Chapter 17 Factorization of Polynomials

Factorization

Motivation We are able to construct the solution of $f(x) \in \mathbb{F}(x)$ in a larger field E that contains $\mathbb{F}$ even if $f(x)$ has no zero in $\mathbb{F}$.

We will need the concept of factorization of polynomial. Further, it is an extension of our study of polynomials in high school.

Definition Let D be an integral domain. Suppose $f(x) \in D(x)$ is neither the zero nor a unit. Then $f(x)$ is irreducible if $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in D[x]$ will imply $g(x)$ or $h(x)$ is a unit in $D[x]$. Otherwise, $f(x)$ is reducible.

Examples (1) $f(x) = 2x^2 + 4$ over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$? (2) $g(x) = x^2 - 2$?

Theorem 17.1 Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$ with degree 2 or 3. Then $f(x)$ is reducible over $\mathbb{F}$ if and only if $f(x)$ has a zero in $\mathbb{F}$.

Proof. If $f(x) = f_1(x)f_2(x)$, then ...

Example $x^2 + 1$ over $\mathbb{Z}_3, \mathbb{Z}_5$.

Theorem 17.2 Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ is reducible over $\mathbb{Q}$ if and only if it is reducible over $\mathbb{Z}$.

To prove the theorem, we need the following concept and lemma.

The content of $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ is $\gcd(a_0, \ldots, a_n)$. If the content of $f(x)$ is 1, then $f(x)$ is primitive.

Lemma Suppose $f(x), g(x) \in \mathbb{Z}[x]$ are primitive. Then $f(x)g(x)$ is primitive.

Proof. If not, let p be a prime factor of the content of $f(x)g(x)$, and apply the ring homomorphism $\bar{\phi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ with $\phi : \mathbb{Z} \to \mathbb{Z}_p$ by $\phi(k) = [k]$. We have

$$0 = \bar{\phi}(f(x)g(x)) = \bar{\phi}(f(x))\bar{\phi}(g(x))$$

so that the product of two nonzero polynomials in the integral domain $\mathbb{Z}_p[x]$ equal to zero, which is a contradiction. □

Proof of Theorem 17.2

Suppose $f(x) \in \mathbb{Z}[x]$.

We may divide $f(x)$ by its content and assume that it is primitive.

Suppose $f(x) = g(x)h(x)$ so that $g(x), h(x) \in \mathbb{Q}[x]$ have lower degrees.

Then $abf(x) = ag(x)bh(x)$ so that $a, b \in \mathbb{N}$ are the smallest integers such that $ag(x), bh(x) \in \mathbb{Z}[x]$.

Suppose c and d are the contents of $ag(x)$ and $bh(x)$, then $abf(x)$ has content ab and $abf(x) = ag(x)bh(x) = (c\tilde{g}(x))(d\tilde{h}(x))$, where $\tilde{g}(x), \tilde{h}(x)$ is primitive. By the lemma, $\tilde{g}(x)\tilde{h}(x)$ is primitive so that cd is the content of $abf(x)$. Consequently, $ab = cd$.

Thus, $ab = cd$ and $f(x) = \tilde{g}(x)\tilde{h}(x)$.

Clearly, if $f(x)$ is reducible in $\mathbb{Z}[x]$, then it is reducible in $\mathbb{Q}[x]$. □

Example $6x^2 + x - 2 = (3x - 3/2)(2x + 4/3) = (2x - 1)(3x + 2)$.

Theorem 17.3 Let p be a prime number, and suppose

$$f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x] \quad \text{with} \quad n \geq 2.$$

Suppose $\tilde{f}(x) = [a_0]_p + \cdots + [a_n]_p x^n$ has degree n, i.e., $p \nmid a_n$.
If $\tilde{f}(x)$ is irreducible then $f(x)$ is irreducible over $\mathbb{Z}$ (or $\mathbb{Q}$).

Proof. We prove the contra-positive. Suppose $f(x) = g(x)h(x)$.
Then $\tilde{f}(x) = \tilde{g}(x)\tilde{h}(x)$ has degree n implies that $\tilde{g}(x)$ and $g(x)$ have the same degree and also $\tilde{h}(x)$ and $h(x)$ have the same degree.
So, $\tilde{f}(x)$ is reducible. □

Theorem 17.4 Suppose $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ with $n \geq 2$. If there is a prime p such that

(a) p does not divide a_n,

(b) p^2 does not divide a_0, and

(c) $p|a_{n-1}, \ldots, p|a_0$,

then $f(x)$ is irreducible over $\mathbb{Z}$.

