2
Integral Domains; Polynomials

2.1 Euclidean Domains

In Chapter 3 we shall start our serious study of fields. But first we need to build our toolkit, which involves polynomial rings over fields. These, as we shall see, are integral domains of a particular kind, and it helps to develop some of the abstract theory of these domains before applying the ideas to polynomials.

An integral domain D is called a **euclidean**[1] **domain** if there is a mapping δ from D into the set $\mathbb{N}^0$ of non-negative integers with the property that $\delta(0) = 0$ and, for all a in D and all b in $D \setminus \{0\}$, there exist q, r in D such that

$$a = qb + r \quad \text{and} \quad \delta(r) < \delta(b)\,. \tag{2.1}$$

From the definition it follows that $\delta^{-1}\{0\} = \{0\}$, for if $\delta(b)$ were equal to 0 it would not be possible to find r such that $\delta(r) < \delta(b)$.

The most important example is the ring $\mathbb{Z}$, where $\delta(a)$ is defined as $|a|$, and where the process, known as the **division algorithm**, is the familiar one (which we have indeed already used in Chapter 1) of dividing a by b and obtaining a **quotient** q and a **remainder** r. If b is positive, then there exists q such that

$$qb \leq a < (q+1)b\,.$$

[1] Euclid of Alexandria, c. 325–265 B.C., is best known for his systematisation of geometry, but he also made significant contributions to number theory, including the *euclidean algorithm* described in the text (applied to the positive integers).

Thus $0 \leq a - qb < b$, and so, taking r as $a - qb$, we see that $a = qb + r$ and $|r| < |b|$. If b is negative, then there exists q such that

$$(q+1)b < a \leq qb\,.$$

Thus $b < r = a - qb \leq 0$, and so again $a = qb + r$ and $|r| < |b|$. We shall come across another important example later.

An integral domain D is called a **principal ideal domain** if all of its ideals are principal.

Theorem 2.1

Every euclidean domain is a principal ideal domain.

Proof

Let D be a euclidean domain. The ideal $\{0\}$ is certainly principal. Let I be a non-zero ideal, and let b be a non-zero element of I such that

$$\delta(b) = \min\left\{\delta(x) \,:\, x \in I \setminus 0\right\}.$$

Let $a \in I$. Then there exist q, r such that $a = qb + r$ and $\delta(r) < \delta(b)$. Since $r = a - qb \in I$, we have a contradiction unless $r = 0$. Thus $a = qb$, and so $I = Db = \langle b \rangle$, a principal ideal. □

Suppose now that a, b are non-zero members of a principal ideal domain D, and let $\langle a, b\rangle = \{sa + tb \,:\, s, t \in D\}$ be the ideal generated by a and b. (See Theorem 1.4.) By our assumption that D is a principal ideal domain, there exists d in D such that $\langle a, b\rangle = \langle d\rangle$. Since $\langle a\rangle \subseteq \langle d\rangle$ and $\langle b\rangle \subseteq \langle d\rangle$, we have, from Theorem 1.5, that $d \mid a$ and $d \mid b$. Since $d \in \langle a, b\rangle$, there exist s, t in D such that $d = sa + tb$. If $d' \mid a$ and $d' \mid b$, then $d' \mid sa + tb$. That is, $d' \mid d$. We say that d is a **greatest common divisor**, or a **highest common factor**, of a and b. It is effectively unique, for, if $\langle a, b\rangle = \langle d\rangle = \langle d^*\rangle$, it follows from Theorem 1.5 (iii) that $d^* \sim d$.

To summarise, d is the greatest common divisor of a and b (write $d = \gcd(a, b)$) if it has the following properties:

(GCD1) $d \mid a$ and $d \mid b$;

(GCD2) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

If $\gcd(a, b) \sim 1$, we say that a and b are **coprime**, or **relatively prime**.

In the case of the domain $\mathbb{Z}$, where the group of units is $\{1, -1\}$, we have, for example, that $\langle 12, 18\rangle = \langle 6\rangle = \langle -6\rangle$.

Remark 2.2

A simple modification of the above argument enables us to conclude that, in a principal ideal domain D, every finite set $\{a_1, a_2, \ldots, a_n\}$ has a greatest common divisor.

In the argument leading to the existence of the greatest common divisor, we assert that "there exists d such that $\langle a, b\rangle = \langle d\rangle$," but give no indication of how this element d might be found. If the domain is euclidean, we do have an algorithm.

The Euclidean Algorithm

Suppose that a and b are non-zero elements of a euclidean domain D, and suppose, without loss of generality, that $\delta(b) \leq \delta(a)$. Then there exist $q_1, q_2, \ldots$ and $r_1, r_2, \ldots$ such that

$$\left.\begin{array}{ll} a = q_1 b + r_1\,, & \delta(r_1) < \delta(b)\,, \\ b = q_2 r_1 + r_2\,, & \delta(r_2) < \delta(r_1)\,, \\ r_1 = q_3 r_2 + r_3\,, & \delta(r_3) < \delta(r_2)\,, \\ r_2 = q_4 r_3 + r_4\,, & \delta(r_4) < \delta(r_3)\,, \\ \ldots\ldots & \end{array}\right\} \tag{2.2}$$

The process must end with some $r_k = 0$, the final equations being

$$\begin{aligned} r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1}\,, \quad \delta(r_{k-1}) < \delta(r_{k-2})\,, \\ r_{k-2} &= q_k r_{k-1}\,. \end{aligned}$$

Now, from the first equation of (2.2), we deduce that

$$\langle a, b\rangle = \langle b, r_1\rangle\,; \tag{2.3}$$

for every element $sa + tb$ in $\langle a, b\rangle$ can be rewritten as $(t + sq_1)b + sr_1 \in \langle b, r_1\rangle$, and every element $xb + yr_1$ in $\langle b, r_1\rangle$ can be rewritten as $ya + (x - yq_1)b \in \langle a, b\rangle$. Similarly, the subsequent equations give

$$\begin{aligned} \langle b, r_1\rangle = \langle r_1, r_2\rangle\,,\ \langle r_1, r_2\rangle = \langle r_2, r_3\rangle\,, \ldots\,, \\ \langle r_{k-3}, r_{k-2}\rangle = \langle r_{k-2}, r_{k-1}\rangle\,,\ \langle r_{k-2}, r_{k-1}\rangle = \langle r_{k-1}\rangle\,. \end{aligned} \tag{2.4}$$

From (2.3) and (2.4) it follows that $\langle a, b\rangle = \langle r_{k-1}\rangle$, and so r_{k-1} is the (essentially unique) greatest common divisor of a and b.

Example 2.3

Determine the greatest common divisor of 615 and 345, and express it in the form $615x + 345y$.

