

4.3 Degree, Leading Coefficients, and Integral Domains

Section 4.2 made $R[x]$ a commutative ring for every commutative ring R (Theorem 4.2.4). This section attaches to each non-zero polynomial its **degree**, the position of its last non-zero coefficient, and asks the school question: is the degree of a product the sum of the degrees? Over $\mathbb{Z}$ it is. Over $\mathbb{Z}/6\mathbb{Z}$ it is not, and the reason is a single product of two elements of R . Sorting out which rings behave like $\mathbb{Z}$ leads to the integral domains, and to the two facts later chapters use most: a polynomial ring over an integral domain has no zero divisors, and its units are the units of R .

Throughout, R is a commutative ring (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1), and polynomials are coefficient sequences (Definition 4.1.1), with the sum and product of Definition 4.2.1.

4.3.1 Degree and leading coefficient

Here is the computation that drives the section. Multiply $p = 2x + 1$ by $q = 3x^2 + x$ by the product formula of Definition 4.2.1, once in $\mathbb{Z}[x]$ and once in $(\mathbb{Z}/6\mathbb{Z})[x]$. The coefficients of p are $1, 2, 0, 0, \dots$ and those of q are $0, 1, 3, 0, \dots$, so

$$\begin{aligned}(pq)_0 &= p_0q_0 = 0, \\(pq)_1 &= p_0q_1 + p_1q_0 = 1, \\(pq)_2 &= p_0q_2 + p_1q_1 + p_2q_0 = 3 + 2 = 5, \\(pq)_3 &= p_0q_3 + p_1q_2 + p_2q_1 + p_3q_0 = 2 \cdot 3 = 6,\end{aligned}$$

and $(pq)_k = 0$ for $k \geq 4$. Over $\mathbb{Z}$ the product is $6x^3 + 5x^2 + x$, with its last non-zero coefficient in position $3 = 1 + 2$. Over $\mathbb{Z}/6\mathbb{Z}$ the same sums are read modulo 6: $(pq)_3 = [6] = [0]$, and the product is $[5]x^2 + x$, whose last non-zero coefficient sits in position 2. The top coefficient of the product was $2 \cdot 3$, the product of the top coefficients of the factors, and in $\mathbb{Z}/6\mathbb{Z}$ that product is $[0]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Multiplication modulo six and modulo five)).

To state any of this we need a name for “the position of the last non-zero coefficient”. A non-zero polynomial has one, because only finitely many of its coefficients are non-zero.

The degree of a polynomial is the position of its last non-zero coefficient; the leading coefficient is the coefficient sitting there.

Definition 4.3.1. Degree, Leading Coefficient, Monic

Let R be a commutative ring and $p \in R[x]$.

- (a) If $p \neq 0$, the **degree** $\deg p$ is the **largest** $n \in \mathbb{N}$ with $p_n \neq 0$. The **leading coefficient** of p is $\text{lc}(p) := p_{\deg p}$, and p is **monic** if $\text{lc}(p) = 1$.
- (b) The zero polynomial has degree $\deg 0 := -\infty$, and **no** leading coefficient.

Here $-\infty$ is a symbol not in $\mathbb{N}$, with the conventions $-\infty < n$ and $-\infty + n = n + (-\infty) = -\infty$ for every $n \in \mathbb{N}$, and $-\infty + (-\infty) = -\infty$.

In words: (a) looks along the coefficient sequence and stops at the last place where it is non-zero;

that place is the degree, and the entry there is the leading coefficient. A polynomial is monic when that entry is 1. Clause (b) gives the zero polynomial, which has no non-zero coefficient at all, a degree below every natural number.

Well-definedness. Let $p \neq 0$, and let N be admissible for p : $p_k = 0$ for every $k > N$ (Definition 4.1.1). The set $S := \{n \in \mathbb{N} : p_n \neq 0\}$ is non-empty, since p is not the zero sequence, and every element of S is at most N . Read in $\mathbb{Z} \supseteq \mathbb{N}$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 2.2.3), S is a non-empty set of integers bounded above, so it has a greatest element (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 2.3.6). That element is $\deg p$. Two facts come with it, and every proof below uses them:

$$p_{\deg p} \neq 0, \quad p_k = 0 \text{ for every } k > \deg p.$$

The second says that $\deg p$ is itself admissible for p , and the least admissible N : any smaller N would leave the non-zero coefficient $p_{\deg p}$ beyond it.

Examples.

- In $\mathbb{Q}[x]$, $\deg(3x^2 - x + 2) = 2$ with leading coefficient 3; $x^2 + 1$ is monic of degree 2. The monomial ax^n with $a \neq 0$ has degree n and leading coefficient a .
- A non-zero constant $a = ax^0$ has degree 0. The constant 0 has degree $-\infty$, not 0: degree 0 means “a constant, and not the zero one”.
- Degree depends on the ring. The integer polynomial $6x^3 + 5x^2 + x$ has degree 3 in $\mathbb{Z}[x]$; its coefficients read in $\mathbb{Z}/6\mathbb{Z}$ give $[5]x^2 + x$, of degree 2. Read in $\mathbb{Z}/5\mathbb{Z}$ they give $x^3 + x$ ($[6] = [1]$, $[5] = [0]$), monic of degree 3.
- **The degenerate ring.** If $1 = 0$ in R , then every $a \in R$ is $a = a \cdot 1 = a \cdot 0 = 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 2.3.2 (b)), so $R = \{0\}$, and the only polynomial over R is the zero sequence. Every polynomial over the zero ring has degree $-\infty$, and no polynomial over it is monic. This is why “monic” will never need the hypothesis $1 \neq 0$: a monic polynomial is non-zero, so its ring has $1 = \text{lc}(p) \neq 0$.

