

6.6 Interpolation and the Chinese Remainder Theorem

Chapter 3 proved that through $n + 1$ points with distinct x -values there passes exactly one polynomial of degree at most n (Theorem 3.7.3). The proof went through an invertible matrix, and it never wrote the polynomial down. This section gives the formula. Then it reads interpolation in the arithmetic of this chapter: “ $p(c) = y$ ” says that p leaves remainder y on division by $x - c$. Prescribing remainders modulo several pairwise coprime polynomials at once is the Chinese Remainder Theorem. We prove it twice, once with Bézout’s identity, which gives a formula, and once by counting dimensions in the quotient spaces $F[x]/\langle m \rangle$.

6.6.1 The Lagrange basis

Suppose we want the polynomial of degree at most n taking prescribed values $y_0, \dots, y_n$ at distinct points $c_0, \dots, c_n$. The problem is linear in the data: if p fits the values (y_i) and q fits (y'_i) , then $p + q$ fits $(y_i + y'_i)$, by Theorem 0.8.5. So it is enough to solve the simplest data sets, a single 1 and zeros everywhere else, and add up.

The polynomial that vanishes at every c_j with $j \neq i$ is easy to write: $\prod_{j \neq i} (x - c_j)$. At c_i it takes the value $\prod_{j \neq i} (c_i - c_j)$, which is a product of nonzero scalars, so we can divide by it. In Example (Dual Bases in $\mathbb{R}[x]_{\leq 2}$) we met these polynomials for the three points $-1, 0, 1$. Here is the general case.

The i -th Lagrange polynomial is the polynomial of degree n that is 1 at the i -th node and 0 at every other node.

Definition 6.6.1. Lagrange Basis

Let $n \in \mathbb{N}$, and let $c_0, c_1, \dots, c_n \in F$ be **distinct**. For $i = 0, \dots, n$, the i -th **Lagrange polynomial** for these nodes is

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

The list $(\ell_0, \dots, \ell_n)$ is the **Lagrange basis** for the nodes $c_0, \dots, c_n$.

In words: the numerator makes ℓ_i vanish at every node except c_i , and the denominator rescales so that the value at c_i is exactly 1. The points c_i are called **nodes**.

Well-definedness. Each denominator $c_i - c_j$ with $j \neq i$ is nonzero because the nodes are **distinct**, so the quotients exist in F . The product has n linear factors, each with leading coefficient $(c_i - c_j)^{-1} \neq 0$, so $\deg \ell_i = n$ by Theorem 0.8.3. The name “basis” is justified by the theorem below.

Examples.

- **One node.** For $n = 0$ the product is empty, so $\ell_0 = 1$. The degenerate case is consistent: a polynomial of degree at most 0 with value y_0 at c_0 is the constant $y_0 = y_0 \ell_0$.
- **Two nodes.** For $c_0 = 0, c_1 = 1$ we get $\ell_0 = \frac{x-1}{0-1} = 1 - x$ and $\ell_1 = \frac{x-0}{1-0} = x$. The line through $(0, y_0)$ and $(1, y_1)$ is $y_0(1 - x) + y_1 x$.
- **Three nodes.** For $-1, 0, 1$, $\ell_{-1} = \frac{x(x-1)}{(-1)(-2)} = \frac{1}{2}x(x-1)$, $\ell_0 = \frac{(x+1)(x-1)}{(1)(-1)} = 1 - x^2$, and

$\ell_1 = \frac{1}{2}x(x+1)$, the polynomials of Example (Dual Bases in $\mathbb{R}[x]_{\leq 2}$). (Here we index the nodes by their values.)

Nonexample by minimal change. Take the nodes 0, 1, 1. The numerator of ℓ_1 is still defined, $(x-0)(x-1)$, but the denominator contains $c_1 - c_2 = 0$, which has no inverse. No rescaling helps: a polynomial that vanishes at $c_2 = 1$ cannot take the value 1 at $c_1 = 1$. The clause that fails is “distinct”.

Everything about the Lagrange polynomials follows from one table of values, the Kronecker delta $\ell_i(c_j) = \delta_{ij}$.

Theorem 6.6.1. Lagrange Interpolation

Let $n \in \mathbb{N}$, let $c_0, \dots, c_n \in F$ be distinct, and let $(\ell_0, \dots, \ell_n)$ be the Lagrange basis for these nodes.

- (a) $\ell_i(c_j) = \delta_{ij}$ for all $i, j \in \{0, \dots, n\}$.
- (b) $(\ell_0, \dots, \ell_n)$ is a basis of $F[x]_{\leq n}$, and every $p \in F[x]_{\leq n}$ satisfies

$$p = \sum_{i=0}^n p(c_i) \ell_i.$$

- (c) For all $y_0, \dots, y_n \in F$, the unique $p \in F[x]_{\leq n}$ with $p(c_i) = y_i$ for every i is

$$p = \sum_{i=0}^n y_i \ell_i.$$

Idea. ① The delta table is a direct evaluation. ② Evaluating a vanishing combination $\sum a_i \ell_i$ at c_j kills every term but a_j , so the list is independent, and it has the right length, so we count instead of checking spanning. ③ The expansion of p and the interpolation formula are the same computation: both sides of a candidate identity are polynomials of degree at most n with the same values at $n+1$ nodes.

Proof.

- (a) By Theorem 0.8.5, $\ell_i(c_j) = \prod_{k \neq i} \frac{c_j - c_k}{c_i - c_k}$. If $j = i$, every factor is 1, so $\ell_i(c_i) = 1$. If $j \neq i$, the factor with $k = j$ is 0, so $\ell_i(c_j) = 0$.
- (b) Each ℓ_i has degree n , so it lies in $F[x]_{\leq n}$. Let $a_0 \ell_0 + \dots + a_n \ell_n = 0$. Evaluating at c_j and using (a) gives $0 = \sum_i a_i \delta_{ij} = a_j$ for each j . Hence the list is linearly independent. It has length $n+1 = \dim F[x]_{\leq n}$ (Example (Standard Bases)), so it is a basis by Theorem 1.6.4 (a).
Now let $p \in F[x]_{\leq n}$, and put $q = p - \sum_i p(c_i) \ell_i \in F[x]_{\leq n}$. By (a), $q(c_j) = p(c_j) - p(c_j) = 0$ for every j . So q has the $n+1$ distinct roots $c_0, \dots, c_n$ and degree at most n . By Corollary 6.1.4, $q = 0$, which is the expansion of p .
- (c) By (a), $(\sum_i y_i \ell_i)(c_j) = \sum_i y_i \delta_{ij} = y_j$, so $\sum_i y_i \ell_i$ has the required values, and it lies in $F[x]_{\leq n}$. By Theorem 3.7.3, it is the only such polynomial. This proves the theorem. ■

So Chapter 3's existence statement now comes with a formula, and the uniqueness half of (c) is the expansion in (b) read backwards: a polynomial of degree at most n is determined by its values at the nodes, because those values are its coordinates in the Lagrange basis.

