

5.3 Irreducible Polynomials and Unique Factorization

Over every field, $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$. Over $\mathbb{Q}$ the last factor cannot be split further; over $\mathbb{F}_5$ it can, and $x^4 - 1$ becomes a product of four factors of degree 1; over $\mathbb{F}_2$ all of them coincide, and $x^4 - 1 = (x + 1)^4$. So the “primes” of $F[x]$ depend on the field F . Once F is fixed, though, every polynomial of positive degree splits into such primes in essentially one way, as every positive integer does in *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.3, and for the same reason: a prime that divides a product divides one of the factors.

Sections 5.1 and 5.2 supplied the tools: division with remainder (Theorem 5.1.2), the monic greatest common divisor and its Bézout identity (Theorem 5.2.2). This section spends them. Throughout, F is a field, and $F[x]$ is a commutative ring with no zero divisors (Theorem 4.2.4 (a), Corollary 4.3.3); degrees of products add (Theorem 4.3.2 (b)), and the units of $F[x]$ are the non-zero constants (Proposition 5.1.1 (e)).

5.3.1 Irreducible polynomials

In $\mathbb{Z}$, a prime is a number $p \geq 2$ whose only positive divisors are 1 and p . Two features of that definition need adjusting for polynomials. “Positive” has no meaning in $F[x]$, and its job there was to ignore the units ± 1 ; in $F[x]$ the units are the non-zero constants, so we ignore those. And “ $p \geq 2$ ” kept the units themselves from counting as primes; in $F[x]$ the condition becomes “degree at least 1”.

An irreducible polynomial is one that cannot be split into two factors of smaller degree.

Definition 5.3.1. Irreducible Polynomial

Let F be a field and $p \in F[x]$. The polynomial p is **irreducible over F** if $\deg p \geq 1$ and, **whenever** $p = gh$ with $g, h \in F[x]$, **one** of g, h is a constant. A polynomial of degree at least 1 that is not irreducible over F is **reducible over F** .

In words: the first clause rules out 0 and the non-zero constants; the second says that every way of writing p as a product uses a constant factor. That constant is never 0, since $p \neq 0$. So p is reducible exactly when $p = gh$ with $\deg g \geq 1$ and $\deg h \geq 1$; then $\deg g + \deg h = \deg p$ (Theorem 4.3.2 (b)), so both factors have degree **strictly** less than $\deg p$.

Examples.

- Every polynomial of degree 1 is irreducible. If $p = gh$ with $\deg p = 1$, the degrees of g and h are natural numbers adding up to 1, so one of them is 0.
- $x^2 + x = x(x + 1)$ and $x^3 = x \cdot x^2$ are reducible over every field: each is a product of two factors of degree at least 1.
- $x^2 + 1$ is reducible over $\mathbb{F}_2$, where $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ because $2 = 0$. Over $\mathbb{Q}$ it is irreducible, as the next proposition shows. The polynomial is the same; the field changed, and with it the answer. This is why the definition says “over F ”.
- If p is irreducible and $a \in F$ is non-zero, then ap is irreducible. First, $\deg(ap) = \deg p \geq 1$ (Theorem 4.3.2 (b)), and a factorization $ap = gh$ gives $p = (a^{-1}g)h$, so $a^{-1}g$ or h is a constant, and then so is g or h . Associates of irreducibles are irreducible.

🕒 **Second reading** · *The degenerate cases: constants*

The constants are kept out by the first clause, and each for a reason. Without it, the polynomial 0 would pass the second clause, since every factorization $0 = gh$ has $g = 0$ or $h = 0$ (Corollary 4.3.3), a constant. But every polynomial divides 0 (Proposition 5.1.1 (a)), so 0 behaves like the integer 0, not like a prime. A non-zero constant a is a unit: it divides everything, and every factorization $a = gh$ has two constant factors, since the degrees add up to 0. If units counted as irreducible, every factorization could be padded with as many of them as we like, just as $(1, 2, 2, 3, 5)$ would pad the factorization of 60 if 1 were prime. The clause $\deg p \geq 1$ plays the part of the integer condition $p \geq 2$.

For polynomials of degree 2 and 3, irreducibility can be decided by looking for roots.

Proposition 5.3.1. Irreducibility in Low Degree

Let F be a field and $p \in F[x]$.

- (a) If $\deg p \geq 2$ and p has a root in F , then p is reducible over F .
- (b) If $\deg p \in \{2, 3\}$, then p is irreducible over F **if and only if** p has no root in F .

Proof. (a) Let $c \in F$ be a root of p . By Theorem 5.1.3 (b), $p = (x - c)q$ for some $q \in F[x]$. Then $\deg q = \deg p - 1 \geq 1$ by Theorem 4.3.2 (b), and $\deg(x - c) = 1$, so neither factor is a constant and p is reducible.

(b) $(\Rightarrow)$ is (a), read contrapositively. $(\Leftarrow)$ Suppose p is reducible, so $p = gh$ with $\deg g, \deg h \geq 1$ and $\deg g + \deg h = \deg p \in \{2, 3\}$. Two natural numbers, each at least 1, with sum 2 or 3: one of them is 1. So p has a factor of degree 1, and Theorem 5.1.3 (c) gives a root of p in F . ■

For $x^2 + 1$ over $\mathbb{Q}$: for every $c \in \mathbb{Q}$, $c^2 \geq 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (e), with $0^2 = 0$), so $c^2 + 1 \geq 1 > 0$ by (b) and (e) of the same proposition. There is no rational root, and (b) makes $x^2 + 1$ irreducible over $\mathbb{Q}$. The same lines work in every ordered field, so $x^2 + 1$ is irreducible over $\mathbb{R}$ as well.

Warning. “No root” does not mean “irreducible” in degree 4 and above. For $c \in \mathbb{Q}$, $c^4 = (c^2)^2 \geq 0$, so $c^4 + 4 \geq 4 > 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (h)): the polynomial $x^4 + 4$ has no rational root. Yet

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

as expanding the right side shows: the terms in x^3 , x^2 and x cancel. Proposition [Proposition 5.3.1](#) (b) is about degrees 2 and 3 only, where every splitting must contain a factor of degree 1; in degree 4 a splitting may be $2 + 2$, with no factor of degree 1 and so no root.

Quick check. Is $2x^2 + 4$ irreducible over $\mathbb{Q}$? Is $x^2 + 2$ irreducible over $\mathbb{F}_3$?

Solution. Over $\mathbb{Q}$, yes: $2x^2 + 4 = 2(x^2 + 2)$, and $x^2 + 2$ has no rational root ($c^2 + 2 \geq 2 > 0$, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (e), (h)), so it is irreducible by Proposition 5.3.1 (b), and so is its associate $2x^2 + 4$. The factor 2 is a constant, so $2 \cdot (x^2 + 2)$ is not a splitting into non-constants. Over $\mathbb{F}_3$, no: $1^2 + 2 = 3 = 0$, so 1 is a root, and indeed $x^2 + 2 = x^2 - 1 = (x - 1)(x + 1)$ in $\mathbb{F}_3$.

