Solutions 4

Factoring integer polynomials

1. (Lagrange interpolation) Let $a_0, \ldots, a_d$ and $b_0, \ldots, b_d$ be elements of a field F. and suppose that the a_i are distinct. Exhibit a polynomial $g(x) \in F[x]$ of degree $\leqslant d$ that satisfies $g(a_i) = b_i$ for each $0 \leqslant i \leqslant d$. Then prove that a polynomial with these properties is unique.

   Solution : Consider the Lagrange basis polynomials
   $$f_i(x) = \prod_{\substack{0 \leqslant j \leqslant d \\ j \neq i}} \frac{x - a_j}{a_i - a_j}$$
   for $0 \leqslant i \leqslant d$. These basis polynomials all have degree d and verify $f_i(a_i) = 1$ and $f_i(a_j) = 0$ when $j \neq i$. It follows that the polynomial
   $$g(x) = \sum_{i=0}^{d} b_i \prod_{\substack{0 \leqslant j \leqslant d \\ j \neq i}} \frac{x - a_j}{a_i - a_j}$$
   is what we are looking for. Assume there were a distinct polynomial $h(x) \in F[x]$, of degree $\leqslant d$ satisfying the same property. Then the difference $g(x) - h(x)$ would define a polynomial in $F[x]$, of degree d, that vanishes at $a_0, \ldots, a_d$. This is impossible since a polynomial of degree d with coefficients in a field can have at most d roots.

2. (Eisenstein criterion) Let R be a unique factorisation domain with field of fractions $\mathcal{F}$. Let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial in $R[x]$ and let $\mathfrak{P}$ be a prime ideal in R. If
   $$a_n \notin \mathfrak{p}, \quad a_i \in \mathfrak{p} \text{ for every } 0 \leqslant i \leqslant n-1, \quad a_0 \notin \mathfrak{p}^2,$$
   then $f(x)$ is irreducible in $\mathcal{F}[x]$.

   (a) When is a principal ideal prime ? When is a maximal ideal prime ?

   Solution : Consider the principal ideal $(p) \subsetneq R$. By definition, requiring (p) to be prime is equivalent to p being a prime element of R. In the unique factorization domain R, a principal ideal (p) is prime if and only if p is irreducible.

   Let $\mathfrak{m}$ be a maximal ideal in R. Then the quotient $R/\mathfrak{m}$ is a field, hence an integral domain and we have shown that $\mathfrak{m}$ must thus be a prime ideal (Serie 2).

(b) Prove the statement for $R = \mathbb{Z}$.

Proof : This is Proposition 12.4.6 in Artin.

(c) Find, for every $n \in \mathbb{N}$, an irreducible integer polynomial of degree n.

Solution : Fix $n \in \mathbb{N}$ and consider

$$x^n + 2^n x^{n-1} + \ldots + 2^2 x + 2.$$

This polynomial satisfies the Eisenstein criterion, and is thus irreducible in $\mathbb{Z}[x]$.

3. Factor the following polynomials into irreducible factors.

(a) $x^3 + x + 1$ in $\mathbb{F}_p[x]$, for $p = 2, 3, 5$.

Solution : If the polynomial factorizes, it must do so in a product of a linear with a quadratic polynomial. In particular, there must be a root of the polynomial in $\mathbb{F}_p$, for $p = 2, 3, 5$. Let $f(x) = x^3 + x + 1 \in \mathbb{Z}[x]$. Then

$$f(0) = 1,\ f(1) = 3,\ f(2) = 11,\ f(3) = 31,\ f(4) = 69.$$

Hence, the polynomial is irreducible over $\mathbb{F}_2$ and $\mathbb{F}_5$. In $\mathbb{F}_3$ it has root 1 and

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

in $\mathbb{F}_3[x]$.

(b) $x^4 + x + 1$ in $\mathbb{Q}[x]$.

Solution : We show that $x^4 + x + 1$ can not be factorized over $\mathbb{Z}$. First we note that there can be no linear factor : a linear factor for $x^4 + x + 1$ would necessarily be of the form $\pm x \pm 1$ but neither $+1$ nor -1 are roots of the polynomial. Hence, if there is a factorisation, it has to be in quadratic terms. There are only two possible cases,

$$x^4 + x + 1 = (x^2 + ax + c)(x^2 + bx + c)$$

with either $c = 1$ or $c = -1$. In either case, the above factorisation would yield the simultaneous equations $(a + b)x^3 = 0$ and $c(a + b)x = x$. We can conclude that the polynomial is irreducible over $\mathbb{Q}$.

(c) $x^3 + 2x^2 - 3x - 3$ in $\mathbb{Q}[x]$.

Solution : Via reduction mod 2, we obtain the polynomial $x^3 + x + 1$ mod 2. We have already shown in (a) that this polynomial is irreducible in $\mathbb{F}_2[x]$. Then $x^3 + 2x^2 - 3x - 3$ is irreducible over $\mathbb{Q}$.

(d) $x^{p-1} + x^{p-2} + \cdots + 1$ in $\mathbb{Q}[x]$ where p is a prime. (**Hint** : Consider the substitution $x = y + 1$.)

Solution : If we substitute $x = y + 1$,

$$\sum_{k=0}^{p-1} (y+1)^k = \frac{(y+1)^p - 1}{y} = \frac{1}{y}\left(\sum_{k=0}^{p} \binom{p}{k} y^k - 1\right) = \sum_{k=1}^{p} \binom{p}{k} y^{k-1}.$$

Then, with the Eisenstein criterion for the prime p, the polynomial in y is irreducible over $\mathbb{Q}$. It follows that the given polynomial in x is also irreducible.