Example. The Chapter 3 Cubic by Lagrange's Formula

Use [Theorem 6.6.1](#) to find the $p \in \mathbb{Q}[x]_{\leq 3}$ with $p(-1) = 2$, $p(0) = 1$, $p(1) = 2$, and $p(2) = 11$, and compare with Example (A cubic through four points).

Solution. The nodes $-1, 0, 1, 2$ are distinct. Write $\ell_{-1}, \ell_0, \ell_1, \ell_2$ for the Lagrange polynomials, indexed by the node. The denominators are $\prod_{j \neq i} (c_i - c_j)$:

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

Expanding,

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

By [Theorem 6.6.1](#) (c), $p = 2\ell_{-1} + \ell_0 + 2\ell_1 + 11\ell_2$. Collecting coefficients:

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

Hence $p = x^3 + x^2 - x + 1$, the polynomial found by elimination in Example (A cubic through four points), as uniqueness demands. The elimination solved a 4×4 system for these particular values. The Lagrange polynomials were computed once, and would serve for any other values at the same nodes.

Warning. The interpolant has degree at most n , not exactly n . Through the three points $(0,0), (1,1), (2,2)$ the formula gives $0 \cdot \ell_0 + 1 \cdot \ell_1 + 2\ell_2$, where $\ell_1 = -x(x-2)$ and $\ell_2 = \frac{1}{2}x(x-1)$; this is $-x^2 + 2x + x^2 - x = x$. The degree-2 terms cancel, because the points lie on a line. Each ℓ_i has degree exactly n , but a combination of them need not.

Quick check. Let $n \geq 1$ and let $(\ell_0, \dots, \ell_n)$ be the Lagrange basis for distinct nodes $c_0, \dots, c_n$. What is $\sum_{i=0}^n c_i \ell_i$?

Solution. It is the polynomial x . Indeed $x \in F[x]_{\leq n}$ since $n \geq 1$, and its values at the nodes are $c_0, \dots, c_n$, so [Theorem 6.6.1](#) (b) gives $x = \sum_i c_i \ell_i$.

6.6.2 Evaluations are the dual basis

The delta table $\ell_i(c_j) = \delta_{ij}$ can be read the other way round. For $c \in F$, evaluation at c is the linear functional $\varepsilon_c: p \mapsto p(c)$ (Example (Four Families of Functionals)), which we restrict to $F[x]_{\leq n}$. Then the table says $\varepsilon_{c_j}(\ell_i) = \delta_{ji}$: the evaluations at the nodes behave on the Lagrange basis exactly as a dual basis must ([Theorem 5.1.3](#)). Exercise (C3: Evaluations as a dual basis) proved from [Theorem 3.7.3](#) that the evaluations form the dual basis of **some** basis. We can now name that basis.

Corollary 6.6.2. Evaluations Are Dual to the Lagrange Basis

Let $c_0, \dots, c_n \in F$ be distinct, with Lagrange basis $(\ell_0, \dots, \ell_n)$. Then $(\varepsilon_{c_0}, \dots, \varepsilon_{c_n})$ is the dual basis of $(\ell_0, \dots, \ell_n)$ in $F[x]_{\leq n}^*$. In particular, every linear functional φ on $F[x]_{\leq n}$ is a combination of evaluations at the nodes:

$$\varphi = \sum_{i=0}^n \varphi(\ell_i) \varepsilon_{c_i}.$$

Proof. The evaluations are linear (Example (Four Families of Functionals)), and $\varepsilon_{c_i}(\ell_j) = \ell_j(c_i) = \delta_{ij}$ by [Theorem 6.6.1](#) (a). Since $(\ell_0, \dots, \ell_n)$ is a basis ([Theorem 6.6.1](#) (b)), the uniqueness in [Theorem 5.1.3](#) (a) shows that the evaluations are its dual basis. The formula for φ is the second formula of [Theorem 5.1.3](#) (c). ■

The first formula of [Theorem 5.1.3](#) (c), $p = \sum_i \varepsilon_{c_i}(p) \ell_i$, is the expansion in [Theorem 6.6.1](#) (b). So Lagrange's formula is the statement “a vector is recovered from its dual-basis coordinates”, for the space $F[x]_{\leq n}$ and the measurements “value at c_i ”.

The formula for φ has a practical reading: **any** linear measurement of a polynomial of degree at most n can be computed from $n + 1$ of its values, with weights $\varphi(\ell_i)$ that do not depend on the polynomial.

Example. Integrals and Slopes from Values

- (a) Find $w_0, w_1, w_2 \in \mathbb{R}$ such that $\int_0^1 p(t) dt = w_0 p(0) + w_1 p(\frac{1}{2}) + w_2 p(1)$ for every $p \in \mathbb{R}[x]_{\leq 2}$.
- (b) Express $p \mapsto p'(0)$ on $\mathbb{R}[x]_{\leq 2}$ as a combination of $\varepsilon_{-1}, \varepsilon_0, \varepsilon_1$.

Solution.

