Chapter 12
Vector Spaces and Field Extensions

We begin this chapter with some basic facts about vector spaces. These will be familiar (at least in the case of real vector spaces) to those readers who have studied linear algebra. We then focus our attention on the particular case of a field extension. A number of properties of field extensions are discussed.

Let F be a field and $f(x) \in F[x]$ a nonconstant polynomial. We demonstrate how to create a field extension in which $f(x)$ splits into a product of polynomials of degree 1. This leads to a classification of all finite fields.

12.1 Vector Spaces

We begin with the definition of a vector space. In most linear algebra courses, vector spaces are defined over $\mathbb{R}$ or, occasionally, $\mathbb{C}$. But we can do the same thing over any field.

If F is a field and V is a set, then a **scalar multiplication** on V is a function from $F \times V$ to V. If $a \in F$, $v \in V$, then we write av for the image of (a, v) under such a function.

Definition 12.1. Let F be a field. Then a **vector space** over F is a set V having an addition operation and a scalar multiplication such that

1. V is an abelian group under addition;
2. $av \in V$ for all $a \in F$ and all $v \in V$;
3. $(a + b)v = av + bv$ for all $a, b \in F$ and all $v \in V$;
4. $a(u + v) = au + av$ for all $a \in F$ and all $u, v \in V$;
5. $a(bv) = (ab)v$ for all $a, b \in F$ and all $v \in V$; and
6. $1v = v$ for all $v \in V$.

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1_12

Of course, condition (2) is redundant, given the definition of a scalar multiplication, but we include it, because it must be checked.

Certainly the most familiar vector space over $\mathbb{R}$ is $\mathbb{R}^n$. We can generalize this.

Example 12.1. Let F be a field. For any positive integer n, let $F^n = \underbrace{F \oplus F \oplus \cdots \oplus F}_{n \text{ times}}$. Then F^n is a vector over F with the usual addition operation and scalar multiplication $a(b_1, \ldots, b_n) = (ab_1, \ldots, ab_n)$, for any $a, b_1, \ldots, b_n \in F$.

Example 12.2. Let F be any field. Then $F[x]$ is a vector space over F with the usual polynomial addition and $a(b_0 + b_1x + \cdots + b_nx^n) = ab_0 + ab_1x + \cdots + ab_nx^n$, for any $a, b_0, \ldots, b_n \in F$.

Example 12.3. Let m and n be any positive integers, and let V be the set of $m \times n$ matrices with entries in a field F. Then V is a vector space over F using matrix addition and scalar multiplication.

The least exciting example of a vector space is the following.

Example 12.4. Let F be any field and V the trivial additive group, $\{0\}$. Then V is a vector space using the only available addition and scalar multiplication options, $0 + 0 = 0$ and $a0 = 0$, for all $a \in F$.

The most important example for our purposes is the following.

Definition 12.2. If F and K are fields, with F a subfield of K, then we say that K is an **extension field** of F.

Example 12.5. Any extension field K of F is a vector space over F, using the addition operation in K and multiplication in K as the scalar multiplication. (All the properties are immediate, except that $1v = v$ for all $v \in K$. To be sure of that, we must know that the identity of F is the identity of K. But this follows from Theorem 8.12.) For example, $\mathbb{R}$ and $\mathbb{C}$ are vector spaces over $\mathbb{Q}$.

Let us mention a few basic properties of vector spaces.

Theorem 12.1. *Let V be a vector space over F. Then*

1. $a0 = 0$ *for all* $a \in F$;
2. $0v = 0$ *for all* $v \in V$; *and*
3. $(-1)v = -v$ *for all* $v \in V$.

Proof. (1) Note that $a0 = a(0 + 0) = a0 + a0$. Adding $-(a0)$ to both sides, we see that $a0 = 0$.

(2) We have $0v = (0 + 0)v = 0v + 0v$. Adding $-0v$ to both sides, we obtain the desired conclusion.

(3) Observe that $v + (-1)v = 1v + (-1)v = (1 - 1)v = 0v = 0$. Thus, $(-1)v = -v$. □

We do have to be a bit careful about which 0 we are using. For example, when we write $0v = 0$ in the theorem above, the first 0 is in F and the second is in V.

Definition 12.3. Let V be a vector space over a field F. Then a subset W of V is said to be a **subspace** of V if it is a vector space over F using the same addition and scalar multiplication.

Example 12.6. If F is a subfield of K, and K is a subfield of L, then L is a vector space over F having K and F as subspaces.

Example 12.7. Regarding $\mathbb{R}[x]$ as a vector space over $\mathbb{Q}$, we note that $\mathbb{Q}[x]$ is a subspace.

