Factoring Polynomials over a Field

Our goal is to find zeros of a polynomial. Suppose we can factor a polynomial over a field F, i.e. $f(x) = g(x)h(x)$. Recall that if ϕ_α is the evaluation homomorphism:

$$f(\alpha) = \phi_\alpha(x) = \phi_\alpha\big(g(x)h(x)\big) = \phi_\alpha\big(g(x)\big)\phi_\alpha\big(h(x)\big) = g(\alpha)h(\alpha).$$

Since F is a field it has no 0 divisors, if $0 = f(\alpha) = g(\alpha)h(\alpha)$ then either $g(\alpha) = 0$ or $h(\alpha) = 0$.

So if we can factor a polynomial $f(x) = g(x)h(x)$, then finding zeros of $f(x)$ is reduced to finding zeros of $g(x)$ and $h(x)$.

Theorem: Division Algorithm for $F[x]$

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$

$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ be elements of $F[x]$, with a_n and b_m both non-zero, and $m > 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that:

$$f(x) = q(x)g(x) + r(x)$$

where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Ex. Let $f(x) = x^4 + x^3 - 3x^2 + 2x + 3$ and $g(x) = x^2 - 2x + 2$ in $\mathbb{Z}_5[x]$. Find $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ and $r(x)$ is of degree less than $g(x)$ (i.e. less than 2).

$$
\begin{array}{r|l}
 & \qquad\qquad x^2 + 3x + 1 \\
\cline{2-2}
x^2 - 2x + 2 & x^4 + x^3 - 3x^2 + 2x + 3 \\
 & \underline{x^4 - 2x^3 + 2x^2} \\
 & \qquad 3x^3 \qquad\quad + 2x \qquad\qquad (-3 - 2 \equiv 0 \bmod 5) \\
 & \qquad \underline{3x^3 - \ x^2 + \ \ x} \qquad\qquad (3(2) \equiv 1 \bmod 5) \\
 & \qquad\qquad\quad x^2 + \ \ x + 3 \\
 & \qquad\qquad\quad \underline{x^2 - 2x + 2} \\
 & \qquad\qquad\qquad\quad 3x + 1
\end{array}
$$

So $q(x) = x^2 + 3x = 1$ and $r(x) = 3x + 1$.

Corollary: (Factor Theorem) An element $\alpha \in F$ is a zero of $f(x) \in F[x]$ if, and only if, $x - \alpha$ is a factor of $f(x)$ in $F[x]$.

Proof: Assume that $f(\alpha) = 0$, for $\alpha \in F$.

By the previous theorem we can write:

$f(x) = (x - \alpha)q(x) + r(x)$, where the degree of $r(x)$ is 0.

Thus $r(x)$ =constant. But $f(\alpha) = 0$ implies that:

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + C \Longrightarrow C = 0.$$

Hence $f(x) = (x - \alpha)q(x)$ and $x - \alpha$ is a factor of $f(x)$.

Now assume that $x-\alpha$ is a factor of $f(x)$ in $F[x]$. Then we have:

$$f(x)=(x-\alpha)q(x).$$

Hence: $$f(\alpha)=(\alpha-\alpha)q(\alpha)=0.$$

So α is a zero of $f(x)\in F[x]$.

Ex. Factor $x^4+3x^3+x^2+2x+3\in\mathbb{Z}_5[x]$ by finding a root α and then dividing $f(x)$ by $x-\alpha$.

Since there are only 5 elements in $\mathbb{Z}_5$ we can just test elements until we find a root:

$\alpha=0, \quad f(0)=3\not\equiv 0 \ mod\ 5$

$\alpha=1, \quad f(1)=1^4+3(1)^3++(1)^2+2(1)+3 \ \equiv 0\ mod\ 5.$

So $\alpha=1$ is a root of $x^4+3x^3+x^2+2x+3.$

$$\begin{array}{rlr}
 & \quad x^3+4x^2+\qquad 2 & \\ \cline{2-2}
x-1 & \big| x^4+3x^3+x^2+2x+3 & \\
 & \underline{x^4-x^3} & \\
 & \quad 4x^3+x^2 & \\
 & \quad \underline{4x^3-4x^2} & \\
 & \qquad\qquad +2x+3 & (1+4\equiv 0\ mod\ 5) \\
 & \qquad\qquad\ \ \underline{2x-2} & \\
 & \qquad\qquad\qquad 0 & (3+2\equiv 0\ mod\ 5)
\end{array}$$

So $x^4 + 3x^3 + +x^2 + 2x + 3 = (x-1)(x^3 + 4x^2 + 2)$ in $\mathbb{Z}_5[x]$

Now find a root of $g(x) = x^3 + 4x^2 + 2$ by testing elements of $\mathbb{Z}_5$.