Non-example by minimal change. The sequence $(1, 1, 1, \dots)$ has no degree: the set S of its non-zero positions is all of $\mathbb{N}$, which has no greatest element. It fails exactly the clause “only finitely many” of Definition 4.1.1, which is what made S bounded above.

◉ **Second reading** · *Why the degree of the zero polynomial is minus infinity*

Any value given to $\deg 0$ is a convention, and the choice is made so that the rule “degrees add under products” survives the zero polynomial. For every q , $0 \cdot q = 0$, so the rule asks for $\deg 0 = \deg 0 + \deg q$. If $\deg 0$ were an integer d , then in any ring with $1 \neq 0$ the case $q = x$, of degree 1, would give $d = d + 1$. No integer works; a symbol $-\infty$ with $-\infty + n = -\infty$ does. The order $-\infty < n$ then lets “ $\deg p \leq n$ ” include the zero polynomial, which is what the sets $R[x]_{\leq n}$ at the end of this section need.

Warning. The leading coefficient is the coefficient of the **highest** power, not the first one written. In $2 + x - 5x^3 \in \mathbb{Q}[x]$, the leading coefficient is -5 , and the polynomial is not monic although its x has coefficient 1. And the zero polynomial has no leading coefficient at all: “ $\text{lc}(p)$ ” silently assumes $p \neq 0$.

4.3.2 The degree of a sum

A sum cannot raise the degree, because adding coefficients position by position creates no non-zero coefficient beyond the last non-zero ones of the summands.

Theorem 4.3.1. Degree of a Sum

Let R be a commutative ring and $p, q \in R[x]$. Then

$$\deg(p + q) \leq \max(\deg p, \deg q),$$

with **equality** when $\deg p \neq \deg q$.

Idea. Beyond the larger of the two degrees both summands have only zero coefficients, so the sum does too. When one degree is strictly larger, the other summand contributes 0 at that top position, and the top coefficient survives.

Proof. Let $M := \max(\deg p, \deg q)$. If $M = -\infty$, then $p = q = 0$, so $p + q = 0$ and both sides are $-\infty$. Otherwise $M \in \mathbb{N}$, and for $k > M$ we have $k > \deg p$ and $k > \deg q$, so $p_k = 0$ and $q_k = 0$ (by the two facts after Definition 4.3.1 when the polynomial is non-zero, and trivially when it is 0). Hence $(p + q)_k = p_k + q_k = 0 + 0 = 0$ for every $k > M$, by Definition 4.2.1 and (F3). So either $p + q = 0$, with degree $-\infty < M$, or $p + q \neq 0$ and its last non-zero coefficient is at a position $\leq M$. In both cases $\deg(p + q) \leq M$.

Now let $\deg p \neq \deg q$; by symmetry $\deg q < \deg p$, so $p \neq 0$ and $M = \deg p$. Then $q_M = 0$, and

$$(p + q)_M = p_M + q_M = p_M + 0 = p_M \neq 0,$$

so $p + q \neq 0$ and $\deg(p + q) \geq M$. With the first part, $\deg(p + q) = M$. ■

Remark. The inequality is strict exactly when $\deg p = \deg q = M \in \mathbb{N}$ and the leading coefficients cancel, $p_M + q_M = 0$: for example $(x^2 + x) + (-x^2 + 1) = x + 1$, of degree $1 < 2$, and $x + (-x) = 0$, of degree $-\infty < 1$.

4.3.3 The degree of a product

The opening computation suggests how a product behaves at the top. In $(pq)_k = \sum_{i=0}^k p_i q_{k-i}$, a term can be non-zero only if $i \leq \deg p$ and $k - i \leq \deg q$; for $k = \deg p + \deg q$ that leaves exactly one term. We call this move **look at the top coefficient**.

Theorem 4.3.2. Degree of a Product

Let R be a commutative ring, let $p, q \in R[x]$ be non-zero, and let $m := \deg p$, $n := \deg q$.

- (a) $(pq)_k = 0$ for every $k > m + n$, and $(pq)_{m+n} = \text{lc}(p) \text{lc}(q)$. Hence $\deg(pq) \leq \deg p + \deg q$

for **all** $p, q \in R[x]$, zero or not; and if $p = 0$ or $q = 0$, then $pq = 0$ and $\deg(pq) = -\infty = \deg p + \deg q$.

(b) $\deg(pq) = m + n$ **if and only if** $\text{lc}(p)\text{lc}(q) \neq 0$, and then $\text{lc}(pq) = \text{lc}(p)\text{lc}(q)$. This holds in particular

- when R has **no zero divisors** ($ab = 0$ implies $a = 0$ or $b = 0$), for example when R is a field (Theorem 2.1.1 (f)); together with the last clause of (a), $\deg(pq) = \deg p + \deg q$ then holds for **all** $p, q \in R[x]$, zero or not;
- when $\text{lc}(p)$ is a unit of R (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Definition 3.5.1), in particular when p is monic.

In words: (a) says that the product has nothing above position $m + n$, and that what sits at $m + n$ is the product of the two leading coefficients, in every commutative ring; (b) says that the degree formula holds precisely when that one product is non-zero, and names two common situations where it is.

Idea. The top of a product comes from the tops of the factors alone. Above $m + n$ every term $p_i q_{k-i}$ has a factor beyond the top of p or beyond the top of q ; at $m + n$ exactly one term escapes, $p_m q_n$. So the only question is whether $p_m q_n$ can be 0, and that is a question about R , not about polynomials.

