

5.1 Division with Remainder

Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Section 3.1 divided -17 by 5 and kept the remainder 3 : a quotient times the divisor, plus something **smaller** than the divisor. Chapter 4 built the ring $F[x]$ of polynomials over a field and gave every non-zero polynomial a degree. For polynomials, “smaller” will mean “of smaller degree”. For instance, in $\mathbb{Q}[x]$,

$$x^4 + 2x^3 - x + 3 = (x^2 + x)(x^2 + x - 1) + 3,$$

and the leftover 3 has degree 0 , below the degree 2 of $x^2 + x - 1$. Three questions are open. Why can one always go on until the degree drops below that of the divisor? Why is the answer unique? And where does it matter that the coefficients lie in a **field**? This section answers all three, and then uses the answer to connect a root of a polynomial with a factor of degree 1 .

Throughout the chapter, F is a field (Definition 2.1.1), and $F[x]$ is the ring of polynomials over F (Definition 4.2.1), a commutative ring by Theorem 4.2.4 (a). A field is an integral domain (Example (Which Rings Are Integral Domains)), so the results of Chapter 4 stated for integral domains apply to $F[x]$. We use the degree $\deg p$ and the leading coefficient $\text{lc}(p)$ of Definition 4.3.1, with $\deg 0 = -\infty$, and the conventions $-\infty < n$ and $-\infty + n = -\infty$ for $n \in \mathbb{N}$ that come with it. A constant $a \in F$ is identified with the polynomial ax^0 (Theorem 4.2.4 (b)), and $(ap)_k = ap_k$ for a constant a (Theorem 4.2.4 (d)). Numerals in F are multiples of 1 : $2 := 1 + 1$, $3 := 2 + 1$, and so on, so that $2 = 0$ in $\mathbb{F}_2$ and $3 = 0$ in $\mathbb{F}_3$ (Definition 2.2.1).

5.1.1 Divisibility over a field

In $\mathbb{Z}$, “ a divides b ” asked whether b is some integer times a . The same question makes sense in any commutative ring, and in $F[x]$ it is the question this chapter is built on. The one new feature is that the answer can depend on the field.

A polynomial g divides f when f is g times some polynomial over the same field.

Definition 5.1.1. Divisibility of Polynomials

Let F be a field and $f, g \in F[x]$.

- (a) g **divides** f **over** F , written $g \mid f$, if **there exists** $h \in F[x]$ with $f = gh$. Then g is a **divisor** (or **factor**) of f , and f is a **multiple** of g . We write $g \nmid f$ when g does not divide f .
- (b) f and g are **associates** if $f = cg$ for some **non-zero** constant $c \in F$.

In words: (a) asks for a cofactor h , and the cofactor must have its coefficients in F ; (b) says that two polynomials are associates when they differ by a non-zero constant factor. When two fields are in play, “ $g \mid f$ in $F[x]$ ” names the field.

Four instances, chosen so that the same symbols give different answers:

- $x - 1 \mid x^2 - 1$ in $\mathbb{Q}[x]$, since $x^2 - 1 = (x - 1)(x + 1)$.
- $2x - 2 \mid x^2 - 1$ in $\mathbb{Q}[x]$, since $x^2 - 1 = (2x - 2)(\frac{1}{2}x + \frac{1}{2})$. The polynomials $x - 1$ and $2x - 2 = 2(x - 1)$ are associates, and the cofactor $\frac{1}{2}x + \frac{1}{2}$ needs the inverse of 2 .
- $x + 1 \mid x^2 + 1$ in $\mathbb{F}_2[x]$, since $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ there: $2 = 0$ in $\mathbb{F}_2$.
- $x + 1 \nmid x^2 + 1$ in $\mathbb{Q}[x]$. Suppose $x^2 + 1 = (x + 1)h$ with $h \in \mathbb{Q}[x]$. Evaluating at -1 respects sums and products (Theorem 4.4.1), so $(-1)^2 + 1 = (-1 + 1) \cdot h(-1)$, that is, $2 = 0 \cdot h(-1) = 0$ in $\mathbb{Q}$, which is false.

Non-example by minimal change. The last two lines use the same symbols, $x + 1$ and $x^2 + 1$. Only the field changed, from $\mathbb{F}_2$ to $\mathbb{Q}$, and with it the value of 2: the evaluation argument gives $2 = 0$, which is true in $\mathbb{F}_2$ and false in $\mathbb{Q}$. So “ $g \mid f$ ” is a statement about g , f **and** F , which is why the definition says “over F ”.

Degenerate cases. Every g divides 0, since $0 = g \cdot 0$. The zero polynomial divides only 0. And a non-zero constant c divides every f , since $f = c(c^{-1}f)$; this is (F8), inverses of non-zero elements, at work in general (the cofactor of $2x - 2$ above was one instance), and it means that non-zero constants are as invisible to divisibility as ± 1 were in $\mathbb{Z}$.

