5.2.1 (b), $\gcd(hf, hg) = hd = h \gcd(f, g)$.

This is the polynomial twin of Number Systems: From \(\nN\) to \(\nR\), Exercise (C2: Scaling the gcd) ($\gcd(ka, kb) = k \gcd(a, b)$ for $k > 0$), with "monic" in place of "positive". Without "monic" the formula fails: $\gcd(2x, 2) = 1 \neq 2 = 2 \gcd(x, 1)$ in $\mathbb{Q}[x]$.

Marking scheme. (10 points) - 2: treats $f = g = 0$ by the convention, and checks that hf, hg are not both 0 otherwise (no zero divisors in $F[x]$). - 4: shows $\langle hf, hg\rangle = \langle hd\rangle$, citing $\langle f, g\rangle = \langle d\rangle$. - 2: shows hd is monic. - 2: concludes $\gcd(hf, hg) = hd$ by the uniqueness of the monic generator.

Fatal errors (0 for the step): asserting that every common divisor of hf and hg is h times a common divisor of f and g (false: 1 divides $x \cdot x$ and $x \cdot (x + 1)$, and 1 is not x times a polynomial); using factorizations into irreducibles, which this section does not have. A second route ($hd = (hf)a + (hg)b$ is a monic common divisor and a combination, so every common divisor divides it) scores 2 for the zero case, 3 for "monic common divisor and combination", 3 for "every common divisor divides hd", 2 for the conclusion by Definition 5.2.2.

Exercise. C3: The gcd of two binomials

Let F be a field. For $m, n \in \mathbb{N}$, not both 0, prove that

$$\gcd(x^m - 1,\, x^n - 1) = x^{\gcd(m,n)} - 1$$

in $F[x]$ (here $x^0 - 1 = 0$, and $\gcd(m, n)$ is the integer gcd). Compute $\gcd(x^{12} - 1, x^{18} - 1)$.

Solution. Two remarks. For $m \geq 1$, $x^m - 1$ is monic of degree m. And for $m \geq n \geq 1$, by the power laws (Lemma 4.1.1 (c)),

$$x^m - 1 = x^{m-n}(x^n - 1) + (x^{m-n} - 1),$$

since $x^{m-n}x^n - x^{m-n} + x^{m-n} - 1 = x^m - 1$.

We prove, by Logic and Proof, Axiom 4.2.1 (through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) on s, the statement $P(s)$: "for all $m, n \in \mathbb{N}$, not both 0, with $m+n \leq s$, the displayed formula holds". $P(0)$ holds vacuously: $m+n \leq 0$ forces $m = n = 0$. Suppose $P(s)$, and let $m + n \leq s + 1$, not both 0. If $m + n \leq s$, use $P(s)$. Otherwise $m + n = s + 1$.

Case $n = 0$. Then $m \geq 1$. The gcd of $x^m - 1$ and 0 is the monic generator of $\langle x^m - 1, 0\rangle = \langle x^m - 1\rangle$ (Theorem 5.2.2 (c)), which is $x^m - 1$. On the integer side, the common divisors of m and 0 are the divisors of m, and the greatest is m (Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (a), (e)), so $\gcd(m, 0) = m$. Both sides are $x^m - 1$. *Case* $m = 0$ is the same, since both gcds are symmetric.

Case $m, n \geq 1$. Both gcds are symmetric, so we may suppose $m \geq n$. By the identity above and Lemma 5.2.4,

$$\gcd(x^m - 1, x^n - 1) = \gcd(x^n - 1, x^{m-n} - 1).$$

The pair $(n, m - n)$ is not $(0, 0)$, since $n \geq 1$, and $n + (m - n) = m < m + n = s + 1$, so $P(s)$ applies to it: the right side is $x^{\gcd(n,m-n)} - 1$. Finally $m = 1 \cdot n + (m - n)$, so Number Systems: From \(\nN\) to \(\nR\), Lemma 3.2.3 gives $\gcd(m, n) = \gcd(n, m - n)$. This proves $P(s + 1)$.

Since every pair (m, n) has $m + n \leq s$ for $s = m + n$, the formula holds for all m, n. For $m = 12$, $n = 18$: $\gcd(12, 18) = 6$, so $\gcd(x^{12} - 1, x^{18} - 1) = x^6 - 1$.

Each polynomial step is one step $(m, n) \mapsto (n, m-n)$ of the subtractive Euclidean algorithm on the exponents.

5.3 Irreducible Polynomials and Unique Factorization

Over every field, $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$. Over $\mathbb{Q}$ the last factor cannot be split further; over $\mathbb{F}_5$ it can, and $x^4 - 1$ becomes a product of four factors of degree 1; over $\mathbb{F}_2$ all of them coincide, and $x^4 - 1 = (x + 1)^4$. So the "primes" of $F[x]$ depend on the field F. Once F is fixed, though, every polynomial of positive degree splits into such primes in essentially one way, as every positive integer does in *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.3, and for the same reason: a prime that divides a product divides one of the factors.

Sections 5.1 and 5.2 supplied the tools: division with remainder (Theorem 5.1.2), the monic greatest common divisor and its Bézout identity (Theorem 5.2.2). This section spends them. Throughout, F is a field, and $F[x]$ is a commutative ring with no zero divisors (Theorem 4.2.4 (a), Corollary 4.3.3); degrees of products add (Theorem 4.3.2 (b)), and the units of $F[x]$ are the

non-zero constants (Proposition 5.1.1 (e)).

5.3.1 Irreducible polynomials

In $\mathbb{Z}$, a prime is a number $p \geq 2$ whose only positive divisors are 1 and p. Two features of that definition need adjusting for polynomials. "Positive" has no meaning in $F[x]$, and its job there was to ignore the units ± 1; in $F[x]$ the units are the non-zero constants, so we ignore those. And "$p \geq 2$" kept the units themselves from counting as primes; in $F[x]$ the condition becomes "degree at least 1".

An irreducible polynomial is one that cannot be split into two factors of smaller degree.

Definition 5.3.1. Irreducible Polynomial

Let F be a field and $p \in F[x]$. The polynomial p is **irreducible over** F if $\deg p \geq 1$ and, **whenever** $p = gh$ with $g, h \in F[x]$, **one** of g, h is a constant. A polynomial of degree at least 1 that is not irreducible over F is **reducible over** F.

In words: the first clause rules out 0 and the non-zero constants; the second says that every way of writing p as a product uses a constant factor. That constant is never 0, since $p \neq 0$. So p is reducible exactly when $p = gh$ with $\deg g \geq 1$ and $\deg h \geq 1$; then $\deg g + \deg h = \deg p$ (Theorem 4.3.2 (b)), so both factors have degree **strictly** less than $\deg p$.

Examples.

- Every polynomial of degree 1 is irreducible. If $p = gh$ with $\deg p = 1$, the degrees of g and h are natural numbers adding up to 1, so one of them is 0.
- $x^2 + x = x(x + 1)$ and $x^3 = x \cdot x^2$ are reducible over every field: each is a product of two factors of degree at least 1.
- $x^2 + 1$ is reducible over $\mathbb{F}_2$, where $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ because $2 = 0$. Over $\mathbb{Q}$ it is irreducible, as the next proposition shows. The polynomial is the same; the field changed, and with it the answer. This is why the definition says "over F".
- If p is irreducible and $a \in F$ is non-zero, then ap is irreducible. First, $\deg(ap) = \deg p \geq 1$ (Theorem 4.3.2 (b)), and a factorization $ap = gh$ gives $p = (a^{-1}g)h$, so $a^{-1}g$ or h is a constant, and then so is g or h. Associates of irreducibles are irreducible.

↻ **Second reading** · *The degenerate cases: constants*

The constants are kept out by the first clause, and each for a reason. Without it, the polynomial 0 would pass the second clause, since every factorization $0 = gh$ has $g = 0$ or $h = 0$ (Corollary 4.3.3), a constant. But every polynomial divides 0 (Proposition 5.1.1 (a)), so 0 behaves like the integer 0, not like a prime. A non-zero constant a is a unit: it divides everything, and every factorization $a = gh$ has two constant factors, since the degrees add up to 0. If units counted as irreducible, every factorization could be padded with as many of them as we like, just as $(1, 2, 2, 3, 5)$ would pad the factorization of 60 if 1 were prime. The clause $\deg p \geq 1$ plays the part of the integer condition $p \geq 2$.

For polynomials of degree 2 and 3, irreducibility can be decided by looking for roots.

Proposition 5.3.1. Irreducibility in Low Degree

Let F be a field and $p \in F[x]$.

(a) If $\deg p \geq 2$ and p has a root in F, then p is reducible over F.

(b) If $\deg p \in \{2, 3\}$, then p is irreducible over F **if and only if** p has no root in F.

Proof. *(a)* Let $c \in F$ be a root of p. By Theorem 5.1.3 (b), $p = (x - c)q$ for some $q \in F[x]$. Then $\deg q = \deg p - 1 \geq 1$ by Theorem 4.3.2 (b), and $\deg(x - c) = 1$, so neither factor is a constant and p is reducible.

(b) ($\Rightarrow$) is (a), read contrapositively. ($\Leftarrow$) Suppose p is reducible, so $p = gh$ with $\deg g, \deg h \geq 1$ and $\deg g + \deg h = \deg p \in \{2, 3\}$. Two natural numbers, each at least 1, with sum 2 or 3: one of them is 1. So p has a factor of degree 1, and Theorem 5.1.3 (c) gives a root of p in F.

■

For $x^2 + 1$ over $\mathbb{Q}$: for every $c \in \mathbb{Q}$, $c^2 \geq 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e), with $0^2 = 0$), so $c^2 + 1 \geq 1 > 0$ by (b) and (e) of the same proposition. There is no rational root, and (b) makes $x^2 + 1$ irreducible over $\mathbb{Q}$. The same lines work in every ordered field, so $x^2 + 1$ is irreducible over $\mathbb{R}$ as well.

Warning. **"No root" does not mean "irreducible" in degree 4 and above.** For $c \in \mathbb{Q}$, $c^4 = (c^2)^2 \geq 0$, so $c^4 + 4 \geq 4 > 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (h)): the polynomial $x^4 + 4$ has no rational root. Yet

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2),$$

as expanding the right side shows: the terms in x^3, x^2 and x cancel. Proposition Proposition 5.3.1 (b) is about degrees 2 and 3 only, where every splitting must contain a factor of degree 1; in degree 4 a splitting may be $2 + 2$, with no factor of degree 1 and so no root.

Quick check. Is $2x^2 + 4$ irreducible over $\mathbb{Q}$? Is $x^2 + 2$ irreducible over $\mathbb{F}_3$?

Solution. Over $\mathbb{Q}$, yes: $2x^2 + 4 = 2(x^2 + 2)$, and $x^2 + 2$ has no rational root ($c^2 + 2 \geq 2 > 0$, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e), (h)), so it is irreducible by Proposition 5.3.1 (b), and so is its associate $2x^2 + 4$. The factor 2 is a constant, so $2 \cdot (x^2 + 2)$ is not a splitting into non-constants. Over $\mathbb{F}_3$, no: $1^2 + 2 = 3 = 0$, so 1 is a root, and indeed $x^2 + 2 = x^2 - 1 = (x - 1)(x + 1)$ in $\mathbb{F}_3$.

5.3.2 Euclid's lemma for polynomials

The definition of an irreducible p speaks about the factors **of** p. Unique factorization needs a statement about the polynomials that p **divides**. As in $\mathbb{Z}$, the bridge is the Bézout identity,

and the move is the one of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.3: **multiply the Bézout identity**.

Theorem 5.3.2. Euclid's Lemma for Polynomials

Let F be a field and $f, g, h \in F[x]$. If $f \mid gh$ and $\gcd(f, g) = 1$, then $f \mid h$.

Proof. Since $\gcd(f, g) = 1$, Corollary 5.2.3 gives $a, b \in F[x]$ with $af + bg = 1$. Multiplying by h,

$$h = h(af + bg) = (ah)f + b(gh).$$

Now $f \mid f$ and $f \mid gh$, so f divides the combination $(ah)f + b(gh)$ (Proposition 5.1.1 (c)). Hence $f \mid h$.

■

The hypothesis $\gcd(f, g) = 1$ is needed. In $\mathbb{Q}[x]$, $x^2 \mid x \cdot x$, but $x^2 \nmid x$, since a divisor of a non-zero polynomial has degree at most its degree (Proposition 5.1.1 (d)); here $\gcd(x^2, x) = x$.

For an irreducible p, the coprimality comes almost free, exactly as it did for a prime number.

Corollary 5.3.3. An Irreducible Dividing a Product

Let F be a field and $p \in F[x]$ irreducible over F.

(a) For every $f \in F[x]$: $p \mid f$ or $\gcd(p, f) = 1$.

(b) For all $g, h \in F[x]$: if $p \mid gh$, then $p \mid g$ or $p \mid h$.

(c) If $(q_1, \ldots, q_l)$ is a list of polynomials in $F[x]$, with $l \in \mathbb{N}$, and $p \mid q_1 q_2 \cdots q_l$, then $l \geq 1$ and $p \mid q_j$ for some $j \in \{1, \ldots, l\}$.

(d) If p and q are monic and irreducible over F and $p \mid q$, then $p = q$.

Here $q_1 q_2 \cdots q_l$, also written $\prod_{j=1}^{l} q_j$, is the product of a finite list in the commutative ring $F[x]$, given by the recursion of Sets, Relations, and Cardinality, Definition 2.3.1 as Lemma 4.1.1 (a) reads it: the empty product is 1, and $\prod_{j=1}^{l+1} q_j = (\prod_{j=1}^{l} q_j) q_{l+1}$.

Idea. For (a), the gcd of p and f is a monic divisor of p, and an irreducible p has only two kinds of divisors: constants and associates of itself. Part (b) is Euclid's lemma in the coprime case of (a). For (c), peel the last factor off the product and apply (b); induction on the length does the rest. For (d), the cofactor of p in q must be a constant, and comparing leading coefficients makes it 1.

Proof. *(a)* Since $p \neq 0$, the gcd $d := \gcd(p, f)$ is monic (Definition 5.2.2, Theorem 5.2.2 (c)). It divides p: write $p = du$ with $u \in F[x]$. As p is irreducible, d or u is a constant. If d is a constant, it is a monic constant, so $d = 1$. If u is a constant, then $u \neq 0$ (as $p \neq 0$) and $d = u^{-1}p$; since $d \mid f$, $f = dk = p(u^{-1}k)$ for some $k \in F[x]$, so $p \mid f$.

(b) Let $p \mid gh$. By (a), $p \mid g$ or $\gcd(p, g) = 1$, and in the second case Theorem 5.3.2 gives $p \mid h$.

(c) By Logic and Proof, Axiom 4.2.1 (on $\mathbb{N} = \omega$, Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) we prove, for every $l \in \mathbb{N}$, the statement $P(l)$: "for every list $(q_1, \ldots, q_l)$ in $F[x]$ with $p \mid \prod_{j=1}^{l} q_j$, we have $l \geq 1$ and $p \mid q_j$ for some $j \leq l$".

Base case $P(0)$. The empty product is 1, and $p \nmid 1$: otherwise $\deg p \leq \deg 1 = 0$ by Proposition 5.1.1 (d), against $\deg p \geq 1$. So the hypothesis of $P(0)$ never holds, and $P(0)$ is true.

Step. Assume $P(l)$, and let $p \mid \prod_{j=1}^{l+1} q_j = (\prod_{j=1}^{l} q_j) q_{l+1}$. By (b), p divides the first factor or $p \mid q_{l+1}$. In the first case $P(l)$ gives $j \leq l$ with $p \mid q_j$; in the second, take $j = l + 1$. Either way $l + 1 \geq 1$, and $P(l + 1)$ holds.

(d) Write $q = pu$ with $u \in F[x]$. As q is irreducible, p or u is a constant, and p is not, since $\deg p \geq 1$. So u is a non-zero constant, and comparing leading coefficients (Theorem 4.3.2 (b)) gives $1 = 1 \cdot u$. Hence $u = 1$ and $p = q$.

■

Part (b) fails for reducible polynomials: $x^2 \mid x \cdot x$ with $x^2 \nmid x$. Part (d) needs "monic": x and $2x$ are irreducible over $\mathbb{Q}$, and each divides the other.

The same multiplication of a Bézout identity combines two coprime divisors.

Proposition 5.3.4. Coprime Divisors of a Polynomial

Let F be a field and $m, n, h \in F[x]$ with $m \mid h$, $n \mid h$ and $\gcd(m, n) = 1$. Then $mn \mid h$.

Proof. Write $h = mk$ with $k \in F[x]$. Then $n \mid mk$, and $\gcd(n, m) = \gcd(m, n) = 1$, since the clauses of Definition 5.2.2 do not depend on the order of the two polynomials. By Theorem 5.3.2, $n \mid k$; say $k = nt$. Then $h = m(nt) = (mn)t$, so $mn \mid h$.

■

Without coprimality the conclusion fails: $x \mid x$ twice over, yet $x \cdot x = x^2 \nmid x$.

Quick check. In $\mathbb{F}_2[x]$, the polynomial $x^2 + 1$ divides $(x+1)(x+1)$, but divides neither factor. Does this contradict Corollary 5.3.3 (b)?

Solution. No. In $\mathbb{F}_2[x]$, $(x + 1)(x + 1) = x^2 + 1$, so $x^2 + 1$ is reducible over $\mathbb{F}_2$, and the corollary says nothing about it. (It divides neither factor because each factor has degree $1 < 2$, Proposition 5.1.1 (d).)

5.3.3 Factors that cannot be split further

The existence half of unique factorization needs a supply of irreducibles: every polynomial of positive degree must have an irreducible factor. In $\mathbb{Z}$, the least divisor at least 2 was prime (Number Systems: From \(\nN\) to \(\nR\), Lemma 3.3.4). For polynomials, size becomes

degree, and the "least divisor" becomes a monic divisor of least positive degree.

Lemma 5.3.5. An Irreducible Factor Exists

Let F be a field and $f \in F[x]$ with $\deg f \geq 1$. Then f has a **monic** irreducible divisor in $F[x]$.

Idea. Among the monic divisors of positive degree, take one of least degree. A splitting of it into two non-constants would produce a monic divisor of smaller positive degree.

Proof. Let c be the leading coefficient of f, and let

$$D := \{\deg d : d \in F[x] \text{ monic},\ \deg d \geq 1,\ d \mid f\} \subseteq \mathbb{N}.$$

The monic associate $c^{-1}f$ has degree $\deg f \geq 1$ and divides $f = c \cdot (c^{-1}f)$, so D is non-empty. By Sets, Relations, and Cardinality, Theorem 2.1.3 (on $\mathbb{N} = \omega$ it is Number Systems: From \(\nN\) to \(\nR\), Theorem 1.6.2), D has a least element n_0; let p be a monic divisor of f of degree n_0. Then $\deg p = n_0 \geq 1$.

Suppose $p = gh$ with $\deg g \geq 1$ and $\deg h \geq 1$. Then $\deg g = n_0 - \deg h < n_0$ (Theorem 4.3.2 (b)). Let g_1 be the monic associate of g, so $g = \mathrm{lc}(g)\, g_1$ and $\deg g_1 = \deg g$. Then $g_1 \mid g$, $g \mid p$ and $p \mid f$, so $g_1 \mid f$ (Proposition 5.1.1 (b)), and $\deg g_1 \in D$ is smaller than n_0, against the choice of n_0. So every factorization $p = gh$ has a constant factor, and p is irreducible. ∎

This is Number Systems: From \(\nN\) to \(\nR\), Lemma 3.3.4 with degree in place of size; the twin is compared with, not used.

5.3.4 Unique factorization

Two facts about products of lists. The proof below handles lists of polynomials, and it uses two facts about their products, both proved by induction on the length from the recursion of the product. Let $(q_1, \ldots, q_l)$ be a list in $F[x]$, with $l \in \mathbb{N}$.

(L1) If every q_j is non-zero, then $\prod_{j=1}^{l} q_j \neq 0$, and its degree is $\sum_{j=1}^{l} \deg q_j$. If every q_j is monic, so is the product.

(L2) If $l \geq 1$ and $j \in \{1, \ldots, l\}$, let $(q'_1, \ldots, q'_{l-1})$ be the list with the entry j removed: $q'_t := q_t$ for $t < j$ and $q'_t := q_{t+1}$ for $j \leq t \leq l-1$. Then $\prod_{t=1}^{l} q_t = (\prod_{t=1}^{l-1} q'_t) q_j$. In particular every entry of a list divides its product.

The names (L1), (L2) are used throughout this chapter.

↻ **Second reading** · *Proofs of (L1) and (L2)*

(L1). Induction on l. For $l = 0$ the product is 1, which is monic of degree 0, the empty sum. If the claim holds for l, then $\prod_{j=1}^{l+1} q_j = (\prod_{j=1}^{l} q_j) q_{l+1}$ is a product of two non-zero polynomials, so it is non-zero with degree $\sum_{j=1}^{l} \deg q_j + \deg q_{l+1}$ and leading coefficient the product of the two

leading coefficients (Theorem 4.3.2 (b)); that is $1 \cdot 1 = 1$ when both factors are monic.

(L2). Induction on $l \geq 1$, for all $j \leq l$ at once. For $l = 1$, $j = 1$, the shortened list is empty and both sides are q_1. Suppose the claim holds for lists of length l, and let $(q_1, \ldots, q_{l+1})$ and $j \leq l+1$ be given. If $j = l+1$, the shortened list is $(q_1, \ldots, q_l)$ and the claim is the recursion itself. If $j \leq l$, the claim for the list $(q_1, \ldots, q_l)$ and the same j gives $\prod_{t=1}^{l} q_t = (\prod_{t=1}^{l-1} r_t) q_j$, where $(r_1, \ldots, r_{l-1})$ is $(q_1, \ldots, q_l)$ with entry j removed. The list $(q'_1, \ldots, q'_l)$ obtained from $(q_1, \ldots, q_{l+1})$ has the first $l-1$ entries $r_1, \ldots, r_{l-1}$ and the last entry $q'_l = q_{l+1}$. So, by the recursion twice and commutativity and associativity in $F[x]$,

$$\begin{aligned} \prod_{t=1}^{l+1} q_t &= \Big(\prod_{t=1}^{l-1} r_t\Big) q_j \, q_{l+1} \\ &= \Big(\Big(\prod_{t=1}^{l-1} r_t\Big) q_{l+1}\Big) q_j = \Big(\prod_{t=1}^{l} q'_t\Big) q_j. \end{aligned}$$

The last clause of (L2) follows: q_j divides $(\prod_t q'_t) q_j$.

Everything is now in place.

Theorem 5.3.6. Unique Factorization of Polynomials

Let F be a field and $f \in F[x]$ with $\deg f \geq 1$ and leading coefficient c.

(a) **Existence.** There are $k \geq 1$ and monic polynomials $p_1, \ldots, p_k$, irreducible over F, with $f = c\, p_1 p_2 \cdots p_k$.

(b) **Uniqueness.** If also $f = c' q_1 q_2 \cdots q_l$ with $c' \in F$, $l \in \mathbb{N}$ and monic polynomials $q_1, \ldots, q_l$ irreducible over F, then $c' = c$, $l = k$, and there is a bijection $\sigma\colon \{1, \ldots, k\} \to \{1, \ldots, l\}$ (Sets, Relations, and Cardinality, Definition 1.4.5) with $q_{\sigma(i)} = p_i$ for every i.

In words: every polynomial of positive degree is its leading coefficient times a product of monic irreducibles, and the leading coefficient and the irreducibles, counted with repetition, are determined by f; only their order is free. The bijection σ says "the same list, possibly in another order": it matches each p_i with an equal $q_{\sigma(i)}$, and each q is used exactly once.

Idea. Existence. Split off one monic irreducible factor (Lemma 5.3.5); the cofactor has smaller degree, so strong induction on the degree factors it.

Uniqueness. Divide by the leading coefficient, so that both products are equal products of monic irreducibles. The last factor p_{k+1} of one list divides the other product, so by Euclid's lemma (in the form Corollary 5.3.3 (c)) it divides one of the q_j, and, both being monic and irreducible, it **equals** it. Cancel it from both sides and use induction on the length.

Before reading on: where is Euclid's lemma used, and why does "monic" turn "p_{k+1} is a constant times q_j" into "$p_{k+1} = q_j$"?

Proof. Existence. We prove, by Logic and Proof, Theorem 4.2.2 on $n \in \mathbb{N}$ (read on ω: its proof uses only Logic and Proof, Axiom 4.2.1 and Number Systems: From \(\nN\) to \(\nR\), Theorem 1.6.1 (a), (b), (d), as in Section 3.1), the statement $E(n)$: "every **monic** $g \in F[x]$ of degree $n \geq 1$ is a product $p_1 \cdots p_k$ of a list of monic irreducibles, $k \geq 1$". For $n = 0$ there is nothing to prove. Let $n \geq 1$, assume $E(m)$ for every $m < n$, and let g be monic of degree n. By Lemma 5.3.5, $g = pu$ with p monic and irreducible, and $u \in F[x]$. Comparing leading coefficients (Theorem 4.3.2 (b)), $1 = 1 \cdot \mathrm{lc}(u)$, so u is monic, and $\deg u = n - \deg p < n$. If $\deg u = 0$, then $u = 1$ and $g = p$ is a list of length 1. Otherwise $E(\deg u)$ gives $u = p_1 \cdots p_r$ with monic irreducibles p_i, and the list $(p_1, \ldots, p_r, p)$ has, by the recursion, the product $(\prod_{i=1}^{r} p_i)p = up = g$. This proves $E(n)$.

Now let f be as in the theorem. Its monic associate $c^{-1}f$ has degree $\deg f \geq 1$, so $c^{-1}f = p_1 \cdots p_k$ by $E(\deg f)$, and $f = c\,p_1 \cdots p_k$.

Uniqueness. By (L1), $q_1 \cdots q_l$ is monic. As $f \neq 0$, $c' \neq 0$, and comparing leading coefficients in $f = c'q_1 \cdots q_l$ (Theorem 4.3.2 (b)) gives $c = c' \cdot 1 = c'$. Multiplying both expressions for f by c^{-1},

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l.$$

It remains to prove, by Logic and Proof, Axiom 4.2.1 on $k \in \mathbb{N}$, the statement $U(k)$: "for every $l \in \mathbb{N}$, if $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_l)$ are lists of monic irreducibles with $\prod_{i=1}^{k} p_i = \prod_{j=1}^{l} q_j$, then $l = k$ and there is a bijection $\sigma\colon \{1, \ldots, k\} \to \{1, \ldots, l\}$ with $q_{\sigma(i)} = p_i$ for every $i \leq k$".

Base case $U(0)$. The empty product is 1, of degree 0. By (L1), $\prod_{j=1}^{l} q_j$ has degree $\sum_j \deg q_j \geq l$, since each $\deg q_j \geq 1$. So $l = 0$, and the empty function $\emptyset \to \emptyset$ is the required bijection.

Step. Assume $U(k)$, and let $(p_1, \ldots, p_{k+1})$ and $(q_1, \ldots, q_l)$ be lists of monic irreducibles with the same product N. By the recursion, $N = (\prod_{i=1}^{k} p_i)p_{k+1}$, so $p_{k+1} \mid N = \prod_{j=1}^{l} q_j$. By Corollary 5.3.3 (c), $l \geq 1$ and $p_{k+1} \mid q_j$ for some $j \leq l$; by Corollary 5.3.3 (d), $p_{k+1} = q_j$. Let $(q'_1, \ldots, q'_{l-1})$ be the q-list with entry j removed. By (L2),

$$\Big(\prod_{i=1}^{k} p_i\Big)p_{k+1} = N = \Big(\prod_{t=1}^{l-1} q'_t\Big)q_j = \Big(\prod_{t=1}^{l-1} q'_t\Big)p_{k+1}.$$

Since $p_{k+1} \neq 0$, we may cancel it (Corollary 4.3.3 (b)): $\prod_{i=1}^{k} p_i = \prod_{t=1}^{l-1} q'_t$. The list $(q'_1, \ldots, q'_{l-1})$ consists of monic irreducibles, so $U(k)$, applied with $l - 1 \in \mathbb{N}$, gives $l - 1 = k$ and a bijection $\sigma'\colon \{1, \ldots, k\} \to \{1, \ldots, l-1\}$ with $q'_{\sigma'(i)} = p_i$.

