7. Some irreducible polynomials

Linear factors $x - \alpha$ of a polynomial $P(x)$ with coefficients in a field k correspond precisely to roots $\alpha \in k$ of the equation $P(x) = 0$. This follows from unique factorization in the ring $k[x]$. [1] Here we also look at some special higher-degree polynomials, over *finite* fields, where we useful structural interpretation of the polynomials. [2]

Here we take for granted the existence of an algebraic closure $\overline{k}$ of a given field, as a fixed universe in which to consider roots of polynomial equations.

1. *Irreducibles over a finite field*

[1.0.1] **Proposition:** Let (non-constant) $M(x)$ be an irreducible in $k[x]$, with field k. Let I be the ideal generated in $k[x]$ by $M(x)$. Let α be the image of x in the field $K = k[x]/I$. Then α is a root of the equation $M(x) = 0$. [3]

Proof: The salient aspects of the ring structure in the quotient can be summarized by the point that the quotient map $k[x] \longrightarrow k[x]/I$ is a ring homomorphism, in fact, a k-algebra homomorphism. Thus, for any polynomial f,

$$f(x) + I = f(x + I)$$

In particular,

$$M(x + I) = M(x) + I = I = 0 + I$$

which shows that $x + I$ is a root of the equations. ///

[1] And this unique factorization follows from the *Euclidean*-ness of the polynomial ring.

[2] All these are *cyclotomic* polynomials, that is, divisors of $x^n - 1$ for some n. A systematic investigation of these polynomials is best done with a little more preparation. But they do provide accessible examples immediately.

[3] This is immediate, when one looks at the proof, but deserves complete explicitness.

[1.0.2] Proposition: [4] Let $P(x)$ be a polynomial in $k[x]$ for a field k. The equation $P(x) = 0$ has a root α generating [5] a degree d extension K of k if and only if $P(x)$ has a degree d irreducible factor $f(x)$ in $k[x]$.

Proof: Let α be a root of $P(x) = 0$ generating a degree d extension [6] $k(\alpha) = k[\alpha]$ over k. Let $M(x)$ be the minimal polynomial for α over k. Let

$$P = Q \cdot M + R$$

in $k[x]$ with $\deg R < \deg M$. Then, evaluating these polynomials at α, $R(\alpha) = 0$, but the minimality of the degree of M with this property assures that $R = 0$. That is, M divides P.

On the other hand, for an irreducible (monic, without loss of generality) $M(x)$ dividing $P(x)$, the quotient $K = k[x]/\langle M(x)\rangle$ is a field containing (a canonical copy of) k, and the image α of x in that extension is a root of $M(x) = 0$. Letting $P = Q \cdot M$,

$$P(\alpha) = Q(\alpha) \cdot M(\alpha) = Q(\alpha) \cdot 0 = 0$$

showing that $P(x) = 0$ has root α. ///

The first two examples use only the correspondence between linear factors and roots in the ground field.

[1.0.3] Example: $x^2 + 1$ is irreducible over $k = \mathbb{Z}/p$ for any prime $p = 3 \bmod 4$.

Indeed, if $x^2 + 1$ had a linear factor then the equation $x^2 + 1 = 0$ would have a root α in k. This alleged root would have the property that $\alpha^2 = -1$. Thus, $\alpha \neq 1$, $\alpha \neq -1$, but $\alpha^4 = 1$. That is, the order of α in $k^\times$ is 4. But the order of $(\mathbb{Z}/p)^\times$ is $p - 1$. The hypothesis $p = 3 \bmod 4$ was exactly designed to deny the existence of an element of order 4 in $(\mathbb{Z}/p)^\times$. Thus, $x^2 + 1$ is irreducible in such $k[x]$.

[1.0.4] Example: $x^2 + x + 1$ is irreducible over $k = \mathbb{Z}/p$ for any prime $p = 2 \bmod 3$.

If $x^2 + x + 1$ had a linear factor then $x^2 + x + 1 = 0$ would have a root α in k, and, since

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

$\alpha^3 = 1$ but $\alpha \neq 1$ since $1 + 1 + 1 \neq 0$ in k. That is, the order of α in $k^\times$ is 3. But the order of $(\mathbb{Z}/p)^\times$ is $p - 1$, and the hypothesis $p = 2 \bmod 3$ exactly precludes any element of order 3 in $(\mathbb{Z}/p)^\times$. Thus, $x^2 + x + 1$ is irreducible in such $k[x]$.

