Chapter 16 Polynomial Rings

Notation Let R be a commutative ring. The ring of polynomials over R in the indeterminate x is the set

$$R[x] = \{a_0 + \cdots + a_n x^n : n \in \mathbb{N},\ a_0, \ldots, a_n \in R\}.$$

We can consider equality, addition, multiplication and degree of a polynomial $f(x) \in R[x]$.

Theorem 16.1 If $\mathbb{D}$ is an integral domain, then $\mathbb{D}[x]$ is an integral domain.

Theorem 16.2 If $\mathbb{F}$ is a field, and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, then there exist unique polynomials $q(x), r(x)$ such that $f(x) = g(x)q(x) + r(x)$ with $\deg(r(x)) \leq \deg(g(x))$.

Corollary Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$, $a \in \mathbb{F}$. Then the following holds.

(a) $f(x) = (x - a)q(x) + f(a)$, i.e., $f(a)$ is the remainder.

(b) $(x - a)$ is a factor of $f(x)$ if and only if $f(a) = 0$.

(c) If $\deg(f(x)) = n$, then $f(x)$ has at most n zeros, counting multiplicities.

Theorem If $\mathbb{F}$ is a finite field, then the nonzero elements in $\mathbb{F}$ is a cyclic group under multiplication.

Definition A principal ideal domain is an integral domain $\mathbb{D}$ in which every ideal has the form $\langle a \rangle = \{ra : r \in \mathbb{D}\}$ for some $a \in \mathbb{D}$.

Theorem 16.3-4 Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a principal ideal domain. In fact, for any ideal A of $F[x]$, $A = \langle g(x) \rangle$, where $g(x)$ is a nonzero monic polynomial in A with minimum degree.

Example 1 Suppose $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ and $A = \langle x^2 - 2 \rangle$. Then

$$\mathbb{F} = \mathbb{Q}[x]/A = \{ax + b + A : a, b \in \mathbb{Q}\}$$

is a field. For every nonzero $ax + b + A \in \mathbb{F}$, the multiplicative inverse is $(ax - b)/(2a^2 - b^2) + A$ as

$$(ax + b + A)((ax - b)/(2a^2 - b^2) + A)$$

$$= (a^2x^2 - b^2)/(2a^2 - b^2) + A = (2a^2 - b^2)/(2a^2 - b^2) + A = 1 + A.$$

Here note that $2a^2 - b \neq 0$ because $a, b \in \mathbb{Q}$. Note that by factor theorem, $f(x)$ has no zeros in $\mathbb{Q}$. But $x + A \in \mathbb{F}$ is a solution of the equation $y^2 - 2 = 0$, where $2 = 2(1 + A) = 2 + A$, as $(x + A)^2 - (2 + A) = (x^2 - 2) + A = 0 + A$.

Corollary Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$. Then $A = \langle f(x) \rangle$ is maximal if and only if $f(x) \neq g(x)h(x)$ for some polynomials $g(x), h(x)$ of lower degrees.

Chapter 17 Factorization of Polynomials

Definition Let $\mathbb{D}$ be an integral domain. A polynomial $f(x)$ in $\mathbb{D}[x]$ is reducible if $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in \mathbb{D}[x]$ such that both $g(x), h(x)$ have degrees smaller than $f(x)$. If $f(x)$ has degree at least 2 and not reducible, then it is irreducible.

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 $\mathbb{F}$.

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 $\mathbb{Z}$.

Proof. 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.

Assertion 1. Suppose $u(x), v(x) \in \mathbb{Z}[x]$ are primitive. We claim that $u(x)v(x)$ is primitive. If not ...

Return to the proof of the theorem.

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 $abf(x) = ag(x)bh(x) = (c\tilde{g}(x))(d\tilde{h}(x))$ with has content cd. Thus, $ad = cd$ and $f(x) = \tilde{g}(x)\tilde{h}(x)$.

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

Theorem 17.3 Let p be a prime number, and suppose $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ with $n \geq 2$. Suppose $\tilde{f}(x) = [a_0]_p + \cdots + [a_n]_p x^n$ has degree n. If $\tilde{f}(x)$ is irreducible then $f(x)$ is irreducible over $\mathbb{Z}$ (or $\mathbb{Q}$).

Proof. If $f(x) = g(x)h(x)$ 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. $\square$

Example Consider $21x^3 - 3x^2 + 2x + 9 \in \mathbb{Q}[x]$.

Try $x = m/n$ for $m = 1, 3, 7, 21$ and $n = \pm 1, 3, 9$.

Send it to $\mathbb{Z}_p[x]$ for $p = 2, 3, 5$.

Example Consider $(3/7)x^4 - (2/7)x^2 + (9/35)x + 3/5$.

Send $35f(x) = 15x^4 - 10x^2 + 9x + 21$ to $\mathbb{Z}_2[x]$ and check irreducibility.

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 p does not divide a_n and p^2 does not divide a_0, but $p|a_{n-1}, \ldots, p|a_0$, 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. □

Example Show that $3x^5 + 15x^4 - 20x^3 + 10x + 20$ is irreducible over $\mathbb{Q}$.

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 Let $\mathbb{F}$ be a field, and $p(x) \in \mathbb{F}[x]$. Then $\langle p(x) \rangle$ is maximal if and only if $p(x)$ is irreducible.

Proof. If $p(x) = g(x)h(x)$ 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 $\mathbb{F}[x]/\langle p(x) \rangle$ is a field.

(b) If $u(x), v(x) \in \mathbb{F}[x]$ and $f(x)|u(x)v(x)$, then $p(x)|u(x)$ or $p(x)|v(x)$.

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....

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 ...