6 Factorization of Polynomials

Recall that if D is an integral domain, $D[x]$ is an integral domain and $U(D[x]) = U(D)$. Both of them are consequences of $\deg f(x)g(x) = \deg f(x) + \deg g(x)$.

Definition 6.1 Let D be an integral domain. A polynomial $f(x) \in D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible* over D if, whenever $f(x)$ is expresses as a product $f(x) = g(x)h(x)$, $g(x)$ and $h(x)$ are from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero nonunit element of $D[x]$ that is not irreducible over D is called *reducible* over D.

If F is a field, $f(x) \in F[x]$ is a non-zero non-unit polynomial if and only if $\deg f(x) \geq 1$. Hence a non-constant polynomial $f(x) \in F[x]$ is irreducible if $f(x)$ can not be expressed as a product of two polynomials of lower degree.

Example 6.1

1. $f(x) = 2x^2 + 4$ is irreducible over $\boldsymbol{Q}$ but reducible over $\boldsymbol{Z}$.
2. $f(x) = 2x^2 + 4$ is irreducible over $\boldsymbol{R}$ but reducible over $\boldsymbol{C}$.
3. Let F be a field. A polynomial $f(x) \in F[x]$ of degree at most three is reducible if and only if there is $a \in F$ such that $f(a) = 0$.

Definition 6.2 The *content* of a nonzero polynomial $f(x) = a_n x^2 + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \boldsymbol{Z}[x]$ is the greatest common divisor of $a_n, a_{n-1}, \ldots, a_0$ and denoted by $c(f(x))$. A *primitive polynomial* is an element of $\boldsymbol{Z}[x]$ with content 1.

1. Every polynomial $f(x) \in \boldsymbol{Z}[x]$ can be written as $f(x) = c(f(x))f_0(x)$, where $f_0(x) \in \boldsymbol{Z}[x]$ is primitive. Since the greatest common divisor is uniquely determined, $c(f(x))$ is uniquely determined.
2. Every polynomial $f(x) \in \boldsymbol{Q}[x]$ can be written as $f(x) = cf_0(x)$, where $c \in \boldsymbol{Q}$ and $f_0(x) \in \boldsymbol{Z}[x]$ is primitive. If $f(x) = dg_0(x)$ for some constant $d \in \boldsymbol{Q}$ and a primitive polynomial $g_0(x)$, then $c = \pm d$. So if both c and d are nonnegative, $c = d$, and $c \in \boldsymbol{Z}$ if and only if $f(x) \in \boldsymbol{Z}[x]$.

Proposition 6.1 (Gauss' Lemma) *Let $f(x)$ and $g(x)$ be primitive polynomials in $\boldsymbol{Z}[x]$. Then $f(x)g(x)$ is also primitive.*

Proof. Suppose $f(x)g(x)$ is not primitive. Let p be a prime factor of $c(f(x)g(x))$. Then $\bar{f}(x)\bar{g}(x) = \overline{f(x)g(x)} = 0 \in \boldsymbol{Z}_p[x]$. Since $\boldsymbol{Z}_p[x]$ is an integral domain, $\bar{f}(x) = 0$ or $\bar{g}(x) = 0$ in $\boldsymbol{Z}_p[x]$. This is absurd. ∎

Proposition 6.2 (Theorem 17.2) *Let $f(x) \in \boldsymbol{Z}[x]$ be a primitive polynomial, then $f(x)$ is irreducible over $\boldsymbol{Z}$ if and only if it is irreducible over $\boldsymbol{Q}$.*

Proof. We may assume that $f(x)$ is primitive. Suppose $f(x) = g(x)h(x)$ in $\boldsymbol{Q}[x]$. Let a and b be the least common multiple of the denominators of $g(x)$ and $h(x)$ respectively. Then

$$ab \cdot f(x) = (a \cdot g(x))(b \cdot h(x)) = c(a \cdot g(x))g_0(x)c(b \cdot h(x))h_0(x),$$

where $g_0(x)$ and $h_0(x)$ are primitive polynomials in $\boldsymbol{Z}[x]$. Now $\pm ab = c(a \cdot g(x))c(b \cdot h(x))$ and $f(x) = \pm g_0(x)h_0(x)$ by the previous proposition. Since $\deg g_0(x) = \deg g(x)$ and $\deg h_0(x) = \deg h(x)$, $f(x)$ is reducible over $\boldsymbol{Z}$. ∎

Proposition 6.3 (Theorem 17.3) *Let p be a prime and suppose that $f(x) \in \boldsymbol{Z}[x]$ be a primitive polynomial with degree $f(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $\boldsymbol{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\bar{f}(x)$ is irreducible over $\boldsymbol{Z}_p$, i.e., in $\boldsymbol{Z}_p[x]$, and $\deg \bar{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over $\boldsymbol{Q}$.*