Let $\tau\colon \{1, \ldots, l-1\} \to \{1, \ldots, l\} \setminus \{j\}$ be $\tau(t) \coloneqq t$ for $t < j$ and $\tau(t) \coloneqq t + 1$ for $t \geq j$. It is a bijection (its inverse sends $s < j$ to s and $s > j$ to $s - 1$), and $q'_t = q_{\tau(t)}$ by the definition of q'. Define $\sigma\colon \{1, \ldots, k+1\} \to \{1, \ldots, l\}$ by $\sigma(i) \coloneqq \tau(\sigma'(i))$ for $i \leq k$ and $\sigma(k+1) \coloneqq j$. On $\{1, \ldots, k\}$, σ is a bijection onto $\{1, \ldots, l\} \setminus \{j\}$, a composite of two bijections; and it sends $k + 1$ to the one remaining point j. So σ is injective and surjective, a bijection. Finally $q_{\sigma(i)} = q_{\tau(\sigma'(i))} = q'_{\sigma'(i)} = p_i$ for $i \leq k$, and $q_{\sigma(k+1)} = q_j = p_{k+1}$; and $l = k + 1$. This proves $U(k + 1)$, and the theorem.

■

The answer to the prompt. Euclid's lemma enters at one line, "$p_{k+1} \mid q_j$ for some j": that is Corollary 5.3.3 (c), whose step is (b), which is Theorem 5.3.2 in the coprime case. "Monic" enters twice. Irreducibility of q_j only gives $q_j = p_{k+1}u$ with u a non-zero constant; both being monic forces $u = 1$ (part (d)), and without that the cancellation would leave a stray constant

u on one side. And the leading coefficients c, c' can be compared only because the products of monic lists are monic.

Remark. In $\mathbb{Z}$, *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.3 stated uniqueness for **non-decreasing** lists of primes (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.3.5), so that two factorizations of the same number are literally equal. Polynomials have no natural order to sort by, so here "the same up to order" is said with a bijection of indices.

Example. The Factorizations of $x^4 - 1$

Factor $x^4 - 1$ into monic irreducibles over $\mathbb{Q}$, over $\mathbb{R}$, over $\mathbb{F}_3$, over $\mathbb{F}_5$ and over $\mathbb{F}_2$.

Solution. Over every field, $(x-1)(x+1) = x^2-1$ and $(x^2-1)(x^2+1) = x^4-1$, by expanding, so

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1).$$

The two factors of degree 1 are irreducible. Everything depends on $x^2 + 1$, which by Proposition 5.3.1 (b) is irreducible exactly when it has no root in the field.

- $\mathbb{Q}$ **and** $\mathbb{R}$**.** No root, since $c^2 + 1 \geq 1 > 0$ in an ordered field (after Proposition 5.3.1). So $(x - 1, x + 1, x^2 + 1)$ is the factorization, with leading coefficient 1.
- $\mathbb{F}_3$**.** The values of $x^2 + 1$ at $0, 1, 2$ are $1, 2, 5 = 2$: no root. The factorization is $(x - 1, x + 1, x^2 + 1)$ again, with $x + 1 = x - 2$.
- $\mathbb{F}_5$**.** Here $2^2 + 1 = 5 = 0$, and indeed $(x - 2)(x - 3) = x^2 - 5x + 6 = x^2 + 1$ in $\mathbb{F}_5$. So $x^4 - 1 = (x - 1)(x - 2)(x - 3)(x - 4)$, using $x + 1 = x - 4$: four factors of degree 1.
- $\mathbb{F}_2$**.** Here $-1 = 1$, so $x - 1 = x + 1$, and $x^2 + 1 = (x + 1)^2$ (the example after Definition 5.3.1). So $x^4 - 1 = (x + 1)^4$: one irreducible, four times.

By Theorem 5.3.6, each of these lists is the only one up to order.

Quick check. Is $x^2 + x + 1$ irreducible over $\mathbb{F}_2$? Over $\mathbb{F}_3$?

Solution. Over $\mathbb{F}_2$, its values at 0 and 1 are 1 and $3 = 1$: no root, so it is irreducible (Proposition 5.3.1 (b)). Over $\mathbb{F}_3$, $1 + 1 + 1 = 3 = 0$, so 1 is a root and it is reducible; indeed $(x - 1)^2 = x^2 - 2x + 1 = x^2 + x + 1$ in $\mathbb{F}_3$.

5.3.5 Rational roots

Over $\mathbb{Q}$, the low-degree test of Proposition 5.3.1 asks for rational roots, and there are infinitely many rationals to try. For a polynomial with integer coefficients and non-zero constant term the candidates can be listed (a zero constant term is dealt with by factoring out a power of x, below). The proof is about integers, not polynomials: here, unlike in the rest of this section, integer results of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3 (Euclid's lemma, lowest terms) are steps of the proof and not only compared with.

Theorem 5.3.7. Rational Root Test

Let $n \geq 1$, let $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ with $a_n \neq 0$, and let $f := \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$. If $u \in \mathbb{Z}$, $v \in \mathbb{Z}_{>0}$, $\gcd(u, v) = 1$ and $f(u/v) = 0$, then $u \mid a_0$ and $v \mid a_n$ in $\mathbb{Z}$.

Idea. Clear denominators: $v^n f(u/v) = 0$ is an equation in $\mathbb{Z}$ in which every term but one is a multiple of u, and every term but another is a multiple of v. Then Euclid's lemma for integers strips the powers of v from $a_0 v^n$, one at a time.

Proof. Multiply $f(u/v) = 0$ by v^n. For $i \leq n$, $(u/v)^i v^i = u^i$ and $v^n = v^{n-i} v^i$ (Lemma 4.1.1 (c), in the commutative ring $\mathbb{Q}$), so

$$a_n u^n + a_{n-1} u^{n-1} v + \cdots + a_1 u v^{n-1} + a_0 v^n = 0,$$

an equation between integers. Every term except the last contains the factor u, and every term except the first contains the factor v (as $n \geq 1$). So

$$a_0 v^n = -u \sum_{i=1}^{n} a_i u^{i-1} v^{n-i}, \qquad a_n u^n = -v \sum_{i=0}^{n-1} a_i u^i v^{n-1-i},$$

and $u \mid a_0 v^n$, $v \mid a_n u^n$ in $\mathbb{Z}$.

We show $u \mid a_0 v^{n-j}$ for every $j \leq n$, by Logic and Proof, Axiom 4.2.1 on j. The case $j = 0$ is the line above. If $u \mid a_0 v^{n-j}$ with $j < n$, then $a_0 v^{n-j} = v \cdot (a_0 v^{n-j-1})$, and $\gcd(u, v) = 1$, so Number Systems: From \(\nN\) to \(\nR\), Theorem 3.3.1 gives $u \mid a_0 v^{n-(j+1)}$. At $j = n$: $u \mid a_0$. The same induction with the roles of u and v exchanged (and $\gcd(v, u) = \gcd(u, v) = 1$) turns $v \mid a_n u^n$ into $v \mid a_n$.

■

Every rational root has such a form: by Number Systems: From \(\nN\) to \(\nR\), Proposition 3.3.6, each $r \in \mathbb{Q}$ is u/v with $u \in \mathbb{Z}$, $v \in \mathbb{Z}_{>0}$ and $\gcd(u, v) = 1$. So, when $a_0 \neq 0$, the rational roots of f are among the finitely many fractions u/v with $u \mid a_0$ and v a positive divisor of a_n: a divisor u of $a_0 \neq 0$ has $-|a_0| \leq u \leq |a_0|$, by Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (d), (e), and likewise $1 \leq v \leq |a_n|$. If $a_0 = 0$, then 0 is a root; let k be the least index with $a_k \neq 0$ (so $k \leq n$). Then $f = x^k g$ with $g := \sum_{i=0}^{n-k} a_{i+k} x^i$, which has integer coefficients and constant term $a_k \neq 0$, and the non-zero rational roots of f are those of g, since $f(r) = r^k g(r)$ (Theorem 4.4.1) and $\mathbb{Q}$ has no zero divisors; apply the test to g when $\deg g \geq 1$, and when $\deg g = 0$, g has no root. The test lists candidates; it does not say which of them are roots.

Example. A Cubic with No Rational Root

Show that $3x^3 + x^2 - 2$ is irreducible over $\mathbb{Q}$.

Solution. By Theorem 5.3.7, a rational root u/v in lowest terms has $u \mid -2$ and v a positive divisor of 3. The divisors of -2 are $\pm 1, \pm 2$, and the positive divisors of 3 are $1, 3$ (a positive

divisor of 3 is at most 3, Number Systems: From \(\nN\) to \(\nR\), Proposition 3.1.1 (e), and $3 = 1 \cdot 2 + 1$). So the candidates are $\pm 1, \pm 2, \pm 1/3, \pm 2/3$. The values of $f := 3x^3 + x^2 - 2$ at them are

c	1	-1	2	-2	$1/3$	$-1/3$	$2/3$	$-2/3$
$f(c)$	2	-4	26	-22	$-16/9$	-2	$-2/3$	$-22/9$

For instance $f(2/3) = 3 \cdot \frac{8}{27} + \frac{4}{9} - 2 = \frac{8}{9} + \frac{4}{9} - 2 = -\frac{2}{3}$. None is 0, so f has no rational root, and as $\deg f = 3$, Proposition 5.3.1 (b) makes f irreducible over $\mathbb{Q}$.

Quick check. Which rational numbers can be roots of $2x^2 + 3x - 2$? Which are?

Solution. The candidates are u/v with $u \mid -2$ and $v \in \{1, 2\}$: $\pm 1, \pm 2, \pm 1/2$. Evaluating, the roots are $1/2$ and -2; indeed $2x^2 + 3x - 2 = (2x - 1)(x + 2)$.

Remark (Looking ahead). Two sharper tests for irreducibility over $\mathbb{Q}$, Gauss's lemma and Eisenstein's criterion, belong to a later algebra volume of the series; nothing in this volume uses them.

5.3.6 Exercises

5.3.6.1 A. Check your understanding

Exercise. A1

These questions are about the uniqueness half of the proof of Theorem 5.3.6.

(a) Which line of the proof uses Euclid's lemma, and through which result?

(b) Where is "monic" used?

(c) In $\mathbb{F}_5[x]$, run the induction step on the two lists $(p_1, p_2, p_3, p_4) = (x-1, x-2, x-3, x-4)$ and $(q_1, q_2, q_3, q_4) = (x-4, x-3, x-2, x-1)$. Which j matches p_4? What is the bijection σ at the end?

(d) Why must the empty list be allowed?

(e) Give the idea of the uniqueness proof in two sentences.

Solution.

(a) The line "$p_{k+1} \mid q_j$ for some $j \le l$". It cites Corollary 5.3.3 (c), proved by induction from (b), which is Theorem 5.3.2 applied when $\gcd(p, g) = 1$.

(b) In $p_{k+1} = q_j$: from $p_{k+1} \mid q_j$ and irreducibility of q_j we only get $q_j = u\, p_{k+1}$ with u a non-zero constant, and comparing the leading coefficients $1 = u$ needs both monic (Corollary 5.3.3 (d)). Also in $c' = c$: the products of the monic lists are monic by (L1).

(c) $p_4 = x - 4$ divides $q_1q_2q_3q_4$; the only q_j it divides is $q_1 = x - 4$, so $j = 1$ and $\sigma(4) = 1$. The shortened list is $(q_1', q_2', q_3') = (x - 3, x - 2, x - 1)$, and $\tau(t) = t + 1$. The step for $k = 2$ matches $p_3 = x - 3$ with q_1', and so on down. Unwinding, $\sigma(i) = 5 - i$: $q_{5-i} = x - i = p_i$ for $i = 1, 2, 3, 4$.

(d) The induction on k starts at $k = 0$, and $U(0)$ is about the empty list, whose product is 1; each step removes one entry, so the empty list is where every chain of steps ends.

(e) The last irreducible of one factorization divides the other product, so by Euclid's lemma it divides, and so equals, one of the other's irreducibles. Cancel it from both sides and apply the induction hypothesis to the two shorter lists.

5.3.6.2 B. Practice

Exercise. B1: Determine which

Determine whether each polynomial is irreducible over the given field. Justify your answer.

(a) $x^2 + 2$ over $\mathbb{Q}$, over $\mathbb{F}_2$, over $\mathbb{F}_3$.

(b) $x^3 + x + 1$ over $\mathbb{F}_2$ and over $\mathbb{F}_3$.

(c) $x^4 + 4$ over $\mathbb{Q}$.

(d) $3x^3 + x^2 - 2$, with its coefficients read in $\mathbb{F}_2$.

Solution.

(a) Over $\mathbb{Q}$: irreducible, since $c^2 + 2 \geq 2 > 0$ for $c \in \mathbb{Q}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e), (h)), so there is no root, and the degree is 2 (Proposition 5.3.1 (b)). Over $\mathbb{F}_2$: $2 = 0$, so the polynomial is $x^2 = x \cdot x$, reducible. Over $\mathbb{F}_3$: $2 = -1$, so it is $x^2 - 1 = (x - 1)(x + 1)$, reducible.

(b) Over $\mathbb{F}_2$: the values at 0 and 1 are 1 and $3 = 1$; no root, degree 3, irreducible. Over $\mathbb{F}_3$: the value at 1 is $3 = 0$, so it is reducible (Proposition 5.3.1 (a)); indeed $x^3 + x + 1 = (x - 1)(x^2 + x + 2)$ in $\mathbb{F}_3$.

(c) Reducible: $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$ (the warning after Proposition 5.3.1), although it has no rational root.

(d) In $\mathbb{F}_2$, $3 = 1$ and $-2 = 0$, so the polynomial is $x^3 + x^2 = x^2(x + 1)$. It has the root 0 and degree 3, so it is reducible.

Exercise. B2: The polynomials vanishing at the square root of two

Let $s \in \mathbb{R}$ be the non-negative square root of 2 (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4, in the complete ordered field $\mathbb{R}$), and let

$$J := \{f \in \mathbb{Q}[x] : f(s) = 0\},$$

where $f(s)$ is computed in $\mathbb{R}$, reading $\mathbb{Q}[x] \subseteq \mathbb{R}[x]$ coefficientwise. Prove that $J = \langle x^2 - 2 \rangle$.

The beginning and the end of a proof are given.

> J is an ideal of $\mathbb{Q}[x]$, since evaluation at s respects sums and products (Theorem 4.4.1). It contains $x^2 - 2$, and $1 \notin J$. Let d be a monic element of least degree

in J. Let $f \in J$, and divide: $f = qd + r$ with $\deg r < \deg d$ (Theorem 5.1.2).

[Blank.]

So $J = \langle d \rangle$. Then $d \mid x^2 - 2$, and $\deg d \geq 2$: $\deg d = 0$ would make $d = 1 \in J$, and $\deg d = 1$ would give $d = x + a$ with $a \in \mathbb{Q}$ and $s = -a$, a rational number whose square is 2, against Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1. Hence $d = x^2 - 2$.

Name the move, then complete it.

Solution. The move is **least degree, then divide**: in a set closed under the right operations, a remainder on division by an element of least degree lies in the set and has smaller degree, so it is 0.

Completion of the blank: $r = f - qd$, and $f, d \in J$, so $r \in J$ because J is an ideal (it absorbs the multiple qd and is closed under differences). A non-zero r would be a non-zero element of J of degree less than $\deg d$; its monic associate would lie in J too and have the same degree, against the choice of d. So $r = 0$, and $f = qd \in \langle d \rangle$. Conversely every multiple of d lies in J. This is the argument of Theorem 5.2.1, run on J.

For the end: $d \mid x^2 - 2$ because $x^2 - 2 \in J = \langle d \rangle$. So $\deg d \leq 2$ (Proposition 5.1.1 (d)), and with $\deg d \geq 2$, $x^2 - 2 = du$ with u a constant; both being monic, $u = 1$. In the language of this section, $x^2 - 2$ is irreducible over $\mathbb{Q}$: it has degree 2 and no rational root, since a root c would satisfy $c^2 = 2$, against Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1 (Proposition 5.3.1 (b)). Every rational polynomial vanishing at s is a multiple of it.

Exercise. B3: The small irreducibles over the two-element field

List all irreducible polynomials of degree at most 3 over $\mathbb{F}_2$, and prove that the list is complete.

Solution. Over $\mathbb{F}_2$ the only non-zero constant is 1, so every non-zero polynomial is monic and associates are equal. There are $2 + 4 + 8 = 14$ polynomials of degree 1, 2 or 3: the coefficient of the top power is 1, and each lower coefficient is 0 or 1.

- **Degree 1:** x and $x + 1$, both irreducible (the first example after Definition 5.3.1).
- **Degrees 2 and 3:** by Proposition 5.3.1 (b), irreducible exactly when there is no root. The value at 0 is the constant term, and the value at 1 is the sum of the coefficients, which is 0 in $\mathbb{F}_2$ exactly when the number of non-zero coefficients is even. So the irreducible ones have constant term 1 and an odd number of non-zero coefficients.

In degree 2, the candidates with constant term 1 are $x^2 + 1$ (two non-zero coefficients) and $x^2 + x + 1$ (three); only $x^2 + x + 1$ is irreducible. In degree 3 they are $x^3 + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$, $x^3 + x^2 + x + 1$, with two, three, three and four non-zero coefficients; so $x^3 + x + 1$ and $x^3 + x^2 + 1$ are irreducible. The complete list is

$$x, \quad x + 1, \quad x^2 + x + 1, \quad x^3 + x + 1, \quad x^3 + x^2 + 1.$$

5.3.6.3 C. Going deeper

Exercise. C1: Exit check: unique factorization

Prove the uniqueness half of Theorem 5.3.6: if $c\,p_1 \cdots p_k = c'q_1 \cdots q_l$ with $c, c' \in F$ non-zero and all p_i, q_j monic irreducible over the field F, then $c = c'$, $l = k$, and the two lists agree up to a bijection of indices. You may cite Euclid's lemma (Theorem 5.3.2) and Corollary 5.3.3.

Solution. The uniqueness part of the proof of Theorem 5.3.6 is a complete answer. Its steps, in order: the products of the monic lists are monic (L1), so comparing leading coefficients gives $c = c'$, and dividing by c leaves equal products; induction on k, with the statement quantified over every length l of the other list; base case $k = 0$, where a non-empty list of monic irreducibles has a product of degree at least 1; in the step, p_{k+1} divides the other product, so it divides some q_j by Corollary 5.3.3 (c), and equals it by (d); remove q_j from its list (L2) and cancel $p_{k+1} \neq 0$ (Corollary 4.3.3 (b)); the induction hypothesis on the shortened lists gives $l - 1 = k$ and a bijection, extended by $k + 1 \mapsto j$.

Marking scheme. (10 points) - 1: compares leading coefficients to get $c = c'$, with a reason that a product of monic polynomials is monic. - 2: sets up an induction on the length of one list (or a least counterexample), with the statement quantified over all lengths of the other list, and proves the base case by a degree argument. - 3: shows that an irreducible of one list divides the other product and **equals** one of its factors, citing Euclid's lemma for several factors **and** "monic irreducible divides monic irreducible implies equal". - 1: justifies the cancellation by the absence of zero divisors in $F[x]$. - 3: applies the induction hypothesis to the shortened lists, with the removal of the matched entry stated, and extends the bijection. Fatal errors (0 for the step): using the uniqueness for a polynomial of smaller degree without an induction set up; concluding $p_{k+1} = q_j$ from $p_{k+1} \mid q_j$ without using that both are monic and irreducible. A proof by strong induction on $\deg f$ maps to the same points: its set-up and the degree-0 case take the 2 points of the induction, and "the cofactor has a unique factorization" takes the last 3.

Exercise. C2: Find the error

Here is a statement and an argument for it.

> **Claim.** $x^4 + 1$ is irreducible over $\mathbb{Q}$.
>
> **Argument.** (1) By Theorem 5.3.7, a rational root of x^4+1 is u/v with $u \mid 1$ and $v \mid 1$, so the only candidates are 1 and -1. (2) Both give the value $1+1 = 2 \neq 0$, so $x^4 + 1$ has no rational root. (3) By Proposition 5.3.1, a polynomial without roots is irreducible. (4) Hence $x^4 + 1$ is irreducible over $\mathbb{Q}$.

Is the claim true? Does the argument prove it? If not, name the line that fails, explain why, give a counterexample to the step, and repair the proof.

Solution. The claim is **true**; the argument does **not** prove it.

Lines (1) and (2) are correct. The failing line is (3). Proposition 5.3.1 (b) is stated for polynomials of degree 2 or 3, and $x^4 + 1$ has degree 4: the line applies a result outside its hypotheses, a "fact" that is not available, entry (N9) of Logic and Proof, Example (What is not allowed). A counterexample to the step: $x^4 + 4$ has no rational root and is reducible (the warning after Proposition 5.3.1).

Repair. Suppose $x^4+1=gh$ with $\deg g, \deg h \geq 1$. The leading coefficients multiply to 1, so replacing g, h by their monic associates we may take both monic. The degrees add up to 4. If one of them is 1, that factor has a root in $\mathbb{Q}$ (Theorem 5.1.3 (c)), against lines (1)–(2). So both have degree 2: $g=x^2+ax+b$, $h=x^2+cx+d$ with $a,b,c,d\in\mathbb{Q}$. Comparing coefficients in

$$(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd$$

with x^4+1 gives $c=-a$, $b+d-a^2=0$, $a(d-b)=0$ and $bd=1$. Since $\mathbb{Q}$ has no zero divisors (Theorem 2.1.1 (f)), $a=0$ or $d=b$.

- If $a=0$: $d=-b$ and $-b^2=1$, impossible since $b^2\geq 0>-1$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)).
- If $d=b$: $b^2=1$, so $b=\pm 1$ (Corollary 2.1.2), and $a^2=2b=\pm 2$. Now $a^2=2$ is impossible by Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1, and $a^2=-2<0$ is impossible since squares are non-negative.

So no splitting exists, and x^4+1 is irreducible over $\mathbb{Q}$.

Exercise. C3: Infinitely many irreducibles

(a) Let F be a field. Prove that no finite list contains every monic irreducible polynomial of $F[x]$: for every list $(p_1,\dots,p_k)$ of monic irreducibles, $k\in\mathbb{N}$, some monic irreducible is not an entry of it.

(b) Let p be prime. Prove that there are exactly p^n monic polynomials of degree n in $\mathbb{F}_p[x]$, for each $n\in\mathbb{N}$, and deduce that $\mathbb{F}_p[x]$ has monic irreducibles of arbitrarily large degree.

Solution (Hint 1). For (a), copy the integer argument: consider $p_1\cdots p_k+1$. For (b), a monic polynomial of degree n is determined by its n lower coefficients.

Solution (Hint 2). For (a): by (L1) the product has degree at least 1 when $k\geq 1$, so $N:=p_1\cdots p_k+1$ has a monic irreducible factor (Lemma 5.3.5).

Solution. *(a)* If $k=0$, the polynomial x is monic and irreducible and not an entry. Let $k\geq 1$ and $P:=p_1\cdots p_k$. By (L1), P is monic of degree $\sum_i \deg p_i\geq 1$. Then $N:=P+1$ has $\deg N=\deg P\geq 1$ (Theorem 4.3.1, the degrees of P and 1 differ), so N has a monic irreducible divisor q (Lemma 5.3.5). If $q=p_i$ for some i, then $q\mid P$ by (L2), and $q\mid N-P=1$ (Proposition 5.1.1 (c)), so $\deg q\leq 0$ (Proposition 5.1.1 (d)), against $\deg q\geq 1$. So q is a monic irreducible that is not an entry of the list.

(b) A monic polynomial of degree n has n lower coefficients $a_0,\dots,a_{n-1}\in\mathbb{F}_p$, and by Definition 4.1.1 (equality coefficientwise) the map sending it to $(a_0,\dots,a_{n-1})$ is a bijection onto the set T_n of such tuples; its inverse puts 1 in position n and zeros above. We show $|T_n|=p^n$ by Logic and Proof, Axiom 4.2.1 on n. T_0 has one element, the empty tuple, and $p^0=1$. The tuples of length $n+1$ split by their last entry into p pairwise disjoint sets,

one for each element of $\mathbb{F}_p$, which has p elements (Definition 2.2.1); each is in bijection with T_n (drop the last entry). Applying Sets, Relations, and Cardinality, Proposition 3.1.5 $p-1$ times (an induction on the number of pieces), $|T_{n+1}| = p \cdot p^n = p^{n+1}$.

So for each $M \in \mathbb{N}$, the monic polynomials of degree at most M form a finite set: a union of the finitely many finite sets for $n = 0, \ldots, M$, pairwise disjoint, again by Sets, Relations, and Cardinality, Proposition 3.1.5. Suppose every monic irreducible of $\mathbb{F}_p[x]$ had degree at most M. Then they would form a subset of a finite set, hence a finite set (Sets, Relations, and Cardinality, Proposition 3.1.6), and a bijection $\{1, \ldots, k\} \to$ that set (Sets, Relations, and Cardinality, Definition 3.1.2) would be a list containing every monic irreducible, against (a). So for every M there is a monic irreducible of degree greater than M.

Marking scheme. (10 points) - 2: (a) builds a polynomial N of degree ≥ 1 that is 1 more than a multiple of $p_1 \cdots p_k$ (e.g. $p_1 \cdots p_k + 1$, or $x\, p_1 \cdots p_k + 1$), and shows $\deg N \geq 1$ for every k, $k = 0$ included (or treats $k = 0$ separately). - 3: (a) takes a monic irreducible factor q of N and shows q is no p_i, since it would divide 1. - 3: (b) counts the monic polynomials of degree n through their coefficient tuples, with an induction or a cited counting result. - 2: (b) concludes by contradiction with (a): a bound on the degrees would make the irreducibles a finite set, hence a list. Fatal errors (0 for the step): claiming that N itself is irreducible; taking "the product of all monic irreducibles" without a finite list.

Exercise. C4: Greatest common divisor and least common multiple

Let $f, g \in F[x]$ be monic, $d := \gcd(f, g)$, and write $f = df_1$, $g = dg_1$.

(a) Prove that $\gcd(f_1, g_1) = 1$.

(b) Prove that $L := df_1g_1$ is a monic common multiple of f and g that divides every common multiple of f and g, and that $d \cdot L = fg$.

(c) In $\mathbb{Q}[x]$, let $f = g = 2x$ (not monic). The gcd is x, and the monic common multiple dividing every common multiple is x. Show that $\gcd(f, g) \cdot x \neq fg$.

Solution. (a) Since $f \neq 0$, d is monic, so $d \neq 0$. By Theorem 5.2.2 (d), $d = af + bg$ for some $a, b \in F[x]$, so $d \cdot 1 = d(af_1 + bg_1)$. Canceling d (Corollary 4.3.3 (b)), $af_1 + bg_1 = 1$, and $\gcd(f_1, g_1) = 1$ by Corollary 5.2.3.

(b) Comparing leading coefficients in $f = df_1$ (Theorem 4.3.2 (b)) gives $\operatorname{lc}(f_1) = 1$; likewise g_1 is monic, so L is monic (L1). It is a common multiple: $L = fg_1 = gf_1$. Let h be a common multiple, $h = fk = gm$ with $k, m \in F[x]$. Then $df_1k = dg_1m$, and canceling d, $f_1k = g_1m$. So $g_1 \mid f_1k$, and $\gcd(g_1, f_1) = 1$ by (a), hence $g_1 \mid k$ by Theorem 5.3.2; say $k = g_1t$. Then $h = df_1g_1t = Lt$, and $L \mid h$. Finally $d \cdot L = (df_1)(dg_1) = fg$.

(c) $\gcd(2x, 2x) = x$ by Definition 5.2.2: x is monic and divides $2x$, and every common divisor h of $2x$ and $2x$ divides $2^{-1}(2x) = x$ (Proposition 5.1.1 (b)). Next, x is monic and a common multiple of $f = g = 2x$, since $2^{-1}(2x) = x$. It divides every common multiple h: $x \mid 2x$ and $2x \mid h$, so $x \mid h$ by Proposition 5.1.1 (b). Any other monic L' with these two properties satisfies $x \mid L'$ and $L' \mid x$, so $L' = x$ by Proposition 5.1.1 (f). But $x \cdot x = x^2 \neq 4x^2 = fg$, since $1 \neq 4$ in $\mathbb{Q}$. The identity of (b) needs f and g monic. For non-zero f, g, the monic associates $\operatorname{lc}(f)^{-1}f$ and $\operatorname{lc}(g)^{-1}g$ have the same common divisors and the same common multiples as f and g, since each divides the other; so (b) applied to them gives $d \cdot L = \operatorname{lc}(f)^{-1} \operatorname{lc}(g)^{-1} fg$.

5.4 Roots, Multiplicity, and the Formal Derivative

Over $\mathbb{Q}$, the polynomial $x^4 - 2x^3 + 2x - 1$ vanishes at 1 and at -1, and nowhere else. Yet it has degree 4, and 1 behaves like three roots at once: $x^4 - 2x^3 + 2x - 1 = (x-1)^3(x+1)$. This section counts roots properly. It proves that a non-zero polynomial of degree n has at most n roots, that a polynomial over an infinite field is determined by its values, and what it means for a root to be repeated; then it shows how to see a repeated root without factoring, through the formal derivative of Section 4.5.