Quick check. In $\mathbb{F}_3[x]$, does $x + 1$ divide $x^2 + 1$? Evaluate at $-1 = 2$.

Solution. No. If $x^2 + 1 = (x + 1)h$, evaluating at 2 (Theorem 4.4.1) gives $2^2 + 1 = (2 + 1)h(2)$, that is, $5 = 0 \cdot h(2) = 0$. In $\mathbb{F}_3$, $5 = 2 \neq 0$. So $x + 1 \nmid x^2 + 1$ in $\mathbb{F}_3[x]$.

The rules below are the ones the chapter uses. Parts (a)–(d) are identities in the commutative ring $F[x]$, plus the inverse of a non-zero constant (F8) for the last clause of (a) and one degree count; parts (e) and (f) say exactly what “invisible” means.

Proposition 5.1.1. Rules for Divisibility of Polynomials

Let F be a field and $f, g, h \in F[x]$.

- (a) $g \mid 0$. $0 \mid f$ if and only if $f = 0$. Every non-zero constant divides every polynomial.
- (b) If $f \mid g$ and $g \mid h$, then $f \mid h$.
- (c) If $h \mid f$ and $h \mid g$, then $h \mid af + bg$ for **all** $a, b \in F[x]$.
- (d) If $g \mid f$ and $f \neq 0$, then $\deg g \leq \deg f$.
- (e) The units of $F[x]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1) are exactly the non-zero constants.
- (f) $f \mid g$ and $g \mid f$ if and only if f and g are associates (this includes $f = g = 0$). Every non-zero f has **exactly one** monic associate, namely $\text{lc}(f)^{-1}f$. Two monic polynomials that divide each other are equal.

Idea. Parts (a)–(c) are rearrangements of equations $f = gh$ by the ring laws, except that the last clause of (a) also uses c^{-1} , from (F8). Part (d) is the degree of a product: a non-zero multiple of g has degree $\deg g$ plus something in $\mathbb{N}$. Part (e) is Chapter 4’s description of the units of $R[x]$, read with $R = F$. For (f), mutual divisibility gives $f = f \cdot uv$, and canceling f makes u a unit, which (e) identifies as a non-zero constant.

Proof. We use the ring laws of $F[x]$ (Theorem 4.2.4 (a)) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 without further mention.

- (a) $0 = g \cdot 0$, so $g \mid 0$. If $0 \mid f$, then $f = 0 \cdot k = 0$ for some k ; conversely $0 \mid 0$ by the first claim. If $c \in F$ is a non-zero constant, then c^{-1} exists by (F8) of Definition 2.1.1, and $f = (cc^{-1})f = c(c^{-1}f)$, so $c \mid f$.

- (b) Let $g = fu$ and $h = gv$. Then $h = (fu)v = f(uv)$, so $f \mid h$.
- (c) Let $f = hu$ and $g = hv$. Then $af + bg = a(hu) + b(hv) = h(au + bv)$, so $h \mid af + bg$.
- (d) Let $f = gu$ with $u \in F[x]$. Since $f \neq 0$, neither g nor u is 0. The field F has no zero divisors (Theorem 2.1.1 (f)), so Theorem 4.3.2 (b) gives $\deg f = \deg g + \deg u$. Here $\deg u \in \mathbb{N}$, so $\deg g \leq \deg f$.
- (e) By Proposition 4.3.4, applied to the integral domain F (Example (Which Rings Are Integral Domains)), the units of $F[x]$ are the constants that are units of F . In a field every non-zero a is a unit, by (F8), and 0 is not, since $0 \cdot v = 0 \neq 1$ for every v (Theorem 2.1.1 (d) and (F7) of Definition 2.1.1). So the units of $F[x]$ are the non-zero constants.
- (f) ($\Leftarrow$) Let $f = cg$ with $c \neq 0$ a constant. Then $g \mid f$, and $g = c^{-1}f$, so $f \mid g$.

($\Rightarrow$) Let $f \mid g$ and $g \mid f$. If $f = 0$, then $0 \mid g$, so $g = 0$ by (a), and $f = 1 \cdot g$. Otherwise write $g = fu$ and $f = gv$. Then $f = fuv$, so $f(1 - uv) = 0$. Since $f \neq 0$, Corollary 4.3.3 (a) gives $1 - uv = 0$, that is, $uv = 1$. So v is a unit of $F[x]$, hence a non-zero constant by (e), and $f = vg$: f and g are associates.

