

## 5.2 Ideals, the Greatest Common Divisor, and the Euclidean Algorithm

Section 5.1 gave  $F[x]$  a division with remainder (Theorem 5.1.2). This section asks what two polynomials have in common. Here is a concrete version of the question. Which polynomials over  $\mathbb{Q}$  can be written as

$$a \cdot (x^2 - 1) + b \cdot (x^2 + x - 2) \quad \text{with } a, b \in \mathbb{Q}[x]?$$

Taking  $a = -1$  and  $b = 1$  gives  $x - 1$ , and hence, multiplying  $a$  and  $b$  by any  $h$ , every multiple  $h \cdot (x - 1)$ . Nothing else can occur:  $x^2 - 1 = (x - 1)(x + 1)$  and  $x^2 + x - 2 = (x - 1)(x + 2)$ , so  $x - 1$  divides every such combination (Proposition 5.1.1 (c)). So the answer is “all multiples of  $x - 1$ , and nothing else”. Why  $x - 1$ , and why should the answer be the set of multiples of a single polynomial? The integer version of this question, in *Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$* , Section 3.2, was answered by a least element; here the answer is a polynomial of least degree.

As in Section 5.1,  $F$  is a field and  $F[x]$  is a commutative ring (Theorem 4.2.4 (a)). So the general notions of *Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$* , Chapter 3 apply to it without change: ideals (Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Definition 3.4.1, clauses (I1)–(I3)), quotient rings (Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Theorem 3.4.1) and units (Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Definition 3.5.1). We recall the clauses: a subset  $I \subseteq F[x]$  is an **ideal** if (I1)  $0 \in I$ , (I2)  $a + b \in I$  for all  $a, b \in I$ , and (I3)  $ra \in I$  for all  $a \in I$  and **all**  $r \in F[x]$ .

### 5.2.1 The ideal generated by finitely many polynomials

The combinations in the opening question form a set that deserves a name and a symbol.

#### Definition 5.2.1. Ideal Generated by Polynomials

Let  $F$  be a field,  $k \in \mathbb{Z}_{>0}$  and  $f_1, \dots, f_k \in F[x]$ . The set

$$\langle f_1, \dots, f_k \rangle := \{a_1 f_1 + \dots + a_k f_k : a_1, \dots, a_k \in F[x]\}$$

is the **ideal generated by**  $f_1, \dots, f_k$ . For one polynomial,  $\langle f \rangle = \{af : a \in F[x]\}$  is the set of multiples of  $f$ .

In words:  $\langle f_1, \dots, f_k \rangle$  collects every way of multiplying each  $f_i$  by a polynomial and adding up. The coefficients  $a_i$  range over **all** of  $F[x]$ , not over  $F$ . The name is earned by two facts.

*It is an ideal, and it contains every  $f_i$ .* (I1):  $0 = 0 \cdot f_1 + \dots + 0 \cdot f_k$ . (I2):  $\sum_i a_i f_i + \sum_i b_i f_i = \sum_i (a_i + b_i) f_i$ . (I3):  $r \sum_i a_i f_i = \sum_i (ra_i) f_i$ . These are the ring laws of  $F[x]$  applied to finite sums (Lemma 4.1.1 (b)). Taking  $a_i = 1$  and the other coefficients 0 shows  $f_i \in \langle f_1, \dots, f_k \rangle$ .

*It lies inside every ideal that contains every  $f_i$ .* If  $J$  is an ideal with  $f_1, \dots, f_k \in J$ , then each  $a_i f_i \in J$  by (I3), and their sum lies in  $J$  by (I2), applied  $k - 1$  times. So  $\langle f_1, \dots, f_k \rangle \subseteq J$ .

So  $\langle f_1, \dots, f_k \rangle$  is the smallest ideal containing  $f_1, \dots, f_k$ . This “smallest” clause is how we will compare two such ideals: to show  $\langle g_1, \dots, g_l \rangle \subseteq \langle f_1, \dots, f_k \rangle$ , it is enough to show that each  $g_j$  lies in  $\langle f_1, \dots, f_k \rangle$ .

Examples:

- $\langle 0 \rangle = \{a \cdot 0\} = \{0\}$ , the degenerate case. It is the only ideal generated by one polynomial that contains no non-zero element, and the main theorem below treats it separately.
- $\langle c \rangle = F[x]$  for a non-zero constant  $c$ : every  $f$  equals  $(c^{-1}f) \cdot c$ .
- For  $c \in F$ , let  $I_c := \{f \in F[x] : f(c) = 0\}$ , the polynomials with root  $c$ . It is an ideal:  $0(c) = 0$ ,  $(f + g)(c) = f(c) + g(c) = 0$ , and  $(rf)(c) = r(c)f(c) = 0$ , by Theorem 4.4.1. Moreover  $I_c = \langle x - c \rangle$ : by the factor theorem (Theorem 5.1.3 (b)),  $f(c) = 0$  if and only if  $x - c \mid f$ , that is,  $f \in \langle x - c \rangle$ .
- In the opening question,  $\langle x^2 - 1, x^2 + x - 2 \rangle = \langle x - 1 \rangle$ .

☞ **Second reading** · *A non-example: large degree*

The set  $T := \{f \in F[x] : \deg f \geq 3\} \cup \{0\}$  satisfies (I1) and (I3) (a non-zero multiple of a polynomial of degree at least 3 has degree at least 3, by Theorem 4.3.2 (b)). But (I2) fails:  $x^3$  and  $-x^3 + x$  lie in  $T$ , and their sum  $x$  has degree 1. So  $T$  is not an ideal. “Large degree” is not a property that sums keep, because leading terms can cancel.

*Quick check.* Is  $\{f \in \mathbb{Q}[x] : f(0) = 1\}$  an ideal of  $\mathbb{Q}[x]$ ? Name the first clause that fails.

*Solution.* No. (I1) fails already: the zero polynomial has  $0(0) = 0 \neq 1$ . (So do (I2), since  $(1 + 1)(0) = 2$ , and (I3), with  $r = 0$ .) Compare  $I_0 = \{f : f(0) = 0\} = \langle x \rangle$ , which is an ideal.

## 5.2.2 Every ideal has one generator

Every example above turned out to be the set of multiples of a single polynomial. That is no accident.

### Theorem 5.2.1. Ideals of $F[x]$ Are Principal

Let  $F$  be a field and  $I$  an ideal of  $F[x]$ .

- If  $I = \{0\}$ , then  $I = \langle 0 \rangle$ .
- If  $I \neq \{0\}$ , there is **exactly one monic**  $d \in F[x]$  with  $I = \langle d \rangle$ . Moreover  $d$  is the only monic element of  $I$  of least degree among the non-zero elements of  $I$ .