5.3.2 Euclid's lemma for polynomials

The definition of an irreducible p speaks about the factors of p . Unique factorization needs a statement about the polynomials that p **divides**. As in $\mathbb{Z}$, the bridge is the Bézout identity, and the move is the one of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.3: **multiply the Bézout identity**.

Theorem 5.3.2. Euclid's Lemma for Polynomials

Let F be a field and $f, g, h \in F[x]$. If $f \mid gh$ and $\gcd(f, g) = 1$, then $f \mid h$.

Proof. Since $\gcd(f, g) = 1$, Corollary 5.2.3 gives $a, b \in F[x]$ with $af + bg = 1$. Multiplying by h ,

$$h = h(af + bg) = (ah)f + b(gh).$$

Now $f \mid f$ and $f \mid gh$, so f divides the combination $(ah)f + b(gh)$ (Proposition 5.1.1 (c)). Hence $f \mid h$. ■

The hypothesis $\gcd(f, g) = 1$ is needed. In $\mathbb{Q}[x]$, $x^2 \mid x \cdot x$, but $x^2 \nmid x$, since a divisor of a non-zero polynomial has degree at most its degree (Proposition 5.1.1 (d)); here $\gcd(x^2, x) = x$.

For an irreducible p , the coprimality comes almost free, exactly as it did for a prime number.

Corollary 5.3.3. An Irreducible Dividing a Product

Let F be a field and $p \in F[x]$ irreducible over F .

- (a) For every $f \in F[x]$: $p \mid f$ or $\gcd(p, f) = 1$.
- (b) For all $g, h \in F[x]$: if $p \mid gh$, then $p \mid g$ or $p \mid h$.
- (c) If $(q_1, \dots, q_l)$ is a list of polynomials in $F[x]$, with $l \in \mathbb{N}$, and $p \mid q_1 q_2 \cdots q_l$, then $l \geq 1$ and $p \mid q_j$ for some $j \in \{1, \dots, l\}$.
- (d) If p and q are monic and irreducible over F and $p \mid q$, then $p = q$.

Here $q_1 q_2 \cdots q_l$, also written $\prod_{j=1}^l q_j$, is the product of a finite list in the commutative ring $F[x]$, given by the recursion of Sets, Relations, and Cardinality, Definition 2.3.1 as Lemma 4.1.1 (a) reads it: the empty product is 1, and $\prod_{j=1}^{l+1} q_j = (\prod_{j=1}^l q_j) q_{l+1}$.

Idea. For (a), the gcd of p and f is a monic divisor of p , and an irreducible p has only two kinds of divisors: constants and associates of itself. Part (b) is Euclid's lemma in the coprime case of (a). For (c), peel the last factor off the product and apply (b); induction on the length does the rest. For (d), the cofactor of p in q must be a constant, and comparing leading coefficients makes it 1.

Proof. (a) Since $p \neq 0$, the gcd $d := \gcd(p, f)$ is monic (Definition 5.2.2, Theorem 5.2.2 (c)). It divides p : write $p = du$ with $u \in F[x]$. As p is irreducible, d or u is a constant. If d is a constant, it is a monic constant, so $d = 1$. If u is a constant, then $u \neq 0$ (as $p \neq 0$) and $d = u^{-1}p$; since $d \mid f$, $f = dk = p(u^{-1}k)$ for some $k \in F[x]$, so $p \mid f$.

(b) Let $p \mid gh$. By (a), $p \mid g$ or $\gcd(p, g) = 1$, and in the second case Theorem 5.3.2 gives $p \mid h$.

(c) By Logic and Proof, Axiom 4.2.1 (on $\mathbb{N} = \omega$, Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\mathbb{R}\setminus)$, Corollary 1.7.3 (b)) we prove, for every $l \in \mathbb{N}$, the statement $P(l)$: “for every list $(q_1, \dots, q_l)$ in $F[x]$ with $p \mid \prod_{j=1}^l q_j$, we have $l \geq 1$ and $p \mid q_j$ for some $j \leq l$ ”.

Base case $P(0)$. The empty product is 1, and $p \nmid 1$: otherwise $\deg p \leq \deg 1 = 0$ by Proposition 5.1.1 (d), against $\deg p \geq 1$. So the hypothesis of $P(0)$ never holds, and $P(0)$ is true.

Step. Assume $P(l)$, and let $p \mid \prod_{j=1}^{l+1} q_j = (\prod_{j=1}^l q_j)q_{l+1}$. By (b), p divides the first factor or $p \mid q_{l+1}$. In the first case $P(l)$ gives $j \leq l$ with $p \mid q_j$; in the second, take $j = l + 1$. Either way $l + 1 \geq 1$, and $P(l + 1)$ holds.

(d) Write $q = pu$ with $u \in F[x]$. As q is irreducible, p or u is a constant, and p is not, since $\deg p \geq 1$. So u is a non-zero constant, and comparing leading coefficients (Theorem 4.3.2 (b)) gives $1 = 1 \cdot u$. Hence $u = 1$ and $p = q$.

■

Part (b) fails for reducible polynomials: $x^2 \mid x \cdot x$ with $x^2 \nmid x$. Part (d) needs “monic”: x and $2x$ are irreducible over $\mathbb{Q}$, and each divides the other.

The same multiplication of a Bézout identity combines two coprime divisors.

Proposition 5.3.4. Coprime Divisors of a Polynomial

Let F be a field and $m, n, h \in F[x]$ with $m \mid h$, $n \mid h$ and $\gcd(m, n) = 1$. Then $mn \mid h$.

Proof. Write $h = mk$ with $k \in F[x]$. Then $n \mid mk$, and $\gcd(n, m) = \gcd(m, n) = 1$, since the clauses of Definition 5.2.2 do not depend on the order of the two polynomials. By Theorem 5.3.2, $n \mid k$; say $k = nt$. Then $h = m(nt) = (mn)t$, so $mn \mid h$.

■

Without coprimality the conclusion fails: $x \mid x$ twice over, yet $x \cdot x = x^2 \nmid x$.

Quick check. In $\mathbb{F}_2[x]$, the polynomial $x^2 + 1$ divides $(x + 1)(x + 1)$, but divides neither factor. Does this contradict [Corollary 5.3.3](#) (b)?

Solution. No. In $\mathbb{F}_2[x]$, $(x + 1)(x + 1) = x^2 + 1$, so $x^2 + 1$ is reducible over $\mathbb{F}_2$, and the corollary says nothing about it. (It divides neither factor because each factor has degree $1 < 2$, Proposition 5.1.1 (d).)