There is a simple test for a subspace.

Theorem 12.2. *Let F be a field and V a vector space over F. Then a subset W of V is a subspace if and only if*

1. $0 \in W$;
2. $w_1 + w_2 \in W$ *for all* $w_1, w_2 \in W$ *(closure under addition); and*
3. $aw \in W$ *for all* $a \in F$ *and* $w \in W$ *(closure under scalar multiplication).*

Proof. If W is a subspace then, in particular, it is an additive subgroup, so (1) and (2) hold. Part (3) is one of the conditions for a vector space. Conversely, suppose that (1), (2) and (3) hold. Noting that (3) tells us that $-w = (-1)w \in W$, for all $w \in W$, we see from Theorem 3.10 that W is an additive subgroup of V. We are given closure under scalar multiplication. The remaining vector space properties hold in V, and therefore in any subset of V. □

Note that in the preceding theorem, condition (1) could be replaced with the condition that W is not the empty set, for if $w \in W$, then $-w \in W$, and therefore $0 = w + (-w) \in W$.

Example 12.8. Let $V = \mathbb{R}^4$, which is a vector space over $\mathbb{R}$. We claim that $W = \{(a, b, 2a - b + 3c, c) : a, b, c \in \mathbb{R}\}$ is a subspace of V. Letting $a = b = c = 0$, we see that $(0, 0, 0, 0) \in W$. To check closure under addition, take $a_i, b_i, c_i \in \mathbb{R}$. Then

$$\begin{aligned}&(a_1, b_1, 2a_1 - b_1 + 3c_1, c_1) + (a_2, b_2, 2a_2 - b_2 + 3c_2, c_2)\\ &= (a_1 + a_2, b_1 + b_2, 2(a_1 + a_2) - (b_1 + b_2) + 3(c_1 + c_2), c_1 + c_2) \in W.\end{aligned}$$

Similarly, if $a \in \mathbb{R}$, then

$$a(a_1, b_1, 2a_1 - b_1 + 3c_1, c_1) = (aa_1, ab_1, 2aa_1 - ab_1 + 3ac_1, ac_1) \in W.$$

Thus, we have closure under scalar multiplication, and the claim is proved.

Exercises

12.1. Let F be a field and n a positive integer. If V is the set of all polynomials of degree n in $F[x]$, together with the zero polynomial, is V a subspace of $F[x]$?

12.2. Let F be a field and n a positive integer. If V is the set of all polynomials of degree at most n in $F[x]$, together with the zero polynomial, show that V is a subspace of $F[x]$.

12.3. Let V be a vector space having subspaces U and W. Show that $U \cap W$ is a subspace of V. Extend this to the intersection of an arbitrary collection of subspaces.

12.4. Let V be a vector space having subspaces U and W. Show that $U + W$ (regarding U and W as additive subgroups of V) is a subspace of V.

12.5. Let V and W be vector spaces over a field F. A function $\alpha : V \to W$ is said to be a linear transformation if $\alpha(v_1 + v_2) = \alpha(v_1) + \alpha(v_2)$ and $\alpha(av_1) = a\alpha(v_1)$ for all $a \in F$, $v_1, v_2 \in V$. If U is a subspace of V, show that $\alpha(U)$ is a subspace of W.

12.6. Let F, V, W and α be as in the preceding exercise. Show that the kernel of α (regarding α as a homomorphism of additive groups) is a subspace of V. Further show that α is one-to-one if and only if the kernel is $\{0\}$.

12.7. Let $F = \mathbb{Z}_{11}$ and $V = F^3$. If $W = \{(a, b, c) \in V : 2a + 3b + 7c = 0\}$, is W a subspace of V?

12.8. Let F be a field with vector spaces V and W. Let $U = V \times W$ be the direct product of the additive groups V and W. Define a scalar multiplication on U via $a(v, w) = (av, aw)$ for all $a \in F$, $v \in V$ and $w \in W$. Is U a vector space over F?

12.9. Let F be a field of characteristic 3 and V a vector space over F. Show that $v + v + v = 0$ for all $v \in F$.

12.10. Suppose that V is a vector space over an infinite field F. Show that V is not the union of a finite number of proper subspaces.

12.2 Basis and Dimension

In order to define a basis for a vector space, we must first discuss linear combinations of vectors.

Definition 12.4. Let V be a vector space over a field F. If $v_1, v_2, \ldots, v_k \in V$, then a vector $v \in V$ is said to be a **linear combination** of the v_i if $v = a_1v_1 + \cdots + a_kv_k$, for some $a_i \in F$.