*Idea.* Take a non-zero element of  $I$  of least degree, and scale it to be monic; call it  $d$ . Its multiples lie in  $I$  by absorption. Conversely, divide any  $f \in I$  by  $d$ : the remainder  $f - qd$  lies in  $I$  and has smaller degree than  $d$ , so it cannot be a non-zero element of  $I$ . It is 0, and  $f$  is a multiple of  $d$ . Uniqueness comes from Proposition 5.1.1 (f): two monic generators divide each other.

*Before reading on:* where is “least degree” used, and why is  $d$  made monic?

*Proof.*

- (a) If  $I = \{0\}$ , then  $I = \{0\} = \langle 0 \rangle$ .
- (b) *Existence.* Let  $I \neq \{0\}$ . The set  $D := \{\deg e : e \in I, e \neq 0\}$  is a non-empty subset of  $\mathbb{N}$ , so it has a least element  $n$  (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). Choose a non-zero  $e \in I$  with  $\deg e = n$ , let  $a := \text{lc}(e) \neq 0$ , and let  $d := a^{-1}e$ . Then  $d \in I$  by (I3), and  $d$  is monic of degree  $n$  (Proposition 5.1.1 (f), Theorem 4.3.2 (b)).

( $\supseteq$ ) For  $h \in F[x]$ ,  $hd \in I$  by (I3). So  $\langle d \rangle \subseteq I$ .

( $\subseteq$ ) Let  $f \in I$ . Since  $d \neq 0$ , Theorem 5.1.2 (a) gives  $q, r \in F[x]$  with  $f = qd + r$  and  $\deg r < \deg d = n$ . Then  $r = f + (-q)d \in I$ , by (I3) and (I2). If  $r \neq 0$ , then  $\deg r \in D$  and  $\deg r < n$ , against the choice of  $n$  as least. So  $r = 0$ , and  $f = qd \in \langle d \rangle$ . Hence  $I = \langle d \rangle$ .

*Uniqueness.* Let  $d'$  be monic with  $I = \langle d' \rangle$ . Then  $d \in \langle d' \rangle$  and  $d' \in \langle d \rangle$  (each generator lies in its own ideal), so  $d' \mid d$  and  $d \mid d'$ . Both are monic, so  $d = d'$  by Proposition 5.1.1 (f).

*The least-degree description.* Let  $d''$  be any monic element of  $I$  with  $\deg d'' = n$ . The argument of ( $\supseteq$ ) and ( $\subseteq$ ) used only that  $d$  is a non-zero element of  $I$  of degree  $n$ ; run with  $d''$  in place of  $d$ , it gives  $I = \langle d'' \rangle$ , and uniqueness gives  $d'' = d$ . This proves the theorem. ■

The answer to the prompt. “Least degree” is used once, in ( $\subseteq$ ): the remainder  $r$  lies in  $I$  and has degree below  $n$ , so minimality forces  $r = 0$ . The minimality is about **non-zero** elements, which is why  $r = 0$  is the conclusion and not a contradiction. Making  $d$  monic plays no part in the existence of a generator:  $e$  itself generates  $I$ , and so does  $2e$  when  $2 \neq 0$  in  $F$ . It is what makes the generator **unique**, because among the associates of  $e$ , all of which generate  $I$ , exactly one is monic.

An ideal of the form  $\langle d \rangle$  is called **principal**, hence the name of the theorem. The proof’s move is the one this chapter is built on, and we name it: **least degree, then divide**. In a set of polynomials closed under the right operations, take a non-zero element  $d$  of least degree; divide any element of the set by  $d$ ; the remainder lies in the set and has smaller degree, so it is 0. It is the polynomial form of “least positive element, then divide” from *Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$* , Section 3.2.

---

🕒 **Second reading** · Comparison with the integers, and two indeterminates

The integer twin is Number Systems: From  $\setminus(\setminus\mathbb{N}\setminus)$  to  $\setminus(\setminus\mathbb{N}\setminus)$ , Theorem 3.4.2: every ideal of  $\mathbb{Z}$  is  $n\mathbb{Z}$  for exactly one  $n \in \mathbb{N}$ . There “ $n \geq 0$ ” picked the generator; here “monic” does. In polynomials in **two** indeterminates the theorem fails (the polynomials with zero constant term are an example, which we state without proof; Exercise A1 asks which step of the proof breaks there, without proving the failure).

---

### 5.2.3 The greatest common divisor

A **common divisor** of  $f$  and  $g$  is a polynomial  $h$  with  $h \mid f$  and  $h \mid g$ . Every non-zero constant is one (Proposition 5.1.1 (a)). For integers, *Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$* , Section 3.2 took the **largest** common divisor. For polynomials, “largest” can only refer to the degree, and associates have the same degree:  $x - 1$  and  $2x - 2$  are both common divisors of  $x^2 - 1$  and  $x^2 + x - 2$  in  $\mathbb{Q}[x]$ , of the same degree. So the definition asks instead for the property that Bézout’s theorem gave the integer gcd, and fixes one associate by asking it to be monic.

*The greatest common divisor is the monic common divisor that every common divisor divides.*

#### Definition 5.2.2. Greatest Common Divisor of Polynomials

Let  $F$  be a field and  $f, g \in F[x]$ , **not both** 0. A **greatest common divisor** of  $f$  and  $g$  is a **monic**  $d \in F[x]$  such that  $d \mid f$ ,  $d \mid g$ , and  $h \mid d$  for **every** common divisor  $h$  of  $f$  and  $g$ . We set  $\gcd(0, 0) := 0$ .

In words:  $d$  is a common divisor, it is “on top” of all common divisors for the relation  $\mid$ , and it is monic.

*At most one.* If  $d$  and  $d'$  are both greatest common divisors of  $f$  and  $g$ , each is a common divisor, so each divides the other; both are monic, so  $d = d'$  (Proposition 5.1.1 (f)). We write  $\gcd(f, g)$  for it once it is known to exist, and the next theorem shows it always does. The condition is symmetric in  $f$  and  $g$ , so  $\gcd(f, g) = \gcd(g, f)$ .

○ **Second reading** · *Why  $\gcd(0, 0)$  is 0*

Every polynomial divides 0, so the common divisors of 0 and 0 are all polynomials, and the only polynomial that every polynomial divides is 0 (Proposition 5.1.1 (a) and (d)); but 0 is not monic. The value 0 keeps “every common divisor divides the gcd” true, and it keeps  $\langle f, g \rangle = \langle \gcd(f, g) \rangle$  true, since  $\langle 0, 0 \rangle = \{0\} = \langle 0 \rangle$ . The gcd clause of Lemma 5.2.4 uses the value  $\gcd(0, 0) = 0$  in the case  $f = g = 0$ .