5.3.3 Factors that cannot be split further

The existence half of unique factorization needs a supply of irreducibles: every polynomial of positive degree must have an irreducible factor. In $\mathbb{Z}$, the least divisor at least 2 was prime (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 3.3.4). For polynomials, size becomes degree, and the “least divisor” becomes a monic divisor of least positive degree.

Lemma 5.3.5. An Irreducible Factor Exists

Let F be a field and $f \in F[x]$ with $\deg f \geq 1$. Then f has a **monic** irreducible divisor in $F[x]$.

Idea. Among the monic divisors of positive degree, take one of least degree. A splitting of it into two non-constants would produce a monic divisor of smaller positive degree.

Proof. Let c be the leading coefficient of f , and let

$$D := \{\deg d : d \in F[x] \text{ monic, } \deg d \geq 1, d \mid f\} \subseteq \mathbb{N}.$$

The monic associate $c^{-1}f$ has degree $\deg f \geq 1$ and divides $f = c \cdot (c^{-1}f)$, so D is non-empty. By Sets, Relations, and Cardinality, Theorem 2.1.3 (on $\mathbb{N} = \omega$ it is Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 1.6.2), D has a least element n_0 ; let p be a monic divisor of f of degree n_0 . Then $\deg p = n_0 \geq 1$.

Suppose $p = gh$ with $\deg g \geq 1$ and $\deg h \geq 1$. Then $\deg g = n_0 - \deg h < n_0$ (Theorem 4.3.2 (b)). Let g_1 be the monic associate of g , so $g = \text{lc}(g)g_1$ and $\deg g_1 = \deg g$. Then $g_1 \mid g$, $g \mid p$ and $p \mid f$, so $g_1 \mid f$ (Proposition 5.1.1 (b)), and $\deg g_1 \in D$ is smaller than n_0 , against the choice of n_0 . So every factorization $p = gh$ has a constant factor, and p is irreducible. ■

This is Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 3.3.4 with degree in place of size; the twin is compared with, not used.

5.3.4 Unique factorization

Two facts about products of lists. The proof below handles lists of polynomials, and it uses two facts about their products, both proved by induction on the length from the recursion of

the product. Let $(q_1, \dots, q_l)$ be a list in $F[x]$, with $l \in \mathbb{N}$.

- (L1) If every q_j is non-zero, then $\prod_{j=1}^l q_j \neq 0$, and its degree is $\sum_{j=1}^l \deg q_j$. If every q_j is monic, so is the product.
- (L2) If $l \geq 1$ and $j \in \{1, \dots, l\}$, let $(q'_1, \dots, q'_{l-1})$ be the list with the entry j removed: $q'_t := q_t$ for $t < j$ and $q'_t := q_{t+1}$ for $j \leq t \leq l-1$. Then $\prod_{t=1}^l q_t = (\prod_{t=1}^{l-1} q'_t) q_j$. In particular every entry of a list divides its product.

The names (L1), (L2) are used throughout this chapter.

○ **Second reading** · *Proofs of (L1) and (L2)*

(L1). Induction on l . For $l = 0$ the product is 1, which is monic of degree 0, the empty sum. If the claim holds for l , then $\prod_{j=1}^{l+1} q_j = (\prod_{j=1}^l q_j) q_{l+1}$ is a product of two non-zero polynomials, so it is non-zero with degree $\sum_{j=1}^l \deg q_j + \deg q_{l+1}$ and leading coefficient the product of the two leading coefficients (Theorem 4.3.2 (b)); that is $1 \cdot 1 = 1$ when both factors are monic.

(L2). Induction on $l \geq 1$, for all $j \leq l$ at once. For $l = 1$, $j = 1$, the shortened list is empty and both sides are q_1 . Suppose the claim holds for lists of length l , and let $(q_1, \dots, q_{l+1})$ and $j \leq l+1$ be given. If $j = l+1$, the shortened list is $(q_1, \dots, q_l)$ and the claim is the recursion itself. If $j \leq l$, the claim for the list $(q_1, \dots, q_l)$ and the same j gives $\prod_{t=1}^l q_t = (\prod_{t=1}^{l-1} r_t) q_j$, where $(r_1, \dots, r_{l-1})$ is $(q_1, \dots, q_l)$ with entry j removed. The list $(q'_1, \dots, q'_l)$ obtained from $(q_1, \dots, q_{l+1})$ has the first $l-1$ entries $r_1, \dots, r_{l-1}$ and the last entry $q'_l = q_{l+1}$. So, by the recursion twice and commutativity and associativity in $F[x]$,

$$\begin{aligned} \prod_{t=1}^{l+1} q_t &= \left(\prod_{t=1}^{l-1} r_t \right) q_j q_{l+1} \\ &= \left(\left(\prod_{t=1}^{l-1} r_t \right) q_{l+1} \right) q_j = \left(\prod_{t=1}^l q'_t \right) q_j. \end{aligned}$$

The last clause of (L2) follows: q_j divides $(\prod_t q'_t) q_j$.

Everything is now in place.

Theorem 5.3.6. Unique Factorization of Polynomials

Let F be a field and $f \in F[x]$ with $\deg f \geq 1$ and leading coefficient c .

- (a) **Existence.** There are $k \geq 1$ and monic polynomials $p_1, \dots, p_k$, irreducible over F , with $f = c p_1 p_2 \cdots p_k$.
- (b) **Uniqueness.** If also $f = c' q_1 q_2 \cdots q_l$ with $c' \in F$, $l \in \mathbb{N}$ and monic polynomials $q_1, \dots, q_l$ irreducible over F , then $c' = c$, $l = k$, and there is a bijection $\sigma: \{1, \dots, k\} \rightarrow \{1, \dots, l\}$ (Sets, Relations, and Cardinality, Definition 1.4.5) with $q_{\sigma(i)} = p_i$ for every i .

In words: every polynomial of positive degree is its leading coefficient times a product of monic irreducibles, and the leading coefficient and the irreducibles, counted with repetition, are determined by f ; only their order is free. The bijection σ says “the same list, possibly in another order”: it matches each p_i with an equal $q_{\sigma(i)}$, and each q is used exactly once.

Idea. Existence. Split off one monic irreducible factor (Lemma 5.3.5); the cofactor has smaller degree, so strong induction on the degree factors it.

Uniqueness. Divide by the leading coefficient, so that both products are equal products of monic irreducibles. The last factor p_{k+1} of one list divides the other product, so by Euclid's lemma (in the form Corollary 5.3.3 (c)) it divides one of the q_j , and, both being monic and irreducible, it **equals** it. Cancel it from both sides and use induction on the length.