Proof. Assume $f(x) = g(x)h(x)$ with

$$g(x) = b_0 + \cdots + b_r x^r \text{ and } h(x) = c_0 + \cdots + c_s x^s.$$

We may assume that $p|b_0$ and p does not divide c_0.

Note that p does not divide $b_r c_s$ so that p does not divide b_r.

Let t be the smallest integer such that p does not divide b_t.

Then

$$p|(b_t a_0 + b_{t-1} a_1 + \cdots + b_0 a_t)$$

so that $p|b_t a_0$, a contradiction. □

Corollary For any prime p, the pth cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$$

is irreducible over $\mathbb{Q}$.

Proof. $\Phi(y+1) = \sum_{j=k}^{p} \binom{p}{k} y^k$ ...

Theorem 17.5 In $\mathbb{F}[x]$, $\langle p(x) \rangle$ is maximal if and only if $p(x)$ is irreducible.

Proof. If $p(x) = g(x)h(x)$ is reducible, then $\langle p(x) \rangle \subseteq \langle g(x) \rangle$.

If A is an ideal not equal to $\mathbb{F}[x]$ and not equal to $\langle p(x) \rangle$ such that $\langle p(x) \rangle \subseteq A$, then $A = \langle g(x) \rangle$ and $p(x) = g(x)h(x)$ such that $g(x)$ has degree less than $p(x)$. □

Corollary Let $\mathbb{F}$ be a field. Suppose $p(x)$ is irreducible.
(a) Then $E = \mathbb{F}[x]/\langle p(x) \rangle$ is a field.
(b) If $u(x), v(x) \in \mathbb{F}[x]$ and $p(x)|u(x)v(x)$, then $p(x)|u(x)$ or $p(x)|v(x)$.
(c) The polynomial $p(y) \in E$ has a zero in E, namely, $x + \langle p(x) \rangle$.

Proof. (a) By the fact that D/A is a field if and only if A is a maximal.
(b) $A = \langle p(x) \rangle$ is maximal, and hence is prime....
(c) Direct checking. □

Theorem 17.6 Every $f(x) \in \mathbb{F}[x]$ can be written as a product of irreducible polynomials. The factorization is unique up to a rearrangement of the factors and multiples of the factors by the field elements.

Proof. By induction on degree. $f(x) = \prod f_i(x)$ such that every $f_i(x)$ is irreducible. If $\prod f_i(x) = \prod g_j(x)$, then $f_i(x)$ divides some g_j ...

Examples

1. Show that $3x^5 + 15x^4 - 20x^3 + 10x + 20$ is irreducible over $\mathbb{Q}$.
2. If $r \in \mathbb{R}$ such that $r + 1/r \in \mathbb{Z} \setminus \{2, -2\}$, than r is irrational.
3. Show that $x^4 + 1$ is reducible over $\mathbb{Z}_p$ for any prime p.
   If $p = 2$ then $x^4 + 1 = (x^2 + 1)^2$. Suppose $p > 2$.
   If there is $a^2 = -1$, then $x^4 + 1 = (x^2 + a)(x^2 - a)$.
   If there is $a^2 = 2$, then $x^4 + 1 = (x^2 + ax + a)(x^2 - ax + 1)$.
   If there is $a^2 = -2$, then $x^4 + 1 = (x^2 + ax - 1)(x^2 - ax - 1)$.
   To show that one of the above holds, consider $\phi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ defined by $\phi(x) = x^2$. Then $\ker(\phi) = \{-1, 1\}$. If $-1, 2 \in H = \phi(\mathbb{Z}_p^*)$ then we are done. Assume not. Since H is isomorphic to $\mathbb{Z}_p^*/\ker(\phi)$ has index 2, we see that $-H = 2H \neq H$ and $H = (-H)(-H) = (-2)H$, i.e., $-2 \in H$.

Theorem 17.6 [Unique Factorization in $\mathbb{Z}[x]$] Every polynomial in $\mathbb{Z}[x]$ can be uniquely express as $b_1 \cdots b_s p_1(x) \cdots p_m(x)$, where $b_1, \ldots, b_s$ are irreducible polynomials of degree zero, and $p_1(x), \ldots, p_m(x)$ are irreducible polynomials of positive degree.

An application to weird dice construction.
Probabilities of the sum $m \in \{2, \ldots, 12\}$ in rowing two dices are determined by the coefficients of:

$$\begin{aligned} & (x + \cdots + x^6)(x + \cdots + x^6) \\ = \quad & [x(x+1)(x^2+x+1)(x^2-x+1)]^2 \\ = \quad & (x + x^2 + x^2 + x^3 + x^3 + x^4)(x + x^3 + x^4 + x^5 + x^6 + x^8). \end{aligned}$$