

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 $\mathbb{N}$ to $\mathbb{R}$), 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 $R \rightarrow R$, $c \mapsto p(c)$.

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 $\mathbb{N}$ to $\mathbb{R}$), 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 $\mathbb{N}$ to $\mathbb{R}$), 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 $(\Sigma 3)$ 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

$$(p + q)(c) = p(c) + q(c), \quad (pq)(c) = p(c)q(c),$$

and $a(c) = a$ for every constant a , and $x(c) = c$.

Idea. Sums are coefficientwise, and the sum rule $(\Sigma 1)$ 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 $(\Sigma 1)$ 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 $\Phi, \Psi: R[x] \times R[x] \rightarrow R$ 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 $\setminus(\setminus nN\setminus)$ to $\setminus(\setminus nR\setminus)$, 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 $R[x] \rightarrow R$ that respects $+$, $\cdot$ and 1 . The quotient map $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ of Number Systems: From $\mathbb{N}$ to $\mathbb{N}$, 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** $\varphi: R \rightarrow S$ is a function such that, **for all** $a, b \in R$,

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b),$$

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 $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ of [Example \(Ring Homomorphisms and Two Impostors\)](#) (i) is not injective.

Consequences. Let $\varphi: R \rightarrow S$ be a ring homomorphism.

- $\varphi(0) = 0$. Let $z := \varphi(0)$. 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 $\mathbb{N}$ to $\mathbb{N}$, 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 $\mathbb{N}$ to $\mathbb{N}$, 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 $\psi: S \rightarrow T$ is another ring homomorphism, then so is $\psi \circ \varphi: R \rightarrow T$: $\psi(\varphi(a + b)) = \psi(\varphi(a) + \varphi(b)) = \psi(\varphi(a)) + \psi(\varphi(b))$, 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 $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $a \mapsto [a]$, for $n \in \mathbb{Z}_{>0}$. (ii) The constants $R \rightarrow R[x]$, $a \mapsto ax^0$. (iii) The map $\mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $[a]_{mn} \mapsto ([a]_m, [a]_n)$, for coprime $m, n \in \mathbb{Z}_{>0}$. (iv) $\mathbb{Z} \rightarrow \mathbb{Z}$, $a \mapsto 2a$. (v) The zero map $\mathbb{Z} \rightarrow \mathbb{Z}$, $a \mapsto 0$.

Solution.

- (i) Yes, by Number Systems: From $\mathbb{N}$ to $\mathbb{N}$, Theorem 3.4.1 (c) with the ideal $n\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{N}$, Definition 3.4.2); more generally, the

quotient map $R \rightarrow R/I$ is one for every ideal I .

(ii) Yes, by Theorem 4.2.4 (b).

(iii) Yes, by Number Systems: From $\mathbb{N}$ to $\mathbb{N}$, 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 $z \mapsto \bar{z}$ 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, $\varphi: R \rightarrow S$ a ring homomorphism, and $s \in S$. Define $\Phi: R[x] \rightarrow S$ 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 $R[x] \rightarrow S$ 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 $\backslash(\backslash nN \backslash)$ to $\backslash(\backslash nR \backslash)$, 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, ($\Sigma 3$) 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 ($\Sigma 1$).

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 ,

$$\begin{aligned} \Phi((ax^m)(bx^n)) &= \Phi((ab)x^{m+n}) = \varphi(ab) s^{m+n} \\ &= \varphi(a)\varphi(b) s^m s^n = (\varphi(a) s^m)(\varphi(b) s^n) \\ &= \Phi(ax^m) \Phi(bx^n). \end{aligned}$$

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 $\Psi: R[x] \rightarrow S$ 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 $R[x] \rightarrow S$ 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 $\backslash(\backslash nN \backslash)$ to $\backslash(\backslash nR \backslash)$, 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 $S = R$, $\varphi = \text{id}_R$ 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 $\varphi: R \rightarrow S$ be a ring homomorphism. For $p \in R[x]$, let $\varphi_*(p)$ be the sequence with $(\varphi_*(p))_k := \varphi(p_k)$. Then $\varphi_*(p) \in S[x]$, and $\varphi_*: R[x] \rightarrow S[x]$ 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** $\varphi(\text{lc}(p)) \neq 0$.

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 $\gamma: R \rightarrow S[x]$, $\gamma(a) := \varphi(a)x^0$: 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 $\Phi: R[x] \rightarrow S[x]$ 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 $d := \deg p$. For $k > d$, $\varphi(p_k) = \varphi(0) = 0$, so $\deg \varphi_*(p) \leq d$; and the coefficient of $\varphi_*(p)$ at d is $\varphi(\text{lc}(p))$, 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 $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ gives $\mathbb{Z}[x] \rightarrow (\mathbb{Z}/n\mathbb{Z})[x]$, which reads every coefficient modulo n and respects sums and products. For $n = 2$,

$$2x^2 + 3x - 1 \mapsto 0x^2 + 1x + 1 = x + 1 \in \mathbb{F}_2[x],$$

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 $S = R[x]$, $\varphi: a \mapsto ax^0$ and $s = q$:

$$p \circ q = \sum_{k=0}^N p_k q^k \quad (N \text{ admissible for } p).$$

By Theorem 4.4.2 (a), $p \mapsto p \circ q$ is a ring homomorphism $R[x] \rightarrow R[x]$ 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 $p(-x) := p \circ (-x)$ 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 $R = S = \mathbb{Z}/8\mathbb{Z}$, $\varphi = \text{id}_{\mathbb{Z}/8\mathbb{Z}}$ and $s = [3]$.