Solution

$$\begin{aligned} 615 &= 1 \times 345 + 270 \\ 345 &= 1 \times 270 + 75 \\ 270 &= 3 \times 75 + 45 \\ 75 &= 1 \times 45 + 30 \\ 45 &= 1 \times 30 + 15 \\ 30 &= 2 \times 15 + 0\,. \end{aligned}$$

The greatest common divisor is 15, the last non-zero remainder, and

$$\begin{aligned} 15 &= 45 - 30 = 45 - (75 - 45) = 2 \times 45 - 75 \\ &= 2 \times (270 - 3 \times 75) - 75 = 2 \times 270 - 7 \times 75 \\ &= 2 \times 270 - 7 \times (345 - 270) = 9 \times 270 - 7 \times 345 \\ &= 9 \times (615 - 345) - 7 \times 345 = 9 \times 615 - 16 \times 345\,. \end{aligned}$$

□

Two elements a and b of a principal ideal domain D are coprime if their greatest common divisor is 1. This happens if and only if there exist s and t in D such that $sa + tb = 1$. For example, 75 and 64 are coprime:

$$\begin{aligned} 75 &= 1 \times 64 + 11 \\ 64 &= 5 \times 11 + 9 \\ 11 &= 1 \times 9 + 2 \\ 9 &= 4 \times 2 + 1\,, \end{aligned}$$

and

$$\begin{aligned} 1 &= 9 - 4 \times 2 = 9 - 4(11 - 9) = 5 \times 9 - 4 \times 11 = 5(64 - 5 \times 11) - 4 \times 11 \\ &= 5 \times 64 - 29 \times 11 = 5 \times 64 - 29(75 - 64) = 34 \times 64 - 29 \times 75\,. \end{aligned}$$

EXERCISES

2.1. For the following pairs (a, b) of integers, find the greatest common divisor, and express it as $sa + tb$, where $s, t \in \mathbb{Z}$

$$\text{(i) } (1218, 846)\,; \qquad \text{(ii) } (851, 779)\,.$$

2.2. Show that a commutative ring with unity is embeddable in a field if and only if it is an integral domain.

2.3. For another example of a euclidean domain, consider the set $\Gamma = \{x + yi : x, y \in \mathbb{Z}\}$ (where $i = \sqrt{-1}$) of **gaussian**[2] **integers**.

(i) Show that Γ is an integral domain.

(ii) For each $z = x + yi$ in Γ, define $\delta(z) = |x + yi|^2 = x^2 + y^2$. Let $a, b \in \Gamma$, with $b \neq 0$. Then $ab^{-1} = u + iv$, where $u, v \in \mathbb{Q}$. There exist integers u', v' such that $|u - u'| \leq \frac{1}{2}$, $|v - v'| \leq \frac{1}{2}$. Let $q = u' + iv'$. Show that $a = qb + r$, where $r \in \Gamma$ and $\delta(r) \leq \frac{1}{2}\,\delta(b)$.

2.4. Let p be a prime number, and let

$$D_p = \left\{ \tfrac{r}{s} \in \mathbb{Q} : r, s \text{ are coprime, and } p \nmid s \right\}.$$

(i) Show that D_p is a subring of $\mathbb{Q}$.

(ii) Describe the units of D_p.

(iii) Show that D_p is a principal ideal domain.

2.2 Unique Factorisation

Let D be an integral domain with group U of units, and let $p \in D$ be such that $p \neq 0$, $p \notin U$. Then p is said to be **irreducible** if it has no proper factors. An equivalent definition in terms of ideals is available, as a result of the following theorem:

Theorem 2.4

Let p be an element of a principal ideal domain D. Then the following statements are equivalent:

(i) p is irreducible;

(ii) $\langle p \rangle$ is a maximal proper ideal of D;

(iii) $D/\langle p \rangle$ is a field.

Proof

(i) $\Rightarrow$ (ii). Suppose that p is irreducible. Then p is not a unit, and so $\langle p \rangle$ is a proper ideal of D. Suppose, for a contradiction, that there is a (principal) ideal

[2] Johann Carl Friedrich Gauss, 1777–1855.

$\langle q\rangle$ such that $\langle p\rangle \subset \langle q\rangle \subset D$. Then $p \in \langle q\rangle$, and so $p = aq$ for some non-unit a. This contradicts the supposed irreducibility of p.

(ii) $\Rightarrow$ (iii). Let $a+\langle p\rangle$ be a non-zero element of $D/\langle p\rangle$. Then $a \notin \langle p\rangle$, and so the ideal $\langle a\rangle + \langle p\rangle$ properly contains $\langle p\rangle$. We are assuming that $\langle p\rangle$ is maximal, and so it follows that $\langle a\rangle + \langle p\rangle = \{sa + tp : s, t \in D\} = D$. Hence there exist s, t in D such that $sa+tp = 1$, and from this we deduce that $(s+\langle p\rangle)(a+\langle p\rangle) = 1+\langle p\rangle$. Thus $D/\langle p\rangle$ is a field.

(iii) $\Rightarrow$ (i). If p is *not* irreducible, then there exist non-units q and r such that $p = qr$. Then $q + \langle p\rangle$ and $r + \langle p\rangle$ are both non-zero elements of $D/\langle p\rangle$, but

$$(q + \langle p\rangle)\,(r + \langle p\rangle) = p + \langle p\rangle = 0 + \langle p\rangle\,.$$

Thus $D/\langle p\rangle$ has divisors of zero, and so certainly is not a field. □

An element d of an integral domain D has a **factorisation into irreducible elements** if there exist irreducible elements $p_1, p_2, \ldots, p_k$ such that $d = p_1 p_2 \ldots p_k$. The factorisation is **essentially unique** if, for irreducible elements $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$,

$$d = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_l$$

implies that $k = l$ and, for some permutation $\sigma : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$,

$$p_i \sim q_{\sigma(i)} \quad (i = 1, 2, \ldots, k)\,.$$

An integral domain D is said to be a **factorial domain**, or to be a **unique factorisation domain**, if every non-unit $a \neq 0$ of D has an essentially unique factorisation into irreducible elements. Here again $\mathbb{Z}$, in which the (positive and negative) prime numbers are the irreducible elements, provides a familiar example: $60 = 2 \times 2 \times 3 \times 5$, and the factorisation is essentially unique, for nothing more different than (say) $(-2) \times (-5) \times 3 \times 2$ is possible.

Theorem 2.5

Every principal ideal domain is factorial.

Proof

We begin with a lemma which at first sight deals with something quite different.

Lemma 2.6

In a principal ideal domain there are no infinite ascending chains of ideals.

Proof

In any integral domain D, an ascending chain

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

of ideals has the property that $I = \bigcup_{j \geq 1} I_j$ is an ideal. To see this, first observe that, if $a, b \in I$, then there exist k, l such that $a \in I_k$, $b \in I_l$, and so $a - b \in I_{\max\{k,l\}} \subseteq I$. Also, if $a \in I$ and $s \in D$, then $a \in I_k$ for some k, and so $sa \in I_k \subseteq I$.