Example 12.9. Let $F = \mathbb{Q}$ and $V = F^3$. If $v_1 = (2, -3, 7)$ and $v_2 = (4, 0, 1)$, then $(24, -6, 19)$ is a linear combination of v_1 and v_2, since $(24, -6, 19) = 2v_1 + 5v_2$.

Definition 12.5. Let F be a field and V a vector space over F. Let $v_1, v_2, \ldots, v_k \in V$. We say that the v_i are **linearly dependent** if there exist $a_1, \ldots, a_k \in F$, not all zero, such that $a_1v_1 + \cdots + a_kv_k = 0$. Otherwise, the v_i are **linearly independent**.

Example 12.10. Let $F = \mathbb{Z}_5$ and $V = F^3$. The vectors $(2, 1, 3)$, $(1, 3, 0)$ and $(2, 1, 4)$ are linearly dependent, since $3(2, 1, 3) + (1, 3, 0) + 4(2, 1, 4) = (0, 0, 0)$. On the other hand, $(1, 0, 4)$, $(3, 2, 1)$ and $(2, 0, 2)$ are linearly independent. Indeed, if $a_1(1, 0, 4) + a_2(3, 2, 1) + a_3(2, 0, 2) = (0, 0, 0)$, then looking at the middle entry, we see immediately that $a_2 = 0$. Then $a_1 + 2a_3 = 4a_1 + 2a_3 = 0$. This yields $3a_1 = 0$, and hence $a_1 = 0$ and, finally, $a_3 = 0$.

Here is a handy test for linear dependence.

Theorem 12.3. *Let V be a vector space over a field F and $v_1, \ldots, v_k \in V$. Then the v_i are linearly dependent if and only if either*

1. *$v_1 = 0$; or*
2. *there exists an $m \geq 2$ such that v_m is a linear combination of $v_1, \ldots, v_{m-1}$.*

Proof. Suppose that the v_i are linearly dependent. Choose $a_i \in F$, not all zero, such that $a_1v_1 + \cdots + a_kv_k = 0$. Let m be the largest positive integer such that $a_m \neq 0$. Then $a_1v_1 + \cdots + a_mv_m = 0$. If $m = 1$, then $a_1v_1 = 0$, with $a_1 \neq 0$. Thus, $v_1 = a_1^{-1}0 = 0$, giving case (1). If $m > 1$, then $v_m = -a_m^{-1}a_1v_1 - \cdots - a_m^{-1}a_{m-1}v_{m-1}$, and so v_m is a linear combination of $v_1, \ldots, v_{m-1}$, which proves case (2).

Conversely, suppose that (1) or (2) is satisfied. If $v_1 = 0$, then $1v_1 + 0v_2 + \cdots + 0v_k = 0$, meaning that the v_i are linearly dependent. If $v_m = b_1v_1 + \cdots + b_{m-1}v_{m-1}$, for some $b_i \in F$, then

$$b_1v_1 + \cdots + b_{m-1}v_{m-1} - 1v_m + 0v_{m+1} + \cdots + 0v_k = 0.$$

Again, the v_i are linearly dependent. □

Linear independence is most useful when combined with another property.

Definition 12.6. Let V be a vector space over a field F, and let $v_1, \ldots, v_k \in V$. Then we say that the v_i **span** V if every $v \in V$ is a linear combination of the v_i.

Example 12.11. Regarding $\mathbb{C}$ as a vector space over $\mathbb{R}$, we note that 1 and i span $\mathbb{C}$, as $a + bi = a1 + bi$.

Example 12.12. Let $F = \mathbb{R}$ and $V = \mathbb{R}^3$. Then the vectors $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$ span V, since $(a, b, c) = a(1, 0, 0) + b(0, 1, 0) + c(0, 0, 1)$.

The following lemma describes a very nice relationship between linear independence and spanning.

Lemma 12.1. *Let V be a vector space over a field F. Suppose that $v_1, \ldots, v_k$ span V. If $w_1, \ldots, w_l \in V$, and $l > k$, then the w_i are linearly dependent.*

Proof. Since the v_i span V, we know that w_1 is a linear combination of the v_i. Let us say that $w_1 = a_1v_1 + \cdots + a_kv_k$, with $a_i \in F$. If all of the a_i are zero, then w_1 is the zero vector. Thus, by Theorem 12.3, we are done. Therefore, we may assume that some a_i is nonzero. Without loss of generality, say $a_1 \neq 0$. We now observe that $w_1, v_2, v_3, \ldots, v_k$ span V. Indeed, if $v \in V$, then $v = b_1v_1 + \cdots + b_kv_k$, for some $b_i \in F$. But

$$v_1 = a_1^{-1}w_1 - a_1^{-1}a_2v_2 - \cdots - a_1^{-1}a_kv_k.$$

Thus,

$$v = b_1a_1^{-1}w_1 + (b_2 - b_1a_1^{-1}a_2)v_2 + \cdots + (b_k - b_1a_1^{-1}a_k)v_k,$$

proving the claim.

