Chapter 2

Some field theory

4 Field Extensions

Definition 4.1
Let F be a field. A subset K that is itself a field under the operations of F is called a *subfield* of F. The field F is called an *extension field* of K. If $K \neq F$, K is called a *proper* subfield of F.

Definition 4.2
A field containing no proper subfields is called a *prime field*.

For example, $\mathbb{F}_p$ is a prime field, since any subfield must contain the elements 0 and 1, and since it is closed under addition it must contain all other elements, i.e. it must be the whole field.

Definition 4.3
The intersection of all subfields of a field F is itself a field, called the *prime subfield* of F.

Remark 4.4
The prime subfield of F is a prime field, as defined above (see Exercise sheet).

Theorem 4.5
The prime subfield of a field F is isomorphic to $\mathbb{Q}$ if F has characteristic 0 and is isomorphic to $\mathbb{F}_p$ if F has characteristic p.

Proof. Denote by $P(F)$ the prime subfield of F. Let F be a field of characteristic 0; then the elements $n1_F$ ($n \in \mathbb{Z}$) are all distinct, and form a subring of F isomorphic to $\mathbb{Z}$. The set

$$Q(F) = \{m1_F/n1_F : m, n \in \mathbb{Z}, n \neq 0\}$$

is a subfield of F isomorphic to $\mathbb{Q}$. Any subfield of F must contain 1 and 0 and so must contain $Q(F)$, so $Q(F) \subseteq P(F)$. Since $Q(F)$ is itself a subfield of F, we also have $P(F) \subseteq Q(F)$, so in fact $Q(F)$ is the prime subfield of F. If F has characteristic p, a similar argument holds with the set

$$Q(F) = \{0 \cdot (1_F), 1 \cdot (1_F), 2 \cdot (1_F), \ldots, (p-1) \cdot 1_F\},$$

and this is isomorphic to $\mathbb{F}_p$. ■

Definition 4.6

- Let K be a subfield of the field F and M any subset of F. Then the field $K(M)$ is defined to be the intersection of all subfields of F containing both K and M; i.e. it is the smallest subfield of F containing both K and M. It is called the extension field obtained by *adjoining* the elements of M.

- For finite $M = \{\alpha_1, \ldots, \alpha_n\}$, we write $K(M) = K(\alpha_1, \ldots, \alpha_n)$.
- If $M = \{\alpha\}$, then $L = K(\alpha)$ is called a *simple extension* of K and α is called a *defining element* of L over K.

The following type of extension is very important in the theory of fields in general.

Definition 4.7

- Let K be a subfield of F and $\alpha \in F$. If α satisfies a nontrivial polynomial equation with coefficients in K, i.e. if

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha_1 + a_0 = 0$$

  for some $a_i \in K$ not all zero, then α is *algebraic over* K.
- An extension L of K is called *algebraic over* K (or an *algebraic extension of* K) if every element in L is algebraic over K.

Example 4.8

- The element $\sqrt[3]{3} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$, since it is a root of the polynomial $x^3 - 3 \in \mathbb{Q}[x]$.
- The element $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$, since it is a root of $x^2 + 1 \in \mathbb{R}[x]$.
- The element $\pi \in \mathbb{R}$ is not algebraic over $\mathbb{Q}$. An element which is not algebraic over a field F is said to be *transcendental* over F.

Given $\alpha \in F$ which is algebraic over some subfield K of F, it can be checked (exercise!) that the set $J = \{f \in K[x] : f(\alpha) = 0\}$ is an ideal of $F[x]$ and $J \neq (0)$. By Theorem 3.4, it follows that there exists a uniquely determined monic polynomial $g \in K[x]$ which generates J, i.e. $J = (g)$.

Definition 4.9

If α is algebraic over K, then the uniquely determined monic polynomial $g \in K[x]$ generating the ideal $J = \{f \in K[x] : f(\alpha) = 0\}$ of $K[x]$ is called the *minimal polynomial* of α over K. We refer to the degree of g as the *degree of α over K*.

The key properties of the minimal polynomial are summarised in the next theorem. The third property is the one most useful in practice.

Theorem 4.10

Let $\alpha \in F$ be algebraic over a subfield K of F, and let g be the minimal polynomial of α. Then

(i) g is irreducible in $K[x]$;

(ii) For $f \in K[x]$, we have $f(\alpha) = 0$ if and only if g divides f;

(iii) g is the monic polynomial of least degree having α as a root.