Here the integers have no twin. Section 5.3 followed *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.3 step by step, but an integer cannot be evaluated at a point. The main new tool is one fact from Section 5.1, the factor theorem (Theorem 5.1.3): c is a root of f if and only if $x - c \mid f$. Throughout, F is a field.

5.4.1 Counting roots

A root of f gives a factor of degree 1. Several distinct roots give several factors, and degrees add, so there cannot be too many of them.

Theorem 5.4.1. Counting Roots

Let F be a field, $f \in F[x]$, $k \geq 1$, and let $c_1, \ldots, c_k \in F$ be **distinct** roots of f. Then

$$(x - c_1)(x - c_2) \cdots (x - c_k) \mid f.$$

If $f \neq 0$, then $k \leq \deg f$. In particular, a non-zero polynomial of degree n has at most n distinct roots in F.

Idea. Peel the roots off one at a time. If $f = (x - c_1) \cdots (x - c_{k-1})\, h$, then the next root c_k must be a root of h: at c_k the product of the factors $c_k - c_i$ is non-zero, because the roots are distinct and a field has no zero divisors. Then the factor theorem splits $x - c_k$ off h. Counting degrees at the end gives $k \leq \deg f$.

Proof. For $k \geq 1$ let $P_k := \prod_{i=1}^{k}(x - c_i)$, the product of a list in $F[x]$ (the recursion of Section 5.3, after Corollary 5.3.3). We prove "$P_k \mid f$ for all distinct roots $c_1, \ldots, c_k$ of f" by Logic and Proof, Axiom 4.2.1 on $k \geq 1$ (on ω, Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)).

For $k = 1$, $P_1 = x - c_1$, and $x - c_1 \mid f$ by Theorem 5.1.3 (b).

Suppose the claim holds for k, and let $c_1, \ldots, c_{k+1}$ be distinct roots of f. By the claim for $c_1, \ldots, c_k$, $f = P_k h$ for some $h \in F[x]$. Evaluating at c_{k+1} (Theorem 4.4.1, applied factor by factor along the recursion),

$$0 = f(c_{k+1}) = (c_{k+1} - c_1)(c_{k+1} - c_2) \cdots (c_{k+1} - c_k)\, h(c_{k+1}).$$

Each $c_{k+1} - c_i$ with $i \leq k$ is non-zero, since the roots are distinct, and a product of non-zero elements of a field is non-zero (Theorem 2.1.1 (g), by induction on the number of factors).

So $h(c_{k+1}) = 0$ by Theorem 2.1.1 (f). By Theorem 5.1.3 (b), $h = (x - c_{k+1})h_1$ for some $h_1 \in F[x]$, and by the recursion

$$f = P_k(x - c_{k+1})h_1 = P_{k+1}h_1.$$

So $P_{k+1} \mid f$.

Now let $f \neq 0$ and write $f = P_k h_1$. Then $h_1 \neq 0$, P_k is monic of degree k by (L1) of Section 5.3, and $\deg f = k + \deg h_1 \geq k$ by Theorem 4.3.2 (b).

■

Both hypotheses have a job: "distinct" in the factors $c_{k+1} - c_i \neq 0$, and "field" in the step "a product of non-zero elements is non-zero".

↻ **Second reading** · *Dropping a hypothesis*

Without "distinct": $1, 1$ is a list of two roots of $x - 1$, but $(x-1)^2 \nmid x - 1$, by degrees (Proposition 5.1.1 (d)). Without "field": over the ring $\mathbb{Z}/8\mathbb{Z}$, which has zero divisors, the polynomial $x^2 - 1$ of degree 2 has the four roots $1, 3, 5, 7$, since $3^2 - 1 = 8$, $5^2 - 1 = 24$ and $7^2 - 1 = 48$ are multiples of 8; there $(3-1)(3+1) = 8 = 0$ with both factors non-zero.

Quick check. Can a polynomial over $\mathbb{Q}$ of degree 3 vanish at $1, 2, 3$ and 4? Can a polynomial of degree at most 3?

Solution. Not one of degree 3: it is non-zero, so it has at most 3 distinct roots (Theorem 5.4.1). A polynomial of degree at most 3 can, but only the zero polynomial, whose degree is $-\infty \leq 3$.

5.4.2 Values determine the polynomial

Section 4.4 insisted that a polynomial is not a function: over $\mathbb{F}_2$, $x^2 + x$ and 0 have the same values (Example (Different Polynomials, Equal Functions)). Its warning promised that over a field such as $\mathbb{Q}$ the values do determine the polynomial. Counting roots pays that promise.

Theorem 5.4.2. Polynomials Determined by Values

Let F be a field and $f, g \in F[x]$.

(a) Let $n \in \mathbb{N}$. If $\deg f \leq n$, $\deg g \leq n$, and $f(c_i) = g(c_i)$ for $n + 1$ distinct elements $c_0, \ldots, c_n \in F$, then $f = g$.

(b) If F is infinite and $f(c) = g(c)$ for **every** $c \in F$, then $f = g$.

Idea. Two polynomials that agree at a point differ by a polynomial with a root there. If they agree at more points than their degree allows, the difference has too many roots, so it is 0. An infinite field has as many points as we need.

Proof. *(a)* By Theorem 4.3.1, $\deg(f-g) \leq \max(\deg f, \deg g) \leq n$ (the degree of $-g$ is that of g). By Theorem 4.4.1, $(f-g)(c_i) = f(c_i) - g(c_i) = 0$, so $c_0, \ldots, c_n$ are $n+1$ distinct roots of $f-g$. If $f-g \neq 0$, Theorem 5.4.1 gives $n+1 \leq \deg(f-g) \leq n$, which is false. So $f-g=0$.

(b) We first find enough distinct elements.

Claim. An infinite set S contains, for every $m \in \mathbb{N}$, a list of m distinct elements: an injective function $\{1, \ldots, m\} \to S$.

Proof. By Logic and Proof, Axiom 4.2.1 on m. For $m=0$ the empty function works. Suppose $s_1, \ldots, s_m$ are distinct elements of S. The set $A \coloneqq \{s_1, \ldots, s_m\}$ has m elements, through the bijection $i \mapsto s_i$, so it is finite (Sets, Relations, and Cardinality, Definition 3.1.2). Since S is infinite (Sets, Relations, and Cardinality, Definition 3.1.3), $A \neq S$, and as $A \subseteq S$, **there is** $s \in S$ with $s \notin A$. Then $s_1, \ldots, s_m, s$ are $m+1$ distinct elements of S.

■

The claim is proved by induction on a statement of the form "there exists a list", and each step takes one element from a non-empty set, once; no sequence of choices is made, so no axiom of choice is used. Now let $n \coloneqq \max(\deg f, \deg g, 0) \in \mathbb{N}$. The claim with $S = F$ and $m = n+1$ gives $n+1$ distinct elements of F, at which f and g agree, and (a) gives $f = g$.

■

Over $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, which are infinite, equality of polynomials and equality of polynomial functions are therefore the same thing. Two polynomials with integer coefficients that agree at every integer are equal too: read them in $\mathbb{Q}[x]$, and apply (a) at $n+1$ distinct integers. Part (a) says more, and it says it over every field: $n+1$ values fix a polynomial of degree at most n. A line is fixed by two points, a parabola by three.

Warning. **Over a finite field, (b) fails.** For a prime p, every $c \in \mathbb{F}_p$ satisfies $c^p = c$ (Theorem 2.6.6 (a)), so the polynomial $x^p - x$, which is **not** 0 (its coefficient of x^p is 1), vanishes at every element of $\mathbb{F}_p$. For $p=2$: $0^2 - 0 = 0$ and $1^2 - 1 = 0$, which is Example (Different Polynomials, Equal Functions). For $p=3$: the values at $0, 1, 2$ are 0, 0 and $8 - 2 = 6 = 0$. There is no conflict with (a): a polynomial of degree p needs $p+1$ points, and $\mathbb{F}_p$ has only p.

Example. Polynomial Functions over a Finite Field

(a) Show that $x^3 + 2x$ and 0 have the same values on $\mathbb{F}_3$, and factor $x^3 + 2x$ in $\mathbb{F}_3[x]$.

(b) Let p be prime. Show that, in $\mathbb{F}_p[x]$,

$$x^p - x = \prod_{c=0}^{p-1}(x-c) = x(x-1)(x-2)\cdots(x-(p-1)).$$

Solution.

(a) In $\mathbb{F}_3$, $2 = -1$, so $x^3+2x = x^3-x$. Its values at $0, 1, 2$ are 0, $1-1=0$ and $8-2=6=0$: the same as those of 0, although $x^3 - x \neq 0$. So $0, 1, 2$ are three distinct roots, and by Theorem 5.4.1, $x(x-1)(x-2) \mid x^3 - x$. Both are monic of degree 3, so the cofactor has degree 0 and, comparing leading coefficients, is 1:

$$x^3 + 2x = x(x-1)(x-2) \quad \text{in } \mathbb{F}_3[x].$$

Expanding confirms it: $x(x-1)(x-2) = x^3 - 3x^2 + 2x = x^3 + 2x$, since $3 = 0$.

(b) The elements $0, 1, \ldots, p-1$ of $\mathbb{F}_p$ are distinct (Definition 2.2.1), and each is a root of $x^p - x$ by the warning. By Theorem 5.4.1, the product P of the $x - c$ divides $x^p - x$; P is monic of degree p by (L1) of Section 5.3, and so is $x^p - x$, because $p \geq 2 > 1$. As in (a), $x^p - x = P \cdot u$ with $\deg u = 0$, and comparing leading coefficients gives $u = 1$.

5.4.3 Re-centering at a point

To study a polynomial near a point c, it helps to write it in powers of $x - c$ instead of powers of x. For x^2 and $c = 1$: $x^2 = 1 + 2(x-1) + (x-1)^2$. Such an expansion always exists and is unique, and it is found by dividing by $x - c$ repeatedly.

Theorem 5.4.3. Expansion in Powers of $x - c$

Let F be a field, $f \in F[x]$ with $\deg f = n \geq 0$, and $c \in F$.

(a) There are **unique** $b_0, b_1, \ldots, b_n \in F$ with

$$f = \sum_{j=0}^{n} b_j (x-c)^j.$$

(b) $b_0 = f(c)$, and b_n is the leading coefficient of f.

(c) For every $h \in F$, $f(c+h) = \sum_{j=0}^{n} b_j h^j$.

By Theorem 4.3.2 (b) and induction on j, each $(x-c)^j$ is monic of degree j; so a sum $\sum_{j=0}^{J} d_j (x-c)^j$ with $d_J \neq 0$ has degree **exactly** J: the term $d_J(x-c)^J$ has degree J, every other non-zero term has smaller degree, and Theorem 4.3.1 (with equality when the degrees differ, applied one term at a time) does the rest. The uniqueness half of (a) below uses this fact; part (b) uses its first clause, that $(x-c)^n$ is monic of degree n.

Idea. Divide f by $x - c$: the remainder is the constant $f(c)$, and the quotient has degree one less. Expand the quotient the same way, by induction, and multiply back by $x - c$. For uniqueness, compare degrees: a non-trivial combination of the powers $(x-c)^j$ has the degree of its highest term, so it is not 0.

Proof. *(a), existence.* By Logic and Proof, Axiom 4.2.1 on n, for every f of degree n. If $n = 0$, f is a non-zero constant $b_0 = b_0(x-c)^0$. Let $\deg f = n+1$. By Theorem 5.1.2 and Theorem 5.1.3 (a), $f = (x-c)q + f(c)$ with $q \in F[x]$. Since $\deg f \geq 1 > \deg f(c)$, Theorem 4.3.1 gives $\deg((x-c)q) = n+1$, so $q \neq 0$ and $\deg q = n$ (Theorem 4.3.2 (b)). By the induction hypothesis, $q = \sum_{j=0}^{n} d_j(x-c)^j$. Then

$$f = f(c) + \sum_{j=0}^{n} d_j(x-c)^{j+1} = \sum_{j=0}^{n+1} b_j(x-c)^j,$$

with $b_0 := f(c)$ and $b_{j+1} := d_j$, by the distributive law for finite sums (Lemma 4.1.1 (b), (Σ2)) and a shift of the summation index.

(a), uniqueness. If $\sum_{j=0}^{n} b_j(x-c)^j = \sum_{j=0}^{n} b'_j(x-c)^j$, then $\sum_{j=0}^{n}(b_j - b'_j)(x-c)^j = 0$ (Lemma 4.1.1 (b), (Σ1), (Σ4)). If some $b_j - b'_j$ were non-zero, the largest such j would be the degree of this sum, by the fact before the Idea; but the sum is 0. So $b_j = b'_j$ for every j.

(b) Evaluate at c (Theorem 4.4.1): $(c-c)^0 = 1$ and $(c-c)^j = 0$ for $j \geq 1$, so $f(c) = b_0$. The terms with $j < n$ have degree less than n, and $b_n(x-c)^n$ has coefficient b_n at x^n, since $(x-c)^n$ is monic of degree n; so the coefficient of x^n in f, its leading coefficient, is b_n.

(c) Evaluate at $c+h$: $(x-c)$ takes the value h there, and Theorem 4.4.1 carries sums, products and powers through.

■

The coefficients b_j are computed by the existence proof: divide by $x-c$, keep the remainder as b_0, divide the quotient by $x-c$, keep the remainder as b_1, and so on until the quotient is a constant, which is b_n. The next example runs this.

Quick check. Expand x^3 in powers of $x-1$ over $\mathbb{Q}$.

Solution. $x^3 = (x-1)(x^2+x+1)+1$, $x^2+x+1 = (x-1)(x+2)+3$, $x+2 = (x-1)\cdot 1+3$. So $b_0 = 1$, $b_1 = 3$, $b_2 = 3$, $b_3 = 1$:

$$x^3 = 1 + 3(x-1) + 3(x-1)^2 + (x-1)^3.$$

5.4.4 Multiplicity

The hook's polynomial $(x-1)^3(x+1)$ is divisible by $(x-1)^3$ and not by $(x-1)^4$. That exponent is what "three roots at once" means.

The multiplicity of a root counts how many factors $x-c$ can be split off.

Definition 5.4.1. Multiplicity of a Root

Let F be a field, $f \in F[x]$ **non-zero**, and $c \in F$. The **multiplicity** of c in f, written $\mathrm{mult}_c(f)$, is the **largest** $m \in \mathbb{N}$ with $(x-c)^m \mid f$. The root c is **simple** if $\mathrm{mult}_c(f) = 1$ and

multiple if $\mathrm{mult}_c(f) \geq 2$.

In words: keep dividing f by $x - c$ while the division comes out exact; the number of exact divisions is the multiplicity.

Well defined. The set $M := \{m \in \mathbb{N} : (x-c)^m \mid f\}$ contains 0, since $(x-c)^0 = 1$ divides f. For $m \in M$, $m = \deg(x-c)^m \leq \deg f$ (Proposition 5.1.1 (d)), so M is bounded above, and it has a greatest element (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.6, with $\mathbb{N} \subseteq \mathbb{Z}$). By the factor theorem (Theorem 5.1.3 (b)), $1 \in M$ exactly when $f(c) = 0$, so

$$\mathrm{mult}_c(f) = 0 \iff f(c) \neq 0.$$

For the direction from right to left: if $f(c) \neq 0$, no $m \geq 1$ lies in M either, since $(x-c)^m = (x-c)^{m-1}(x-c)$ (Lemma 4.1.1 (c)), so $(x-c)^m \mid f$ would give $x - c \mid f$ (Proposition 5.1.1 (b)), that is, $1 \in M$. Hence $M = \{0\}$. A multiplicity 0 means "not a root". The zero polynomial is excluded because every power of $x - c$ divides it, and M would have no greatest element.

Examples. In $\mathbb{Q}[x]$, $\mathrm{mult}_1((x-1)^2) = 2$: $(x-1)^2$ divides itself, and $(x-1)^3$ does not, by degrees. $\mathrm{mult}_0(x^2 + x) = 1$: the value at 0 is 0, and x^2 does not divide $x^2 + x$, since division with remainder gives $x^2 + x = x^2 \cdot 1 + x$ with remainder $x \neq 0$. And $\mathrm{mult}_2(x^2 + x) = 0$, since the value at 2 is $6 \neq 0$.

The definition asks for a largest exponent, which is awkward to check directly. The next lemma replaces it by a single evaluation.

Lemma 5.4.4. Multiplicity through the Cofactor

Let F be a field, $f \in F[x]$ non-zero, $c \in F$ and $m \in \mathbb{N}$.

(a) $\mathrm{mult}_c(f) = m$ **if and only if** $f = (x-c)^m g$ for some $g \in F[x]$ with $g(c) \neq 0$.

(b) Such a g is unique.

(c) If $f = \sum_{j=0}^{n} b_j (x-c)^j$ is the expansion of Theorem 5.4.3, then $\mathrm{mult}_c(f)$ is the **least** j with $b_j \neq 0$.

Idea. If the cofactor g vanished at c, one more factor $x - c$ would split off; if one more factor split off, cancellation would make g vanish at c. For (c), the expansion displays the cofactor directly.

Proof. *(a)* ($\Rightarrow$) Let $m = \mathrm{mult}_c(f)$, so $f = (x-c)^m g$ for some g. If $g(c) = 0$, then $g = (x-c)g_1$ (Theorem 5.1.3 (b)) and $(x-c)^{m+1} \mid f$, against the maximality of m. So $g(c) \neq 0$.

($\Leftarrow$) Let $f = (x-c)^m g$ with $g(c) \neq 0$; then $m \in M$. Suppose some $m' > m$ were in M. Then $(x-c)^{m+1}$ divides $(x-c)^{m'}$, hence f: say $f = (x-c)^{m+1}k = (x-c)^m((x-c)k)$. Canceling $(x-c)^m \neq 0$ (Corollary 4.3.3 (b)) gives $g = (x-c)k$, so $g(c) = 0$, a contradiction. So m is the largest element of M.

(b) If $(x-c)^m g = (x-c)^m g'$, cancel $(x-c)^m \neq 0$.

(c) The coefficient b_n is the leading coefficient of f, so it is non-zero, and the set of j with $b_j \neq 0$ has a least element J (Sets, Relations, and Cardinality, Theorem 2.1.3). The terms

with $j < J$ vanish, so, taking the factor $(x-c)^J$ out of the remaining terms,

$$f = (x-c)^J g, \qquad g \coloneqq \sum_{i=0}^{n-J} b_{J+i}(x-c)^i.$$

Evaluating at c, as in Theorem 5.4.3 (b), $g(c) = b_J \neq 0$. By (a), $\operatorname{mult}_c(f) = J$.

■

The factor g is the **cofactor** of c in f. Multiplicities of a product add, because cofactors multiply.

Proposition 5.4.5. Multiplicity of a Product

Let F be a field, $f, g \in F[x]$ non-zero and $c \in F$. Then $\operatorname{mult}_c(fg) = \operatorname{mult}_c(f) + \operatorname{mult}_c(g)$.

Proof. Let $m \coloneqq \operatorname{mult}_c(f)$ and $n \coloneqq \operatorname{mult}_c(g)$. By Lemma 5.4.4 (a), $f = (x-c)^m u$ and $g = (x-c)^n v$ with $u(c) \neq 0$ and $v(c) \neq 0$. Then $fg = (x-c)^{m+n}uv$ (Lemma 4.1.1 (c), commutativity of $F[x]$), $fg \neq 0$ (Corollary 4.3.3 (a); a field is an integral domain), and $(uv)(c) = u(c)v(c) \neq 0$ (Theorem 4.4.1, Theorem 2.1.1 (f)). By Lemma 5.4.4 (a) again, $\operatorname{mult}_c(fg) = m + n$.

■

Quick check. Over $\mathbb{Q}$, find $\operatorname{mult}_0(x^5 + x^3)$ and $\operatorname{mult}_2(x^3 - 4x)$.

Solution. $x^5 + x^3 = x^3(x^2+1)$, and the cofactor x^2+1 has value $1 \neq 0$ at 0, so $\operatorname{mult}_0 = 3$ by Lemma 5.4.4 (a). $x^3 - 4x = (x-2)\cdot x(x+2)$, with cofactor value $2 \cdot 4 = 8 \neq 0$ at 2, so $\operatorname{mult}_2 = 1$: a simple root.

All roots can now be split off at once. The roots of a non-zero f form a finite set: otherwise the claim in the proof of Theorem 5.4.2 (b), applied to the set of roots, would give $\deg f + 1$ distinct roots, against Theorem 5.4.1. So they can be listed without repetition.

Theorem 5.4.6. Splitting Off All Roots

Let F be a field and $f \in F[x]$ non-zero. Let $c_1, \ldots, c_k \in F$, $k \in \mathbb{N}$, be the distinct roots of f in F (every root of f in F is one of them), and $m_i \coloneqq \operatorname{mult}_{c_i}(f)$. Then

$$f = (x-c_1)^{m_1}(x-c_2)^{m_2}\cdots(x-c_k)^{m_k}\, g$$

for some $g \in F[x]$ with **no** root in F, and $m_1 + m_2 + \cdots + m_k \leq \deg f$.

Idea. Split off the full power of one root with Lemma 5.4.4. The cofactor keeps every other root, with the same multiplicity, because the power just removed does not vanish there; induction on the number of roots does the rest.

Proof. By Logic and Proof, Axiom 4.2.1 on k, we prove: for every non-zero f and every list $c_1, \dots, c_k$ of distinct elements of F whose entries are exactly the roots of f in F, the displayed factorization holds with g rootless. For $k = 0$, f has no root, and $g := f$ works with the empty product 1.

Assume the statement for k, and let the roots of f be exactly the distinct $c_1, \dots, c_{k+1}$. By Lemma 5.4.4 (a), $f = (x - c_{k+1})^{m_{k+1}} g_1$ with $g_1(c_{k+1}) \neq 0$; then $g_1 \neq 0$.

The roots of g_1 are exactly $c_1, \dots, c_k$. A root c of g_1 is a root of f (Theorem 4.4.1), and $c \neq c_{k+1}$, so $c = c_i$ with $i \leq k$. Conversely, for $i \leq k$, the polynomial $(x - c_{k+1})^{m_{k+1}}$ has the value $(c_i - c_{k+1})^{m_{k+1}} \neq 0$ at c_i (a power of a non-zero element of a field, Theorem 2.1.1 (g)), so its multiplicity at c_i is 0, and Proposition 5.4.5 gives

$$\operatorname{mult}_{c_i}(g_1) = m_i - 0 = m_i \geq 1.$$

So c_i is a root of g_1, with the same multiplicity as in f.

The statement for k, applied to g_1 and $c_1, \dots, c_k$, gives $g_1 = \prod_{i=1}^{k} (x - c_i)^{m_i}\, g$ with g rootless. Hence, by commutativity and associativity and the recursion of the product,

$$f = \Big(\prod_{i=1}^{k} (x - c_i)^{m_i}\Big)(x - c_{k+1})^{m_{k+1}}\, g = \Big(\prod_{i=1}^{k+1} (x - c_i)^{m_i}\Big) g.$$

For the degree, the product is monic of degree $\sum_i m_i$ by (L1) of Section 5.3, and $g \neq 0$, so $\deg f = \sum_i m_i + \deg g \geq \sum_i m_i$ (Theorem 4.3.2 (b)).

■

So the multiplicities add up to at most $\deg f$: counted with multiplicity, a non-zero polynomial of degree n still has at most n roots. The case where nothing is left over has a name.

Definition 5.4.2. Splitting over a Field

Let F be a field and $f \in F[x]$ non-zero of degree n. The polynomial f **splits over** F if

$$f = a(x - a_1)(x - a_2) \cdots (x - a_n)$$

for some $a, a_1, \dots, a_n \in F$, repetitions among the a_i allowed. For $n = 0$ this says that $f = a$ is a non-zero constant.

If f splits, the multiplicities of its roots add up to **exactly** n: the rootless factor g of Theorem 5.4.6 is then a constant.

↻ **Second reading** · *Why nothing is left over*

In the factorization of Theorem 5.4.6, suppose the rootless g had degree at least 1; it would have a monic irreducible factor q (Lemma 5.3.5), say $g = qh$. Since $g \mid f$, also $q \mid f$ (Proposition 5.1.1 (b)). As $f \neq 0$, $a \neq 0$, and q divides $a^{-1} f = (x - a_1)(x - a_2) \cdots (x - a_n)$ (Proposition 5.1.1 (c)). By Corollary 5.3.3 (c), $n \geq 1$ and $q \mid x - a_i$ for some i. Each $x - a_i$ is monic and, having degree 1, irreducible (Section 5.3), so Corollary 5.3.3 (d) gives $q = x - a_i$. Then $g(a_i) = q(a_i)h(a_i) = 0$ (Theorem 4.4.1), against g rootless. Hence g is a constant, non-zero as $f \neq 0$, and $\deg f = \sum_i m_i$

(Theorem 4.3.2 (b)).

For example, x^2-2 does not split over $\mathbb{Q}$: a splitting $a(x-a_1)(x-a_2)$ would make a_1 a rational root, and $a_1^2=2$ is impossible (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1). Over $\mathbb{R}$ it splits, as $(x-s)(x+s)$ with s the non-negative square root of 2 (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4).

Example. Multiplicities by Repeated Division

Find the roots of $f \coloneqq x^4-2x^3+2x-1 \in \mathbb{Q}[x]$ with their multiplicities, and expand f in powers of $x-1$.

Solution. The value at 1 is $1-2+2-1=0$, so divide by $x-1$, and keep dividing while the remainder is 0:

$$\begin{aligned} x^4-2x^3+2x-1 &= (x-1)(x^3-x^2-x+1)+0,\\ x^3-x^2-x+1 &= (x-1)(x^2-1)+0,\\ x^2-1 &= (x-1)(x+1)+0,\\ x+1 &= (x-1)\cdot 1+2. \end{aligned}$$

So $f=(x-1)^3(x+1)$, and the cofactor $x+1$ has the value $2\neq 0$ at 1: $\mathrm{mult}_1(f)=3$ by Lemma 5.4.4 (a). At -1, the cofactor of $x+1$ is $(x-1)^3$, with value $(-2)^3=-8\neq 0$, so $\mathrm{mult}_{-1}(f)=1$. There are no other roots: $f(c)=(c-1)^3(c+1)=0$ forces $c=1$ or $c=-1$ (Theorem 2.1.1 (f)). The multiplicities add up to $4=\deg f$, and f splits over $\mathbb{Q}$, with $a=1$ and $(a_1,a_2,a_3,a_4)=(1,1,1,-1)$.

The remainders $0,0,0,2$ and the last quotient 1 are the coefficients $b_0,\dots,b_4$ of Theorem 5.4.3 at $c=1$, by its existence proof:

$$f=2(x-1)^3+(x-1)^4,$$

and the least j with $b_j\neq 0$ is 3, the multiplicity, as Lemma 5.4.4 (c) says. Expanding $(x-1)^3((x-1)+2)$ confirms the expansion.

5.4.5 Repeated roots and the derivative

Finding multiplicities by division needs the root first. The formal derivative detects repeated roots, and repeated factors, without knowing them. Section 4.5 defined it with no limits: for $f=\sum_k f_k x^k$,

$$f' \coloneqq \sum_{k\geq 1}(k\cdot f_k)x^{k-1}$$

(Definition 4.5.1), where $k\cdot f_k$ is the k-th multiple and $k\cdot 1$ may be 0 in F. It obeys the rules of calculus (Theorem 4.5.1): it is additive with $(af)'=af'$ for a constant a; the product rule $(fg)'=f'g+fg'$ holds; and $(g^m)'=(m\cdot 1)g^{m-1}g'$, in particular $\big((x-c)^m\big)'=(m\cdot 1)(x-c)^{m-1}$ for $m\geq 1$. In characteristic 0, $f'=0$ only for constant f, and $\deg f'=\deg f-1$ when $\deg f\geq 1$ (Proposition 4.5.2 (a)); in characteristic p a non-constant polynomial can have derivative 0: over $\mathbb{F}_2$, $(x^2)'=(2\cdot 1)x=0$.

At a double root the graph of a real polynomial touches the axis, with slope 0. The formal

version of that picture needs no graph and no slope.

Theorem 5.4.7. Repeated Roots and the Derivative

Let F be a field, $f \in F[x]$ non-zero and $c \in F$.

(a) c is a multiple root of f **if and only if** $f(c) = 0$ and $f'(c) = 0$.
(b) If $\mathrm{mult}_c(f) = m \geq 1$ and $m \cdot 1 \neq 0$ in F, then $f' \neq 0$ and $\mathrm{mult}_c(f') = m - 1$.

Idea. Write $f = (x-c)^m g$ with $g(c) \neq 0$ and differentiate by the product rule. Both terms contain $(x-c)^{m-1}$, so $f' = (x-c)^{m-1}B$ with a bracket B whose value at c is $(m \cdot 1)g(c)$. Everything follows from looking at m and at that value.

