

5.5 Interpolation, Quotient Rings, and the Chinese Remainder Theorem

Section 5.4 proved a uniqueness statement: two polynomials of degree at most n that agree at $n + 1$ distinct points are equal (Theorem 5.4.2 (a)). It said nothing about existence. Is there, for instance, a quadratic through the points $(0, 1)$, $(1, 3)$, $(2, 7)$? This section builds one by a formula. It then reads the same question as three congruences. By Theorem 5.1.3 (a), “the value at c is y ” says that f leaves the remainder y on division by $x - c$. So we look for f with

$$f \equiv 1 \pmod{x}, \quad f \equiv 3 \pmod{x-1}, \quad f \equiv 7 \pmod{x-2}.$$

Three congruences to coprime moduli: that is the Chinese remainder theorem of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 3.5.3), with polynomials in place of integers. On the way we meet the classes modulo a polynomial m . They form a ring $F[x]/\langle m \rangle$, and it is a field exactly when m is irreducible, as $\mathbb{Z}/p\mathbb{Z}$ is a field exactly when p is prime.

Throughout, F is a field. “Polynomial” means an element of $F[x]$ unless another field is named.

5.5.1 Polynomials through given points

The points at which values are prescribed are called **nodes**. Suppose the nodes are $c_0, \dots, c_n \in F$ and the values $y_0, \dots, y_n \in F$. Fitting all the values at once is hard. Fitting one value while ignoring the others would be easy if we had, for each node c_i , a polynomial that is 1 at c_i and 0 at every other node: then y_0 times the first, plus y_1 times the second, and so on, has every value right. A polynomial that vanishes at the nodes c_j with $j \neq i$ is a multiple of the product of the factors $x - c_j$ (Theorem 5.4.1); the simplest is that product itself. Its value at c_i is the product of the numbers $c_i - c_j$, and dividing by that product makes the value 1.

Each Lagrange polynomial is 1 at its own node and 0 at all the others.

Definition 5.5.1. Lagrange Polynomials

Let $n \in \mathbb{N}$ and let $c_0, \dots, c_n \in F$ be **distinct**. For $i \in \{0, \dots, n\}$, the i -th **Lagrange polynomial** of these nodes is

$$\ell_i := \prod_{\substack{j=0 \\ j \neq i}}^n (c_i - c_j)^{-1} (x - c_j) \in F[x],$$

the product, in increasing order of j , of the n polynomials $(c_i - c_j)^{-1}(x - c_j)$ with $j \neq i$.

The inverse $(c_i - c_j)^{-1}$ exists because $c_i \neq c_j$ for $j \neq i$, and F is a field. The product of a list of polynomials is given by the recursion of Sets, Relations, and Cardinality, Definition 2.3.1, read in the commutative ring $F[x]$ (Theorem 4.2.4 (a)); the pattern *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* used for lists of integers.

Examples.

- *Two nodes.* For the nodes $0, 1 \in \mathbb{Q}$: $\ell_0 = (0-1)^{-1}(x-1) = 1-x$ and $\ell_1 = (1-0)^{-1}(x-0) = x$. Indeed $\ell_0(0) = 1$, $\ell_0(1) = 0$, $\ell_1(0) = 0$, $\ell_1(1) = 1$.

- *Three nodes.* For the nodes $0, 1, 2 \in \mathbb{Q}$, the polynomial ℓ_0 is

$$\ell_0 = (0 - 1)^{-1}(x - 1) \cdot (0 - 2)^{-1}(x - 2) = \frac{1}{2}(x - 1)(x - 2).$$

It vanishes at 1 and 2, and $\ell_0(0) = \frac{1}{2} \cdot (-1)(-2) = 1$.

- *Over a finite field.* In $\mathbb{F}_3$, with the nodes $0, 1, 2$, the same formula gives $\ell_0 = 2^{-1}(x - 1)(x - 2) = 2(x - 1)(x - 2)$, since $2 \cdot 2 = 4 = 1$ in $\mathbb{F}_3$. Its value at 0 is $2 \cdot (-1)(-2) = 4 = 1$.

☪ **Second reading** · *One node, and a repeated node*

One node ($n = 0$). The product defining ℓ_0 has no factors, so $\ell_0 = 1$, the empty product. The theorem below then says that the only polynomial of degree at most 0 with value y_0 at c_0 is the constant y_0 , which is right.

A repeated node. Change the nodes $0, 1$ of the first example to $0, 0$. The clause that fails is “distinct”: the factor $(c_0 - c_1)^{-1} = 0^{-1}$ does not exist. Nothing can repair this. A polynomial cannot have the value 1 at 0 and also the value 2 at 0, so with a repeated node some prescribed values have no interpolating polynomial at all.

The next theorem says that the Lagrange polynomials do what they were built for, and that the polynomial they produce is the only one.

Theorem 5.5.1. Lagrange Interpolation

Let $n \in \mathbb{N}$, let $c_0, \dots, c_n \in F$ be distinct, and let $y_0, \dots, y_n \in F$. Let $\ell_0, \dots, \ell_n$ be the Lagrange polynomials of the nodes (Definition 5.5.1).

- For all $i, k \in \{0, \dots, n\}$, $\ell_i(c_k) = 1$ if $k = i$ and $\ell_i(c_k) = 0$ if $k \neq i$. Each ℓ_i has degree exactly n .
- The polynomial $p := \sum_{i=0}^n y_i \ell_i$ satisfies $\deg p \leq n$ and $p(c_k) = y_k$ for every k .
- It is the **only** polynomial of degree at most n with $p(c_k) = y_k$ for every k .
- Every $q \in F[x]$ with $\deg q \leq n$ satisfies $q = \sum_{i=0}^n q(c_i) \ell_i$.

Try it first (ten minutes): for the nodes $0, 1, 2 \in \mathbb{Q}$, write down ℓ_0, ℓ_1, ℓ_2 and check (a) on them. Then find a quadratic through $(0, 1)$, $(1, 3)$, $(2, 7)$. Why can there be no second one?

Idea. The direct attempt writes $p = a_0 + a_1x + a_2x^2$ and solves the three equations $p(0) = 1$, $p(1) = 3$, $p(2) = 7$ for a_0, a_1, a_2 . It works here, but it gives no formula, and for $n + 1$ nodes it is a system of $n + 1$ equations. The Lagrange polynomials replace the system by a sum: (a) is “evaluate at a root”, since every factor $x - c_j$ with $j \neq i$ vanishes at c_j , and (b) follows from (a) term by term. The second question, why there is no other quadratic, is not answered by any construction. It is answered by counting roots: two such quadratics differ by a polynomial of degree at most 2 with three roots.

Proof.

- Let $i, k \in \{0, \dots, n\}$. Evaluation respects products (Theorem 4.4.1), so $\ell_i(c_k)$ is the

product of the values of the factors at c_k :

$$\ell_i(c_k) = \prod_{\substack{j=0 \\ j \neq i}}^n (c_i - c_j)^{-1} (c_k - c_j).$$

If $k \neq i$, the factor with $j = k$ is $(c_i - c_k)^{-1} \cdot 0 = 0$, so the product is 0. If $k = i$, every factor is $(c_i - c_j)^{-1} (c_i - c_j) = 1$, so the product is 1. For the degree, each factor $(c_i - c_j)^{-1} x - (c_i - c_j)^{-1} c_j$ has degree 1, since its coefficient of x is non-zero. A field has no zero divisors, so by Theorem 4.3.2 (b) the degree of a product is the sum of the degrees; with n factors, $\deg \ell_i = n$.

