CHAPTER 9

Field Extensions

9.1. Ideals in Polynomial Rings

We shall discuss field extensions in the language of quotient rings of the form $R[X]/I$, where R is a field and I is an ideal in $R[X]$. We therefore first need to understand the structure of ideals in $R[X]$, where R is a field. Then we need to find out under what conditions $R[X]/I$ is a field. Also there is the question of whether $R[X]/I$ *contains* the field R.

THEOREM 9.1. *Suppose that R is a field. Then every ideal in $R[X]$ is of the form $\langle a(X)\rangle$, where $a(X) \in R[X]$.*

PROOF. Suppose that I is an ideal in $R[X]$. If $I = \{0\}$, then clearly $I = \langle 0\rangle$. Suppose now that I is a non-zero ideal. Let $a(X) \in I$ be non-zero and of smallest degree. We shall show that $I = \langle a(X)\rangle$. Clearly $\langle a(X)\rangle \subseteq I$. Suppose now that $b(X) \in I$. Then there exist polynomials $q(X), r(X) \in R[X]$ such that $b(X) = a(X)q(X) + r(X)$, where $r(X) = 0$ or $\deg r(X) < \deg a(X)$. Clearly $r(X) \in I$. If $r(X) \neq 0$, then the requirement $\deg r(X) < \deg a(X)$ contradicts the minimality of the degree of $a(X)$. It follows that $r(X) = 0$, so that $b(X) = a(X)q(X) \in \langle a(X)\rangle$. Hence $I = \langle a(X)\rangle$. ○

EXAMPLE. Consider the ideal $\langle X^2 + 1\rangle$ in $\mathbb{R}[X]$. Note that $\mathbb{R}$ is a field. In view of Propositions 8.2 and 8.3, $\mathbb{R}[X]$ is a commutative ring with unity. Let J be an ideal in $\mathbb{R}[X]$ satisfying

$$\langle X^2 + 1\rangle \subsetneqq J \subseteq \mathbb{R}[X].$$

By Theorem 9.1, there exists a polynomial $b(X) \in \mathbb{R}[X]$ such that $J = \langle b(X)\rangle$. Since $\langle X^2 + 1\rangle \neq J$, we must have $b(X) \neq r(X^2 + 1)$ for any non-zero $r \in \mathbb{R}$. On the other hand, since $\langle X^2 + 1\rangle \subset J$, we must have $X^2+1 = b(X)q(X)$ for some polynomial $q(X) \in \mathbb{R}[X]$. Note now that X^2+1 is irreducible in $\mathbb{R}[X]$. It follows that we must have $b(X) = r$ for some non-zero $r \in \mathbb{R}$, so that $J = \langle 1\rangle = \mathbb{R}[X]$. Hence $\langle X^2+1\rangle$ is maximal in $\mathbb{R}[X]$. It now follows from Theorem 7.14 that $\mathbb{R}[X]/\langle X^2+1\rangle$ is a field.

Our example motivates the second step of our argument.

THEOREM 9.2. *Suppose that R is a field, and that the polynomial $a(X) \in R[X]$ is non-constant and irreducible in $R[X]$. Then $R[X]/\langle a(X)\rangle$ is a field.*

PROOF. Note that R is a field. In view of Propositions 8.2 and 8.3, $R[X]$ is a commutative ring with unity. Let J be an ideal in $R[X]$ satisfying

$$\langle a(X)\rangle \subsetneqq J \subseteq R[X].$$

By Theorem 9.1, there exists a polynomial $b(X) \in R[X]$ such that $J = \langle b(X)\rangle$. Since $\langle a(X)\rangle \neq J$, we must have $b(X) \neq ra(X)$ for any non-zero $r \in R$. On the other hand, since $\langle a(X)\rangle \subset J$, we must have $a(X) = b(X)q(X)$ for some polynomial $q(X) \in R[X]$. Since $a(X)$ is irreducible in $R[X]$, we must have $b(X) = r$ for some non-zero $r \in R$, so that $J = \langle 1\rangle = R[X]$. Hence $\langle a(X)\rangle$ is maximal in $R[X]$. It now follows from Theorem 7.14 that $R[X]/\langle a(X)\rangle$ is a field. ○

We shall continue with our example of the ideal $\langle X^2 + 1\rangle$ in $\mathbb{R}[X]$. However, to understand the motivation of our approach, we need the following result on evaluation homomorphisms.