#### Theorem 5.2.2. Bézout’s Theorem for Polynomials

Let  $F$  be a field, let  $f, g \in F[x]$  be not both 0, and let  $d$  be the monic polynomial with  $\langle f, g \rangle = \langle d \rangle$  (Theorem 5.2.1).

- (a)  $d \mid f$  and  $d \mid g$ .
- (b) Every common divisor of  $f$  and  $g$  divides  $d$ .
- (c)  $d = \gcd(f, g)$ . So  $\gcd(f, g)$  exists, and  $\langle f, g \rangle = \langle \gcd(f, g) \rangle$ .
- (d)  $\gcd(f, g) = af + bg$  for some  $a, b \in F[x]$ .
- (e)  $\gcd(f, g)$  has the largest degree among the common divisors of  $f$  and  $g$ , and a common divisor of that degree is an associate of  $\gcd(f, g)$ .

The ideal  $\langle f, g \rangle$  contains  $f$  and  $g$ , one of which is non-zero, so  $\langle f, g \rangle \neq \{0\}$  and the monic  $d$  exists and is unique by Theorem 5.2.1 (b).

*Idea.* Everything is read off from  $\langle f, g \rangle = \langle d \rangle$ , used in both directions. Since  $f$  and  $g$  lie in the ideal, they are multiples of  $d$ . Since  $d$  lies in the ideal, it is a combination of  $f$  and  $g$ , and a combination is divisible by every common divisor.

*Proof.*

- (a)  $f, g \in \langle f, g \rangle = \langle d \rangle$ , so  $f$  and  $g$  are multiples of  $d$ .
- (b) Since  $d \in \langle d \rangle = \langle f, g \rangle$ , there are  $a_0, b_0 \in F[x]$  with  $d = a_0f + b_0g$ . If  $h \mid f$  and  $h \mid g$ , then  $h \mid a_0f + b_0g = d$  by Proposition 5.1.1 (c).
- (c) By (a) and (b),  $d$  is a monic common divisor that every common divisor divides; so  $d = \gcd(f, g)$  by Definition 5.2.2. Then  $\langle f, g \rangle = \langle d \rangle = \langle \gcd(f, g) \rangle$ .
- (d) This is  $d = a_0f + b_0g$  from (b).
- (e) Let  $h$  be a common divisor. By (b),  $h \mid d$ , and  $d \neq 0$ , so  $\deg h \leq \deg d$  by Proposition 5.1.1 (d). If  $\deg h = \deg d$ , write  $d = hu$ ; then  $\deg u = 0$  by Theorem 4.3.2 (b), so  $u$  is a non-zero constant and  $d$  and  $h$  are associates. This proves the theorem. ■

For the opening question:  $\langle x^2 - 1, x^2 + x - 2 \rangle = \langle d \rangle$  with  $d$  monic, and  $d = \gcd(x^2 - 1, x^2 + x - 2) = x - 1$ , because  $x - 1$  is a monic common divisor and a combination, so every common divisor divides it.

🔄 **Second reading** • *Why the definition is not the integer one*

*Number Systems:* From  $\mathbb{N}$  to  $\mathbb{R}$ , Section 3.2 defined the integer gcd as the **largest** common divisor (Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Definition 3.2.2) and then proved Bézout's theorem (Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Theorem 3.2.1). Here the order is reversed: the definition uses the divisibility property, which for integers was a consequence, and part (e) recovers “largest” as a consequence, up to associates.

Pairs with no common divisor of positive degree get a name.

### Definition 5.2.3. Coprime Polynomials

Let  $F$  be a field. Polynomials  $f, g \in F[x]$  are **coprime over**  $F$  if  $\gcd(f, g) = 1$ .

For example,  $x$  and  $x + 1$  are coprime over every field, since  $(x + 1) - x = 1$  and the next corollary applies; 0 and 0 are not, since  $\gcd(0, 0) = 0$ .

### Corollary 5.2.3. Coprime Means 1 Is a Combination

Let  $F$  be a field and  $f, g \in F[x]$ . Then  $f$  and  $g$  are coprime if and only if  $af + bg = 1$  for some  $a, b \in F[x]$ .

*Proof.* ( $\Rightarrow$ ) If  $\gcd(f, g) = 1$ , then  $f, g$  are not both 0, since  $\gcd(0, 0) = 0 \neq 1$ , and [Theorem 5.2.2](#) (d) gives  $a, b$  with  $af + bg = 1$ .

( $\Leftarrow$ ) Let  $af + bg = 1$ . Then  $f, g$  are not both 0, since otherwise  $af + bg = 0 \neq 1$ . Since  $1 \in \langle f, g \rangle$ , every  $h = h \cdot 1$  lies in  $\langle f, g \rangle$  by (I3), so  $\langle f, g \rangle = F[x] = \langle 1 \rangle$ . The polynomial 1 is monic, so by the uniqueness in [Theorem 5.2.1](#) (b) it is the monic generator of  $\langle f, g \rangle$ , and [Theorem 5.2.2](#) (c) gives  $\gcd(f, g) = 1$ . ■

*Quick check.* Find  $\gcd(2x - 2, 4x^2 - 4)$  in  $\mathbb{Q}[x]$ .

*Solution.*  $4x^2 - 4 = (2x - 2)(2x + 2)$ , so  $2x - 2$  divides both, and every common divisor divides  $2x - 2$ . But  $2x - 2$  is not monic. Its monic associate  $x - 1$  has the same divisors and multiples (Proposition 5.1.1 (f), (b)), so  $\gcd(2x - 2, 4x^2 - 4) = x - 1$ , not  $2x - 2$ .

## 5.2.4 The Euclidean algorithm

Bézout's theorem finds  $\gcd(f, g)$  as an element of least degree, which is no way to compute it. A computation needs a step that lowers degrees without changing the ideal. Division with remainder is that step.

### Lemma 5.2.4. One Step of the Euclidean Algorithm

Let  $F$  be a field and  $f, g, q, r \in F[x]$  with  $f = qg + r$ . Then  $\langle f, g \rangle = \langle g, r \rangle$ , and hence  $\gcd(f, g) = \gcd(g, r)$ .

*Proof.* ( $\supseteq$ )  $g \in \langle f, g \rangle$ , and  $r = f + (-q)g \in \langle f, g \rangle$ ; by the smallest-ideal property of [Definition 5.2.1](#),  $\langle g, r \rangle \subseteq \langle f, g \rangle$ . ( $\subseteq$ )  $f = qg + 1 \cdot r \in \langle g, r \rangle$  and  $g \in \langle g, r \rangle$ , so  $\langle f, g \rangle \subseteq \langle g, r \rangle$  in the same way.