- (b) Each term $y_i \ell_i$ has degree at most n (Theorem 4.3.2 (a)), so $\deg p \leq n$ by Theorem 4.3.1, applied one term at a time. Evaluating at c_k and using (a),

$$p(c_k) = \sum_{i=0}^n y_i \ell_i(c_k) = y_k,$$

since every term with $i \neq k$ is $y_i \cdot 0 = 0$, and the term $i = k$ is $y_k \cdot 1$ (($\Sigma 3$) of Lemma 4.1.1).

- (c) Let $q \in F[x]$ with $\deg q \leq n$ and $q(c_k) = y_k$ for every k . Then p and q both have degree at most n and agree at the $n+1$ distinct points $c_0, \dots, c_n$. By Theorem 5.4.2 (a), $q = p$.
- (d) Let $\deg q \leq n$, and apply (b) and (c) with $y_i := q(c_i)$. The polynomial $\sum_i q(c_i) \ell_i$ and q itself both have degree at most n and the values $q(c_0), \dots, q(c_n)$ at the nodes, so they are equal by (c). This proves the theorem. ■

So for distinct nodes and any values, there is exactly one polynomial of degree at most n through the points, and (b) writes it down. Part (d) says that a polynomial of degree at most n is determined by its values at $n+1$ nodes, and rebuilt from them by the same formula. Where the linear-algebra companion, Chapter 6, speaks of “the Lagrange basis”, this book has only the formula (d); no basis is defined here.

Warning. The bound “degree at most n ” in (c) is what makes the interpolant unique. Without it, uniqueness fails: p and $p + (x - c_0)(x - c_1) \cdots (x - c_n)$ have the same values at every node, and the second has degree $n+1$. For the nodes 0, 1 and the values 5, 8, both $5 + 3x$ and $5 + 3x + x(x - 1) = 5 + 2x + x^2$ pass through (0, 5) and (1, 8).

Quick check. Write down the Lagrange polynomials of the nodes 0, 1 in $\mathbb{Q}$, and use them to find the line through (0, 5) and (1, 8).

Solution. $\ell_0 = 1 - x$ and $\ell_1 = x$ (the first example after Definition 5.5.1). By Theorem 5.5.1 (b), the line is $5\ell_0 + 8\ell_1 = 5(1 - x) + 8x = 5 + 3x$. Check: its values at 0 and 1 are 5 and 8.

Here is a cubic, worked through the formula.

Example. A cubic through four points

Find the polynomial $p \in \mathbb{Q}[x]$ of degree at most 3 with $p(-1) = 2$, $p(0) = 1$, $p(1) = 2$ and $p(2) = 11$.

Solution. The nodes $c_0 = -1$, $c_1 = 0$, $c_2 = 1$, $c_3 = 2$ are distinct. From [Definition 5.5.1](#), with the denominators computed first,

$$\begin{aligned}\ell_0 &= ((-1)(-2)(-3))^{-1}x(x-1)(x-2) = (-6)^{-1}(x^3 - 3x^2 + 2x), \\ \ell_1 &= ((1)(-1)(-2))^{-1}(x+1)(x-1)(x-2) = 2^{-1}(x^3 - 2x^2 - x + 2), \\ \ell_2 &= ((2)(1)(-1))^{-1}(x+1)x(x-2) = (-2)^{-1}(x^3 - x^2 - 2x), \\ \ell_3 &= ((3)(2)(1))^{-1}(x+1)x(x-1) = 6^{-1}(x^3 - x).\end{aligned}$$

By [Theorem 5.5.1](#) (b), $p = 2\ell_0 + \ell_1 + 2\ell_2 + 11\ell_3$. Collect each power of x :

$$\begin{aligned}x^3 &: -\frac{1}{3} + \frac{1}{2} - 1 + \frac{11}{6} = 1, & x^2 &: 1 - 1 + 1 = 1, \\ x &: -\frac{2}{3} - \frac{1}{2} + 2 - \frac{11}{6} = -1, & 1 &: 0 + 1 + 0 + 0 = 1.\end{aligned}$$

So $p = x^3 + x^2 - x + 1$. Check the four values: $p(-1) = -1 + 1 + 1 + 1 = 2$, $p(0) = 1$, $p(1) = 1 + 1 - 1 + 1 = 2$, $p(2) = 8 + 4 - 2 + 1 = 11$. By [Theorem 5.5.1](#) (c), no other polynomial of degree at most 3 has these values.

5.5.2 Congruence modulo a polynomial

The opening question turned values into remainders. To compute with remainders as *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3 did with integers, we need the relation “same remainder” and the classes it makes.

Definition 5.5.2. Congruence Modulo a Polynomial

Let $m \in F[x]$. Polynomials $f, g \in F[x]$ are **congruent modulo m** , written $f \equiv g \pmod{m}$, if $m \mid f - g$ (Definition 5.1.1), that is, if $f - g \in \langle m \rangle$ (Definition 5.2.1).

In words: f and g differ by a multiple of m . The set $\langle m \rangle$ of multiples of m is an ideal of the commutative ring $F[x]$ (Definition 5.2.1), so the relation is the relation $\sim_I$ of Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Theorem 3.4.1 for the ideal $I = \langle m \rangle$, and Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Theorem 3.4.1 (a) makes it an equivalence relation. We write $[f] = f + \langle m \rangle$ for the class of f , and $[f]_m$ when the modulus must be named.

Examples.

- $x^2 \equiv -1 \pmod{x^2 + 1}$, since $x^2 - (-1) = 1 \cdot (x^2 + 1)$.
- For every $c \in F$, $f \equiv f(c) \pmod{x - c}$: by Theorem 5.1.3 (a), $f = q(x - c) + f(c)$ for some q , so $f - f(c)$ is a multiple of $x - c$.
- Two polynomials are congruent modulo m exactly when they leave the same remainder on division by $m \neq 0$; this is (b) of the next theorem.

◉ **Second reading** · *The degenerate moduli 0 and the constants*

For $m = 0$, $f \equiv g \pmod{0}$ means $0 \mid f - g$, that is, $f = g$ (Proposition 5.1.1 (a)): every class is a single polynomial. For a non-zero constant m , every f is a multiple of m (Proposition 5.1.1 (a)), so all polynomials are congruent and there is one class; the ring it forms is the zero ring, in which $[1] = [0]$. Both cases are legal and neither is useful, which is why the next theorem asks for $\deg m \geq 1$.

Quick check. Is $x^3 \equiv x \pmod{x^2 + 1}$ in $\mathbb{Q}[x]$? In $\mathbb{F}_2[x]$?

Solution. Divide: $x^3 = x(x^2 + 1) - x$, so $x^3 \equiv -x$, and $x^3 - x = x(x^2 + 1) - 2x$. Hence $x^3 \equiv x$ exactly when $x^2 + 1 \mid -2x$. In $\mathbb{Q}[x]$ the polynomial $-2x$ is non-zero of degree $1 < 2$, so $x^2 + 1$ does not divide it (Proposition 5.1.1 (d)): **no**. In $\mathbb{F}_2[x]$, $-2x = 0$, which every polynomial divides: **yes**. The same symbols give different answers over different fields.