Now suppose that D is a principal ideal domain, and let

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots \tag{2.5}$$

be an ascending chain of (principal) ideals. From the previous paragraph, we know that the union of all the ideals in this chain must be an ideal, and, by our assumption about D, this must be a principal ideal $\langle a \rangle$. Since $a \in \bigcup_{j \geq 1} \langle a_j \rangle$, we must have that $a \in \langle a_k \rangle$ for some k. Thus $\langle a \rangle \subseteq \langle a_k \rangle$ and, since it is clear that we also have $\langle a_k \rangle \subseteq \langle a \rangle$, it follows that $\langle a \rangle = \langle a_k \rangle$. Hence

$$\langle a_k \rangle = \langle a_{k+1} \rangle = \langle a_{k+2} \rangle \cdots = \langle a \rangle ,$$

and so the infinite chain of inclusions (2.5) terminates at $\langle a_k \rangle$. □

Returning now to the proof of Theorem 2.5, we show first that any $a \neq 0$ in D can be expressed as a product of irreducible elements. Let a be a non-unit in D. Then either a is irreducible, or it has a proper divisor a_1. Similarly, either a_1 is irreducible, or a_1 has a proper divisor a_2. Continuing, we obtain a sequence $a = a_0, a_1, a_2, \ldots$ in which, for $i = 1, 2, \ldots$, a_i is a proper divisor of a_{i-1}. The sequence must terminate at some a_k, since otherwise we would have an infinite ascending sequence

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots ,$$

and Lemma 2.6 would be contradicted. Hence a has a proper irreducible divisor $a_k = z_1$, and $a = z_1 b_1$. If b_1 is irreducible, then the proof is complete. Otherwise we can repeat the argument we used for a to find a proper irreducible divisor z_2 of b_1, and $a = z_1 z_2 b_2$. We continue this process. It too must terminate, since otherwise we would have an infinite ascending sequence

$$\langle a \rangle \subset \langle b_1 \rangle \subset \langle b_2 \rangle \subset \cdots ,$$

in contradiction to Lemma 2.6. Hence some b_l must be irreducible, and so $a = z_1 z_2 \ldots z_{l-1} b_l$ is a product of irreducible elements.

To show that the product is essentially unique, we need another lemma:

Lemma 2.7

Let D be a principal ideal domain, let p be an irreducible element in D, and let $a, b \in D$. Then

$$p \mid ab \;\Rightarrow\; p \mid a \;\text{ or }\; p \mid b\,.$$

Proof

Suppose that $p \mid ab$ and $p \not\mid a$. Then the greatest common divisor of a and p must be 1, and so there exist s, t in D such that $sa + tp = 1$. Hence $sab + tpb = b$, and so, since p clearly divides $sab + tpb$, it follows that $p \mid b$. □

It is a routine matter to extend this result to products of more than two elements:

Corollary 2.8

Let D be a principal ideal domain, let p be an irreducible element in D, and let $a_1, a_2, \ldots a_m \in D$. Then

$$p \mid a_1 a_2 \ldots a_m \;\Rightarrow\; p \mid a_1 \;\text{ or }\; p \mid a_2 \;\text{ or }\; \ldots \;\text{ or }\; p \mid a_m\,.$$

To complete the proof of Theorem 2.5, suppose that

$$p_1 p_2 \ldots p_k \sim q_1 q_2 \ldots q_l\,, \tag{2.6}$$

where $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$ are irreducible. Suppose first that $k = 1$. Then $l = 1$, since $q_1 q_2 \ldots q_l$ is irreducible, and so $p_1 \sim q_1$. Suppose inductively that, for all $n \geq 2$ and all $k < n$, any statement of the form (2.6) implies that $k = l$ and that, for some permutation σ of $\{1, 2, \ldots, k\}$,

$$q_i \sim p_{\sigma(i)}\ (i = 1, 2, \ldots k)\,.$$

Let $k = n$. Since $p_1 \mid q_1 q_2 \ldots q_l$, it follows from Corollary 2.8 that $p_1 \mid q_j$ for some j in $\{1, 2, \ldots, l\}$. Since q_j is irreducible and p_1 is not a unit, we deduce that $p_1 \sim q_j$, and by cancellation we then have

$$p_2 p_3 \ldots p_n \sim q_1 \ldots q_{j-1} q_{j+1} \ldots q_l\,.$$

By the induction hypothesis, we have that $n - 1 = l - 1$ and that, for $i \in \{1, 2, \ldots, n\} \setminus \{j\}$, $q_i \sim p_{\sigma(i)}$ for some permutation σ of $\{2, 3, \ldots, n\}$. Hence, extending σ to a permutation σ of $\{1, 2, \ldots, n\}$ by defining $\sigma(1) = j$, we obtain the desired result. □

As a consequence of Theorem 2.1, we have the following immediate corollary:

Corollary 2.9

Every euclidean domain is factorial.

EXERCISES

2.5. (i) Determine the group of units of Γ, the domain of gaussian integers.

(ii) Express 5 as a product of irreducible elements of Γ.

(iii) Does
$$13 = (2+3i)(2-3i) = (3+2i)(3-2i)$$
contradict unique factorisation in Γ?

2.6. Let $R = \{a + bi\sqrt{3} : a, b \in \mathbb{Z}\}$.

(i) Show that R is a subring of $\mathbb{C}$.

(ii) Show that the map $\varphi : R \to \mathbb{Z}$ given by
$$\varphi(a + bi\sqrt{3}) = a^2 + 3b^2$$
preserves multiplication: for all u, v in R,
$$\varphi(uv) = \varphi(u)\varphi(v)\,.$$
Show also that $\varphi(u) > 3$ unless $u \in \{0, 1, -1\}$.

(iii) Show that the units of R are 1 and -1.

(iv) Show that $1 + i\sqrt{3}$ and $1 - i\sqrt{3}$ are irreducible, and deduce that R is not a unique factorisation domain.

2.3 Polynomials

Throughout this section, R is an integral domain and K is a field.

For reasons that will emerge, we begin by describing a polynomial in abstract terms. The more familiar description of a polynomial will appear shortly. A **polynomial** f with coefficients in R is a sequence $(a_0, a_1, \ldots)$, where $a_i \in R$

for all $i \geq 0$, and where only finitely many of $\{a_0, a_1, \ldots\}$ are non-zero. If the last non-zero element in the sequence is a_n, we say that f has **degree** n, and write $\partial f = n$. The entry a_n is called the **leading coefficient** of f. If $a_n = 1$ we say that the polynomial is **monic**. In the case where *all* of the coefficients are 0, it is convenient to ascribe the formal degree of $-\infty$ to the polynomial $(0, 0, 0, \ldots)$, and to make the conventions, for every n in $\mathbb{Z}$,

$$-\infty < n\,, \quad -\infty + (-\infty) = -\infty\,, \quad -\infty + n = -\infty\,. \tag{2.7}$$

Polynomials $(a, 0, 0, \ldots)$ of degree 0 or $-\infty$ are called **constant**. For others of small degree we have names as follows:

∂f	1	2	3	4	5	6
name	linear	quadratic	cubic	quartic	quintic	sextic

(Fortunately we shall have no occasion to refer to "septic" polynomials!)

