

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 4. 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 ω to $\aleph_1$* , 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 $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.4, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.6); every integer as n or $-n$ with $n \in \mathbb{N}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.4.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.5.1), with the rule that the reciprocal of a positive element of an ordered field is positive (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.1.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.1.3); integer linear combinations and Bézout’s identity (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.2.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.2.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, Definition 3.4.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.4.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Multiplication modulo six and modulo five)), the first finite groups of the chapter; the principal ideals of $\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1, Number

Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.3). Section 3.1 also uses the prime factorization (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.3.1) as a second instance of the recursion pattern, and Section 3.2's Exercise C3 recovers Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, 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 4.2; 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 8.6.
- 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.-1.1 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; homo-

morphisms, isomorphisms and kernels, with no clause for the identity, which follows; the product of two groups; examples $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $k \mapsto g^k$, 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.-1.2 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.