- (a) Integration over $[0, 1]$ is a linear functional on $\mathbb{R}[x]_{\leq 2}$ (Example (Four Families of Functionals)). For the nodes $0, \frac{1}{2}, 1$,

$$\begin{aligned}\ell_0 &= \frac{(x - \frac{1}{2})(x - 1)}{(-\frac{1}{2})(-1)} = 2x^2 - 3x + 1, \\ \ell_{1/2} &= \frac{x(x - 1)}{(\frac{1}{2})(-\frac{1}{2})} = -4x^2 + 4x, \\ \ell_1 &= \frac{x(x - \frac{1}{2})}{(1)(\frac{1}{2})} = 2x^2 - x.\end{aligned}$$

Their integrals are $\frac{2}{3} - \frac{3}{2} + 1 = \frac{1}{6}$, $-\frac{4}{3} + 2 = \frac{2}{3}$, and $\frac{2}{3} - \frac{1}{2} = \frac{1}{6}$. By [Corollary 6.6.2](#),

$$\int_0^1 p(t) dt = \frac{1}{6} p(0) + \frac{2}{3} p(\frac{1}{2}) + \frac{1}{6} p(1) \quad \text{for all } p \in \mathbb{R}[x]_{\leq 2}.$$

Check with $p = x^2$: the right side is $\frac{2}{3} \cdot \frac{1}{4} + \frac{1}{6} = \frac{1}{3} = \int_0^1 t^2 dt$. This is Simpson's rule, which here is exact rather than approximate because p has degree at most 2.

- (b) With $\ell_{-1} = \frac{1}{2}x(x - 1)$, $\ell_0 = 1 - x^2$, and $\ell_1 = \frac{1}{2}x(x + 1)$, the derivatives at 0 are $-\frac{1}{2}$, 0, and $\frac{1}{2}$. Hence $p'(0) = \frac{1}{2}(p(1) - p(-1))$ for every $p \in \mathbb{R}[x]_{\leq 2}$, the symmetric difference quotient, exact on quadratics.

6.6.3 Congruences and the Chinese Remainder Theorem

Now we change the point of view. By Theorem 6.1.3, the remainder of p on division by $x - c$ is $p(c)$. So the interpolation conditions $p(c_i) = y_i$ say that p leaves the remainder y_i on division by $x - c_i$, for each i . Nothing in this reformulation needs the divisors to be linear. What happens if we prescribe the remainders modulo arbitrary polynomials $m_1, \dots, m_k$? The integers faced the same question long ago, which explains the name of the answer. We first need the language of congruences, copied from $\mathbb{Z}$.

Definition 6.6.2. Congruence Modulo a Polynomial

Let $m \in F[x]$. Two polynomials $f, g \in F[x]$ are **congruent modulo** m , written $f \equiv g \pmod{m}$, if $m \mid f - g$.

For example, $x^2 \equiv -1 \pmod{x^2 + 1}$, and $f \equiv f(c) \pmod{x - c}$ for every f , by Theorem 6.1.3. Congruence modulo m is an equivalence relation, and it respects sums and products: if $f \equiv f'$ and $g \equiv g' \pmod{m}$, then $f + g - (f' + g') = (f - f') + (g - g')$ and $fg - f'g' = f(g - g') + (f - f')g'$ are divisible by m . By Theorem 6.1.1, if $m \neq 0$, every f is congruent modulo m to **exactly one** polynomial of degree less than $\deg m$, its remainder: $f = qm + r$ gives $f \equiv r$, and if $f \equiv r \equiv r'$ with both degrees below $\deg m$, then $m \mid r - r'$ with $\deg(r - r') < \deg m$, which forces $r - r' = 0$.

Interpolation needed distinct nodes. The general condition is that the moduli share no factor, and the proof needs a way to pass from “coprime in pairs” to “coprime to the product”.

Lemma 6.6.3. Coprime to Each, Coprime to the Product

- (a) Let $p, q_1, \dots, q_s \in F[x]$. If p is coprime to each q_j , then there are $a, b \in F[x]$ with $ap + bq_1 \cdots q_s = 1$, and p is coprime to $q_1 \cdots q_s$.
- (b) Let $m_1, \dots, m_k \in F[x]$ be nonzero and **pairwise coprime**, that is, $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. If $m_i \mid h$ for every i , then $m_1 \cdots m_k \mid h$.

Proof.

- (a) By Corollary 6.2.4, for each j there are a_j, b_j with $a_j p + b_j q_j = 1$. Multiplying these s identities,

$$1 = \prod_{j=1}^s (a_j p + b_j q_j) = ap + (b_1 \cdots b_s) q_1 \cdots q_s$$

for some $a \in F[x]$, because every term of the expanded product except $(b_1 q_1) \cdots (b_s q_s)$ contains a factor $a_j p$. Let $d = \gcd(p, q_1 \cdots q_s)$. By Theorem 6.2.3, d divides p and $q_1 \cdots q_s$, hence divides $ap + b q_1 \cdots q_s = 1$, where $b = b_1 \cdots b_s$. So d is a nonzero constant by Theorem 0.8.3, and being monic, $d = 1$. Hence p and $q_1 \cdots q_s$ are coprime (Definition 6.2.3).

- (b) We use induction on k . For $k = 1$ there is nothing to prove. Let $k \geq 2$. The moduli $m_1, \dots, m_{k-1}$ are pairwise coprime and each divides h , so by the induction hypothesis $M := m_1 \cdots m_{k-1}$ divides h , say $h = Mg$. Since $m_k \mid h = Mg$, and m_k is coprime to M by (a), Theorem 6.2.8 gives $m_k \mid g$, say $g = m_k g'$. Then $h = m_1 \cdots m_k g'$, as claimed. ■

Theorem 6.6.4. Chinese Remainder Theorem for Polynomials

Let $m_1, \dots, m_k \in F[x]$ be nonzero and pairwise coprime, and put $m = m_1 \cdots m_k$. For all $r_1, \dots, r_k \in F[x]$:

- (a) there is $f \in F[x]$ with $f \equiv r_i \pmod{m_i}$ for every i ;
- (b) if f and g both satisfy (a), then $f \equiv g \pmod{m}$;
- (c) there is **exactly one** such f with $\deg f < \deg m$.

Idea. Copy Lagrange. There, ℓ_i was 1 at c_i and 0 at the other nodes; in the new language, $\ell_i \equiv 1 \pmod{x - c_i}$ and $\ell_i \equiv 0 \pmod{x - c_j}$. So we look for e_i with $e_i \equiv 1 \pmod{m_i}$ and $e_i \equiv 0 \pmod{m_j}$ for $j \neq i$, and then $f = \sum_i r_i e_i$ works. To be 0 modulo every other m_j , e_i should be a multiple of $M_i = \prod_{j \neq i} m_j$; to be 1 modulo m_i , it should be $1 - a m_i$. Bézout's identity $a m_i + b M_i = 1$ provides exactly such an element: $e_i = b M_i$.