The monic associate. Let $f \neq 0$ and $a := \text{lc}(f) \neq 0$. The polynomial $a^{-1}f$ has the coefficients $a^{-1}f_k$ (Theorem 4.2.4 (d)). These vanish exactly where the f_k do, since $a^{-1} \neq 0$ (as $a \cdot 0 = 0 \neq 1 = aa^{-1}$, by Theorem 2.1.1 (d), (F7), (F8)) and F has no zero divisors, so $\deg(a^{-1}f) = \deg f$ and $\text{lc}(a^{-1}f) = a^{-1}a = 1$. If also cf is monic for a constant $c \neq 0$, the same computation gives $\text{lc}(cf) = ca = 1$, so $c = a^{-1}$ (uniqueness of inverses, Theorem 2.1.1 (c)). So $a^{-1}f$ is the only monic associate of f .

Monic and mutually dividing. Let f, g be monic with $f \mid g$ and $g \mid f$. By what we proved, $f = cg$ with a non-zero constant c , and comparing leading coefficients, $1 = \text{lc}(f) = c \text{lc}(g) = c$. So $f = g$. This proves the proposition. ■

Parts (e) and (f) are the polynomial form of a fact about $\mathbb{Z}$: in Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (f) and (g), the units of $\mathbb{Z}$ were ± 1 , and two **positive** integers that divide each other are equal. In $F[x]$ the units are the non-zero constants, and the role of “positive” is played by “monic”: among the associates of a non-zero polynomial, exactly one is monic. So whenever a polynomial is to be singled out from its associates, it is made monic.

The hypothesis $f \neq 0$ in (d) cannot be dropped: $x^5 \mid 0$, and $\deg x^5 = 5 > -\infty = \deg 0$.

Quick check. In $\mathbb{Q}[x]$, list the associates of $3x + 6$ that have integer coefficients and leading coefficient between -3 and 3 . Which one is monic?

Solution. The associates are $c(3x + 6)$ with $c \in \mathbb{Q}$, $c \neq 0$; the leading coefficient is $3c$. Leading coefficients $\pm 1, \pm 2, \pm 3$ give $\pm(x + 2)$, $\pm(2x + 4)$, $\pm(3x + 6)$, all with integer coefficients. The monic one is $x + 2 = \frac{1}{3}(3x + 6)$.

5.1.2 Division with remainder

Now the theorem. The tool is the one *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.1 used for integers, with degree in place of size: among all $f - hg$, take one of **least degree**, and show that its degree is below $\deg g$.

Theorem 5.1.2. Division with Remainder in $F[x]$

Let F be a field, and let $f, g \in F[x]$ with $g \neq 0$.

(a) There are **unique** $q, r \in F[x]$ with

$$f = qg + r \quad \text{and} \quad \deg r < \deg g.$$

(b) $g \mid f$ if and only if $r = 0$.

The polynomials q and r are the **quotient** and the **remainder** of f on division by g .

Since $\deg 0 = -\infty < \deg g$, the remainder $r = 0$ is allowed.

Idea. Look at all polynomials $f - hg$, $h \in F[x]$. If 0 is among them, f is a multiple of g and we are done. Otherwise their degrees are natural numbers, and well-ordering gives one, r , of least degree n . If $n \geq \deg g$, we can kill the leading term of r by subtracting a constant times a power of x times g : the constant is $\text{lc}(r)\text{lc}(g)^{-1}$, and that inverse is where the field is needed. The result is again of the form $f - hg$ and has smaller degree, against the choice of r . Uniqueness: two answers give $(q - q')g = r' - r$, and a non-zero multiple of g cannot have degree below $\deg g$. We call this move **compare degrees**.

Proof.

(a) *Existence.* Let $m := \deg g \in \mathbb{N}$ and $b := \text{lc}(g) \neq 0$, and let

$$S := \{f - hg : h \in F[x]\}.$$

If $0 \in S$, say $0 = f - qg$, then $r := 0$ and this q satisfy $f = qg + r$ and $\deg r = -\infty < m$. Suppose $0 \notin S$. Then every element of S has a degree in $\mathbb{N}$, and $D := \{\deg s : s \in S\} \subseteq \mathbb{N}$ is non-empty, since $f = f - 0 \cdot g \in S$. By the well-ordering of $\mathbb{N}$ (Sets, Relations, and Cardinality, Theorem 2.1.3; on $\mathbb{N} = \omega$ it is Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Theorem 1.6.2), D has a least element n . Choose $q \in F[x]$ with $r := f - qg$ of degree n , and let $a := \text{lc}(r) \neq 0$.