Before reading on: which line needs R to have no zero divisors, and which works in every ring?

Proof. (a) Let $k \geq m + n$ and $0 \leq i \leq k$, and consider the term $p_i q_{k-i}$ of $(pq)_k$ (Definition 4.2.1). If $i > m$, then $p_i = 0$. If $i \leq m$, then $k - i \geq k - m \geq n$, and $k - i > n$ (so $q_{k-i} = 0$) unless $k = m + n$ and $i = m$. So every term with $i \neq m$, or with $k > m + n$, has a factor 0, and is 0 by Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (b) with (F6).

For $k > m + n$, all terms of $(pq)_k$ are 0, so $(pq)_k = 0$ by $(\Sigma 3)$ of Lemma 4.1.1 (b) (with $j = 0$). For $k = m + n$, every term with $i \neq m$ is 0, and $m \leq m + n$, so $(\Sigma 3)$ with $j = m$ leaves

$$(pq)_{m+n} = p_m q_n = \text{lc}(p)\text{lc}(q).$$

For the inequality, let $p, q \in R[x]$ be arbitrary. If $p = 0$, every coefficient of pq is a sum of terms $0 \cdot q_{k-i} = 0$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (b), (F6)), so $pq = 0$, and both sides of the inequality are $-\infty$ by the conventions of Definition 4.3.1, which is also the last clause of (a); likewise if $q = 0$. If $p, q \neq 0$ and $pq = 0$, the left side is $-\infty < m + n$. Otherwise $pq \neq 0$, and since $(pq)_k = 0$ for every $k > m + n$, its last non-zero coefficient is at a position $\leq m + n$: $\deg(pq) \leq m + n$.

(b) By (a), $m + n$ is admissible for pq , and $(pq)_{m+n} = \text{lc}(p)\text{lc}(q)$. If this element is non-zero, then $pq \neq 0$, its last non-zero coefficient is at $m + n$, and so $\deg(pq) = m + n$ and $\text{lc}(pq) = (pq)_{m+n} = \text{lc}(p)\text{lc}(q)$. If it is 0, then $(pq)_k = 0$ for every $k \geq m + n$, so $\deg(pq) < m + n$.

For the two situations: $p_m \neq 0$ and $q_n \neq 0$ by Definition 4.3.1, so if R has no zero divisors, $p_m q_n \neq 0$. If $u := p_m$ is a unit and $u q_n = 0$, then $q_n = (u^{-1}u)q_n = u^{-1}(u q_n) = u^{-1} \cdot 0 = 0$, by (F6), (F7), (F5) and Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (b), against $q_n \neq 0$; so $p_m q_n \neq 0$. A monic p has $p_m = 1$, a unit since $1 \cdot 1 = 1$. This proves the theorem.

The answer to the prompt. Part (a), including the inequality, uses only (F1)–(F7), (F9), Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b), ($\Sigma 3$) of Lemma 4.1.1 (b), and the two facts after Definition 4.3.1 and its conventions, all valid in every commutative ring: it holds over $\mathbb{Z}/6\mathbb{Z}$ as over $\mathbb{Q}$. Part (b) as an equivalence also holds in every ring. “No zero divisors” enters in one line, the first sentence of the last paragraph, and only to decide that $p_m q_n \neq 0$; the unit hypothesis is a second, different way to decide the same thing.

Warning. The degree formula is not automatic. In $(\mathbb{Z}/6\mathbb{Z})[x]$, the opening computation gives

$$([2]x + [1])([3]x^2 + x) = [5]x^2 + x,$$

a product of polynomials of degrees 1 and 2 that has degree 2, not 3. The coefficient $(pq)_3$ is $\text{lc}(p)\text{lc}(q) = [2][3] = [6] = [0]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Multiplication modulo six and modulo five)). Part (a) of Theorem 4.3.2 holds here; the hypothesis of (b) fails.

Quick check. Let $p, q \in \mathbb{Q}[x]$ with $\deg p = 3$ and $\deg q = 2$. What are $\deg(pq)$, $\deg(p + q)$ and $\deg(p^2)$, where $p^2 := pp$? Can you say what $\deg(p - x^3)$ is?

Solution. $\deg(pq) = 5$ and $\deg(p^2) = 6$, by Theorem 4.3.2 (b): $\mathbb{Q}$ is a field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.4.3), so it has no zero divisors. $\deg(p + q) = 3$, by the equality case of Theorem 4.3.1, since $3 \neq 2$. The degree of $p - x^3$ is not determined: it is 3 if $\text{lc}(p) \neq 1$, at most 2 if p is monic, and $-\infty$ if $p = x^3$. The difference has coefficient $\text{lc}(p) - 1$ at position 3, and that coefficient decides.

4.3.4 Integral domains

Theorem 4.3.2 (b) asks for one property of R : a product of two non-zero elements is non-zero. The integers have it, every field has it, $\mathbb{Z}/6\mathbb{Z}$ lacks it. A ring that has it, and is not the zero ring, gets a name.

An integral domain is a commutative ring in which a product is zero only when a factor is zero.

Definition 4.3.2. Integral Domain

An **integral domain** is a commutative ring R with $1 \neq 0$ and **no zero divisors**: for all $a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$.

In words: the zero ring is excluded, and the rule “a product vanishes only if a factor vanishes”, the rule used to solve $(x - 1)(x - 2) = 0$ at school, holds in R . Equivalently, by contraposition: the product of two non-zero elements is non-zero.