Proof. Suppose $f(x) = g(x)h(x)$ with $g(x), h(x) \in \boldsymbol{Z}[x]$. Then $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$. Since $\boldsymbol{Z}_p[x]$ is an integral domain and $\deg f(x) = \deg \bar{f}(x)$ by assumption, we have

$$\deg g(x) + \deg h(x) = \deg f(x) = \deg \bar{f}(x) = \deg \bar{g}(x) + \deg \bar{h}(x) \leq \deg g(x) + \deg h(x).$$

Hence $\deg g(x) = \deg \bar{g}(x)$ and $\deg h(x) = \deg \bar{h}(x)$. Since $\bar{f}(x)$ is irreducible, the only possibility is either $\deg g(x) = 0$ or $\deg h(x) = 0$, say $\deg g(x) = 0$. Since $f(x)$ is primitive, $g(x) \in U(\boldsymbol{Z}) = \{\pm 1\}$ and $f(x)$ is irreducible over $\boldsymbol{Z}$, and hence it is irreducible over $\boldsymbol{Q}$ by Proposition 6.2. ■

Example 6.2

1. Let $f(x) = 21x^3 - 3x^2 + 2x + 9$. Then $\bar{f}(x) = x^3 + x^2 + 1 \in \boldsymbol{Z}_2[x]$ is irreducible as $f(0) \neq 0 \neq f(1)$. So $f(x)$ is irreducible over $\boldsymbol{Q}$ by Example 6.2–3.
2. Let $g(x) = x^5 + 2x + 4$. Then $\bar{g}(x) = x^5 - x + 1 \in \boldsymbol{Z}_3[x]$. Irreducible polynomial of degree at most 2 are x, $x+1$, x^2+1, x^2+x+2 and x^2-x-1 in $\boldsymbol{Z}_3[x]$.
3. $h(x) = x^4 + 1 \in \boldsymbol{Q}[x]$ is irreducible but it is reducible over $\boldsymbol{Z}_p$ for every prime p. (Exercise 29).

Proposition 6.4 (Theorem 17.4 Eisenstein's Criterion (1850)) *Let*

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

If there is a prime p such that $p \mid a_0$, $p \mid a_1, \ldots, p \mid a_{n-1}$, but $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible over $\boldsymbol{Q}$.

Proof. We may assume that $f(x)$ is primitive. Suppose that $f(x)$ is reducible over $\boldsymbol{Z}$ and

$$f(x) = (b_0 + b_1 x + \cdots + b_r x^r)(c_0 + c_1 x + \cdots + c_s x^s)$$

where b_i, $c_j \in \boldsymbol{Z}$, $r, s < n$, and $r + s = n$. Then

$$a_i = b_0 c_i + b_1 c_{i-1} + \cdots + b_i c_0.$$

Now by hypothesis $p \mid a_0 = b_0 c_0$ but $p^2 \nmid a_0$; thus p must divide exactly one of b_0 and c_0, say $p \mid b_0$ and $p \nmid c_0$. Also p cannot divide every b_i since otherwise it would divide $a_n = b_0 c_n + \cdots + b_n c_0$. Therefore, there is a smallest positive integer k such that $p \nmid b_k$. Now p divides each of $b_0, b_1, \ldots, b_{k-1}$ and also $p \mid a_k$ since $k \leq r < n$. Since $a_k = (b_0 c_k + \cdots + b_{k-1} c_1) + b_k c_0$, it follows that $p \mid b_k c_0$. Hence $p \mid b_k$ or $p \mid c_0$, both of which are forbidden. ■

Example 6.3 If p is a prime, the polynomial $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $\boldsymbol{Q}$.

$$\begin{aligned} g(x) &= f(x+1) = 1 + (x+1) + (x+1)^2 + \cdots + (x+1)^{p-1} \\ &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{2} x + \binom{p}{1}. \end{aligned}$$

Hence we can apply Eisenstein's Criterion.

