LECTURE 19

Irreducibles and Unique Factorization

THEOREM 19.1. *Let F be a field. Then f is a unit in $F[x]$ if and only if f is a non-zero constant polynomial.*

Proof. Suppose f is a unit in $F[x]$. Then $f \neq 0_F$ and there exists $g \neq 0_F$ in $F[x]$ such that

$$fg = 1_F \quad .$$

Calculating the degrees both sides of this equation yields

$$\deg(f) + \deg(g) = 0 \quad .$$

Since the degree of any element of $F[x]$ is always a non-negative integer, we conclude that $\deg(f) = \deg(g) = 0$. So f must be a non-zero constant polynomial.

Conversely, if $c \in F$ and $c \neq 0_F$, then $c^{-1} \in F \subset F[x]$ exists since F is a field. So c is a unit in $F[x]$. □

DEFINITION 19.2. *Let F be a field. A polynomial $f \in F[x]$ is said to an **associate** of another polynomial $g \in F[x]$ if*

$$f = cg \quad .$$

for some nonzero $c \in F$.

Remark: Suppose p is an arbitrary polynomial of degree n, say

$$p = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$$

with $a_n \neq 0_F$. Then there is precisely one associate g of p that is monic; namely

$$g = a_n^{-1} p \quad .$$

DEFINITION 19.3. *Let F be a field. A nonconstant polynomial $p \in F[x]$ is said to be **irreducible** if its only divisors are its associates and the nonzero constants polynomials (the units of $F[x]$). A nonconstant polynomial that is not irreducible is said to be **reducible**.*

The following theorem shows that the irreducible polynomials in $F[x]$ have essentially the same divisibility properties as the prime numbers in $\mathbb{Z}$.

THEOREM 19.4. *Let F be a field and p a nonconstant polynomial in $F[x]$. Then the following conditions are equivalent:*

(1) *p is irreducible.*
(2) *If b and c are any polynomials such that $p \mid bc$, then $p \mid b$ or $p \mid c$.*
(3) *If r and s are any polynomials such that $p = rs$, then r or s is a nonzero constant polynomial.*

Proof.

(1) $\Rightarrow$ (2)

Suppose

$$p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad , \quad a_n \neq 0 \quad ,$$

is irreducible and suppose $p \mid bc$. Consider

$$d = GCD\,(p, b) \quad .$$

By definition d is the monic polynomial of highest degree that divides p and b. Since p is irreducible its only divisors of the form $q = c \in F$, $c \neq 0_F$, and $r = cp$, $c \in F$. The only monic divisors of p are thus 1_F and $a_n^{-1}p$. Thus,

$$d \in \left\{1_F, a_n^{-1}p\right\} \quad .$$

If $d = 1_F$, then p and b are relatively prime and Theorem 4.6 then implies $p \mid c$. If $d = a_n^{-1}p$, then $a_n^{-1}p$ divides b and hence so does p. Thus, if p is irreducible and $p \mid bc$, then $p \mid b$ or $p \mid c$.

(2) $\Rightarrow$ (3)

Now assume that p has the property that if $p \mid bc$ then $p \mid b$ or $p \mid c$.

If $p = rs$, then certainly $p \mid rs$. But then by hypothesis, $p \mid r$ or $p \mid s$. However,

$$\deg(p) = \deg(r) + \deg(s) \tag{1}$$

and we must also have

$$\deg(p) \leq \deg(r) \quad \text{or} \quad \deg(p) \leq \deg(s) \quad . \tag{2}$$

But (1) and (2) can not be both be satisfied unless either $\deg(r) = 0$ or $\deg(s) = 0$. Hence either r or s must be a nonzero constant polynomial.

(3) $\Rightarrow$ (1)

Now assume property (3) is true. Let q be any divisor of p. Then

$$p = qw$$

for some nonzero $w \in F[x]$. Property (3) implies either q or w is a nonzero element of F. Thus, either $q = c$ or $p = cq$. Thus, any divisor of p is either a nonzero constant polynomial or an associate of p. Hence, p is irreducible. □

Corollary 19.5. *Let F be a field and p an irreducible polynomial in $F[x]$. If $p \mid s_1 s_2 \cdots s_k$, then p must divide at least one of the polynomials s_i.*

Proof. This is proved by applying Property (2) of Theorem 4.8 repeatedly. If p divides $s_1 s_2 \cdots s_k = s_1 (s_2 \cdots s_k)$ then either p divides s_1 or p divides $s_2 \cdots s_k$. If the first case holds we are done, if not then $p \mid s_2 (s_3 \cdots s_k)$, so Property (2) implies either $p \mid s_2$ or $p \mid s_3 \cdots s_k$. If $p \mid s_2$ we are done; if not $p \mid s_3 (s_4 \cdots s_k)$. Continuing in this manner, one ends up the statement that either p divides one of the s_i, $i < k$, or $p \mid s_k$. Hence the conclusion of the Corollary follows. □

Theorem 19.6. *Let F be a field. Every nonconstant polynomial is a product of irreducible polynomials in $F[x]$. This factorization is unique in the following sense. If*

$$f = p_1 \cdots p_r \qquad \text{and} \qquad f = q_1 \cdots q_s \quad ,$$

with each p_i and each q_j irreducible, then $r = s$ and one can rearrange and relabel the factors q_i so that q_i is an associate of p_i, $i = 1, 2, \ldots, k$.