Example. Which Rings Are Integral Domains

Decide which of the following are integral domains: $\mathbb{Z}$; a field, and in particular $\mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z}$ for a prime p ; $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$ not prime (Sets, Relations, and Cardinality, Definition 2.2.2); $\mathbb{Z}/1\mathbb{Z}$; and $\mathbb{Z} \times \mathbb{Z}$ with componentwise operations, $(a, b) + (c, d) := (a + c, b + d)$ and $(a, b)(c, d) := (ac, bd)$.

Solution. $\mathbb{Z}$: *yes*. It is a commutative ring with $1 \neq 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.1), and an ordered commutative ring (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.4), so $ab = 0$ implies $a = 0$ or $b = 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (f).

A field: *yes*. A field has $1 \neq 0$ (Definition 2.1.1) and no zero divisors (Theorem 2.1.1 (f)). So $\mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.4.3) and $\mathbb{Z}/p\mathbb{Z}$ for p prime (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2) are integral domains.

$\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$ not prime: *no*. By Sets, Relations, and Cardinality, Definition 2.2.2, n has a positive divisor $r \notin \{1, n\}$; write $n = rs$. As in the proof of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2 ($\Rightarrow$), $1 < r < n$ and $0 < s < n$. Then $[r] \neq [0]$: otherwise $n \mid r$ with $n, r > 0$, and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (e) would give $n \leq r$, against $r < n$. Likewise $[s] \neq [0]$. But $[r][s] = [rs] = [n] = [0]$, by the multiplication of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.4.2 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1 (b)).

$\mathbb{Z}/1\mathbb{Z}$: *no*. It has $[1] = [0]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (c)); it is the zero ring.

$\mathbb{Z} \times \mathbb{Z}$: *no*. Each ring axiom holds componentwise, because it holds in each coordinate in $\mathbb{Z}$, with zero $(0, 0)$ and one $(1, 1) \neq (0, 0)$. But $(1, 0)(0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$, with both factors non-zero.

Putting the second and third answers together with Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2: for $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if it is a field, if and only if n is prime.

Now the payoff. Over an integral domain the degree formula holds without exception, and the polynomial ring inherits the property it was built from.

Corollary 4.3.3. Polynomial Rings over Integral Domains

Let R be a commutative ring.

- (a) If R is an integral domain, $p, q \in R[x]$ and $pq = 0$, then $p = 0$ or $q = 0$. So $R[x]$ is an integral domain.
- (b) (Cancellation) If R is an integral domain, $p, q, r \in R[x]$, $pq = pr$ and $p \neq 0$, then $q = r$.
- (c) Conversely, if $R[x]$ is an integral domain, then so is R .

Proof. (a) Let $p \neq 0$ and $q \neq 0$. Since R has no zero divisors, Theorem 4.3.2 (b) gives $\deg(pq) = \deg p + \deg q \in \mathbb{N}$, so $\deg(pq) \neq -\infty$ and $pq \neq 0$. By contraposition, $pq = 0$ implies $p = 0$ or $q = 0$. Moreover $R[x]$ is a commutative ring (Theorem 4.2.4 (a)), and $1 \neq 0$

in $R[x]$ because $1 \neq 0$ in R (Theorem 4.2.4 (b)). So $R[x]$ is an integral domain.

(b) By (F9) of $R[x]$ and Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (c), $p(q - r) = pq - pr = 0$. By (a) and $p \neq 0$, $q - r = 0$, so $q = r$ (add r to both sides, with (F2), (F1), (F4), (F3)).

(c) The map $a \mapsto ax^0$ from R to $R[x]$ is injective and preserves sums, products and 1 (Theorem 4.2.4 (b)). If $1 = 0$ in R , then the one of $R[x]$, which is $1x^0$, equals $0x^0$, the zero polynomial, against $1 \neq 0$ in $R[x]$. If $ab = 0$ in R , then $(ax^0)(bx^0) = (ab)x^0 = 0x^0$ is the zero polynomial, so $ax^0 = 0x^0$ or $bx^0 = 0x^0$, and by injectivity $a = 0$ or $b = 0$. ■

With $R = \mathbb{Q}$, Definition 4.3.1, Theorem 4.3.2 (b) and part (a) are the polynomial algebra that the ordered field $\mathbb{Q}(t)$ of Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Example (A Non-Archimedean Ordered Field) took on school credit: the degree and the leading coefficient of a polynomial, the rule $\text{lc}(pq) = \text{lc}(p)\text{lc}(q)$, and the absence of zero divisors in $\mathbb{Q}[t]$ (the letter t there plays the part of our x). Building fractions p/q of polynomials is a further step, which this volume does not take.

The cancellation law (b) is what makes it legitimate to “divide both sides by p ” in an identity of polynomials over $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{F}_p$. Over $\mathbb{Z}/6\mathbb{Z}$ it fails: $[2] \cdot [3]x = [0] = [2] \cdot [0]$ with $[2] \neq [0]$ and $[3]x \neq [0]$.

4.3.5 Units of a polynomial ring

The degree also tells us which polynomials can be inverted. If $pq = 1$ and degrees add, then $\deg p + \deg q = 0$, so both are constants.

Proposition 4.3.4. Units of a Polynomial Ring

Let R be an integral domain. Then the units of $R[x]$ are exactly the constants a with $a \in R^\times$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Definition 3.5.1): identifying a with ax^0 , $(R[x])^\times = R^\times$.