Before reading on: where is Euclid's lemma used, and why does “monic” turn “ p_{k+1} is a constant times q_j ” into “ $p_{k+1} = q_j$ ”?

Proof. Existence. We prove, by Logic and Proof, Theorem 4.2.2 on $n \in \mathbb{N}$ (read on ω : its proof uses only Logic and Proof, Axiom 4.2.1 and Number Systems: From $\setminus(\setminus n \mathbb{N} \setminus)$ to $\setminus(\setminus n \mathbb{R} \setminus)$, Theorem 1.6.1 (a), (b), (d), as in Section 3.1), the statement $E(n)$: “every **monic** $g \in F[x]$ of degree $n \geq 1$ is a product $p_1 \cdots p_k$ of a list of monic irreducibles, $k \geq 1$ ”. For $n = 0$ there is nothing to prove. Let $n \geq 1$, assume $E(m)$ for every $m < n$, and let g be monic of degree n . By Lemma 5.3.5, $g = pu$ with p monic and irreducible, and $u \in F[x]$. Comparing leading coefficients (Theorem 4.3.2 (b)), $1 = 1 \cdot \text{lc}(u)$, so u is monic, and $\deg u = n - \deg p < n$. If $\deg u = 0$, then $u = 1$ and $g = p$ is a list of length 1. Otherwise $E(\deg u)$ gives $u = p_1 \cdots p_r$ with monic irreducibles p_i , and the list $(p_1, \dots, p_r, p)$ has, by the recursion, the product $(\prod_{i=1}^r p_i)p = up = g$. This proves $E(n)$.

Now let f be as in the theorem. Its monic associate $c^{-1}f$ has degree $\deg f \geq 1$, so $c^{-1}f = p_1 \cdots p_k$ by $E(\deg f)$, and $f = cp_1 \cdots p_k$.

Uniqueness. By (L1), $q_1 \cdots q_l$ is monic. As $f \neq 0$, $c' \neq 0$, and comparing leading coefficients in $f = c'q_1 \cdots q_l$ (Theorem 4.3.2 (b)) gives $c = c' \cdot 1 = c'$. Multiplying both expressions for f by c^{-1} ,

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l.$$

It remains to prove, by Logic and Proof, Axiom 4.2.1 on $k \in \mathbb{N}$, the statement $U(k)$: “for every $l \in \mathbb{N}$, if $(p_1, \dots, p_k)$ and $(q_1, \dots, q_l)$ are lists of monic irreducibles with $\prod_{i=1}^k p_i = \prod_{j=1}^l q_j$, then $l = k$ and there is a bijection $\sigma: \{1, \dots, k\} \rightarrow \{1, \dots, l\}$ with $q_{\sigma(i)} = p_i$ for every $i \leq k$ ”.

Base case $U(0)$. The empty product is 1, of degree 0. By (L1), $\prod_{j=1}^l q_j$ has degree $\sum_j \deg q_j \geq l$, since each $\deg q_j \geq 1$. So $l = 0$, and the empty function $\emptyset \rightarrow \emptyset$ is the required bijection.

Step. Assume $U(k)$, and let $(p_1, \dots, p_{k+1})$ and $(q_1, \dots, q_l)$ be lists of monic irreducibles with the same product N . By the recursion, $N = (\prod_{i=1}^k p_i)p_{k+1}$, so $p_{k+1} \mid N = \prod_{j=1}^l q_j$. By Corollary 5.3.3 (c), $l \geq 1$ and $p_{k+1} \mid q_j$ for some $j \leq l$; by Corollary 5.3.3 (d), $p_{k+1} = q_j$. Let $(q'_1, \dots, q'_{l-1})$ be the q -list with entry j removed. By (L2),

$$\left(\prod_{i=1}^k p_i\right)p_{k+1} = N = \left(\prod_{t=1}^{l-1} q'_t\right)q_j = \left(\prod_{t=1}^{l-1} q'_t\right)p_{k+1}.$$

Since $p_{k+1} \neq 0$, we may cancel it (Corollary 4.3.3 (b)): $\prod_{i=1}^k p_i = \prod_{t=1}^{l-1} q'_t$. The list $(q'_1, \dots, q'_{l-1})$ consists of monic irreducibles, so $U(k)$, applied with $l-1 \in \mathbb{N}$, gives $l-1 = k$ and a bijection $\sigma': \{1, \dots, k\} \rightarrow \{1, \dots, l-1\}$ with $q'_{\sigma'(i)} = p_i$.

Let $\tau: \{1, \dots, l-1\} \rightarrow \{1, \dots, l\} \setminus \{j\}$ be $\tau(t) := t$ for $t < j$ and $\tau(t) := t+1$ for $t \geq j$. It is a bijection (its inverse sends $s < j$ to s and $s > j$ to $s-1$), and $q'_t = q_{\tau(t)}$ by the definition of

q' . Define $\sigma: \{1, \dots, k+1\} \rightarrow \{1, \dots, l\}$ by $\sigma(i) := \tau(\sigma'(i))$ for $i \leq k$ and $\sigma(k+1) := j$. On $\{1, \dots, k\}$, σ is a bijection onto $\{1, \dots, l\} \setminus \{j\}$, a composite of two bijections; and it sends $k+1$ to the one remaining point j . So σ is injective and surjective, a bijection. Finally $q_{\sigma(i)} = q_{\tau(\sigma'(i))} = q'_{\sigma'(i)} = p_i$ for $i \leq k$, and $q_{\sigma(k+1)} = q_j = p_{k+1}$; and $l = k+1$. This proves $U(k+1)$, and the theorem. ■

The answer to the prompt. Euclid's lemma enters at one line, " $p_{k+1} \mid q_j$ for some j ": that is [Corollary 5.3.3](#) (c), whose step is (b), which is [Theorem 5.3.2](#) in the coprime case. "Monic" enters twice. Irreducibility of q_j only gives $q_j = p_{k+1}u$ with u a non-zero constant; both being monic forces $u = 1$ (part (d)), and without that the cancellation would leave a stray constant u on one side. And the leading coefficients c, c' can be compared only because the products of monic lists are monic.

Remark. In $\mathbb{Z}$, *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.3 stated uniqueness for **non-decreasing** lists of primes (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.3.5), so that two factorizations of the same number are literally equal. Polynomials have no natural order to sort by, so here "the same up to order" is said with a bijection of indices.

Example. The Factorizations of $x^4 - 1$

Factor $x^4 - 1$ into monic irreducibles over $\mathbb{Q}$, over $\mathbb{R}$, over $\mathbb{F}_3$, over $\mathbb{F}_5$ and over $\mathbb{F}_2$.

Solution. Over every field, $(x-1)(x+1) = x^2 - 1$ and $(x^2 - 1)(x^2 + 1) = x^4 - 1$, by expanding, so

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

The two factors of degree 1 are irreducible. Everything depends on $x^2 + 1$, which by [Proposition 5.3.1](#) (b) is irreducible exactly when it has no root in the field.

