Chapter 7

Polynomial Rings

7.1 Polynomials

A polynomial of degree n over a ring A is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

where $a_i \in A$ and $a_n \neq 0$.

(It is better not to think of $f(x)$ as a *function*, since a non-zero polynomial may take the value 0 for all $x \in A$, particularly if A is finite.)

We know how to add and multiply polynomials, so the polynomials over A form a ring.

Definition 7.1. *We denote the ring of polynomials over the ring A by $A[x]$.*

In practice we will be concerned almost entirely with polynomials over a field k. We will assume in the rest of the chapter that k denotes a field.

In this case we do not really distinguish between $f(x)$ and $cf(x)$, where $c \neq 0$. To this end we often restrict the discussion to *monic* polynomials, ie polynomials with leading coefficient 1:

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

7.2 Long division

Proposition 7.1. *Suppose k is a field, and suppose $f(x), g(x) \in k[x]$, with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in k[x]$ with $\deg(r(x)) < \deg(g(x))$ such that*

$$f(x) = q(x)g(x) + r(x).$$

Proof. We begin by listing some obvious properties of the degree of a polynomial over a field:

Lemma 7.1. *1.* $\deg(f+g) \leq \max(\deg(f), \deg(g))$*;*

2. $\deg(fg) = \deg(f)\ \deg(g)$.

The existence of $q(x)$ and $r(x)$ follows easily enough by induction on $\deg(f(x))$. To see that the result is unique, suppose

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

Then

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

The term on the left has degree $\geq \deg(g(x))$, while that on the right has degree $< \deg(g(x))$. □

7.3 Irreducibility

Definition 7.2. *The polynomial $p(x) \in k[x]$ is said to be irreducible if it cannot be factorised into polynomials of lower degree:*

$$p(x) = g(x)h(x) \implies g(x) \text{ of } h(x) \text{ is constant.}$$

In particular, any linear polynomial (ie of degree 1) is irreducible.

7.4 The Euclidean Algorithm for polynomials

Proposition 7.2. *Any two polynomials $f(x), g(x) \in k[x]$ have a* gcd *$d(x)$, ie*

$$d(x) \mid f(x),\ g(x);$$

and

$$e(x) \mid f(x),\ g(x) \implies e(x) \mid d(x).$$

Furthermore, there exist polynomials $u(x), v(x)$ such that

$$d(x) = u(x)f(x) + v(x)g(x).$$

Proof. The Euclidean Algorithm extends almost unchanged; the only difference is that $\deg(r(x))$ takes the place of $|r|$.

Thus first we divide $f(x)$ by $g(x)$:

$$f(x) = q_0(x)g(x) + r_0(x),$$

where $\deg(r_0(x)) < \deg(g(x))$.

If $r_0(x) = 0$ we are done; otherwise we divide $g(x)$ by $r_0(x)$:

$$g(x)(x) = q_1(x)r_0(x) + r_1(x),$$

where $\deg(r_1(x)) < \deg(r_0(x))$.

Since the polynomials are reducing in degree, we must reach 0 after at most $\deg(g(x))$ steps. It follows, by exactly the same argument we used with the Euclidean Algorithm in $\mathbb{Z}$, that the last non-zero remainder $r_s(x)$ is the required gcd:

$$\gcd(f(x), g(x)) = r_s(x).$$

The last part of the Proposition, the fact that $d(x)$ is a linear combination (with polynomial coefficients) of $f(x)$ and $g(x)$, follows exactly as before. □

7.5 Unique factorisation

Theorem 7.1. *A monic polynomial $f(x) \in k[x]$ can be expressed as a product of irreducible monic polynomials, and the expression is unique up to order.*

Proof. If $f(x)$ is not itself irreducible then $f(x) = g(x)h(x)$, where $g(x),\ h(x)$ are of lower degree. The result follows by induction on $\deg(f(x))$.