Addition of polynomials is defined as follows:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)\,.$$

Multiplication is more complicated:

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots)\,,$$

where, for $k = 0, 1, 2, \ldots$,

$$c_k = \sum_{\{(i,j)\,:\,i+j=k\}} a_i b_j\,.$$

Thus

$$c_0 = a_0 b_0\,,\ c_1 = a_0 b_1 + a_1 b_0\,,\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0\,, \ldots\,.$$

With respect to these two operations, the set P of all polynomials with coefficients in R becomes a commutative ring with unity. Most of the ring axioms are easily verified, and it is clear that the zero element is $(0, 0, 0, \ldots)$, the unity element is $(1, 0, 0, \ldots)$, and the negative of $(a_0, a_1, \ldots)$ is $(-a_0, -a_1, \ldots)$. The only axiom that causes significant difficulty is the associativity of multiplication. Let $p = (a_0, a_1, \ldots)$, $q = (b_0, b_1, \ldots)$, $r = (c_0, c_1, \ldots)$ be polynomials. (Recall that, in each case, only finitely many entries are non-zero.) Then $(pq)r = (d_0, d_1, \ldots)$, where, for $m = 0, 1, 2, \ldots$

$$\begin{aligned} d_m &= \sum_{\{(k,l)\,:\,k+l=m\}} \Big(\sum_{\{(i,j)\,:\,i+j=k\}} a_i b_j \Big) c_l = \sum_{\{(i,j,l)\,:\,i+j+l=m\}} a_i b_j c_l \\ &= \sum_{\{(i,n)\,:\,i+n=m\}} a_i \Big(\sum_{\{(j,l)\,:\,j+l=n\}} b_j c_l \Big)\,, \end{aligned}$$

which is the mth entry of $p(qr)$. Thus multiplication is associative.

There is a monomorphism $\theta : R \to P$ given by

$$\theta(a) = (a, 0, 0, \ldots) \quad (a \in R)\,.$$

We may identify the constant polynomial $\theta(a) = (a, 0, 0, \ldots)$ with the element a of R.

Let X be the polynomial $(0, 1, 0, 0, \ldots)$. Then the multiplication rule gives $X^2 = (0, 0, 1, 0, \ldots)$, $X^3 = (0, 0, 0, 1, 0, \ldots)$ and, in general,

$$X^n = (x_0, x_1, \ldots)\,, \text{ where } x_m = \begin{cases} 1 & \text{if } m = n \\ 0 & \text{otherwise.} \end{cases}$$

Then a polynomial

$$(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$$

of degree n can be written as

$$\theta(a_0) + \theta(a_1)X + \theta(a_2)X^2 + \cdots + \theta(a_n)X^n\,,$$

or as

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \tag{2.8}$$

if we make the identification of $\theta(a_i)$ with a_i.

We have arrived at the common definition of a polynomial, in which X is regarded as an "indeterminate". The notation (2.8) is certainly useful, and assuredly makes the definition of multiplication seem less arbitrary. It is important, however, to note that we are talking here of *polynomial forms*, wholly determined by the coefficients a_i, and that X is not a member of R, or indeed of anything else, except of course of the ring P of polynomials. We sometimes write $f = f(X)$ and say that it is a **polynomial over R in the indeterminate X.** The ring P of all such polynomials is written $R[X]$. We refer to it simply as the **polynomial ring** of R.

We summarise some of the main facts about polynomials, some of which we already know.

Theorem 2.10

Let D be an integral domain, and let $D[X]$ be the polynomial ring of D. Then

(i) $D[X]$ is an integral domain.

(ii) if $p, q \in D[X]$, then

$$\partial(p + q) \leq \max\{\partial p, \partial q\}\,.$$

(iii) for all p, q in $D[X]$,

$$\partial(pq) = \partial p + \partial q\,.$$

(iv) The group of units of $D[X]$ coincides with the group of units of D.

Proof

(i) We have already noted that $D[X]$ is a commutative ring with unity. To show that there are no divisors of 0, suppose that p and q are non-zero polynomials with leading terms a_m, b_n respectively. The product of p and q then has leading term $a_m b_n$. Since D, by assumption, has no zero divisors, the coefficient $a_m b_n$ is non-zero, and so certainly $pq \neq 0$.

(ii) Let p and q be non-zero. Suppose that $\partial p = m$, $\partial q = n$, and suppose, without loss of generality, that $m \geq n$. If $m > n$ then it is clear that the leading term of $p + q$ is a_m, and so $\partial(p + q) = \max\{\partial p, \partial q\}$. If $m = n$ then we may have $a_m + b_m = 0$, and so all we can say is that $\partial(p + q) \leq \max\{\partial p, \partial q\}$. The conventions established in (2.7) ensure that this result holds also if one or both of p, q are equal to 0.

(iii) By the argument in (i), if p and q are non-zero, then $\partial(pq) = m + n = \partial p + \partial q$. If one or both of p and q are zero, then the result holds by the conventions established in (2.7).

(iv) Let $p, q \in D[X]$, and suppose that $pq = 1$. From Part (iii) we deduce that $\partial p = \partial q = 0$. Thus $p, q \in D$, and $pq = 1$ if and only if p and q are in the group of units of D. □

Since the ring of polynomials over the integral domain D is itself an integral domain, we can repeat the process, and form the ring of polynomials with coefficients in $D[X]$. We need to use a different letter for a new indeterminate, and the new integral domain is $(D[X])[Y]$, more usually denoted by $D[X, Y]$. It consists of polynomials in the two indeterminates X and Y with coefficients in D. This can be repeated, and we obtain the integral domain $D[X_1, X_2, \ldots, X_n]$.

The field of fractions of $D[X]$ consists of **rational forms**

$$\frac{a_0 + a_1 X + \cdots + a_m X^m}{b_0 + b_1 X + \cdots + b_n X^n}\,,$$

where the denominator is not the zero polynomial. The field is denoted by $D(X)$ (with round rather than square brackets). In a similar way one arrives at the field $D(X_1, X_2, \ldots, X_n)$ of rational forms in the n indeterminates $X_1, X_2, \ldots, X_n$, with coefficients in D.

The point already made, that a polynomial is wholly determined by its coefficients, is underlined by the following result:

Theorem 2.11

Let D, D' be integral domains, and let $\varphi : D \to D'$ be an isomorphism. Then the mapping $\hat{\varphi} : D[X] \to D'[X]$ defined by

$$\hat{\varphi}(a_0 + a_1X + \cdots + a_nX^n) = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$$

is an isomorphism.

Proof

The proof is routine. □

The isomorphism $\hat{\varphi}$ is called the **canonical extension** of φ. A further extension $\varphi^* : D(X) \to D'(X)$ is defined by

$$\varphi^*(f/g) = \hat{\varphi}(f)/\hat{\varphi}(g) \quad \big(f/g \in D(X)\big)\,. \tag{2.9}$$

We shall be especially interested in the ring $K[X]$ of polynomials over a field K. The group of units of $K[X]$ is the group of units of K, namely the group K^* of non-zero elements of the field K, and in the usual way we write $f \sim g$ if $f = ag$ for some a in K^*.

The integral domain $K[X]$ has an important property closely analogous to a property of the domain of integers:

Theorem 2.12

Let K be a field, and let f, g be elements of the polynomial ring $K[X]$, with $g \neq 0$. Then there exist unique elements q, r in $K[X]$ such that $f = qg + r$ and $\partial r < \partial g$.