Proof. Let p be a unit of $R[x]$, with $pq = 1$. Since $1 \neq 0$ in $R[x]$ (Corollary 4.3.3 (a)) and $0 \cdot q = 0$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (b) in the commutative ring $R[x]$, Theorem 4.2.4 (a)), we have $p \neq 0$, and likewise $q \neq 0$. By Theorem 4.3.2 (b), $\deg p + \deg q = \deg 1 = 0$. Two natural numbers with sum 0 are both 0, so $\deg p = \deg q = 0$: $p = ax^0$ and $q = bx^0$ with $a = p_0$, $b = q_0 \in R$ (0 is admissible for p and q by the facts after Definition 4.3.1, so Proposition 4.2.1 with $N = 0$ applies). Then $(ab)x^0 = (ax^0)(bx^0) = 1x^0$ (Theorem 4.2.4 (b)), so $ab = 1$ by injectivity of $a \mapsto ax^0$, and $a \in R^\times$.

Conversely, if $a \in R^\times$ with $ab = 1$, then $(ax^0)(bx^0) = (ab)x^0 = 1x^0$, so the constant a is a unit of $R[x]$. ■

For a field F , $F^\times$ consists of the non-zero elements (by (F8), and 0 is not a unit since $0 \cdot b = 0 \neq 1$ by Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (b) and (F6)). So the units of $F[x]$ are the non-zero constants. Over $\mathbb{Z}$, an integral domain (Example (Which Rings Are

(Integral Domains)), the units of $\mathbb{Z}[x]$ are the constants 1 and -1 , since $\mathbb{Z}^\times = \{1, -1\}$ (the examples after Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 3.5.1): 2 is a unit of $\mathbb{Q}[x]$ and not of $\mathbb{Z}[x]$.

Warning. Without “integral domain”, non-constant units exist. In $(\mathbb{Z}/4\mathbb{Z})[x]$,

$$(1 + [2]x)^2 = 1 + [4]x + [4]x^2 = 1,$$

by the product formula: the coefficients are $1 \cdot 1$, $1 \cdot [2] + [2] \cdot 1$ and $[2][2]$. So $1 + [2]x$ is a unit of degree 1, its own inverse. The proof above breaks at Theorem 4.3.2 (b): $\text{lc}(p) \text{lc}(p) = [2][2] = [0]$, so degrees do not add.

4.3.6 Polynomials of bounded degree

Many later arguments fix a bound on the degree: interpolation through $n + 1$ points looks for a polynomial of degree at most n , and the linear-algebra companion treats such polynomials as a vector space. Two sets get names.

Definition 4.3.3. Polynomials of Degree at Most n

Let R be a commutative ring and $n \in \mathbb{N}$. The set of **polynomials of degree at most n** is

$$R[x]_{\leq n} := \{p \in R[x] : \deg p \leq n\}.$$

There are two ways to describe this set, and it is worth seeing that they agree. A polynomial has $\deg p \leq n$ exactly when $p_k = 0$ for every $k > n$: for $p \neq 0$ by the two facts after Definition 4.3.1, and for $p = 0$ both hold. By Proposition 4.2.1, such a p is the sum $p_0 + p_1x + \cdots + p_nx^n$ of its first $n + 1$ monomials, and every such sum, with $a_0, \dots, a_n \in R$ arbitrary, has its coefficients beyond n equal to 0. So

$$R[x]_{\leq n} = \{a_0 + a_1x + \cdots + a_nx^n : a_0, \dots, a_n \in R\}.$$

The first description is about degrees; the second is the one used for computing. Some of the a_i , including a_n , may be 0, and $0 \in R[x]_{\leq n}$ (all $a_i = 0$; $-\infty \leq n$).

The set is closed under the operations that do not raise the degree. If $p, q \in R[x]_{\leq n}$, then $p + q \in R[x]_{\leq n}$ by Theorem 4.3.1; $-p \in R[x]_{\leq n}$, since $(-p)_k = -p_k = -0 = 0$ for $k > n$; and $ap \in R[x]_{\leq n}$ for every constant a , since $(ap)_k = ap_k = a \cdot 0 = 0$ for $k > n$ (Theorem 4.2.4 (d), Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.2 (b)). It is not closed under products: $x^n \cdot x \notin R[x]_{\leq n}$ when $1 \neq 0$.

Example. Membership in Polynomials of Bounded Degree

Which of $3x^2 - 2x + 1$, $5x + 7$, -4 , 0 and $x^3 - x^3 + x$ lie in $\mathbb{Q}[x]_{\leq 2}$? Which lie in $\mathbb{Q}[x]_{\leq 0}$?

Solution. The degrees are 2, 1, 0, $-\infty$ and 1: the last expression is the polynomial x , since its coefficient in position 3 is $1 + (-1) = 0$. An expression containing x^3 can still have degree below 3; the degree belongs to the polynomial, not to the way it is written. So all five lie in $\mathbb{Q}[x]_{\leq 2}$, and exactly -4 and 0 lie in $\mathbb{Q}[x]_{\leq 0}$, the set of constants.

Definition 4.3.4. Polynomials of Degree Exactly n

Let R be a commutative ring and $n \in \mathbb{N}$. The set of **polynomials of degree exactly n** is $R[x]_{=n} := \{p \in R[x] : \deg p = n\}$.

The second description also counts these sets over a finite ring. Over $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$, whose elements are $0, 1, 2$ (Number Systems: From $\mathbb{N}$ to $\mathbb{N}R$), Theorem 3.4.3 (b)), $\mathbb{F}_3[x]_{\leq 1}$ consists of the polynomials $a_0 + a_1x$, and distinct pairs (a_0, a_1) give distinct polynomials, since a_0 and a_1 are the coefficients (Proposition 4.2.1). So it has $3 \cdot 3 = 9$ elements, one for each pair. Those in $\mathbb{F}_3[x]_{=1}$ are the ones with $a_1 \neq 0$: $x, x+1, x+2, 2x, 2x+1, 2x+2$, that is $3 \cdot 2 = 6$ of them. The remaining 3 are the constants $0, 1, 2$.