- $\mathbb{Q}$ and $\mathbb{R}$. No root, since $c^2 + 1 \geq 1 > 0$ in an ordered field (after [Proposition 5.3.1](#)). So $(x-1, x+1, x^2 + 1)$ is the factorization, with leading coefficient 1.
- $\mathbb{F}_3$. The values of $x^2 + 1$ at 0, 1, 2 are 1, 2, 5 = 2: no root. The factorization is $(x-1, x+1, x^2 + 1)$ again, with $x+1 = x-2$.
- $\mathbb{F}_5$. Here $2^2 + 1 = 5 = 0$, and indeed $(x-2)(x-3) = x^2 - 5x + 6 = x^2 + 1$ in $\mathbb{F}_5$. So $x^4 - 1 = (x-1)(x-2)(x-3)(x-4)$, using $x+1 = x-4$: four factors of degree 1.
- $\mathbb{F}_2$. Here $-1 = 1$, so $x-1 = x+1$, and $x^2 + 1 = (x+1)^2$ (the example after [Definition 5.3.1](#)). So $x^4 - 1 = (x+1)^4$: one irreducible, four times.

By [Theorem 5.3.6](#), each of these lists is the only one up to order.

Quick check. Is $x^2 + x + 1$ irreducible over $\mathbb{F}_2$? Over $\mathbb{F}_3$?

Solution. Over $\mathbb{F}_2$, its values at 0 and 1 are 1 and 3 = 1: no root, so it is irreducible ([Proposition 5.3.1](#) (b)). Over $\mathbb{F}_3$, $1 + 1 + 1 = 3 = 0$, so 1 is a root and it is reducible; indeed

$$(x-1)^2 = x^2 - 2x + 1 = x^2 + x + 1 \text{ in } \mathbb{F}_3.$$

5.3.5 Rational roots

Over $\mathbb{Q}$, the low-degree test of [Proposition 5.3.1](#) asks for rational roots, and there are infinitely many rationals to try. For a polynomial with integer coefficients and non-zero constant term the candidates can be listed (a zero constant term is dealt with by factoring out a power of x , below). The proof is about integers, not polynomials: here, unlike in the rest of this section, integer results of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3 (Euclid's lemma, lowest terms) are steps of the proof and not only compared with.

Theorem 5.3.7. Rational Root Test

Let $n \geq 1$, let $a_0, a_1, \dots, a_n \in \mathbb{Z}$ with $a_n \neq 0$, and let $f := \sum_{i=0}^n a_i x^i \in \mathbb{Q}[x]$. If $u \in \mathbb{Z}$, $v \in \mathbb{Z}_{>0}$, $\gcd(u, v) = 1$ and $f(u/v) = 0$, then $u \mid a_0$ and $v \mid a_n$ in $\mathbb{Z}$.

Idea. Clear denominators: $v^n f(u/v) = 0$ is an equation in $\mathbb{Z}$ in which every term but one is a multiple of u , and every term but another is a multiple of v . Then Euclid's lemma for integers strips the powers of v from $a_0 v^n$, one at a time.

Proof. Multiply $f(u/v) = 0$ by v^n . For $i \leq n$, $(u/v)^i v^i = u^i$ and $v^n = v^{n-i} v^i$ (Lemma 4.1.1 (c), in the commutative ring $\mathbb{Q}$), so

$$a_n u^n + a_{n-1} u^{n-1} v + \dots + a_1 u v^{n-1} + a_0 v^n = 0,$$

an equation between integers. Every term except the last contains the factor u , and every term except the first contains the factor v (as $n \geq 1$). So

$$a_0 v^n = -u \sum_{i=1}^n a_i u^{i-1} v^{n-i}, \quad a_n u^n = -v \sum_{i=0}^{n-1} a_i u^i v^{n-1-i},$$

and $u \mid a_0 v^n$, $v \mid a_n u^n$ in $\mathbb{Z}$.

We show $u \mid a_0 v^{n-j}$ for every $j \leq n$, by Logic and Proof, Axiom 4.2.1 on j . The case $j = 0$ is the line above. If $u \mid a_0 v^{n-j}$ with $j < n$, then $a_0 v^{n-j} = v \cdot (a_0 v^{n-j-1})$, and $\gcd(u, v) = 1$, so Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.3.1 gives $u \mid a_0 v^{n-(j+1)}$. At $j = n$: $u \mid a_0$. The same induction with the roles of u and v exchanged (and $\gcd(v, u) = \gcd(u, v) = 1$) turns $v \mid a_n u^n$ into $v \mid a_n$. ■

Every rational root has such a form: by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.3.6, each $r \in \mathbb{Q}$ is u/v with $u \in \mathbb{Z}$, $v \in \mathbb{Z}_{>0}$ and $\gcd(u, v) = 1$. So, when $a_0 \neq 0$, the rational roots of f are among the finitely many fractions u/v with $u \mid a_0$ and v a positive divisor of a_n : a divisor u of $a_0 \neq 0$ has $-|a_0| \leq u \leq |a_0|$, by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (d), (e), and likewise $1 \leq v \leq |a_n|$. If $a_0 = 0$, then 0 is a root; let k be the least index with $a_k \neq 0$ (so $k \leq n$). Then $f = x^k g$ with $g := \sum_{i=0}^{n-k} a_{i+k} x^i$, which has integer coefficients and constant term $a_k \neq 0$, and the non-zero rational roots of f are those

of g , since $f(r) = r^k g(r)$ (Theorem 4.4.1) and $\mathbb{Q}$ has no zero divisors; apply the test to g when $\deg g \geq 1$, and when $\deg g = 0$, g has no root. The test lists candidates; it does not say which of them are roots.

Example. A Cubic with No Rational Root

Show that $3x^3 + x^2 - 2$ is irreducible over $\mathbb{Q}$.

Solution. By Theorem 5.3.7, a rational root u/v in lowest terms has $u \mid -2$ and v a positive divisor of 3. The divisors of -2 are $\pm 1, \pm 2$, and the positive divisors of 3 are 1, 3 (a positive divisor of 3 is at most 3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (e), and $3 = 1 \cdot 2 + 1$). So the candidates are $\pm 1, \pm 2, \pm 1/3, \pm 2/3$. The values of $f := 3x^3 + x^2 - 2$ at them are

c	1	-1	2	-2	1/3	-1/3	2/3	-2/3
$f(c)$	2	-4	26	-22	-16/9	-2	-2/3	-22/9

For instance $f(2/3) = 3 \cdot \frac{8}{27} + \frac{4}{9} - 2 = \frac{8}{9} + \frac{4}{9} - 2 = -\frac{2}{3}$. None is 0, so f has no rational root, and as $\deg f = 3$, Proposition 5.3.1 (b) makes f irreducible over $\mathbb{Q}$.