$g(0) = 2 \neq 0$

$g(1) = 1^3 + 4(1)^2 + 2 = 7 \equiv 2 \ (mod\ 5)$

$g(2) = 2^3 + 4(2)^2 + 2 = 26 \equiv 1 \ (mod\ 5)$

$g(3) = 3^3 + 4(3)^2 + 2 = 65 \equiv 0 \ (mod\ 5)$. So 3 is a root.

$$
\begin{array}{r|l}
 & \quad x^2 + 2x + 1 \\ \hline
x - 3 & x^3 + 4x^2 + \qquad 2 \\
 & \underline{x^3 - 3x^2} \\
 & \qquad 2x^2 \\
 & \qquad \underline{2x^2 - x} \\
 & \qquad\qquad x + 2 \\
 & \qquad\qquad \underline{x - 3} \\
 & \qquad\qquad\quad 0
\end{array}
$$

So $x^4 + 3x^3 + x^2 + 2x + 3 = (x-1)(x-3)(x^2 + 2x + 1) \in \mathbb{Z}_5[x]$.

But $x^2 + 2x + 1 = (x+1)^2$ so we get:

$x^4 + 3x^3 + x^2 + 2x + 3 = (x-1)(x-3)(x+1)^2 \in \mathbb{Z}_5[x]$.

Corollary: A non-zero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field.

This follows from the previous Corollary. If α_1 is a zero of $f(x)$ then:

$$f(x) = (x - \alpha_1)q_1(x); \qquad \text{where degree of } q_1(x) \text{ is } n-1.$$

We can repeat this process at most $n-1$ times before the degree of $q_k(x)$ is 0.

Thus $f(x)$ can have at most n zeros.

Corollary: If G is a finite subgroup of the multiplicative group F^*, $\cdot$ of a field F, then G is cyclic. In particular, the multiplicative group of all non-zero elements of a finite field is cyclic.

Ex. Find all generators of the cyclic multiplicative group of units of $\mathbb{Z}_5$.

Recall that if a is a generator of a finite cyclic group G of order n, then the other generators of G are elements of the form a^r where r is relatively prime to n. In this case, G is the multiplicative group $G = \{1, 2, 3, 4\}$ of elements in $\mathbb{Z}_5$ thus, $|G| = 4$.

Notice also that 2 is a generator of G since:

$$2^1 = 2, \qquad 2^2 = 4, \qquad 2^3 \equiv 3\ (mod\ 5), \qquad 2^4 \equiv 1\ (mod\ 5).$$

So the other generators of G will be 2^r where r is relatively prime to 4 so $2^3 \equiv 3\ (mod\ 5)$ is the only other generator of G. So $\{2, 3\}$ are the generators of G.

Def. A non-constant polynomial $f(x) \in F[x]$ is **irreducible over $\boldsymbol{F}$** or is an **irreducible polynomial in $\boldsymbol{F[x]}$** if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two non-constant polynomials $g(x)$ and $h(x)$ in $F[x]$ both lower degree than the degree of $f(x)$. If $f(x) \in F[x]$ is not irreducible over F, then $f(x)$ is **reducible over $\boldsymbol{F}$**.

Notice that a polynomial can be irreducible over one field but reducible over a larger field.

Ex. $f(x) = x^2 - 3$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$, since:

$$x^2 - 3 = \left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right).$$

Ex. Let's show $f(x) = x^3 + x^2 + 3x + 1$ in $\mathbb{Z}_5[x]$ is irreducible over $\mathbb{Z}_5$.