5.5.3 The ring of classes modulo a polynomial

Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Chapter 3 built $\mathbb{Z}/n\mathbb{Z}$ as the quotient of $\mathbb{Z}$ by the ideal $n\mathbb{Z}$, and found in each class exactly one remainder in $\{0, \dots, n-1\}$. The same construction works for $F[x]$ and an ideal $\langle m \rangle$, and division with remainder again picks one representative per class, now “of degree less than $\deg m$ ”.

Theorem 5.5.2. The Ring of Polynomials Modulo m

Let $m \in F[x]$ with $d := \deg m \geq 1$, and write $[f] = f + \langle m \rangle$.

- (a) $F[x]/\langle m \rangle$, with $[f] + [g] := [f + g]$ and $[f][g] := [fg]$, is a commutative ring with zero $[0]$ and one $[1]$, and $[1] \neq [0]$.
- (b) Each class contains **exactly one** polynomial of degree less than d : the remainder of any of its members on division by m . In particular $f \equiv g \pmod{m}$ if and only if f and g leave the same remainder, and sending each class to its member of degree less than d is a bijection from $F[x]/\langle m \rangle$ onto $\{r \in F[x] : \deg r < d\}$.
- (c) The map $F \rightarrow F[x]/\langle m \rangle$, $c \mapsto [c]$ (c a constant), is injective and preserves $+$ and $\cdot$.
- (d) $[f]$ is a unit of $F[x]/\langle m \rangle$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$ applied to the ideal $\langle m \rangle$; only $[1] \neq [0]$ needs the degree. Part (b) is division with remainder read twice: existence of the remainder puts one polynomial of small degree into each class, and “compare degrees” shows a class cannot hold two, since their difference would be a non-zero multiple of m of

Idea. Part (a) is the quotient theorem of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* applied to the ideal $\langle m \rangle$; only $[1] \neq [0]$ needs the degree. Part (b) is division with remainder read twice: existence of the remainder puts one polynomial of small degree into each class, and “compare degrees” shows a class cannot hold two, since their difference would be a non-zero multiple of m of

smaller degree than m . Part (d) translates $[a][f] = [1]$ into a Bézout identity, exactly as for $\mathbb{Z}/n\mathbb{Z}$.

Proof.

(a) By Definition 5.2.1, $\langle m \rangle$ is an ideal of the commutative ring $F[x]$, so Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Theorem 3.4.1 (a)–(c) give the commutative ring $F[x]/\langle m \rangle$ with these operations, zero $[0]$ and one $[1]$. By Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Theorem 3.4.1 (d), $[1] = [0]$ would mean $1 \in \langle m \rangle$, that is, $m \mid 1$; then $\deg m \leq \deg 1 = 0$ by Proposition 5.1.1 (d), against $d \geq 1$. So $[1] \neq [0]$.

(b) Since $d \geq 1$, $m \neq 0$. *Existence.* Let $f \in F[x]$. By Theorem 5.1.2 (a), $f = qm + r$ with $\deg r < d$. Then $f - r = qm \in \langle m \rangle$, so $r \in [f]$. *Uniqueness.* Let $r, r' \in [f]$ with $\deg r, \deg r' < d$. Then $r - r' \in \langle m \rangle$ (both are $\sim$ to f , and $\sim$ is an equivalence relation), so $m \mid r - r'$, and $\deg(r - r') < d$ by Theorem 4.3.1. If $r - r' \neq 0$, then $d \leq \deg(r - r')$ by Proposition 5.1.1 (d), a contradiction. So $r = r'$.

Hence two polynomials are congruent exactly when their classes are equal (Sets, Relations, and Cardinality, Theorem 2.5.1 (b)), exactly when the classes have the same member of degree less than d , which is the common remainder. The map “class $\mapsto$ its member of degree less than d ” is a function by the uniqueness just proved. It is injective, since two classes with a common member are equal (Sets, Relations, and Cardinality, Theorem 2.5.1 (c)); and it is surjective, since a polynomial r with $\deg r < d$ is the member of degree less than d of its own class $[r]$.

(c) For constants c, c' , $[c] + [c'] = [c + c']$ and $[c][c'] = [cc']$ by the definition of the operations, where $c + c'$ and cc' are computed in F (Theorem 4.2.4 (b)). If $[c] = [c']$, then c and c' are members of one class of degree at most $0 < d$, so $c = c'$ by (b).

(d) ($\Leftarrow$) Suppose $\gcd(f, m) = 1$. By Corollary 5.2.3 there are $a, b \in F[x]$ with $af + bm = 1$; let a, b be any such pair. Then $af - 1 = -bm \in \langle m \rangle$, so $[a][f] = [af] = [1]$. So $[f]$ is a unit, and its inverse, which is unique (Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Definition 3.5.1), is $[a]$.

($\Rightarrow$) Suppose $[a][f] = [1]$ for some $a \in F[x]$ (every element of the quotient is a class, Sets, Relations, and Cardinality, Definition 2.5.4). Then $af - 1 \in \langle m \rangle$: $af - 1 = km$ for some $k \in F[x]$. Hence $af + (-k)m = 1$, and $\gcd(f, m) = 1$ by Corollary 5.2.3. This proves the theorem. ■

So $F[x]/\langle m \rangle$ is a ring whose elements may be named by the polynomials of degree less than $\deg m$, and by (c) its constants form a copy of F . From now on we write c for the class $[c]$ of a constant when no confusion can arise. A computation in the quotient is: compute with representatives, then replace the result by its remainder. The integer twins are Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Theorem 3.4.3 (b) (one remainder per class) and Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Theorem 3.5.1 (units).

Quick check. In $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$, show that $[x + 1]$ is a unit, and find its inverse with (d).

Solution. Divide: $x^2 - 2 = (x - 1)(x + 1) - 1$. Hence $(x - 1)(x + 1) + (-1)(x^2 - 2) = 1$, so $\gcd(x + 1, x^2 - 2) = 1$ (Corollary 5.2.3), and by Theorem 5.5.2 (d) with $a = x - 1$, $[x + 1]$ is a unit with $[x + 1]^{-1} = [x - 1]$. Check: $(x + 1)(x - 1) = x^2 - 1 \equiv 2 - 1 = 1 \pmod{x^2 - 2}$.

When is every non-zero class a unit? By (d), when every f with $m \nmid f$ is coprime to m . For an irreducible m , Corollary 5.3.3 (a) says exactly this. For a reducible m , a factor of m of smaller positive degree is neither a multiple of m nor coprime to it.

Theorem 5.5.3. The Quotient Is a Field Exactly When m Is Irreducible

Let $m \in F[x]$ with $\deg m \geq 1$. Then $F[x]/\langle m \rangle$ is a field (Definition 2.1.1) **if and only if** m is irreducible over F (Definition 5.3.1).

Proof. By Theorem 5.5.2 (a), $F[x]/\langle m \rangle$ is a commutative ring with $[1] \neq [0]$. So it is a field exactly when every non-zero element is a unit.

($\Leftarrow$) Let m be irreducible and $[f] \neq [0]$. Then $f \notin \langle m \rangle$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1 (d), that is, $m \nmid f$. By Corollary 5.3.3 (a), $\gcd(m, f) = 1$; the definition of the gcd (Definition 5.2.2) is symmetric in its two arguments, so $\gcd(f, m) = 1$. Hence $[f]$ is a unit by Theorem 5.5.2 (d).