Proof

If $f = 0$ the result is trivial, since $f = 0g + 0$. So suppose that $f \neq 0$. The proof is by induction on ∂f. First, suppose that $\partial f = 0$, so that $f \in K^*$. If $\partial g = 0$ also, let $q = f/g$ and $r = 0$; otherwise, let $q = 0$ and $r = f$.

Suppose now that $\partial f = n$, and suppose also that the theorem holds for all polynomials f of all degrees up to $n - 1$. If $\partial g > \partial f$, let $q = 0$ and $r = f$. So suppose now that $\partial g \leq \partial f$. Let f, g have leading terms a_nX^n, b_mX^m, respectively, where $m \leq n$. Then the polynomial

$$h = f - \left(\frac{a_n}{b_m}\, X^{n-m}\right) g$$

has degree at most $n-1$, and so we may assume that there exist q_1, r such that $h = q_1 g + r$, with $\partial r < \partial g$. It follows that $f = qg + r$, where $q = q_1 + (a_n/b_m)X^{n-m}$.

To prove uniqueness, suppose that

$$f = qg + r = q'g + r' \,, \text{ with } \partial r, \partial r' < \partial g \,.$$

Then $r - r' = (q' - q)g$, and so $\partial\big((q'-q)g\big) = \partial(r - r') < \partial g$. By Theorem 2.10, this cannot happen unless $q' - q = 0$. Hence $q = q'$, and consequently $r = r'$ also. □

Example 2.13

An actual calculation of q and r for a given pair of polynomials f and d involves a procedure reminiscent of a long division sum. Let $f = X^4 - X$ and $d = X^2 + 3X + 2$.

$$\begin{array}{r|l}
 & X^2 - 3X + 7 \\
\hline
X^2+3X+2 & X^4 \qquad\quad - X \\
 & \underline{X^4 + 3X^3 + 2X^2} \\
 & -3X^3 - 2X^2 - X \\
 & \underline{-3X^3 - 9X^2 - 6X} \\
 & 7X^2 + 5X \\
 & \underline{7X^2 + 21X + 14} \\
 & -16X - 14
\end{array}$$

Thus $X^4 - X = (X^2 - 3X + 7)(X^2 + 3X + 2) - (16X + 14)$.

Alternatively, one may equate coefficients in the equality

$$X^4 - X = (X^2 + pX + q)(X^2 + 3X + 2) + (rX + s) \,,$$

finding that $p = -3$, $q = 7$, $r = -16$, $s = -14$.

Theorem 2.14

If K is a field, then $K[X]$ is a euclidean domain.

Proof

The map ∂ does not quite have the properties of the map δ involved in the definition of a euclidean domain, but if, for all f in $K[X]$ we define $\delta(f)$ as $2^{\partial f}$, with the convention that $2^{-\infty} = 0$, we have exactly the right properties. □

As a consequence of Theorem 2.1, Corollary 2.9 and Theorem 2.4 we can summarise the important properties of $K[X]$ as follows.

Theorem 2.15

Let K be a field. Then:

(i) every pair (f, g) of non-zero polynomials in $K[X]$ has a greatest common divisor d, which can be expressed as $af + bg$, with a, b in $K[X]$;

(ii) $K[X]$ is a principal ideal domain;

(iii) $K[X]$ is a factorial domain;

(iv) if $f \in K[X]$, then $K[X]/\langle f\rangle$ is a field if and only if f is irreducible.

Example 2.16

The euclidean algorithm is valid in $K[X]$ (if K is a field) but the calculation can be tedious. Taking a very simple case, we consider the polynomials X^2+X+1 and X^3+2X-4 in $\mathbb{Q}[X]$. Then one may calculate that

$$\begin{aligned} X^3+2X-4 &= (X-1)(X^2+X+1)+2X-3\\ X^2+X+1 &= \left(\tfrac{1}{2}X+\tfrac{5}{4}\right)(2X-3)+\tfrac{19}{4}\,, \end{aligned}$$

and so the greatest common divisor is $\frac{19}{4}$. Recall, however, that the group of units of $\mathbb{Q}[X]$ is $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, and so $\frac{19}{4} \sim 1$. The two polynomials are coprime. "Unwinding" the algorithm gives

$$\begin{aligned} \tfrac{19}{4} &= (X^2+X+1) - \left(\tfrac{1}{2}X+\tfrac{5}{4}\right)(2X-3)\\ &= (X^2+X+1) - \left(\tfrac{1}{2}X+\tfrac{5}{4}\right)[(X^3+2X-4)-(X-1)(X^2+X+1)]\\ &= \left(\tfrac{1}{2}X^2+\tfrac{3}{4}X-\tfrac{1}{4}\right)(X^2+X+1) - \left(\tfrac{1}{2}X+\tfrac{5}{4}\right)(X^3+2X-4)\,. \end{aligned}$$

The **irreducible** elements in the ring $K[X]$ of polynomials over K will be a major area of interest in subsequent chapters.

Example 2.17

Since X^2+1 is irreducible in $\mathbb{R}[X]$, it follows from Theorem 2.15 that $\mathbb{R}[X]/\langle X^2+1\rangle$ is a field. Denote it by K. The elements of K are residue classes of the form $a+bX+\langle X^2+1\rangle$, where $a, b \in \mathbb{R}$. The addition is given simply by the rule

$$\big(a+bX+\langle X^2+1\rangle\big)+\big(c+dX+\langle X^2+1\rangle\big) = (a+c)+(b+d)X+\langle X^2+1\rangle\,.$$

Multiplication is a little more difficult:

$$\begin{aligned}&\big(a + bX + \langle X^2+1\rangle\big)\big(c + dX + \langle X^2+1\rangle\big)\\ &\quad = ac + (ad+bc)X + bdX^2 + \langle X^2+1\rangle\\ &\quad = (ac-bd) + (ad+bc)X + bd(X^2+1) + \langle X^2+1\rangle\\ &\quad = (ac-bd) + (ad+bc)X + \langle X^2+1\rangle\,.\end{aligned}$$

This is reminiscent of the rule for adding and multiplying complex numbers. Indeed it is more than reminiscent: the map $\varphi : \mathbb{R}[X]/\langle X^2+1\rangle \to \mathbb{C}$, given by

$$\varphi\big(a + bX + \langle X^2+1\rangle\big) = a + bi \quad (a, b \in \mathbb{R})\,,$$

is in fact an isomorphism.

We have already emphasised that polynomials, as we have defined them, are *polynomial forms*, entirely determined by their coefficients. For example, if we write $f = a_0 + a_1X + \cdots + a_nX^n = 0$, we mean that f is the zero polynomial, that is to say, $a_0 = a_1 = \cdots = a_n = 0$. Let D be an integral domain and let $\alpha \in D$. The **homomorphism** σ_α from $D[X]$ into D is defined by

$$\sigma_\alpha(a_0 + a_1X + \cdots + a_nX^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n\,. \tag{2.10}$$

The verification that this is a homomorphism is entirely routine, and is omitted. We frequently want to write $\sigma_\alpha(f)$ more simply as $f(\alpha)$.

