Abstract Algebra

Factorization

ThinkBS: Basic Sciences in Engineering Education

Kadir Has University, Turkey

Let E and F be fields, with $F \leq E$. We say that $f(x) \in F[x]$ factors in $F[x]$, if $f(x) = g(x)h(x)$ for $g(x)$, $h(x) \in F[x]$.

Let $\alpha \in E$. For the evaluation homomorphism ϕ_α, We have

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

Thus if $\alpha \in E$, then $f(\alpha) = 0$ if and only if either $g(\alpha) = 0$ or $h(\alpha) = 0$. Hence the attempt to find a zero of $f(x)$ reduces to the problem of finding a zero of a factor of $f(x)$. This is one reason why it is useful to study factorization of polynomials.

Division Algorithm for F[x]

Let

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

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

be two elements of $F[x]$, with a_n and b_m both nonzero elements of F and $m > 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Example: For $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1 \in \mathbb{Z}_5[x]$ and $g(x) = x^2 - 2x + 3$, we have $q(x) = x^2 - x - 3$ and $r(x) = x + 3$. Here $deg(r(x)) = 1 < deg(g(x)) = 2$ and one can check that $x^4 - 3x^3 + 2x^2 + 4x - 1 = (x^2 - 2x + 3)(x^2 - x - 3) + (x + 3)$

For the details of algorithm, look at Part 6 Section 28 of the textbook.

Factor Theorem and Irreducible Polynomials

An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $(x - a)$ is a factor of $f(x)$ in $F[x]$.

As a corollary one can conclude that a nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.

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

Note that we emphasize on the field because a polymomial $f(x)$ may be irreducible over F, but may not be irreducible if viewed over a larger field E containing F.

Irreducible Polynomials: Examples

Example 1: $f(x) = x^2 - 2$ viewed in $\mathbb{Q}[x]$ has no zeros in $\mathbb{Q}$ (why?) and hence is irreducible over $\mathbb{Q}$. But if we consider $f(x) = x^2 - 2 \in \mathbb{R}[x]$ then it factors as $f(x) = (x - \sqrt{2})(x + \sqrt{2})$.

Example 2: $f(x) = x^2 + 1 \in \mathbb{R}[x]$ is irreducible but $f(x) = x^2 + 1 \in \mathbb{C}[x]$ is reducible. (why?)

Example 3: $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ is irreducible over $\mathbb{Z}_5[x]$ because no element of $\mathbb{Z}_5[x]$ is a zero of $f(x)$.

In general we can say that if $f(x)$ is of degree 2 or 3, then $f(x)$ is reducible over F if and only if it has a zero in F.

Factorization in F[x]

For $f(x)$, $g(x) \in F[x]$ we say that $g(x)$ divides $f(x)$ in $F[x]$ if there exists $q(x) \in F[x]$ such that $f(x) = g(x)q(x)$.

Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x)$, $s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$. By induction we can generalize this result to product of finitely many polynomials.

Uniqueness Theorem: If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit (that is, nonzero constant) factors in F.