Proof.

- (a) Fix i , and let $M_i = \prod_{j \neq i} m_j$. Since m_i is coprime to each m_j with $j \neq i$, Lemma 6.6.3 (a) gives $a_i, b_i \in F[x]$ with $a_i m_i + b_i M_i = 1$. Put $e_i = b_i M_i$. Then $e_i - 1 = -a_i m_i$, so $e_i \equiv 1 \pmod{m_i}$, and $m_j \mid M_i \mid e_i$ for $j \neq i$, so $e_i \equiv 0 \pmod{m_j}$. Let $f =$

$r_1e_1 + \cdots + r_ke_k$. Since congruence modulo m_j respects sums and products,

$$f \equiv r_1 \cdot 0 + \cdots + r_j \cdot 1 + \cdots + r_k \cdot 0 = r_j \pmod{m_j}$$

for each j .

- (b) If f and g satisfy (a), then $f - g \equiv r_i - r_i = 0 \pmod{m_i}$, that is, $m_i \mid f - g$, for every i . By [Lemma 6.6.3](#) (b), $m \mid f - g$.
- (c) Since each $m_i \neq 0$, $m \neq 0$ (Theorem 0.8.3). Let f be as in (a), and let f_0 be its remainder on division by m (Theorem 6.1.1). Then $m_i \mid m \mid f - f_0$, so $f_0 \equiv f \equiv r_i \pmod{m_i}$ for each i , and $\deg f_0 < \deg m$. If g is another solution with $\deg g < \deg m$, then $m \mid f_0 - g$ by (b), and $\deg(f_0 - g) < \deg m$, so $f_0 = g$. This proves the theorem. ■

Lagrange is the case $m_i = x - c_i$. For distinct nodes, $(x - c_j) - (x - c_i) = c_i - c_j$ is a nonzero constant, so $\frac{1}{c_i - c_j}(x - c_j) - \frac{1}{c_i - c_j}(x - c_i) = 1$, and any common divisor of $x - c_i$ and $x - c_j$ divides 1: the moduli are pairwise coprime. The congruence $f \equiv y_i \pmod{x - c_i}$ means $f(c_i) = y_i$ by Theorem 6.1.3, and $\deg m = n + 1$. So part (c) is Theorem 3.7.3. The element e_i has degree less than $n + 1$ after reduction modulo m , is 1 at c_i and 0 at the other nodes, so after reduction it is ℓ_i .

Example. A Linear and a Quadratic Modulus

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

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

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

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

and the moduli are coprime, since any common divisor divides 1.

The elements e_i . Put $e_1 = \frac{1}{5}(x^2 + 1)$ and $e_2 = -\frac{1}{5}(x + 2)(x - 2) = 1 - e_1$. Then e_1 is a multiple of $x^2 + 1$ and $e_1 = 1 + \frac{1}{5}(x + 2)(x - 2) \equiv 1 \pmod{x - 2}$; symmetrically, $e_2 \equiv 0 \pmod{x - 2}$ and $e_2 \equiv 1 \pmod{x^2 + 1}$.

Combine and reduce. By the proof of [Theorem 6.6.4](#), $f \equiv 1 \cdot e_1 + (2x - 1)e_2 \pmod{(x - 2)(x^2 + 1)}$. Expanding,

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

Dividing by $m = (x - 2)(x^2 + 1) = x^3 - 2x^2 + x - 2$ gives quotient $-\frac{2}{5}$ and remainder

$$f = \frac{1}{5}(-2x^2 + 10x - 7).$$

Check. $f(2) = \frac{1}{5}(-8 + 20 - 7) = 1$, so $f \equiv 1 \pmod{x - 2}$. Modulo $x^2 + 1$, $x^2 \equiv -1$, so $f \equiv \frac{1}{5}(2 + 10x - 7) = 2x - 1$.

Warning. The moduli must be coprime in pairs; coprime as a whole family is not enough. Without coprimality a system can be unsolvable: with $m_1 = x$ and $m_2 = x^2$, the system $f \equiv 0 \pmod{x}$, $f \equiv 1 \pmod{x^2}$ has no solution: the first condition says $f(0) = 0$, the second says $f = 1 + x^2q$, so $f(0) = 1$. For three moduli, x , $x - 1$, and $x(x - 1)$ have no common factor, yet the first and third share x , and $f \equiv 0 \pmod{x}$, $f \equiv 1 \pmod{x(x - 1)}$ is again impossible.

Example. Values and Slopes by CRT

- (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 $f'(c) = b$.
- (b) Find the $p \in \mathbb{Q}[x]_{\leq 3}$ with $p(0) = 2$, $p'(0) = -1$, $p(1) = 1$, and $p'(1) = 3$.

Solution.

- (a) Divide by $(x - c)^2$: $f = q(x - c)^2 + r$ with $\deg r \leq 1$ (Theorem 6.1.1). Writing $r = r_0 + r_1(x - c)$, which is possible because $(1, x - c)$ is a basis of $F[x]_{\leq 1}$ by Theorem 1.4.4 and Theorem 1.6.4, the uniqueness of the remainder says $f \equiv a + b(x - c)$ exactly when $r_0 = a$ and $r_1 = b$. Now $f(c) = r_0$. By Theorem 6.4.4, $f' = q'(x - c)^2 + 2q(x - c) + r_1$, so $f'(c) = r_1$. Hence the congruence holds if and only if $f(c) = a$ and $f'(c) = b$.
- (b) By (a), the conditions are $p \equiv 2 - x \pmod{x^2}$ and $p \equiv 1 + 3(x - 1) \pmod{(x - 1)^2}$. The moduli are coprime, since

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

So $e_0 = (2x + 1)(x - 1)^2$ is $\equiv 0 \pmod{(x - 1)^2}$ and $\equiv 1 \pmod{x^2}$, while $e_1 = -(2x - 3)x^2 = 3x^2 - 2x^3$ is $\equiv 0 \pmod{x^2}$ and $\equiv 1 \pmod{(x - 1)^2}$. The polynomial e_1 is the smooth step $3x^2 - 2x^3$ of Example (Prescribing Values and Slopes): value 0 and slope 0 at 0, value 1 and slope 0 at 1. By Theorem 6.6.4, p is the remainder of

$$(2 - x)e_0 + (3x - 2)e_1 = -8x^4 + 20x^3 - 12x^2 - x + 2$$

on division by $x^2(x - 1)^2 = x^4 - 2x^3 + x^2$. Adding $8(x^4 - 2x^3 + x^2)$ gives

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

Check. $p(0) = 2$; $p' = 12x^2 - 8x - 1$, so $p'(0) = -1$; $p(1) = 4 - 4 - 1 + 2 = 1$; $p'(1) = 12 - 8 - 1 = 3$.