If $f(\alpha) = 0$, then we say that α is a **root**, or a **zero**, of the polynomial f. The following result is crucial to the understanding of roots and factorisations.

Theorem 2.18 (The Remainder Theorem)

Let K be a field, let $\beta \in K$ and let f be a non-zero polynomial in $K[X]$. Then the remainder upon dividing f by $X - \beta$ is $f(\beta)$. In particular, β is a root of f if and only if $(X - \beta) \mid f$.

Proof

By the division algorithm (Theorem 2.12), there exist q, r in $K[X]$ such that

$$f = (x-\beta)q + r\,,\ \text{where } \partial r < \partial(x-\beta) = 1\,. \tag{2.11}$$

Thus r is a constant. Substituting β for X, we see that $f(\beta) = r$. In particular, $f(\beta) = 0$ if and only if $r = 0$, that is, if and only if $(X - \beta) \mid q$. □

EXERCISES

2.7. Verify the distributive law $f(g+h) = fg + fh$ for a polynomial ring.

2.8. For the following pairs (f, g) of polynomials, find polynomials q, r such that $f = qg + r\,, \quad \partial r < \partial g$.

(i) $f = X^3 + X + 1\,,\ g = X^2 + X + 1$;

(ii) $f = X^7 + 1\,,\ g = X^3 + 1$.

2.9. Show that $\mathbb{Z}[X]$ is not a principal ideal domain.

2.10. Show that, even if K is a field, $K[X, Y]$ is not a principal ideal domain.

2.11. For each of the following pairs (f, g) of polynomials, find the greatest common divisor, and express it in the form $pf + qg$, where p and q are polynomials:

(i) $f = X^5 + X^4 - 2X^3 - X^2 + X,\ \ g = X^3 + X - 2$;

(ii) $f = X^3 + 2X^2 + 7X - 1,\ \ g = X^2 + 3X + 4$.

2.12. Show that, in $\mathbb{Z}_p[X]$,

$$X(X-1)(X-2)\dots\big(X-(p-1)\big) = X^p - X\,.$$

2.13. Let K be an infinite field, and let f, g be polynomials of degree n. Suppose that there exist distinct elements $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$ in K such that $f(\alpha_i) = g(\alpha_i)$ $(i = 1, 2, \dots, n+1)$. Show that $f = g$.

2.4 Irreducible Polynomials

In Example 2.17 we saw a way of constructing the complex field from the real field. This is a very special case of a more general technique.

Theorem 2.19

Let K be a field, and let $g(X)$ be an irreducible polynomial in $K[X]$. Then $K[X]/\langle g(X)\rangle$ is a field containing K up to isomorphism.

Proof

We know from Theorem 2.15 that $K[X]/\langle g(X)\rangle$ is a field. The map $\varphi : K \to K[X]/\langle g(X)\rangle$ given by

$$\varphi(a) = a + \langle g(X)\rangle \quad (a \in K)$$

is easily seen to be a homomorphism. It is even a monomorphism, since

$$a + \langle g(X)\rangle = b + \langle g(X)\rangle \;\Rightarrow\; a - b \in \langle g(X)\rangle \;\Rightarrow\; a = b\,.$$

□

It is clear, therefore, that we will have a highly effective method of constructing new fields provided we have a way of identifying irreducible polynomials. Certainly every linear polynomial is irreducible, and if the field of coefficients is the complex field $\mathbb{C}$, that is the end of the matter, for, by the Fundamental Theorem of Algebra (see [8]) every polynomial in $\mathbb{C}[X]$ factorises, essentially uniquely, into linear factors. Linear polynomials, it must be said, are of little interest as far as Theorem 2.19 is concerned, for $K[X]/\langle g(X)\rangle$ coincides with $\varphi(K)$ in this case, and so is isomorphic to K: if $g(X) = X - a$, then, for all f in $K[X]$ we have that $f = q(X-a)+f(a)$, and so $f+\langle g\rangle = f(a)+\langle g\rangle \in \varphi(K)$.

For polynomials in $\mathbb{R}[X]$ the situation is only a little more complicated. Consider a typical polynomial

$$g(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \tag{2.12}$$

in $\mathbb{R}[X]$. If $\gamma \in \mathbb{C} \setminus \mathbb{R}$ is a root, then

$$a_n\gamma^n + a_{n-1}\gamma^{n-1} + \cdots + a_1\gamma + a_0 = 0\,.$$

Hence the complex conjugate of the left-hand side is zero also. That is, since the coefficients $a_0, a_1, \ldots, a_n$ are real,

$$a_n\bar{\gamma}^n + a_{n-1}\bar{\gamma}^{n-1} + \cdots + a_1\bar{\gamma} + a_0\,.$$

Thus the non-real roots of the polynomial occur in conjugate pairs, and we obtain a factorisation

$$g(X) = a_n(X-\beta_1)\ldots(X-\beta_r)(X-\gamma_1)(X-\bar{\gamma}_1)\ldots(X-\gamma_s)(X-\bar{\gamma}_s)\,,$$

in $\mathbb{C}[X]$, where $\beta_1, \ldots, \beta_r \in \mathbb{R}$, $\gamma_1, \ldots, \gamma_s \in \mathbb{C}\setminus\mathbb{R}$, $r, s \geq 0$ and $r + 2s = n$. This gives rise to a factorisation

$$a_n(X-\beta_1)\ldots(X-\beta_r)\big(X^2 - (\gamma_1+\bar{\gamma}_1)X + \gamma_1\bar{\gamma}_1\big)\ldots\big(X^2 - \big(\gamma_s+\bar{\gamma}_s\big)X + \gamma_s\bar{\gamma}_s\big)$$

in $\mathbb{R}[X]$. In this factorisation the quadratic factors are irreducible in $\mathbb{R}[X]$, for if they had real linear factors, they would have two distinct factorisations in $\mathbb{C}[X]$, and we know that this cannot happen.

We have proved the following result:

Theorem 2.20

The irreducible elements of the polynomial ring $\mathbb{R}[X]$ are either linear or quadratic. Every polynomial (2.12) in $\mathbb{R}[X]$ has a unique factorisation

$$a_n(X-\beta_1)\dots(X-\beta_r)(X^2+\lambda_1 X+\mu_1)\dots(X^2+\lambda_s X+\mu_s)\,,$$

in $\mathbb{R}[X]$, where $a_n \in \mathbb{R}$, $r, s \geq 0$ and $r+2s=n$.

We can of course easily determine whether a quadratic polynomial aX^2+bX+c in $\mathbb{R}[X]$ is irreducible: it is irreducible if and only if the **discriminant** $b^2-4ac<0$.

This much is relatively straightforward. Unfortunately, we shall be mostly interested in $\mathbb{Q}[X]$, and here the situation is not so easy, for, as we shall see, in $\mathbb{Q}[X]$ there are irreducible polynomials of arbitrarily large degree.