Proof. (i) Since g has the root α, it has positive degree. Suppose $g = h_1h_2$ in $K[x]$ with $1 \leq \deg(h_i) < \deg(g)$ $(i = 1, 2)$. This implies $0 = g(\alpha) = h_1(\alpha)h_2(\alpha)$, and so one of h_1 or h_2 must lie in J and hence is divisible by g, a contradiction.
(ii) Immediate from the definition of g.
(iii) Any monic polynomial in $K[x]$ having α as a root must be a multiple of g by (ii), and so is either equal to g or has larger degree than g. ■

Example 4.11

- The element $\sqrt[3]{3} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^3 - 3 \in \mathbb{Q}[x]$. Since $x^3 - 3$ is irreducible over $\mathbb{Q}$, it is the minimal polynomial of $\sqrt[3]{3}$ over $\mathbb{Q}$, and hence $\sqrt[3]{3}$ has degree 3 over $\mathbb{Q}$.

- The element $i = \sqrt{-1} \in \mathbb{C}$ is algebraic over the subfield $\mathbb{R}$ of $\mathbb{C}$, since it is a root of the polynomial $x^2 + 1 \in \mathbb{R}[x]$. Since $x^2 + 1$ is irreducible over $\mathbb{R}$, it is the minimal polynomial of i over $\mathbb{R}$, and hence i has degree 2 over $\mathbb{R}$.

5 Field extensions as vector spaces

Let L be an extension field of K. An important observation is that L may be viewed as a vector space over K. The elements of L are the "vectors" and the elements of K are the "scalars".

We briefly recall the main properties of a vector space.

Definition 5.1
A *vector space* V over F is a non-empty set of objects (called vectors) upon which two operations are defined

- addition: there is some rule which produces, from any two objects in V, another object in V (denote this operation by $+$)
- scalar multiplication: there is some rule which produces, from an element of F (a scalar) and an object in V, another object in V

and these objects and operations obey the Vector Space Axioms:

1. $x + y = y + x$ for all $x, y \in V$
2. $(x + y) + z = x + (y + z)$ for all $x, y, z \in V$
3. there exists an object $0 \in V$ such that $x + 0 = x$ for all $x \in V$
4. for every $x \in V$ there exists an object $-x$ such that $x + (-x) = 0$
5. $\lambda(x + y) = \lambda x + \lambda y$ for all $x, y \in V$ and all scalars $\lambda \in F$
6. $(\lambda + \mu)x = \lambda x + \mu x$ for all $x \in V$ and all scalars $\lambda, \mu \in F$
7. $(\lambda\mu)x = \lambda(\mu x)$ for all $x \in V$ and all scalars $\lambda, \mu \in F$
8. $1x = x$ for all $x \in V$

Definition 5.2

- A basis of a vector space V over F is defined as a subset $\{v_1, \ldots, v_n\}$ of vectors in V that are linearly independent and span V. If $v_1, \ldots, v_n$ is a list of vectors in V, then these vectors form a basis if and only if every $v \in V$ can be *uniquely* written as

$$v = a_1 v_1 + \cdots + a_n v_n$$

  where $a_1, \ldots, a_n$ are elements of the base field F.

- A vector space will have many different bases, but there are always the same number of basis vectors in each. The number of basis vectors in any basis is called the *dimension* of V over F.
- Suppose V has dimension n over F. Then any sequence of more than n vectors in V is linearly dependent.

To see that the vector space axioms hold for a field L over a subfield K, note that the elements of L form an abelian group under addition, and that any "vector" $\alpha \in L$ may be multiplied by an $r \in K$ (a "scalar") to get $r\alpha \in L$ (this is just multiplication in L). Finally, the laws for multiplication by scalars hold since, for $r, s \in L$ and $\alpha, \beta \in K$ we have $r(\alpha + \beta) = r\alpha + r\beta$, $(r + s)\alpha = r\alpha + s\alpha$, $(rs)\alpha = r(s\alpha)$ and $1\alpha = \alpha$.

Example 5.3
Take $L = \mathbb{C}$ and let K be its subfield $\mathbb{R}$. Then we can easily check that $\mathbb{C}$ is a vector space over $\mathbb{R}$. Since we know from school that $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$, it is clear that a basis is given by $\{1, i\}$.