Example. Comparing the Two Sets

Decide whether each of $x^2 + 1$, $3x - 2$ and 0 lies in $\mathbb{Q}[x]_{\leq 2}$ and in $\mathbb{Q}[x]_{=2}$. Then express $R[x]_{\leq n}$ through $R[x]_{=n}$ and $R[x]_{\leq n-1}$ for $n \geq 1$, and decide whether $\mathbb{Q}[x]_{=2}$ is closed under addition.

Solution. $x^2 + 1$ has degree 2, so it lies in both sets. $3x - 2$ has degree 1: it lies in $\mathbb{Q}[x]_{\leq 2}$ but not in $\mathbb{Q}[x]_{=2}$. The zero polynomial has degree $-\infty$: it lies in $\mathbb{Q}[x]_{\leq 2}$ and not in $\mathbb{Q}[x]_{=2}$.

For $n \geq 1$, a polynomial of degree at most n has degree exactly n or degree at most $n - 1$, and not both, so

$$R[x]_{\leq n} = R[x]_{=n} \cup R[x]_{\leq n-1}, \quad R[x]_{=n} \cap R[x]_{\leq n-1} = \emptyset.$$

$\mathbb{Q}[x]_{=2}$ is **not** closed under addition: $x^2 + x$ and $-x^2 + 1$ both have degree 2, and their sum $x + 1$ has degree 1. It does not contain 0 either. In the linear-algebra companion, the first of the two sets is a subspace of the space of polynomials and the second is not, for exactly these two reasons.

4.3.7 Exercises

4.3.7.1 A. Check your understanding

Exercise. A1

- In the proof of Theorem 4.3.2, where is the hypothesis “ R has no zero divisors” used?
- Run the proof of Theorem 4.3.2 (a) on $p = 2x + 1$ and $q = 3x^2 + x$, once over $\mathbb{Z}$ and once over $\mathbb{Z}/6\mathbb{Z}$: what is $m + n$, and which element is $(pq)_{m+n}$?
- True or false: $\deg(p + q) = \max(\deg p, \deg q)$ for all $p, q \in \mathbb{Q}[x]$. Justify your answer.
- Give the idea of the proof of Theorem 4.3.2 in two sentences.
- For which $n \geq 2$ is $(\mathbb{Z}/n\mathbb{Z})[x]$ an integral domain?

Solution.

- Only in (b), to conclude that $\text{lc}(p)\text{lc}(q) \neq 0$ from $\text{lc}(p) \neq 0$ and $\text{lc}(q) \neq 0$. Part (a), the

vanishing above $m + n$ and the value at $m + n$, holds in every commutative ring.

- (b) $m = 1, n = 2, m + n = 3$, and $(pq)_3 = p_1q_2 = 2 \cdot 3$: over $\mathbb{Z}$ this is $6 \neq 0$, so $\deg(pq) = 3$; over $\mathbb{Z}/6\mathbb{Z}$ it is $[6] = [0]$, so $\deg(pq) < 3$ (in fact 2, by the warning after the theorem).
- (c) False: $p = x, q = -x$ give $p + q = 0$, of degree $-\infty$, while $\max(\deg p, \deg q) = 1$. Equality is only guaranteed when $\deg p \neq \deg q$ ([Theorem 4.3.1](#)).
- (d) In the k -th coefficient of pq with $k \geq m + n$, every term but p_mq_n has a factor beyond the top of p or of q , hence vanishes. So the product's top is the product of the tops, and the degree formula holds exactly when that one product in R is non-zero.
- (e) Exactly for n prime. If n is prime, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain ([Example \(Which Rings Are Integral Domains\)](#)), so $(\mathbb{Z}/n\mathbb{Z})[x]$ is one by [Corollary 4.3.3](#) (a). If n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain ([Example \(Which Rings Are Integral Domains\)](#)), so $(\mathbb{Z}/n\mathbb{Z})[x]$ is not one by [Corollary 4.3.3](#) (c).

4.3.7.2 B. Practice

Exercise. B1: Put the proof in order

Below are eight lines. Six of them, in a suitable order, form a proof of [Corollary 4.3.3](#) (a), “if R is an integral domain and $pq = 0$ in $R[x]$, then $p = 0$ or $q = 0$ ”; two are distractors. Write an admissible order, say which other orders are admissible, and say why each distractor fails.

- (i) R has no zero divisors, so $p_mq_n \neq 0$.
- (ii) By contraposition, $pq = 0$ implies $p = 0$ or $q = 0$.
- (iii) Let $m := \deg p$ and $n := \deg q$, so $p_m \neq 0$ and $q_n \neq 0$.
- (iv) $(pq)_{m+n} = \sum_{i=0}^{m+n} p_iq_{m+n-i}$, and this is non-zero because each of its terms is non-zero.
- (v) Hence pq has a non-zero coefficient, so $pq \neq 0$.
- (vi) Suppose $p \neq 0$ and $q \neq 0$.
- (vii) By [Theorem 4.3.2](#) (a), $(pq)_{m+n} = p_mq_n$.
- (viii) $p_mq_n \neq 0$ because R is a commutative ring.

