Chapter 6

Polynomial Rings

6.1 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 6.1. *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:

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

6.2 Long division

Proposition 6.1. *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 6.1. *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 $< \deg(g(x))$. □

6.3 Irreducibility

Definition 6.2. *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.

6.4 The Euclidean Algorithm for polynomials

Proposition 6.2. *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. □

6.5 Unique factorisation

Theorem 6.1. *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 6.2. *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

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

□

6.6 Quotient fields

We have seen that if p is a prime number then $\mathbb{Z}/(p)$ is a field. The analogous result holds for irreducible polynomials.

Theorem 6.2. *Suppose $p(x) \in k[x]$ is irreducible. Then the quotient-ring $k[x]/(p(x))$ is a field.*

Proof. Suppose $f(x)$ is coprime to $p(x)$, ie represents a non-zero element of $k[x]$ mod $p(x)$. Then we can find polynomials $u(x), v(x)$ such that

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

But then

$$f(x)u(x) \equiv 1 \bmod p(x),$$

ie $fx)$ has the inverse $u(x)$ modulo $p(x)$. □

This is particularly striking if k is a prime field $\mathbb{F}_p$.

Corollary 6.1. *Suppose $f(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n. Then $K = \mathbb{F}_p[x]/(f(x))$ is a finite field with p^n elements.*

Proof. This follows from the fact that the residues modulo $f(x)$ are represented by the p^n polynomials

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \qquad (0 \le a_0, a_1, \ldots, a_{n-1} < p).$$

□

Example: Let us look at the first irreducible polynomials in $\mathbb{F}_2[x]$.

Every linear polynomial $x - c$ in $k[x]$ is irreducible, by definition. Thus there are two irreducible polynomials of degree 1 in $\mathbb{F}_2[x]$: x and $x + 1$.

If one of the four polynomials of degree 2 is not irreducible then it must be one of the 3 products of x and $x + 1$,

$$x^2, x(x+1) = x^2 + x, (x+1)^2 = x^2 + 1.$$

This leave one irredicible polynomial of degree 2: $x^2 + x + 1$.

Turning to the eight polynomials of degree 3, there are four linear products:

$$x^3,\ x^2(x+1) = x^3 + x,\ x(x+1)^2 = x^3 + x,\ (x+1)^3 = x^3 + x^2 + x + 1.$$

There are two other 'composite' polynomials:

$$x(x^2 + x + 1) = x^3 + x^2 + x + 1,\ (x+1)(x^2 + x + 1) = x^3 + 1.$$

We are left with two irreducibles:

$$x^3 + x^2 + 1,\ x^3 + x + 1.$$

Each polynomial of degree d in $F_2[x]$ can be represented by d digits. Thus the irreducible polynomials listed above can be written:

$$10,\ 11,\ 111,\ 1101,\ 1011, \dots .$$

These compare with the familar prime numbers, in binary form:

$$10,\ 11,\ 101,\ 111,\ 1001, \dots .$$

The field $\mathbb{F}_2[x]/(x^2 + x + 1)$ has 4 elements, represented by the residues $0, 1, x, x + 1$. The addition and multiplication tables for this field of order 4 are

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

In the same way, the two irreducible polynomials of degree 3 define fields of order 8. However, we shall see later that there is just one field of each prime power p^n, up to isomorphism. It follows that the two fields of order 8 must be two models of the same field.

6.7 Gauss' Lemma

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

Proposition 6.3. *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 6.3. *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 ±.

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 6.4. *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. □

6.8 Euclidean domains, PIDs and UFDs

Definition 6.3. *An integral domain A is said to be a euclidean domain if there exists a function $N : A \to \mathbb{N}$ such that $N(a) = 0 \iff a = 0$, and given $a, b \in A$ with $b \neq 0$ there exists $q, r \in A$ with*

$$a = bq + r$$

with $N(r) < N(b)$.

Definition 6.4. *An element e of a ring A is said to be a unit if $ef = 1$ for some element $f \in A$.*

Proposition 6.4. *The units in a ring A form a multiplicative group $A^\times$.*

Examples: $Z^\times = \{\pm 1\}$.
If k is a field then $k^\times = k \setminus \{0\}$.