($\Rightarrow$) Let m be not irreducible. Since $\deg m \geq 1$, Definition 5.3.1 gives $g, h \in F[x]$, neither a constant, with $m = gh$. Then $g, h \neq 0$ and $\deg g, \deg h \geq 1$, and $\deg g + \deg h = \deg m$ (Theorem 4.3.2 (b)), so $\deg g, \deg h < \deg m$. A non-zero polynomial of degree less than $\deg m$ is not a multiple of m (Proposition 5.1.1 (d)), so $[g] \neq [0]$ and $[h] \neq [0]$. But $[g][h] = [gh] = [m] = [0]$. In a field a product of non-zero elements is non-zero (Theorem 2.1.1 (f)), so $F[x]/\langle m \rangle$ is not a field. This proves the theorem. ■

This is Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2 with “prime” replaced by “irreducible”. It manufactures new fields: from F and an irreducible m of degree d , a field whose elements are named by the polynomials of degree less than d .

Example. A field with four elements, and the complex numbers again

- (i) Describe $\mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$, and show that it is a field with four elements.
- (ii) Describe $\mathbb{R}[x]/\langle x^2 + 1 \rangle$.

Solution.

- (i) Let $m := x^2 + x + 1 \in \mathbb{F}_2[x]$. Its values are $m(0) = 1$ and $m(1) = 1 + 1 + 1 = 1$ in $\mathbb{F}_2$, so m has no root in $\mathbb{F}_2$; it has degree 2, so it is irreducible by Proposition 5.3.1 (b), and the quotient is a field by Theorem 5.5.3. By Theorem 5.5.2 (b), its elements are the classes of the polynomials of degree less than 2 over $\mathbb{F}_2$, namely $0, 1, x, x + 1$: four elements. Write $\alpha := [x]$. Since $x^2 - (x + 1) = x^2 + x + 1$ in $\mathbb{F}_2[x]$ (where $-1 = 1$),

$x^2 \equiv x + 1$, and so

$$\alpha^2 = \alpha + 1, \quad \alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1 = 1, \quad (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = \alpha,$$

using $2 = 0$ in $\mathbb{F}_2$. The multiplication table of the non-zero elements is therefore

$\cdot$	1	α	$\alpha + 1$
1	1	α	$\alpha + 1$
α	α	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	1	α

and every non-zero element has an inverse in it, as the theorem promised. Also $\alpha^3 = \alpha \cdot \alpha^2 = \alpha(\alpha + 1) = 1$. This is the four-element field of Exercise (C1: A Field with Four Elements). There the rule $\alpha^2 = 1 + \alpha$ is part of the definition of the multiplication; here it is computed, as the remainder of x^2 on division by $x^2 + x + 1$.

- (ii) The polynomial $x^2 + 1 \in \mathbb{R}[x]$ has no real root, since $c^2 + 1 \geq 1 > 0$ for every $c \in \mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)); it has degree 2, so it is irreducible (Proposition 5.3.1 (b)), and $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a field. Its elements are the classes $[a + bx]$ with $a, b \in \mathbb{R}$, each named by exactly one such polynomial, and $[x]^2 = [x^2] = [-1]$. So it is a field containing a copy of $\mathbb{R}$ (Theorem 5.5.2 (c)) and an element whose square is -1 : it looks like the complex numbers of Chapter 1, and Exercise B3 shows it is a copy of them.

The theorem needs “irreducible”, and having no root is not a substitute: Section 5.3 showed that the two differ from degree 4 on.

Warning. “ m has no root, so $F[x]/\langle m \rangle$ is a field” is false. The polynomial $m = (x^2 + 1)^2 \in \mathbb{R}[x]$ has no real root: for every $c \in \mathbb{R}$, $c^2 + 1 > 0$ (Example (A field with four elements, and the complex numbers again) (ii)), so $m(c) = (c^2 + 1)^2 > 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e). But $[x^2 + 1] \neq [0]$, since $x^2 + 1$ has degree $2 < 4 = \deg m$, while $[x^2 + 1]^2 = [(x^2 + 1)^2] = [0]$. A non-zero element with square zero cannot be a unit, so $\mathbb{R}[x]/\langle (x^2 + 1)^2 \rangle$ is not a field.

Quick check. Is $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ a field? Is $\mathbb{R}[x]/\langle x^2 - 2 \rangle$?

Solution. $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$: **yes**. A rational root c would give $c^2 = 2$, impossible by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1; so $x^2 - 2$ is irreducible over $\mathbb{Q}$ (Proposition 5.3.1 (b)), and Theorem 5.5.3 applies. $\mathbb{R}[x]/\langle x^2 - 2 \rangle$: **no**. With s the positive square root of 2 in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4), $x^2 - 2 = (x - s)(x + s)$ is reducible over $\mathbb{R}$, and the theorem says the quotient is not a field; concretely $[x - s][x + s] = [0]$.

5.5.4 The Chinese remainder theorem for polynomials

Now several congruences at once. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3 solved two congruences to coprime integer moduli by writing 1 as a combination of the moduli and multiplying (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.3). With polynomials the move is the same, and we take k moduli at once. The one new ingredient is that coprimality survives products.

Lemma 5.5.4. Coprime to Each Factor, Coprime to the Product

- (a) Let $s \geq 1$ and $p, q_1, \dots, q_s \in F[x]$. If $\gcd(p, q_j) = 1$ for every j , then $\gcd(p, q_1 \cdots q_s) = 1$.
- (b) Let $k \geq 1$ and let $m_1, \dots, m_k \in F[x]$ be **pairwise coprime**: $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. If $m_i \mid h$ for every i , then $m_1 \cdots m_k \mid h$.

In words: a polynomial coprime to each factor is coprime to the product, and pairwise coprime divisors of h divide h together.

🕒 **Second reading** · The proof: multiply the Bézout identities

Idea. For (a), write 1 as a combination of p and each factor, and multiply the identities: every term of the product but one contains p , and the remaining term is a multiple of the product of the factors. For (b), the product of the first k moduli is coprime to the next one by (a), so two coprime divisors combine (Proposition 5.3.4); induction adds one modulus at a time.

Proof.

- (a) We apply Logic and Proof, Axiom 4.2.1 (on $\mathbb{N} = \omega$, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 1.7.3 (b)) to $P(n)$: “the claim holds for $s = n + 1$ ”. $P(0)$, the case $s = 1$, has nothing to prove. Suppose $P(n)$, that is, the claim for $s = n + 1$, and let p be coprime to each of $q_1, \dots, q_{s+1}$. Write $Q := q_1 \cdots q_s$, so that $q_1 \cdots q_{s+1} = Qq_{s+1}$ by the product recursion (Sets, Relations, and Cardinality, Definition 2.3.1, read in $F[x]$). By the induction hypothesis and Corollary 5.2.3, $ap + bQ = 1$ and $a'p + b'q_{s+1} = 1$ for some $a, b, a', b' \in F[x]$. Multiplying the two identities and expanding,

$$p(aa'p + ab'q_{s+1} + a'bQ) + (bb')Qq_{s+1} = 1.$$

So $\gcd(p, Qq_{s+1}) = 1$ by Corollary 5.2.3.