The same recipe handles any finite set of nodes c_i with multiplicities k_i : the moduli $(x - c_i)^{k_i}$ are pairwise coprime for distinct nodes, by Lemma 6.6.3 (a) applied twice: first $x - c_i$ is coprime to $(x - c_j)^{k_j}$, and then $(x - c_j)^{k_j}$ is coprime to $(x - c_i)^{k_i}$. So for any prescribed remainders modulo $(x - c_i)^{k_i}$, there is exactly one polynomial of degree less than $k_1 + \cdots + k_s$ with those remainders. In characteristic 0, the Taylor expansion of Theorem 6.4.7 translates “the remainder modulo $(x - c)^k$ ” into the values $f(c), f'(c), \dots, f^{(k-1)}(c)$, and this is **Hermite interpolation**.

6.6.4 The quotient space $F[x]/\langle m \rangle$

Congruence modulo m is equality of cosets. The ideal $\langle m \rangle$ is a subspace of $F[x]$: it is nonempty and closed under addition and under multiplication by constant polynomials (Definition 6.2.1). So the quotient space $F[x]/\langle m \rangle$ of Definition 4.4.3 exists, and by Lemma 4.4.3 (b),

$$f + \langle m \rangle = g + \langle m \rangle \iff f - g \in \langle m \rangle \iff f \equiv g \pmod{m}.$$

An element of $F[x]/\langle m \rangle$ is a polynomial “known only modulo m ”. We cannot quote Theorem 4.4.5 for its dimension, because $F[x]$ is infinite-dimensional (Theorem 1.3.3). The remainder does the job instead.

Theorem 6.6.5. Dimension of $F[x]/\langle m \rangle$

Let $m \in F[x]$ be nonzero of degree d . Then $F[x]/\langle m \rangle$ is finite-dimensional with

$$\dim F[x]/\langle m \rangle = \deg m = d.$$

If $d \geq 1$, the cosets $(1 + \langle m \rangle, x + \langle m \rangle, \dots, x^{d-1} + \langle m \rangle)$ form a basis.

Proof. If $d = 0$, then m is a nonzero constant, and every $f = (m^{-1}f)m$ lies in $\langle m \rangle$. So $\langle m \rangle = F[x]$ and the quotient is the zero space, of dimension 0.

Let $d \geq 1$, and define $\rho: F[x] \rightarrow F[x]_{\leq d-1}$ by letting $\rho(f)$ be the remainder of f on division by m (Theorem 6.1.1). *Linear.* If $f = q_1m + \rho(f)$ and $g = q_2m + \rho(g)$, then for $c \in F$,

$$cf + g = (cq_1 + q_2)m + (c\rho(f) + \rho(g)),$$

and $\deg(c\rho(f) + \rho(g)) < d$ by Theorem 0.8.2. By the uniqueness in Theorem 6.1.1, $\rho(cf + g) = c\rho(f) + \rho(g)$. *Surjective.* If $\deg r < d$, then $r = 0 \cdot m + r$, so $\rho(r) = r$. *Kernel.* $\rho(f) = 0$ exactly when $f = qm$ for some q , that is, $f \in \langle m \rangle$.

By the First Isomorphism Theorem (Theorem 4.4.7), $\bar{\rho}: F[x]/\langle m \rangle \rightarrow F[x]_{\leq d-1}$, $f + \langle m \rangle \mapsto \rho(f)$, is a well-defined injective linear map with image $\text{im } \bar{\rho} = F[x]_{\leq d-1}$, so it is an isomorphism. Since $\bar{\rho}(x^j + \langle m \rangle) = x^j$ for $j < d$, and $(1, x, \dots, x^{d-1})$ is a basis of $F[x]_{\leq d-1}$ (Example (Standard Bases)), the inverse isomorphism $\bar{\rho}^{-1}$ carries it to the basis $(x^j + \langle m \rangle)_{j < d}$ (Theorem 2.5.2). Hence $\dim F[x]/\langle m \rangle = d$. ■

For example, $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ has basis $(1 + \langle x^2 + 1 \rangle, x + \langle x^2 + 1 \rangle)$, so each element is $a + bx + \langle x^2 + 1 \rangle$ for unique $a, b \in \mathbb{R}$.

Remark. Cosets can also be **multiplied**: $(f + \langle m \rangle)(g + \langle m \rangle) := fg + \langle m \rangle$ is well defined, because congruence modulo m respects products. In $\mathbb{R}[x]/\langle x^2 + 1 \rangle$, $x \cdot x = x^2 \equiv -1$, so the coset of x squares to minus the coset of 1, and $(a + bx)(a' + b'x) \equiv (aa' - bb') + (ab' + a'b)x$: this is multiplication in $\mathbb{C}$, with the coset of x playing the role of i .

The Chinese Remainder Theorem now becomes a statement about linear maps. Reducing a polynomial modulo each m_i records its k remainders; the theorem says that this record, taken

modulo m , is a perfect dictionary. Recall from Definition 4.4.1 that $V_1 \times \cdots \times V_k$ is the space of lists with entrywise operations.

Theorem 6.6.6. CRT as an Isomorphism

Let $m_1, \dots, m_k \in F[x]$ be nonzero and pairwise coprime, and put $m = m_1 \cdots m_k$. Then

$$\begin{aligned} \Phi: F[x]/\langle m \rangle &\rightarrow F[x]/\langle m_1 \rangle \times \cdots \times F[x]/\langle m_k \rangle, \\ f + \langle m \rangle &\mapsto (f + \langle m_1 \rangle, \dots, f + \langle m_k \rangle), \end{aligned}$$

is a well-defined isomorphism of vector spaces.