For the gcds: if  $f = g = 0$ , then  $r = 0$ , and both gcds are  $\gcd(0, 0) = 0$ . Otherwise  $\langle f, g \rangle \neq \{0\}$ , so  $\langle g, r \rangle \neq \{0\}$  and  $g, r$  are not both 0. By [Theorem 5.2.2](#) (c),  $\gcd(f, g)$  and  $\gcd(g, r)$  are monic generators of the same ideal, so they are equal by the uniqueness in [Theorem 5.2.1](#) (b). ■

The lemma does not ask  $r$  to be the remainder. Choosing the remainder makes the degree drop, and repeating the step gives a sequence. To define “repeat” without “and so on”, we use the recursion theorem, as in Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Theorem 3.2.4.

### Theorem 5.2.5. The Euclidean Algorithm for Polynomials

Let  $F$  be a field and  $f, g \in F[x]$  with  $g \neq 0$ . Define pairs  $(u_k, v_k) \in F[x] \times F[x]$  for  $k \in \mathbb{N}$  by

$(u_0, v_0) := (f, g)$  and

$$(u_{k+1}, v_{k+1}) := \begin{cases} (v_k, r_k) & \text{if } v_k \neq 0, \\ (u_k, v_k) & \text{if } v_k = 0, \end{cases}$$

where, when  $v_k \neq 0$ ,  $r_k$  is the remainder of  $u_k$  on division by  $v_k$ . Then:

- (a)  $\langle u_k, v_k \rangle = \langle f, g \rangle$  for every  $k \in \mathbb{N}$ ;
- (b) there is a least  $K \in \mathbb{N}$  with  $v_K = 0$ ; moreover  $1 \leq K \leq \deg g + 1$ , and  $\deg v_{k+1} < \deg v_k$  for every  $k < K$ ;
- (c)  $u_K \neq 0$ , and  $\gcd(f, g)$  is the monic associate of  $u_K$ .

In practice the sequence is written as a chain of divisions  $u_k = q_k v_k + r_k$ ,  $k = 0, \dots, K-1$ , each dividing the previous divisor by the previous remainder, until a remainder is 0. The degrees of the remainders fall, and  $u_K = v_{K-1}$  is the last non-zero remainder  $r_{K-2}$  if  $K \geq 2$ , and  $g$  itself if  $K = 1$  (then  $g \mid f$ ).

◉ **Second reading** · *Why the sequence exists*

The sequence is well defined. Let  $G: F[x] \times F[x] \rightarrow F[x] \times F[x]$  send  $(u, v)$  to  $(v, r)$ , where  $r$  is the remainder of  $u$  on division by  $v$ , if  $v \neq 0$ , and to  $(u, v)$  if  $v = 0$ . This is a function, since the remainder exists and is unique (Theorem 5.1.2 (a)). The recursion theorem (Sets, Relations, and Cardinality, Theorem 2.3.1, read on  $\mathbb{N} = \omega$  by Number Systems: From  $\setminus(\setminus \mathbb{N} \setminus)$  to  $\setminus(\setminus \mathbb{N} \setminus)$ , Corollary 1.7.3 (b)), with  $X = F[x] \times F[x]$ , starting value  $(f, g)$  and step  $(k, P) \mapsto G(P)$ , gives exactly one sequence of pairs with the displayed properties.

*Idea.* Part (a) is [Lemma 5.2.4](#) once per step, carried along by induction. For (b), the degrees of the second entries are natural numbers that drop by at least one per step while the entries are non-zero, so a zero entry must come within  $\deg g + 1$  steps. For (c), at the first zero, (a) reads  $\langle f, g \rangle = \langle u_K, 0 \rangle = \langle u_K \rangle$ , and the monic generator of this ideal is the gcd.

*Proof.*

- (a) We use Logic and Proof, Axiom 4.2.1 (through Number Systems: From  $\setminus(\setminus \mathbb{N} \setminus)$  to  $\setminus(\setminus \mathbb{N} \setminus)$ , Corollary 1.7.3 (b)) on  $k$ , for  $P(k)$ : “ $\langle u_k, v_k \rangle = \langle f, g \rangle$ ”.  $P(0)$  holds since  $(u_0, v_0) = (f, g)$ . Suppose  $P(k)$ . If  $v_k \neq 0$ , then  $u_k = q_k v_k + r_k$  for some  $q_k$ , and [Lemma 5.2.4](#) gives  $\langle u_{k+1}, v_{k+1} \rangle = \langle v_k, r_k \rangle = \langle u_k, v_k \rangle = \langle f, g \rangle$ . If  $v_k = 0$ , the pair does not change, and  $P(k+1)$  is  $P(k)$ .

- (b) *A bound.* We show by Logic and Proof, Axiom 4.2.1 on  $k$  the statement  $Q(k)$ : “if  $v_0, \dots, v_k$  are all non-zero, then  $\deg v_k + k \leq \deg g$ ”.  $Q(0)$  holds since  $v_0 = g$ . Suppose  $Q(k)$ , and let  $v_0, \dots, v_{k+1}$  be non-zero. Then  $v_k \neq 0$ , so  $v_{k+1} = r_k$  has  $\deg v_{k+1} < \deg v_k$ , and as both degrees lie in  $\mathbb{N}$ ,  $\deg v_{k+1} + 1 \leq \deg v_k$ . With  $Q(k)$ ,  $\deg v_{k+1} + (k+1) \leq \deg v_k + k \leq \deg g$ , which is  $Q(k+1)$ .

*The first zero.* If  $v_0, \dots, v_k$  were all non-zero for  $k := \deg g + 1$ , then  $Q(k)$  would give  $\deg v_k \leq -1$ , impossible for a non-zero polynomial. So  $\{k \in \mathbb{N} : v_k = 0\}$  is non-empty, and it has a least element  $K$  (Sets, Relations, and Cardinality, Theorem 2.1.3). Since  $v_0 = g \neq 0$ ,  $K \geq 1$ . By the choice of  $K$ ,  $v_0, \dots, v_{K-1}$  are non-zero, so  $Q(K-1)$  gives

$0 \leq \deg v_{K-1} \leq \deg g - (K-1)$ , that is,  $K \leq \deg g + 1$ . For  $k < K$ ,  $v_k \neq 0$ , so  $v_{k+1} = r_k$  and  $\deg v_{k+1} < \deg v_k$  by Theorem 5.1.2 (a).

- (c) Since  $K-1 < K$ ,  $v_{K-1} \neq 0$ , so the step gives  $u_K = v_{K-1} \neq 0$ . By (a) with  $k = K$ , and since  $v_K = 0$ ,

$$\langle f, g \rangle = \langle u_K, 0 \rangle = \langle u_K \rangle,$$

where  $\langle u_K, 0 \rangle = \{au_K + b \cdot 0\} = \langle u_K \rangle$ . Let  $c := \text{lc}(u_K)^{-1}$ . The monic associate  $cu_K$  generates the same ideal as  $u_K$ , because each is a multiple of the other ( $u_K = c^{-1} \cdot cu_K$ ). So  $cu_K$  is a monic generator of  $\langle f, g \rangle$ , and since  $g \neq 0$ , Theorem 5.2.2 (c) and the uniqueness in Theorem 5.2.1 (b) give  $\gcd(f, g) = cu_K$ . ■

To find  $a, b$  with  $\gcd(f, g) = af + bg$ , run the step of Lemma 5.2.4 backwards.