Solution. An admissible order is (vi), (iii), (vii), (i), (v), (ii). Line (vi) must come first: it introduces the assumptions that m and n need (the degree of the zero polynomial is $-\infty$, not a position). Line (iii) must come before (vii) and (i), which use m, n, p_m, q_n . Lines (vii) and (i) do not use each other, so they may come in either order; both must precede (v), which combines them. Line (ii) closes the contrapositive and comes last. So the admissible orders are exactly

$$\begin{aligned} & \text{(vi), (iii), (vii), (i), (v), (ii) and} \\ & \text{(vi), (iii), (i), (vii), (v), (ii).} \end{aligned}$$

Line (iv) fails twice: the terms p_iq_{m+n-i} with $i \neq m$ are 0, not non-zero, and even a sum of non-zero terms can be 0 ($1 + (-1) = 0$). Line (viii) gives a false reason: in the commutative ring $\mathbb{Z}/6\mathbb{Z}$, $[2] \neq [0]$ and $[3] \neq [0]$ but $[2][3] = [0]$. The hypothesis that does the work is “no zero divisors”, which is line (i).

Exercise. B2: Units in polynomial rings

- (a) Show that for **every** commutative ring R , each unit of R is a unit of $R[x]$: $R^\times \subseteq (R[x])^\times$.
- (b) Find the inverse of $1 + [3]x$ in $(\mathbb{Z}/9\mathbb{Z})[x]$.
- (c) Show that $1 + [2]x + [2]x^2$ is a unit of $(\mathbb{Z}/4\mathbb{Z})[x]$.

Hint: in (b), what is $[3]^2$ in $\mathbb{Z}/9\mathbb{Z}$?

Solution.

- (a) The second paragraph of the proof of [Proposition 4.3.4](#) uses nothing about R beyond Theorem 4.2.4 (b): if $ab = 1$ in R , then $(ax^0)(bx^0) = (ab)x^0 = 1x^0$, which is the one of $R[x]$.
- (b) By the product formula, $(1 + [3]x)(1 - [3]x)$ has coefficients 1 , $[3] - [3] = [0]$ and $-[3][3] = -[9] = [0]$, so it equals 1 . Since $-[3] = [6]$, the inverse is $1 + [6]x$. (It is unique by Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Definition 3.5.1.)
- (c) Let $p := 1 + [2]x + [2]x^2$, with coefficients $1, [2], [2]$. The coefficients of $p^2 = pp$ are, by the product formula,

$$\begin{aligned} (p^2)_0 &= 1, & (p^2)_1 &= [2] + [2] = [4], \\ (p^2)_2 &= [2] + [4] + [2] = [8], & (p^2)_3 &= [4] + [4] = [8], \end{aligned}$$

and $(p^2)_4 = [2][2] = [4]$. In $\mathbb{Z}/4\mathbb{Z}$, $[4] = [8] = [0]$, so $p^2 = 1$, and p is a unit, its own inverse. Again $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, and [Proposition 4.3.4](#) does not apply.

Exercise. B3: Counting polynomials over a finite field

Let p be a prime and $n \in \mathbb{N}$. How many elements do $\mathbb{F}_p[x]_{\leq n}$ and $\mathbb{F}_p[x]_{=n}$ have?

Hint: Exercise (B1: Polynomials of bounded length as tuples).

Solution. Since $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has the p elements $0, 1, \dots, p-1$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.4.3 (b)), the non-zero elements $1, \dots, p-1$ form a set with $p-1$ elements.

At most n . By the description after [Definition 4.3.3](#), $\mathbb{F}_p[x]_{\leq n}$ is the set of polynomials q with $q_k = 0$ for every $k > n$. By Exercise (B1: Polynomials of bounded length as tuples) with $N = n$, $q \mapsto (q_0, \dots, q_n)$ is a bijection from this set onto $\mathbb{F}_p^{n+1}$ (for $n = 0$, with $\mathbb{F}_p^1$ read as $\mathbb{F}_p$, as there). A tuple $(a_0, \dots, a_n)$ is the same as the function $\{1, \dots, n+1\} \rightarrow \mathbb{F}_p$, $i \mapsto a_{i-1}$, so by Sets, Relations, and Cardinality, Exercise (C2: Counting products and functions) (b) there are p^{n+1} of them. So $\mathbb{F}_p[x]_{\leq n}$ has p^{n+1} elements.

Exactly n . The same bijection maps $\mathbb{F}_p[x]_{=n}$ onto the tuples $(a_0, \dots, a_n)$ with $a_n \neq 0$: such a tuple is a pair of an arbitrary $(a_0, \dots, a_{n-1})$, p^n choices as before, and a non-zero a_n , $p-1$ choices. By Sets, Relations, and Cardinality, Exercise (C2: Counting products and functions) (a), there are $(p-1)p^n$ of them. (For $n = 0$ these are the $p-1$ non-zero constants,

and $(p-1)p^0 = p-1$.) For example, over $\mathbb{F}_2$ there are $2^3 = 8$ polynomials of degree at most 2 and $1 \cdot 2^2 = 4$ of degree exactly 2.

4.3.7.3 C. Going deeper

Exercise. C1: Exit check: polynomial rings over integral domains

Let R be a commutative ring. Prove [Theorem 4.3.2](#) (a) and (b) (for (b), the equivalence, the leading coefficient, and the case of no zero divisors), and then prove [Corollary 4.3.3](#) (a) and (c).