Proof. Let $m := \mathrm{mult}_c(f)$. If $m = 0$, then $f(c) \neq 0$, so both sides of (a) are false, and (b) does not apply. Let $m \geq 1$, and write $f = (x-c)^m g$ with $g(c) \neq 0$ (Lemma 5.4.4 (a)). By Theorem 4.5.1,

$$\begin{aligned} f' &= (m \cdot 1)(x-c)^{m-1} g + (x-c)^m g' \\ &= (x-c)^{m-1} B, \qquad B := (m \cdot 1)g + (x-c)g'. \end{aligned}$$

At c, $B(c) = (m \cdot 1)g(c)$ (Theorem 4.4.1).

(a) Here $f(c) = 0$. If $m \geq 2$, then $m - 1 \geq 1$ and $f'(c) = 0^{m-1}B(c) = 0$. If $m = 1$, then $f' = B$ and $f'(c) = (1 \cdot 1)g(c) = g(c) \neq 0$. So $f'(c) = 0$ exactly when $m \geq 2$, that is, when c is a multiple root.

(b) If $m \cdot 1 \neq 0$, then $B(c) = (m \cdot 1)g(c) \neq 0$ by Theorem 2.1.1 (f). So $B \neq 0$, hence $f' \neq 0$ (Corollary 4.3.3), and Lemma 5.4.4 (a) applied to $f' = (x-c)^{m-1}B$ gives $\mathrm{mult}_c(f') = m - 1$.

■

The hypothesis $m \cdot 1 \neq 0$ in (b) is needed. Over $\mathbb{F}_3$, $f = x^3$ has $\mathrm{mult}_0(f) = 3$, but $f' = (3 \cdot 1)x^2 = 0$, whose multiplicity is not even defined. Part (a) holds over every field.

Remark. **The polynomial $x^p - x$ has only simple roots.** Over $\mathbb{F}_p$, $(x^p - x)' = (p \cdot 1)x^{p-1} - 1$ by Theorem 4.5.1, and this is -1, since $p \cdot 1 = 0$ in $\mathbb{F}_p$ (Example (The characteristics of the standard fields): $\mathrm{char}\,\mathbb{F}_p = p$). The derivative -1 vanishes nowhere, so by (a) no root of $x^p - x$ is multiple. By Example (Polynomial Functions over a Finite Field) (b), every $c \in \mathbb{F}_p$ is a root, and each is simple: $x^p - x$ is the product of the p distinct factors $x - c$. This is the fact that Section 4.5's warning set aside.

The same computation, with an irreducible factor in place of $x - c$, detects repeated factors through a gcd, which the Euclidean algorithm of Section 5.2 computes without factoring anything.

Corollary 5.4.8. Repeated Factors and the Greatest Common Divisor

Let F be a field and $f \in F[x]$ with $\deg f \geq 1$.

(a) If $p \in F[x]$ is irreducible and $p^2 \mid f$, then $p \mid \gcd(f, f')$. So if $\gcd(f, f') = 1$, no irreducible divides f twice, and f has no multiple root in F.

(b) If F has characteristic 0 (Definition 2.5.1) and $\gcd(f, f') \neq 1$, then $p^2 \mid f$ for some irreducible p.

Idea. For (a), differentiate $p^2 g$: every term keeps a factor p. For (b), take an irreducible p dividing both f and f'. If p divided f only once, $f = pg$, then p would divide $f' - pg' = p'g$, and hence p', which in characteristic 0 is non-zero of smaller degree.

Proof. *(a)* Write $f = p^2 g$. By Theorem 4.5.1,

$$f' = (2 \cdot 1) p p' g + p^2 g' = p((2 \cdot 1) p' g + p g'),$$

so p divides both f and f', and hence divides $\gcd(f, f')$ (Theorem 5.2.2 (b); $f \neq 0$). If $\gcd(f, f') = 1$, this would give $p \mid 1$, impossible since $\deg p \geq 1$ (Proposition 5.1.1 (d)). A multiple root c would give $(x - c)^2 \mid f$ with $x - c$ irreducible.

(b) Let $d := \gcd(f, f')$. It is monic ($f \neq 0$) and $d \neq 1$, so $\deg d \geq 1$, and d has a monic irreducible divisor p (Lemma 5.3.5). Then $p \mid f$ and $p \mid f'$ (Proposition 5.1.1 (b)). As for multiplicities, the set of $m \in \mathbb{N}$ with $p^m \mid f$ contains 0 and 1 and is bounded by $\deg f$ ($m \leq m \deg p = \deg p^m$); let $m \geq 1$ be its greatest element and write $f = p^m g$. Then $p \nmid g$, since otherwise $p^{m+1} \mid f$.

Suppose $m = 1$. Then $f' = p'g + pg'$, and p divides f' and pg', so $p \mid f' - pg' = p'g$ (Proposition 5.1.1 (c)). By Corollary 5.3.3 (b), $p \mid p'$ or $p \mid g$, and $p \nmid g$. But F has characteristic 0 and $\deg p \geq 1$, so $p' \neq 0$ and $\deg p' = \deg p - 1 < \deg p$ (Proposition 4.5.2 (a)); then $p \nmid p'$ by Proposition 5.1.1 (d). This contradiction shows $m \geq 2$, and $p^2 \mid f$. ∎

Characteristic 0 is used once, at $\deg p' = \deg p - 1$. Over $\mathbb{Q}$, a polynomial f therefore has a repeated irreducible factor exactly when $\gcd(f, f') \neq 1$, and that question is answered by the Euclidean algorithm (Theorem 5.2.5) with no factoring at all.

Quick check. Is 1 a multiple root of $x^3 - 3x + 2 \in \mathbb{Q}[x]$?

Solution. Yes. $f(1) = 1 - 3 + 2 = 0$, $f' = 3x^2 - 3$ and $f'(1) = 0$, so Theorem 5.4.7 (a) applies. Indeed $x^3 - 3x + 2 = (x - 1)^2 (x + 2)$.

5.4.6 Exercises

5.4.6.1 A. Check your understanding

Exercise. A1

(a) Find mult_1 and mult_{-1} of $x^4 - 2x^3 + 2x - 1 \in \mathbb{Q}[x]$.

(b) In $\mathbb{F}_3[x]$, let $f = x^3$. Is 0 a multiple root by the test of Theorem 5.4.7 (a)? Does part (b) apply?

(c) True or false: a polynomial over $\mathbb{Q}$ of degree at most 2 that vanishes at $1, 2, 3$ is the zero polynomial.

(d) True or false: a polynomial over $\mathbb{F}_2$ that vanishes at every element of $\mathbb{F}_2$ is the zero polynomial.

Solution.

(a) 3 and 1 (Example (Multiplicities by Repeated Division)).

(b) Yes: $f(0) = 0$ and $f' = (3 \cdot 1)x^2 = 0$, so $f'(0) = 0$, and 0 is a multiple root (its multiplicity is 3). Part (b) does not apply: $m = 3$ and $3 \cdot 1 = 0$ in $\mathbb{F}_3$; indeed $f' = 0$, and its multiplicity is not 2, it is not defined.

(c) True: a non-zero polynomial of degree at most 2 has at most 2 distinct roots (Theorem 5.4.1), or Theorem 5.4.2 (a) with $n = 2$ and $g = 0$.

(d) False: $x^2 + x \neq 0$ vanishes at 0 and 1 (Example (Different Polynomials, Equal Functions)). Part (b) of Theorem 5.4.2 needs an infinite field.

5.4.6.2 B. Practice

Exercise. B1: Put the proof in order

The following lines contain a proof of the divisibility part of Theorem 5.4.1, shuffled, together with two lines that do not belong. Write the seven correct lines in an order that makes a proof, say which other orders are also admissible, and say why each of the other two lines fails.

(i) We use induction on k; for $k = 1$, $x - c_1 \mid f$ by the factor theorem.

(ii) Assume the claim for every list of $k - 1$ distinct roots, and let $c_1, \ldots, c_k$ be distinct roots of f.

(iii) Write $f = (x - c_1) \cdots (x - c_{k-1})\, h$.

(iv) Evaluate at c_k: $0 = (c_k - c_1) \cdots (c_k - c_{k-1})\, h(c_k)$.

(v) Each $c_k - c_i$, $i < k$, is non-zero, since the roots are distinct.
(v′) Each $c_k - c_i$, $i < k$, is non-zero, since $c_k \neq 0$.

(vi) A product of non-zero elements of a field is non-zero, so $h(c_k) = 0$.
(vi′) $h(c_k) = 0$, because $f(c_k) = 0$.

(vii) By the factor theorem, $h = (x - c_k)h_1$, so $f = (x - c_1) \cdots (x - c_k)\, h_1$.

Solution. An admissible order is (i), (ii), (iii), (iv), (v), (vi), (vii):

> We use induction on k; for $k = 1$, $x - c_1 \mid f$ by the factor theorem. Assume the claim for every list of $k-1$ distinct roots, and let $c_1, \ldots, c_k$ be distinct roots of f. Write $f = (x-c_1) \cdots (x-c_{k-1})h$. Evaluate at c_k: $0 = (c_k-c_1) \cdots (c_k-c_{k-1})h(c_k)$. Each $c_k - c_i$, $i < k$, is non-zero, since the roots are distinct. A product of non-zero elements of a field is non-zero, so $h(c_k) = 0$. By the factor theorem, $h = (x-c_k)h_1$, so $f = (x - c_1) \cdots (x - c_k)h_1$.

Lines (i) and (ii) set up the induction and come first, in that order; (iii) uses the hypothesis of (ii). Line (v) uses only the distinctness from (ii), so it may come anywhere after (ii) and before (vi); in particular (iv) and (v) may be exchanged, and (v) may even precede (iii). Line (vi) needs both (iv) and (v), and (vii) needs (vi) and (iii). So the admissible orders are: (i), (ii), then (iii), (iv), (v) with (iv) after (iii) and (v) anywhere among them, then (vi), (vii).

The distractor (v′) gives a wrong reason: $c_k = 0$ is allowed, and $c_k \neq 0$ says nothing about $c_k - c_i$. The distractor (vi′) skips the cancellation: $f(c_k) = 0$ only says that the product in (iv) is 0, and passing to $h(c_k) = 0$ needs both (v) and the absence of zero divisors. Over a ring with zero divisors the step fails: over $\mathbb{Z}/8\mathbb{Z}$, $x^2 - 1 = (x-1)(x+1)$ has the root 3, yet neither factor vanishes at 3.

Exercise. B2: Expansions at a point

(a) Expand $x^3 - 2x + 5 \in \mathbb{Q}[x]$ in powers of $x - 1$.

(b) Find $\mathrm{mult}_{-2}(x^3 - 3x + 2)$ from the first two coefficients of an expansion in powers of $x + 2$.

Solution.

(a) Divide by $x - 1$ three times:

$$\begin{aligned} x^3 - 2x + 5 &= (x-1)(x^2 + x - 1) + 4, \\ x^2 + x - 1 &= (x-1)(x+2) + 1, \\ x + 2 &= (x-1) \cdot 1 + 3. \end{aligned}$$

By the existence proof of Theorem 5.4.3, $x^3 - 2x + 5 = 4 + (x-1) + 3(x-1)^2 + (x-1)^3$. Expanding the right side gives back $x^3 - 2x + 5$.

(b) Here $c = -2$ and $x - c = x + 2$. First $x^3 - 3x + 2 = (x+2)(x^2 - 2x + 1) + 0$, so $b_0 = 0$; then $x^2 - 2x + 1 = (x+2)(x-4) + 9$, so $b_1 = 9 \neq 0$. By Lemma 5.4.4 (c), $\mathrm{mult}_{-2} = 1$: -2 is a simple root.

Exercise. B3: Functions on a finite field

Let p be prime and $f, g \in \mathbb{F}_p[x]$. Prove that $f(c) = g(c)$ for every $c \in \mathbb{F}_p$ if and only if $x^p - x \mid f - g$. Then find a polynomial of degree less than 5 with the same values on $\mathbb{F}_5$ as $x^7 + x$.

Solution. ($\Leftarrow$) If $f - g = (x^p - x)h$, then for $c \in \mathbb{F}_p$, $f(c) - g(c) = (c^p - c)h(c) = 0$, since $c^p = c$ (Theorem 2.6.6 (a)).

($\Rightarrow$) If f and g agree on $\mathbb{F}_p$, then $0, 1, \ldots, p-1$ are p distinct roots of $f - g$, so $\prod_{c=0}^{p-1}(x - c) \mid f - g$ by Theorem 5.4.1, and that product is $x^p - x$ (Example (Polynomial Functions over a Finite Field) (b)).

For $p = 5$: $x^7 = x^2 \cdot x^5$, and $x^7 - x^3 = x^2(x^5 - x)$, so $(x^7 + x) - (x^3 + x) = x^2(x^5 - x)$ is

a multiple of $x^5 - x$. By the first part, $x^3 + x$ has the same values as $x^7 + x$ on $\mathbb{F}_5$, and its degree is $3 < 5$.

5.4.6.3 C. Going deeper

Exercise. C1: The coefficients as derivatives

Let F be a field of characteristic 0, $f \in F[x]$ of degree $n \geq 0$, $c \in F$, and $f = \sum_{j=0}^{n} b_j (x-c)^j$ as in Theorem 5.4.3. Prove that

$$b_j = \frac{f^{(j)}(c)}{j! \cdot 1} \qquad (0 \leq j \leq n),$$

where $f^{(j)}$ is the j-th formal derivative (Definition 4.5.1). Check the formula on the expansion of Exercise B2 (a) at $j = 2$.

Solution (Hint 1). Compute the j-th derivative of $(x-c)^i$ first.

Solution (Hint 2). By induction on j, $\big((x-c)^i\big)^{(j)} = \big((i(i-1)\cdots(i-j+1)) \cdot 1\big)(x-c)^{i-j}$ for $j \leq i$, and 0 for $j > i$.

Solution. The derivatives of the powers. We prove the formula of Hint 2 by Logic and Proof, Axiom 4.2.1 on j, for all i. For $j = 0$ the coefficient is the empty product 1. Suppose it holds for j. If $j + 1 \leq i$, then $i - j \geq 1$ and, by Theorem 4.5.1 (a) and (c),

$$\big((x-c)^i\big)^{(j+1)} = \big((i \cdots (i-j+1)) \cdot 1\big)\big((i-j) \cdot 1\big)(x-c)^{i-j-1},$$

and $(u \cdot 1)(v \cdot 1) = (uv) \cdot 1$ (Lemma 2.5.1 (b)) gives the coefficient $(i \cdots (i-j)) \cdot 1$. If $j+1 = i+1$, the i-th derivative is the constant $(i! \cdot 1)$, whose derivative is 0; and the derivative of 0 is 0 for larger j.

The coefficients. Since the derivative is additive with $(af)' = af'$ for constants a (Theorem 4.5.1 (a)), so is the j-th derivative (induction on j), and

$$f^{(j)} = \sum_{i=j}^{n} b_i \big((i \cdots (i-j+1)) \cdot 1\big)(x-c)^{i-j}.$$

At $x = c$, every term with $i > j$ vanishes, and the term $i = j$ is $b_j(j! \cdot 1)$. So $f^{(j)}(c) = (j! \cdot 1) b_j$. In characteristic 0, $j! \cdot 1 \neq 0$ (Definition 2.5.1, as $j! \geq 1$), and dividing gives the formula.

Check. For $f = x^3 - 2x + 5$, $f'' = 6x$ and $f''(1) = 6$, so $b_2 = 6/2 = 3$, as in Exercise B2 (a).

Exercise. C2: Repeated factors through the gcd

(a) Using only $\gcd(f, f')$, decide whether $f := x^4 - 2x^3 + 2x - 1 \in \mathbb{Q}[x]$ has a repeated irreducible factor.

(b) Over $\mathbb{F}_2$, let $f := x^4 + 1$. Compute f' and $\gcd(f, f')$, and explain why part (b) of Corollary 5.4.8 does not apply.

Solution.

(a) $f' = 4x^3 - 6x^2 + 2$. The Euclidean algorithm (Theorem 5.2.5):

$$f = \left(\tfrac{1}{4}x - \tfrac{1}{8}\right)f' - \tfrac{3}{4}(x^2 - 2x + 1),$$
$$f' = \left(-\tfrac{3}{4}(x^2 - 2x + 1)\right)\left(-\tfrac{8}{3}(2x + 1)\right) + 0.$$

The last non-zero remainder is $-\frac{3}{4}(x^2 - 2x + 1)$, so $\gcd(f, f') = x^2 - 2x + 1 \neq 1$. As $\mathbb{Q}$ has characteristic 0, Corollary 5.4.8 (b) says that f has a repeated irreducible factor. (Indeed $f = (x - 1)^3(x + 1)$, Example (Multiplicities by Repeated Division).)

(b) $f' = (4 \cdot 1)x^3 = 0$ in $\mathbb{F}_2$. Then $\langle f, 0\rangle = \langle f\rangle$, whose monic generator is f itself, so $\gcd(f, f') = f = x^4 + 1 \neq 1$ (Theorem 5.2.2 (c)). Part (b) of the corollary assumes characteristic 0, and $\mathbb{F}_2$ has characteristic 2 (Definition 2.5.1: $1 \neq 0$, $2 \cdot 1 = 0$). Its proof uses that hypothesis at $\deg p' = \deg p - 1$, which fails in characteristic 2: $(x^2 + 1)' = 0$. Here the conclusion happens to hold anyway, since $x^4 + 1 = (x + 1)^4$ in $\mathbb{F}_2$, but it is not given by the corollary; the gcd f records only that $f' = 0$.

5.5 Interpolation, Quotient Rings, and the Chinese Remainder Theorem

Section 5.4 proved a uniqueness statement: two polynomials of degree at most n that agree at $n + 1$ distinct points are equal (Theorem 5.4.2 (a)). It said nothing about existence. Is there, for instance, a quadratic through the points $(0, 1)$, $(1, 3)$, $(2, 7)$? This section builds one by a formula. It then reads the same question as three congruences. By Theorem 5.1.3 (a), "the value at c is y" says that f leaves the remainder y on division by $x - c$. So we look for f with

$$f \equiv 1 \pmod{x}, \qquad f \equiv 3 \pmod{x - 1}, \qquad f \equiv 7 \pmod{x - 2}.$$

Three congruences to coprime moduli: that is the Chinese remainder theorem of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3 (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3), with polynomials in place of integers. On the way we meet the classes modulo a polynomial m. They form a ring $F[x]/\langle m\rangle$, and it is a field exactly when m is irreducible, as $\mathbb{Z}/p\mathbb{Z}$ is a field exactly when p is prime.

Throughout, F is a field. "Polynomial" means an element of $F[x]$ unless another field is named.

5.5.1 Polynomials through given points

The points at which values are prescribed are called **nodes**. Suppose the nodes are $c_0, \ldots, c_n \in F$ and the values $y_0, \ldots, y_n \in F$. Fitting all the values at once is hard. Fitting one value while ignoring the others would be easy if we had, for each node c_i, a polynomial that is 1 at c_i and 0 at every other node: then y_0 times the first, plus y_1 times the second, and so on, has every value right. A polynomial that vanishes at the nodes c_j with $j \neq i$ is a multiple of the product of the factors $x - c_j$ (Theorem 5.4.1); the simplest is that product itself. Its value at c_i is the product of the numbers $c_i - c_j$, and dividing by that product makes the value 1.

Each Lagrange polynomial is 1 *at its own node and* 0 *at all the others.*

Definition 5.5.1. Lagrange Polynomials

Let $n \in \mathbb{N}$ and let $c_0, \dots, c_n \in F$ be **distinct**. For $i \in \{0, \dots, n\}$, the i-th **Lagrange polynomial** of these nodes is

$$\ell_i := \prod_{\substack{j=0 \\ j \neq i}}^{n} (c_i - c_j)^{-1}(x - c_j) \in F[x],$$

the product, in increasing order of j, of the n polynomials $(c_i - c_j)^{-1}(x - c_j)$ with $j \neq i$.

The inverse $(c_i - c_j)^{-1}$ exists because $c_i \neq c_j$ for $j \neq i$, and F is a field. The product of a list of polynomials is given by the recursion of Sets, Relations, and Cardinality, Definition 2.3.1, read in the commutative ring $F[x]$ (Theorem 4.2.4 (a)); the pattern *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$ used for lists of integers.

Examples.

- *Two nodes.* For the nodes $0, 1 \in \mathbb{Q}$: $\ell_0 = (0-1)^{-1}(x-1) = 1-x$ and $\ell_1 = (1-0)^{-1}(x-0) = x$. Indeed $\ell_0(0) = 1$, $\ell_0(1) = 0$, $\ell_1(0) = 0$, $\ell_1(1) = 1$.
- *Three nodes.* For the nodes $0, 1, 2 \in \mathbb{Q}$, the polynomial ℓ_0 is

  $$\ell_0 = (0-1)^{-1}(x-1) \cdot (0-2)^{-1}(x-2) = \tfrac{1}{2}(x-1)(x-2).$$

  It vanishes at 1 and 2, and $\ell_0(0) = \frac{1}{2} \cdot (-1)(-2) = 1$.
- *Over a finite field.* In $\mathbb{F}_3$, with the nodes $0, 1, 2$, the same formula gives $\ell_0 = 2^{-1}(x-1)(x-2) = 2(x-1)(x-2)$, since $2 \cdot 2 = 4 = 1$ in $\mathbb{F}_3$. Its value at 0 is $2 \cdot (-1)(-2) = 4 = 1$.

↻ **Second reading** · *One node, and a repeated node*

One node ($n = 0$). The product defining ℓ_0 has no factors, so $\ell_0 = 1$, the empty product. The theorem below then says that the only polynomial of degree at most 0 with value y_0 at c_0 is the constant y_0, which is right.

A repeated node. Change the nodes $0, 1$ of the first example to $0, 0$. The clause that fails is "distinct": the factor $(c_0 - c_1)^{-1} = 0^{-1}$ does not exist. Nothing can repair this. A polynomial cannot have the value 1 at 0 and also the value 2 at 0, so with a repeated node some prescribed values have no interpolating polynomial at all.

The next theorem says that the Lagrange polynomials do what they were built for, and that the polynomial they produce is the only one.

Theorem 5.5.1. Lagrange Interpolation

Let $n \in \mathbb{N}$, let $c_0, \dots, c_n \in F$ be distinct, and let $y_0, \dots, y_n \in F$. Let $\ell_0, \dots, \ell_n$ be the Lagrange polynomials of the nodes (Definition 5.5.1).

(a) For all $i, k \in \{0, \dots, n\}$, $\ell_i(c_k) = 1$ if $k = i$ and $\ell_i(c_k) = 0$ if $k \neq i$. Each ℓ_i has degree exactly n.

(b) The polynomial $p \coloneqq \sum_{i=0}^{n} y_i \ell_i$ satisfies $\deg p \leq n$ and $p(c_k) = y_k$ for every k.

(c) It is the **only** polynomial of degree at most n with $p(c_k) = y_k$ for every k.

(d) Every $q \in F[x]$ with $\deg q \leq n$ satisfies $q = \sum_{i=0}^{n} q(c_i)\ell_i$.

Try it first (ten minutes): for the nodes $0, 1, 2 \in \mathbb{Q}$, write down ℓ_0, ℓ_1, ℓ_2 and check (a) on them. Then find a quadratic through $(0, 1)$, $(1, 3)$, $(2, 7)$. Why can there be no second one?

Idea. The direct attempt writes $p = a_0 + a_1 x + a_2 x^2$ and solves the three equations $p(0) = 1$, $p(1) = 3$, $p(2) = 7$ for a_0, a_1, a_2. It works here, but it gives no formula, and for $n + 1$ nodes it is a system of $n + 1$ equations. The Lagrange polynomials replace the system by a sum: (a) is "evaluate at a root", since every factor $x - c_j$ with $j \neq i$ vanishes at c_j, and (b) follows from (a) term by term. The second question, why there is no other quadratic, is not answered by any construction. It is answered by counting roots: two such quadratics differ by a polynomial of degree at most 2 with three roots.

Proof.

(a) Let $i, k \in \{0, \ldots, n\}$. Evaluation respects products (Theorem 4.4.1), so $\ell_i(c_k)$ is the product of the values of the factors at c_k:

$$\ell_i(c_k) = \prod_{\substack{j=0 \\ j \neq i}}^{n} (c_i - c_j)^{-1}(c_k - c_j).$$

If $k \neq i$, the factor with $j = k$ is $(c_i - c_k)^{-1} \cdot 0 = 0$, so the product is 0. If $k = i$, every factor is $(c_i - c_j)^{-1}(c_i - c_j) = 1$, so the product is 1. For the degree, each factor $(c_i - c_j)^{-1}x - (c_i - c_j)^{-1}c_j$ has degree 1, since its coefficient of x is non-zero. A field has no zero divisors, so by Theorem 4.3.2 (b) the degree of a product is the sum of the degrees; with n factors, $\deg \ell_i = n$.

(b) Each term $y_i \ell_i$ has degree at most n (Theorem 4.3.2 (a)), so $\deg p \leq n$ by Theorem 4.3.1, applied one term at a time. Evaluating at c_k and using (a),

$$p(c_k) = \sum_{i=0}^{n} y_i \ell_i(c_k) = y_k,$$

since every term with $i \neq k$ is $y_i \cdot 0 = 0$, and the term $i = k$ is $y_k \cdot 1$ ((Σ3) of Lemma 4.1.1).

(c) Let $q \in F[x]$ with $\deg q \leq n$ and $q(c_k) = y_k$ for every k. Then p and q both have degree at most n and agree at the $n + 1$ distinct points $c_0, \ldots, c_n$. By Theorem 5.4.2 (a), $q = p$.

(d) Let $\deg q \leq n$, and apply (b) and (c) with $y_i \coloneqq q(c_i)$. The polynomial $\sum_i q(c_i)\ell_i$ and q itself both have degree at most n and the values $q(c_0), \ldots, q(c_n)$ at the nodes, so they are equal by (c). This proves the theorem.

■

So for distinct nodes and any values, there is exactly one polynomial of degree at most n through the points, and (b) writes it down. Part (d) says that a polynomial of degree at most n

is determined by its values at $n+1$ nodes, and rebuilt from them by the same formula. Where the linear-algebra companion, Chapter 6, speaks of "the Lagrange basis", this book has only the formula (d); no basis is defined here.

Warning. The bound "degree at most n" in (c) is what makes the interpolant unique. Without it, uniqueness fails: p and $p+(x-c_0)(x-c_1)\cdots(x-c_n)$ have the same values at every node, and the second has degree $n+1$. For the nodes $0,1$ and the values $5,8$, both $5+3x$ and $5+3x+x(x-1)=5+2x+x^2$ pass through $(0,5)$ and $(1,8)$.

Quick check. Write down the Lagrange polynomials of the nodes $0,1$ in $\mathbb{Q}$, and use them to find the line through $(0,5)$ and $(1,8)$.

Solution. $\ell_0 = 1-x$ and $\ell_1 = x$ (the first example after Definition 5.5.1). By Theorem 5.5.1 (b), the line is $5\ell_0+8\ell_1 = 5(1-x)+8x = 5+3x$. Check: its values at 0 and 1 are 5 and 8.

Here is a cubic, worked through the formula.

Example. A cubic through four points

Find the polynomial $p \in \mathbb{Q}[x]$ of degree at most 3 with $p(-1)=2$, $p(0)=1$, $p(1)=2$ and $p(2)=11$.

Solution. The nodes $c_0=-1$, $c_1=0$, $c_2=1$, $c_3=2$ are distinct. From Definition 5.5.1, with the denominators computed first,

$$\begin{aligned}
\ell_0 &= \big((-1)(-2)(-3)\big)^{-1}x(x-1)(x-2) = (-6)^{-1}(x^3-3x^2+2x),\\
\ell_1 &= \big((1)(-1)(-2)\big)^{-1}(x+1)(x-1)(x-2) = 2^{-1}(x^3-2x^2-x+2),\\
\ell_2 &= \big((2)(1)(-1)\big)^{-1}(x+1)x(x-2) = (-2)^{-1}(x^3-x^2-2x),\\
\ell_3 &= \big((3)(2)(1)\big)^{-1}(x+1)x(x-1) = 6^{-1}(x^3-x).
\end{aligned}$$

By Theorem 5.5.1 (b), $p = 2\ell_0+\ell_1+2\ell_2+11\ell_3$. Collect each power of x:

$$\begin{aligned}
x^3:&\ -\tfrac{1}{3}+\tfrac{1}{2}-1+\tfrac{11}{6}=1, \qquad x^2:\ 1-1+1=1,\\
x:&\ -\tfrac{2}{3}-\tfrac{1}{2}+2-\tfrac{11}{6}=-1, \qquad 1:\ 0+1+0+0=1.
\end{aligned}$$

So $p = x^3+x^2-x+1$. Check the four values: $p(-1) = -1+1+1+1 = 2$, $p(0)=1$, $p(1)=1+1-1+1=2$, $p(2)=8+4-2+1=11$. By Theorem 5.5.1 (c), no other polynomial of degree at most 3 has these values.