Definition 6.5. *An ideal in an integral domain A is a non-empty subset $I \subset A$ with the properties*

1. *$a, b \in I \implies a + b \in I$,*
2. *$a \in A, b \in I \implies ab \in I$,*

Example: The whole ring A is an ideal in A, and so is the set $\{0\}$.
If $a \in A$ then $(a) = \{ax : x \in A\}$ is an ideal. An ideal of this form is said to be principal.
If $a, b \in A$ then

$$b \mid a \iff (a) \subset (b).$$

Also

$$(a) = (b) \iff b = eb,$$

where e is a unit.

Definition 6.6. *An integral domain A is said to be a* principal ideal domain *(PID) if every ideal $I \subset A$ is principal: $I = (a)$ for some $a \in A$.*

Proposition 6.5. *A euclidean domain is a principal ideal domain.*

Proof. Suppose I is an ideal in the euclidean domain A. If $I \neq (0)$ let $d \in I$ be a non-zero element with minimal $N(d)$. Suppose $a \in I$. Then $d \mid a$, for else

$$a = qd + r,$$

with $N(r) < N(d)$; and then $r \in I$ contradicts the definition of d. □

Definition 6.7. *An element p in an integral domain A is said to be* primitive *if $p \mid ab \implies p \mid a$ or $p \mid b$.*

Proposition 6.6. *A primitive element p cannot be factored; if $p = ab$ then either a or b*

Proof. Since $p \mid p = ab$, $p \mid a$ or $p \mid b$. Suppose $p \mid a$, say $a = pc$. Then $p = pcb \implies bc = 1$, so that b is a unit. □

Definition 6.8. *A* unique factorisation domain *(UFD) is an integral domain A with the property that every non-zero element $a \in A$ is expressible in the form*

$$a = ep_1p_2 \dots p_r,$$

where e is a unit and $p_1, p_2, \dots, p_r$ are primitive elements.

We allow $a = e$ with $r = 0$. Also, we note that we can omit e if $r \geq 1$ since ep is primitive if p is primitive.

Theorem 6.3. *A principal ideal domain is a unique factorisation domain:*

$$\textit{PID} \implies \textit{UFD}.$$

Proof. Suppose A is a PID; and suppose $a \in A$, $a \neq 0$. We may assume that a is not a unit, since the result holds trivially (with no primitive elements) in that case.

We must show that a cannot be factorised into an arbitrarily large number of non-units. Suppose that is false.

Then in particular $x = y_0z_0$, where y_0, z_0 are non-units. One of y_0, z_0, say y_0, can be factorised into an arbitrarily large number of non-units. In particular $y_0 = y_1z_1$, where y_1, z_1 are non-units. One of y_1, z_1, say y_1, can be factorised into an arbitrarily large number of non-units. In particular $y_1 = y_2z_2$, where y_2, z_2 are non-units.

Continuing in this way, we obtain an infinite sequence

$$y_1, y_2, y_3, \dots,$$

such that $y_{i+1} \mid y_i$ for all i. Thus

$$(y_1) \subset (y_2) \subset (y_3) \subset \cdots$$

Let

$$I = (y_1) \cup (y_2) \cup (y_3) \cup \cdots .$$

It is readily verified that I is an ideal. Since A is a PID, it follows that $I = (d)$ for some $d \in A$. Thus $d \in (y_n)$ for some n. But $y_{n+1} \in (d)$. It follows that $y_n \mid y_{n+1}$. Since $y_{n+1} \mid y_n$, it follows that $y_n = y_{n+1}e$ with e a unit. But then $y_{n+1}e = y_{n+1}z_{n+1} \implies z_{n+1} = e$, contrary to hypothesis.

Let

$$x = ep_1 \cdots p_r$$

be an expression for x with the maximal number r of primitive elements. Then p_i cannot be factored, or we would get an expression for x with $r + 1$ primitive elements; so $p_1, \dots, p_r$ are primitive elements. □