- (b) We apply Logic and Proof, Axiom 4.2.1 (on $\mathbb{N} = \omega$, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 1.7.3 (b)) to $P(n)$: “the claim holds for $k = n + 1$ ”. $P(0)$, the case $k = 1$, has nothing to prove. Suppose $P(n)$, that is, the claim for $k = n + 1$, and let $m_1, \dots, m_{k+1}$ be pairwise coprime, each dividing h . With $M := m_1 \cdots m_k$, the induction hypothesis gives $M \mid h$. The modulus m_{k+1} is coprime to each of $m_1, \dots, m_k$, so $\gcd(m_{k+1}, M) = 1$ by (a), and $\gcd(M, m_{k+1}) = 1$ since the gcd is symmetric (Definition 5.2.2). By Proposition 5.3.4, $Mm_{k+1} = m_1 \cdots m_{k+1}$ divides h .

Without coprimality (b) fails: for $m_1 = m_2 = x$ and $h = x$, each m_i divides h , but $m_1 m_2 = x^2$ does not (Proposition 5.1.1 (d)); here $\gcd(m_1, m_2) = x \neq 1$.

Theorem 5.5.5. Chinese Remainder Theorem for Polynomials

Let $k \geq 1$, let $m_1, \dots, m_k \in F[x]$ be non-zero and pairwise coprime, and let $m := m_1 \cdots m_k$. For each i , let M_i be the product of the m_j with $j \neq i$ (in increasing order of j).

- (a) For each i there are $a_i, b_i \in F[x]$ with $a_i M_i + b_i m_i = 1$. Put $e_i := a_i M_i$. Then $e_i \equiv 1 \pmod{m_i}$ and $e_i \equiv 0 \pmod{m_j}$ for $j \neq i$, and for all $r_1, \dots, r_k \in F[x]$ the polynomial $f := \sum_{i=1}^k r_i e_i$ satisfies

$$f \equiv r_i \pmod{m_i} \quad \text{for every } i \in \{1, \dots, k\}.$$

- (b) A polynomial g satisfies the same k congruences **if and only if** $g \equiv f \pmod{m}$.
 (c) Exactly one polynomial of degree less than $\deg m$ satisfies the k congruences.
 (d) The rule $\Phi([f]_m) := ([f]_{m_1}, \dots, [f]_{m_k})$ is a well-defined **bijection**

$$\Phi: F[x]/\langle m \rangle \rightarrow F[x]/\langle m_1 \rangle \times \cdots \times F[x]/\langle m_k \rangle,$$

and, with $+$ and $\cdot$ on the right taken componentwise, Φ preserves $+$ and $\cdot$ and sends $[1]_m$ to $([1]_{m_1}, \dots, [1]_{m_k})$.

Idea. This is the integer proof of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.3 with k moduli. The identity $a_i M_i + b_i m_i = 1$ makes a polynomial e_i that is 1 modulo m_i and 0 modulo every other modulus, as e_i is 1 at one node and 0 at the others. Then $\sum r_i e_i$ has every remainder right. Uniqueness modulo m is Lemma 5.5.4 (b): a difference divisible by every m_i is divisible by their product. Part (c) picks the remainder modulo m , and (d) restates (a) and (b) as a bijection.

Proof. By (L2) of Section 5.3, applied to the list $(m_1, \dots, m_k)$ with the entry i removed, $m = M_i m_i$, so $m_i \mid m$; and $m_j \mid M_i$ for $j \neq i$, by the last clause of (L2), since m_j is an entry of the list whose product is M_i . By (L1) of Section 5.3, $m \neq 0$, since every m_i is non-zero.

- (a) If $k = 1$, then $M_1 = 1$ (the empty product), and $a_1 := 1, b_1 := 0$ will do. If $k \geq 2$, then m_i is coprime to each m_j with $j \neq i$, so Lemma 5.5.4 (a) gives $\gcd(m_i, M_i) = 1$; by the symmetry of the gcd and Corollary 5.2.3, $a_i M_i + b_i m_i = 1$ for some a_i, b_i . In either case $e_i - 1 = -b_i m_i$, so $e_i \equiv 1 \pmod{m_i}$; and for $j \neq i$, $m_j \mid M_i \mid e_i$, so $e_i \equiv 0 \pmod{m_j}$.

Now fix j . In $f - r_j = \sum_{i \neq j} r_i e_i + r_j(e_j - 1)$, every term with $i \neq j$ is a multiple of m_j , and so is $r_j(e_j - 1) = -r_j b_j m_j$. A sum of multiples of m_j is a multiple of m_j (Proposition 5.1.1 (c), and induction on the number of terms). So $f \equiv r_j \pmod{m_j}$.

- (b) ($\Rightarrow$) Suppose $g \equiv r_i \pmod{m_i}$ for every i . Then $m_i \mid (g - r_i) - (f - r_i) = g - f$ for every i (Proposition 5.1.1 (c)). The m_i are pairwise coprime, so $m \mid g - f$ by Lemma 5.5.4 (b).
 (b). ($\Leftarrow$) Suppose $m \mid g - f$. Since $m_i \mid m$, $m_i \mid g - f$ (Proposition 5.1.1 (b)), and then

$m_i \mid (g - f) + (f - r_i) = g - r_i$ for every i .

- (c) *Existence.* Since $m \neq 0$, divide f by m : $f = qm + r$ with $\deg r < \deg m$ (Theorem 5.1.2). Then $r \equiv f \pmod{m}$, so r satisfies the k congruences by (b). *Uniqueness.* If g and g' both satisfy them and have degree less than $\deg m$, then $g \equiv f \equiv g' \pmod{m}$ by (b), so $m \mid g - g'$, while $\deg(g - g') < \deg m$ (Theorem 4.3.1). A non-zero multiple of m has degree at least $\deg m$ (Proposition 5.1.1 (d)), so $g = g'$. (If every m_i is a non-zero constant, then $\deg m = 0$, and the one solution of degree less than 0 is the zero polynomial.)
- (d) *Well defined.* Fix i . If $f \equiv g \pmod{m}$, then $f \equiv g \pmod{m_i}$, since $m_i \mid m$. By Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Theorem 2.2.1 (a), applied to the identity map of $F[x]$ with congruence modulo m on the source and modulo m_i on the target, there is exactly one function $F[x]/\langle m \rangle \rightarrow F[x]/\langle m_i \rangle$ sending $[f]_m$ to $[f]_{m_i}$. Taking these k functions together gives Φ .

Surjective. An element of the target is $([r_1]_{m_1}, \dots, [r_k]_{m_k})$ for some $r_1, \dots, r_k \in F[x]$ (Sets, Relations, and Cardinality, Definition 2.5.4). With f as in (a), $[f]_{m_i} = [r_i]_{m_i}$ for every i (Sets, Relations, and Cardinality, Theorem 2.5.1 (b)), so $\Phi([f]_m)$ is that element.

Injective. If $\Phi([f]_m) = \Phi([g]_m)$, then $[f]_{m_i} = [g]_{m_i}$, that is, $m_i \mid g - f$, for every i (Sets, Relations, and Cardinality, Theorem 2.5.1 (b)). By Lemma 5.5.4 (b), $m \mid g - f$, that is, $[g]_m = [f]_m$.