PROPOSITION 9.3. *Suppose that R and S are commutative rings, and that R is a subring of S. Suppose further that $x \in S$ is fixed. Then the function $\phi_x : R[X] \to S$, defined by $a(X)\phi_x = a(x)$ for every $a(X) \in R[X]$, is a ring homomorphism.*

PROOF. Suppose that $a(X), b(X) \in R[X]$. Write $f(X) = a(X) + b(X)$. Then

$$(a(X) + b(X))\phi_x = f(x) \quad \text{and} \quad a(X)\phi_x + b(X)\phi_x = a(x) + b(x).$$

Note that $f(x) = a(x) + b(x)$ in view of Lemma 8.7. It follows that ϕ_x satisfies (RH1). Next, write $g(X) = a(X)b(X)$. Then

$$(a(X)b(X))\phi_x = g(x) \quad \text{and} \quad a(X)\phi_x b(X)\phi_x = a(x)b(x).$$

Note that $g(x) = a(x)b(x)$ in view of Lemma 8.8. It follows that ϕ_x satisfies (RH2). $\bigcirc$

EXAMPLE. We shall now show that the field $\mathbb{R}[X]/\langle X^2 + 1\rangle$ is isomorphic to

$$\mathbb{C} = \mathbb{R}(\mathrm{i}) = \{x + y\mathrm{i} : x, y \in \mathbb{R}\}.$$

Consider the function $\phi_{\mathrm{i}} : \mathbb{R}[X] \to \mathbb{C}$, defined by $a(X)\phi_{\mathrm{i}} = a(\mathrm{i})$ for every $a(X) \in \mathbb{R}[X]$. By Proposition 9.3, $\phi_{\mathrm{i}} : \mathbb{R}[X] \to \mathbb{C}$ is a ring homomorphism. In view of the Fundamental theorem of ring homomorphisms, it remains to show that $\ker \phi_{\mathrm{i}} = \langle X^2+1\rangle$ and $(\mathbb{R}[X])\phi_{\mathrm{i}} = \mathbb{C}$. To show that $(\mathbb{R}[X])\phi_{\mathrm{i}} = \mathbb{C}$, note that for every $x, y \in \mathbb{R}$, the polynomial $x + yX \in \mathbb{R}[X]$ satisfies $(x + yX)\phi_{\mathrm{i}} = x + y\mathrm{i}$. To show that $\ker \phi_{\mathrm{i}} = \langle X^2 + 1\rangle$, note first of all that if $a(X) \in \langle X^2 + 1\rangle$, then $a(X) = (X^2 + 1)q(X)$ for some $q(X) \in \mathbb{R}[X]$. It follows that $a(X)\phi_{\mathrm{i}} = (\mathrm{i}^2+1)q(\mathrm{i}) = 0$, so that $a(X) \in \ker \phi_{\mathrm{i}}$. Hence $\langle X^2+1\rangle \subseteq \ker \phi_{\mathrm{i}}$. On the other hand, we know that $\ker \phi_{\mathrm{i}}$ is an ideal in $\mathbb{R}[X]$ and that $\ker \phi_{\mathrm{i}} \neq \mathbb{R}[X]$. Since $\langle X^2 + 1\rangle$ is maximal, it follows that $\langle X^2 + 1\rangle = \ker \phi_{\mathrm{i}}$, as required. Now that $\mathbb{R}[X]/\langle X^2 + 1\rangle$ is isomorphic to a field $\mathbb{C}$ which contains the field $\mathbb{R}$ as well as a root of the polynomial $X^2 + 1$, we can say that the field $\mathbb{R}[X]/\langle X^2 + 1\rangle$ contains the field $\mathbb{R}$ as well as a root of the polynomial $X^2 + 1$. In other words, we can think of the field $\mathbb{R}[X]/\langle X^2 + 1\rangle$ as an extension of the field $\mathbb{R}$.