Suppose $n \geq m$. Let $t := (ab^{-1})x^{n-m}$, a monomial with $n - m \in \mathbb{N}$ and non-zero coefficient ab^{-1} : $b^{-1} \neq 0$, since $b \cdot 0 = 0 \neq 1 = bb^{-1}$ (Theorem 2.1.1 (d), (F7), (F8)), so $ab^{-1} \neq 0$ by Theorem 2.1.1 (f). Then $\deg t = n - m$ and $\text{lc}(t) = ab^{-1}$, so by Theorem 4.3.2 (b), tg has degree $(n - m) + m = n$ and leading coefficient $ab^{-1}b = a$. Let

$$r_1 := r - tg = f - (q + t)g,$$

an element of S . By Theorem 4.3.1 (with $\deg(-p) = \deg p$ for every p , since $(-p)_k = -p_k$), $\deg r_1 \leq \max(\deg r, \deg tg) = n$, and the coefficient of x^n in r_1 is $a - a = 0$. So $\deg r_1 < n$ (or $r_1 = 0$). But $r_1 \neq 0$, since $0 \notin S$, and then $\deg r_1 \in D$ is smaller

than the least element n of D . This contradiction shows $n < m$. So $f = qg + r$ with $\deg r < \deg g$.

Uniqueness. Let $f = qg + r = q'g + r'$ with $\deg r < m$ and $\deg r' < m$. Then

$$(q - q')g = r' - r,$$

and $\deg(r' - r) \leq \max(\deg r', \deg r) < m$ by Theorem 4.3.1 (using $\deg(-r) = \deg r$ as above). If $q \neq q'$, then Theorem 4.3.2 (b) gives $\deg((q - q')g) = \deg(q - q') + m \geq m$, a contradiction. So $q = q'$, hence $r' - r = 0 \cdot g = 0$ and $r = r'$.

- (b) ($\Leftarrow$) If $r = 0$, then $f = qg$, so $g \mid f$. ($\Rightarrow$) If $f = hg$, then $f = hg + 0$ with $\deg 0 < \deg g$ is a division with remainder; by the uniqueness in (a), $r = 0$. This proves the theorem. ■

The field is used in two places. The first is the inverse b^{-1} of the leading coefficient of g , which builds the monomial t . The second is the degree of a product, in $\deg(tg) = n$ and in the uniqueness: Theorem 4.3.2 (b) needs the product of the leading coefficients to be non-zero, and a field has no zero divisors. The hypothesis $g \neq 0$ is needed as well: for $g = 0$ no r has $\deg r < -\infty$.

The existence proof is also a procedure. Each pass replaces r by $r - tg$, which removes the leading term of r , and the degree drops by at least one. Starting from f , at most $\deg f - \deg g + 1$ passes are needed when $\deg f \geq \deg g$, and none when $\deg f < \deg g$: then $q = 0$ and $r = f$. This is the long division of school algebra, now with a proof that it stops and that its answer is the only one. Chapter 4 did not divide polynomials with remainder, so this is where the volume first does it. Its integer twin is Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.1.2, whose least-element proof the one above follows.

Example. Long division in two fields

- (i) In $\mathbb{Q}[x]$, divide $f = 2x^4 - 3x^3 + x^2 + 4x - 1$ by $g = 2x^2 - x + 3$.
 (ii) In $\mathbb{F}_3[x]$, divide $f = x^4 + x + 2$ by $g = 2x^2 + 1$.

Solution.

- (i) Here $\text{lc}(g) = 2$, with inverse $\frac{1}{2}$. Each pass subtracts tg , where t is the leading term of the current remainder divided by $2x^2$:

$$\begin{aligned} f - x^2g &= -2x^3 - 2x^2 + 4x - 1, \\ (-2x^3 - 2x^2 + 4x - 1) - (-x)g &= -3x^2 + 7x - 1, \\ (-3x^2 + 7x - 1) - (-\tfrac{3}{2})g &= \tfrac{11}{2}x + \tfrac{7}{2}. \end{aligned}$$

The last line has degree $1 < 2$, so we stop. Adding up the t 's,

$$2x^4 - 3x^3 + x^2 + 4x - 1 = (x^2 - x - \tfrac{3}{2})(2x^2 - x + 3) + \tfrac{11}{2}x + \tfrac{7}{2}.$$

Check: $(x^2 - x - \frac{3}{2})(2x^2 - x + 3) = 2x^4 - 3x^3 + x^2 - \frac{3}{2}x - \frac{9}{2}$, and adding $\frac{11}{2}x + \frac{7}{2}$ gives f .

- (ii) In $\mathbb{F}_3$, $2 \cdot 2 = 4 = 1$, so $\text{lc}(g)^{-1} = 2^{-1} = 2$. The first t is $1 \cdot 2 \cdot x^2 = 2x^2$, and

$2x^2 \cdot g = 4x^4 + 2x^2 = x^4 + 2x^2$. The second t is 2, and $2g = 4x^2 + 2 = x^2 + 2$:

$$\begin{aligned} f - 2x^2g &= -2x^2 + x + 2 = x^2 + x + 2, \\ (x^2 + x + 2) - 2g &= x. \end{aligned}$$

So $x^4 + x + 2 = (2x^2 + 2)(2x^2 + 1) + x$ in $\mathbb{F}_3[x]$. Check: $(2x^2 + 2)(2x^2 + 1) = 4x^4 + 6x^2 + 2 = x^4 + 2$ in $\mathbb{F}_3$, and adding x gives f .

