LECTURE 17

Polynomial Arithmetic and the Division Algorithm

DEFINITION 17.1. *Let R be any ring. A* ***polynomial with coefficients in*** *R is an expression of the form*

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$$

where each a_i is an element of R. The a_i are called the ***coefficients*** *of the polynomial and the element x is called an* ***indeterminant****.*

DEFINITION 17.2. *Let R be any ring. The* ***polynomial ring*** *$R[x]$ is the set of all polynomials with coefficients in R with an operation of addition defined by*

$$\begin{aligned}(a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_nx^n) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots \\ &\quad \cdots + (a_n + b_n)x^n\end{aligned}$$

(although, it appears that we are assuming the same powers of x to appear in each of the polynomials above; we can do this without loss of generality by inserting zero coefficients whereever necessary) and an operation of multiplication defined by

$$\begin{aligned}(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m) &= a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots \\ &\quad \cdots + \left(\sum_{i=0}^{k} a_ib_{k-i}\right)x^k + \cdots \\ &\quad \cdots + a_nb_mx^{n+m} \quad .\end{aligned}$$

DEFINITION 17.3. *Let R be a ring and let $f = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial in $R[x]$ such that $a_n \neq 0_R$. Then a_n is called the* ***leading coefficient*** *of f. The* ***degree*** *of f is the integer n.*

Because we seem to be on familiar ground, it is important to point out that strange things can sometimes happen. Consider the ring of polynomials over $\mathbb{Z}_4$. Then

$$\begin{aligned}([2]x + [1])^2 &= [2][2]x^2 + [2][1]x + [1][2]x + [1][1] \\ &= [4]x^2 + [4]x + [1] \\ &= [0]x^2 + [0]x + [1] \\ &= [1]\end{aligned}$$

Such peculiar circumstances can be avoided if we restrict our attention to polynomials over integral domains.

THEOREM 17.4. *If R is an integral domain and f, g are nonzero polynomials in $R[x]$, then*

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

Proof. Suppose

$$\begin{aligned}f &= a_0 + a_1x + \cdots + a_nx^n \\ g &= b_0 + b_1x + \cdots + b_mx^m\end{aligned}$$

are polynomials of degree n and m, respectively. Then the highest possible degree of fg is $n + m$, and the coefficient of x^{n+m} in fg is a_nb_m. Since R is an integral domain, $a_nb_m = 0_R$ if and only if $a_n = 0_R$ or $b_n = 0_R$. But since f and g are nonzero polynomials, a_n and b_m cannot equal 0_R. Thus, $a_nb_m \neq 0_R$ and so the degree of fg is $n + m = \deg(f) + \deg(g)$. □

COROLLARY 17.5. *If R is an integral domain, then so is $R[x]$.*

Proof. Since R is an integral domain, it is in particular a commutative ring with identity. From the definition of multiplication in $R[x]$, it follows very easily that $R[x]$ is also a commutative with identity $1_{R[x]} = 1_R$. The proof of Theorem 4.1 shows that the product of nonzero polynomials in $R[x]$ is non-zero. Therefore, $R[x]$ is an integral domain. □

THEOREM 17.6. *The Division Algorithm in $F[x]$ Let F be a field and $f, g \in F[x]$ with $g \neq 0_F$. Then there exists unique polynomials q and r in $F[x]$ such that*

$$\begin{array}{ll} (i) & f = gq + r \\ (ii) & \text{either } r = 0_F \text{ or } deg\,(r) < deg\,(g) \end{array}$$

Proof. We first prove the existence of the polynomials q and r.

Case 1: Suppose $f = 0$, then the proposition is true with q and $r = 0_R$.

Case 2: Suppose $\deg(f) < \deg(g)$. Then the proposition is true with $q = 0_F$ and $r = f$.

Case 3: If $\deg(f \geq \deg(g))$, then the proof of existence is by induction on the degree of f.

(i) If $\deg(f) = 0$, then $\deg(g) = 0$ also. Hence $f = a$ and $g = b$ for some nonzero a and b in F. Since F is a field, b is a unit and
$$a = b(b^{-1}a) \quad .$$
Thus, the theorem is true with $q = b^{-1}a$ and $r = 0_F$.

(ii) Now assume that the proposition is true whenever $\deg(f) < n$. We must show that it is true when f has degree n; say
$$f = a_n x^n + \cdots + a_1 x + a_0$$
with $a_n \neq 0_F$. The divisor g must have the form
$$g = b_m x^m + \cdots + b_1 x + b_0$$
with $b_m \neq 0_F$ and $m \leq n$. Since F is a field and $b_m \neq 0_F$, b_m is a unit. Multiply the divisor g by $a_n b_m^{-1} x^{n-m}$ to obtain
$$\begin{aligned} a_n b_m^{-1} x^{n-m} g &= a_n b_m^{-1} x^{n-m} \left(b_m x^m + \cdots + b_1 x + b_0\right) \\ &= a_n x^n + a_n b_m^{-1} b_{m-1} x^{m-1} + \cdots + a_n b_m^{-1} b_0 x^{n-m} \quad . \end{aligned}$$
Since the leading term of this polynomial is identical to that of f, the difference
$$f - a_n b_m^{-1} x^{n-m} g$$
is a polynomial of degree less than n. We now apply the induction hypothesis with g as divisor and $f - a_n b_m^{-1} x^{n-m} g$ as the dividend (or use Case 1 if $f - a_n b_m^{-1} x^{n-m} g = 0_F$). There thus exists polynomials q_1 and r such that
$$f - a_n b_m^{-1} x^{n-m} g = q_1 g + r$$
and
$$r = 0_F \quad \text{or} \quad \deg(r) < \deg(g) \quad .$$
Therefore,
$$f = \left(a_n b_m^{-1} x^{n-m} + q_1\right) g + r$$
and
$$r = 0_F \quad \text{or} \quad \deg(r) < \deg(g) \quad .$$
Hence, the proposition is true with $q = a_n b_m^{-1} x^{n-m} + q_1$ when $\deg(f) = n$. This completes the induction and shows that q and r exist for any dividend f and any divisor g.

To prove that q and r are unique, suppose that q' and r' are polynomials satisfying

$$f = q'g + r'$$

and

$$r' = 0_F \quad \text{or} \quad \deg(r') < \deg(g) \quad .$$

Then we would have

$$qg + r = f = q'g + r'$$

or

$$g(q - q') = r' - r \quad . \tag{1}$$

If $q - q' \neq 0_F$, then, by Theorem 4.1, the degree of the polynomial on the left hand side of (1) is greater than or equal to the degree of g. But since the polynomials r' and r are either zero or have degree strictly less than that of g, the right hand side of (1) must have degree strictly less than that of g. Thus, unless $q - q' = 0_F$ the degrees of the two sides of (1) can not be the same; i.e., we have a contradiction. Therefore, $q - q' = 0_F$, or equivalently, $q_1 = q$. But then the left hand side of (1) is zero; so we must have $r' - r = 0_F$ or $r' = r$. Thus, the polynomials q and r are unique. $\square$