5.5.2 Congruence modulo a polynomial

The opening question turned values into remainders. To compute with remainders as *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3 did with integers, we need the relation "same remainder" and

the classes it makes.

Definition 5.5.2. Congruence Modulo a Polynomial

Let $m \in F[x]$. Polynomials $f, g \in F[x]$ are **congruent modulo** m, written $f \equiv g \pmod{m}$, if $m \mid f - g$ (Definition 5.1.1), that is, if $f - g \in \langle m \rangle$ (Definition 5.2.1).

In words: f and g differ by a multiple of m. The set $\langle m \rangle$ of multiples of m is an ideal of the commutative ring $F[x]$ (Definition 5.2.1), so the relation is the relation $\sim_I$ of Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 for the ideal $I = \langle m \rangle$, and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (a) makes it an equivalence relation. We write $[f] = f + \langle m \rangle$ for the class of f, and $[f]_m$ when the modulus must be named.

Examples.

- $x^2 \equiv -1 \pmod{x^2+1}$, since $x^2 - (-1) = 1 \cdot (x^2+1)$.
- For every $c \in F$, $f \equiv f(c) \pmod{x-c}$: by Theorem 5.1.3 (a), $f = q(x-c) + f(c)$ for some q, so $f - f(c)$ is a multiple of $x - c$.
- Two polynomials are congruent modulo m exactly when they leave the same remainder on division by $m \neq 0$; this is (b) of the next theorem.

Second reading · *The degenerate moduli 0 and the constants*

For $m = 0$, $f \equiv g \pmod{0}$ means $0 \mid f - g$, that is, $f = g$ (Proposition 5.1.1 (a)): every class is a single polynomial. For a non-zero constant m, every f is a multiple of m (Proposition 5.1.1 (a)), so all polynomials are congruent and there is one class; the ring it forms is the zero ring, in which $[1] = [0]$. Both cases are legal and neither is useful, which is why the next theorem asks for $\deg m \geq 1$.

Quick check. Is $x^3 \equiv x \pmod{x^2+1}$ in $\mathbb{Q}[x]$? In $\mathbb{F}_2[x]$?

Solution. Divide: $x^3 = x(x^2+1) - x$, so $x^3 \equiv -x$, and $x^3 - x = x(x^2+1) - 2x$. Hence $x^3 \equiv x$ exactly when $x^2+1 \mid -2x$. In $\mathbb{Q}[x]$ the polynomial $-2x$ is non-zero of degree $1 < 2$, so x^2+1 does not divide it (Proposition 5.1.1 (d)): **no**. In $\mathbb{F}_2[x]$, $-2x = 0$, which every polynomial divides: **yes**. The same symbols give different answers over different fields.

5.5.3 The ring of classes modulo a polynomial

Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Chapter 3 built $\mathbb{Z}/n\mathbb{Z}$ as the quotient of $\mathbb{Z}$ by the ideal $n\mathbb{Z}$, and found in each class exactly one remainder in $\{0, \ldots, n-1\}$. The same construction works for $F[x]$ and an ideal $\langle m \rangle$, and division with remainder again picks one representative per class, now "of degree less than $\deg m$".

Theorem 5.5.2. The Ring of Polynomials Modulo m

Let $m \in F[x]$ with $d := \deg m \geq 1$, and write $[f] = f + \langle m \rangle$.

(a) $F[x]/\langle m \rangle$, with $[f] + [g] := [f + g]$ and $[f][g] := [fg]$, is a commutative ring with zero $[0]$ and one $[1]$, and $[1] \neq [0]$.

(b) Each class contains **exactly one** polynomial of degree less than d: the remainder of any of its members on division by m. In particular $f \equiv g \pmod{m}$ if and only if f and g leave the same remainder, and sending each class to its member of degree less than d is a bijection from $F[x]/\langle m \rangle$ onto $\{r \in F[x] : \deg r < d\}$.

(c) The map $F \to F[x]/\langle m \rangle$, $c \mapsto [c]$ (c a constant), is injective and preserves $+$ and $\cdot$.

(d) $[f]$ is a unit of $F[x]/\langle m \rangle$ (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1) **if and only if** $\gcd(f, m) = 1$. In that case $[f]^{-1} = [a]$ for **any** $a, b \in F[x]$ with $af + bm = 1$.

Idea. Part (a) is the quotient theorem of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$ applied to the ideal $\langle m \rangle$; only $[1] \neq [0]$ needs the degree. Part (b) is division with remainder read twice: existence of the remainder puts one polynomial of small degree into each class, and "compare degrees" shows a class cannot hold two, since their difference would be a non-zero multiple of m of smaller degree than m. Part (d) translates $[a][f] = [1]$ into a Bézout identity, exactly as for $\mathbb{Z}/n\mathbb{Z}$.

Proof.

(a) By Definition 5.2.1, $\langle m \rangle$ is an ideal of the commutative ring $F[x]$, so Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (a)–(c) give the commutative ring $F[x]/\langle m \rangle$ with these operations, zero $[0]$ and one $[1]$. By Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (d), $[1] = [0]$ would mean $1 \in \langle m \rangle$, that is, $m \mid 1$; then $\deg m \leq \deg 1 = 0$ by Proposition 5.1.1 (d), against $d \geq 1$. So $[1] \neq [0]$.

(b) Since $d \geq 1$, $m \neq 0$. *Existence.* Let $f \in F[x]$. By Theorem 5.1.2 (a), $f = qm + r$ with $\deg r < d$. Then $f - r = qm \in \langle m \rangle$, so $r \in [f]$. *Uniqueness.* Let $r, r' \in [f]$ with $\deg r, \deg r' < d$. Then $r - r' \in \langle m \rangle$ (both are $\sim$ to f, and $\sim$ is an equivalence relation), so $m \mid r - r'$, and $\deg(r - r') < d$ by Theorem 4.3.1. If $r - r' \neq 0$, then $d \leq \deg(r - r')$ by Proposition 5.1.1 (d), a contradiction. So $r = r'$.
Hence two polynomials are congruent exactly when their classes are equal (Sets, Relations, and Cardinality, Theorem 2.5.1 (b)), exactly when the classes have the same member of degree less than d, which is the common remainder. The map "class $\mapsto$ its member of degree less than d" is a function by the uniqueness just proved. It is injective, since two classes with a common member are equal (Sets, Relations, and Cardinality, Theorem 2.5.1 (c)); and it is surjective, since a polynomial r with $\deg r < d$ is the member of degree less than d of its own class $[r]$.

(c) For constants c, c', $[c]+[c'] = [c+c']$ and $[c][c'] = [cc']$ by the definition of the operations, where $c + c'$ and cc' are computed in F (Theorem 4.2.4 (b)). If $[c] = [c']$, then c and c' are members of one class of degree at most $0 < d$, so $c = c'$ by (b).

(d) ($\Leftarrow$) Suppose $\gcd(f, m) = 1$. By Corollary 5.2.3 there are $a, b \in F[x]$ with $af + bm = 1$; let a, b be any such pair. Then $af - 1 = -bm \in \langle m \rangle$, so $[a][f] = [af] = [1]$. So $[f]$ is a unit, and its inverse, which is unique (Number Systems: From \(\nN\) to \(\nR\), Definition 3.5.1), is $[a]$.

($\Rightarrow$) Suppose $[a][f] = [1]$ for some $a \in F[x]$ (every element of the quotient is a class, Sets, Relations, and Cardinality, Definition 2.5.4). Then $af - 1 \in \langle m \rangle$: $af - 1 = km$ for some $k \in F[x]$. Hence $af + (-k)m = 1$, and $\gcd(f, m) = 1$ by Corollary 5.2.3. This proves the theorem.

■

So $F[x]/\langle m \rangle$ is a ring whose elements may be named by the polynomials of degree less than $\deg m$, and by (c) its constants form a copy of F. From now on we write c for the class $[c]$ of a constant when no confusion can arise. A computation in the quotient is: compute with representatives, then replace the result by its remainder. The integer twins are Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.3 (b) (one remainder per class) and Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.1 (units).

Quick check. In $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$, show that $[x + 1]$ is a unit, and find its inverse with (d).

Solution. Divide: $x^2 - 2 = (x - 1)(x + 1) - 1$. Hence $(x - 1)(x + 1) + (-1)(x^2 - 2) = 1$, so $\gcd(x + 1, x^2 - 2) = 1$ (Corollary 5.2.3), and by Theorem 5.2.2 (d) with $a = x - 1$, $[x + 1]$ is a unit with $[x + 1]^{-1} = [x - 1]$. Check: $(x + 1)(x - 1) = x^2 - 1 \equiv 2 - 1 = 1 \pmod{x^2 - 2}$.

When is every non-zero class a unit? By (d), when every f with $m \nmid f$ is coprime to m. For an irreducible m, Corollary 5.3.3 (a) says exactly this. For a reducible m, a factor of m of smaller positive degree is neither a multiple of m nor coprime to it.

Theorem 5.5.3. The Quotient Is a Field Exactly When m Is Irreducible

Let $m \in F[x]$ with $\deg m \geq 1$. Then $F[x]/\langle m \rangle$ is a field (Definition 2.1.1) **if and only if** m is irreducible over F (Definition 5.3.1).

Proof. By Theorem 5.5.2 (a), $F[x]/\langle m \rangle$ is a commutative ring with $[1] \neq [0]$. So it is a field exactly when every non-zero element is a unit.

($\Leftarrow$) Let m be irreducible and $[f] \neq [0]$. Then $f \notin \langle m \rangle$ by Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (d), that is, $m \nmid f$. By Corollary 5.3.3 (a), $\gcd(m, f) = 1$; the definition of the gcd (Definition 5.2.2) is symmetric in its two arguments, so $\gcd(f, m) = 1$. Hence $[f]$ is a unit by Theorem 5.5.2 (d).

($\Rightarrow$) Let m be not irreducible. Since $\deg m \geq 1$, Definition 5.3.1 gives $g, h \in F[x]$, neither a constant, with $m = gh$. Then $g, h \neq 0$ and $\deg g, \deg h \geq 1$, and $\deg g + \deg h = \deg m$ (Theorem 4.3.2 (b)), so $\deg g, \deg h < \deg m$. A non-zero polynomial of degree less than $\deg m$ is not a multiple of m (Proposition 5.1.1 (d)), so $[g] \neq [0]$ and $[h] \neq [0]$. But $[g][h] = [gh] = [m] = [0]$. In a field a product of non-zero elements is non-zero (Theorem 2.1.1 (f)), so $F[x]/\langle m \rangle$ is not a field. This proves the theorem.

■

This is Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.2 with "prime" replaced by

"irreducible". It manufactures new fields: from F and an irreducible m of degree d, a field whose elements are named by the polynomials of degree less than d.

Example. A field with four elements, and the complex numbers again

(i) Describe $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$, and show that it is a field with four elements.

(ii) Describe $\mathbb{R}[x]/\langle x^2+1\rangle$.

Solution.

(i) Let $m := x^2+x+1 \in \mathbb{F}_2[x]$. Its values are $m(0)=1$ and $m(1)=1+1+1=1$ in $\mathbb{F}_2$, so m has no root in $\mathbb{F}_2$; it has degree 2, so it is irreducible by Proposition 5.3.1 (b), and the quotient is a field by Theorem 5.5.3. By Theorem 5.5.2 (b), its elements are the classes of the polynomials of degree less than 2 over $\mathbb{F}_2$, namely $0, 1, x, x+1$: four elements. Write $\alpha := [x]$. Since $x^2-(x+1) = x^2+x+1$ in $\mathbb{F}_2[x]$ (where $-1=1$), $x^2 \equiv x+1$, and so

$$\alpha^2 = \alpha+1, \qquad \alpha(\alpha+1) = \alpha^2+\alpha = 2\alpha+1 = 1, \qquad (\alpha+1)^2 = \alpha^2+2\alpha+1 = \alpha,$$

using $2=0$ in $\mathbb{F}_2$. The multiplication table of the non-zero elements is therefore

$\cdot$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

and every non-zero element has an inverse in it, as the theorem promised. Also $\alpha^3 = \alpha\cdot\alpha^2 = \alpha(\alpha+1) = 1$. This is the four-element field of Exercise (C1: A Field with Four Elements). There the rule $\alpha^2 = 1+\alpha$ is part of the definition of the multiplication; here it is computed, as the remainder of x^2 on division by x^2+x+1.

(ii) The polynomial $x^2+1 \in \mathbb{R}[x]$ has no real root, since $c^2+1 \geq 1 > 0$ for every $c \in \mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)); it has degree 2, so it is irreducible (Proposition 5.3.1 (b)), and $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field. Its elements are the classes $[a+bx]$ with $a, b \in \mathbb{R}$, each named by exactly one such polynomial, and $[x]^2 = [x^2] = [-1]$. So it is a field containing a copy of $\mathbb{R}$ (Theorem 5.5.2 (c)) and an element whose square is -1: it looks like the complex numbers of Chapter 1, and Exercise B3 shows it is a copy of them.

The theorem needs "irreducible", and having no root is not a substitute: Section 5.3 showed that the two differ from degree 4 on.

Warning. "m has no root, so $F[x]/\langle m\rangle$ is a field" is false. The polynomial $m = (x^2+1)^2 \in \mathbb{R}[x]$ has no real root: for every $c \in \mathbb{R}$, $c^2+1 > 0$ (Example (A field with four elements, and the complex numbers again) (ii)), so $m(c) = (c^2+1)^2 > 0$ by Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e). But $[x^2+1] \neq [0]$, since x^2+1 has degree $2 < 4 = \deg m$, while $[x^2+1]^2 = [(x^2+1)^2] = [0]$. A non-zero element with square zero cannot be a unit, so $\mathbb{R}[x]/\langle (x^2+1)^2\rangle$ is not a field.

Quick check. Is $\mathbb{Q}[x]/\langle x^2-2\rangle$ a field? Is $\mathbb{R}[x]/\langle x^2-2\rangle$?

Solution. $\mathbb{Q}[x]/\langle x^2-2\rangle$: **yes**. A rational root c would give $c^2=2$, impossible by Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1; so x^2-2 is irreducible over $\mathbb{Q}$ (Proposition 5.3.1 (b)), and Theorem 5.5.3 applies. $\mathbb{R}[x]/\langle x^2-2\rangle$: **no**. With s the positive square root of 2 in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), $x^2-2=(x-s)(x+s)$ is reducible over $\mathbb{R}$, and the theorem says the quotient is not a field; concretely $[x-s][x+s]=[0]$.

5.5.4 The Chinese remainder theorem for polynomials

Now several congruences at once. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 3 solved two congruences to coprime integer moduli by writing 1 as a combination of the moduli and multiplying (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3). With polynomials the move is the same, and we take k moduli at once. The one new ingredient is that coprimality survives products.

Lemma 5.5.4. Coprime to Each Factor, Coprime to the Product

(a) Let $s\geq 1$ and $p,q_1,\dots,q_s\in F[x]$. If $\gcd(p,q_j)=1$ for every j, then $\gcd(p,q_1\cdots q_s)=1$.

(b) Let $k\geq 1$ and let $m_1,\dots,m_k\in F[x]$ be **pairwise coprime**: $\gcd(m_i,m_j)=1$ whenever $i\neq j$. If $m_i\mid h$ for every i, then $m_1\cdots m_k\mid h$.

In words: a polynomial coprime to each factor is coprime to the product, and pairwise coprime divisors of h divide h together.

↻ **Second reading** · *The proof: multiply the Bézout identities*

Idea. For (a), write 1 as a combination of p and each factor, and multiply the identities: every term of the product but one contains p, and the remaining term is a multiple of the product of the factors. For (b), the product of the first k moduli is coprime to the next one by (a), so two coprime divisors combine (Proposition 5.3.4); induction adds one modulus at a time.

Proof.

(a) We apply Logic and Proof, Axiom 4.2.1 (on $\mathbb{N}=\omega$, Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) to $P(n)$: "the claim holds for $s=n+1$". $P(0)$, the case $s=1$, has nothing to prove. Suppose $P(n)$, that is, the claim for $s=n+1$, and let p be coprime to each of $q_1,\dots,q_{s+1}$. Write $Q:=q_1\cdots q_s$, so that $q_1\cdots q_{s+1}=Qq_{s+1}$ by the product recursion (Sets, Relations, and Cardinality, Definition 2.3.1, read in $F[x]$). By the induction hypothesis and Corollary 5.2.3, $ap+bQ=1$ and $a'p+b'q_{s+1}=1$ for

some $a, b, a', b' \in F[x]$. Multiplying the two identities and expanding,

$$p\,(aa'p + ab'q_{s+1} + a'bQ) + (bb')\,Qq_{s+1} = 1.$$

So $\gcd(p, Qq_{s+1}) = 1$ by Corollary 5.2.3.

(b) We apply Logic and Proof, Axiom 4.2.1 (on $\mathbb{N} = \omega$, Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3 (b)) to $P(n)$: "the claim holds for $k = n + 1$". $P(0)$, the case $k = 1$, has nothing to prove. Suppose $P(n)$, that is, the claim for $k = n + 1$, and let $m_1, \dots, m_{k+1}$ be pairwise coprime, each dividing h. With $M \coloneqq m_1 \cdots m_k$, the induction hypothesis gives $M \mid h$. The modulus m_{k+1} is coprime to each of $m_1, \dots, m_k$, so $\gcd(m_{k+1}, M) = 1$ by (a), and $\gcd(M, m_{k+1}) = 1$ since the gcd is symmetric (Definition 5.2.2). By Proposition 5.3.4, $Mm_{k+1} = m_1 \cdots m_{k+1}$ divides h.

■

Without coprimality (b) fails: for $m_1 = m_2 = x$ and $h = x$, each m_i divides h, but $m_1 m_2 = x^2$ does not (Proposition 5.1.1 (d)); here $\gcd(m_1, m_2) = x \neq 1$.

Theorem 5.5.5. Chinese Remainder Theorem for Polynomials

Let $k \geq 1$, let $m_1, \dots, m_k \in F[x]$ be non-zero and pairwise coprime, and let $m \coloneqq m_1 \cdots m_k$. For each i, let M_i be the product of the m_j with $j \neq i$ (in increasing order of j).

(a) For each i there are $a_i, b_i \in F[x]$ with $a_i M_i + b_i m_i = 1$. Put $e_i \coloneqq a_i M_i$. Then $e_i \equiv 1 \pmod{m_i}$ and $e_i \equiv 0 \pmod{m_j}$ for $j \neq i$, and for all $r_1, \dots, r_k \in F[x]$ the polynomial $f \coloneqq \sum_{i=1}^{k} r_i e_i$ satisfies

$$f \equiv r_i \pmod{m_i} \qquad \text{for every } i \in \{1, \dots, k\}.$$

(b) A polynomial g satisfies the same k congruences **if and only if** $g \equiv f \pmod{m}$.

(c) Exactly one polynomial of degree less than $\deg m$ satisfies the k congruences.

(d) The rule $\Phi([f]_m) \coloneqq ([f]_{m_1}, \dots, [f]_{m_k})$ is a well-defined **bijection**

$$\Phi\colon F[x]/\langle m\rangle \to F[x]/\langle m_1\rangle \times \cdots \times F[x]/\langle m_k\rangle,$$

and, with $+$ and $\cdot$ on the right taken componentwise, Φ preserves $+$ and $\cdot$ and sends $[1]_m$ to $([1]_{m_1}, \dots, [1]_{m_k})$.

Idea. This is the integer proof of Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3 with k moduli. The identity $a_i M_i + b_i m_i = 1$ makes a polynomial e_i that is 1 modulo m_i and 0 modulo every other modulus, as ℓ_i is 1 at one node and 0 at the others. Then $\sum r_i e_i$ has every remainder right. Uniqueness modulo m is Lemma 5.5.4 (b): a difference divisible by every m_i is divisible by their product. Part (c) picks the remainder modulo m, and (d) restates (a) and (b) as a bijection.

Proof. By (L2) of Section 5.3, applied to the list $(m_1, \dots, m_k)$ with the entry i removed, $m = M_i m_i$, so $m_i \mid m$; and $m_j \mid M_i$ for $j \neq i$, by the last clause of (L2), since m_j is an entry

of the list whose product is M_i. By (L1) of Section 5.3, $m \neq 0$, since every m_i is non-zero.

(a) If $k = 1$, then $M_1 = 1$ (the empty product), and $a_1 := 1$, $b_1 := 0$ will do. If $k \geq 2$, then m_i is coprime to each m_j with $j \neq i$, so Lemma 5.5.4 (a) gives $\gcd(m_i, M_i) = 1$; by the symmetry of the gcd and Corollary 5.2.3, $a_i M_i + b_i m_i = 1$ for some a_i, b_i. In either case $e_i - 1 = -b_i m_i$, so $e_i \equiv 1 \pmod{m_i}$; and for $j \neq i$, $m_j \mid M_i \mid e_i$, so $e_i \equiv 0 \pmod{m_j}$.
Now fix j. In $f - r_j = \sum_{i \neq j} r_i e_i + r_j(e_j - 1)$, every term with $i \neq j$ is a multiple of m_j, and so is $r_j(e_j - 1) = -r_j b_j m_j$. A sum of multiples of m_j is a multiple of m_j (Proposition 5.1.1 (c), and induction on the number of terms). So $f \equiv r_j \pmod{m_j}$.

(b) ($\Rightarrow$) Suppose $g \equiv r_i \pmod{m_i}$ for every i. Then $m_i \mid (g - r_i) - (f - r_i) = g - f$ for every i (Proposition 5.1.1 (c)). The m_i are pairwise coprime, so $m \mid g - f$ by Lemma 5.5.4 (b). ($\Leftarrow$) Suppose $m \mid g - f$. Since $m_i \mid m$, $m_i \mid g - f$ (Proposition 5.1.1 (b)), and then $m_i \mid (g - f) + (f - r_i) = g - r_i$ for every i.

(c) *Existence.* Since $m \neq 0$, divide f by m: $f = qm + r$ with $\deg r < \deg m$ (Theorem 5.1.2). Then $r \equiv f \pmod{m}$, so r satisfies the k congruences by (b). *Uniqueness.* If g and g' both satisfy them and have degree less than $\deg m$, then $g \equiv f \equiv g' \pmod{m}$ by (b), so $m \mid g - g'$, while $\deg(g - g') < \deg m$ (Theorem 4.3.1). A non-zero multiple of m has degree at least $\deg m$ (Proposition 5.1.1 (d)), so $g = g'$. (If every m_i is a non-zero constant, then $\deg m = 0$, and the one solution of degree less than 0 is the zero polynomial.)

(d) *Well defined.* Fix i. If $f \equiv g \pmod{m}$, then $f \equiv g \pmod{m_i}$, since $m_i \mid m$. By Number Systems: From \(\nN\) to \(\nR\), Theorem 2.2.1 (a), applied to the identity map of $F[x]$ with congruence modulo m on the source and modulo m_i on the target, there is exactly one function $F[x]/\langle m \rangle \to F[x]/\langle m_i \rangle$ sending $[f]_m$ to $[f]_{m_i}$. Taking these k functions together gives Φ.

Surjective. An element of the target is $([r_1]_{m_1}, \ldots, [r_k]_{m_k})$ for some $r_1, \ldots, r_k \in F[x]$ (Sets, Relations, and Cardinality, Definition 2.5.4). With f as in (a), $[f]_{m_i} = [r_i]_{m_i}$ for every i (Sets, Relations, and Cardinality, Theorem 2.5.1 (b)), so $\Phi([f]_m)$ is that element.

Injective. If $\Phi([f]_m) = \Phi([g]_m)$, then $[f]_{m_i} = [g]_{m_i}$, that is, $m_i \mid g - f$, for every i (Sets, Relations, and Cardinality, Theorem 2.5.1 (b)). By Lemma 5.5.4 (b), $m \mid g - f$, that is, $[g]_m = [f]_m$.

Operations. By the definition of $+$ in each quotient (Number Systems: From \(\nN\) to \(\nR\), Theorem 3.4.1 (b)) and of the componentwise sum,

$$\begin{aligned}\Phi([f]_m + [g]_m) &= \Phi([f+g]_m) = ([f+g]_{m_1}, \ldots, [f+g]_{m_k}) \\ &= ([f]_{m_1} + [g]_{m_1}, \ldots, [f]_{m_k} + [g]_{m_k}) = \Phi([f]_m) + \Phi([g]_m).\end{aligned}$$

The same lines with fg in place of $f + g$ give the product, and $\Phi([1]_m) = ([1]_{m_1}, \ldots, [1]_{m_k})$ by definition. This proves the theorem.

■

In (a) the solution is built from the moduli alone, and the right-hand sides r_i enter linearly; the e_i depend only on $m_1, \ldots, m_k$. Part (c) is the version used in computation: reduce any solution modulo m. Compared with Number Systems: From \(\nN\) to \(\nR\), Theorem 3.5.3, this theorem allows any number $k \geq 1$ of moduli in one step, where the integer theorem combines two at a time.

Quick check. Find the polynomial $f \in \mathbb{Q}[x]$ of degree less than 2 with $f \equiv 3 \pmod{x}$ and $f \equiv 5 \pmod{x-1}$.

Solution. By Theorem 5.1.3 (b), $f \equiv 3 \pmod{x}$ says that 0 is a root of $f-3$, that is, $f(0) = 3$; likewise the second congruence says $f(1) = 5$. By Theorem 5.5.1, $f = 3(1-x)+5x = 3+2x$. (The Chinese remainder route: $x-(x-1) = 1$, so $e_1 = -(x-1) = 1-x$ and $e_2 = x$, and $f = 3e_1 + 5e_2$, the same polynomial.)

The check is no accident. Interpolation is the Chinese remainder theorem for the moduli $x - c_i$.

Proposition 5.5.6. Interpolation Is the Chinese Remainder Theorem for Linear Moduli

Let $n \in \mathbb{N}$, let $c_0, \ldots, c_n \in F$ be distinct, let $y_0, \ldots, y_n \in F$, and let $m := (x-c_0)\cdots(x-c_n)$.

(a) The moduli $x-c_0, \ldots, x-c_n$ are pairwise coprime, and $\deg m = n+1$.

(b) For $f \in F[x]$ and each i: $f \equiv y_i \pmod{x-c_i}$ **if and only if** $f(c_i) = y_i$.

(c) The polynomial of degree less than $n+1$ given by Theorem 5.5.5 (c) for the right-hand sides $y_0, \ldots, y_n$ is $\sum_i y_i \ell_i$, the interpolating polynomial of Theorem 5.5.1. In particular, the remainder of the polynomial e_i of Theorem 5.5.5 (a) on division by m is the Lagrange polynomial ℓ_i.

In words: the congruences modulo $x - c_i$ are the values at c_i, so the polynomial of the Chinese remainder theorem is the interpolating polynomial, and its building blocks e_i, reduced modulo m, are the Lagrange polynomials.

Second reading · *The proof: evaluate, and compare by uniqueness*

Idea. Two linear moduli differ by a non-zero constant, which is a Bézout identity after scaling. A congruence modulo $x - c$ is a statement about the value at c, by the factor theorem. And two polynomials of degree less than $n+1$ solving the same congruences are equal, by the uniqueness half of the Chinese remainder theorem; so it is enough to check that the Lagrange formula solves them.

Proof.

(a) For $i \neq j$, $(x-c_i)-(x-c_j) = c_j - c_i$, a non-zero constant. Multiplying by its inverse,

$$(c_j-c_i)^{-1}(x-c_i) - (c_j-c_i)^{-1}(x-c_j) = 1,$$

so $\gcd(x-c_i, x-c_j) = 1$ by Corollary 5.2.3. Each factor of m has degree 1, so $\deg m = n+1$ by Theorem 4.3.2 (b).

(b) By Theorem 5.1.3 (b), $x-c_i \mid f-y_i$ if and only if c_i is a root of $f-y_i$, and $(f-y_i)(c_i) = f(c_i) - y_i$ by Theorem 4.4.1.

(c) The polynomial $p := \sum_i y_i \ell_i$ has degree at most $n < n+1$ and $p(c_i) = y_i$ for every i

(Theorem 5.5.1 (b)), so by (b) it satisfies the congruences $p \equiv y_i \pmod{x - c_i}$. By the uniqueness in Theorem 5.5.5 (c), it is the solution of degree less than $\deg m$. For the second claim, fix i and take the right-hand sides 1 at the index i and 0 elsewhere. By Theorem 5.5.5 (a), e_i satisfies these congruences, and so does its remainder on division by m, which is congruent to e_i modulo m (Theorem 5.5.5 (b)) and has degree less than $\deg m$. By the first claim, with these right-hand sides, that remainder is $\sum_j y_j \ell_j = \ell_i$.