Quick check. Find two different pairs (q, r) with $x^2 = q(x^2 + 1) + r$ in $\mathbb{Q}[x]$ and $\deg r \leq 2$. Which condition in part (a) of the theorem does the second one fail?

Solution. $(q, r) = (1, -1)$: $1 \cdot (x^2 + 1) - 1 = x^2$, with $\deg(-1) = 0 < 2$. And $(q, r) = (0, x^2)$: $0 \cdot (x^2 + 1) + x^2 = x^2$, with $\deg r = 2$. The second fails $\deg r < \deg g = 2$. Uniqueness holds only among remainders of degree **strictly** below that of the divisor; $(1, -1)$ is the quotient and remainder.

Warning. Division with remainder needs the leading coefficient of the divisor to be invertible. Take the polynomials in $\mathbb{Q}[x]$ all of whose coefficients lie in $\mathbb{Z}$, and try to divide x^2 by $2x$ **among them**: $x^2 = q \cdot 2x + r$ with $\deg r < 1$. Comparing the coefficients of x^2 gives $1 = 2q_1$ (Lemma 4.2.2 (a)), and no integer q_1 satisfies it, since 1 is odd (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.1.3 (a)). In $\mathbb{Q}[x]$ there is no problem: $x^2 = \frac{1}{2}x \cdot 2x + 0$. Exercise C1 shows that integer coefficients are kept when the divisor is monic.

5.1.3 Roots and factors of degree one

Division by a polynomial of degree 1 has a remainder of degree at most 0, that is, a constant. Which constant? Evaluate: the divisor $x - c$ vanishes at c , so the quotient term disappears and the remainder is read off. We call this move **evaluate at a root**.

Theorem 5.1.3. Remainder Theorem and Factor Theorem

Let F be a field, $f \in F[x]$ and $c \in F$.

- (a) The remainder of f on division by $x - c$ is the constant $f(c)$.
- (b) c is a root of f if and only if $x - c \mid f$.
- (c) f has a factor of degree 1 in $F[x]$ if and only if f has a root in F .

Idea. Divide by $x - c$ and evaluate at c : the term with the quotient vanishes, and what is left is the remainder. Part (b) is then the divisibility test of Theorem 5.1.2 (b), and for (c) a factor $ax + b$ of degree 1 is made monic, which turns it into some $x - c$.

Proof.

- (a) The polynomial $x - c$ is non-zero, of degree 1 and monic. By [Theorem 5.1.2](#) (a), $f = q \cdot (x - c) + r$ with $\deg r < 1$, so r is a constant (possibly 0). Evaluation at c respects sums and products, sends x to c and a constant to itself ([Theorem 4.4.1](#)), so

$$f(c) = q(c) \cdot (c - c) + r = q(c) \cdot 0 + r = r.$$

- (b) By (a), $f = q \cdot (x - c) + f(c)$ is the division of f by $x - c$. By [Theorem 5.1.2](#) (b), $x - c \mid f$ if and only if this remainder is 0, that is, $f(c) = 0$.
- (c) ($\Leftarrow$) If $f(c) = 0$, then $x - c \mid f$ by (b), and $x - c$ has degree 1. ($\Rightarrow$) Let $ax + b \mid f$ with $a, b \in F$, $a \neq 0$. Then $ax + b = a(x - (-a^{-1}b))$, so $x - (-a^{-1}b) \mid ax + b$, and by [Proposition 5.1.1](#) (b), $x - (-a^{-1}b) \mid f$. By (b), $-a^{-1}b$ is a root of f . ■

Part (b) is the **factor theorem**, and it turns a question about values (is $f(c) = 0$?) into a question about divisibility. Part (c) turns the search for factors of degree 1 into a search for roots.

Example. Remainders without dividing

- (a) In $\mathbb{Q}[x]$, find the remainder of $f = x^5 - 3x^3 + 2x + 7$ on division by $x - 2$.
- (b) In $\mathbb{Q}[x]$, find the remainder of x^5 on division by $x^2 - x$.

Solution.

- (a) By [Theorem 5.1.3](#) (a), the remainder is

$$f(2) = 32 - 24 + 4 + 7 = 19.$$

- (b) The divisor $x^2 - x$ has degree 2, so the remainder has degree at most 1: $x^5 = q \cdot (x^2 - x) + ax + b$ with $a, b \in \mathbb{Q}$ ([Theorem 5.1.2](#) (a)). The divisor vanishes at 0 and at 1. Evaluating at both ([Theorem 4.4.1](#)),

$$0 = q(0) \cdot 0 + b, \quad 1 = q(1) \cdot 0 + a + b,$$

so $b = 0$ and $a = 1$. The remainder is x . Check: $x^5 - x = (x^2 - x)(x^3 + x^2 + x + 1)$.