Quadratic polynomials present no great problem:

Theorem 2.21

Let $g(X)=X^2+a_1X+a_0$ be a polynomial with coefficients in $\mathbb{Q}$. Then:

(i) if $g(X)$ is irreducible over $\mathbb{R}$, then it is irreducible over $\mathbb{Q}$;

(ii) if $g(X)=(X-\beta_1)(X-\beta_2)$, with $\beta_1,\beta_2\in\mathbb{R}$, then $g(X)$ is irreducible in $\mathbb{Q}[X]$ if and only if β_1 and β_2 are irrational.

Proof

(i) Let $g(X)$ be irreducible over $\mathbb{R}$. If $g(X)=(X-q_1)(X-q_2)$ were a factorisation in $\mathbb{Q}[X]$, it would also be a factorisation in $\mathbb{R}[X]$, and we would have a contradiction.

(ii) If β_1, β_2 were rational we would have a factorisation in $\mathbb{Q}[X]$, and $g(X)$ would not be irreducible. If β_1, β_2 are irrational, then $(X-\beta_1)(X-\beta_2)$ is the *only* factorisation in $\mathbb{R}[X]$, and so a factorisation in $\mathbb{Q}[X]$ into linear factors is not possible. □

Remark 2.22

With regard to part (ii) of the theorem, it is clear that, if one or other of β_1,β_2 is irrational, then both are irrational.

Example 2.23

Examine the following polynomials for irreducibility in $\mathbb{R}[X]$ and $\mathbb{Q}[X]$:

$$X^2 + X + 1\,, \quad X^2 + X - 1\,, \quad X^2 + X - 2\,.$$

Solution

The first polynomial is irreducible over $\mathbb{R}$, since the discriminant is -3. It follows that it is irreducible over $\mathbb{Q}$.

The second polynomial factorises over $\mathbb{R}$ as $(X - \beta_1)(X - \beta_2)$, where

$$\beta_1 = \frac{-1 + \sqrt{5}}{2}\,, \quad \beta_2 = \frac{-1 - \sqrt{5}}{2}\,.$$

It is irreducible over $\mathbb{Q}$.

The third polynomial factorises over $\mathbb{Q}$ as $(X - 1)(X + 2)$ and so is not irreducible. □

To take the matter further we need some new ideas. Observe that in Example 2.23 the factorisation of $X^2 + X - 2$ over $\mathbb{Q}$ is in fact a factorisation over $\mathbb{Z}$. This prompts a question.

- Is it possible for a non-constant polynomial $p(X)$ in $\mathbb{Z}[X]$ to be irreducible over $\mathbb{Z}$ but not over $\mathbb{Q}$?

The answer is no:

Theorem 2.24 (Gauss's Lemma)

Let f be a non-constant polynomial in $\mathbb{Z}[X]$, irreducible over $\mathbb{Z}$. Then f, considered as a polynomial in $\mathbb{Q}[X]$, is irreducible over $\mathbb{Q}$.

Proof

Suppose, for a contradiction, that $f = gh$, with $g, h \in \mathbb{Q}[X]$ and $\partial g, \partial h < \partial f$. Then there exists a positive integer n such that $nf = g'h'$, where $g', h' \in \mathbb{Z}[X]$, and $\partial g' = \partial g$, $\partial h' = \partial h$. Let us suppose that n is the *smallest* positive integer with this property. Let

$$g' = a_0 + a_1 X + \cdots + a_k X^k\,, \quad h' = b_0 + b_1 X + \cdots + b_l X^l\,.$$

If $n = 1$, then $g' = g$, $h' = h$, and we have an immediate contradiction. Otherwise, let p be a prime factor of n.

Lemma 2.25

Either p divides all the coefficients of g', or p divides all the coefficients of h'.

Proof

Suppose, for a contradiction, that p does not divide all the coefficients of g', and that p does not divide all the coefficients of h'. Suppose that p divides $a_0, \ldots, a_{i-1}$, but $p \nmid a_i$, and that p divides $b_0, \ldots, b_{j-1}$, but $p \nmid b_j$. The coefficient of X^{i+j} in nf is

$$a_0 b_{i+j} + \cdots + a_i b_j + \cdots a_{i+j} b_0 \,.$$

In this sum, all the terms preceding $a_i b_j$ are divisible by p, since p divides $a_0, \ldots, a_{j-1}$; and all the terms following $a_i b_j$ are divisible by p, since p divides $b_0, \ldots, b_{j-1}$. Hence only the term $a_i b_j$ is not divisible by p, and it follows that the coefficient of X^{i+j} in nf is not divisible by p. This gives a contradiction, since the coefficients of f are integers, and so certainly all the coefficients of nf are divisible by p. □

Returning now to the proof of Theorem 2.24, we may suppose, without loss of generality, that $g' = pg''$, where $g'' \in \mathbb{Z}[X]$. It follows that $(n/p)f = g''h'$, and this contradicts the choice of n as the least positive integer with this property. Hence a factorisation over $\mathbb{Q}$ is not possible, and f is irreducible over $\mathbb{Q}$. □

We have seen that there is no difficulty in determining the irreducibility of quadratic polynomials in $\mathbb{Q}[X]$. Theorem 2.24 makes it reasonably straightforward to deal with monic cubic polynomials over $\mathbb{Z}$.

Example 2.26

Show that $g = X^3 + 2X^2 + 4X - 6$ is irreducible over $\mathbb{Q}$.

Solution

If the polynomial g factorises over $\mathbb{Q}$, then it factorises over $\mathbb{Z}$, and at least one of the factors must be linear:

$$g = X^3 + 2X^2 + 4X - 6 = (X - a)(X^2 + bX + c)\,. \tag{2.13}$$

Then $ac = 6$ and so $a \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. If we substitute a for X in g we must have $g(a) = 0$. However, the values of $g(a)$ are as follows:

a	1	-1	2	-2	3	-3	6	-6
$g(a)$	1	-9	14	-10	51	-27	306	-174

.

Hence the factorisation (2.13) is impossible, and so g is irreducible over $\mathbb{Q}$. □

This technique will not work for a polynomial of degree exceeding 3, and indeed there is no easy way to determine irreducibility over $\mathbb{Q}$. One important technique, due to Eisenstein[3], is as follows:

Theorem 2.27 (Eisenstein's Criterion)

Let

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

be a polynomial, where $a_0, a_1, \ldots, a_n$ are integers with greatest common divisor equal to 1. Suppose that there exists a prime number p such that

(i) $p \nmid a_n$,

(ii) $p \mid a_i \quad (i = 0, \ldots, n-1)$,

(iii) $p^2 \nmid a_0$.

Then f is irreducible over $\mathbb{Q}$.

Proof

By Gauss's Lemma (Theorem 2.24), it is sufficient to prove that f is irreducible over $\mathbb{Z}$. Suppose, for a contradiction, that $f = gh$, where

$$g = b_0 + b_1X + \cdots + b_rX^r\,, \quad h = c_0 + c_1X + \cdots + c_sX^s\,,$$

with $r, s < n$ and $r + s = n$. Since $a_0 = b_0c_0$, it follows from (ii) that $p \mid b_0$ or $p \mid c_0$. Since $p^2 \nmid a_0$, the coefficients b_0 and c_0 cannot both be divisible by p, and we may assume, without loss of generality, that

$$p \mid b_0\,, \quad p \nmid c_0\,. \tag{2.14}$$

Suppose inductively that p divides $b_0, b_1, \ldots, b_{k-1}$, where $1 \leq k \leq r$. Then

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0\,.$$

Since p divides each of a_k, b_0c_k, $b_1c_{k-1}, \ldots, b_{k-1}c_1$, it follows that $p \mid b_kc_0$, and hence, from (2.14), $p \mid b_k$.