Proof.

Existence:

Let S be the set of all polynomials of degree ≥ 1 which are not the product of irreducibles. We want to show that S is empty. We will use a proof by contradiction.

Suppose S is non-empty and set

$$R = \{n \in \mathbb{N} \mid n = \deg(f) \text{ for some} f \in S\} \quad .$$

Since S is non-empty, R is an non-empty subset of $\mathbb{N}$ and so by the Well-Ordering Axiom, R has a least member r. Let p be a corresponding element of S.

Since $p \in S$, p is not a product of irreducibles; and so it is not itself an irreducible polynomial. Therefore, p must be divisible by some other nonconstant polynomials,

$$p = qr$$

at least one of which, say q, is not the product of irreducibles. But then

$$\deg(p) = \deg(q) + \deg(r) \leq \deg(q) + 1 \quad .$$

Since q is not the product of irreducibles, it belongs to S and has degree strictly less than p. But p was choosen to be an element of least degree in S. Hence, we have a contradiction, unless S is empty.

Uniqueness:

Now suppose

$$\begin{aligned} f(x) &= p_1(x)p_2(x)\cdots p_m(x) \\ &= q_1(x)q_2(x)\cdots q_n(x) \end{aligned} \tag{5}$$

with $p_1(x), \dots, p_m(x)$ and $q_1(x), \dots, q_n(x)$ all irreducible. We then have

$$q_1(x)q_2(x)\cdots q_n(x) = p_1(x)\left(p_2(x)\cdots p_m(x)\right) \quad . \tag{6}$$

Thus,

$$p_1(x) \mid q_1(x)\cdots q_n(x) \quad . \tag{7}$$

By Corollary 4.9, $p_1(x)$ must divide at least one of the $q_i(x)$. By reordering the $q_i(x)$ we can assume without loss of generality that $p_1(x) \mid q_1(x)$. But since $q_1(x)$ is by hypothesis irreducible its only non-constant divisors are its associates. Thus,

$$q_1(x) = c_1 p_1(x) \quad , \quad \text{for some } c_1 \in F. \tag{8}$$

Substituting (8) into the left hand side of (6) and then dividing both sides by $p_1(x)$ yields

$$c_1 q_2(x)\cdots q_n(x) = p_2(x)\left(p_3(x)\cdots p_m(x)\right) \quad . \tag{9}$$

Applying Corollary 4.9 again, we conclude that $p_2(x)$ must divide one of the factors $q_2(x), \dots, q_n(x)$ of the left hand side of (9). By reordering the $q_i(x)$, we can assume without loss of generality that $p_2(x) \mid q_2(x)$. Since $q_2(x)$ is irreducible, we must have

$$q_2(x) = c_2 p_2(x) \quad , \quad \text{for some } c_2 \in \mathbb{F} \text{ .} \tag{10}$$

Substituting (10) into the left hand side of (9) we get

$$c_1 c_2 q_3(x) q_4(x)\cdots q_n(x) = p_3(x)p_4(x)\cdots p_m(x) \quad .$$

We can continue in this manner to peal off irreducible factors from both sides of (10).

If $m > n$, then eventually we would reach

$$c_1 c_2 \cdots c_m = p_{m+1}(x)p_{m+2}(x)\cdots p_n(x) \quad . \tag{11}$$

But the left hand side of (11) is just a constant, while the right hand side is a product of non-constant polynomials. This can not happen (there is no way that the degrees of two sides can match). Therefore, we cannot have $m > n$.

If $m < n$, then eventually we would reach

$$c_1 c_2 \cdots c_n q_{n+1}(x)q_{n+2}(x)\cdots q_m(x) = 1_F \quad . \tag{19.1}$$

This can not occur either, because we cannot have a nonconstant polynomial dividing 1. Thus, we cannot have $m < n$ either.

Thus, $m = n$, and the peeling off procedure leads to

$$\begin{aligned} q_1(x) &= c_1 p_1(x) \\ q_2(x) &= c_2 p_2(x) \\ &\vdots \\ q_m(x) &= c_m p_m(x) \end{aligned}$$

with

$$c_1 c_2 \cdots c_m = 1_F$$

for a suitable reordering of the factors $q_1(x), \ldots, q_m(x)$. Thus, after a suitable reordering each factor $q_i(x)$ is an associate of the corresponding factor $p_i(x)$. $\square$