Quick check. Without dividing, decide whether $x + 1$ divides $x^7 + 1$ in $\mathbb{Q}[x]$, and whether $x - 1$ does.

Solution. $x + 1 = x - (-1)$, and $(-1)^7 + 1 = -1 + 1 = 0$, so $x + 1 \mid x^7 + 1$ by [Theorem 5.1.3](#) (b). For $x - 1$, the remainder is $1^7 + 1 = 2 \neq 0$ in $\mathbb{Q}$, so $x - 1 \nmid x^7 + 1$. (Over $\mathbb{F}_2$, $2 = 0$ and both divide.)

Remark (Looking ahead). Section 5.5 builds, for any finite list of distinct points of F , the polynomial of least degree that takes prescribed values there. Exercise C2 below is the case of two points: the remainder of f on division by $(x - a)(x - b)$.

5.1.4 Exercises

5.1.4.1 A. Check your understanding

Exercise. A1

- (a) State [Theorem 5.1.2](#) with every hypothesis.
- (b) Name the two places in its proof where “ F is a field” is used.
- (c) Let $f \in F[x]$, and let $c \in F$ be a non-zero constant. What are the quotient and the remainder of f on division by c ?
- (d) True or false, with a reason: for $f, g \in \mathbb{Q}[x]$, if $f \mid g$ and $g \mid f$, then $f = g$. The same question in $\mathbb{F}_2[x]$.

Solution.

- (a) Let F be a field and $f, g \in F[x]$ with $g \neq 0$. Then there are unique $q, r \in F[x]$ with $f = qg + r$ and $\deg r < \deg g$; and $g \mid f$ if and only if $r = 0$.
- (b) The inverse $\text{lc}(g)^{-1}$, which builds the monomial $t = \text{lc}(r) \text{lc}(g)^{-1} x^{n-m}$; and the absence of zero divisors in F , through [Theorem 4.3.2 \(b\)](#), which gives $\deg(tg) = n$ and, in the uniqueness, $\deg((q - q')g) \geq \deg g$.
- (c) $q = c^{-1}f$ and $r = 0$: indeed $f = (c^{-1}f)c + 0$, and $\deg 0 = -\infty < 0 = \deg c$. By uniqueness this is the division.
- (d) In $\mathbb{Q}[x]$: false. $x \mid 2x$ and $2x \mid x$ ($x = \frac{1}{2} \cdot 2x$), but $x \neq 2x$. By [Proposition 5.1.1 \(f\)](#), mutual divisibility only makes f and g associates. In $\mathbb{F}_2[x]$: true. By (f), $f = cg$ with c a non-zero constant, and the only non-zero element of $\mathbb{F}_2$ is 1; so $f = g$.

5.1.4.2 B. Practice

Exercise. B1: Two long divisions

- (a) In $\mathbb{Q}[x]$, divide $x^4 - 3x^3 + 2x - 5$ by $3x^2 - 1$.
- (b) In $\mathbb{F}_5[x]$, divide $x^4 + 2x^3 + 3x + 1$ by $2x^2 + 3$, and decide whether $2x^2 + 3$ divides $x^4 + 2x^3 + 3x + 1$ in $\mathbb{F}_5[x]$.

Solution.

- (a) $\text{lc}(3x^2 - 1)^{-1} = \frac{1}{3}$. The passes subtract $\frac{1}{3}x^2$, $-x$ and $\frac{1}{9}$ times the divisor:

$$\begin{aligned} (x^4 - 3x^3 + 2x - 5) - \frac{1}{3}x^2(3x^2 - 1) &= -3x^3 + \frac{1}{3}x^2 + 2x - 5, \\ (-3x^3 + \frac{1}{3}x^2 + 2x - 5) + x(3x^2 - 1) &= \frac{1}{3}x^2 + x - 5, \\ (\frac{1}{3}x^2 + x - 5) - \frac{1}{9}(3x^2 - 1) &= x - \frac{44}{9}. \end{aligned}$$

So the quotient is $\frac{1}{3}x^2 - x + \frac{1}{9}$ and the remainder is $x - \frac{44}{9}$, of degree $1 < 2$. Check: $(3x^2 - 1)(\frac{1}{3}x^2 - x + \frac{1}{9}) = x^4 - 3x^3 + x - \frac{1}{9}$, and adding $x - \frac{44}{9}$ gives $x^4 - 3x^3 + 2x - 5$.