■

So two routes lead to the same polynomial. The Lagrange route needs only evaluation and the root count; the Chinese remainder route needs Bézout identities, and in exchange it works for moduli of any degree. The next two examples use moduli that are not all linear.

Example. A linear and a quadratic modulus

Find the polynomial $f \in \mathbb{Q}[x]$ of degree less than 3 with

$$f \equiv 1 \pmod{x - 2} \qquad \text{and} \qquad f \equiv 2x - 1 \pmod{x^2 + 1}.$$

Solution. A Bézout identity. Divide: $x^2 + 1 = (x + 2)(x - 2) + 5$. Hence

$$1 = \tfrac{1}{5}(x^2 + 1) - \tfrac{1}{5}(x + 2)(x - 2),$$

so the moduli $m_1 := x - 2$ and $m_2 := x^2 + 1$ are coprime (Corollary 5.2.3), and $m = (x - 2)(x^2 + 1) = x^3 - 2x^2 + x - 2$ has degree 3.

The polynomials e_1, e_2. Here $M_1 = x^2 + 1$ and $M_2 = x - 2$. The identity reads $a_1 M_1 + b_1 m_1 = 1$ with $a_1 = \tfrac{1}{5}$, and $a_2 M_2 + b_2 m_2 = 1$ with $a_2 = -\tfrac{1}{5}(x + 2)$. So

$$e_1 = \tfrac{1}{5}(x^2 + 1), \qquad e_2 = -\tfrac{1}{5}(x + 2)(x - 2) = -\tfrac{1}{5}(x^2 - 4).$$

Assemble and reduce. By Theorem 5.5.5 (a),

$$\begin{aligned} 1 \cdot e_1 + (2x - 1)e_2 &= \tfrac{1}{5}(x^2 + 1 - (2x - 1)(x^2 - 4)) \\ &= \tfrac{1}{5}(-2x^3 + 2x^2 + 8x - 3). \end{aligned}$$

Its remainder on division by m is found by adding $\tfrac{2}{5}m$: since $-2x^3 + 2x^2 + 8x - 3 + 2(x^3 - 2x^2 + x - 2) = -2x^2 + 10x - 7$,

$$f = -\tfrac{2}{5}x^2 + 2x - \tfrac{7}{5},$$

the unique solution of degree less than 3 (Theorem 5.5.5 (c)).

Check. $f(2) = -\tfrac{8}{5} + 4 - \tfrac{7}{5} = 1$, which is the first congruence (Proposition 5.5.6 (b)). Modulo $x^2 + 1$, replace x^2 by -1: $f \equiv \tfrac{2}{5} + 2x - \tfrac{7}{5} = 2x - 1$.

Squares of linear moduli prescribe a value and a derivative at once.

Example. Values and derivatives at once

(a) Let $c, a, b \in F$ and $f \in F[x]$. Show that $f \equiv a + b(x - c) \pmod{(x-c)^2}$ if and only if $f(c) = a$ and $f'(c) = b$ (the formal derivative of Definition 4.5.1).

(b) Find the polynomial $p \in \mathbb{Q}[x]$ of degree at most 3 with $p(0) = 2$, $p'(0) = -1$, $p(1) = 1$ and $p'(1) = 3$.

Solution.

(a) Divide by $(x-c)^2$, which has degree 2: $f = q(x-c)^2 + r$ with $\deg r \leq 1$ (Theorem 5.1.2). Every polynomial of degree at most 1 can be written $\alpha + \beta(x - c)$ with $\alpha, \beta \in F$: if $r = r_0 + r_1 x$, take $\beta := r_1$ and $\alpha := r_0 + r_1 c$. Evaluating at c (Theorem 4.4.1), $f(c) = q(c) \cdot 0 + \alpha = \alpha$. By Theorem 4.5.1 (a)–(c),

$$f' = q'(x-c)^2 + (2 \cdot 1)\, q\, (x - c) + \beta,$$

so $f'(c) = \beta$. Now $f \equiv a + b(x-c)$ if and only if $r \equiv a + b(x-c)$, and both have degree less than 2, so by Theorem 5.5.2 (b) this holds if and only if $\alpha + \beta(x-c) = a + b(x-c)$. Comparing the coefficients of x and then the constant terms, that is $\beta = b$ and $\alpha = a$, that is, $f'(c) = b$ and $f(c) = a$.

(b) By (a), the conditions say $p \equiv 2 - x \pmod{x^2}$ and $p \equiv 1 + 3(x-1) = 3x - 2 \pmod{(x-1)^2}$. The moduli are coprime: expanding,

$$(2x+1)(x-1)^2 + (3-2x)x^2 = (2x^3 - 3x^2 + 1) + (3x^2 - 2x^3) = 1.$$

So, with $m_1 = x^2$ and $m_2 = (x-1)^2$, Theorem 5.5.5 (a) gives $e_1 = 2x^3 - 3x^2 + 1$ and $e_2 = 3x^2 - 2x^3$, and

$$(2 - x)e_1 + (3x - 2)e_2 = -8x^4 + 20x^3 - 12x^2 - x + 2.$$

Adding $8m = 8(x^4 - 2x^3 + x^2)$ gives the remainder modulo $m = x^2(x-1)^2$:

$$p = 4x^3 - 4x^2 - x + 2.$$

Check: $p(0) = 2$; $p' = 12x^2 - 8x - 1$, so $p'(0) = -1$; $p(1) = 4 - 4 - 1 + 2 = 1$; $p'(1) = 12 - 8 - 1 = 3$. By Theorem 5.5.5 (c), p is the only polynomial of degree less than 4 with these four conditions.

This section met the Chinese remainder theorem three times: as interpolation (moduli $x - c_i$), as a value and a derivative at a point (moduli $(x-c)^2$), and in general. In each case the ring $F[x]/\langle m \rangle$ of Theorem 5.5.2 is the place where the computation happens.

5.5.5 Exercises

5.5.5.1 A. Check your understanding

Exercise. A1

(a) Finish the Try it first before Theorem 5.5.1: find the polynomial of degree at most 2 through $(0, 1)$, $(1, 3)$, $(2, 7)$ in $\mathbb{Q}[x]$.

(b) Describe the classes of $F[x]/\langle x\rangle$. Which ring is it, up to renaming?

(c) True or false: $\mathbb{R}[x]/\langle x^2-1\rangle$ is a field. Justify your answer.

(d) Where does the proof of Theorem 5.5.1 (c) use that the nodes are distinct, and where do (a) and (b) use it?

Solution.

(a) With the nodes $0, 1, 2$, Definition 5.5.1 gives

$$\ell_0 = \tfrac{1}{2}(x-1)(x-2), \qquad \ell_1 = -x(x-2), \qquad \ell_2 = \tfrac{1}{2}x(x-1).$$

So $p = \ell_0 + 3\ell_1 + 7\ell_2 = \frac{1}{2}(x^2-3x+2) - 3(x^2-2x) + \frac{7}{2}(x^2-x) = x^2+x+1$. Check: $p(0)=1$, $p(1)=3$, $p(2)=7$. It is the only one of degree at most 2 (Theorem 5.5.1 (c)).

(b) By Theorem 5.5.2 (b) with $d=1$, each class contains exactly one polynomial of degree less than 1, a constant; the constant in $[f]$ is $f(0)$, the remainder on division by $x-0$ (Theorem 5.1.3 (a)). So the classes are the $[c]$, $c \in F$, and they are distinct for distinct c. By Theorem 5.5.2 (c), $c \mapsto [c]$ preserves $+$ and $\cdot$; it is injective, and surjective by what was just said. So $F[x]/\langle x\rangle$ is F with each element c renamed $[c]$; and $[f] = [f(0)]$, so passing to the quotient is "evaluate at 0".

(c) **False.** $x^2-1 = (x-1)(x+1)$ is reducible, so Theorem 5.5.3 says the quotient is not a field. Concretely, $[x-1] \neq [0] \neq [x+1]$ (degree $1 < 2$), while $[x-1][x+1] = [x^2-1] = [0]$.

(d) Part (c) uses distinctness only through Theorem 5.4.2 (a), which needs the $n+1$ points to be distinct, ultimately because the root count of Section 5.4 counts distinct roots. Parts (a) and (b) use it to form the inverses $(c_i - c_j)^{-1}$ in the definition of ℓ_i.

5.5.5.2 B. Practice

Exercise. B1

Find the polynomial $f \in \mathbb{Q}[x]$ of degree less than 4 with $f \equiv 1 \pmod{x^2}$ and $f \equiv -1 \pmod{x^2+1}$.

Solution. The moduli are coprime, since $(x^2+1) - x^2 = 1$ (Corollary 5.2.3), so by Theorem 5.5.5 (c) there is exactly one such f. The first congruence says $f - 1 = x^2 h$ for some $h \in \mathbb{Q}[x]$. Then

$$f + 1 = 2 + x^2 h = (2-h) + h(x^2+1),$$

so the second congruence holds if and only if $x^2+1 \mid 2-h$, that is, $h \equiv 2 \pmod{x^2+1}$. The choice $h=2$ gives $f = 1+2x^2$, of degree $2<4$. Check: $f-1 = 2x^2$ and $f+1 = 2(x^2+1)$. Hence $f = 1+2x^2$.

Exercise. B2

In $\mathbb{Q}[x]/\langle x^3-2\rangle$, show that $[x^2+1]$ is a unit, and compute its inverse.

Solution. Run the Euclidean algorithm (Theorem 5.2.5) on x^3-2 and x^2+1:

$$x^3-2 = x(x^2+1)+(-x-2),$$
$$x^2+1 = (-x+2)(-x-2)+5.$$

The last remainder is the non-zero constant 5, so the gcd is 1. Back-substitute:

$$\begin{aligned} 5 &= (x^2+1)-(-x+2)\big((x^3-2)-x(x^2+1)\big) \\ &= (-x^2+2x+1)(x^2+1)+(x-2)(x^3-2). \end{aligned}$$

Dividing by 5: $\frac{1}{5}(-x^2+2x+1)\cdot(x^2+1)+\frac{1}{5}(x-2)\cdot(x^3-2)=1$. By Theorem 5.5.2 (d), $[x^2+1]$ is a unit and

$$[x^2+1]^{-1} = \left[\tfrac{1}{5}(-x^2+2x+1)\right].$$

Check: $(x^2+1)(-x^2+2x+1) = -x^4+2x^3+2x+1$, and with $x^3\equiv 2$, $x^4\equiv 2x$, this is $\equiv -2x+4+2x+1=5$.

Exercise. B3

(a) Write the addition and multiplication tables of $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$, with its elements named $0, 1, \alpha, \alpha+1$ as in Example (A field with four elements, and the complex numbers again), and check from the table that every non-zero element is a unit.

(b) Show that $\varphi(a+bi) \coloneqq [a+bx]$ $(a,b\in\mathbb{R})$ is a bijection $\mathbb{C}\to\mathbb{R}[x]/\langle x^2+1\rangle$ that preserves $+$ and $\cdot$ and sends 1 to $[1]$.

Solution.

(a) Addition is coefficientwise in $\mathbb{F}_2$, where $1+1=0$:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

The products come from $\alpha^2=\alpha+1$, $\alpha(\alpha+1)=1$, $(\alpha+1)^2=\alpha$ (Example (A field with four elements, and the complex numbers again)). Each non-zero row of the multiplication table contains 1: $1^{-1}=1$, $\alpha^{-1}=\alpha+1$, $(\alpha+1)^{-1}=\alpha$.

(b) Every complex number is $a+bi$ for exactly one pair $(a,b)\in\mathbb{R}^2$ (Proposition 1.1.1 and the comparison of real and imaginary parts after it), and every element of $\mathbb{R}[x]/\langle x^2+1\rangle$ is $[a+bx]$ for exactly one such pair, by Theorem 5.5.2 (b) (the polynomials of degree less than 2 are the $a+bx$, distinct for distinct pairs). So φ is a bijection. Sums: φ of $(a+bi)+(c+di)=(a+c)+(b+d)i$ is $[(a+c)+(b+d)x]=[a+bx]+[c+dx]$. Products: in $\mathbb{R}[x]$,

$$(a+bx)(c+dx) = (ac-bd)+(ad+bc)x+bd(x^2+1),$$

so $[a+bx][c+dx]=[(ac-bd)+(ad+bc)x]$, which is φ of $(a+bi)(c+di)=(ac-bd)+(ad+bc)i$ (Definition 1.1.1, Proposition 1.1.1). Finally $\varphi(1)=[1]$. So the field of Chapter

1 could have been built as this quotient: the multiplication rule of Definition 1.1.1 is "multiply, then replace x^2 by -1".

5.5.5.3 C. Going deeper

Exercise. C1: Two routes to the same theorem

Let $c_0, \dots, c_n \in F$ be distinct and $m := (x - c_0) \cdots (x - c_n)$.

(a) Prove, using Theorem 5.5.1 and the root count but no Bézout identity, that for all $r_0, \dots, r_n \in F[x]$ some f satisfies $f \equiv r_i \pmod{x - c_i}$ for every i, and that g satisfies the same congruences if and only if $g \equiv f \pmod{m}$.

(b) Conversely, derive from Theorem 5.5.5 that for all $y_0, \dots, y_n \in F$ exactly one polynomial of degree at most n satisfies $p(c_k) = y_k$ for every k (the content of Theorem 5.5.1 (b) and (c), without the formula $\sum_i y_i \ell_i$).

(c) Which derivation is shorter, and why?

Solution.

(a) By the second example after Definition 5.5.2, $r_i \equiv r_i(c_i) \pmod{x - c_i}$. Let $f := \sum_i r_i(c_i)\ell_i$. By Theorem 5.5.1 (b), $f(c_i) = r_i(c_i)$, so $f \equiv r_i(c_i) \equiv r_i \pmod{x - c_i}$, by Proposition 5.5.6 (b) and transitivity. If g also satisfies the congruences, then $g - f \equiv 0 \pmod{x - c_i}$ for every i, so each c_i is a root of $g - f$ (Theorem 5.1.3 (b)). The c_i are distinct roots, so $m \mid g - f$ by Theorem 5.4.1. Conversely, if $m \mid g - f$, then each $x - c_i$ divides m (it is an entry of the list whose product is m, (L2) of Section 5.3) and so divides $g - f$ (Proposition 5.1.1 (b)), and $g \equiv f \equiv r_i \pmod{x - c_i}$.

(b) By Proposition 5.5.6 (a), (b), the moduli $x - c_i$ are pairwise coprime, $\deg m = n + 1$, and "$f(c_i) = y_i$ for every i" is the system $f \equiv y_i \pmod{x - c_i}$. By Theorem 5.5.5 (c), exactly one polynomial of degree less than $n + 1$, that is, of degree at most n, solves it. That is the existence of an interpolating polynomial and its uniqueness at once, without the formula for ℓ_i; identifying it with $\sum_i y_i \ell_i$ still needs Theorem 5.5.1 (a).

(c) The route in (a) is shorter in what it needs: evaluation and the root count. The route in (b) passes through Lemma 5.5.4 and Bézout identities for the moduli. The Lagrange route is shorter because linear moduli are special: "divisible by $x - c$" can be tested by evaluating at c, which turns every congruence into an equation in F. For moduli of higher degree, evaluation at a single point is no longer enough. For $(x - c)^2$, Example (Values and derivatives at once) (a) needs the derivative as well as the value. For $x^2 + 1$ over $\mathbb{Q}$ in Example (A linear and a quadratic modulus), the modulus has no root in $\mathbb{Q}$, so no evaluation in $\mathbb{Q}$ detects divisibility at all. The Chinese remainder route handles every modulus in the same way.

Exercise. C2: Every function on a prime field is a polynomial

Let p be a prime. Prove that every function $\varphi\colon \mathbb{F}_p \to \mathbb{F}_p$ is the polynomial function $c \mapsto f(c)$ of **exactly one** $f \in \mathbb{F}_p[x]$ with $\deg f < p$.

Solution. The elements $0, 1, \dots, p-1$ of $\mathbb{F}_p$ are p distinct elements (Definition 2.2.1), and there are no others. Use them as nodes, $c_i := i$ for $i = 0, \dots, p-1$, so $n = p-1$.

Existence. With $y_i := \varphi(i)$, Theorem 5.5.1 (b) gives f with $\deg f \leq p-1 < p$ and $f(i) = \varphi(i)$ for every i. Since the i are all the elements of $\mathbb{F}_p$, the polynomial function of f is φ.

Uniqueness. If g also has degree less than p and the function φ, then f and g have degree at most $p-1$ and agree at the p distinct nodes, so $f = g$ by Theorem 5.5.1 (c).

So over $\mathbb{F}_p$ every function is a polynomial function, and the polynomials of degree less than p correspond one to one to the functions $\mathbb{F}_p \to \mathbb{F}_p$. (As a count: both sets have p^p elements, p choices for each of p coefficients, or for each of p values.) Interpolation over $\mathbb{F}_p$ can use at most p nodes, since $\mathbb{F}_p$ has no more distinct elements. Polynomials of degree p or more are no longer determined by their functions: x^p and x have the same function by Theorem 2.6.6 (a), which is the warning of Section 5.4.

5.6 The Fundamental Theorem of Algebra

Over $\mathbb{Q}$ the polynomial $x^2 - 2$ has no root, and over $\mathbb{R}$ the polynomial $x^2 + 1$ has none. Chapter 1 announced that over $\mathbb{C}$ this stops: every non-constant complex polynomial has a root. This section proves it, and then reads off what it says about factoring complex and real polynomials.

No argument from the field axioms alone can prove the theorem. The field $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ of Example (Rational and Integer Complex Numbers) satisfies every field axiom, and it contains an element i with $i^2 = -1$, just as $\mathbb{C}$ does. Yet $x^2 - 2$ has no root in it. If $(a+bi)^2 = 2$ with $a, b \in \mathbb{Q}$, then comparing real and imaginary parts (Definition 1.1.1), $a^2 - b^2 = 2$ and $2ab = 0$, so $a = 0$ or $b = 0$ ($\mathbb{Q}$ has no zero divisors, Theorem 2.1.1 (f), and $2 \neq 0$). If $b = 0$, then $a^2 = 2$, which no rational satisfies (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1). If $a = 0$, then $-b^2 = 2$, impossible since $-b^2 \leq 0$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)). So the proof must use a property of $\mathbb{R}$ that $\mathbb{Q}$ lacks. It is the supremum property of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 5 (Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3).

The plan has two halves. First, $|p|$ attains a smallest value on $\mathbb{C}$ (Theorem 5.6.3). Second, at any point where p is not 0, some nearby point gives $|p|$ a smaller value (Lemma 5.6.5). So at a point where the smallest value is attained, p must be 0. The first half is where completeness is invoked directly (Steps 2 and 5); the second half uses it only indirectly, through square roots (see the remark after the minimum theorem).

Throughout, p is a polynomial in $\mathbb{C}[x]$, and $p(z)$ is its value at $z \in \mathbb{C}$ (Definition 4.4.1). Inequalities are between real numbers; the modulus $|z|$ is a non-negative real (Definition 1.2.1).

5.6.1 Two estimates

Second reading · *The facts about the modulus used in this section*

All of them are from Chapter 1. For $z, w \in \mathbb{C}$: $|z|^2 = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2$ (Definition 1.2.1); $|\operatorname{Re} z| \leq |z|$, $|\operatorname{Im} z| \leq |z|$ and $|z| \leq |\operatorname{Re} z| + |\operatorname{Im} z|$ (Lemma 1.3.1); $|zw| = |z||w|$, so $|z^j| = |z|^j$ by induction on j, and $|z| = 0$ only for $z = 0$ (Theorem 1.2.2 (d), (e)); $|z_1 + \cdots + z_m| \leq |z_1| + \cdots + |z_m|$

and $|z| - |w| \le |z + w|$ (Corollary 1.3.3 (b), (c)). For a real number the modulus is the absolute value of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 4 (Proposition 1.2.1), so the rules of Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 apply to it.

Three facts about powers of non-negative reals are used as well, each by induction on the exponent with Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (c): if $0 \le a \le b$, then $a^j \le b^j$; if $a \ge 1$ and $i \le j$, then $a^i \le a^j$; if $0 < t \le 1$ and $i \le j$, then $t^j \le t^i$.

The first estimate says that $|p(z)|$ is large when $|z|$ is large, so the search for a smallest value can be confined to a bounded region.

Lemma 5.6.1. Growth of a Complex Polynomial

Let $p = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x]$ with $n = \deg p \ge 1$, so $a_n \ne 0$. Let

$$A := |a_0| + \cdots + |a_{n-1}|, \qquad R := \max\Big\{1, \frac{2A}{|a_n|}\Big\}.$$

Then for every $z \in \mathbb{C}$ with $|z| \ge R$,

$$|p(z)| \ge \tfrac{1}{2}|a_n||z|^n \ge \tfrac{1}{2}|a_n||z|.$$

In words: beyond the radius R, the top term outweighs all the others together, at least by half.

↻ **Second reading** · *The proof: the top term against the rest*

Proof. Let $|z| \ge R$. Then $|z| \ge 1$, so $|z|^j \le |z|^{n-1}$ for $0 \le j \le n-1$. Write $p(z) = a_n z^n + w$ with $w := \sum_{j=0}^{n-1} a_j z^j$ (the sum recursion). By Corollary 1.3.3 (b) and Theorem 1.2.2 (d),

$$|w| \le \sum_{j=0}^{n-1} |a_j||z|^j \le A|z|^{n-1}.$$

By Corollary 1.3.3 (c), which is the reverse triangle inequality (a) with the second number negated, $|p(z)| \ge |a_n||z|^n - |w| \ge |z|^{n-1}(|a_n||z| - A)$. Since $|z| \ge 2A/|a_n|$ and $|a_n| > 0$, $A \le \frac{1}{2}|a_n||z|$, so $|a_n||z| - A \ge \frac{1}{2}|a_n||z|$. Hence $|p(z)| \ge \frac{1}{2}|a_n||z|^n$. Finally $|z|^n \ge |z|$, since $|z| \ge 1$ and $n \ge 1$.

■

The second estimate replaces continuity, which this volume does not have. It bounds how much p can change between two points of a bounded region, with an explicit constant.

Lemma 5.6.2. A Lipschitz Bound for a Complex Polynomial

Let $p = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x]$ and let $M \in \mathbb{R}$ with $M \geq 0$. Put

$$L := \sum_{j=1}^{n} j|a_j| M^{j-1} \qquad (j|a_j| \text{ the multiple } (j \cdot 1)|a_j| \text{ in } \mathbb{R}).$$

Then $|p(z) - p(w)| \leq L|z - w|$ for all $z, w \in \mathbb{C}$ with $|z| \leq M$ and $|w| \leq M$.

In words: on the disc of radius M, p moves at most L times as far as its argument.

↻ **Second reading** · *The proof: factor each difference of powers*

Proof. Let $|z|, |w| \leq M$. Termwise (the sum rules (Σ1), (Σ2), (Σ4) of Lemma 4.1.1), $p(z) - p(w) = \sum_{j=0}^{n} a_j (z^j - w^j)$, and the term $j = 0$ is 0. For $j \geq 1$, Lemma 1.1.4 gives

$$z^j - w^j = (z - w) \sum_{i=0}^{j-1} z^i w^{j-1-i}.$$

Each of the j terms of the sum has modulus $|z|^i |w|^{j-1-i} \leq M^i M^{j-1-i} = M^{j-1}$. So $|z^j - w^j| \leq jM^{j-1}|z - w|$ by Corollary 1.3.3 (b), and summing over j with the same corollary, $|p(z) - p(w)| \leq \sum_{j=1}^{n} |a_j|\, jM^{j-1}|z - w| = L|z - w|$.

■

This is the only "continuity" the proof below needs, and it comes with a constant that can be computed.

Quick check. For $p = x^2 + 1$, compute A and R of Lemma 5.6.1, and the constant L of Lemma 5.6.2 for $M = 4$.

Solution. Here $a_0 = 1$, $a_1 = 0$, $a_2 = 1$, $n = 2$. So $A = |1| + |0| = 1$ and $R = \max\{1, 2 \cdot 1/1\} = 2$. For $M = 4$, $L = 1 \cdot 0 \cdot 4^0 + 2 \cdot 1 \cdot 4^1 = 8$. (Check of the Lipschitz bound in one case: $|p(z) - p(w)| = |z^2 - w^2| = |z + w||z - w| \leq 8|z - w|$ when $|z|, |w| \leq 4$.)

5.6.2 The smallest value of the modulus is attained

We now look for a point where $|p|$ is smallest. The infimum of the values $|p(z)|$ exists by completeness; the work is to find a point **at** which it is attained. We trap such a point in smaller and smaller squares.

For $\sigma, \tau \in \mathbb{R}$ and $s \in \mathbb{R}$ with $s > 0$, let

$$S(\sigma, \tau, s) := \{z \in \mathbb{C} : \sigma \leq \operatorname{Re} z \leq \sigma + s,\ \tau \leq \operatorname{Im} z \leq \tau + s\},$$

the closed square with lower-left corner $\sigma + \tau i$ and side s. (In this section σ and τ are real numbers. Chapter 3 uses the same letters for permutations, which do not appear here.) Each such square contains its corner, so it is non-empty. Its four **quarters**, in this fixed order, are

$$\begin{aligned} &S(\sigma, \tau, s/2), && S(\sigma + s/2, \tau, s/2), \\ &S(\sigma, \tau + s/2, s/2), && S(\sigma + s/2, \tau + s/2, s/2). \end{aligned}$$

Each quarter lies in the square, and every point of the square lies in some quarter: $\operatorname{Re} z \leq \sigma + s/2$ or $\operatorname{Re} z \geq \sigma + s/2$, and likewise for $\operatorname{Im} z$, since $\leq$ is a total order on $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (i)).

Theorem 5.6.3. The Modulus of a Complex Polynomial Attains Its Minimum

For every $p \in \mathbb{C}[x]$ there is $z^* \in \mathbb{C}$ with $|p(z^*)| \leq |p(z)|$ for **every** $z \in \mathbb{C}$.

Idea. Confine the search to one big square S_0 by the growth lemma. The infimum m of $|p|$ over S_0 exists. Cut S_0 into four quarters: the infimum over S_0 is the least of the four infima, so some quarter has the **same** infimum m; keep the first such quarter, and repeat. We call this move **keep the quarter that keeps the infimum**. The squares shrink to a single point z^*, which completeness supplies as a supremum of corners. Near z^* every square still has points where $|p|$ is almost m, and the Lipschitz bound says $|p(z^*)|$ is almost the same; so $|p(z^*)| = m$. This is the bisection of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 5, now in the plane. *Before reading on: why keep a quarter whose* ***infimum*** *equals the square's, rather than a quarter containing a point where* $|p|$ *is smallest?*

Proof. If p is a constant a_0 (including 0), then $p(z) = a_0$ for every z, and $z^* := 0$ works. Let $n := \deg p \geq 1$, with leading coefficient $a_n \neq 0$, let R be as in Lemma 5.6.1, and let

$$\rho := \max\Big\{R, \frac{2|p(0)|}{|a_n|}\Big\},$$

so $\rho \geq 1$.

Step 1 (a square that suffices). Let $S_0 := S(-\rho, -\rho, 2\rho)$. It contains 0. If $z \notin S_0$, then $|\operatorname{Re} z| > \rho$ or $|\operatorname{Im} z| > \rho$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 4.1.3 (d)), so $|z| > \rho \geq R$ (Lemma 1.3.1), and by Lemma 5.6.1,

$$|p(z)| \geq \tfrac{1}{2}|a_n||z| > \tfrac{1}{2}|a_n|\rho \geq |p(0)|. \tag{1}$$

Step 2 (the infimum; completeness, first use). For a square S, the set $V(S) := \{|p(z)| : z \in S\} \subseteq \mathbb{R}$ is non-empty and bounded below by 0. So it has an infimum $m(S)$ in $\mathbb{R}$ (Sets, Relations, and Cardinality, Definition 2.6.5); the fold after the proof derives this from the supremum property. Two consequences are used: $m(S) \leq |p(z)|$ for every $z \in S$; and for every $\varepsilon > 0$ there is $z \in S$ with $|p(z)| < m(S) + \varepsilon$, since otherwise $m(S) + \varepsilon$ would be a lower bound of $V(S)$ larger than the greatest one. If $S' \subseteq S$, then $m(S)$ is a lower bound of $V(S') \subseteq V(S)$, so $m(S) \leq m(S')$.