EXAMPLE. The polynomial $X^2 + X + 1$ is irreducible in $\mathbb{Z}_2[X]$. It follows from Theorem 9.2 that $\mathbb{Z}_2[X]/\langle X^2 + X + 1\rangle$ is a field. We can use Proposition 9.3 to show that $\mathbb{Z}_2[X]/\langle X^2 + X + 1\rangle$ is isomorphic to the field $\mathbb{Z}_2(\alpha) = \{x + y\alpha : x, y \in \mathbb{Z}_2\}$, where $\alpha^2 + \alpha + 1 = 0$. We can therefore think of the field $\mathbb{Z}_2[X]/\langle X^2 + X + 1\rangle$ as an extension of the field $\mathbb{Z}_2$.

Slightly abusing terminology, we have the following situation in general.

THEOREM 9.4. *Suppose that R is a field, and that the polynomial $a(X) \in R[X]$ is irreducible in $R[X]$ and has degree at least 2. Then the field $R[X]/\langle a(X)\rangle$ contains the field R as well as a root of the polynomial $a(X)$.*

PROOF. Write $F = R[X]/\langle a(X)\rangle$. Consider the function $\phi : R \to F$ defined for every $x \in R$ by $x\phi = x + \langle a(X)\rangle$. It is not difficult to show that $\phi : R \to F$ is a ring homomorphism with $\ker \phi = \{0\}$. It follows from Proposition 7.7 that $\phi : R \to F$ is one-to-one. Hence $R\phi$ is a field isomorphic to R. Note that $R\phi \subseteq F$. It follows that F contains R if we identify every $x \in R$ with the coset $x + \langle a(X)\rangle \in F$. Now let $\alpha = X + \langle a(X)\rangle \in F$. Suppose that

$$a(X) = a_0 + a_1X + \ldots + a_nX^n,$$

where $a_0, a_1, \ldots, a_n \in R$. Then

$$\begin{aligned} a(\alpha) &= a_0 + a_1\alpha + \ldots + a_n\alpha^n \\ &= a_0 + a_1(X + \langle a(X)\rangle) + \ldots + a_n(X + \langle a(X)\rangle)^n \\ &= a_0 + a_1(X + \langle a(X)\rangle) + \ldots + a_n(X^n + \langle a(X)\rangle) \\ &= (a_0 + a_1X + \ldots + a_nX^n) + \langle a(X)\rangle \\ &= \langle a(X)\rangle, \end{aligned}$$

the zero element of F, so that α is a root of $a(X)$. $\bigcirc$

REMARK. Note that in the proof, we have shown that F contains an isomorphic copy of R. As is common in algebra, we abuse terminology and say that F contains R.

9.2. The Structure of an Extension Field

EXAMPLE. Consider the field $\mathbb{Q}$ and the polynomial $a(X) = X^3 - 5 \in \mathbb{Q}[X]$. By Theorem 9.4, the field $F = \mathbb{Q}[X]/\langle X^3 - 5\rangle$ contains $\mathbb{Q}$ as well as a root of the polynomial $X^3 - 5$. It can be seen, by applying the Fundamental theorem of ring homomorphisms to the evaluation homomorphism $\phi_{\sqrt[3]{5}} : \mathbb{Q}[X] \to \mathbb{R}$, defined for every polynomial $q(X) \in \mathbb{Q}[X]$ by $(q(X))\phi_{\sqrt[3]{5}} = q(\sqrt[3]{5})$, that F is isomorphic to the field

$$\mathbb{Q}(\sqrt[3]{5}) = \{x + y\sqrt[3]{5} + z(\sqrt[3]{5})^2 : x, y, z \in \mathbb{Q}\}.$$