Idea. The map that does not care about well-definedness is $\Psi: f \mapsto (f + \langle m_i \rangle)_i$ on $F[x]$ itself. Its kernel is the set of polynomials divisible by every m_i , which is $\langle m \rangle$ by Lemma 6.6.3. So the First Isomorphism Theorem makes Φ well defined and injective in one stroke. For surjectivity we do **not** construct a preimage. We count: both sides have dimension $\deg m$, because degrees add under products.

Proof. Let $\Psi: F[x] \rightarrow F[x]/\langle m_1 \rangle \times \cdots \times F[x]/\langle m_k \rangle$, $\Psi(f) = (f + \langle m_1 \rangle, \dots, f + \langle m_k \rangle)$. Each entry is a quotient map, which is linear by Theorem 4.4.4 (c), and the operations in the product are entrywise, so Ψ is linear. By Lemma 4.4.3 (b), $\Psi(f) = 0$ if and only if $m_i \mid f$ for every i . If $m \mid f$, then $m_i \mid f$ for all i , since $m_i \mid m$; conversely, if every $m_i \mid f$, then $m \mid f$ by Lemma 6.6.3 (b). Hence $\ker \Psi = \langle m \rangle$.

By the First Isomorphism Theorem (Theorem 4.4.7), the rule $f + \langle m \rangle \mapsto \Psi(f)$ is a well-defined injective linear map; this is Φ . By Theorem 6.6.5, Theorem 0.8.3, and Theorem 4.4.1,

$$\begin{aligned} \dim F[x]/\langle m \rangle &= \deg m = \sum_{i=1}^k \deg m_i = \sum_{i=1}^k \dim F[x]/\langle m_i \rangle \\ &= \dim (F[x]/\langle m_1 \rangle \times \cdots \times F[x]/\langle m_k \rangle). \end{aligned}$$

Since Φ is injective between spaces of the same finite dimension, it is bijective by Corollary 2.3.2 (e), hence an isomorphism (Definition 2.5.2). ■

Surjectivity of Φ is the existence part of Theorem 6.6.4, and injectivity is the uniqueness part. So the count has given a second proof of the Chinese Remainder Theorem, one that never uses Bézout's identity for existence. It is the same trade as in Example (Interpolation as a Count): counting proves that a solution exists, and the Bézout construction says what it is. By the remark above, Φ also respects products of cosets, since reduction modulo each m_i does. In Chapter 9 this splitting of $F[x]/\langle m \rangle$ into pieces, one for each coprime factor of m , reappears as a splitting of a space on which an operator acts. The next section begins that story.

Quick check. What is $\dim \mathbb{Q}[x]/\langle x^3 - x \rangle$? Into which three spaces does Theorem 6.6.6 split it, and what does Φ do to the coset of x^2 ?

Solution. By [Theorem 6.6.5](#), the dimension is 3. Since $x^3 - x = x(x-1)(x+1)$ with distinct linear factors, which are pairwise coprime, Φ maps it isomorphically onto $\mathbb{Q}[x]/\langle x \rangle \times \mathbb{Q}[x]/\langle x-1 \rangle \times \mathbb{Q}[x]/\langle x+1 \rangle$, a product of three one-dimensional spaces. Modulo $x - c$, a polynomial is congruent to its value at c , so $\Phi(x^2 + \langle x^3 - x \rangle)$ is the list of cosets of the constants 0, 1, 1: the values of x^2 at 0, 1, -1.

6.6.5 Exercises

6.6.5.1 A. Check your understanding

Exercise. A1

- (a) Define the Lagrange basis for distinct nodes $c_0, \dots, c_n$, and state the value of ℓ_i at c_j .
- (b) True or false: for four distinct nodes, the polynomial of degree at most 3 through the four points always has degree exactly 3. Justify your answer.
- (c) State the Chinese Remainder Theorem for polynomials, with all hypotheses.
- (d) True or false: if $\gcd(m_1, m_2, m_3) = 1$, then every system $f \equiv r_i \pmod{m_i}$, $i = 1, 2, 3$, has a solution. Justify your answer.
- (e) What is $\dim_{\mathbb{R}} \mathbb{R}[x]/\langle x^4 + 1 \rangle$? Give a basis.
- (f) Which functional on $F[x]_{\leq n}$ is the i -th vector of the dual basis (Theorem 5.1.3) of the Lagrange basis?

Solution.

- (a) For distinct $c_0, \dots, c_n \in F$, $\ell_i = \prod_{j \neq i} \frac{x - c_j}{c_i - c_j}$ ([Definition 6.6.1](#)), and $\ell_i(c_j) = \delta_{ij}$ ([Theorem 6.6.1](#) (a)).
- (b) False. The points $(0, 0), (1, 0), (2, 0), (3, 0)$ are fitted by the zero polynomial, of degree $-\infty$; by uniqueness (Theorem 3.7.3), that is the interpolant.
- (c) If $m_1, \dots, m_k \in F[x]$ are nonzero and pairwise coprime and $m = m_1 \cdots m_k$, then for all $r_1, \dots, r_k \in F[x]$ there is f with $f \equiv r_i \pmod{m_i}$ for each i , unique modulo m , and exactly one such f has $\deg f < \deg m$ ([Theorem 6.6.4](#)).
- (d) False. $x, x-1, x(x-1)$ have gcd 1 as a family, but $f \equiv 0 \pmod{x}$, $f \equiv 0 \pmod{x-1}$, $f \equiv 1 \pmod{x(x-1)}$ has no solution: the last condition gives $f(0) = 1$, contradicting the first.
- (e) 4, with basis $(1, x, x^2, x^3)$ of cosets modulo $\langle x^4 + 1 \rangle$, by [Theorem 6.6.5](#).
- (f) Evaluation at the i -th node, $\varepsilon_{c_i} : p \mapsto p(c_i)$ ([Corollary 6.6.2](#)).