Quick check. Which rational numbers can be roots of $2x^2 + 3x - 2$? Which are?

Solution. The candidates are u/v with $u \mid -2$ and $v \in \{1, 2\}$: $\pm 1, \pm 2, \pm 1/2$. Evaluating, the roots are $1/2$ and -2 ; indeed $2x^2 + 3x - 2 = (2x - 1)(x + 2)$.

Remark (Looking ahead). Two sharper tests for irreducibility over $\mathbb{Q}$, Gauss's lemma and Eisenstein's criterion, belong to a later algebra volume of the series; nothing in this volume uses them.

5.3.6 Exercises

5.3.6.1 A. Check your understanding

Exercise. A1

These questions are about the uniqueness half of the proof of Theorem 5.3.6.

- Which line of the proof uses Euclid's lemma, and through which result?
- Where is "monic" used?
- In $\mathbb{F}_5[x]$, run the induction step on the two lists $(p_1, p_2, p_3, p_4) = (x-1, x-2, x-3, x-4)$ and $(q_1, q_2, q_3, q_4) = (x-4, x-3, x-2, x-1)$. Which j matches p_4 ? What is the bijection σ at the end?

- (d) Why must the empty list be allowed?
- (e) Give the idea of the uniqueness proof in two sentences.

Solution.

- (a) The line “ $p_{k+1} \mid q_j$ for some $j \leq l$ ”. It cites [Corollary 5.3.3](#) (c), proved by induction from (b), which is [Theorem 5.3.2](#) applied when $\gcd(p, g) = 1$.
- (b) In $p_{k+1} = q_j$: from $p_{k+1} \mid q_j$ and irreducibility of q_j we only get $q_j = u p_{k+1}$ with u a non-zero constant, and comparing the leading coefficients $1 = u$ needs both monic ([Corollary 5.3.3](#) (d)). Also in $c' = c$: the products of the monic lists are monic by (L1).
- (c) $p_4 = x - 4$ divides $q_1 q_2 q_3 q_4$; the only q_j it divides is $q_1 = x - 4$, so $j = 1$ and $\sigma(4) = 1$. The shortened list is $(q'_1, q'_2, q'_3) = (x - 3, x - 2, x - 1)$, and $\tau(t) = t + 1$. The step for $k = 2$ matches $p_3 = x - 3$ with q'_1 , and so on down. Unwinding, $\sigma(i) = 5 - i$: $q_{5-i} = x - i = p_i$ for $i = 1, 2, 3, 4$.
- (d) The induction on k starts at $k = 0$, and $U(0)$ is about the empty list, whose product is 1; each step removes one entry, so the empty list is where every chain of steps ends.
- (e) The last irreducible of one factorization divides the other product, so by Euclid’s lemma it divides, and so equals, one of the other’s irreducibles. Cancel it from both sides and apply the induction hypothesis to the two shorter lists.

5.3.6.2 B. Practice

Exercise. B1: Determine which

Determine whether each polynomial is irreducible over the given field. Justify your answer.

- (a) $x^2 + 2$ over $\mathbb{Q}$, over $\mathbb{F}_2$, over $\mathbb{F}_3$.
- (b) $x^3 + x + 1$ over $\mathbb{F}_2$ and over $\mathbb{F}_3$.
- (c) $x^4 + 4$ over $\mathbb{Q}$.
- (d) $3x^3 + x^2 - 2$, with its coefficients read in $\mathbb{F}_2$.

Solution.

- (a) Over $\mathbb{Q}$: irreducible, since $c^2 + 2 \geq 2 > 0$ for $c \in \mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (e), (h)), so there is no root, and the degree is 2 ([Proposition 5.3.1](#) (b)). Over $\mathbb{F}_2$: $2 = 0$, so the polynomial is $x^2 = x \cdot x$, reducible. Over $\mathbb{F}_3$: $2 = -1$, so it is $x^2 - 1 = (x - 1)(x + 1)$, reducible.
- (b) Over $\mathbb{F}_2$: the values at 0 and 1 are 1 and $3 = 1$; no root, degree 3, irreducible. Over $\mathbb{F}_3$: the value at 1 is $3 = 0$, so it is reducible ([Proposition 5.3.1](#) (a)); indeed $x^3 + x + 1 = (x - 1)(x^2 + x + 2)$ in $\mathbb{F}_3$.
- (c) Reducible: $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$ (the warning after [Proposition 5.3.1](#)), although it has no rational root.
- (d) In $\mathbb{F}_2$, $3 = 1$ and $-2 = 0$, so the polynomial is $x^3 + x^2 = x^2(x + 1)$. It has the root 0 and degree 3, so it is reducible.

Exercise. B2: The polynomials vanishing at the square root of two

Let $s \in \mathbb{R}$ be the non-negative square root of 2 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 6.1.4, in the complete ordered field $\mathbb{R}$, and let

$$J := \{f \in \mathbb{Q}[x] : f(s) = 0\},$$

where $f(s)$ is computed in $\mathbb{R}$, reading $\mathbb{Q}[x] \subseteq \mathbb{R}[x]$ coefficientwise. Prove that $J = \langle x^2 - 2 \rangle$.

The beginning and the end of a proof are given.

J is an ideal of $\mathbb{Q}[x]$, since evaluation at s respects sums and products (Theorem 4.4.1). It contains $x^2 - 2$, and $1 \notin J$. Let d be a monic element of least degree in J . Let $f \in J$, and divide: $f = qd + r$ with $\deg r < \deg d$ (Theorem 5.1.2).

[Blank.]

So $J = \langle d \rangle$. Then $d \mid x^2 - 2$, and $\deg d \geq 2$: $\deg d = 0$ would make $d = 1 \in J$, and $\deg d = 1$ would give $d = x + a$ with $a \in \mathbb{Q}$ and $s = -a$, a rational number whose square is 2, against Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1. Hence $d = x^2 - 2$.

Name the move, then complete it.

Solution. The move is **least degree, then divide**: in a set closed under the right operations, a remainder on division by an element of least degree lies in the set and has smaller degree, so it is 0.

Completion of the blank: $r = f - qd$, and $f, d \in J$, so $r \in J$ because J is an ideal (it absorbs the multiple qd and is closed under differences). A non-zero r would be a non-zero element of J of degree less than $\deg d$; its monic associate would lie in J too and have the same degree, against the choice of d . So $r = 0$, and $f = qd \in \langle d \rangle$. Conversely every multiple of d lies in J . This is the argument of Theorem 5.2.1, run on J .