Writing $s = \sqrt[3]{5}$ and noting that $s^3 - 5 = 0$, we then have the factorization

$$X^3 - 5 = (X - s)(X^2 + sX + s^2)$$

in $F[X]$. We now investigate the roots of the polynomial $X^2 + sX + s^2$. Note that the roots

$$X = \frac{-s \pm \sqrt{s^2 - 4s^2}}{2} = \frac{-s \pm \sqrt{-3s^2}}{2}$$

do not lie in F. To see this, note that if $-3s^2 = u^2$ for some $u \in F$, then since F is isomorphic to $\mathbb{Q}(\sqrt[3]{5})$, there would be some $v \in \mathbb{Q}(\sqrt[3]{5})$ such that $v^2 = -3(\sqrt[3]{5})^2$, clearly impossible since $v^2 \geqslant 0$ for every $v \in \mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$. It follows that the polynomial $X^2 + sX + s^2$ is irreducible over F. By Theorem 9.4 again, the field

$$K = F[X]/\langle X^2 + sX + s^2\rangle$$

contains F, which contains $\mathbb{Q}$. Furthermore, K contains a root t of $X^2 + sX + s^2$. It follows that

$$X^3 - 5 = (X - s)(X - t)(X - w)$$

in K, since the remaining factor on dividing $X^2 + sX + s^2$ by $X - t$ in K must be a linear factor. Hence K contains $\mathbb{Q}$ and all the three roots of $X^3 - 5$. Finally, note that K is isomorphic to the field

$$(\mathbb{Q}(\sqrt[3]{5}))(\sqrt{3}\mathrm{i}) = \{x + y\sqrt{3}\mathrm{i} : x, y \in \mathbb{Q}(\sqrt[3]{5})\} = \mathbb{Q}(\sqrt[3]{5}, \sqrt{3}\mathrm{i}).$$

THEOREM 9.5. *Suppose that R is a field, and that the polynomial $a(X) \in R[X]$ is irreducible in $R[X]$ and has degree $n \geqslant 2$. Let $\alpha = X + \langle a(X)\rangle$, and identify every $x \in R$ with the coset $x + \langle a(X)\rangle \in R[X]/\langle a(X)\rangle$. Then the field $R[X]/\langle a(X)\rangle$ consists of all elements of the form*

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1}, \quad c_0, c_1, c_2, \ldots, c_{n-1} \in R.$$

PROOF. Write $F = R[X]/\langle a(X)\rangle$. Any element of F is of the form $b(X) + \langle a(X)\rangle$, where $b(X) \in R[X]$. We can write $b(X) = a(X)q(X) + r(X)$, where $q(X), r(X) \in Q[X]$ and either $r(X) = 0$ or $\deg r(X) < n$. Then

$$b(X) + \langle a(X)\rangle = r(X) + \langle a(X)\rangle.$$

We can write

$$r(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1},$$

where $c_0, c_1, \ldots, c_{n-1} \in R$. It follows that every element of F can be written in the form

$$c_0 + c_1X + \ldots + c_{n-1}X^{n-1} + \langle a(X)\rangle = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}$$

if we identify each $c_i \in R$ with the coset $c_i + \langle a(X)\rangle \in F$ for every $i = 0, 1, \ldots, n-1$. ◯

DEFINITION. Suppose that R is a field, and that α is given as in Theorem 9.5. We write

$$R(\alpha) = \{c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1} : c_0, c_1, c_2, \ldots, c_{n-1} \in R\}.$$

An immediate consequence of Theorem 9.5 is the following useful result.

PROPOSITION 9.6. *Suppose that R is a field with k elements, and that the polynomial $a(X) \in R[X]$ is irreducible in $R[X]$ and has degree $n \geqslant 2$. Then the field $F = R[X]/\langle a(X)\rangle$ has k^n elements.*

9.3. Characteristic of a Field

DEFINITION. Suppose that F is a field. For every $m \in \mathbb{N}$, consider the statement

$$\underbrace{a + \ldots + a}_{m} = 0 \text{ for all } a \in F.$$

(i) If the statement is false for every $m \in \mathbb{N}$, then we say that the field F has characteristic 0.
(ii) If the statement is true for some $m \in \mathbb{N}$, then let k be the smallest value of m for which the statement holds. In this case, we say that the field F has characteristic k.