Solution. Degree of a product. Let $p, q \neq 0$, $m = \deg p$, $n = \deg q$, so $p_m \neq 0$, $q_n \neq 0$, and $p_i = 0$ for $i > m$, $q_j = 0$ for $j > n$. Let $k \geq m+n$ and $0 \leq i \leq k$. If $i > m$, then $p_i = 0$. If $i \leq m$, then $k-i \geq n$, with equality only when $k = m+n$ and $i = m$; otherwise $q_{k-i} = 0$. So for $k > m+n$ every term $p_i q_{k-i}$ of $(pq)_k$ is 0 (Number Systems: From $\setminus(\setminus n \mathbb{N} \setminus)$ to $\setminus(\setminus n \mathbb{R} \setminus)$, Proposition 2.3.2 (b) with (F6)), and $(pq)_k = 0$; for $k = m+n$, every term with $i \neq m$ is 0, and the sum is $p_m q_n$ by $(\Sigma 3)$ of Lemma 4.1.1. Hence $\deg(pq) \leq m+n$ when $pq \neq 0$, and trivially when $pq = 0$; if $p = 0$ or $q = 0$, then $pq = 0$ and both sides are $-\infty$.

If $p_m q_n \neq 0$, then pq has a non-zero coefficient at $m+n$ and none beyond, so $\deg(pq) = m+n$ and $\text{lc}(pq) = p_m q_n$. If $p_m q_n = 0$, all coefficients from $m+n$ on vanish, and $\deg(pq) < m+n$.

No zero divisors. Let R be an integral domain and $p, q \neq 0$. Then $p_m q_n \neq 0$, since R has no zero divisors, so pq has a non-zero coefficient and $pq \neq 0$. Contraposition gives (a); with $R[x]$ a commutative ring (Theorem 4.2.4 (a)) and $1x^0 \neq 0x^0$ because $1 \neq 0$ in R , $R[x]$ is an integral domain.

The converse. Let $R[x]$ be an integral domain. If $1 = 0$ in R , the one $1x^0$ of $R[x]$ is the zero polynomial, a contradiction. If $ab = 0$ in R , then $(ax^0)(bx^0) = (ab)x^0 = 0$ (Lemma 4.2.2 (b)), so one factor is the zero polynomial, and its only possibly non-zero coefficient, a or b , is 0.

Marking scheme. (10 points)

- 3: shows that every coefficient of pq above $m+n$ vanishes, treating both cases $i > m$ and $i \leq m$ of the index argument, and the case $p = 0$ or $q = 0$ of the inequality.
- 2: shows that $(pq)_{m+n} = \text{lc}(p)\text{lc}(q)$, with the other terms of that coefficient shown to be 0.
- 1: derives $\deg(pq) = \deg p + \deg q$ and $\text{lc}(pq) = \text{lc}(p)\text{lc}(q)$ from $\text{lc}(p)\text{lc}(q) \neq 0$, and that this holds when R has no zero divisors.
- 1: shows the converse direction of the equivalence: $\text{lc}(p)\text{lc}(q) = 0$ gives $\deg(pq) < m+n$.
- 2: concludes that $R[x]$ has no zero divisors and $1 \neq 0$ in $R[x]$.
- 1: proves the converse through the constants.

Fatal errors (0 for the step): “the leading term of pq is $\text{lc}(p)\text{lc}(q)x^{m+n}$ ” without showing that the other terms of the $(m+n)$ -th coefficient vanish; using $\deg(pq) = \deg p + \deg q$ in an arbitrary commutative ring. A proof through the **lowest** non-zero coefficients (as in the repair of [Exercise \(C2: Find the error\)](#)) earns the same points for (a) of the corollary, with the index argument mirrored.

Exercise. C2: Find the error

Here is an argument.

Claim. If R is an integral domain, then $R[x]$ has no zero divisors.

Proof. Let $p, q \in R[x]$ be non-zero. (1) Then $p_0 \neq 0$ and $q_0 \neq 0$. (2) The constant term of pq is $(pq)_0 = p_0q_0$. (3) Since R has no zero divisors, $p_0q_0 \neq 0$. (4) So $pq \neq 0$.

Is the claim true? Does the argument prove it? If not, name the first line that fails, say why, give a counterexample to that step, and repair the proof.

Solution. The claim is true: it is [Corollary 4.3.3](#) (a). The argument does not prove it.

The failing line is (1). A non-zero polynomial may have constant term 0: $p = x$ is non-zero, with $p_0 = 0$. That is a counterexample to the step from “ $p \neq 0$ ” to “ $p_0 \neq 0$ ”. The step generalizes from the constants, where it is true, to all polynomials, where no result supports it: it cites a general “fact” that is neither proved nor true, entry (N9) of Logic and Proof, Example (What is not allowed). Lines (2), (3) and (4) are correct: (2) is the product formula at $k = 0$, and (3), (4) follow once (1) is granted.

Two repairs. The book’s repair looks at the **top** coefficients: with $m = \deg p$, $n = \deg q$, [Theorem 4.3.2](#) (a) gives $(pq)_{m+n} = p_mq_n \neq 0$.

The argument can also be repaired at the **bottom**. Let i_0 and j_0 be the least indices with $p_{i_0} \neq 0$ and $q_{j_0} \neq 0$; they exist because the sets of non-zero positions are non-empty subsets of $\mathbb{N}$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 2.3.6, bounded below by 0). In $(pq)_{i_0+j_0} = \sum_{i=0}^{i_0+j_0} p_iq_{i_0+j_0-i}$, a term with $i < i_0$ has $p_i = 0$, and a term with $i > i_0$ has $i_0 + j_0 - i < j_0$, so $q_{i_0+j_0-i} = 0$. By $(\Sigma 3)$, $(pq)_{i_0+j_0} = p_{i_0}q_{j_0}$, which is non-zero since R has no zero divisors. So $pq \neq 0$. This is the index argument of [Theorem 4.3.2](#), mirrored.