

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 $\mathbb{N}$ to $\mathbb{R}$, 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

$$(p + q)_k := p_k + q_k, \quad (-p)_k := -p_k, \quad (pq)_k := \sum_{i=0}^k p_i q_{k-i}.$$

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 $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N} \rightarrow R$, 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 $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b) with (F6). A sum whose terms are all 0 is 0 (Lemma 4.1.1 (b), ($\Sigma 3$) with $j = k + 1$), so $(pq)_k = 0$, and $m + n$ is admissible for pq .

So $+$ and $\cdot$ are functions $R[x] \times R[x] \rightarrow R[x]$, and $p \mapsto -p$ is a function $R[x] \rightarrow R[x]$. 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

$$\begin{aligned}(pq)_0 &= p_0q_0 = 2, \\(pq)_1 &= p_0q_1 + p_1q_0 = 2 - 1 = 1, \\(pq)_2 &= p_0q_2 + p_1q_1 + p_2q_0 = 0 - 1 + 3 = 2, \\(pq)_3 &= p_0q_3 + p_1q_2 + p_2q_1 + p_3q_0 = 0 + 0 + 3 + 0 = 3.\end{aligned}$$

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 $(pq)_k = p_kq_k$ 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 $(x \cdot x)_2 = x_0x_2 + x_1x_1 + x_2x_0 = 0 + 1 + 0 = 1$ 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 $+: T \times T \rightarrow T$ 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 $j \leq N$, 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 $j \leq N$; 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) $((ax^m)q)_k = a q_{k-m}$ for $k \geq m$, and $((ax^m)q)_k = 0$ for $k < m$.
- (b) $(ax^m)(bx^n) = (ab)x^{m+n}$.

Proof.

- (a) By Definition 4.2.1, $((ax^m)q)_k = \sum_{i=0}^k (ax^m)_i q_{k-i}$. For $i \neq m$, $(ax^m)_i = 0$, so the i -th term is $0 \cdot q_{k-i} = 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (b) with (F6)). By $(\Sigma 3)$ of Lemma 4.1.1 (b) with $j = m$, the sum is the term with $i = m$, namely $a q_{k-m}$, when $m \leq k$, and 0 when $m > k$.
- (b) Apply (a) with $q = bx^n$. For $k < m$ the coefficient is 0. For $k \geq m$ 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 $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, 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 $ax^m \cdot bx^n = abx^{m+n}$, 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 $p, p', q, q' \in R[x]$,

$$(p + p')q = pq + p'q \tag{*}$$

$$p(q + q') = pq + pq'. \quad (**)$$

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 $(\Sigma 1)$. 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 $+: T \times T \rightarrow T$. Let Φ, Ψ be maps of one, two or three polynomial arguments to T , that is, both maps $R[x] \rightarrow T$, both $R[x]^2 \rightarrow T$ or both $R[x]^3 \rightarrow T$, 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 $p_0 x^0$, so $p = p_0 x^0$ 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 $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1), with zero the zero polynomial, negative $-p$ as defined there, and one $1 := 1x^0$. 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 $R \rightarrow R[x]$, $a \mapsto ax^0$, 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 $1x^n$, and the product of the constant a with it is the monomial ax^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 $p \in R[x]$, $(ap)_k = ap_k$ 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 ax^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 $p = a_0 + a_1x$, $q = b_0 + b_1x$ and $r = c_0 + c_1x$, 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 $R[x] \times R[x] \rightarrow R[x]$. We check the clauses of Number Systems: From $\backslash(\backslash \mathbb{N} \backslash)$ to $\backslash(\backslash \mathbb{N} R \backslash)$, 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 $\Phi(p, q) := pq$ and $\Psi(p, q) := qp$. 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 $\backslash(\backslash \mathbb{N} \backslash)$ to $\backslash(\backslash \mathbb{N} R \backslash)$, 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 $\Phi(p, q, r) := (pq)r$ and $\Psi(p, q, r) := p(qr)$. Each is additive in each argument, by two applications of $(*)$ and $(**)$; for instance, in the middle argument,

$$(p(q + q'))r = (pq + pq')r = (pq)r + (pq')r, \quad p((q + q')r) = p(qr + q'r) = p(qr) + p(q'r),$$

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

$$((ax^m)(bx^n))(cx^l) = ((ab)c)x^{(m+n)+l} = (a(bc))x^{m+(n+l)} = (ax^m)((bx^n)(cx^l)),$$

where the middle equality is (F5) in R and $(m+n)+l = m+(n+l)$ in $\mathbb{N}$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\mathbb{R}\setminus)$, 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 $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\mathbb{R}\setminus)$, Definition 3.4.1, Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\mathbb{R}\setminus)$, 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.

- Where is the commutativity of R , $ab = ba$, used?
- Run the monomial check of (F5) on $(2x)(3x^2)(x)$ in $\mathbb{Z}[x]$: compute both groupings.
- In the proof of (F5), which additivity does Lemma 4.2.3 need for the third argument? Write out both identities.
- Give the idea of the proof of (F5) in two sentences.

Solution.

- 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 $(p_i + p'_i)q_{k-i} = p_i q_{k-i} + p'_i q_{k-i}$ 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 $\mathbb{N}$ to $\mathbb{R}$, 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**.
- 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 $6x^4$.
- 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.
- 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 $\sigma: R[x] \rightarrow R[x]$ 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),

$$\Phi(ax^m, bx^n) = \sigma((ab)x^{m+n}) = ((-1)^{m+n} ab)x^{m+n},$$

$$\Psi(ax^m, bx^n) = ((-1)^m a)x^m \cdot ((-1)^n b)x^n = ((-1)^{m+n} a(-1)^n b)x^{m+n}.$$

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 ($\Sigma 3$), $(ax^m)(bx^n) = (ab)x^{m+n}$.

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 $\Phi, \Psi: R[x] \rightarrow R[x]$ 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 ($(\Sigma 1)$) 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 $(\Sigma 1)$ – $(\Sigma 4)$ 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 $\mathbb{N} \rightarrow R$, with sum and product given by the formulas of [Definition 4.2.1](#).

- Show that the formulas define functions $R^{\mathbb{N}} \times R^{\mathbb{N}} \rightarrow R^{\mathbb{N}}$.
- Show that $R[x] \subseteq R^{\mathbb{N}}$ is closed under the sum and the product.
- Let $s := (1, 1, 1, \dots)$. Show that $(1 - x)s = 1$.
- Which step of the proof of [Lemma 4.2.3](#) (with one argument) does not reach the elements of $R^{\mathbb{N}}$?

Solution.

- 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 $\mathbb{N} \rightarrow R$.
- 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 .
- $1 - x = (1, -1, 0, 0, \dots)$. 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 $\backslash(\backslash \mathbb{N} \backslash)$ to $\backslash(\backslash \mathbb{N} \backslash)$, [Proposition 2.3.2 \(b\)](#) with (F6)). By $(\Sigma 1)$ and $(\Sigma 3)$, the sum is $1 \cdot 1 + (-1) \cdot 1 = 1 + (-1) = 0$, by (F7) and (F4). So $(1 - x)s = (1, 0, 0, \dots) = 1$.
- 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 $\mathbb{Z}[x]$.