EXAMPLES. (1) Consider the field $\mathbb{Q}$. Note that for every $m \in \mathbb{N}$, there exists $a \in \mathbb{Q}$ such that $ma \neq 0$. It follows that the field $\mathbb{Q}$ has characteristic 0. It can also be checked that the fields $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}(\sqrt[3]{5})$ all have characteristic 0.
(2) Recall that for every prime p, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ is a field. It is not difficult to check that $\mathbb{Z}_p$ has characteristic p.

THEOREM 9.7. *The characteristic of a field is either* 0 *or a prime.*

PROOF. Suppose that the field F is of non-zero characteristic k. Then the element 1 has order k in the additive group $(F, +)$, for if $m < k$ and 1 is of order m, then

$$\underbrace{a + \ldots + a}_{m} = (\underbrace{1 + \ldots + 1}_{m})a = 0$$

for every $a \in F$, so that F has characteristic at most m, a contradiction. Suppose now that k is not a prime. Then we can write $k = rs$ where $1 < r, s < k$, so that

$$(\underbrace{1 + \ldots + 1}_{r})(\underbrace{1 + \ldots + 1}_{s}) = \underbrace{1 + \ldots + 1}_{rs} = \underbrace{1 + \ldots + 1}_{k} = 0,$$

and so F has zero divisors. Hence k must be prime. ◯

THEOREM 9.8. *Suppose that F is a field.*
(i) *If F has characteristic* 0*, then F contains $\mathbb{Q}$.*
(ii) *If F has non-zero characteristic p, where p is prime, then F contains $\mathbb{Z}_p$.*

PROOF. Let H denote the additive subgroup of $(F, +)$ generated by 1. Define $\phi : \mathbb{Z} \to F$ by writing

$$m\phi = \begin{cases} 0, & \text{if } m = 0, \\ \underbrace{1 + \ldots + 1}_{m}, & \text{if } m \in \mathbb{N}, \\ -((-m)\phi), & \text{if } -m \in \mathbb{N}. \end{cases}$$

It is not difficult to see that $\phi : \mathbb{Z} \to F$ is a ring homomorphism with $\mathbb{Z}\phi = H$.
(i) If F has characteristic 0, then $\ker \phi = \{0\}$. By the Fundamental theorem of ring homomorphisms, $\mathbb{Z}$ is isomorphic to H. Then it is not difficult to show that

$$Q = \{xy^{-1} : x, y \in H,\ y \neq 0\}$$

is isomorphic to

$$\mathbb{Q} = \{ab^{-1} : a, b \in \mathbb{Z},\ b \neq 0\}.$$

Note now that Q is a field and $Q \subseteq F$. It follows that F contains $\mathbb{Q}$.
(ii) If F has characteristic p, then $\ker \phi = \langle p \rangle$. By the Fundamental theorem of ring homomorphisms, $\mathbb{Z}/\langle p \rangle$ is isomorphic to H. Since $\mathbb{Z}/\langle p \rangle$ and $\mathbb{Z}_p$ are isomorphic, it follows that $\mathbb{Z}_p$ is isomorphic to H. Note now that H is a subfield of F. It follows that F contains $\mathbb{Z}_p$. ◯

9.4. Finite Fields

In view of Theorem 9.8, any finite field must have characteristic p, where p is prime. Furthermore, it can be shown that the number of elements of a finite field must be of the form p^n, where p is prime and $n \in \mathbb{N}$. Our main task in this section, however, is to show that for every prime p and every $n \in \mathbb{N}$, there is a field containing precisely p^n elements.

To do this, one might have hoped to start with the field $\mathbb{Z}_p$ and use Proposition 9.6. For this approach to succeed, one must find a polynomial $a(X) \in \mathbb{Z}_p[X]$ which is irreducible in $\mathbb{Z}_p[X]$ and has degree n. However, it turns out to be rather difficult to prove the existence of such polynomials.

We therefore take an alternative approach, and shall exhibit a polynomial with p^n distinct roots and show that the collection of these roots form a field. We therefore first need some mechanism to detect repeated roots.

Definition. Suppose that F is a field, and that the polynomial

$$a(X) = \sum_{k=0}^{n} a_k X^k \in F[X].$$

Then the polynomial

$$a'(X) = \sum_{k=1}^{n} k a_k X^{k-1} \in F[X]$$

is known as the derivative of the polynomial $a(X)$.