[1.0.5] Example: $P(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $k = \mathbb{Z}/p$ for prime $p \neq \pm 1 \bmod 5$ and $p \neq 5$. Note that

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

Thus, any root of $P(x) = 0$ has order [7] 5 or 1 (in whatever field it lies). The only element of order 1 is the identity element 1. If $P(x)$ had a linear factor in $k[x]$, then $P(x) = 0$ would have a root in k. Since

[4] This assertion should not be surprising, when one looks at the technique of the proof, which is nearly identical to the proof that linear factors correspond to roots in the base field.

[5] As earlier, the field extension $k(\alpha)$ *generated by* α makes sense only inside a fixed larger field. Throughout the present discussion we fix an algebraic closure of any ground field k and consider extensions inside that algebraic closure.

[6] Since the degree of the extension is finite, it is equal to polynomials in α over k, as we saw earlier.

[7] By Lagrange.

$1+1+1+1+1 \neq 0$ in k, 1 is not a root, so any possible root must have order 5. [8] But the order of $k^\times = (\mathbb{Z}/p)^\times$ is $p-1$, which is not divisible by 5, so there is no root in the base field k.

If $P(x)$ had an irreducible *quadratic* factor $q(x)$ in $k[x]$, then $P(x) = 0$ would have a root in a quadratic extension K of k. Since $[K : k] = 2$, the field K has p^2 elements, and

$$K^\times = p^2 - 1 = (p-1)(p+1)$$

By Lagrange, the order of any element of $K^\times$ is a divisor of $p^2 - 1$, but 5 does not divide $p^2 - 1$, so there is no element in K of order 5. That is, there is no quadratic irreducible factor.

By additivity of degrees in products, lack of factors up to half the degree of a polynomial assures that the polynomial is irreducible. Thus, since the quartic $x^4 + x^3 + x^2 + x + 1$ has no linear or quadratic factors, it is irreducible.

[1.0.6] Example: $P(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible over $k = \mathbb{Z}/p$ for prime $p = 3 \bmod 7$ or $p = 5 \bmod 7$.

Note that

$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

Thus, any root of $P(x) = 0$ has order 7 or 1 (in whatever field it lies). The only element of order 1 is the identity element 1. If $P(x)$ had a linear factor in $k[x]$, then $P(x) = 0$ would have a root in k. Since $1+1+1+1+1+1+1 \neq 0$ in k, 1 is not a root, so any possible root must have order 7. But the order of $k^\times = (\mathbb{Z}/p)^\times$ is $p-1$, which is not divisible by 7, so there is no root in the base field k.

If $P(x)$ had an irreducible *quadratic* factor $q(x)$ in $k[x]$, then $P(x) = 0$ would have a root in a quadratic extension K of k. Since $[K : k] = 2$, the field K has p^2 elements, and

$$|K^\times| = p^2 - 1 = (p-1)(p+1)$$

By Lagrange, the order of any element of $K^\times$ is a divisor of $p^2 - 1$, but 7 divides neither $3^2 - 1 = 8 = 1 \bmod 7$ nor $5^2 - 1 = 24 = 3 \bmod 7$, so there is no element in K of order 7. That is, there is no quadratic irreducible factor.

If $P(x)$ had an irreducible *cubic* factor $q(x)$ in $k[x]$, then $P(x) = 0$ would have a root in a cubic extension K of k. Since $[K : k] = 3$, the field K has p^3 elements, and

$$|K^\times| = p^3 - 1$$

By Lagrange, the order of any element of $K^\times$ is a divisor of $p^3 - 1$, but 7 divides neither $3^3 - 1 = 26 = 5 \bmod 7$ nor $5^3 - 1 = -8 = -1 \bmod 7$, so there is no element in K of order 7. That is, there is no cubic irreducible factor.

By additivity of degrees in products, lack of factors up to half the degree of a polynomial assures that the polynomial is irreducible. Thus, since the sextic $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ has no linear, quadratic, or cubic factors, it is irreducible.

[1.0.7] Example: $P(x) = (x^{11} - 1)/(x - 1)$ is irreducible over $k = \mathbb{Z}/p$ for prime p of order 10 (multiplicatively) mod 11. That is, modulo $p = 2, 6, 7, 8 \bmod 11$ this polynomial is irreducible. [9]

[8] The only other positive divisor of 5, thinking of Lagrange.