Definition 5.4
Let L be an extension field of K. If L is finite-dimensional as a vector space over K, then L is said to be a *finite extension* of K. The dimension of the vector space L over K is called the *degree* of L over K and written $[L : K]$.

Example 5.5
From above, $\mathbb{C}$ is a finite extension of $\mathbb{R}$ of degree 2.

Theorem 5.6
If L is a finite extension of K and M is a finite extension of L, then M is a finite extension of K with

$$[M : K] = [M : L][L : K].$$

Proof. Let $[M : L] = m$, $[L : K] = n$; let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis of M over L and let $\{\beta_1, \ldots, \beta_n\}$ be a basis of L over K. We shall use them to form a basis of M over K of appropriate cardinality.

Every $\alpha \in M$ can be expressed as a linear combination $\alpha = \gamma_1\alpha_1 + \cdots + \gamma_m\alpha_m$ for some $\gamma_1, \ldots, \gamma_m \in L$. Writing each γ_i as a linear combination of the β_j's we get

$$\alpha = \sum_{i=1}^{m} \gamma_i\alpha_i = \sum_{i=1}^{m}(\sum_{j=1}^{n} r_{ij}\beta_j)\alpha_i = \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\beta_j\alpha_i$$

with coefficients $r_{ij} \in K$. We claim that the mn elements $\beta_j\alpha_i$ form a basis of M over K. Clearly they span M; it suffices to show that they are linearly independent over K.

Suppose we have

$$\sum_{i=1}^{m}\sum_{j=1}^{n} s_{ij}\beta_j\alpha_i = 0$$

where the coefficients $s_{ij} \in K$. Then

$$\sum_{i=1}^{m}(\sum_{j=1}^{n} s_{ij}\beta_j)\alpha_i = 0,$$

and since the α_i are linearly independent over L we must have

$$\sum_{j=1}^{n} s_{ij}\beta_j = 0$$

for $1 \leq i \leq m$. Now, since the β_j are linearly independent over K, it follows that all the s_{ij} are 0, as required. ■

Theorem 5.7
Every finite extension of K is algebraic over K.

Proof. Let L be a finite extension of K and let $[L : K] = m$. For $\alpha \in L$, the $m+1$ elements $1, \alpha, \ldots, \alpha^m$ must be linearly dependent over K, i.e. must satisfy $a_0 + a_1\alpha + \cdots a_m\alpha^m = 0$ for some $a_i \in K$ (not all zero). Thus α is algebraic over K. ■

Remark 5.8
The converse of Theorem 5.7 is not true, however. See the Exercise sheet for an example of an algebraic extension of $\mathbb{Q}$ which is not a finite extension.

We now relate our new vector space viewpoint to the residue class rings considered previously.

Theorem 5.9
Let F be an extension field of K and $\alpha \in F$ be algebraic of degree n over K and let g be the minimal polynomial of α over K. Then

(i) $K(\alpha)$ is isomorphic to $K[x]/(g)$;

(ii) $[K(\alpha) : K] = n$ and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of $K(\alpha)$ over K;

(iii) Every $\beta \in K(\alpha)$ is algebraic over K and its degree over K is a divisor of n.

Proof. (i) Consider the "evaluation at α" mapping $\tau : K[x] \to K(\alpha)$, defined by

$$\tau(f) = f(\alpha) \text{ for } f \in K[x];$$

it is easily shown that this is a homomorphism. Then

$$\ker\tau = \{f \in K[x] : f(\alpha) = 0\} = (g)$$

by the definition of the minimal polynomial. Let S be the image of τ, i.e. the set of polynomial expressions in α with coefficients in K. By the First Isomorphism Theorem for rings we have $S \cong K[x]/(g)$. Since g is irreducible, by Theorem 3.8, $K[x]/(g)$ is a field and so S is a field. Since $K \subseteq S \subseteq K(\alpha)$ and $\alpha \in S$, we have $S = K(\alpha)$ by the definition of $K(\alpha)$, and (i) follows.
(ii) Spanning set: Since $S = K(\alpha)$, any $\beta \in K(\alpha)$ can be written in the form $\beta = f(\alpha)$ for some polynomial $f \in K[x]$. By the division algorithm, $f = qg + r$ for some $q, r \in K[x]$ and $\deg(r) < \deg(g) = n$. Then