6.6.5.2 B. Practice

Exercise. B1: A Lagrange interpolant

Let $c_0, c_1, c_2, c_3 = 0, 1, 2, 3$. Write down the Lagrange basis for these nodes in factored form, and use it to find the $p \in \mathbb{Q}[x]_{\leq 3}$ with $p(0) = 1$, $p(1) = 0$, $p(2) = 1$, and $p(3) = 10$. Hence compute $p(4)$.

Solution. The denominators $\prod_{j \neq i} (c_i - c_j)$ are $(-1)(-2)(-3) = -6$, $(1)(-1)(-2) = 2$, $(2)(1)(-1) = -2$, and $(3)(2)(1) = 6$. So

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

By Theorem 6.6.1 (c), $p = \ell_0 + 0 \cdot \ell_1 + \ell_2 + 10\ell_3$. Expanding each needed term,

$$\begin{aligned}\ell_0 &= -\frac{1}{6}(x^3 - 6x^2 + 11x - 6), \\ \ell_2 &= -\frac{1}{2}(x^3 - 4x^2 + 3x), \\ 10\ell_3 &= \frac{5}{3}(x^3 - 3x^2 + 2x).\end{aligned}$$

The coefficient of x^3 is $-\frac{1}{6} - \frac{1}{2} + \frac{5}{3} = 1$; of x^2 , $1 + 2 - 5 = -2$; of x , $-\frac{11}{6} - \frac{3}{2} + \frac{10}{3} = 0$; the constant is 1. Hence

$$p = x^3 - 2x^2 + 1.$$

Check: $p(0) = 1$, $p(1) = 0$, $p(2) = 8 - 8 + 1 = 1$, $p(3) = 27 - 18 + 1 = 10$. Hence $p(4) = 64 - 32 + 1 = 33$.

Exercise. B2: A CRT system

Find the polynomial $f \in \mathbb{Q}[x]$ of degree less than 3 with $f \equiv 2 \pmod{x-1}$ and $f \equiv x \pmod{x^2+1}$. Hence describe all $g \in \mathbb{Q}[x]$ satisfying both congruences.

Solution. Bézout. $x^2 + 1 = (x+1)(x-1) + 2$, so $\frac{1}{2}(x^2 + 1) - \frac{1}{2}(x+1)(x-1) = 1$, and the moduli are coprime.

The elements e_i . $e_1 = \frac{1}{2}(x^2 + 1)$ is a multiple of $x^2 + 1$ and $e_1 = 1 + \frac{1}{2}(x+1)(x-1) \equiv 1 \pmod{x-1}$. And $e_2 = 1 - e_1 = -\frac{1}{2}(x+1)(x-1)$ is a multiple of $x-1$ with $e_2 \equiv 1 \pmod{x^2+1}$.

Combine and reduce. By the proof of Theorem 6.6.4, $f \equiv 2e_1 + xe_2 = (x^2 + 1) - \frac{1}{2}x(x^2 - 1) = -\frac{1}{2}x^3 + x^2 + \frac{1}{2}x + 1$. Modulo $m = (x-1)(x^2+1) = x^3 - x^2 + x - 1$, add $\frac{1}{2}m$:

$$f = -\frac{1}{2}x^3 + x^2 + \frac{1}{2}x + 1 + \frac{1}{2}(x^3 - x^2 + x - 1) = \frac{1}{2}x^2 + x + \frac{1}{2} = \frac{1}{2}(x+1)^2.$$

Check. $f(1) = 2$. Modulo $x^2 + 1$, $f \equiv \frac{1}{2}(-1) + x + \frac{1}{2} = x$.

By Theorem 6.6.4 (b), and since every $g \equiv f \pmod{m}$ satisfies both congruences (because $x-1$ and x^2+1 divide m), the solutions are exactly $g = \frac{1}{2}(x+1)^2 + h(x-1)(x^2+1)$ with $h \in \mathbb{Q}[x]$.

Exercise. B3: The Lagrange basis sums to one

Let $c_0, \dots, c_n \in F$ be distinct with Lagrange basis $(\ell_0, \dots, \ell_n)$.

- (a) Prove that $\ell_0 + \ell_1 + \cdots + \ell_n = 1$.
- (b) Prove more generally that $\sum_{i=0}^n c_i^k \ell_i = x^k$ for $k = 0, 1, \dots, n$ (with $c^0 = 1$).
- (c) For $n = 2$ and nodes $0, 1, 2$, verify (a) by expanding.

Solution.

- (a) This is (b) with $k = 0$.
- (b) Let $0 \leq k \leq n$. Then $x^k \in F[x]_{\leq n}$, and its value at c_i is c_i^k (Definition 0.8.6). By [Theorem 6.6.1](#) (b), $x^k = \sum_i c_i^k \ell_i$.
- (c) $\ell_0 = \frac{(x-1)(x-2)}{2} = \frac{1}{2}x^2 - \frac{3}{2}x + 1$, $\ell_1 = \frac{x(x-2)}{-1} = -x^2 + 2x$, $\ell_2 = \frac{x(x-1)}{2} = \frac{1}{2}x^2 - \frac{1}{2}x$. Adding: x^2 has coefficient $\frac{1}{2} - 1 + \frac{1}{2} = 0$, x has $-\frac{3}{2} + 2 - \frac{1}{2} = 0$, and the constant is 1. So the sum is 1.

6.6.5.3 C. Going deeper

Exercise. C1: Interpolation over a finite field

Let p be a prime and $F = \mathbb{F}_p$.

- (a) Explain why [Theorem 6.6.1](#) cannot be applied with more than p nodes.
- (b) Let $E: \mathbb{F}_p[x]_{\leq p} \rightarrow \mathbb{F}_p^p$, $E(f) = (f(0), f(1), \dots, f(p-1))$. Prove that E is linear and surjective but not injective, and find a nonzero polynomial in $\ker E$.
- (c) Deduce that every function $\mathbb{F}_p \rightarrow \mathbb{F}_p$ is the polynomial function of exactly one polynomial of degree at most $p-1$, but of more than one polynomial of degree at most p .

Solution.