[9] By this point, one might have guessed that the irreducibility will be assured by taking primes p such that $p^d \neq 1$ for $d < 10$. The fact that there are such primes can be verified in an *ad hoc* fashion by simply looking for them, and Dirichlet's theorem on primes in arithmetic progressions assures that there are infinitely many such. The presence of primitive roots $2, 6, 7, 8$ (that is, generators for the cyclic group $(\mathbb{Z}/11)^\times$) modulo 11 is yet another issue, when we replace 11 by a different prime.

Again, any root of $P(x) = 0$ has order 11 or 1 (in whatever field it lies). The only element of order 1 is the identity element 1. If $P(x)$ had a linear factor in $k[x]$, then $P(x) = 0$ would have a root in k. Since $11 \neq 0$ in k, 1 is not a root, so any possible root must have order 11. But the order of $k^\times = (\mathbb{Z}/p)^\times$ is $p-1$, which is not divisible by 11, so there is no root in the base field k.

If $P(x)$ had an irreducible degree d factor $q(x)$ in $k[x]$, then $P(x) = 0$ would have a root in a degree d extension K of k. The field K has p^d elements, so

$$|K^\times| = p^d - 1$$

By Lagrange, the order of any element of $K^\times$ is a divisor of $p^d - 1$, but 11 divides none of $p-1$, p^2-1, p^3-1, p^4-1, ..., p^9-1, by design.

2. *Worked examples*

[7.1] *(Lagrange interpolation)* Let $\alpha_1, \ldots, \alpha_n$ be *distinct* elements in a field k, and let $\beta_1, \ldots, \beta_n$ be any elements of k. Prove that there is a unique polynomial $P(x)$ of degree $< n$ in $k[x]$ such that, for all indices i,

$$P(\alpha_i) = \beta_i$$

Indeed, letting

$$Q(x) = \prod_{i=1}^n (x - \alpha_i)$$

show that

$$P(x) = \sum_{i=1}^n \frac{Q(x)}{(x-\alpha_i)\cdot Q'(\alpha_i)} \cdot \beta_i$$

Since the α_i are distinct,

$$Q'(\alpha_i) = \prod_{j\neq i} (\alpha_i - \alpha_j) \neq 0$$

(One could say more about purely algebraic notions of derivative, but maybe not just now.) Evaluating $P(x)$ at $x \longrightarrow \alpha_i$,

$$\frac{Q(x)}{(x-\alpha_j)} \text{ evaluated at } x \longrightarrow \alpha_i \; = \begin{cases} 1 & (\text{for } j = i) \\ 0 & (\text{for } j = i) \end{cases}$$

Thus, all terms but the i^{th} vanish in the sum, and the i^{th} one, by design, gives β_i. For uniqueness, suppose $R(x)$ were another polynomial of degree $< n$ taking the same values at n distinct points α_i as does $Q(x)$. Then $Q - R$ is of degree $< n$ and vanishes at n points. A non-zero degree ℓ polynomial has at most ℓ zeros, so it must be that $Q - R$ is the 0 polynomial.

[7.2] *(Simple case of partial fractions)* Let $\alpha_1, \ldots, \alpha_n$ be *distinct* elements in a field k. Let $R(x)$ be any polynomial in $k[x]$ of degree $< n$. Show that there exist unique constants $c_i \in k$ such that in the field of rational functions $k(x)$

$$\frac{R(x)}{(x-\alpha_1)\ldots(x-\alpha_n)} = \frac{c_1}{x-\alpha_1} + \ldots + \frac{c_n}{x-\alpha_n}$$

In particular, let

$$Q(x) = \prod_{i=1}^n (x - \alpha_i)$$

and show that

$$c_i = \frac{R(\alpha_i)}{Q'(\alpha_i)}$$

We might emphasize that the field of rational functions $k(x)$ is most precisely the *field of fractions* of the polynomial ring $k[x]$. Thus, in particular, equality $r/s = r'/s'$ is exactly equivalent to the equality $rs' = r's$ (as in elementary school). Thus, to test whether or not the indicated expression performs as claimed, we test whether or not

$$R(x) = \sum_i \left(\frac{R(\alpha_i)}{Q'(\alpha_i)} \cdot \frac{Q(x)}{x - \alpha_i} \right)$$

One might notice that this is the previous problem, in case $\beta_i = R(\alpha_i)$, so its correctness is just a special case of that, as is the uniqueness (since $\deg R < n$).