**Algorithm. Back-substitution.** Write out the divisions  $u_k = q_kv_k + r_k$  for  $k = 0, \dots, K-1$ , so that  $u_{k+1} = v_k$  and  $v_{k+1} = r_k$ . Start from  $u_K = 1 \cdot u_K + 0 \cdot v_K$ . Then, for  $k = K-1, K-2, \dots, 0$  in turn, rewrite a combination  $su_{k+1} + tv_{k+1} = sv_k + tr_k$  as one of  $u_k$  and  $v_k$ , by substituting  $r_k = u_k - q_kv_k$ :

$$sv_k + t(u_k - q_kv_k) = tu_k + (s - tq_k)v_k.$$

After  $k = 0$  the combination is one of  $u_0 = f$  and  $v_0 = g$ ; multiply it by  $\text{lc}(u_K)^{-1}$  to get  $\gcd(f, g)$ , and multiply out to check. (By hand one starts from the last division with a non-zero remainder, as in the example below.)

Nothing rests on the procedure: existence is Theorem 5.2.2 (d), and multiplying out checks the  $a, b$  found.

### Example. A run of the Euclidean algorithm

In  $\mathbb{Q}[x]$ , compute  $\gcd(f, g)$  for  $f = x^4 - x^3 - 3x^2 + x + 2$  and  $g = x^3 - 2x - 1$ , and write it as  $af + bg$ .

**Solution.** The chain of divisions (each by Theorem 5.1.2, the remainder of degree below the divisor's) is

$$\begin{aligned} x^4 - x^3 - 3x^2 + x + 2 &= (x-1)(x^3 - 2x - 1) + (1 - x^2), \\ x^3 - 2x - 1 &= (-x)(1 - x^2) + (-x - 1), \\ 1 - x^2 &= (x-1)(-x-1) + 0. \end{aligned}$$

So  $(u_k, v_k)$  runs through  $(f, g)$ ,  $(g, 1-x^2)$ ,  $(1-x^2, -x-1)$ ,  $(-x-1, 0)$ :  $K = 3$  and  $u_3 = -x-1$ . Its monic associate is  $x+1$ , so  $\gcd(f, g) = x+1$  by Theorem 5.2.5 (c).

Back-substitution, from the second division up:

$$\begin{aligned} -x-1 &= g + x(1-x^2) = g + x(f - (x-1)g) \\ &= xf + (1-x^2+x)g. \end{aligned}$$

Multiplying by  $-1$ :

$$x + 1 = (-x) \cdot f + (x^2 - x - 1) \cdot g.$$

Check:  $(-x)f = -x^5 + x^4 + 3x^3 - x^2 - 2x$  and  $(x^2 - x - 1)g = x^5 - x^4 - 3x^3 + x^2 + 3x + 1$ ; the sum is  $x + 1$ .

*Warning.* Bézout coefficients are **not** unique. Since  $gf - fg = 0$ ,

$$x + 1 = (-x + g) \cdot f + (x^2 - x - 1 - f) \cdot g$$

as well, with coefficients of degrees 3 and 4. So “the” coefficients mean nothing by themselves; back-substitution produces one pair, and any other pair works as well.

*Quick check.* Run the algorithm on  $f = x^3$  and  $g = x^2 + 1$  in  $\mathbb{Q}[x]$ . Are they coprime?

*Solution.*  $x^3 = x \cdot (x^2 + 1) + (-x)$ , then  $x^2 + 1 = (-x)(-x) + 1$ , then  $-x = (-x) \cdot 1 + 0$ . The last non-zero remainder is 1, already monic, so  $\gcd(x^3, x^2 + 1) = 1$ : they are coprime. Back-substitution gives  $1 = (x^2 + 1) - x^2 = (x^2 + 1) + x \cdot (-x) = (x^2 + 1) + x(x^3 - x(x^2 + 1)) = x \cdot x^3 + (1 - x^2)(x^2 + 1)$ .

## 5.2.5 Changing the field

The same pair of polynomials can be read over a bigger field:  $x^2 - 2 \in \mathbb{Q}[x]$  is also an element of  $\mathbb{R}[x]$ , where it factors as  $(x - \sqrt{2})(x + \sqrt{2})$ . Factorizations depend on the field; division and the gcd do not, because the Euclidean algorithm never leaves the smaller field.

Recall that a **subfield** of a field  $L$  is a subset  $K \subseteq L$  containing 0 and 1 and closed under  $+$ ,  $\cdot$ , negatives and inverses of non-zero elements (Definition 2.3.1; Proposition 2.3.1 is the practical check). Then  $K$  is a field with the operations of  $L$ , and  $K[x] \subseteq L[x]$ : a polynomial with coefficients in  $K$  is one with coefficients in  $L$ , and sums, products, degrees and leading coefficients are computed by the same formulas in both rings. The examples are  $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ , with  $\mathbb{R} \subseteq \mathbb{C}$  by Proposition 1.1.1 and Theorem 1.2.4.

### Proposition 5.2.6. Division and gcd Do Not Depend on the Field

Let  $L$  be a field,  $K \subseteq L$  a subfield, and  $f, g \in K[x]$ .

- (a) If  $g \neq 0$ , the quotient and the remainder of  $f$  on division by  $g$  are the same in  $K[x]$  and in  $L[x]$ .
- (b) If  $g \neq 0$ , then  $g \mid f$  in  $L[x]$  if and only if  $g \mid f$  in  $K[x]$ .
- (c)  $\gcd(f, g)$  is the same computed in  $K[x]$  or in  $L[x]$ . In particular,  $f$  and  $g$  are coprime over  $K$  if and only if they are coprime over  $L$ .