For the end: $d \mid x^2 - 2$ because $x^2 - 2 \in J = \langle d \rangle$. So $\deg d \leq 2$ (Proposition 5.1.1 (d)), and with $\deg d \geq 2$, $x^2 - 2 = du$ with u a constant; both being monic, $u = 1$. In the language of this section, $x^2 - 2$ is irreducible over $\mathbb{Q}$: it has degree 2 and no rational root, since a root c would satisfy $c^2 = 2$, against Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1 (Proposition 5.3.1 (b)). Every rational polynomial vanishing at s is a multiple of it.

Exercise. B3: The small irreducibles over the two-element field

List all irreducible polynomials of degree at most 3 over $\mathbb{F}_2$, and prove that the list is complete.

Solution. Over $\mathbb{F}_2$ the only non-zero constant is 1, so every non-zero polynomial is monic and associates are equal. There are $2 + 4 + 8 = 14$ polynomials of degree 1, 2 or 3: the coefficient of the top power is 1, and each lower coefficient is 0 or 1.

- **Degree 1:** x and $x + 1$, both irreducible (the first example after Definition 5.3.1).
- **Degrees 2 and 3:** by Proposition 5.3.1 (b), irreducible exactly when there is no root. The value at 0 is the constant term, and the value at 1 is the sum of the coefficients,

which is 0 in $\mathbb{F}_2$ exactly when the number of non-zero coefficients is even. So the irreducible ones have constant term 1 and an odd number of non-zero coefficients.

In degree 2, the candidates with constant term 1 are $x^2 + 1$ (two non-zero coefficients) and $x^2 + x + 1$ (three); only $x^2 + x + 1$ is irreducible. In degree 3 they are $x^3 + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$, $x^3 + x^2 + x + 1$, with two, three, three and four non-zero coefficients; so $x^3 + x + 1$ and $x^3 + x^2 + 1$ are irreducible. The complete list is

$$x, \quad x + 1, \quad x^2 + x + 1, \quad x^3 + x + 1, \quad x^3 + x^2 + 1.$$

5.3.6.3 C. Going deeper

Exercise. C1: Exit check: unique factorization

Prove the uniqueness half of [Theorem 5.3.6](#): if $c p_1 \cdots p_k = c' q_1 \cdots q_l$ with $c, c' \in F$ non-zero and all p_i, q_j monic irreducible over the field F , then $c = c'$, $l = k$, and the two lists agree up to a bijection of indices. You may cite Euclid's lemma ([Theorem 5.3.2](#)) and [Corollary 5.3.3](#).

Solution. The uniqueness part of the proof of [Theorem 5.3.6](#) is a complete answer. Its steps, in order: the products of the monic lists are monic (L1), so comparing leading coefficients gives $c = c'$, and dividing by c leaves equal products; induction on k , with the statement quantified over every length l of the other list; base case $k = 0$, where a non-empty list of monic irreducibles has a product of degree at least 1; in the step, p_{k+1} divides the other product, so it divides some q_j by [Corollary 5.3.3](#) (c), and equals it by (d); remove q_j from its list (L2) and cancel $p_{k+1} \neq 0$ ([Corollary 4.3.3](#) (b)); the induction hypothesis on the shortened lists gives $l - 1 = k$ and a bijection, extended by $k + 1 \mapsto j$.

Marking scheme. (10 points) - 1: compares leading coefficients to get $c = c'$, with a reason that a product of monic polynomials is monic. - 2: sets up an induction on the length of one list (or a least counterexample), with the statement quantified over all lengths of the other list, and proves the base case by a degree argument. - 3: shows that an irreducible of one list divides the other product and **equals** one of its factors, citing Euclid's lemma for several factors **and** "monic irreducible divides monic irreducible implies equal". - 1: justifies the cancellation by the absence of zero divisors in $F[x]$. - 3: applies the induction hypothesis to the shortened lists, with the removal of the matched entry stated, and extends the bijection. Fatal errors (0 for the step): using the uniqueness for a polynomial of smaller degree without an induction set up; concluding $p_{k+1} = q_j$ from $p_{k+1} \mid q_j$ without using that both are monic and irreducible. A proof by strong induction on $\deg f$ maps to the same points: its set-up and the degree-0 case take the 2 points of the induction, and "the cofactor has a unique factorization" takes the last 3.

Exercise. C2: Find the error

Here is a statement and an argument for it.

Claim. $x^4 + 1$ is irreducible over $\mathbb{Q}$.

Argument. (1) By [Theorem 5.3.7](#), a rational root of $x^4 + 1$ is u/v with $u \mid 1$ and $v \mid 1$, so the only candidates are 1 and -1 . (2) Both give the value $1 + 1 = 2 \neq 0$, so $x^4 + 1$ has no rational root. (3) By [Proposition 5.3.1](#), a polynomial without

roots is irreducible. (4) Hence $x^4 + 1$ is irreducible over $\mathbb{Q}$.

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

Solution. The claim is **true**; the argument does **not** prove it.

Lines (1) and (2) are correct. The failing line is (3). [Proposition 5.3.1](#) (b) is stated for polynomials of degree 2 or 3, and $x^4 + 1$ has degree 4: the line applies a result outside its hypotheses, a “fact” that is not available, entry (N9) of Logic and Proof, Example (What is not allowed). A counterexample to the step: $x^4 + 4$ has no rational root and is reducible (the warning after [Proposition 5.3.1](#)).

Repair. Suppose $x^4 + 1 = gh$ with $\deg g, \deg h \geq 1$. The leading coefficients multiply to 1, so replacing g, h by their monic associates we may take both monic. The degrees add up to 4. If one of them is 1, that factor has a root in $\mathbb{Q}$ (Theorem 5.1.3 (c)), against lines (1)–(2). So both have degree 2: $g = x^2 + ax + b$, $h = x^2 + cx + d$ with $a, b, c, d \in \mathbb{Q}$. Comparing coefficients in

$$(x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd$$

with $x^4 + 1$ gives $c = -a$, $b + d - a^2 = 0$, $a(d - b) = 0$ and $bd = 1$. Since $\mathbb{Q}$ has no zero divisors (Theorem 2.1.1 (f)), $a = 0$ or $d = b$.

- If $a = 0$: $d = -b$ and $-b^2 = 1$, impossible since $b^2 \geq 0 > -1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)).
- If $d = b$: $b^2 = 1$, so $b = \pm 1$ (Corollary 2.1.2), and $a^2 = 2b = \pm 2$. Now $a^2 = 2$ is impossible by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1, and $a^2 = -2 < 0$ is impossible since squares are non-negative.

So no splitting exists, and $x^4 + 1$ is irreducible over $\mathbb{Q}$.