- (b) In $\mathbb{F}_5$, $2 \cdot 3 = 6 = 1$, so $2^{-1} = 3$. The passes subtract $3x^2$, x and 3 times the divisor, with $3x^2(2x^2 + 3) = x^4 + 4x^2$, $x(2x^2 + 3) = 2x^3 + 3x$ and $3(2x^2 + 3) = x^2 + 4$:

$$(x^4 + 2x^3 + 3x + 1) - (x^4 + 4x^2) = 2x^3 + x^2 + 3x + 1,$$

$$(2x^3 + x^2 + 3x + 1) - (2x^3 + 3x) = x^2 + 1,$$

$$(x^2 + 1) - (x^2 + 4) = 2,$$

using $-4 = 1$ and $-3 = 2$ in $\mathbb{F}_5$. So the quotient is $3x^2 + x + 3$ and the remainder is the constant 2. Since $2 \neq 0$ in $\mathbb{F}_5$, [Theorem 5.1.2](#) (b) gives $2x^2 + 3 \nmid x^4 + 2x^3 + 3x + 1$ in $\mathbb{F}_5[x]$.

Exercise. B2: A factor of a difference of powers

Let F be a field, $c \in F$ and $n \in \mathbb{Z}_{>0}$. Deduce from Lemma 1.1.4 that

$$x^n - c^n = (x - c) \sum_{j=0}^{n-1} c^j x^{n-1-j},$$

and hence that $x - c \mid x^n - c^n$. Then give a second proof of the divisibility with [Theorem 5.1.3](#).

Solution. $F[x]$ is a commutative ring (Theorem 4.2.4 (a)), so Lemma 1.1.4 applies in it. Take $z = c$ and $w = x$:

$$c^n - x^n = (c - x) \sum_{j=0}^{n-1} c^j x^{n-1-j}.$$

Negate both sides: $-(c^n - x^n) = x^n - c^n$ and $-((c - x)s) = (x - c)s$ for every $s \in F[x]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (a), (c)). This is the displayed identity, and it shows $x - c \mid x^n - c^n$. Taking $z = c$, $w = x$ rather than $z = x$, $w = c$ gives the sum in the stated order, with no re-indexing.

Second proof. By Theorem 4.2.4 (c), x^n is the monomial $1x^n$, whose value at c is $1 \cdot c^n = c^n$ (Definition 4.4.1, the monomial example after it). So the value of $x^n - c^n$ at c is $c^n - c^n = 0$ (Theorem 4.4.1, for the sum and the constant $-c^n$), so c is a root and $x - c \mid x^n - c^n$ by [Theorem 5.1.3](#) (b). This proof gives the divisibility at once but not the quotient.

Exercise. B3: One remainder over every field

Let F be any field. Show that the remainder of x^{100} on division by $x^2 - 1$ in $F[x]$ is 1. Then explain why, over $\mathbb{Q}$, evaluating at the roots 1 and -1 also finds it, and why that method alone does not settle the question over $\mathbb{F}_2$.

Solution. By Lemma 1.1.4 in $F[x]$ with $z = x^2$, $w = 1$ and $n = 50$, since $(x^2)^k = x^{2k}$ and

$1^k = 1$ (Lemma 4.1.1 (c)),

$$(x^2 - 1) \sum_{j=0}^{49} x^{2j} = x^{100} - 1.$$

So $x^{100} = (\sum_{j=0}^{49} x^{2j})(x^2 - 1) + 1$, and $\deg 1 = 0 < 2 = \deg(x^2 - 1)$. By the uniqueness in [Theorem 5.1.2](#) (a), the remainder is 1, over every field.

Over $\mathbb{Q}$ by evaluation. Write $x^{100} = q(x^2 - 1) + ax + b$. Evaluating at 1 and -1 gives $1 = a + b$ and $1 = -a + b$; subtracting, $2a = 0$, so $a = 0$ since $2 \neq 0$ in $\mathbb{Q}$; then $b = 1$.

Over $\mathbb{F}_2$. There $-1 = 1$, so the two roots coincide and evaluation gives the single equation $1 = a + b$. It does not determine a and b (both $(0, 1)$ and $(1, 0)$ satisfy it), so the uniqueness argument above is needed.

5.1.4.3 C. Going deeper

Exercise. C1: Monic divisors keep integer coefficients

Call $p \in \mathbb{Q}[x]$ an **integer polynomial** if every coefficient of p lies in $\mathbb{Z}$.

- (a) Let f, g be integer polynomials with g monic. Prove that the quotient and the remainder of f on division by g in $\mathbb{Q}[x]$ are integer polynomials.
- (b) Prove the same if $\text{lc}(g) = -1$.
- (c) Explain why the least-degree argument of [Theorem 5.1.2](#) still works when S is replaced by $\{f - hg : h \text{ an integer polynomial}\}$, for g monic.

Solution (Hint 1). Rerun the existence proof of [Theorem 5.1.2](#), but only with integer polynomials h .