Operations. By the definition of $+$ in each quotient (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Theorem 3.4.1 (b)) and of the componentwise sum,

$$\begin{aligned} \Phi([f]_m + [g]_m) &= \Phi([f + g]_m) = ([f + g]_{m_1}, \dots, [f + g]_{m_k}) \\ &= ([f]_{m_1} + [g]_{m_1}, \dots, [f]_{m_k} + [g]_{m_k}) = \Phi([f]_m) + \Phi([g]_m). \end{aligned}$$

The same lines with fg in place of $f + g$ give the product, and $\Phi([1]_m) = ([1]_{m_1}, \dots, [1]_{m_k})$ by definition. This proves the theorem. ■

In (a) the solution is built from the moduli alone, and the right-hand sides r_i enter linearly; the e_i depend only on $m_1, \dots, m_k$. Part (c) is the version used in computation: reduce any solution modulo m . Compared with Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Theorem 3.5.3, this theorem allows any number $k \geq 1$ of moduli in one step, where the integer theorem combines two at a time.

Quick check. Find the polynomial $f \in \mathbb{Q}[x]$ of degree less than 2 with $f \equiv 3 \pmod{x}$ and $f \equiv 5 \pmod{x - 1}$.

Solution. By Theorem 5.1.3 (b), $f \equiv 3 \pmod{x}$ says that 0 is a root of $f - 3$, that is, $f(0) = 3$; likewise the second congruence says $f(1) = 5$. By Theorem 5.5.1, $f = 3(1 - x) + 5x = 3 + 2x$. (The Chinese remainder route: $x - (x - 1) = 1$, so $e_1 = -(x - 1) = 1 - x$ and $e_2 = x$, and $f = 3e_1 + 5e_2$, the same polynomial.)

The check is no accident. Interpolation is the Chinese remainder theorem for the moduli $x - c_i$.

Proposition 5.5.6. Interpolation Is the Chinese Remainder Theorem for Linear Moduli

Let $n \in \mathbb{N}$, let $c_0, \dots, c_n \in F$ be distinct, let $y_0, \dots, y_n \in F$, and let $m := (x - c_0) \cdots (x - c_n)$.

- (a) The moduli $x - c_0, \dots, x - c_n$ are pairwise coprime, and $\deg m = n + 1$.
- (b) For $f \in F[x]$ and each i : $f \equiv y_i \pmod{x - c_i}$ **if and only if** $f(c_i) = y_i$.
- (c) The polynomial of degree less than $n + 1$ given by [Theorem 5.5.5](#) (c) for the right-hand sides $y_0, \dots, y_n$ is $\sum_i y_i \ell_i$, the interpolating polynomial of [Theorem 5.5.1](#). In particular, the remainder of the polynomial e_i of [Theorem 5.5.5](#) (a) on division by m is the Lagrange polynomial ℓ_i .

In words: the congruences modulo $x - c_i$ are the values at c_i , so the polynomial of the Chinese remainder theorem is the interpolating polynomial, and its building blocks e_i , reduced modulo m , are the Lagrange polynomials.

○ **Second reading** · The proof: evaluate, and compare by uniqueness

Idea. Two linear moduli differ by a non-zero constant, which is a Bézout identity after scaling. A congruence modulo $x - c$ is a statement about the value at c , by the factor theorem. And two polynomials of degree less than $n + 1$ solving the same congruences are equal, by the uniqueness half of the Chinese remainder theorem; so it is enough to check that the Lagrange formula solves them.

Proof.

- (a) For $i \neq j$, $(x - c_i) - (x - c_j) = c_j - c_i$, a non-zero constant. Multiplying by its inverse,

$$(c_j - c_i)^{-1}(x - c_i) - (c_j - c_i)^{-1}(x - c_j) = 1,$$

so $\gcd(x - c_i, x - c_j) = 1$ by Corollary 5.2.3. Each factor of m has degree 1, so $\deg m = n + 1$ by Theorem 4.3.2 (b).

- (b) By Theorem 5.1.3 (b), $x - c_i \mid f - y_i$ if and only if c_i is a root of $f - y_i$, and $(f - y_i)(c_i) = f(c_i) - y_i$ by Theorem 4.4.1.
- (c) The polynomial $p := \sum_i y_i \ell_i$ has degree at most $n < n + 1$ and $p(c_i) = y_i$ for every i ([Theorem 5.5.1](#) (b)), so by (b) it satisfies the congruences $p \equiv y_i \pmod{x - c_i}$. By the uniqueness in [Theorem 5.5.5](#) (c), it is the solution of degree less than $\deg m$. For the second claim, fix i and take the right-hand sides 1 at the index i and 0 elsewhere. By [Theorem 5.5.5](#) (a), e_i satisfies these congruences, and so does its remainder on division by m , which is congruent to e_i modulo m ([Theorem 5.5.5](#) (b)) and has degree less than $\deg m$. By the first claim, with these right-hand sides, that remainder is $\sum_j y_j \ell_j = \ell_i$.

■

So two routes lead to the same polynomial. The Lagrange route needs only evaluation and the root count; the Chinese remainder route needs Bézout identities, and in exchange it works for

moduli of any degree. The next two examples use moduli that are not all linear.

Example. A linear and a quadratic modulus

Find the polynomial $f \in \mathbb{Q}[x]$ of degree less than 3 with

$$f \equiv 1 \pmod{x-2} \quad \text{and} \quad f \equiv 2x-1 \pmod{x^2+1}.$$

Solution. A Bézout identity. Divide: $x^2+1 = (x+2)(x-2) + 5$. Hence

$$1 = \frac{1}{5}(x^2+1) - \frac{1}{5}(x+2)(x-2),$$

so the moduli $m_1 := x-2$ and $m_2 := x^2+1$ are coprime (Corollary 5.2.3), and $m = (x-2)(x^2+1) = x^3-2x^2+x-2$ has degree 3.

The polynomials e_1, e_2 . Here $M_1 = x^2+1$ and $M_2 = x-2$. The identity reads $a_1M_1+b_1m_1 = 1$ with $a_1 = \frac{1}{5}$, and $a_2M_2+b_2m_2 = 1$ with $a_2 = -\frac{1}{5}(x+2)$. So

$$e_1 = \frac{1}{5}(x^2+1), \quad e_2 = -\frac{1}{5}(x+2)(x-2) = -\frac{1}{5}(x^2-4).$$

Assemble and reduce. By Theorem 5.5.5 (a),

$$\begin{aligned} 1 \cdot e_1 + (2x-1)e_2 &= \frac{1}{5}(x^2+1 - (2x-1)(x^2-4)) \\ &= \frac{1}{5}(-2x^3+2x^2+8x-3). \end{aligned}$$

Its remainder on division by m is found by adding $\frac{2}{5}m$: since $-2x^3+2x^2+8x-3+2(x^3-2x^2+x-2) = -2x^2+10x-7$,

$$f = -\frac{2}{5}x^2+2x-\frac{7}{5},$$

the unique solution of degree less than 3 (Theorem 5.5.5 (c)).

Check. $f(2) = -\frac{8}{5}+4-\frac{7}{5} = 1$, which is the first congruence (Proposition 5.5.6 (b)). Modulo x^2+1 , replace x^2 by -1 : $f \equiv \frac{2}{5}+2x-\frac{7}{5} = 2x-1$.

Squares of linear moduli prescribe a value and a derivative at once.