4.4.6 Polynomials and polynomial functions

Every polynomial $p \in R[x]$ has a polynomial function $R \rightarrow R$. The functions $R \rightarrow R$ 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 $R \rightarrow R$ (Sets, Relations, and Cardinality, Definition 1.4.1), with the pointwise operations $(f + g)(c) := f(c) + g(c)$ and $(fg)(c) := f(c)g(c)$, is a commutative ring, whose zero and one are the constant functions with values 0 and 1.
- (b) The map $\varepsilon: R[x] \rightarrow R^R$, $\varepsilon(p) := (c \mapsto p(c))$, 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 $c_1, \dots, c_r$ lists the elements of R without repetition, then

$$P := \prod_{j=1}^r (x - c_j)$$

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 $R[x] \rightarrow R$ 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 $R \rightarrow R$, 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 $\alpha, \beta: R[x] \rightarrow R$, $\alpha(p) := (p \circ q)(c)$, $\beta(p) := p(q(c))$. 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 $S = R$, $\varphi = \text{id}_R$ 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 $P_j := \prod_{i=1}^j (x - c_i)$, 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 $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, 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 $\mathbb{F}_2 \rightarrow \mathbb{F}_2$.

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.

- Where in the proof is $\varphi(1) = 1$ used?
- Where is the commutativity of S used?
- 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 $\text{lc}(q^k) = \text{lc}(q)^k$. 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 $\text{lc}(q)^k \text{lc}(q)$.

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 $\mathbb{F}_2 \rightarrow \mathbb{F}_2$ (given by the values at 0 and 1). How many functions $\mathbb{F}_2 \rightarrow \mathbb{F}_2$ are there, and how many of the eight polynomials give each one?

Solution. By Definition 4.3.3, the elements are $a_0 + a_1x + a_2x^2$ 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 $\mathbb{F}_2 \rightarrow \mathbb{F}_2$ 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 $T_c: R[x] \rightarrow R[x]$ by $T_c(p) := p \circ (x + c)$. 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 $s = x$, $T_{-c} \circ T_c = \text{id}_{R[x]}$. Exchanging c and $-c$ (and $-(-c) = c$), $T_c \circ T_{-c} = \text{id}_{R[x]}$. 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, $\varphi: R \rightarrow S$ a ring homomorphism and $s \in S$, and let $\Phi(p) := \sum_{k=0}^N \varphi(p_k)s^k$ for N admissible for p . Then $\Phi: R[x] \rightarrow S$ is a well-defined ring homomorphism with $\Phi(a) = \varphi(a)$ for constants and $\Phi(x) = s$, and it is the only ring homomorphism $R[x] \rightarrow S$ 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 $(\Sigma 1)$.

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,

$$\Phi((ab)x^{m+n}) = \varphi(a)\varphi(b)s^m s^n = (\varphi(a)s^m)(\varphi(b)s^n),$$

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 $R[x] \rightarrow R[x]$ (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 $S = R[x]$, $\varphi: a \mapsto ax^0$ 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 $[0], \dots, [7]$ 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 $1, \dots, p - 1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, 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 $t_1, \dots, t_r$ in a commutative ring and a bijection σ of $\{1, \dots, r\}$, 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 $u_1, \dots, u_{r+1}$ 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 $k \leq r$, it follows from the rule for the first r entries (induction on the length) and (F5), (F6):

$$\begin{aligned} \prod_{j=1}^{r+1} u_j &= \left(\prod_{j=1}^r u_j \right) u_{r+1} = \left(\left(\prod_{j \leq r, j \neq k} u_j \right) u_k \right) u_{r+1} \\ &= \left(\left(\prod_{j \leq r, j \neq k} u_j \right) u_{r+1} \right) u_k, \end{aligned}$$

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 $i \geq k$, 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 $i \geq k$) is never k ; it is injective because σ and this index map are; and every $j \leq r$ is $\sigma(m)$ for some $m \neq k$, so $j = \sigma'(m)$ if $m < k$ and $j = \sigma'(m - 1)$ if $m > k$. By the deletion rule and the hypothesis for r , $\prod_{j=1}^{r+1} t_{\sigma(j)} = \left(\prod_{i=1}^r t_i \right) t_{r+1} = \prod_{j=1}^{r+1} t_j$.

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, $Q \neq 0$ (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 $p \geq 2$, the positions p and 1 differ), and $1 \neq 0$ in F ; so it is not the zero polynomial. For every $c \in F$, $c^p - c = 0$: if $c \neq 0$, $c^p = c^{p-1}c = c$ by (b); and $0^p = 0$ since $p \geq 1$. 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).