Solution (Hint 2). Let $S_{\mathbb{Z}} := \{f - hg : h \text{ an integer polynomial}\}$. If $0 \notin S_{\mathbb{Z}}$, take $r = f - qg \in S_{\mathbb{Z}}$ of least degree n (Sets, Relations, and Cardinality, Theorem 2.1.3) and suppose $n \geq \deg g$.

Solution. Sums, negatives and products of integer polynomials are integer polynomials: their coefficients are sums of products of coefficients (Definition 4.2.1), and $\mathbb{Z}$ is closed under $+$, $-$, $\cdot$.

- (c) and (a). Let $m := \deg g$ and

$$S_{\mathbb{Z}} := \{f - hg : h \text{ an integer polynomial}\} \subseteq \mathbb{Q}[x],$$

whose elements are integer polynomials. Run the existence proof with $S_{\mathbb{Z}}$ in place of S . If $0 \in S_{\mathbb{Z}}$, then $f = qg$ with q an integer polynomial and $r = 0$. Otherwise take $r = f - qg \in S_{\mathbb{Z}}$ of least degree n (Sets, Relations, and Cardinality, Theorem 2.1.3), and suppose $n \geq m$. With $a := \text{lc}(r) \in \mathbb{Z}$ and $b = 1$, the monomial $t = ax^{n-m}$ is an integer polynomial, so $r - tg = f - (q + t)g \in S_{\mathbb{Z}}$, and it has degree $< n$ or is 0, exactly as in the proof. Both contradict the choice of r . So $\deg r < m$, and $f = qg + r$ with q, r integer polynomials. This is a division with remainder in $\mathbb{Q}[x]$, so by uniqueness ([Theorem 5.1.2](#) (a)) these q, r are **the** quotient and remainder. The argument works

because the step $r \mapsto r - tg$ never leaves $S_{\mathbb{Z}}$: it needs $b^{-1} \in \mathbb{Z}$, and $b = 1$ gives $b^{-1} = 1$. That answers (c).

- (d) If $\text{lc}(g) = -1$, then $b^{-1} = -1 \in \mathbb{Z}$, and the same proof runs with $t = -ax^{n-m}$. (Alternatively, divide f by the monic $-g$: $f = q(-g) + r = (-q)g + r$.)

Exercise. C2: The remainder modulo a quadratic with known roots

Let F be a field, $f \in F[x]$ and $a, b \in F$.

- (a) If $a \neq b$, prove that the remainder of f on division by $(x - a)(x - b)$ is

$$f(a)(a - b)^{-1}(x - b) + f(b)(b - a)^{-1}(x - a).$$

- (b) If $a = b$, write $f = (x - a)h + f(a)$ (Theorem 5.1.3 (a)) and prove that the remainder of f on division by $(x - a)^2$ is $h(a)(x - a) + f(a)$.
(c) Hence find the remainder of x^{100} on division by $x^2 - 3x + 2$ in $\mathbb{Q}[x]$.

Solution (Hint 1). The remainder has degree at most 1. Which values does it take at a and at b ?

Solution (Hint 2). Write $f = q(x - a)(x - b) + r$ with $\deg r \leq 1$, and let s be the displayed polynomial.

Solution.

- (a) The divisor $(x - a)(x - b)$ is monic of degree 2 (Theorem 4.3.2 (b)), so Theorem 5.1.2 (a) gives $f = q(x - a)(x - b) + r$ with $\deg r \leq 1$. Evaluating at a and at b (Theorem 4.4.1) kills the first term: $r(a) = f(a)$ and $r(b) = f(b)$. Let s be the displayed polynomial; it has degree at most 1, and $s(a) = f(a) \cdot 1 + f(b) \cdot 0 = f(a)$, $s(b) = f(b)$. So $r - s$ has degree at most 1 and the two roots $a \neq b$. If $r - s \neq 0$, then $x - a \mid r - s$ (Theorem 5.1.3 (b)), say $r - s = (x - a)k$, and $\deg k \leq 0$ by Theorem 4.3.2 (b), so k is a constant; evaluating at b gives $0 = (b - a)k$, so $k = 0$ because $b - a \neq 0$, and then $r - s = 0$ after all. Hence $r = s$.
(b) Divide h by $x - a$: $h = (x - a)h_2 + h(a)$ (Theorem 5.1.3 (a)). Then

$$f = (x - a)^2 h_2 + h(a)(x - a) + f(a),$$

and $h(a)(x - a) + f(a)$ has degree at most $1 < 2$. By uniqueness, it is the remainder.

- (c) $x^2 - 3x + 2 = (x - 1)(x - 2)$. By (a) with $a = 1$, $b = 2$, $f(1) = 1$ and $f(2) = 2^{100}$, the remainder is

$$1 \cdot (-1)^{-1}(x - 2) + 2^{100} \cdot 1^{-1}(x - 1) = (2^{100} - 1)x + (2 - 2^{100}).$$