Lecture notes Abstract Modern Algebra: Lecture 22

1 Rings of polynomials II

1.1 Irreducible polynomials

Definition 1. A non-constant polynomial $f(x) \in F[x]$ is irreducible over a field F if $f(x)$ **cannot be expressed as a product of two polynomials** $g(x)$ and $h(x)$ in $F[x]$, where the degrees of $g(x)$ and $h(x)$ are both smaller than the degree of $f(x)$. Irreducible polynomials function as the "prime numbers" of polynomial rings. A polynomial that is not irreducible is called then reducible.

Example 2. The polynomial $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$. The polynomial $x^2 + 1$ is irreducible over $\mathbb{R}[x]$. The polynomial $x^2 - x - 1$ is irreducible over $\mathbb{Q}[x]$ and of course also over $\mathbb{Z}[x]$.

Definition 3. A principal ideal domain (PID), is an integral domain where every ideal is generated by one element.

Proposition 4. *Let F be a field. Then, the ring $F[x]$ is a PID.*

Proof. Suppose that I is a nontrivial ideal in $F[x]$, and let $p(x) \in I$ be a nonzero element of minimal degree. If $\deg p(x) = 0$, then $p(x)$ is a nonzero constant and 1 must be in I. Since 1 generates all of $F[x]$, the ideal $I = F[x] = \langle 1 \rangle$ is a principal ideal. Now assume that our polynomial $p(x)$ of minimal degree in I has $\deg p(x) > 0$ and let $f(x)$ be any element in I. By the division algorithm there exist $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = p(x)q(x) + r(x)$ and $\deg r(x) < \deg p(x)$. Since both $f(x)$ and $p(x)$ are in I and I is an ideal, $r(x) = f(x) - p(x)q(x)$ is also in I. However, since we chose $p(x)$ to be of minimal degree, $r(x)$ must be the zero polynomial and $I = \langle p(x) \rangle$ is a principal ideal. □

Theorem 5. *Let F be a field and suppose that $p(x) \in F[x]$. Then the ideal generated by $p(x)$ is maximal if and only if $p(x)$ is irreducible.*

Proof. Suppose that $p(x)$ generates a maximal ideal of $F[x]$. Then $\langle p(x) \rangle$ is also a prime ideal of $F[x]$. Since a maximal ideal must be properly contained inside $F[x]$, the polynomial $p(x)$ cannot be a constant polynomial. Let us assume that $p(x)$ factors into two polynomials of lesser degree, say $p(x) = f(x)g(x)$. Since $\langle p(x) \rangle$ is a prime ideal one of these factors, say $f(x)$, is in $\langle p(x) \rangle$ and therefore be a multiple of $p(x)$. But this would imply that $\langle p(x) \rangle \subset \langle f(x) \rangle$, which is impossible since $\langle p(x) \rangle$ is maximal. Conversely, suppose that $p(x)$ is irreducible over $F[x]$. Let I be an ideal in $F[x]$ containing $\langle p(x) \rangle$. Since $F[x]$ is a PID, the ideal I is a principal ideal; hence, $I = \langle f(x) \rangle$ for some $f(x \in F[x]$. Since $p(x) \in I$, it must be the case that $p(x) = f(x)g(x)$ for some $g(x)$. However, $p(x)$ is irreducible; hence, either $f(x)$ or

$g(x)$ is a constant polynomial. If $f(x)$ is constant, then $I = F[x]$ and we are done. If $g(x)$ is constant, then $f(x)$ is a constant multiple of I and $I = \langle p(x) \rangle$. Thus, there are no proper ideals of $F[x]$ that properly contain $\langle p(x) \rangle$. $\square$

Corollary 6. *Let F be a field, a prime ideal of $F[x]$ is also maximal.*

Proof. Let $P \neq 0$ be a prime ideal in $F[x]$. Suppose that $P = \langle p \rangle$. If $p = a \cdot b$ is reducible $(\deg(a), \deg(b) < \deg(p)$), then $a \in P$ or $b \in P$. Suppose, for example, that $a = pa_0 \in P$. We will have $p = pb_0 b \Rightarrow p(1 - b_0 b) = 0 \Rightarrow b_0 b = 1$ and b is invertible in $F[x]$. This gives $\deg(b(x)) = 0$ and $\deg(a(x)) = \deg(p)$. $\square$

Corollary 7. *On the ring of polynomials $F[x]$ over the field F, the following three coincide:*

1. *Prime ideals.*
2. *Maximal ideals.*
3. *Ideals generated by irreducible.*

We would like to be able to determine whether or not a polynomial is irreducible.