Example. Values and derivatives at once

- (a) Let $c, a, b \in F$ and $f \in F[x]$. Show that $f \equiv a + b(x-c) \pmod{(x-c)^2}$ if and only if $f(c) = a$ and $f'(c) = b$ (the formal derivative of Definition 4.5.1).
- (b) Find the polynomial $p \in \mathbb{Q}[x]$ of degree at most 3 with $p(0) = 2$, $p'(0) = -1$, $p(1) = 1$ and $p'(1) = 3$.

Solution.

- (a) Divide by $(x-c)^2$, which has degree 2: $f = q(x-c)^2 + r$ with $\deg r \leq 1$ (Theorem 5.1.2). Every polynomial of degree at most 1 can be written $\alpha + \beta(x-c)$ with $\alpha, \beta \in F$: if $r = r_0 + r_1x$, take $\beta := r_1$ and $\alpha := r_0 + r_1c$. Evaluating at c (Theorem 4.4.1),

$f(c) = q(c) \cdot 0 + \alpha = \alpha$. By Theorem 4.5.1 (a)–(c),

$$f' = q'(x - c)^2 + (2 \cdot 1)q(x - c) + \beta,$$

so $f'(c) = \beta$. Now $f \equiv a + b(x - c)$ if and only if $r \equiv a + b(x - c)$, and both have degree less than 2, so by Theorem 5.5.2 (b) this holds if and only if $\alpha + \beta(x - c) = a + b(x - c)$. Comparing the coefficients of x and then the constant terms, that is $\beta = b$ and $\alpha = a$, that is, $f'(c) = b$ and $f(c) = a$.

- (b) By (a), the conditions say $p \equiv 2 - x \pmod{x^2}$ and $p \equiv 1 + 3(x - 1) = 3x - 2 \pmod{(x - 1)^2}$. The moduli are coprime: expanding,

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

So, with $m_1 = x^2$ and $m_2 = (x - 1)^2$, Theorem 5.5.5 (a) gives $e_1 = 2x^3 - 3x^2 + 1$ and $e_2 = 3x^2 - 2x^3$, and

$$(2 - x)e_1 + (3x - 2)e_2 = -8x^4 + 20x^3 - 12x^2 - x + 2.$$

Adding $8m = 8(x^4 - 2x^3 + x^2)$ gives the remainder modulo $m = x^2(x - 1)^2$:

$$p = 4x^3 - 4x^2 - x + 2.$$

Check: $p(0) = 2$; $p' = 12x^2 - 8x - 1$, so $p'(0) = -1$; $p(1) = 4 - 4 - 1 + 2 = 1$; $p'(1) = 12 - 8 - 1 = 3$. By Theorem 5.5.5 (c), p is the only polynomial of degree less than 4 with these four conditions.

This section met the Chinese remainder theorem three times: as interpolation (moduli $x - c_i$), as a value and a derivative at a point (moduli $(x - c)^2$), and in general. In each case the ring $F[x]/\langle m \rangle$ of Theorem 5.5.2 is the place where the computation happens.

5.5.5 Exercises

5.5.5.1 A. Check your understanding

Exercise. A1

- Finish the Try it first before Theorem 5.5.1: find the polynomial of degree at most 2 through $(0, 1)$, $(1, 3)$, $(2, 7)$ in $\mathbb{Q}[x]$.
- Describe the classes of $F[x]/\langle x \rangle$. Which ring is it, up to renaming?
- True or false: $\mathbb{R}[x]/\langle x^2 - 1 \rangle$ is a field. Justify your answer.
- Where does the proof of Theorem 5.5.1 (c) use that the nodes are distinct, and where do (a) and (b) use it?

Solution.

- (a) With the nodes $0, 1, 2$, Definition 5.5.1 gives

$$\ell_0 = \frac{1}{2}(x - 1)(x - 2), \quad \ell_1 = -x(x - 2), \quad \ell_2 = \frac{1}{2}x(x - 1).$$

So $p = \ell_0 + 3\ell_1 + 7\ell_2 = \frac{1}{2}(x^2 - 3x + 2) - 3(x^2 - 2x) + \frac{7}{2}(x^2 - x) = x^2 + x + 1$. Check: $p(0) = 1$, $p(1) = 3$, $p(2) = 7$. It is the only one of degree at most 2 (Theorem 5.5.1

- (c)).
- (b) By [Theorem 5.5.2](#) (b) with $d = 1$, each class contains exactly one polynomial of degree less than 1, a constant; the constant in $[f]$ is $f(0)$, the remainder on division by $x - 0$ (Theorem 5.1.3 (a)). So the classes are the $[c]$, $c \in F$, and they are distinct for distinct c . By [Theorem 5.5.2](#) (c), $c \mapsto [c]$ preserves $+$ and $\cdot$; it is injective, and surjective by what was just said. So $F[x]/\langle x \rangle$ is F with each element c renamed $[c]$; and $[f] = [f(0)]$, so passing to the quotient is “evaluate at 0”.
- (c) **False.** $x^2 - 1 = (x - 1)(x + 1)$ is reducible, so [Theorem 5.5.3](#) says the quotient is not a field. Concretely, $[x - 1] \neq [0] \neq [x + 1]$ (degree $1 < 2$), while $[x - 1][x + 1] = [x^2 - 1] = [0]$.
- (d) Part (c) uses distinctness only through Theorem 5.4.2 (a), which needs the $n + 1$ points to be distinct, ultimately because the root count of Section 5.4 counts distinct roots. Parts (a) and (b) use it to form the inverses $(c_i - c_j)^{-1}$ in the definition of ℓ_i .

5.5.5.2 B. Practice

Exercise. B1

Find the polynomial $f \in \mathbb{Q}[x]$ of degree less than 4 with $f \equiv 1 \pmod{x^2}$ and $f \equiv -1 \pmod{x^2 + 1}$.

Solution. The moduli are coprime, since $(x^2 + 1) - x^2 = 1$ (Corollary 5.2.3), so by [Theorem 5.5.5](#) (c) there is exactly one such f . The first congruence says $f - 1 = x^2 h$ for some $h \in \mathbb{Q}[x]$. Then

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

so the second congruence holds if and only if $x^2 + 1 \mid 2 - h$, that is, $h \equiv 2 \pmod{x^2 + 1}$. The choice $h = 2$ gives $f = 1 + 2x^2$, of degree $2 < 4$. Check: $f - 1 = 2x^2$ and $f + 1 = 2(x^2 + 1)$. Hence $f = 1 + 2x^2$.

Exercise. B2

In $\mathbb{Q}[x]/\langle x^3 - 2 \rangle$, show that $[x^2 + 1]$ is a unit, and compute its inverse.

Solution. Run the Euclidean algorithm (Theorem 5.2.5) on $x^3 - 2$ and $x^2 + 1$:

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

The last remainder is the non-zero constant 5, so the gcd is 1. Back-substitute:

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

Dividing by 5: $\frac{1}{5}(-x^2 + 2x + 1) \cdot (x^2 + 1) + \frac{1}{5}(x - 2) \cdot (x^3 - 2) = 1$. By [Theorem 5.5.2](#) (d), $[x^2 + 1]$ is a unit and

$$[x^2 + 1]^{-1} = [\tfrac{1}{5}(-x^2 + 2x + 1)].$$

Check: $(x^2 + 1)(-x^2 + 2x + 1) = -x^4 + 2x^3 + 2x + 1$, and with $x^3 \equiv 2$, $x^4 \equiv 2x$, this is $\equiv -2x + 4 + 2x + 1 = 5$.