Remark. It is not difficult to check the product rule, that if $c(X) = a(X)b(X)$ in $F[X]$, then we must have $c'(X) = a'(X)b(X) + a(X)b'(X)$.

Proposition 9.9. *Suppose that F is a field, and that $a(X) \in F[X]$. Then $a(X)$ has multiple roots if and only if $a(X)$ and $a'(X)$ have a non-constant common factor in $F[X]$.*

Proof. ($\Rightarrow$) Suppose that x is a multiple root of $a(X)$. Let $b(X) \in F[X]$ be an irreducible factor of $a(X)$ having x as a root. Then $\deg b(X) > 0$ and $b^2(X)$ is a factor of $a(X)$, so that we can write $a(X) = b^2(X)q(X)$, where $q(X) \in F[X]$. It follows that

$$a'(X) = 2b(X)b'(X)q(X) + b^2(X)q'(X) = b(X)(2b'(X)q(X) + b(X)q'(X)),$$

so that $a(X)$ and $a'(X)$ have a common factor $b(X)$. Since $\deg b(X) > 0$, this common factor is clearly non-constant.

($\Leftarrow$) Suppose now that $a(X)$ and $a'(X)$ have some non-constant common factor $b(X) \in F[X]$. Let x be a root of $b(X)$, and let K be a field which contains F as well as the root x. Then $a(X)$ and $a'(X)$ have $(X - x)$ as a common factor in $K[X]$. It follows that $a(X) = (X - x)q(X)$ for some $q(X) \in K[X]$, so that

$$a'(X) = q(X) + (X - x)q'(X).$$

Now $(X - x)$ is a factor of both $a'(X)$ and $(X - x)q'(X)$, hence also of $q(X)$. It follows that $q(X) = (X - x)r(X)$ for some $r(X) \in K[X]$, so that $a(X) = (X - x)^2 r(X)$ in $K[X]$. Clearly x is a multiple root of $a(X)$. ◯

Theorem 9.10. *For every prime p and every $n \in \mathbb{N}$, there is a field containing precisely p^n elements.*

To prove Theorem 9.10, consider the polynomial $a(X) = X^{p^n} - X \in \mathbb{Z}_p[X]$. Then

$$a'(X) = p^n X^{p^n - 1} - 1 = -1$$

in $\mathbb{Z}_p[X]$. It follows from Proposition 9.9 that $a(X)$ has no multiple roots. Let F be the set of all the p^n distinct roots of $a(X)$. Next, note that by a finite number of applications of Theorem 9.4, there exists a field K which contains $\mathbb{Z}_p$ as well as all the p^n roots of $a(X)$. We shall show in the following two lemmas that F is a subfield of K.

Lemma 9.11. *Suppose that $x, y \in R$, where R is a field of characteristic prime p. Then for every $n \in \mathbb{N}$, we have $(x - y)^{p^n} = x^{p^n} - y^{p^n}$.*

Proof. We shall prove the assertion by induction on n. For $n = 1$, note that by the Binomial theorem, which holds in every field, we have

$$(x - y)^p = x^p + (\underbrace{u + \ldots + u}_{p}) - y^p = x^p - y^p,$$

where $u \in R$. Suppose now that the assertion is true for $n = k$, so that $(x-y)^{p^k} = x^{p^k} - y^{p^k}$. Then

$$(x-y)^{p^{k+1}} = ((x-y)^{p^k})^p = (x^{p^k} - y^{p^k})^p = (x^{p^k})^p - (y^{p^k})^p = x^{p^{k+1}} - y^{p^{k+1}}.$$

The result follows from the Principle of induction. ◯

LEMMA 9.12. *F is a subfield of K.*

PROOF. We need to show that F is a subring of K, and that the multiplicative inverse of any non-zero element of F lies in F. Suppose that $x, y \in F$. Then $x^{p^n} = x$ and $y^{p^n} = y$. It follows from Lemma 9.11 that $(x-y)^{p^n} = x^{p^n} - y^{p^n} = x - y$, so that $x - y \in F$. This gives (SG). On the other hand, $(xy)^{p^n} = x^{p^n} y^{p^n} = xy$, so that $xy \in F$. This gives (SR). Finally, note that if $x \in F$ and $x \neq 0$, then $(x^{-1})^{p^n} = (x^{p^n})^{-1} = x^{-1}$, so that $x^{-1} \in F$. ◯

REMARKS. (1) It can be shown for every prime p and every $n \in \mathbb{N}$, any two fields containing precisely p^n elements are isomorphic to each other. It follows that there is essentially only one field containing precisely p^n elements. We denote this field by $\mathrm{GF}(p^n)$, and call this a Galois field.