Lemma 8. *(Gauss lemma) If a monic polynomial $p(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}[x]$, then is also reducible over $\mathbb{Z}[x]$ as the product*

$$f(x) = a(x)b(x)$$

of monic polynomials $a(x), b(x) \in \mathbb{Z}[x]$.

Proof. Let $p(x) = \alpha(x)\beta(x)$ on $\mathbb{Q}[x]$ with

$$\alpha(x) = \frac{c_1}{d_1}(a_0 + a_1 x + \cdots + a_m x^m) = \frac{c_1}{d_1}\alpha_1(x),$$

$$\beta(x) = \frac{c_2}{d_2}(b_0 + b_1 x + \cdots + b_n x^n) = \frac{c_2}{d_2}\beta_1(x),$$

for polynomials $\alpha_1(x)$ and $\beta_1(x)$ in $\mathbb{Z}[x]$ with coefficients without any common factors. Consider the fraction $\frac{c}{d}$ as the product of $\frac{c_1}{d_1}$ and $\frac{c_2}{d_2}$ expressed in lowest terms. Hence, $dp(x) = c\alpha_1(x)\beta_1(x)$ If $d = 1$,then $ca_m b_n = 1$ since $p(x)$ is a monic polynomial. Hence, either $c = 1$ or $c = -1$. If $c = 1$, then either $a_m = b_n = 1$ or $a_m = b_n = -1$. In the first case $p(x) = \alpha_1(x)\beta_1(x)$, where $\alpha_1(x)$ and $\beta_1(x)$ are monic polynomials with $\deg \alpha(x) = \deg \alpha_1(x)$ and $\deg \beta(x) = \deg \beta_1(x)$. In the second case we take $a(x) = -\alpha_1(x)$ and $b(x) = -\beta_1(x)$ as the correct monic polynomials since $p(x) = (-\alpha_1(x))(-\beta_1(x)) = a(x)b(x)$. The case in which $c = -1$ can be handled similarly. Now suppose that $d \neq 1$. Since $\gcd(c, d) = 1$, there exists a prime p such that p divides d and p does not divide c. Also, since the coefficients of $\alpha_1(x)$ are relatively prime, there exists a coefficient a_i such that p does not divide a_i. Similarly, there exists a coefficient b_j of $\beta_1(x)$ such that p does not divide b_j. Let us reduce the polynomials α_1 and β_1 mod p to obtain $\alpha_1'(x)$ and $\beta_1'(x)$. We get $0 = d = \alpha_1'(x)\beta_1'(x)$. However, this is impossible since $\mathbb{Z}p[x]$ is an integral domain. $\square$

Theorem 9. *(Eisenstein's Criterion) Let p be a prime and suppose that*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

If the number p is such that p divides a_i for $i = 0, 1, \ldots, n-1$, but p does not divide a_n and p^2 does not divide a_0, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. By Gauss's Lemma, we need only show that $f(x)$ does not factor into polynomials of lower degree in $\mathbb{Z}[x]$. Let

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

be a factorization in $\mathbb{Z}[x]$, with b_r and c_s not equal to zero and $r, s < n$. Since p^2 does not divide $a_0 = b_0 c_0$, either b_0 or c_0 is not divisible by p. Suppose that p divides c_0 and not b_0. Since p does not divide $a_n = b_r c_s$, neither b_r nor c_s is divisible by p. Let m be the smallest value of k such that p does not divide c_k. Then

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0$$

is not divisible by p, since each term on the right-hand side of the equation is divisible by p except for $b_0 c_m$. Therefore, $s = m = n$ since a_i is divisible by p for $m < n$. Hence, $f(x)$ cannot be factored into polynomials of lower degree and therefore must be irreducible. $\square$

Example 10. The polynomial $f(x) = x^5 + 7x^4 + 14x^3 + 21x^2 + 35$ is irreducible over $\mathbb{Z}$ using $p = 7$.

Example 11. Let p be a prime number. The polynomial $f(x) = \dfrac{(x+1)^p - 1}{x}$ is irreducible on $\mathbb{Z}[x]$. We express

$$f(x) = x^{p-1} + p x^{p-2} + \frac{1}{2} p(p-1) x^{p-3} + \cdots + \frac{1}{2} p(p-1) x + p,$$

where the coefficients are $\binom{p}{k}$, for $k = 1, \ldots, p-1$, are all divisible by p. The independent term however is $a_0 = p$ not divisible by p^2 and we can apply Eisenstein.