Step 3 (a quarter with the same infimum). Let S be a square and $Q_1, \ldots, Q_4$ its quarters. Each $m(Q_i) \geq m(S)$ by Step 2. Let μ be the least of the four numbers $m(Q_i)$. Every $z \in S$ lies in some Q_i, so $|p(z)| \geq m(Q_i) \geq \mu$: μ is a lower bound of $V(S)$, hence

$\mu \le m(S)$. So $\mu = m(S)$, and some quarter has $m(Q_i) = m(S)$. Let $q(S)$ be the **first** quarter, in the fixed order, with $m(Q_i) = m(S)$. This is a rule: q is a function from squares to squares.

Step 4 (the nested squares). Identify the square $S(\sigma, \tau, s)$ with the triple (σ, τ, s). By Sets, Relations, and Cardinality, Theorem 2.3.1 (read on $\mathbb{N} = \omega$ through Number Systems: From \(\nN\) to \(\nR\), Corollary 1.7.3), there is exactly one sequence of squares $S_k = S(\sigma_k, \tau_k, s_k)$, $k \in \mathbb{N}$, with S_0 as in Step 1 and $S_{k+1} = q(S_k)$. By induction on k:

- $s_k = 2\rho/2^k$, the power 2^k taken in $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Definition 4.2.1), since each quarter has half the side;
- $m(S_k) = m$, where $m := m(S_0)$, by the choice of q;
- $\sigma_k \le \sigma_{k'} \le \sigma_k + s_k - s_{k'}$ and $\tau_k \le \tau_{k'} \le \tau_k + s_k - s_{k'}$ for all $k' \ge k$, since the corner of a quarter is σ or $\sigma + s/2$ and its far edge $\sigma + s/2$ or $\sigma + s$. In particular $S_{k'} \subseteq S_k \subseteq S_0$.

Step 5 (the common point; completeness, second use). The set $\{\sigma_k : k \in \mathbb{N}\}$ is non-empty and bounded above by $\sigma_0 + s_0$ (Step 4 with $k = 0$). By Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3 it has a supremum σ^* (Number Systems: From \(\nN\) to \(\nR\), Definition 5.6.1). Fix k. Then $\sigma_k \le \sigma^*$, and $\sigma_k + s_k$ is an upper bound of the set: for $k' \ge k$, $\sigma_{k'} \le \sigma_k + s_k$ by Step 4, and for $k' < k$, $\sigma_{k'} \le \sigma_k$ by Step 4 with the roles of k and k' exchanged. So $\sigma_k \le \sigma^* \le \sigma_k + s_k$ for every k. In the same way $\tau^* := \sup\{\tau_k : k \in \mathbb{N}\}$ satisfies $\tau_k \le \tau^* \le \tau_k + s_k$. Hence $z^* := \sigma^* + \tau^* i$ lies in every S_k.

Step 6 (the value at the common point). For $z, w \in S_k$, $|\mathrm{Re}(z - w)| \le s_k$ and $|\mathrm{Im}(z - w)| \le s_k$, so $|z - w| \le 2s_k$ (Lemma 1.3.1). Every point of S_0 has modulus at most $\rho + \rho = 2\rho$, by the same lemma. Let L be the constant of Lemma 5.6.2 for $M = 2\rho$.

Let $\varepsilon \in \mathbb{R}$ with $\varepsilon > 0$. By Number Systems: From \(\nN\) to \(\nR\), Theorem 5.4.2 there is $k \in \mathbb{N}$ with $k > 8\rho L/\varepsilon$; then $2^k \ge k + 1 > 8\rho L/\varepsilon$ by Number Systems: From \(\nN\) to \(\nR\), Lemma 5.6.1, so

$$2s_k L = \frac{4\rho L}{2^k} < \frac{\varepsilon}{2}. \tag{2}$$

This k depends on ε (and on p, through ρ and L). Since $m(S_k) = m$, Step 2 gives a point $w \in S_k$ with $|p(w)| < m + \varepsilon/2$ ($\exists$E: the point w is used only inside this argument for this ε). Both z^* and w lie in $S_k \subseteq S_0$, so by the triangle inequality (Theorem 1.3.2), the Lipschitz bound and (2),

$$|p(z^*)| \le |p(w)| + |p(z^*) - p(w)| < m + \frac{\varepsilon}{2} + L \cdot 2s_k < m + \varepsilon.$$

As $\varepsilon > 0$ was arbitrary, $|p(z^*)| \le m$: otherwise $\varepsilon := |p(z^*)| - m > 0$ would give $|p(z^*)| < |p(z^*)|$. Also $|p(z^*)| \ge m$, since $z^* \in S_0$. So $|p(z^*)| = m$.

Step 7 (the minimum over all of the plane). Let $z \in \mathbb{C}$. If $z \in S_0$, then $|p(z)| \ge m = |p(z^*)|$. If $z \notin S_0$, then $|p(z)| > |p(0)| \ge m$ by (1), since $0 \in S_0$. This proves the theorem.

■

↻ **Second reading** · *Step 2: why the infimum exists*

Let $V \subseteq \mathbb{R}$ be non-empty and bounded below by 0, and let B be the set of lower bounds of V. Then $0 \in B$, and every element of V is an upper bound of B, so B is non-empty and bounded above; by Number Systems: From \(\nN\) to \(\nR\), Theorem 5.6.3 it has a supremum m

(Number Systems: From \(\nN\) to \(\nR\), Definition 5.6.1). Each $v \in V$ is an upper bound of B, so $m \leq v$: m is a lower bound of V. Each lower bound u of V is in B, so $u \leq m$. Thus m is the greatest lower bound of V, its infimum in the sense of Sets, Relations, and Cardinality, Definition 2.6.5.

The answer to the prompt. A quarter containing a point where $|p|$ is smallest is what the theorem is trying to prove exists, so it cannot be used to choose quarters. The infimum of a quarter always exists, by completeness, and Step 3 shows that some quarter keeps it. Choosing "the first such quarter in a fixed order" makes the step a rule, so the recursion theorem applies and no choice is made at any stage; compare Number Systems: From \(\nN\) to \(\nR\), Example (Picking Representatives Is a Use of Choice), where a proof that picks infinitely many objects without a rule uses the axiom of choice.

Remark. The supremum property is invoked directly in Steps 2 and 5 and nowhere else in this chapter. It also enters indirectly, through the non-negative real square roots of Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4, which that result derives from the supremum: they give the modulus used in every inequality of this section, and the complex square roots of Proposition 1.4.1 used in the next lemma. In $\mathbb{Q}(i)$, with $\mathbb{Q}$ in place of $\mathbb{R}$, both fail; Exercise C1 (c) asks where.

Quick check. In Step 3, why does it matter that there are only **four** quarters?

Solution. The proof takes μ, the least of the numbers $m(Q_1), \ldots, m(Q_4)$. A finite list of real numbers has a least element, so μ exists and equals one of them; that is what produces a quarter with $m(Q_i) = m(S)$. With infinitely many pieces, the infimum of their infima need not be attained by any one piece.

5.6.3 A direction in which the modulus decreases

The second half of the plan is algebra, together with complex square roots (Proposition 1.4.1). Near a point z_0, write $p(z_0 + h) = b_0 + b_k h^k +$ (higher powers of h), with $b_0 = p(z_0)$. If we can choose the direction of h so that $b_k h^k$ points back toward 0 from b_0, and h so small that the higher terms do not undo the gain, then $|p|$ decreases. Dividing by b_0, the first need is a ζ for which $c\zeta^k$ has negative real part.

Lemma 5.6.4. A Direction with Negative Real Part

Let $c \in \mathbb{C}$ with $c \neq 0$, and let $k \in \mathbb{N}$ with $k \geq 1$. Then there is $\zeta \in \mathbb{C}$ with $\mathrm{Re}(c\zeta^k) < 0$.

Try it first (ten minutes): for $c = i$, find ζ with $\mathrm{Re}(c\zeta^3) < 0$. Then find ζ with $\mathrm{Re}(c\zeta^2) < 0$.

Idea. For $k = 3$, the four "axis" directions $\zeta \in \{1, -1, i, -i\}$ already turn c around: ζ^3 runs through $1, -1, -i, i$, and $i \cdot i = -1$. For $k = 2$ they do not: $\zeta^2 \in \{1, -1\}$ for these four, and $c\zeta^2 \in \{i, -i\}$ has real part 0. What works for $k = 2$ is a square root of a direction that works

for $k = 1$: $\eta = i$ gives $\mathrm{Re}(i \cdot i) = -1$, and if $\zeta^2 = \eta$, then $c\zeta^2 = c\eta$. So odd k is handled by the axes, and even $k = 2j$ by a square root of a direction for j, which is strong induction. Square roots of complex numbers come from real square roots (Proposition 1.4.1), so no polar form is needed.

Second reading · *The proof: the axes for odd k, a square root for even k*

Proof. We prove, by strong induction on k (Logic and Proof, Theorem 4.2.2, on $\mathbb{N} = \omega$), the statement: if $k \geq 1$, then for every non-zero $c \in \mathbb{C}$ there is ζ with $\mathrm{Re}(c\zeta^k) < 0$. For $k = 0$ there is nothing to prove. Let $k \geq 1$, assume the statement for every smaller exponent, and let $c \neq 0$. By Number Systems: From \(\nN\) to \(\nR\), Proposition 1.6.4 (d), $k = 2j + 1$ or $k = 2j$ for some $j \in \mathbb{N}$.

Case 1: k odd, $k = 2j + 1$. Since $i^2 = -1$, the power laws (Proposition 1.1.3 (a)–(c)) give $i^k = (i^2)^j i = (-1)^j i \in \{i, -i\}$, $(-1)^k = -1$ and $(-i)^k = (-1)^k i^k = -i^k$. So as ζ runs through $1, -1, i, -i$, the products $c\zeta^k$ run through $c, -c$ and $ic, -ic$ (in some order). If $\mathrm{Re}\, c \neq 0$, one of $\mathrm{Re}\, c$ and $\mathrm{Re}(-c) = -\mathrm{Re}\, c$ is negative. If $\mathrm{Re}\, c = 0$, then $c = bi$ with $b := \mathrm{Im}\, c \neq 0$, and $ic = -b$, $-ic = b$: one of them has negative real part.

Case 2: k even, $k = 2j$ with $1 \leq j < k$. By the induction hypothesis for j, there is η with $\mathrm{Re}(c\eta^j) < 0$. Then $\eta \neq 0$, since otherwise $c\eta^j = 0$. By Proposition 1.4.1 there is ζ with $\zeta^2 = \eta$, and $\zeta^k = (\zeta^2)^j = \eta^j$ (Proposition 1.1.3 (b)). So $\mathrm{Re}(c\zeta^k) = \mathrm{Re}(c\eta^j) < 0$. This proves the lemma.

■

With polar form one would take ζ to be a k-th root of $-\overline{c}/|c|$. This volume's k-th roots of complex numbers (Theorem 1.6.2) rest on the cosine and sine of Axiom 1.5.2, which it borrows from analysis. The proof above uses only the complex square roots of Proposition 1.4.1, which Section 1.4 builds from the real square roots of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4).

Quick check. For $c = i$ and $k = 1$, which $\zeta \in \{1, -1, i, -i\}$ gives $\mathrm{Re}(c\zeta) < 0$?

Solution. $\zeta = i$: $c\zeta = i \cdot i = -1$, with real part $-1 < 0$. The others give i, $-i$ and $-i \cdot i = 1$, with real parts $0, 0, 1$.

Now the descent itself. Re-centering at z_0 is Theorem 5.4.3 of Section 5.4.

Lemma 5.6.5. d'Alembert's Lemma

Let $p \in \mathbb{C}[x]$ be non-constant, and let $z_0 \in \mathbb{C}$ with $p(z_0) \neq 0$. Then there is $z \in \mathbb{C}$ with $|p(z)| < |p(z_0)|$.

Idea. Expand around z_0: $p(z_0+h) = b_0(1+(b_k/b_0)h^k+\dots)$, where k is the first index $j \geq 1$ with $b_j \neq 0$. With $h = t\zeta$, $t > 0$ real and ζ from the previous lemma, the bracket is $1 + t^k u + E$ with $\operatorname{Re} u < 0$. For small $s > 0$, $|1+su|$ is about $1 - s\alpha$ with $\alpha = -\operatorname{Re} u$, and E is of order t^{k+1}, smaller than the gain $t^k\alpha$. The proof fixes t first and then checks the inequality. *Before reading on: where is k, the first index with $b_k \neq 0$, used?*

Proof. Let $n := \deg p \geq 1$. By Theorem 5.4.3 there are $b_0, \dots, b_n \in \mathbb{C}$ with $p = \sum_{j=0}^{n} b_j(x - z_0)^j$, $b_0 = p(z_0) \neq 0$ and $b_n \neq 0$ (the leading coefficient of p). So the set of $j \in \{1, \dots, n\}$ with $b_j \neq 0$ contains n, and it has a least element k (Sets, Relations, and Cardinality, Theorem 2.1.3): $k \geq 1$, $b_k \neq 0$, and $b_j = 0$ for $1 \leq j < k$.

Let $c := b_k/b_0 \neq 0$. By Lemma 5.6.4 there is ζ with $\operatorname{Re}(c\zeta^k) < 0$. Put

$$u := c\zeta^k, \qquad \alpha := -\operatorname{Re} u > 0, \qquad B := \sum_{j=k+1}^{n} \left|\frac{b_j}{b_0}\right| |\zeta|^j \geq 0.$$

Then $\alpha \leq |u|$ (Lemma 1.3.1), so $|u| > 0$. Choose

$$t := \min\Big\{1, \frac{\alpha}{|u|^2}, \frac{\alpha}{4B}\Big\} \qquad \text{(the last entry omitted if } B = 0\text{)},$$

a real number with $0 < t \leq 1$. It depends only on p, z_0 and ζ. We show that $z := z_0 + t\zeta$ works.

The expansion. By Theorem 5.4.3 (c) with $h = t\zeta$, and since $b_j = 0$ for $1 \leq j < k$,

$$p(z_0 + t\zeta) = b_0 + b_k t^k \zeta^k + \sum_{j=k+1}^{n} b_j t^j \zeta^j = b_0(1 + t^k u + E),$$

where $E := \sum_{j=k+1}^{n} (b_j/b_0) t^j \zeta^j$. Since $0 < t \leq 1$, $t^j \leq t^{k+1}$ for $j \geq k+1$, so $|E| \leq t^{k+1} B$ (Corollary 1.3.3 (b)).

The main term. Let $s \in \mathbb{R}$ with $0 < s \leq \alpha/|u|^2$. Since $1 + su$ has real part $1 - s\alpha$ and imaginary part $s \operatorname{Im} u$,

$$|1+su|^2 = (1-s\alpha)^2 + s^2(\operatorname{Im} u)^2 = 1 - 2s\alpha + s^2|u|^2 \leq 1 - s\alpha,$$

where the last step uses $s|u|^2 \leq \alpha$. Also $(1 - s\alpha/2)^2 = 1 - s\alpha + s^2\alpha^2/4 \geq 1 - s\alpha$, and $1 - s\alpha/2 > 0$ because $s\alpha \leq \alpha^2/|u|^2 \leq 1$. Two non-negative reals whose squares are in the order $|1+su|^2 \leq (1 - s\alpha/2)^2$ are in the same order (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g)), so

$$|1 + su| \leq 1 - \frac{s\alpha}{2}. \tag{3}$$

The choice of t at work. Let $s := t^k$. Then $0 < s \leq t \leq \alpha/|u|^2$, so (3) applies; and $tB \leq \alpha/4$.

Hence, by Theorem 1.2.2 (d) and the triangle inequality,

$$|p(z_0+t\zeta)| \le |b_0|(|1+t^k u|+|E|) \le |b_0|\Big(1-\frac{t^k\alpha}{2}+t^k\cdot tB\Big)$$
$$\le |b_0|\Big(1-\frac{t^k\alpha}{4}\Big) < |b_0| = |p(z_0)|,$$

the last step because $|b_0|>0$ and $t^k\alpha>0$. This proves the lemma.

■

Where k is used. The index k is the first non-zero coefficient after b_0, so the expansion has no terms between b_0 and $b_k t^k\zeta^k$. A term $b_j t^j\zeta^j$ with $1\le j<k$ would be of order t^j, larger than the gain $t^k\alpha$ for small t, and in an uncontrolled direction. And the direction lemma is applied with this exponent k.

Example. One step of descent

Run the proof of Lemma 5.6.5 for $p=x^3+x^2+1$ at $z_0=0$, and compare with moving along the real axis.

Solution. Here the expansion around 0 is p itself: $b_0=1$, $b_1=0$, $b_2=1$, $b_3=1$. So $k=2$ and $c=b_2/b_0=1$.

The direction. The proof of Lemma 5.6.4 for $k=2=2\cdot 1$ first finds a direction for $j=1$: since $\operatorname{Re} c=1\neq 0$, $\eta=-1$ works, with $\operatorname{Re}(c\eta)=-1$. Then it takes a square root of $\eta=-1$; the formula of Proposition 1.4.1 (with $a=-1$, $b=0$, $r=1$) gives $\zeta=0+1\cdot i=i$.

The constants. $u=c\zeta^2=-1$, $\alpha=1$, $|u|^2=1$, $B=|b_3/b_0||\zeta|^3=1$, so $t=\min\{1,1,1/4\}=1/4$.

The new point. $z=i/4$, and

$$p(i/4)=-\frac{i}{64}-\frac{1}{16}+1=\frac{15}{16}-\frac{i}{64},\qquad |p(i/4)|^2=\frac{225}{256}+\frac{1}{4096}=\frac{3601}{4096}<1.$$

The proof's bound is $1-t^2\alpha/4=63/64$, and indeed $3601/4096\le(63/64)^2=3969/4096$.

The real axis. $p(1/4)=1/64+1/16+1=69/64>1$. Moving from 0 to the right increases $|p|$; the direction $\zeta=i$ chosen by the lemma decreases it. The direction matters.

5.6.4 The theorem, and complex polynomials

Theorem 5.6.6. Fundamental Theorem of Algebra

Every non-constant $p\in\mathbb{C}[x]$ has a root in $\mathbb{C}$.

Proof. By Theorem 5.6.3 there is $z^*\in\mathbb{C}$ with $|p(z^*)|\le|p(z)|$ for every $z\in\mathbb{C}$. Suppose $p(z^*)\neq 0$. By Lemma 5.6.5, applied at $z_0=z^*$, some z has $|p(z)|<|p(z^*)|$, a contradiction. So $p(z^*)=0$.

■

Chapter 1 announced the theorem for expressions $\sum_{k=0}^{n} a_k z^k$ with $a_n \neq 0$ and $n \geq 1$. Such an expression is the value at z of the non-constant polynomial $\sum_{k=0}^{n} a_k x^k$ (Definition 4.4.1), so every complex polynomial expression of positive degree has a root.

Corollary 5.6.7. Complex Polynomials Split

(a) Every non-zero $p \in \mathbb{C}[x]$ splits over $\mathbb{C}$ (Definition 5.4.2): $p = a(x - z_1) \cdots (x - z_n)$ with $n = \deg p$, a the leading coefficient of p, and $z_1, \ldots, z_n \in \mathbb{C}$. The multiplicities of the roots of p add up to n.

(b) The irreducible polynomials of $\mathbb{C}[x]$ are exactly those of degree 1.

Proof.

(a) Let $c_1, \ldots, c_k$ be the distinct roots of p in $\mathbb{C}$, with multiplicities $m_1, \ldots, m_k$. By Theorem 5.4.6, $p = (x - c_1)^{m_1} \cdots (x - c_k)^{m_k} g$ with $g \in \mathbb{C}[x]$ having no root in $\mathbb{C}$. Then $g \neq 0$, since $p \neq 0$, and g is constant, since a non-constant g would have a root by Theorem 5.6.6. A product of monic polynomials is monic (Theorem 4.3.2 (b)), so comparing leading coefficients, $g = a$; and comparing degrees, $\deg p = m_1 + \cdots + m_k$. Writing each power $(x - c_i)^{m_i}$ as the product of m_i factors $x - c_i$ gives the displayed form.

(b) A polynomial of degree 1 is irreducible (the examples after Definition 5.3.1). Conversely, let p be irreducible over $\mathbb{C}$. Then $\deg p \geq 1$, so p has a root c (Theorem 5.6.6), and $p = (x - c)h$ by Theorem 5.1.3 (b). Since $x - c$ is not constant, h is a non-zero constant, and $\deg p = 1$.

■

Example. Factoring a quartic over the reals and over the complex numbers

Factor $x^4 + 1$ into linear factors over $\mathbb{C}$, and into irreducible factors over $\mathbb{R}$.

Solution. *Over* $\mathbb{C}$. Since $i^2 = -1$, $x^4 + 1 = x^4 - i^2 = (x^2 - i)(x^2 + i)$. The formula of Proposition 1.4.1 gives the square roots: for i ($a = 0$, $b = 1$, $r = 1$), $w_1 := \frac{\sqrt{2}}{2}(1 + i)$; for $-i$ ($b = -1$), $w_2 := \frac{\sqrt{2}}{2}(1 - i)$. Here $\sqrt{1/2} = \sqrt{2}/2$, since $\sqrt{2}/2 \geq 0$ and $(\sqrt{2}/2)^2 = 1/2$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4). Since $w_1^2 = i$ and $w_2^2 = -i$ (Proposition 1.4.1 (a)), expanding gives $x^2 - i = x^2 - w_1^2 = (x - w_1)(x + w_1)$ and $x^2 + i = x^2 - w_2^2 = (x - w_2)(x + w_2)$, so

$$x^4 + 1 = (x - w_1)(x + w_1)(x - w_2)(x + w_2).$$

Over $\mathbb{R}$. Note $w_2 = \overline{w_1}$ and $-w_2 = \overline{-w_1}$. Pair each root with its conjugate:

$$(x - w_1)(x - \overline{w_1}) = x^2 - \sqrt{2}\,x + 1, \qquad (x + w_1)(x + \overline{w_1}) = x^2 + \sqrt{2}\,x + 1,$$

since $w_1 + \overline{w_1} = 2\operatorname{Re} w_1 = \sqrt{2}$ and $w_1\overline{w_1} = |w_1|^2 = \frac{1}{2} + \frac{1}{2} = 1$ (Theorem 1.2.2 (c)). So

$$x^4 + 1 = (x^2 + \sqrt{2}\,x + 1)(x^2 - \sqrt{2}\,x + 1),$$

which can be checked directly: the right side is $(x^2+1)^2 - 2x^2 = x^4 + 1$. Neither quadratic has a real root, since for every $c \in \mathbb{R}$, $c^2 \pm \sqrt{2}\,c + 1 = (c \pm \frac{\sqrt{2}}{2})^2 + \frac{1}{2} > 0$; so both are irreducible over $\mathbb{R}$ (Proposition 5.3.1 (b)). No polar form was used: only the square roots of $\pm i$.

Quick check. Factor $x^3 - 1$ over $\mathbb{R}$ and over $\mathbb{C}$.

Solution. $x^3 - 1 = (x-1)(x^2 + x + 1)$ (Lemma 1.1.4, or expand). The quadratic has no real root, since for every $c \in \mathbb{R}$, $c^2 + c + 1 = (c + \frac{1}{2})^2 + \frac{3}{4} > 0$, so this is the factorization over $\mathbb{R}$ (Proposition 5.3.1 (b)). Over $\mathbb{C}$: a square root of -3 is $i\sqrt{3}$, and $z_\pm := (-1 \pm i\sqrt{3})/2$ satisfy $z^2 + z + 1 = 0$ (expand: $z_\pm^2 = (-1 \mp i\sqrt{3})/2$, and $z_\pm^2 + z_\pm + 1 = -1 + 1 = 0$). They are distinct roots, so $(x - z_+)(x - z_-) \mid x^2 + x + 1$ (Theorem 5.4.1); both are monic of degree 2, so they are equal, and $x^3 - 1 = (x-1)(x - z_+)(x - z_-)$.

5.6.5 Real polynomials

A real polynomial is also a complex one, so it splits over $\mathbb{C}$. The question is what that says over $\mathbb{R}$. The answer comes from conjugation: the non-real roots of a real polynomial come in conjugate pairs, and each pair makes a real quadratic factor.

For $f = \sum_k f_k x^k \in \mathbb{C}[x]$, write $\bar{f} := \sum_k \overline{f_k}\, x^k$, the polynomial with conjugated coefficients. A polynomial in $\mathbb{R}[x]$ is one in $\mathbb{C}[x]$ whose coefficients are real ($\mathbb{R} \subseteq \mathbb{C}$, Proposition 1.1.1).

Proposition 5.6.8. Conjugate Roots of Real Polynomials

(a) The map $\mathbb{C}[x] \to \mathbb{C}[x]$, $f \mapsto \bar{f}$, is a ring homomorphism (Definition 4.4.2), and $\overline{f(z)} = \bar{f}(\overline{z})$ for every $f \in \mathbb{C}[x]$ and $z \in \mathbb{C}$.

(b) Let $f \in \mathbb{R}[x]$, $f \neq 0$, and $z \in \mathbb{C}$. Then z is a root of f if and only if $\overline{z}$ is, and $\operatorname{mult}_{\overline{z}}(f) = \operatorname{mult}_z(f)$.

Idea. Conjugating every coefficient is a substitution homomorphism, so it respects sums, products and powers, and it commutes with evaluation once the point is conjugated too. A real polynomial is its own conjugate; so conjugating a root, or a factorization $(x - z)^m g$, gives a root, or a factorization $(x - \overline{z})^m \bar{g}$, of the same polynomial.

Proof.

(a) Conjugation $\mathbb{C} \to \mathbb{C}$ preserves $+$ and $\cdot$ (Theorem 1.2.2 (a), (b)) and sends 1 to 1, so it is a ring homomorphism (see also Example (Conjugation and Other Automorphisms)); followed by the constants $\mathbb{C} \to \mathbb{C}[x]$ (Theorem 4.2.4 (b)) it is a ring homomorphism $\varphi\colon \mathbb{C} \to \mathbb{C}[x]$, a composite of two. By Theorem 4.4.2 with $R = \mathbb{C}$, $S = \mathbb{C}[x]$ and

$s = x$, the map $f \mapsto \sum_k \varphi(f_k)x^k = \bar{f}$ is a ring homomorphism. For the values, $\overline{z^k} = \overline{z}^k$ by induction with Theorem 1.2.2 (b), and then, through the sum recursion with Theorem 1.2.2 (a), (b),

$$\overline{f(z)} = \overline{\sum_k f_k z^k} = \sum_k \overline{f_k}\,\overline{z}^k = \bar{f}(\overline{z}).$$

For real coefficients this is the computation of Proposition 1.6.4.

(b) The coefficients of f are real, so $\bar{f} = f$ (Proposition 1.2.1: $\overline{a} = a$ for $a \in \mathbb{R}$). By (a), $f(\overline{z}) = \bar{f}(\overline{z}) = \overline{f(z)}$, and $\overline{w} = 0$ if and only if $w = 0$ ($\overline{0} = 0$ by Definition 1.2.1, and conversely $w = \overline{\overline{w}}$ by Theorem 1.2.2 (a)); so z is a root exactly when $\overline{z}$ is. Let $m := \operatorname{mult}_z(f)$. By Lemma 5.4.4 (a), $f = (x - z)^m g$ with $g(z) \neq 0$. Apply the homomorphism of (a): $f = \bar{f} = (x - \overline{z})^m \bar{g}$, and $\bar{g}(\overline{z}) = \overline{g(z)} \neq 0$. By Lemma 5.4.4 (a) again, $\operatorname{mult}_{\overline{z}}(f) = m$.

■

Quick check. The number $2 + i$ is a root of $x^2 - 4x + 5 \in \mathbb{R}[x]$. Name the other root without computing, and factor the polynomial over $\mathbb{C}$.

Solution. By Proposition 5.6.8 (b), $\overline{2 + i} = 2 - i$ is a root. The two roots are distinct, so $(x - 2 - i)(x - 2 + i)$ divides the polynomial (Theorem 5.4.1); both are monic of degree 2, so $x^2 - 4x + 5 = (x - 2 - i)(x - 2 + i)$. (Check: the product is $(x - 2)^2 + 1$.)

Corollary 5.6.9. The Irreducible Real Polynomials

A polynomial $p \in \mathbb{R}[x]$ is irreducible over $\mathbb{R}$ if and only if $\deg p = 1$, or $\deg p = 2$ and p has no real root.

Idea. An irreducible real polynomial has a complex root z by the theorem. A real root splits off a real linear factor. A non-real root brings its conjugate along, and the two together split off the real quadratic $(x - z)(x - \overline{z})$, first in $\mathbb{C}[x]$ and then, because division does not depend on the field, in $\mathbb{R}[x]$. Irreducibility leaves nothing else.

Proof. ($\Leftarrow$) A polynomial of degree 1 is irreducible, and one of degree 2 without a root in $\mathbb{R}$ is irreducible by Proposition 5.3.1 (b).