(2) We can show that the number of elements of a finite field F must be of the form p^n, where p is prime and $n \in \mathbb{N}$. As noted in Theorem 9.8, F must be an extension of $\mathbb{Z}_p$. It is easily checked that F can be viewed as a vector space over $\mathbb{Z}_p$, where vector addition is addition in F and scalar multiplication is multiplication of an element in F by an element in $\mathbb{Z}_p$. Since F is finite, it must have a finite basis over $\mathbb{Z}_p$. Let $x_1, \ldots, x_n$ be such a basis. Then

$$F = \{c_1x_1 + \ldots + c_nx_n : c_1, \ldots, c_n \in \mathbb{Z}_p\}.$$

Clearly there are precisely p choices for each coefficient c_i. Hence F has precisely p^n elements. We have therefore completely solved the problem of the number of elements of a finite field.

EXAMPLES. (1) Consider the case $p = 2$ and $n = 3$. Then $a(X) = X^8 - X \in \mathbb{Z}_2[X]$. This can be factorized into irreducible factors in $\mathbb{Z}_2[X]$ as

$$a(X) = X^8 - X = X(X+1)(X^3+X+1)(X^3+X^2+1).$$

By Theorem 9.4, the field $F = \mathbb{Z}_2[X]/\langle X^3+X+1\rangle$ contains a root x of X^3+X+1. Then

$$X^3 + X + 1 = (X - x)(X^2 + xX + (x^2+1))$$

in $F[X]$. By Proposition 9.6 and Theorem 9.5, F has 8 elements, and these are 0, 1, x, $x+1$, x^2, x^2+1, x^2+x and x^2+x+1. By trial and error, we see that x^2 and x^2+x are the two other roots of X^3+X+1. It follows that $x+1$, x^2+1 and x^2+x+1 are the roots of X^3+X^2+1. We also conclude that F consists of the 8 distinct roots of $X^8 - X$.

(2) Consider the case $p = 3$ and $n = 2$. Then $a(X) = X^9 - X \in \mathbb{Z}_3[X]$. This can be factorized into irreducible factors in $\mathbb{Z}_3[X]$ as

$$a(X) = X^9 - X = X(X+1)(X+2)(X^2+1)(X^2+X+2)(X^2+2X+2).$$

Let x be a root of one of the three quadratic factors. Then the 9 roots are of the form $ax+b$, where $a, b \in \mathbb{Z}_3$. Also, the three fields below are isomorphic to each other:

$$\mathbb{Z}_3[X]/\langle X^2+1\rangle, \quad \mathbb{Z}_3[X]/\langle X^2+X+2\rangle, \quad \mathbb{Z}_3[X]/\langle X^2+2X+2\rangle.$$

9.5. Connection with Group Theory

Suppose that F is a finite field. Then the set F^* of all the non-zero elements of F forms a group under multiplication. We are interested in understanding the structure of this group. We start with an example.

EXAMPLE. Let F be the Galois field $\mathrm{GF}(3^2)$. Then F^* has 8 elements. By the Fundamental theorem of finite abelian groups, F^* is isomorphic to precisely one of the following:

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

If F^* is isomorphic to either of the last two direct products, then the order of every element of F^* must divide 4. It follows that all 8 elements of F^* must satisfy the polynomial equation $X^4 - 1 = 0$, so that this equation has more roots than its degree, a contradiction. It follows that F^* must be isomorphic to $\mathbb{Z}_8$.

Generalizing this, we have the following important result.