We conclude that $p \mid b_r$, and so, since $a_n = b_rc_s$, we have that $p \mid a_n$, a contradiction to the assumption (i). Hence f is irreducible. □

[3] Ferdinand Gotthold Max Eisenstein, 1823–1852.

Remark 2.28

It is clear from Theorem 2.27 that there exist irreducible polynomials in $\mathbb{Q}[X]$ of arbitrarily high degree.

Example 2.29

The polynomial $X^5 + 2X^3 + \frac{8}{7}X^2 - \frac{4}{7}X + \frac{2}{7}$ is irreducible over $\mathbb{Q}$, since $7X^5 + 14X^3 + 8X^2 - 4X + 2$ satisfies Eisenstein's Criterion, with $p = 2$.

It is sometimes possible to apply the Eisenstein test after a suitable adjustment:

Example 2.30

Show that

$$f(X) = 2X^5 - 4X^4 + 8X^3 + 14X^2 + 7$$

is irreducible over $\mathbb{Q}$.

Solution

The polynomial f does not satisfy the required conditions. If, however, there exists a factorisation $f = gh$ with (say) $\partial g = 3$ and $\partial h = 2$, then

$$7X^5 + 14X^3 + 8X^2 - 4X + 2 = X^5 f(1/X) = \big(X^3 g(1/X)\big)\big(X^2 h(1/X)\big)$$

is a factorisation of $7X^5 + 14X^3 + 8X^2 - 4X + 2$, and from Example 2.29 we know that this cannot happen. □

The next example will eventually prove important:

Example 2.31

Show that, if $p > 2$ is prime, then

$$f(X) = 1 + X + X^2 + \cdots + X^{p-1}$$

is irreducible over $\mathbb{Q}$.

Solution

Observe that $f(X) = (X^p - 1)/(X - 1)$. If $g(X)$ is defined as $f(X + 1)$, it follows that

$$g(X) = \frac{1}{X}\big((X+1)^p - 1\big) = \sum_{r=0}^{p-1} \binom{p}{r} X^{p-r-1}\,.$$

As was observed in the proof of Theorem 1.17, the coefficients

$$\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$$

are all divisible by p. Hence g is irreducible, by the Eisenstein Criterion.

If $f = uv$, with $\partial u, \partial v < \partial f$ and $\partial u + \partial v = \partial f$, then

$$g(X) = u(X+1)v(X+1)\,.$$

The factors $u(X+1)$ and $v(X+1)$ are polynomials in X, of the same degrees (respectively) as u and v. We thus have a contradiction, since g is irreducible. □

Another device for determining irreducibility over $\mathbb{Z}$ (and consequently over $\mathbb{Q}$) is to map the polynomial onto $\mathbb{Z}_p[X]$ for some suitably chosen prime p. Let $g = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, and let p be a prime not dividing a_n. For each i in $\{0, 1, \ldots, n\}$, let $\overline{a}_i$ denote the residue class $a_i + \langle p\rangle$ in the field $\mathbb{Z}_p = \mathbb{Z}/\langle p\rangle$, and write the polynomial $\overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$ as $\overline{g}$. Our choice of p ensures that $\partial\overline{g} = n$. Suppose that $g = uv$, with $\partial u, \partial v < \partial f$ and $\partial u + \partial v = \partial g$. Then $\overline{g} = \overline{u}\,\overline{v}$. If we can show that $\overline{g}$ is irreducible in $\mathbb{Z}_p[X]$, then we have a contradiction, and we deduce that g is irreducible. The advantage of transferring the problem from $\mathbb{Z}[X]$ to $\mathbb{Z}_p[X]$ is that $\mathbb{Z}_p$ is finite, and the verification of irreducibility is a matter of checking a finite number of cases.

Example 2.32

Show that

$$g = 7X^4 + 10X^3 - 2X^2 + 4X - 5$$

is irreducible over $\mathbb{Q}$.

Solution

If we choose $p = 3$, then, in the notation of the paragraph preceding this example,

$$\overline{g} = X^4 + X^3 + X^2 + X + 1\,.$$

The elements of $\mathbb{Z}_3$ may be taken as $0, 1, -1$, with $1 + 1 = -1$.

We show first that $\overline{g}$ has no linear factor, for

$$\overline{g}(0) = 1\,, \quad \overline{g}(1) = -1\,, \quad \overline{g}(-1) = 1\,.$$

There remains the possibility that (in $\mathbb{Z}_3[X]$)

$$X^4 + X^3 + X^2 + X + 1 = (X^2 + aX + b)\,(X^2 + cX + d)\,.$$

Equating coefficients gives

$$\begin{aligned} a+c &= 1\,, & b+ac+d &= 1\,,\\ bd &= 1\,, & ad+bc &= 1\,. \end{aligned}$$

Hence either (i) $b = d = 1$ or (ii) $b = d = -1$. In case (i) we deduce that $ac = -1$, and so $a = \pm 1$, $c = \mp 1$. In either case $a + c = 0$, and we have a contradiction. In case (ii) we deduce that $ac = 0$. If $a = 0$ then $c = 1$, and so $1 = ad + bc = b$, a contradiction. Similarly, if $c = 0$ then $a = 1$, and then $1 = ad + bc = d$, again a contradiction.

We have shown that $\overline{g}$ is irreducible over $\mathbb{Z}_3$, and it follows that g is irreducible over $\mathbb{Q}$. □

Remark 2.33

The choice of the prime p is, of course, crucial. If, in the above example, we had used $p = 2$, we would have obtained $\overline{g} = X^4 + 1$, and in $\mathbb{Z}_2[X]$ this is far from irreducible, since $X^4 + 1 = (X + 1)^4$. It is important to realise that if our $\overline{g}$ is not irreducible then we can draw no conclusion at all.

EXERCISES

2.14. Show that $X^3 + 2X^2 - 3X + 5$ is irreducible over $\mathbb{Q}$.

2.15. Show that

$$X^3 + 3X + 12\,, \quad X^4 + 2X - 6\,, \quad X^5 + 5X^2 - 10$$

are irreducible over $\mathbb{Q}$.

2.16. By making suitable transformations, use the Eisenstein criterion to show that

$$5X^4 - 10X^3 + 10X - 3\,, \quad X^4 + 4X^3 + 3X^2 - 2X + 4$$

are irreducible.

2.17. By using the technique of Example 2.32, show that

$$4X^4 - 2X^2 + X - 5\,, \quad 3X^4 - 7X + 5$$

are irreducible.

http://www.springer.com/978-1-85233-986-9

Fields and Galois Theory
Howie, J.M.
2006, X, 226 p. 22 illus., Softcover
ISBN: 978-1-85233-986-9