Exercise. B3

- Write the addition and multiplication tables of $\mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$, with its elements named $0, 1, \alpha, \alpha + 1$ as in [Example \(A field with four elements, and the complex numbers again\)](#), and check from the table that every non-zero element is a unit.
- Show that $\varphi(a + bi) := [a + bx]$ ($a, b \in \mathbb{R}$) is a bijection $\mathbb{C} \rightarrow \mathbb{R}[x]/\langle x^2 + 1 \rangle$ that preserves $+$ and $\cdot$ and sends 1 to $[1]$.

Solution.

- Addition is coefficientwise in $\mathbb{F}_2$, where $1 + 1 = 0$:

+	0	1	α	$\alpha + 1$	$\cdot$	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$	0	0	0	0	0
1	1	0	$\alpha + 1$	α	1	0	1	α	$\alpha + 1$
α	α	$\alpha + 1$	0	1	α	0	α	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	α	1	0	$\alpha + 1$	0	$\alpha + 1$	1	α

The products come from $\alpha^2 = \alpha + 1$, $\alpha(\alpha + 1) = 1$, $(\alpha + 1)^2 = \alpha$ ([Example \(A field with four elements, and the complex numbers again\)](#)). Each non-zero row of the multiplication table contains 1: $1^{-1} = 1$, $\alpha^{-1} = \alpha + 1$, $(\alpha + 1)^{-1} = \alpha$.

- Every complex number is $a + bi$ for exactly one pair $(a, b) \in \mathbb{R}^2$ (Proposition 1.1.1 and the comparison of real and imaginary parts after it), and every element of $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is $[a + bx]$ for exactly one such pair, by [Theorem 5.5.2](#) (b) (the polynomials of degree less than 2 are the $a + bx$, distinct for distinct pairs). So φ is a bijection. Sums: φ of $(a + bi) + (c + di) = (a + c) + (b + d)i$ is $[(a + c) + (b + d)x] = [a + bx] + [c + dx]$. Products: in $\mathbb{R}[x]$,

$$(a + bx)(c + dx) = (ac - bd) + (ad + bc)x + bd(x^2 + 1),$$

so $[a + bx][c + dx] = [(ac - bd) + (ad + bc)x]$, which is φ of $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ (Definition 1.1.1, Proposition 1.1.1). Finally $\varphi(1) = [1]$. So the field of Chapter 1 could have been built as this quotient: the multiplication rule of Definition 1.1.1 is “multiply, then replace x^2 by -1 ”.

5.5.5.3 C. Going deeper

Exercise. C1: Two routes to the same theorem

Let $c_0, \dots, c_n \in F$ be distinct and $m := (x - c_0) \cdots (x - c_n)$.

- Prove, using [Theorem 5.5.1](#) and the root count but no Bézout identity, that for all $r_0, \dots, r_n \in F[x]$ some f satisfies $f \equiv r_i \pmod{x - c_i}$ for every i , and that g satisfies the same congruences if and only if $g \equiv f \pmod{m}$.
- Conversely, derive from [Theorem 5.5.5](#) that for all $y_0, \dots, y_n \in F$ exactly one poly-

mial of degree at most n satisfies $p(c_k) = y_k$ for every k (the content of [Theorem 5.5.1](#) (b) and (c), without the formula $\sum_i y_i \ell_i$).

(c) Which derivation is shorter, and why?

Solution.

- (a) By the second example after [Definition 5.5.2](#), $r_i \equiv r_i(c_i) \pmod{x - c_i}$. Let $f := \sum_i r_i(c_i) \ell_i$. By [Theorem 5.5.1](#) (b), $f(c_i) = r_i(c_i)$, so $f \equiv r_i(c_i) \equiv r_i \pmod{x - c_i}$, by [Proposition 5.5.6](#) (b) and transitivity. If g also satisfies the congruences, then $g - f \equiv 0 \pmod{x - c_i}$ for every i , so each c_i is a root of $g - f$ ([Theorem 5.1.3](#) (b)). The c_i are distinct roots, so $m \mid g - f$ by [Theorem 5.4.1](#). Conversely, if $m \mid g - f$, then each $x - c_i$ divides m (it is an entry of the list whose product is m , (L2) of Section 5.3) and so divides $g - f$ ([Proposition 5.1.1](#) (b)), and $g \equiv f \equiv r_i \pmod{x - c_i}$.
- (b) By [Proposition 5.5.6](#) (a), (b), the moduli $x - c_i$ are pairwise coprime, $\deg m = n + 1$, and “ $f(c_i) = y_i$ for every i ” is the system $f \equiv y_i \pmod{x - c_i}$. By [Theorem 5.5.5](#) (c), exactly one polynomial of degree less than $n + 1$, that is, of degree at most n , solves it. That is the existence of an interpolating polynomial and its uniqueness at once, without the formula for ℓ_i ; identifying it with $\sum_i y_i \ell_i$ still needs [Theorem 5.5.1](#) (a).
- (c) The route in (a) is shorter in what it needs: evaluation and the root count. The route in (b) passes through [Lemma 5.5.4](#) and Bézout identities for the moduli. The Lagrange route is shorter because linear moduli are special: “divisible by $x - c$ ” can be tested by evaluating at c , which turns every congruence into an equation in F . For moduli of higher degree, evaluation at a single point is no longer enough. For $(x - c)^2$, [Example \(Values and derivatives at once\)](#) (a) needs the derivative as well as the value. For $x^2 + 1$ over $\mathbb{Q}$ in [Example \(A linear and a quadratic modulus\)](#), the modulus has no root in $\mathbb{Q}$, so no evaluation in $\mathbb{Q}$ detects divisibility at all. The Chinese remainder route handles every modulus in the same way.

Exercise. C2: Every function on a prime field is a polynomial

Let p be a prime. Prove that every function $\varphi: \mathbb{F}_p \rightarrow \mathbb{F}_p$ is the polynomial function $c \mapsto f(c)$ of **exactly one** $f \in \mathbb{F}_p[x]$ with $\deg f < p$.

Solution. The elements $0, 1, \dots, p - 1$ of $\mathbb{F}_p$ are p distinct elements ([Definition 2.2.1](#)), and there are no others. Use them as nodes, $c_i := i$ for $i = 0, \dots, p - 1$, so $n = p - 1$.

Existence. With $y_i := \varphi(i)$, [Theorem 5.5.1](#) (b) gives f with $\deg f \leq p - 1 < p$ and $f(i) = \varphi(i)$ for every i . Since the i are all the elements of $\mathbb{F}_p$, the polynomial function of f is φ .

Uniqueness. If g also has degree less than p and the function φ , then f and g have degree at most $p - 1$ and agree at the p distinct nodes, so $f = g$ by [Theorem 5.5.1](#) (c).

So over $\mathbb{F}_p$ every function is a polynomial function, and the polynomials of degree less than p correspond one to one to the functions $\mathbb{F}_p \rightarrow \mathbb{F}_p$. (As a count: both sets have p^p elements, p choices for each of p coefficients, or for each of p values.) Interpolation over $\mathbb{F}_p$ can use at most p nodes, since $\mathbb{F}_p$ has no more distinct elements. Polynomials of degree p or more are no longer determined by their functions: x^p and x have the same function by [Theorem 2.6.6](#) (a), which is the warning of Section 5.4.