$$\beta = f(\alpha) = q(\alpha)g(\alpha) + r(\alpha) = r(\alpha),$$

and so β is a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ with coefficients in K.
L.I.: if $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$ for some $a_0, \ldots, a_{n-1} \in K$, then the polynomial $h = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in K[x]$ has α as a root, and is thus a multiple of its minimal polynomial g. Since $\deg(h) < n = \deg(g)$, this is possible only if $h = 0$, i.e. $a_0 = \cdots = a_{n-1} = 0$. Thus the elements $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over K.
(iii) $K(\alpha)$ is a finite extension of K by (ii), and so $\beta \in K(\alpha)$ is algebraic over K by Theorem 5.7. Moreover, $K(\beta)$ is a subfield of $K(\alpha)$. If d is the degree of β over K, then $n = [K(\alpha) : K] = [K(\alpha) : K(\beta)][K(\beta) : K] = [K(\alpha) : K(\beta)]d$, i.e. d divides n. ■

Remark 5.10
This theorem tells us that the elements of the simple extension $K(\alpha)$ of K are polynomial expressions in α, and any $\beta \in K(\alpha)$ can be uniquely expressed in the form $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ for some $a_i \in K$.

Example 5.11
Consider the simple extension $\mathbb{R}(i)$ of $\mathbb{R}$. We saw earlier that i has minimal polynomial $x^2 + 1$ over $\mathbb{R}$.

So $\mathbb{R}(i) \cong \mathbb{R}[x]/(x^2 + 1)$, and $\{1, i\}$ is a basis for $\mathbb{R}(i)$ over $\mathbb{R}$. So

$$\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}.$$

Example 5.12
Consider the simple extension $\mathbb{Q}(\sqrt[3]{3})$ of $\mathbb{Q}$. We saw earlier that $\sqrt[3]{3}$ has minimal polynomial $x^3 - 3$ over $\mathbb{Q}$.

So $\mathbb{Q}(\sqrt[3]{3}) \cong \mathbb{Q}[x]/(x^3 - 3)$, and $\{1, \sqrt[3]{3}, (\sqrt[3]{3})^2\}$ is a basis for $\mathbb{Q}(\sqrt[3]{3})$ over $\mathbb{Q}$. So

$$\mathbb{Q}(\sqrt[3]{3}) = \{a + b\sqrt[3]{3} + c(\sqrt[3]{3})^2 : a, b, c \in \mathbb{Q}\}.$$

Note that we have been assuming that both K and α are embedded in some larger field F. Next, we will consider constructing a simple algebraic extension without reference to a previously given larger field, i.e. "from the ground up".

The next result, due to Kronecker, is one of the most fundamental results in the theory of fields: it says that, given any non-constant polynomial over any field, there exists an extension field in which the polynomial has a root.

Theorem 5.13 (Kronecker)
Let $f \in K[x]$ be irreducible over the field K. Then there exists a simple algebraic extension of K with a root of f as a defining element.

Proof.

- Consider the residue class ring $L = K[x]/(f)$, which is a field since f is irreducible. Its elements are the residue classes $[h] = h + (f)$, with $h \in K[x]$.

- For any $a \in K$, think of a as a constant polynomial in $K[x]$ and form the residue class $[a]$. The mapping $a \mapsto [a]$ gives an isomorphism from K onto a subfield K' of L (exercise: check!), so K' may be identified with K. Thus we can view L as an extension of K.

- For every $h = a_0 + a_1x + \cdots + a_mx^m \in K[x]$, we have

$$\begin{aligned} [h] &= [a_0 + a_1x + \cdots + a_mx^m] \\ &= [a_0] + [a_1][x] + \cdots + [a_m][x]^m \\ &= a_0 + a_1[x] + \cdots + a_m[x]^m \end{aligned}$$

  (making the identification $[a_i] = a_i$). So, every element of L can be written as a polynomial in $[x]$ with coefficients in K. Since any field containing K and $[x]$ must contain these expressions, L is a simple extension of K obtained by adjoining $[x]$.

- If $f = b_0 + b_1x + \cdots + b_nx^n$, then

$$f([x]) = b_0 + b_1[x] + \cdots + b_n[x]^n = [f] = [0],$$

  i.e. $[x]$ is a root of f and L is a simple algebraic extension of K.