*In words: computing a quotient, a remainder or a gcd never needs an element outside the smaller field.*

◉ **Second reading** · *The proof: the algorithm never leaves the smaller field*

*Proof.*

- (a) Let  $f = qg + r$  with  $q, r \in K[x]$  and  $\deg r < \deg g$  be the division in  $K[x]$  (Theorem 5.1.2 (a)). The same equation holds in  $L[x]$ , and the degrees are the same there, so it is a division with remainder in  $L[x]$ . By the uniqueness in  $L[x]$ , it is **the** division there.
- (b) By (a), the remainder  $r$  is the same in both rings, and by Theorem 5.1.2 (b), applied in each ring,  $g \mid f$  holds in that ring if and only if  $r = 0$ .
- (c) If  $f = g = 0$ , both gcds are 0. If  $g = 0 \neq f$ , then  $\langle f, 0 \rangle = \langle f \rangle$  in either ring, generated by the monic associate  $\text{lc}(f)^{-1}f$ , so  $\gcd(f, 0) = \text{lc}(f)^{-1}f$  in either ring (Theorem 5.2.2 (c) and the uniqueness in Theorem 5.2.1 (b)). The inverse  $\text{lc}(f)^{-1}$  is the same in  $K$  and in  $L$ , since  $K$  is closed under inverses and inverses in  $L$  are unique (Theorem 2.1.1 (c)). If  $g \neq 0$ , run Theorem 5.2.5 in  $K[x]$  and in  $L[x]$ . By Logic and Proof, Axiom 4.2.1 (through Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ ), Corollary 1.7.3 (b)) on  $k$ , the pairs  $(u_k, v_k)$  agree: they agree for  $k = 0$ , and if they agree at  $k$ , the next pair is  $(v_k, r_k)$  with the same remainder  $r_k$  by (a), or the same pair. So the first index with  $v_k = 0$  is the same in both runs, the polynomial  $u$  at that index is the same, and so is its monic associate, by the remark on inverses. By Theorem 5.2.5 (c), the two gcds are equal. In particular one is 1 if and only if the other is. ■

For example,  $x^2 + 1$  and  $x - 1$  are coprime over  $\mathbb{Q}$  ( $x^2 + 1 = (x + 1)(x - 1) + 2$  and  $0 \cdot (x - 1) + \frac{1}{2} \cdot 2 = 1$ ; apply Lemma 5.2.4 and Corollary 5.2.3), so they are coprime over  $\mathbb{C}$  as well, although  $x^2 + 1 = (x - i)(x + i)$  has factors of degree 1 only over  $\mathbb{C}$ .

*Quick check.* Compute  $\gcd(x^2 - 2, x^3 - 2x)$  in  $\mathbb{Q}[x]$ . Over  $\mathbb{R}$ ,  $x - \sqrt{2}$  divides both. Why is the gcd over  $\mathbb{R}$  still not  $x - \sqrt{2}$ ?

*Solution.* The divisions are  $x^2 - 2 = 0 \cdot (x^3 - 2x) + (x^2 - 2)$  and  $x^3 - 2x = x \cdot (x^2 - 2) + 0$ , so  $K = 2$  and  $u_2 = x^2 - 2$ , which is monic:  $\gcd = x^2 - 2$  in  $\mathbb{Q}[x]$ . By Proposition 5.2.6 (c) it is  $x^2 - 2$  in  $\mathbb{R}[x]$  too. The common divisor  $x - \sqrt{2}$  is not the gcd because the gcd must be divisible by **every** common divisor, and  $x + \sqrt{2}$  is another one; both divide  $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ .

*Remark* (Looking ahead). Section 5.6 uses part (b) of the last proposition with  $\mathbb{R} \subseteq \mathbb{C}$ , to bring a divisibility found in  $\mathbb{C}[x]$  back to  $\mathbb{R}[x]$ .

## 5.2.6 Exercises

### 5.2.6.1 A. Check your understanding

#### Exercise. A1

These questions are about the proof of [Theorem 5.2.1](#).

- Where is “least degree” used?
- Why is  $d$  made monic, and what would fail without it?
- Run the proof on  $I := \{f \in \mathbb{Q}[x] : f(1) = 0 \text{ and } f(-1) = 0\}$ : show that  $I$  is an ideal, and find  $d$ .
- The polynomials in two indeterminates  $x, y$  over  $\mathbb{Q}$  with zero constant term (such as  $x, y, x^2y - 3y$ ) are closed under sums and under multiplication by any polynomial in  $x, y$ . Name the step of the proof that has no analogue there. (A prose answer; no proof that the theorem fails is asked for.)
- State the idea of the proof in two sentences.

*Solution.*

- Once, in  $(\subseteq)$ : the remainder  $r = f - qd$  lies in  $I$  and has degree below  $n = \deg d$ ; since  $n$  is least among the degrees of non-zero elements of  $I$ ,  $r$  cannot be non-zero, so  $r = 0$ .
- For uniqueness. Every associate of  $d$  generates  $I$  (for instance  $2d$  when  $2 \neq 0$  in  $F$ :  $d = \frac{1}{2} \cdot 2d$ ), so without a normalization “the generator” would not be one polynomial. Exactly one associate is monic (Proposition 5.1.1 (f)).
- $I = I_1 \cap I_{-1}$  in the notation after [Definition 5.2.1](#). Each clause (I1)–(I3) holds in  $I_1$  and in  $I_{-1}$ , hence in the intersection. The polynomial  $x^2 - 1$  lies in  $I$ , since  $1 - 1 = 0$  and  $(-1)^2 - 1 = 0$ . No non-zero element of  $I$  has degree at most 1: if  $f = ax + b$  with  $f(1) = a + b = 0$  and  $f(-1) = -a + b = 0$ , adding gives  $2b = 0$ , so  $b = 0$  (as  $2 \neq 0$  in  $\mathbb{Q}$ ), and then  $a = 0$ . So the least degree is 2, and the proof’s  $d$  is the monic element  $x^2 - 1$  (any element of degree 2, scaled to be monic, is  $x^2 - 1$  by the uniqueness clause). Hence  $I = \langle x^2 - 1 \rangle$ .
- The division step,  $f = qd + r$  with  $\deg r < \deg d$ , which the proof applies to an arbitrary  $f \in I$  and the element  $d$  of least degree. Two indeterminates have no division with remainder of that kind. In this ideal,  $x$  and  $y$  both have the least possible degree, 1, and dividing  $y$  by  $x$  would need a leftover in the ideal of degree below 1, that is, 0; so  $x$  would have to divide  $y$ , and it does not. (That this ideal is generated by no single polynomial is true, but not proved here.)
- Take a non-zero element  $d$  of  $I$  of least degree, made monic. Dividing any element of  $I$  by  $d$  leaves a remainder that lies in  $I$  and has smaller degree, so it is 0, and  $I$  consists of the multiples of  $d$ .

### 5.2.6.2 B. Practice

#### Exercise. B1: A gcd and its common root

In  $\mathbb{Q}[x]$ , let  $f = x^3 + x^2 + x + 1$  and  $g = x^3 + x + 2$ . Compute  $\gcd(f, g)$  with the Euclidean algorithm, and write it as  $af + bg$ . Hence show that  $-1$  is the only common root of  $f$  and  $g$

in  $\mathbb{Q}$ .