Proposition 6.5 (Theorem 17.5) *Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x)\rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F.*

Proof. By Theorem 5.3, $F[x]$ is a principal ideal domain. So if A is an ideal with $\langle p(x)\rangle \subseteq A \subseteq F[x]$, then $A = \langle q(x)\rangle$ for some polynomial $q(x) \in F[x]$. $p(x) \in \langle q(x)\rangle$ if and only if $q(x) \mid p(x)$, and $\langle q(x)\rangle = F[x]$ if and only if $q(x)$ is a nonzero constant. ∎

Corollary 6.6 *Let F be a field and $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.*

Proof. $\langle p(x)\rangle$ is a prime ideal. ∎

Example 6.4

1. $x^n - p$ is irreducible over $\boldsymbol{Q}$ for a positive integer n and a prime p.
2. Recall that $f(x) = 21x^3 - 3x^2 + 2x + 9$ is irreducible over $\boldsymbol{Q}$ and $\bar{f}(x) = x^3 + x^2 + 1 \in \boldsymbol{Z}_2[x]$ is irreducible over $\boldsymbol{Z}_2$ by Example 6.2. Hence $\boldsymbol{Q}[x]/\langle f(x)\rangle$ is a field with infinitely many elements and $\boldsymbol{Z}_2[x]/\langle \bar{f}(x)\rangle$ is a field with 2^3 elements.
3. Similarly, $g(x) = x^5 + 2x + 4$ is irreducible over $\boldsymbol{Q}$ and $\bar{g}(x) = x^5 - x + 1 \in \boldsymbol{Z}_3[x]$ is irreducible over $\boldsymbol{Z}_3$ by Example 6.2. Hence $\boldsymbol{Q}[x]/\langle g(x)\rangle$ is a field with infinitely many elements and $\boldsymbol{Z}_3[x]/\langle \bar{g}(x)\rangle$ is a field with 3^5 elements.

Theorem 6.7 (Theorem 17.6 (Unique Factorization in $\boldsymbol{Z}[x]$)) *Every polynomial in $\boldsymbol{Z}[x]$ that is not the zero polynomial or a unit in $\boldsymbol{Z}[x]$ can be written in the form $b_1 b_2 \cdots b_s$ $p_1(x)p_2(c)\cdots p_m(x)$ where b_i's are irreducible polynomial of degree 0*[13] *and $p_i(x)$'s are irreducible polynomials of positive degree. Furthermore such decomposition is unique, i.e.,*

$$b_1 b_2 \cdots b_s p_1(x)p_2(x)\cdots p_m(x) = c_1 c_2 \cdots c_t q_1(x) q_2(x) \cdots q_n(x)$$

implies, $s = t$, $m = n$ and, after renumbering the c's and $q(x)$'s, we have $b_i = \pm c_i$ for $i = 1, 2, \ldots, s$, and $p_i(x) = \pm q_i(x)$. for $i = 1, 2, \ldots, m$.

Proof. (a) Any non-constant polynomial $f(x)$ in $\boldsymbol{Z}[x]$ is expressible as a product of irreducible elements of $\boldsymbol{Z}$ and primitive irreducible polynomials over $\boldsymbol{Z}$.

Proof of (a). First of all write $f(x) = c(f(x))f_0(x)$ where $f_0(x) \in \boldsymbol{Z}[x]$ is primitive using Lemma 7.9. Hence $c(f(x))$ is either a unit, i.e., 1 in this case, or a product of irreducibles of $\boldsymbol{Z}$, i.e., $\pm p$, where p is a prime. So we can assume that $f(x)$ is primitive. If $f(x)$ is irreducible, we are done. So assume $f(x) = g(x)h(x)$ where $g(x), h(x)$ are non-unit polynomials $\boldsymbol{Z}[x]$. Since $f(x)$ is primitive, $g(x)$ and $h(x)$ are primitive polynomials of degree at least 1. Hence by induction on degree, $f(x)$ can be written as a product of irreducible primitive polynomials of positive degree. ∎

(b) The uniqueness of expression.

Proof of (b). Suppose

$$b_1 b_2 \cdots b_s p_1(x)p_2(c)\cdots p_m(x) = c_1 c_2 \cdots c_t q_1(x) q_2(c) \cdots q_n(x)$$

Then $c(f(x)) = \pm b_1 b_2 \cdots b_s = \pm c_1 c_2 \cdots c_t$. Hence by the uniqueness of factorization in $\boldsymbol{Z}$, this decomposition is unique. Thus we have $p_1(x)p_2(c)\cdots p_m(x) = q_1(x)q_2(c)\cdots q_n(x)$. Since $\langle p_1(x)\rangle$ is a maximal ideal in $\boldsymbol{Q}[x]$, there exists $q_i(x)$ such that $q_i(x) = h(x)p_1(x)$. Since both $q_i(x)$ and $p(x)$ are primitive and irreducible, $h(x) = h_1/h_2$ with $h_1, h_2 \in \boldsymbol{Z}$ and $h_2 q_i(x) = h_1 p(x)$ implies that $h_2 = \pm h_1$. Therefore, $q_i(x) = \pm p(x)$. Now the uniqueness follows by induction. ∎

[13] b is an irreducible polynomial of degree 0 if and only if b or $-b$ is a prime number in $\boldsymbol{Z}$.