($\Rightarrow$) Let p be irreducible over $\mathbb{R}$. Then $\deg p \geq 1$, and by Theorem 5.6.6, p, as an element of $\mathbb{C}[x]$, has a root $z \in \mathbb{C}$.

Case 1: $z \in \mathbb{R}$. Then $x - z \mid p$ in $\mathbb{R}[x]$ (Theorem 5.1.3 (b), over $\mathbb{R}$), so $p = (x - z)h$ with $h \in \mathbb{R}[x]$; since $x - z$ is not constant, h is constant, and $\deg p = 1$.

Case 2: $z \notin \mathbb{R}$. Then $\overline{z} \neq z$ (Example (Conjugation and Other Automorphisms)), and $\overline{z}$ is also a root (Proposition 5.6.8 (b)). So the two distinct roots give $q := (x - z)(x - \overline{z}) \mid p$ in

$\mathbb{C}[x]$ (Theorem 5.4.1). By Theorem 1.2.2 (c),

$$q = x^2 - (z + \overline{z})x + z\overline{z} = x^2 - 2(\operatorname{Re} z)x + |z|^2,$$

which has real coefficients. Since $\mathbb{R}$ is a subfield of $\mathbb{C}$ (Example (Rational and Integer Complex Numbers)), Proposition 5.2.6 (b) gives $q \mid p$ in $\mathbb{R}[x]$: $p = qh$ with $h \in \mathbb{R}[x]$. Since q is not constant, h is constant, and $\deg p = 2$. Finally p has no real root: a root would make p, of degree 2, reducible (Proposition 5.3.1 (a)). This proves the corollary.

■

Theorem 5.6.10. Factorization of Real Polynomials

Let $f \in \mathbb{R}[x]$ be non-constant, with leading coefficient a. Then $f = a\,p_1 \cdots p_k$ for a list $p_1, \ldots, p_k$ $(k \geq 1)$ of monic polynomials in $\mathbb{R}[x]$, each of the form $x - c$ with $c \in \mathbb{R}$ or a quadratic with no real root. If r entries are linear and s are quadratic, then $r + 2s = \deg f$. The list is unique up to order, in the sense of Theorem 5.3.6 (b).

Proof. By Theorem 5.3.6 (a) over $F = \mathbb{R}$, $f = a\,p_1 \cdots p_k$ with monic irreducible p_i, and the list is unique up to order by part (b). By Corollary 5.6.9 each p_i has degree 1, so it is $x - c$ with $c \in \mathbb{R}$ (monic), or degree 2 with no real root. Degrees add over a product (Theorem 4.3.2 (b), induction on k), so $\deg f = r \cdot 1 + s \cdot 2$.

■

When the linear entries come first in the list, the factorization reads $f = a(x - c_1) \cdots (x - c_r)\, q_1 \cdots q_s$, the familiar form. (Reordering a list does not change its product, by repeated use of commutativity; nothing below needs this.) For $x^4 + 1$, $r = 0$ and $s = 2$ (Example (Factoring a quartic over the reals and over the complex numbers)).

Corollary 5.6.11. Real Polynomials of Odd Degree Have a Real Root

Every $f \in \mathbb{R}[x]$ of odd degree has a root in $\mathbb{R}$.

Proof. Factor $f = a\,p_1 \cdots p_k$ as in Theorem 5.6.10, with $r + 2s = \deg f$. If $r = 0$, then $\deg f = 2s$ is even, which an odd number is not (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a)). So $r \geq 1$: some $p_i = x - c$ with $c \in \mathbb{R}$. By (L2) of Section 5.3, $x - c$ divides $p_1 \cdots p_k$, hence divides $f = a\,p_1 \cdots p_k$ (Proposition 5.1.1 (b)), so $f(c) = 0$ by Theorem 5.1.3 (b).

■

Quick check. A real cubic f has exactly one real root c. What are r, s and $\operatorname{mult}_c(f)$?

Solution. Every linear entry $x - c'$ divides f, so c' is a real root (Theorem 5.1.3 (b)); hence each linear entry is $x - c$. Then $r + 2s = 3$ is odd, so $r \geq 1$ (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a), as in the proof of Corollary 5.6.11), and $(r, s) = (1, 1)$ or $(3, 0)$. Multiplicities add over the list (Proposition 5.4.5): a quadratic entry q has $q(c) \neq 0$, so $\text{mult}_c(q) = 0$, and $\text{mult}_c(f) = r$, which is 1 or 3. Examples: $x(x^2 + 1)$ and x^3.

Warning. Beyond degree 2, "no real root" does not make a real polynomial irreducible. The polynomial $x^4 + 1$ has no real root, since $c^4 + 1 = (c^2)^2 + 1 \geq 1$ for every $c \in \mathbb{R}$, yet it is the product of two real quadratics (Example (Factoring a quartic over the reals and over the complex numbers)). Corollary 5.6.9 says that every irreducible real polynomial has degree at most 2; so a real polynomial of degree 4 or more is always reducible, root or no root.

Remark (Looking ahead). *Analysis on the Real Line*, Chapter 6 proves the intermediate value theorem for continuous functions on an interval. With it, the odd-degree corollary has a second proof that uses no complex numbers: a real polynomial of odd degree takes values of both signs.

5.6.6 Exercises

5.6.6.1 A. Check your understanding

Exercise. A1

These parts are about the proof of Theorem 5.6.3.

(a) Where is the completeness of $\mathbb{R}$ used?

(b) Why does Step 3 take "the **first** quarter in a fixed order" with the same infimum, rather than "a quarter" with the same infimum?

(c) Run Steps 1–4 for $p = x^2 + 1$: find ρ, S_0, m, S_1 and S_2.

(d) Give the idea of the proof in two sentences.

Solution.

(a) Directly, twice: in Step 2, for the existence of each infimum $m(S)$, and in Step 5, for the suprema σ^* and τ^* that give the common point. Indirectly, through the real square roots behind the modulus (Definition 1.2.1, built on Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), which every inequality of the proof uses.

(b) "A quarter with the same infimum" exists, but there may be several, and naming one at each of infinitely many stages without a rule is a use of the axiom of choice. "The first one in a fixed order" is a rule, a function q from squares to squares, so Sets, Relations, and Cardinality, Theorem 2.3.1 defines the whole sequence (S_k) at once.

(c) Here $a_0 = 1$, $a_1 = 0$, $a_2 = 1$, so $A = 1$, $R = \max\{1, 2\} = 2$, and $2|p(0)|/|a_2| = 2$; hence $\rho = 2$ and $S_0 = S(-2, -2, 4)$. The infimum is $m = 0$: $|p| \geq 0$, and $p(-i) = 0$ with $-i \in S_0$. The first quarter of S_0 is $S(-2, -2, 2)$, which contains $-i$ (real part $0 \in [-2, 0]$,

imaginary part $-1 \in [-2,0]$); so its infimum is $0 = m$, and $S_1 = S(-2,-2,2)$. The quarters of S_1 have side 1. The first, $S(-2,-2,1)$, has no point with $|p|$ small: for $z = a+bi$ in it, $a,b \in [-2,-1]$, so $|p(z)| \geq |\mathrm{Im}(z^2+1)| = |2ab| \geq 2$ (Lemma 1.3.1), and its infimum is at least $2 > 0$. The second, $S(-1,-2,1)$, contains $-i$, so its infimum is 0, and $S_2 = S(-1,-2,1)$.

(d) The infimum of $|p|$ over a big square is what we want to attain; halving keeps a quarter with the same infimum, chosen by a rule. The squares shrink to one point, and the Lipschitz bound forces the value there to be the infimum.

5.6.6.2 B. Practice

Exercise. B1

Factor $x^4 - x^2 - 2$ into irreducible factors over $\mathbb{Q}$, over $\mathbb{R}$ and over $\mathbb{C}$. Then factor $x^4 + 4$ over $\mathbb{R}$ and over $\mathbb{C}$.

Solution. $x^4 - x^2 - 2$. Expanding shows $x^4 - x^2 - 2 = (x^2-2)(x^2+1)$. Over $\mathbb{Q}$: $x^2 - 2$ has no rational root (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.1) and $x^2 + 1$ has none ($c^2 + 1 > 0$, Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (e)), so both are irreducible (Proposition 5.3.1 (b)), and the factorization is $(x^2-2)(x^2+1)$. Over $\mathbb{R}$: $x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2})$ (Number Systems: From \(\nN\) to \(\nR\), Proposition 6.1.4), while x^2+1 still has no real root: $(x-\sqrt{2})(x+\sqrt{2})(x^2+1)$. Over $\mathbb{C}$: $x^2+1 = (x-i)(x+i)$, so $(x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i)$.

$x^4 + 4$. By the warning of Section 5.3, $x^4 + 4 = (x^2+2x+2)(x^2-2x+2)$, and $c^2 \pm 2c + 2 = (c \pm 1)^2 + 1 > 0$ for every $c \in \mathbb{R}$; so this is the factorization over $\mathbb{R}$ (Corollary 5.6.9). Over $\mathbb{C}$: $-1 \pm i$ are the roots of $x^2 + 2x + 2$ ($(-1+i)^2 = -2i$, and $-2i + 2(-1+i) + 2 = 0$; then its conjugate, by Proposition 5.6.8 (b)), and $1 \pm i$ those of $x^2 - 2x + 2$ likewise. So $x^4 + 4 = (x+1-i)(x+1+i)(x-1-i)(x-1+i)$, each quadratic being the product of its two distinct linear factors (Theorem 5.4.1, monic and of the same degree).

Exercise. B2

Run the proof of Lemma 5.6.5 for $p = x^3 - 2$ at $z_0 = 1$: find $b_0, \ldots, b_3$, k, c, ζ, u, α, B, t and the new point z, and compare $|p(z)|$ with $|p(1)|$.

Solution. Expansion around 1. Writing $x = (x-1)+1$ and expanding, $x^3 = (x-1)^3 + 3(x-1)^2 + 3(x-1) + 1$, so

$$x^3 - 2 = -1 + 3(x-1) + 3(x-1)^2 + (x-1)^3,$$

and by the uniqueness in Theorem 5.4.3, $(b_0, b_1, b_2, b_3) = (-1, 3, 3, 1)$. So $k = 1$ and $c = b_1/b_0 = -3$.

Direction. $k = 1$ is odd and $\mathrm{Re}\, c = -3 \neq 0$; $\zeta = 1$ gives $\mathrm{Re}(c\zeta) = -3 < 0$. So $u = -3$, $\alpha = 3$, $|u|^2 = 9$.

Constants. $B = |b_2/b_0||\zeta|^2 + |b_3/b_0||\zeta|^3 = 3 + 1 = 4$, and

$$t = \min\Big\{1, \frac{3}{9}, \frac{3}{16}\Big\} = \frac{3}{16}.$$

New point. $z = 1 + \frac{3}{16} = \frac{19}{16}$, and $p(19/16) = 6859/4096 - 2 = -1333/4096$. So $|p(z)| = 1333/4096 < 1 = |p(1)|$, well inside the proof's bound $1 - t\alpha/4 = 55/64$.

Exercise. B3

Let $f \in \mathbb{R}[x]$ have degree 5 and exactly one real root c. What can the multiplicity of c be, and how many quadratic factors without real root does f have? Give an example for each possibility.

Solution. Factor $f = a\,p_1 \cdots p_k$ as in Theorem 5.6.10, with r linear and s quadratic entries, $r + 2s = 5$. Each linear entry $x - c'$ divides f, so c' is a real root (Theorem 5.1.3 (b)); hence every linear entry is $x - c$. Multiplicities add over products (Proposition 5.4.5, with induction on k); $\mathrm{mult}_c(x - c) = 1$, a quadratic entry q has $q(c) \neq 0$ and so $\mathrm{mult}_c(q) = 0$, and the constant $a \neq 0$ has multiplicity 0. So $\mathrm{mult}_c(f) = r$. Since $r + 2s = 5$ is odd, $r \geq 1$ (Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a), as in the proof of Corollary 5.6.11), so the possibilities are $(r, s) = (1, 2)$, $(3, 1)$, $(5, 0)$: the multiplicity of c is 1, 3 or 5, with 2, 1 or 0 quadratic factors. Examples with $c = 0$: $x(x^2 + 1)^2$, $x^3(x^2 + 1)$, x^5. Each has only the real root 0, since $t^2 + 1 > 0$ for every $t \in \mathbb{R}$.

5.6.6.3 C. Going deeper

Exercise. C1: Exit check: the descent and the theorem

(a) Prove Lemma 5.6.5 from Lemma 5.6.4 and Theorem 5.4.3.

(b) Deduce Theorem 5.6.6 from (a) and Theorem 5.6.3.

(c) The field $\mathbb{Q}(i)$ of Example (Rational and Integer Complex Numbers) satisfies the field axioms, and $x^2 - 2$ has no root in it. Say which steps of the whole proof fail when $\mathbb{R}$ is replaced by $\mathbb{Q}$ and $\mathbb{C}$ by $\mathbb{Q}(i)$, and why $x^2 - 2$ shows that some step must fail.

Solution (Hint 1). Expand p around z_0 and divide by $p(z_0)$. Which coefficient after the constant one decides what happens near z_0?

Solution (Hint 2). Let k be the least $j \geq 1$ with $b_j \neq 0$, and fix a real t with $0 < t \leq 1$ before estimating $|p(z_0 + t\zeta)|$.

Solution.

(a) Let $n := \deg p \geq 1$. By Theorem 5.4.3, $p = \sum_{j=0}^{n} b_j(x - z_0)^j$ with $b_0 = p(z_0) \neq 0$ and $b_n \neq 0$; let k be the least $j \geq 1$ with $b_j \neq 0$ (Sets, Relations, and Cardinality,

Theorem 2.1.3; n is such a j). Let $c := b_k/b_0$, take ζ with $\operatorname{Re}(c\zeta^k) < 0$ (Lemma 5.6.4), and put $u := c\zeta^k$, $\alpha := -\operatorname{Re} u > 0$ (so $0 < \alpha \le |u|$), $B := \sum_{j=k+1}^{n} |b_j/b_0||\zeta|^j$, and

$$t := \min\{1, \alpha/|u|^2, \alpha/(4B)\}$$

(the last entry omitted if $B = 0$). Then $p(z_0 + t\zeta) = b_0(1 + t^k u + E)$ with $|E| \le t^{k+1}B$, since $b_j = 0$ for $1 \le j < k$ and $t^j \le t^{k+1}$ for $j > k$. With $s := t^k \le t \le \alpha/|u|^2$,

$$|1 + su|^2 = 1 - 2s\alpha + s^2|u|^2 \le 1 - s\alpha \le (1 - s\alpha/2)^2,$$

and $1 - s\alpha/2 > 0$ because $s\alpha \le \alpha^2/|u|^2 \le 1$ (as $\alpha \le |u|$); two non-negative reals are ordered as their squares (Number Systems: From \(\nN\) to \(\nR\), Proposition 2.3.5 (g)), so $|1 + su| \le 1 - s\alpha/2$. Using $tB \le \alpha/4$,

$$|p(z_0 + t\zeta)| \le |b_0|(1 - t^k\alpha/2 + t^{k+1}B) \le |b_0|(1 - t^k\alpha/4) < |b_0|.$$

(b) Let p be non-constant. By Theorem 5.6.3, some z^* has $|p(z^*)| \le |p(z)|$ for all z. If $p(z^*) \neq 0$, (a) gives z with $|p(z)| < |p(z^*)|$: a contradiction. So $p(z^*) = 0$.

(c) Completeness fails in $\mathbb{Q}$, and with it two kinds of step. *The infimum and the supremum.* Step 2 of Theorem 5.6.3 needs the infimum of a set of values, and Step 5 the supremum of the corners σ_k; in $\mathbb{Q}$ a bounded set need not have either (Number Systems: From \(\nN\) to \(\nR\), Theorem 2.6.2: the positive rationals q with $q^2 < 2$ have no rational supremum). *The square roots.* The modulus $\sqrt{a^2 + b^2}$ need not be rational ($|1+i| = \sqrt{2}$), and the square roots of Proposition 1.4.1, used in Case 2 of Lemma 5.6.4, need real square roots. The polynomial $x^2 - 2$ is non-constant with coefficients in $\mathbb{Q}(i)$ and no root there (the opening of this section), so the theorem is false for $\mathbb{Q}(i)$; a proof that went through unchanged would prove a falsehood, so some step must fail. In fact the failure for $x^2 - 2$ is exactly a missing square root: its roots in $\mathbb{C}$ are $\pm\sqrt{2}$.

Marking scheme. (10 points)

- 2: re-centers at z_0 with $b_0 = p(z_0) \neq 0$, and takes k to be the first index $j \ge 1$ with $b_j \neq 0$, with a reason that it exists.
- 1: obtains a direction ζ with $\operatorname{Re}(c\zeta^k) < 0$ from Lemma 5.6.4.
- 2: proves that the leading term decreases by a definite amount: $|1 + su| \le 1 - \kappa s$ or $|1 + su|^2 \le 1 - \kappa s$ (or the same kind of bound for $|1 + su + E|^2$ directly), with an explicit $\kappa > 0$ (for example $\kappa = \alpha/2$, resp. α), for all s in an explicit range such as $0 < s \le \alpha/|u|^2$.
- 2: bounds the tail by $t^{k+1}B$ and fixes t explicitly before the estimate that uses it.
- 2: concludes $|p(z_0 + t\zeta)| < |p(z_0)|$, and derives the theorem by contradiction with the minimum.
- 1: (c) names both uses of completeness (the infimum of Step 2, with the supremum of Step 5; the real square roots behind the modulus and behind the complex square roots of the direction lemma), and says why $x^2 - 2$ forces a failure.

Fatal errors (0 for the step): choosing t after the inequality that needs it, or letting it depend on the point being estimated; assuming the minimum exists without citing Theorem 5.6.3; using polar form or k-th roots of complex numbers, which this chapter does not have (a k-th root is accepted only with a proof). A proof that obtains the direction by polar form, if the reader has it from elsewhere, earns the 1 point of the direction step only together with a proof of the k-th root it uses.

Exercise. C2: Faded: the real polynomials vanishing at a non-real number

Let $\alpha \in \mathbb{C}$ with $\alpha \notin \mathbb{R}$, and let $J := \{f \in \mathbb{R}[x] : f(\alpha) = 0\}$, evaluating in $\mathbb{C}$. You are given only: J is an ideal of $\mathbb{R}[x]$, and $q := x^2 - 2(\operatorname{Re}\alpha)x + |\alpha|^2 \in J$. *Name the move, then complete it:* show that $J = \langle q \rangle$ and that q is irreducible over $\mathbb{R}$.

Solution. The move is **least degree, then divide**, as in Theorem 5.2.1. Since $q \neq 0$ is in J, the degrees of the non-zero elements of J form a non-empty subset of $\mathbb{N}$; let $e \in J$ have the least degree (Sets, Relations, and Cardinality, Theorem 2.1.3), and let d be its monic associate, which is in J because J is an ideal. Divide q by d: $q = hd + r$ with $\deg r < \deg d$ (Theorem 5.1.2). Then $r = q - hd \in J$, and a non-zero r would have smaller degree than the least; so $r = 0$ and $d \mid q$.

The degree of d. A non-zero constant does not vanish at α, so $\deg d \geq 1$. If $\deg d = 1$, then $d = x - c$ with $c \in \mathbb{R}$, and $d(\alpha) = 0$ gives $\alpha = c \in \mathbb{R}$, which is excluded. So $\deg d \geq 2$, and since $d \mid q$ with $\deg q = 2$, $\deg d = 2$ (Proposition 5.1.1 (d)). Then $q = hd$ with $\deg h = 0$, and comparing leading coefficients of the monic q and d, $h = 1$: $d = q$.

$J = \langle q \rangle$. Multiples of q are in J. For $f \in J$, divide: $f = gq + r$ with $\deg r < 2$; $r = f - gq \in J$, and a non-zero element of J has degree at least 2; so $r = 0$ and $f \in \langle q \rangle$.

Irreducible. If $q = gh$ with $g, h \in \mathbb{R}[x]$ non-constant, both have degree 1, and $0 = q(\alpha) = g(\alpha)h(\alpha)$ (Theorem 4.4.1), so $g(\alpha) = 0$ or $h(\alpha) = 0$ (Theorem 2.1.1 (f)): an element of J of degree 1, which was just excluded. So q is irreducible.

Exercise. C3: Find the error

Here is an argument.

> **Claim.** For every non-constant $p \in \mathbb{C}[x]$, $|p|$ attains a minimum on $\mathbb{C}$.
>
> **Proof.** (1) Let $m := \inf\{|p(z)| : z \in \mathbb{C}\}$, which exists since the set is non-empty and bounded below by 0. (2) For each $k \geq 1$, pick $z_k \in \mathbb{C}$ with $|p(z_k)| < m + 1/k$. (3) Since $|p(z_k)| < m + 1 \leq |p(0)| + 1$, Lemma 5.6.1 puts the z_k in a bounded set. (4) So they converge to some $z^* \in \mathbb{C}$. (5) Then $|p(z^*)| = \lim |p(z_k)| = m$.

Is the claim true? Does the argument prove it? Name the line that fails and the reason, give a counterexample to the illegal step, and say how the proof in the text avoids it.

Solution (Hint 1). For each line, ask which result of this volume or of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* justifies it.

Solution (Hint 2). Is every bounded sequence of real numbers convergent?

Solution. **The claim is true:** it is Theorem 5.6.3. **The argument does not prove it.**

Line (4) fails. "The z_k lie in a bounded set, so they converge" uses a general "fact" that is

neither proved here nor true: entry (N9) of Logic and Proof, Example (What is not allowed). Counterexample to the step: $z_k := (-1)^k$ lies in the bounded set $\{z : |z| \le 1\}$ and does not converge. (What is true, that a bounded sequence has a convergent **subsequence**, is not available in this volume; and the subsequence would still have to be chosen by a rule.) There is no counterexample to the conclusion.

Two further slips. Line (2) picks infinitely many z_k with no rule given, which is a use of the axiom of choice (compare Number Systems: From \(\nN\) to \(\nR\), Example (Picking Representatives Is a Use of Choice)). Line (5) moves $|p|$ past a limit, which needs continuity; Lemma 5.6.2 would supply it, but the line cites nothing.

The repair is the bisection of Theorem 5.6.3: it chooses squares by a rule ("the first quarter with the same infimum"), finds the common point as a supremum of corners, and replaces the limit by the Lipschitz estimate of Step 6. No sequence is ever asked to converge.

Marking scheme. (10 points)

- 2: says the claim is true and the argument, as written, does not prove it.
- 3: names line (4) and the reason: "bounded implies convergent" is unproved and false, (N9).
- 2: a counterexample to the step, such as $z_k = (-1)^k$.
- 1: names one further slip: the rule-less choice in line (2), or the unproved continuity in line (5).
- 2: describes the repair: squares chosen by a rule, the common point from completeness, the Lipschitz bound in place of a limit.

Fatal errors (0 for the step): a counterexample to the conclusion (there is none); "repairing" line (4) by citing Bolzano–Weierstrass as if it were proved in this volume.

5.6.6.4 R. Review

Exercise. R1

Let F be a field. Show that there are no non-zero $f, g \in F[x]$ with $f^2 = xg^2$.

Solution. This uses the degree of a product from Chapter 4 (Theorem 4.3.2 (b)), which holds over a field since a field has no zero divisors. Suppose $f, g \neq 0$ and $f^2 = xg^2$. Then $\deg(f^2) = 2\deg f$, and $\deg(xg^2) = 1 + 2\deg g$. So the natural number $2\deg f$ would equal $2\deg g + 1$: even and odd at once, which Number Systems: From \(\nN\) to \(\nR\), Corollary 3.1.3 (a) rules out. Hence no such f, g exist.

Exercise. R2

In $\mathbb{Q}[x]/\langle x^2 - 2\rangle$, show that every non-zero class $[a + bx]$ $(a, b \in \mathbb{Q})$ is a unit, by multiplying it by $[a - bx]$. Compute $[1 + x]^{-1}$.

Solution. In $\mathbb{Q}[x]$, $(a+bx)(a-bx) = a^2 - b^2x^2 = (a^2 - 2b^2) - b^2(x^2 - 2)$, so $[a+bx][a-bx] = [a^2 - 2b^2]$. If $(a, b) \neq (0, 0)$, the rational number $N := a^2 - 2b^2$ is non-zero: if $b = 0$, then $N = a^2 \neq 0$; if $b \neq 0$, then $N = 0$ would give $(a/b)^2 = 2$, against Number Systems: From

\(\nN\) to \(\nR\), Theorem 2.6.1. So $[a+bx]\cdot[N^{-1}(a-bx)]=[1]$, and $[a+bx]$ is a unit. Every class is $[a+bx]$ for exactly one pair (Theorem 5.5.2 (b)), and the zero class is the pair $(0,0)$, so every non-zero class is a unit: $\mathbb{Q}[x]/\langle x^2-2\rangle$ is a field, as Theorem 5.5.3 also says (x^2-2 is irreducible over $\mathbb{Q}$). For $1+x$: $N=1-2=-1$, so $[1+x]^{-1}=[-(1-x)]=[x-1]$. Check: $(1+x)(x-1)=x^2-1=1+(x^2-2)$.

This is the computation of Example (The Field Generated by the Square Root of Two) in Chapter 2, "multiply by the conjugate", with $[x]$ in place of $\sqrt{2}$: the class $[a+bx]$ behaves as $a+b\sqrt{2}$, and $(1+\sqrt{2})^{-1}=\sqrt{2}-1$.

Exercise. R3

Let $m,n\in\mathbb{Z}_{>0}$. Prove that $\gcd(2^m-1,2^n-1)=2^{\gcd(m,n)}-1$ in $\mathbb{Z}$.

Solution. The method is the integer Euclidean step of *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 3 (Number Systems: From \(\nN\) to \(\nR\), Lemma 3.2.3), used on the exponents and on the numbers at once. We prove the claim for all $m,n\geq 1$ by strong induction on $m+n$ (Logic and Proof, Theorem 4.2.2).

If $m=n$, both sides are 2^m-1: the gcd of a positive integer with itself is that integer (it divides both, and every common divisor is at most it, Number Systems: From \(\nN\) to \(\nR\), Definition 3.2.2), and $\gcd(m,m)=m$. If $m>n$, then

$$2^m-1=2^{m-n}(2^n-1)+(2^{m-n}-1),$$

and $2^n-1>0$, so Number Systems: From \(\nN\) to \(\nR\), Lemma 3.2.3 gives $\gcd(2^m-1,2^n-1)=\gcd(2^n-1,2^{m-n}-1)$. Likewise $m=1\cdot n+(m-n)$ gives $\gcd(m,n)=\gcd(n,m-n)$. Since $n+(m-n)=m<m+n$ and $m-n\geq 1$, the induction hypothesis gives $\gcd(2^n-1,2^{m-n}-1)=2^{\gcd(n,m-n)}-1=2^{\gcd(m,n)}-1$. If $m<n$, exchange the roles (the gcd is symmetric). For example, $\gcd(2^{12}-1,2^{18}-1)=\gcd(4095,262143)=63=2^6-1$.

This is the integer twin of Exercise C3 of Section 5.2 (Exercise (C3: The gcd of two binomials)), where x^m-1 and x^n-1 play the parts of 2^m-1 and 2^n-1.

Exercise. R4

Is x^4+x+1 irreducible over $\mathbb{F}_2$?

Solution. **Yes.** *The tool* is a degree count over a finite field: list the possible factorizations and check each.

The values are $0+0+1=1$ at 0 and $1+1+1=1$ at 1, so $f:=x^4+x+1$ has no root in $\mathbb{F}_2$, and hence no factor of degree 1 (Theorem 5.1.3 (c)). A factorization into non-constant factors would then be $f=gh$ with $\deg g=\deg h=2$. Over $\mathbb{F}_2$ the only non-zero constant is 1, so g and h are monic. A root of g or h would be a root of f, so both are rootless quadratics, hence irreducible (Proposition 5.3.1 (b)). The monic quadratics over $\mathbb{F}_2$ are x^2, $x^2+1=(x+1)^2$, $x^2+x=x(x+1)$ and x^2+x+1; only the last is rootless. So $g=h=x^2+x+1$, and $gh=x^4+2x^3+3x^2+2x+1=x^4+x^2+1\neq f$ in $\mathbb{F}_2[x]$. So f is irreducible.

Look-alikes that fail. "No root, hence irreducible" (Proposition 5.3.1) applies only in degrees 2 and 3; in degree 4 it is the error of Exercise C2 of Section 5.3, and $x^4+x^2+1 = (x^2+x+1)^2$ is a rootless reducible quartic over $\mathbb{F}_2$. The rational root test (Theorem 5.3.7) is about $\mathbb{Q}$, not $\mathbb{F}_2$. Eisenstein's criterion is not in this volume.