[7.3] Show that the ideal I generated in $\mathbb{Z}[x]$ by $x^2 + 1$ and 5 is *not* maximal.

We will show that the quotient is not a field, which implies (by the standard result proven above) that the ideal is not maximal (proper).

First, let us make absolutely clear that the quotient of a ring R by an ideal $I = Rx + Ry$ generated by two elements can be expressed as a two-step quotient, namely

$$(R/\langle x \rangle)/\langle \bar{y} \rangle \approx R/(Rx + Ry)$$

where the $\langle \bar{y} \rangle$ is the principal ideal generated by the *image* $\bar{y}$ of y in the quotient $R/\langle x \rangle$. The principal ideal generated by y in the quotient $R/\langle x \rangle$ is the set of cosets

$$\langle \bar{y} \rangle = \{(r + Rx) \cdot (y + Rx) : r \in R\} = \{ry + Rx : r \in R\}$$

noting that the multiplication of cosets in the quotient ring is *not* just the element-wise multiplication of the cosets. With this explication, the natural map is

$$r + \langle x \rangle = r + \langle x \rangle \longrightarrow r + \langle x \rangle + \langle y \rangle' = r + (Rx + Rx)$$

which is visibly the same as taking the quotient in a single step.

Thus, first

$$\mathbb{Z}[x]/\langle 5 \rangle \approx (\mathbb{Z}/5)[x]$$

by the map which reduces the coefficients of a polynomial modulo 5. In $(\mathbb{Z}/5)[x]$, the polynomial $x^2 + 1$ *does* factor, as

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

(where these 2s are in $\mathbb{Z}/5$, not in $\mathbb{Z}$). Thus, the quotient $(\mathbb{Z}/5)[x]/\langle x^2 + 1 \rangle$ has proper zero divisors $\bar{x} - 2$ and $\bar{x} + 2$, where $\bar{x}$ is the image of x in the quotient. Thus, it's not even an integral domain, much less a field.

[7.4] Show that the ideal I generated in $\mathbb{Z}[x]$ by $x^2 + x + 1$ and 7 is *not* maximal.

As in the previous problem, we compute the quotient in two steps. First,

$$\mathbb{Z}[x]/\langle 7 \rangle \approx (\mathbb{Z}/7)[x]$$

by the map which reduces the coefficients of a polynomial modulo 7. In $(\mathbb{Z}/7)[x]$, the polynomial $x^2 + x + 1$ *does* factor, as

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

(where 2 and 4 are in $\mathbb{Z}/7$). Thus, the quotient $(\mathbb{Z}/7)[x]/\langle x^2 + x + 1 \rangle$ has proper zero divisors $\bar{x} - 2$ and $\bar{x} - 4$, where $\bar{x}$ is the image of x in the quotient. Thus, it's not even an integral domain, so certainly not a field.

Exercises

7.[2.0.1] Show that $x^2 + x + 1$ is irreducible in $\mathbb{F}_5[x]$, and in $\mathbb{F}_{29}[x]$.

7.[2.0.2] Show that $x^3 - a$ is irreducible in $\mathbb{F}_7[x]$ unless $a = 0$ or ± 1.

7.[2.0.3] Determine how $x^5 + 1$ factors into irreducibles in $\mathbb{F}_2[x]$.

7.[2.0.4] Exhibit an irreducible quintic in $\mathbb{F}_{11}[x]$.

7.[2.0.5] Show that the ideal generated by $x^2 - x + 1$ and 13 in $\mathbb{Z}[x]$ is *not* maximal.

7.[2.0.6] Show that the ideal generated by $x^2 - x + 1$ and 17 in $\mathbb{Z}[x]$ *is* maximal.

7.[2.0.7] Let $\alpha_1, \ldots, \alpha_n$ be distinct elements of a field k not of characteristic 2. Show that there are elements $a_1, b_1, \ldots, a_n, b_n$ in k such that

$$\frac{1}{(x-\alpha_1)^2 \ldots (x-\alpha_n)^2} = \frac{a_1}{x-\alpha_1} + \frac{b_1}{(x-\alpha_1)^2} + \ldots + \frac{a_n}{x-\alpha_n} + \frac{b_n}{(x-\alpha_n)^2}$$