- (a) The theorem needs distinct nodes, and $\mathbb{F}_p$ has only p elements, so there are no $p+1$ distinct nodes.
- (b) *Linear.* Each entry $f \mapsto f(c)$ is linear by Theorem 0.8.5. *Surjective.* The p elements $0, 1, \dots, p-1$ of $\mathbb{F}_p$ are distinct nodes, so for every $(y_0, \dots, y_{p-1})$, [Theorem 6.6.1](#) (c) with $n = p-1$ gives $f = \sum_i y_i \ell_i \in \mathbb{F}_p[x]_{\leq p-1} \subseteq \mathbb{F}_p[x]_{\leq p}$ with $E(f) = (y_0, \dots, y_{p-1})$. *Not injective.* $\dim \mathbb{F}_p[x]_{\leq p} = p+1 > p = \dim \mathbb{F}_p^p$, so E is not injective by Corollary 2.3.2 (c). Concretely, $g = \prod_{c \in \mathbb{F}_p} (x - c)$ is monic of degree p , hence nonzero, and $g(c) = 0$ for every $c \in \mathbb{F}_p$, because one factor vanishes (Theorem 0.8.5).
- (c) A function $\mathbb{F}_p \rightarrow \mathbb{F}_p$ is the same as its list of values $(y_0, \dots, y_{p-1})$. By (b), the restriction of E to $\mathbb{F}_p[x]_{\leq p-1}$ is surjective, and it is injective because a polynomial of degree at most $p-1$ vanishing at p distinct points is 0 (Corollary 6.1.4). So exactly one polynomial of degree at most $p-1$ has the given values. In degree at most p , if f has the given values, so does $f + g \neq f$, with g from (b). Unlike over $\mathbb{R}$, a polynomial over $\mathbb{F}_p$ is not determined by its function.

Exercise. C2: Newton's form of the interpolant

Let $c_0, \dots, c_n \in F$ be distinct. Put $N_0 = 1$ and $N_k = (x - c_0)(x - c_1) \cdots (x - c_{k-1})$ for

$$1 \leq k \leq n+1.$$

- (a) Prove that $(N_0, \dots, N_n)$ is a basis of $F[x]_{\leq n}$.
- (b) Let $p = \sum_{k=0}^n a_k N_k$. Show that $p(c_i) = \sum_{k=0}^i a_k N_k(c_i)$ and $N_i(c_i) \neq 0$. Explain why the coefficients $a_0, a_1, \dots$ of the interpolant can be found one at a time, and show that $a_0 = y_0$ and $a_1 = \frac{y_1 - y_0}{c_1 - c_0}$.
- (c) Let $p_n \in F[x]_{\leq n}$ interpolate $y_0, \dots, y_n$ at $c_0, \dots, c_n$, and let c_{n+1} be a further node, distinct from the others, with a value y_{n+1} . Prove that the interpolant $p_{n+1} \in F[x]_{\leq n+1}$ is

$$p_{n+1} = p_n + \frac{y_{n+1} - p_n(c_{n+1})}{N_{n+1}(c_{n+1})} N_{n+1}.$$

- (d) Find the Newton form of the interpolant of [Exercise \(B1: A Lagrange interpolant\)](#), and then the interpolant after adding the point $(4, 0)$. Why is this more economical than recomputing with Lagrange's formula?

Hint: for (c), check the values of the right-hand side at all $n+2$ nodes.

Solution.

- (a) N_k is a product of k monic linear factors, so it is monic of degree k (Theorem 0.8.3). The polynomials $N_0, \dots, N_n$ are nonzero with pairwise distinct degrees, hence linearly independent by Theorem 1.4.4. The list has length $n+1 = \dim F[x]_{\leq n}$, so it is a basis by Theorem 1.6.4 (a).
- (b) For $k > i$, N_k contains the factor $x - c_i$, so $N_k(c_i) = 0$; this gives the formula for $p(c_i)$. And $N_i(c_i) = \prod_{j < i} (c_i - c_j)$ is a product of nonzero scalars, since the nodes are distinct, so it is nonzero. The conditions $p(c_i) = y_i$ therefore form a lower triangular system: the i -th equation involves only $a_0, \dots, a_i$, with coefficient $N_i(c_i) \neq 0$ on a_i . Solving in the order $i = 0, 1, \dots, n$ determines each a_i from the earlier ones. For $i = 0$: $p(c_0) = a_0$, so $a_0 = y_0$. For $i = 1$: $y_1 = a_0 + a_1(c_1 - c_0)$, so $a_1 = \frac{y_1 - y_0}{c_1 - c_0}$, the slope of the chord, the first “divided difference”.
- (c) Let q be the right-hand side; the division is legal because $N_{n+1}(c_{n+1}) \neq 0$ by (b). Then $\deg q \leq n+1$. For $i \leq n$, $N_{n+1}(c_i) = 0$, so $q(c_i) = p_n(c_i) = y_i$. At c_{n+1} , $q(c_{n+1}) = p_n(c_{n+1}) + y_{n+1} - p_n(c_{n+1}) = y_{n+1}$. By Theorem 3.7.3, $q = p_{n+1}$.
- (d) With nodes $0, 1, 2, 3$: $N_1 = x$, $N_2 = x(x-1)$, $N_3 = x(x-1)(x-2)$. Forward substitution: $a_0 = p(0) = 1$; $0 = p(1) = 1 + a_1$, so $a_1 = -1$; $1 = p(2) = 1 - 2 + 2a_2$, so $a_2 = 1$; $10 = p(3) = 1 - 3 + 6 + 6a_3$, so $a_3 = 1$. Thus

$$p_3 = 1 - x + x(x-1) + x(x-1)(x-2) = x^3 - 2x^2 + 1,$$

agreeing with [Exercise \(B1: A Lagrange interpolant\)](#). Adding $(4, 0)$: $p_3(4) = 33$ and $N_4(4) = 4 \cdot 3 \cdot 2 \cdot 1 = 24$, so by (c)

$$\begin{aligned} p_4 &= x^3 - 2x^2 + 1 - \frac{33}{24} x(x-1)(x-2)(x-3) \\ &= x^3 - 2x^2 + 1 - \frac{11}{8} x(x-1)(x-2)(x-3). \end{aligned}$$

One checks $p_4(4) = 33 - \frac{11}{8} \cdot 24 = 0$. Adding a node changes **every** Lagrange polynomial, since each ℓ_i acquires a new factor; in Newton's form the old coefficients $a_0, \dots, a_n$ survive and only one new coefficient is computed.