*Solution.* The divisions are

$$\begin{aligned} x^3 + x^2 + x + 1 &= 1 \cdot (x^3 + x + 2) + (x^2 - 1), \\ x^3 + x + 2 &= x \cdot (x^2 - 1) + (2x + 2), \\ x^2 - 1 &= \left(\frac{1}{2}x - \frac{1}{2}\right)(2x + 2) + 0. \end{aligned}$$

So  $K = 3$ ,  $u_3 = 2x + 2$ , and  $\gcd(f, g) = x + 1$  (Theorem 5.2.5 (c)). Back-substitution:

$$2x + 2 = g - x(x^2 - 1) = g - x(f - g) = (-x)f + (x + 1)g,$$

so

$$x + 1 = \left(-\frac{1}{2}x\right)f + \frac{1}{2}(x + 1)g.$$

Check:  $-\frac{1}{2}xf = -\frac{1}{2}(x^4 + x^3 + x^2 + x)$  and  $\frac{1}{2}(x + 1)g = \frac{1}{2}(x^4 + x^3 + x^2 + 3x + 2)$ ; the sum is  $\frac{1}{2}(2x + 2) = x + 1$ .

*Common roots.*  $f(-1) = -1 + 1 - 1 + 1 = 0$  and  $g(-1) = -1 - 1 + 2 = 0$ , so  $-1$  is a common root. Let  $c \in \mathbb{Q}$  be any common root. By Theorem 5.1.3 (b),  $x - c$  divides  $f$  and  $g$ , so it divides  $x + 1$  by Theorem 5.2.2 (b). Both are monic of degree 1, so they are associates by Theorem 5.2.2 (e) (equal degree), hence equal (Proposition 5.1.1 (f)). So  $x - c = x + 1$ , and  $c = -1$ .

### Exercise. B2: A gcd over the field with two elements

In  $\mathbb{F}_2[x]$ , let  $f = x^4 + x^3 + x + 1$  and  $g = x^3 + x^2 + x + 1$ . Show that  $\gcd(f, g) = x^2 + 1$  and that  $x^2 + 1 = 1 \cdot f + x \cdot g$ .

*Solution.* In  $\mathbb{F}_2$ ,  $-1 = 1$  and  $1 + 1 = 0$ . First,  $xg = x^4 + x^3 + x^2 + x$ , so

$$f - xg = -x^2 + 1 = x^2 + 1,$$

that is,  $f = x \cdot g + (x^2 + 1)$ , a division with remainder. Next,  $(x + 1)(x^2 + 1) = x^3 + x^2 + x + 1 = g$ , so  $g = (x + 1)(x^2 + 1) + 0$ . The algorithm stops with  $u_2 = x^2 + 1$ , which is monic, so  $\gcd(f, g) = x^2 + 1$ . Finally  $x^2 + 1 = f - xg = 1 \cdot f + x \cdot g$ , since  $-x = x$  in  $\mathbb{F}_2[x]$ .

### 5.2.6.3 C. Going deeper

#### Exercise. C1: Exit check: ideals of $F[x]$ and Bézout

Let  $F$  be a field.

- Prove that for every ideal  $I \neq \{0\}$  of  $F[x]$  there is exactly one monic  $d$  with  $I = \langle d \rangle$ .
- Let  $f, g \in F[x]$ , not both 0, and let  $d$  be the monic generator of  $\langle f, g \rangle$ . Prove that  $d \mid f$ ,  $d \mid g$ , that every common divisor of  $f$  and  $g$  divides  $d$ , that  $d = \gcd(f, g)$ , and that  $d = af + bg$  for some  $a, b \in F[x]$ .

*Solution.*

- (a) *A generator.* The degrees of the non-zero elements of  $I$  form a non-empty subset of  $\mathbb{N}$ , which has a least element  $n$  (Sets, Relations, and Cardinality, Theorem 2.1.3). Let  $e \in I$  be non-zero of degree  $n$ , and  $d := \text{lc}(e)^{-1}e$ . Then  $d \in I$  by (I3), and  $d$  is monic of degree  $n$ . Every multiple  $hd$  lies in  $I$  by (I3), so  $\langle d \rangle \subseteq I$ . Conversely, let  $f \in I$ , and divide:  $f = qd + r$  with  $\deg r < n$  (Theorem 5.1.2 (a)). Then  $r = f + (-q)d \in I$  by (I3) and (I2). If  $r \neq 0$ , it is a non-zero element of  $I$  of degree less than  $n$ , against the choice of  $n$ ; so  $r = 0$  and  $f \in \langle d \rangle$ . Hence  $I = \langle d \rangle$ .

*Uniqueness.* If also  $I = \langle d' \rangle$  with  $d'$  monic, then  $d \in \langle d' \rangle$  and  $d' \in \langle d \rangle$ , so  $d$  and  $d'$  divide each other. Then  $d' = cd$  for a non-zero constant  $c$  (Proposition 5.1.1 (f)), and comparing leading coefficients gives  $c = 1$ .

- (b) The ideal  $\langle f, g \rangle$  is not  $\{0\}$ , since it contains  $f$  and  $g$ ; let  $d$  be its monic generator, from (a). Since  $f, g \in \langle d \rangle$ ,  $d \mid f$  and  $d \mid g$ . Since  $d \in \langle f, g \rangle$ ,  $d = af + bg$  for some  $a, b \in F[x]$ . If  $h \mid f$  and  $h \mid g$ , then  $h \mid af + bg = d$  (Proposition 5.1.1 (c)). So  $d$  is a monic common divisor that every common divisor divides:  $d = \gcd(f, g)$  by Definition 5.2.2.

**Marking scheme.** (10 points) - 1: a non-zero element of least degree exists, with the well-ordering of  $\mathbb{N}$  cited. - 1: it is made monic, and the monic element is shown to lie in  $I$  (absorption). - 3: an arbitrary element of  $I$  is divided by  $d$ , and the remainder is shown to lie in  $I$ . - 2: minimality of the degree forces the remainder to be 0. - 1: uniqueness of the monic generator (by any route: mutual divisibility, or minimality of the degree applied to the difference). - 2:  $d \mid f$ ,  $d \mid g$ ,  $d = af + bg$ , and “every common divisor divides  $d$ ” are read off from  $\langle f, g \rangle = \langle d \rangle$ , and  $d = \gcd(f, g)$  is concluded from the definition.

Fatal errors (0 for the step): assuming that the gcd is a combination of  $f$  and  $g$  (circular); “ $d$  divides  $f$  because  $d$  has least degree”, with no division step; citing Theorem 5.2.5 (c) or the gcd clause of Lemma 5.2.4 for (b) (both are proved from Bézout’s theorem). A second route for (b), the Euclidean algorithm with back-substitution by induction on the number of steps, may use the ideal equality of Lemma 5.2.4; it earns the 2 points of (b) when it shows that the monic associate of the last non-zero remainder divides  $f$  and  $g$ , is a combination of them, and is divisible by every common divisor. Existence in (a) has no second route here.