Exercise. C3: Infinitely many irreducibles

- Let F be a field. Prove that no finite list contains every monic irreducible polynomial of $F[x]$: for every list $(p_1, \dots, p_k)$ of monic irreducibles, $k \in \mathbb{N}$, some monic irreducible is not an entry of it.
- Let p be prime. Prove that there are exactly p^n monic polynomials of degree n in $\mathbb{F}_p[x]$, for each $n \in \mathbb{N}$, and deduce that $\mathbb{F}_p[x]$ has monic irreducibles of arbitrarily large degree.

Solution (Hint 1). For (a), copy the integer argument: consider $p_1 \cdots p_k + 1$. For (b), a monic polynomial of degree n is determined by its n lower coefficients.

Solution (Hint 2). For (a): by (L1) the product has degree at least 1 when $k \geq 1$, so $N := p_1 \cdots p_k + 1$ has a monic irreducible factor ([Lemma 5.3.5](#)).

Solution. (a) If $k = 0$, the polynomial x is monic and irreducible and not an entry. Let $k \geq 1$ and $P := p_1 \cdots p_k$. By (L1), P is monic of degree $\sum_i \deg p_i \geq 1$. Then $N := P + 1$ has $\deg N = \deg P \geq 1$ (Theorem 4.3.1, the degrees of P and 1 differ), so N has a monic irreducible divisor q (Lemma 5.3.5). If $q = p_i$ for some i , then $q \mid P$ by (L2), and $q \mid N - P = 1$ (Proposition 5.1.1 (c)), so $\deg q \leq 0$ (Proposition 5.1.1 (d)), against $\deg q \geq 1$. So q is a monic irreducible that is not an entry of the list.

(b) A monic polynomial of degree n has n lower coefficients $a_0, \dots, a_{n-1} \in \mathbb{F}_p$, and by Definition 4.1.1 (equality coefficientwise) the map sending it to $(a_0, \dots, a_{n-1})$ is a bijection onto the set T_n of such tuples; its inverse puts 1 in position n and zeros above. We show $|T_n| = p^n$ by Logic and Proof, Axiom 4.2.1 on n . T_0 has one element, the empty tuple, and $p^0 = 1$. The tuples of length $n + 1$ split by their last entry into p pairwise disjoint sets, one for each element of $\mathbb{F}_p$, which has p elements (Definition 2.2.1); each is in bijection with T_n (drop the last entry). Applying Sets, Relations, and Cardinality, Proposition 3.1.5 $p - 1$ times (an induction on the number of pieces), $|T_{n+1}| = p \cdot p^n = p^{n+1}$.

So for each $M \in \mathbb{N}$, the monic polynomials of degree at most M form a finite set: a union of the finitely many finite sets for $n = 0, \dots, M$, pairwise disjoint, again by Sets, Relations, and Cardinality, Proposition 3.1.5. Suppose every monic irreducible of $\mathbb{F}_p[x]$ had degree at most M . Then they would form a subset of a finite set, hence a finite set (Sets, Relations, and Cardinality, Proposition 3.1.6), and a bijection $\{1, \dots, k\} \rightarrow$ that set (Sets, Relations, and Cardinality, Definition 3.1.2) would be a list containing every monic irreducible, against (a). So for every M there is a monic irreducible of degree greater than M .

Marking scheme. (10 points) - 2: (a) builds a polynomial N of degree ≥ 1 that is 1 more than a multiple of $p_1 \cdots p_k$ (e.g. $p_1 \cdots p_k + 1$, or $x p_1 \cdots p_k + 1$), and shows $\deg N \geq 1$ for every k , $k = 0$ included (or treats $k = 0$ separately). - 3: (a) takes a monic irreducible factor q of N and shows q is no p_i , since it would divide 1. - 3: (b) counts the monic polynomials of degree n through their coefficient tuples, with an induction or a cited counting result. - 2: (b) concludes by contradiction with (a): a bound on the degrees would make the irreducibles a finite set, hence a list. Fatal errors (0 for the step): claiming that N itself is irreducible; taking “the product of all monic irreducibles” without a finite list.

Exercise. C4: Greatest common divisor and least common multiple

Let $f, g \in F[x]$ be monic, $d := \gcd(f, g)$, and write $f = df_1$, $g = dg_1$.

- (a) Prove that $\gcd(f_1, g_1) = 1$.
- (b) Prove that $L := df_1g_1$ is a monic common multiple of f and g that divides every common multiple of f and g , and that $d \cdot L = fg$.
- (c) In $\mathbb{Q}[x]$, let $f = g = 2x$ (not monic). The gcd is x , and the monic common multiple dividing every common multiple is x . Show that $\gcd(f, g) \cdot x \neq fg$.

Solution. (a) Since $f \neq 0$, d is monic, so $d \neq 0$. By Theorem 5.2.2 (d), $d = af + bg$ for some $a, b \in F[x]$, so $d \cdot 1 = d(af_1 + bg_1)$. Canceling d (Corollary 4.3.3 (b)), $af_1 + bg_1 = 1$, and $\gcd(f_1, g_1) = 1$ by Corollary 5.2.3.

(b) Comparing leading coefficients in $f = df_1$ (Theorem 4.3.2 (b)) gives $\text{lc}(f_1) = 1$; likewise g_1 is monic, so L is monic (L1). It is a common multiple: $L = fg_1 = gf_1$. Let h be a common multiple, $h = fk = gm$ with $k, m \in F[x]$. Then $df_1k = dg_1m$, and canceling d , $f_1k = g_1m$.

So $g_1 \mid f_1 k$, and $\gcd(g_1, f_1) = 1$ by (a), hence $g_1 \mid k$ by [Theorem 5.3.2](#); say $k = g_1 t$. Then $h = df_1 g_1 t = Lt$, and $L \mid h$. Finally $d \cdot L = (df_1)(dg_1) = fg$.

(c) $\gcd(2x, 2x) = x$ by Definition 5.2.2: x is monic and divides $2x$, and every common divisor h of $2x$ and $2x$ divides $2^{-1}(2x) = x$ (Proposition 5.1.1 (b)). Next, x is monic and a common multiple of $f = g = 2x$, since $2^{-1}(2x) = x$. It divides every common multiple h : $x \mid 2x$ and $2x \mid h$, so $x \mid h$ by Proposition 5.1.1 (b). Any other monic L' with these two properties satisfies $x \mid L'$ and $L' \mid x$, so $L' = x$ by Proposition 5.1.1 (f). But $x \cdot x = x^2 \neq 4x^2 = fg$, since $1 \neq 4$ in $\mathbb{Q}$. The identity of (b) needs f and g monic. For non-zero f, g , the monic associates $\text{lc}(f)^{-1}f$ and $\text{lc}(g)^{-1}g$ have the same common divisors and the same common multiples as f and g , since each divides the other; so (b) applied to them gives $d \cdot L = \text{lc}(f)^{-1} \text{lc}(g)^{-1} fg$.