Since $f(x)$ is degree 3, If $f(x)$ can be factored in $\mathbb{Z}_5[x]$, then at least one factor is linear. Thus $f(x)$ must have a zero in $\mathbb{Z}_5$. However, in $\mathbb{Z}_5$:

$f(0) = 1$

$f(1) = 6 \equiv 1 \ (mod\ 5)$

$f(2) = 2^3 + +2^2 + 3(2) + 1 = 19 \equiv 4 \ (mod\ 5)$

$f(3) = 3^3 + 3^2 + 3(3) + 1 = 46 \equiv 1 \ (mod\ 5)$

$f(4) = 4^3 + 4^2 + 3(4) + 1 = 93 \equiv 3 \ (mod\ 5)$.

Thus $f(x)$ doesn't have a zero in $\mathbb{Z}_5$, and so $f(x)$ is irreducible over $\mathbb{Z}_5$.

Theorem: Let $f(x) \in F[x]$ and let $f(x)$ be degree 2 or 3. Then $f(x)$ is reducible over F if, and only if, it has a zero in F.

Proof: If $f(x)$ is reducible then:

$f(x) = p(x)q(x)$; where the degrees of $p(x)$, $q(x)$ are each at least 1 and their sum is the degree of $f(x)$ (either 2 or 3).

Thus the degree of $p(x)$ or $q(x)$ is 1.

Hence $f(x)$ has a zero in F.

If $f(x)$ has a zero, α, in F, then we can write:

$f(x) = (x - \alpha)q(x)$; where the degree of $q(x)$ is at least 1.

Hence $f(x)$ is reducible over F.

Notice that if $f(x)$ is degree 4 then it's possible that $f(x)$ is reducible without having a root in F. For example:

$$f(x) = x^4 - 9 = (x^2 - 3)(x^2 + 3)$$

factors over $F = \mathbb{Q}$, but doesn't have a zero in $\mathbb{Q}$.

Theorem: If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if, and only if, it has such a factorization of the same degrees r and s in $\mathbb{Z}[x]$.

Corollary: If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, with $a_0 \neq 0$, and if $f(x)$ has a zero in $\mathbb{Q}$; then it has a zero m in $\mathbb{Z}$, and m must divide a_0.

Proof: Since $f(x) \in \mathbb{Z}[x]$ by the previous theorem if it factors in $\mathbb{Q}[x]$, it factors in $\mathbb{Z}[x]$.

Since $f(x)$ has a zero in $\mathbb{Q}$ it has a linear factor in $\mathbb{Q}[x]$. So in $\mathbb{Z}[x]$ we have:

$$f(x) = (x - m)\left(x^{n-1} + \cdots - \frac{a_0}{m}\right) \qquad \text{where} \quad \frac{a_0}{m} \in \mathbb{Z}.$$

So m divides a_0.

Ex. Notice that $x^2 - 3$ in $\mathbb{Q}[x]$ factors over $\mathbb{Q}$ if, and only if, it factors over $\mathbb{Z}$ (since the coefficients are in $\mathbb{Z}$). But in order to factor over $\mathbb{Z}$, it would have to have a zero in $\mathbb{Z}$ (which it clearly doesn't). Thus, $x^2 - 3$ is irreducible over $\mathbb{Q}$.

Theorem: Eisenstein Criterion

Let $p \in \mathbb{Z}$ be a prime. Suppose:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

and $a_n \not\equiv 0 \ (mod\ p)$, but $a_i \equiv 0 \ (mod\ p)$ for $i < n$,

with $a_0 \not\equiv 0 \ (mod\ p^2)$.

Then $f(x)$ is irreducible over $\mathbb{Q}$.

Ex. Show that $f(x) = 11x^5 - 3x^4 - 9x^2 - 12$ is irreducible over $\mathbb{Q}$.

If we take $p = 3$, notice that $11 \not\equiv 0 \ (mod\ 3)$,

$-3, -9, -12$ are $\equiv 0 \ (mod\ 3)$, and

$-12 \not\equiv 0 \ (mod\ 9)$.

Thus by the Eisenstein criterion, $f(x)$ is irreducible over $\mathbb{Q}$.

Ex. Show that $f(x) = 2x^6 - 7x^5 + 21x^3 - 14x + 14$ is irreducible over $\mathbb{Q}$.

If we take $p = 7$, notice that $2 \not\equiv 0 \ (mod\ 7)$,

$-7, 21, -14, 14$ are $\equiv 0 \ (mod\ 7)$, and

$14 \not\equiv 0 \ (mod\ 49)$.

Thus by the Eisenstein criterion, $f(x)$ is irreducible over $\mathbb{Q}$.