■

Example 5.14
Consider the prime field $\mathbb{F}_3$ and the polynomial $x^2 + x + 2 \in \mathbb{F}_3[x]$, irreducible over $\mathbb{F}_3$. Take θ to be a "root" of f, in the sense that θ is the residue class $[x] = x + (f) \in L = \mathbb{F}_3[x]/(f)$. Explicitly, we have:

$$\begin{aligned} f(\theta) = f([x]) &= f(x + (f)) \\ &= (x + (f))^2 + (x + (f)) + (2 + (f)) \\ &= x^2 + x + 2 + (f) \\ &= f + (f) \\ &= 0 + (f) \\ &= [0]. \end{aligned}$$

The other root of f in L is $2\theta+2$, since $f(2\theta+2) = \theta^2+\theta+2 = 0$. By Theorem 5.9, the simple algebraic extension $L = \mathbb{F}_3(\theta)$ consists of the nine elements $0, 1, 2, \theta, \theta+1, \theta+2, 2\theta, 2\theta+1, 2\theta+2$.

Example 5.15
Consider the polynomial $f = x^2+x+1 \in \mathbb{F}_2[x]$, irreducible over $\mathbb{F}_2$. Let θ be the root $[x] = x+(f)$ of f; then the simple algebraic extension $L = \mathbb{F}_2(\theta)$ consists of the four elements $0, 1, \theta, \theta+1$. (The other root is $\theta + 1$). The tables for addition and multiplication are precisely those of Example 3.9, now appropriately relabelled. We give the addition table:

$+$	0	1	θ	$\theta+1$
0	0	1	θ	$\theta+1$
1	1	0	$\theta+1$	θ
θ	θ	$\theta+1$	0	1
$\theta+1$	$\theta+1$	θ	1	0

.

Note that, in the above examples, adjoining either of two roots of f would yield the same extension field.

Theorem 5.16
Let F be an extension field of the field K and $\alpha, \beta \in F$ be two roots of a polynomial $f \in K[x]$ that is irreducible over K. Then $K(\alpha)$ and $K(\beta)$ are isomorphic under an isomorphism mapping α to β and keeping the elements of K fixed.

Proof. By Theorem 5.9 both are isomorphic to the field $K[x]/(f)$ since the irreducible f is the minimal polynomial of both α and β. ■

Given a polynomial, we now want an extension field which contains all its roots.

Definition 5.17
Let $f \in K[x]$ be a polynomial of positive degree and F an extension field of K. Then we say that f *splits in* F if f can be written as a product of linear factors in $F[x]$, i.e. if there exist elements $\alpha_1, \ldots, \alpha_n \in F$ such that

$$f = a(x - \alpha_1) \cdots (x - \alpha_n)$$

where a is the leading coefficient of f. The field F is called a *splitting field* of f over K if it splits in F and if $F = K(\alpha_1, \ldots, \alpha_n)$.

So, a splitting field F of a polynomial f over K is an extension field containing all the roots of f, and is “smallest possible” in the sense that no subfield of F contains all roots of f. The following result answers the questions: can we always find a splitting field, and how many are there?

Theorem 5.18 (Existence and uniqueness of splitting field)

(i) If K is a field and f any polynomial of positive degree in $K[x]$, then there exists a splitting field of f over K.

(ii) Any two splitting fields of f over K are isomorphic under an isomorphism which keeps the elements of K fixed and maps roots of f into each other.

So, we may therefore talk of *the* splitting field of f over K. It is obtained by adjoining to K finitely many elements algebraic over K, and so we can show (exercise!) that it is a finite extension of K.

Example 5.19
Find the splitting field of the polynomial $f = x^2 + 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

The polynomial f splits in $\mathbb{C}$, where it factors as $(x - i\sqrt{2})(x + i\sqrt{2})$. However, $\mathbb{C}$ itself is not the splitting field for f. It turns out to be sufficient to adjoin just one of the complex roots of f to $\mathbb{Q}$. The field $K = \mathbb{Q}(i\sqrt{2})$ contains both of the roots of f, and no smaller subfield has this property, so K is the splitting field for F.

Splitting fields will be central to our characterization of finite fields, in the next chapter.