THEOREM 9.13. *Suppose that F is a finite field. Then the multiplicative group F^* of all the non-zero elements of F is cyclic.*

PROOF. We apply the Fundamental theorem of finite abelian groups to F^*. Then F^* is isomorphic to a direct product of cyclic groups of prime power order. Grouping together all the factors involving the same primes, we conclude that F^* is isomorphic to the direct product

$$G_{q_1} \times \ldots \times G_{q_s},$$

where $q_1, \ldots, q_s$ are distinct primes, and where, for every $q = q_1, \ldots, q_s$,

$$G_q = \mathbb{Z}_{q^{\alpha_1}} \times \ldots \times \mathbb{Z}_{q^{\alpha_k}},$$

where $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Write $a = \alpha_1 + \ldots + \alpha_k$ and $b = \max\{\alpha_1, \ldots, \alpha_k\}$. If $b < a$, then the order of any element in G_q divides $q^b < q^a$. It follows that every element of G_q must satisfy the polynomial equation $X^{q^b} - 1 = 0$, so that this equation has more roots than its degree, a contradiction. It follows that $b = a$ and so $G_q = \mathbb{Z}_{q^a}$. Hence F^* is isomorphic to a direct product

$$\mathbb{Z}_{q_1^{a_1}} \times \ldots \times \mathbb{Z}_{q_s^{a_s}},$$

where $q_1, \ldots, q_s$ are distinct primes and $a_1, \ldots, a_s \in \mathbb{N}$. It follows from Proposition 5.3(iii) that F^* is cyclic. $\bigcirc$

Problems for Chapter 9

1. Show that $\langle X^2+1\rangle$ is a prime ideal but not a maximal ideal in $\mathbb{Z}[X]$. What can we say about the quotient ring $\mathbb{Z}[X]/\langle X^2+1\rangle$?

2. Suppose that R is a field, and that $a(X) \in R[X]$ is reducible. Show that $R[X]/\langle a(X)\rangle$ has zero divisors.

3. Show that $\mathbb{Z}_2[X]/\langle X^2+1\rangle$ has precisely 4 elements. Is $\mathbb{Z}_2[X]/\langle X^2+1\rangle$ a field?

4. Show that $\mathbb{Z}_3[X]/\langle X^2+1\rangle$ has precisely 9 elements. Is $\mathbb{Z}_3[X]/\langle X^2+1\rangle$ a field?

5. Consider the field $\mathbb{Z}_2$ and the polynomial X^3+X+1.
   (i) Find a field which contains $\mathbb{Z}_2$ as well as a root of X^3+X+1.
   (ii) Find a field which contains $\mathbb{Z}_2$ as well as all the roots of X^3+X+1.

6. Consider the field $\mathbb{Z}_5$ and the polynomial X^2+2.
   (i) Find a field F which contains $\mathbb{Z}_5$ as well as a root of X^2+2.
   (ii) How many elements does F have? Describe the elements.
   (iii) Find an element that generates F^*.

7. Suppose that F is a field of characteristic 0. Define $\phi : \mathbb{Q} \to F$ by writing, for every $a \in \mathbb{Z}$ and $b \in \mathbb{N}$,

$$\left(\frac{a}{b}\right)\phi = \begin{cases} \dfrac{\overbrace{1+\ldots+1}^{a}}{\underbrace{1+\ldots+1}_{b}}, & \text{if } a>0, \\ 0, & \text{if } a=0, \\ -\left(\dfrac{-a}{b}\right)\phi, & \text{if } a<0. \end{cases}$$

   (i) Show that ϕ is well defined.
   (ii) Show that ϕ is a ring homomorphism.
   (iii) Show that ϕ is one-to-one.
   (iv) Show that F is an extension of $\mathbb{Q}$.

8. Consider the field $\mathbb{Z}_2$ and the polynomial $X^4+X^3+X^2+X+1$.
   (i) Show that $a(X)$ is irreducible over $\mathbb{Z}_2$.
   (ii) How many elements does the field $F = \mathbb{Z}_2[X]/\langle a(X)\rangle$ have?
   (iii) What is the order of the multiplicative group F^*?
   (iv) Let s be a root of $a(X)$. Show that s does not generate F^*.