### Exercise. C2: Scaling the gcd

Let  $F$  be a field,  $f, g \in F[x]$ , and  $h \in F[x]$  monic. Prove that  $\gcd(hf, hg) = h \gcd(f, g)$ .

*Solution* (Hint 1). Compare the ideals  $\langle hf, hg \rangle$  and  $\langle f, g \rangle$ .

*Solution* (Hint 2). Show first that  $\langle hf, hg \rangle = \{hu : u \in \langle f, g \rangle\}$ .

*Solution.* If  $f = g = 0$ , then  $hf = hg = 0$ , and both sides are 0:  $\gcd(0, 0) = 0 = h \cdot 0$ .

Otherwise let  $d := \gcd(f, g)$ , monic, with  $\langle f, g \rangle = \langle d \rangle$  (Theorem 5.2.2 (c)). Since  $h$  is monic,  $h \neq 0$ , and one of  $hf, hg$  is non-zero (Corollary 4.3.3 (a)); so Theorem 5.2.2 applies to  $(hf, hg)$  as well.

*The ideals.* For  $a, b \in F[x]$ ,  $a(hf) + b(hg) = h(af + bg)$ . As  $a, b$  range over  $F[x]$ ,  $af + bg$  ranges over  $\langle f, g \rangle = \langle d \rangle$ , so

$$\langle hf, hg \rangle = \{h \cdot cd : c \in F[x]\} = \{c \cdot hd : c \in F[x]\} = \langle hd \rangle.$$

*The generator.*  $hd$  is monic, since  $\text{lc}(hd) = \text{lc}(h)\text{lc}(d) = 1$  (Theorem 4.3.2 (b)). By Theorem 5.2.2 (c),  $\langle hf, hg \rangle = \langle \gcd(hf, hg) \rangle$  with  $\gcd(hf, hg)$  monic; by the uniqueness in Theorem 5.2.1 (b),  $\gcd(hf, hg) = hd = h \gcd(f, g)$ .

This is the polynomial twin of Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Exercise (C2: Scaling the gcd) ( $\gcd(ka, kb) = k \gcd(a, b)$  for  $k > 0$ ), with “monic” in place of “positive”. Without “monic” the formula fails:  $\gcd(2x, 2) = 1 \neq 2 = 2 \gcd(x, 1)$  in  $\mathbb{Q}[x]$ .

**Marking scheme.** (10 points) - 2: treats  $f = g = 0$  by the convention, and checks that  $hf, hg$  are not both 0 otherwise (no zero divisors in  $F[x]$ ). - 4: shows  $\langle hf, hg \rangle = \langle hd \rangle$ , citing  $\langle f, g \rangle = \langle d \rangle$ . - 2: shows  $hd$  is monic. - 2: concludes  $\gcd(hf, hg) = hd$  by the uniqueness of the monic generator.

Fatal errors (0 for the step): asserting that every common divisor of  $hf$  and  $hg$  is  $h$  times a common divisor of  $f$  and  $g$  (false: 1 divides  $x \cdot x$  and  $x \cdot (x + 1)$ , and 1 is not  $x$  times a polynomial); using factorizations into irreducibles, which this section does not have. A second route ( $hd = (hf)a + (hg)b$  is a monic common divisor and a combination, so every common divisor divides it) scores 2 for the zero case, 3 for “monic common divisor and combination”, 3 for “every common divisor divides  $hd$ ”, 2 for the conclusion by Definition 5.2.2.

### Exercise. C3: The gcd of two binomials

Let  $F$  be a field. For  $m, n \in \mathbb{N}$ , not both 0, prove that

$$\gcd(x^m - 1, x^n - 1) = x^{\gcd(m, n)} - 1$$

in  $F[x]$  (here  $x^0 - 1 = 0$ , and  $\gcd(m, n)$  is the integer gcd). Compute  $\gcd(x^{12} - 1, x^{18} - 1)$ .

*Solution. Two remarks.* For  $m \geq 1$ ,  $x^m - 1$  is monic of degree  $m$ . And for  $m \geq n \geq 1$ , by the power laws (Lemma 4.1.1 (c)),

$$x^m - 1 = x^{m-n}(x^n - 1) + (x^{m-n} - 1),$$

since  $x^{m-n}x^n - x^{m-n} + x^{m-n} - 1 = x^m - 1$ .

We prove, by Logic and Proof, Axiom 4.2.1 (through Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Corollary 1.7.3 (b)) on  $s$ , the statement  $P(s)$ : “for all  $m, n \in \mathbb{N}$ , not both 0, with  $m + n \leq s$ , the displayed formula holds”.  $P(0)$  holds vacuously:  $m + n \leq 0$  forces  $m = n = 0$ . Suppose  $P(s)$ , and let  $m + n \leq s + 1$ , not both 0. If  $m + n \leq s$ , use  $P(s)$ . Otherwise  $m + n = s + 1$ .

*Case  $n = 0$ .* Then  $m \geq 1$ . The gcd of  $x^m - 1$  and 0 is the monic generator of  $\langle x^m - 1, 0 \rangle = \langle x^m - 1 \rangle$  (Theorem 5.2.2 (c)), which is  $x^m - 1$ . On the integer side, the common divisors of  $m$  and 0 are the divisors of  $m$ , and the greatest is  $m$  (Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Proposition 3.1.1 (a), (e)), so  $\gcd(m, 0) = m$ . Both sides are  $x^m - 1$ . *Case  $m = 0$*  is the same, since both gcds are symmetric.

*Case  $m, n \geq 1$ .* Both gcds are symmetric, so we may suppose  $m \geq n$ . By the identity above and [Lemma 5.2.4](#),

$$\gcd(x^m - 1, x^n - 1) = \gcd(x^n - 1, x^{m-n} - 1).$$

The pair  $(n, m - n)$  is not  $(0, 0)$ , since  $n \geq 1$ , and  $n + (m - n) = m < m + n = s + 1$ , so  $P(s)$  applies to it: the right side is  $x^{\gcd(n, m-n)} - 1$ . Finally  $m = 1 \cdot n + (m - n)$ , so Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , Lemma 3.2.3 gives  $\gcd(m, n) = \gcd(n, m - n)$ . This proves  $P(s + 1)$ .

Since every pair  $(m, n)$  has  $m + n \leq s$  for  $s = m + n$ , the formula holds for all  $m, n$ . For  $m = 12, n = 18$ :  $\gcd(12, 18) = 6$ , so  $\gcd(x^{12} - 1, x^{18} - 1) = x^6 - 1$ .

Each polynomial step is one step  $(m, n) \mapsto (n, m - n)$  of the subtractive Euclidean algorithm on the exponents.