To prove uniqueness we establish the polynomial version of Euclid's Lemma;

Lemma 7.2. *If $p(x)$ is irreducible then*

$$p(x) \mid f(x)\ g(x) \implies p(x) \mid f(x) \text{ or } p(x) \mid g(x).$$

Proof. As with the classic Euclidean Algorithm, suppose $p(x) \nmid f(x)$. Then

$$\gcd(p(x), f(x)) = 1.$$

Hence there exist $u(x), v(x)$ such that

$$u(x)p(x) + v(x)f(x) = 1.$$

Multiplying by $g(x)$,

$$u(x)p(x)g(x) + v(x)f(x)g(x) = g(x).$$

Now $p(x)$ divides both terms on the left. Hence $p(x) \mid g(x)$, as required. □

To prove uniqueness, we argue by induction on $\deg(f(x))$. Suppose

$$f(x) = p_1(x) \cdots p_r(x) = q_1(x) \cdots q_s(x).$$

Then $p_1(x) \mid q_j(x)$, and so $p_1(x) = q_j(x)$, for some j; and the result follows on applying the inductive hypothesis to

$$f(x)/p_1(x) = p_2(x) \cdots p_r(x) = q_1(x) \cdots q_{r-1}(x)q_{r+1}(x) \cdots q_s(x).$$

□

7.6 Gauss' Lemma

Factorisation of polynomials over the rationals plays an important role in elementary number theory. The following result simplifies the issue.

Proposition 7.3. *Suppose $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ factorises in $\mathbb{Q}[x]$ if and only if it factorises in $\mathbb{Z}[x]$.*

Proof.

Lemma 7.3. *Each polynomial $f(x) \in \mathbb{Q}[x]$ can be expressed in the form*

$$f(x) = qF(x)$$

where $q \in \mathbb{Q}$, $F(x) \in \mathbb{Z}[x]$ and the coefficients of $F(x)$ are coprime; moreover, this expression is unique up to $\pm$.

Proof. It is evident that $f(x)$ can be brought to this form, by multiplying by the lcm of the coefficients and then taking out the gcd of the resulting integer coefficients.

If there were two such expressions, then multiplying across we would have

$$n_1 F_1(x) = n_2 F_2(x).$$

The gcd of the coefficients on the left is $|n_1|$, while the gcd of those on the right is $|n_2|$. Thus $n_1 = \pm n_2$, and the result follows. □

Lemma 7.4. *Suppose*

$$u(x) = v(x)w(x),$$

where $u(x), v(x), w(x) \in \mathbb{Z}[x]$. If the coefficients of $v(x)$ are coprime, and those of $w(x)$ are also coprime, then the same is true of $u(x)$.

Proof. Suppose to the contrary that the prime p divides all the coefficients of $f(x)$. Let

$$v(x) = b_r x^r + \cdots + b_0,\ w(x) = c_s x^s + \cdots + c_0,\ u(x) = a_{r+s} x^{r+s} + \cdots + a_0.$$

By hypothesis, p does not divide all the b_i, or all the c_j. Suppose

$$p \mid b_r, b_{r-1}, \ldots, b_{i+1} \text{ but } p \nmid b_i,$$

and similarly

$$p \mid c_s, c_{s-1}, \ldots, c_{j+1} \text{ but } p \nmid c_j,$$

Then

$$p \nmid a_{i+j} = b_{i+j}c_0 + b_{i+j-1}c_1 + \cdots + b_i c_j + b_{i-1}c_{j+1} + \cdots + b_0 c_{i+j},$$

for p divides every term in the sum except $b_i c_j$, which it does not divide since

$$p \mid b_i c_j \implies p \mid b_i \text{ or } p \mid c_j.$$

So p does not divide all the coefficients of $u(x)$, contrary to hypothesis. □

Writing $f(x), g(x), h(x)$ in the form of the first Lemma,

$$q_1 F(x) = (q_2 G(x))(q_3 H(x)),$$

where the coefficients of each of $F(x), G(x), H(x)$ are coprime integers. Thus

$$F(x) = (q_2 q_3 / q_1) G(x) H(x).$$

Since the coefficients of both $F(x)$ and $G(x)H(x)$ are coprime, by the second Lemma they are equal up to sign, and the result follows. □