17 Factorization of Polynomials

Definition 17.1. *Irreducible Polynomial, Reducible Polynomial*
Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be irreducible over D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ 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.

EXAMPLE 1 The polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Z}$, since $2x^2 + 4 = 2(x^2 + 2)$ and neither 2 nor $x^2 + 2$ is a unit in $\mathbb{Z}[x]$.
EXAMPLE 2 The polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$.
EXAMPLE 3 The polynomial $x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.
EXAMPLE 4 The polynomial $x^2 + 1$ is irreducible over $\mathbb{Z}_3$ but reducible over $\mathbb{Z}_5$.

Theorem 17.1. *Reducibility Test for Degrees 2 and 3*
Let $\mathbb{F}$ be a field. If $f(x) \in \mathbb{F}[x]$ and deg f(x) is 2 or 3, then f(x) is reducible over $\mathbb{F}$ if and only if $f(x)$ has a zero in $\mathbb{F}$.

Definition 17.2. *Content at a Polynomial, Primitive Polynomial*
The content *of a nonzero polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, where the a's are integers, is the greatest common divisor of the integers $a_n, a_{n-1}, \ldots, a_0$. A primitive polynomial is an element of $\mathbb{Z}[x]$ with content 1.*

Lemma 17.1. *Gauss's Lemma*
The product of two primitive polynomials is primitive.

Theorem 17.2. *Reducibility over $\mathbb{Q}$ Implies Reducibility over $\mathbb{Z}$*
Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Theorem 17.3. *Mod p Irreducibility Test*
Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $deg(f(x)) \leq 1$.
Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $degf(x) = degf(x)$ then $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 17.4. *Eisenstein's Criterion (1850)*
Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$.
If there is a prime p such that $p \nmid a_n, p|a_{n-1}, \ldots, p|a_0$ and $p^2 \nmid a_0$. then $f(x)$ is irreducible over $\mathbb{Q}$.

Corollary 17.5. *Irreducibility of pth Cyclotomic Polynomial*
For any prime p, the pth cyclotomic polynomial

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

is irreducible over $\mathbb{Q}$.

Theorem 17.6. *$\langle p(x) \rangle$ is Maximal If and Only If $p(x)$ is Irreducible*
Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $\mathbb{F}[x]$ if and only if $p(x)$ is irreducible over $\mathbb{F}$.

Theorem 17.7. *Unique Factorization in $\mathbb{Z}[x]$*
Every polynomial in $\mathbb{Z}[x]$ that is not the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form $b_1b_2 \ldots b_sp_1(x)p_2(x) \ldots p_m(x)$, where the b_i's are irreducible polynomials of degree 0 and the pl(x)'s are irreducible polynomials of positive degree. Furthermore, if

$$b_1b_2 \ldots b_sp_1(x)p_2(x) \ldots p_m(x) = c_1c_2 \ldots c_tq_1(x)q_2(x) \ldots q_n(x),$$

where the b_i's and c_i's are irreducible polynomials of degree 0 and the $p_i(x)$'s and $q_i(x)$'s are irreducible polynomials of positive degree, then $s = t, m = n$, and, after renumbering the c's and $q(x)$'s, we have $b_i = \pm c_i$ for $i = 1, \ldots, s$ and $p_i(x) = \pm q_i(x)$ for $i = 1, \ldots, m$.

2. Suppose that D is an integral domain and $\mathbb{F}$ is a field containing D. If $f(x) \in D[x]$ and $f(x)$ is irreducible over $\mathbb{F}$ but reducible over D, what can you say about the factorization of $f(x)$ over D?

4. Suppose that $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If r is rational and $x - r$ divides $f(x)$, show that r is an integer.

7. Suppose there is a real number r with the property that $r + 1/r$ is an odd integer. Prove that r is irrational.

8. Show that the equation $x^2 + y^2 = 2003$ has no solutions in the integers.