Now consider w_2. It is a linear combination of $w_1, v_2, v_3, \ldots, v_k$. Let us say that $w_2 = c_1w_1 + c_2v_2 + c_3v_3 + \cdots + c_kv_k$, with $c_i \in F$. If $c_i = 0$ for all $i \geq 2$, then w_2 is a linear combination of w_1, proving that the w_i are linearly dependent. Thus, we may assume that there exists an $i \geq 2$ with $c_i \neq 0$. Without loss of generality, say $c_2 \neq 0$. But then v_2 is a linear combination of $w_1, w_2, v_3, v_4, \ldots, v_k$. And just as before, we now deduce that $w_1, w_2, v_3, v_4, \ldots, v_k$ span V.

Repeat this argument. We will conclude either that the w_i are linearly dependent or, eventually, that $w_1, \ldots, w_k$ span V. But then w_{k+1} is a linear combination of $w_1, \ldots, w_k$. By Theorem 12.3, the w_i are linearly dependent. □

What we really need is a basis for a vector space.

Definition 12.7. Let V be a vector space over a field F. We say that $v_1, \ldots, v_k \in V$ form a **basis** for V if they are linearly independent and span V.

Example 12.13. Regarding $\mathbb{C}$ as a vector space over $\mathbb{R}$, we can see that 1 and i form a basis for $\mathbb{C}$.

Example 12.14. For any field F and any positive integer n, the vectors

$$(1, 0, 0, \ldots, 0), (0, 1, 0, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, 1)$$

form a basis for F^n.

Example 12.15. Let F be any field and $V = F[x]$. Then V has no finite basis. Indeed, if $v_1, \ldots, v_k \in V$, then any linear combination of these vectors must have degree no larger than the maximum of the degrees of the v_i. On the other hand, for any positive integer n, let W be the set of all polynomials having degree at most n (including the zero polynomial). By Exercise 12.2, W is a subspace of V, and the polynomials $1, x, x^2, \ldots, x^n$ form a basis.

Theorem 12.4. *Let V be a vector space over a field F. If $v_1, \ldots, v_k$ form a basis for V, then every element of V can be written uniquely in the form $a_1v_1 + \cdots + a_kv_k$, with $a_i \in F$.*

Proof. Since a basis spans the space, only the uniqueness needs to be proved. Suppose that

$$a_1 v_1 + \cdots + a_k v_k = b_1 v_1 + \cdots + b_k v_k,$$

with $a_i, b_i \in F$. Then

$$(a_1 - b_1)v_1 + \cdots + (a_k - b_k)v_k = 0.$$

By linear independence, $a_i = b_i$ for all i. □

Bases are not unique. For instance, $(1, 0)$ and $(0, 1)$ form a basis for $\mathbb{R}^2$ over $\mathbb{R}$, but so do $(1, 3)$ and $(5, 2)$. However, any two bases for a vector space must have the same number of vectors.

Theorem 12.5. *Let V be a vector space over a field F. If $v_1, \ldots, v_k$ and $w_1, \ldots, w_l$ are bases for V, then $k = l$.*

Proof. Suppose the theorem is false. Without loss of generality, say $k < l$. Then $v_1, \ldots, v_k$ span V. Since $k < l$, Lemma 12.1 tells us that $w_1, \ldots, w_l$ are linearly dependent. We have a contradiction. □

Definition 12.8. Let V be a vector space over a field F. If $v_1, \ldots, v_k$ is a basis for V, then we say that V has **dimension** k, and write $\dim V = k$ (or $\dim_F V = k$, if the field is unclear from the context). We also stipulate that $\dim\{0\} = 0$. In either of these cases, V is **finite-dimensional**. If V has no finite basis, then V is **infinite-dimensional**.

Example 12.16. For any field F and positive integer n, $\dim F^n = n$. See Example 12.14.

Example 12.17. The dimension of $\mathbb{C}$ over $\mathbb{R}$ is 2. See Example 12.13.

Example 12.18. If F is any field, then $F[x]$ is infinite-dimensional. The vector space consisting of the polynomials of degree at most n over F, including the zero polynomial, has dimension $n + 1$. See Example 12.15.

In a finite-dimensional space, we can discard vectors from a spanning set to obtain a basis, or add vectors to a linearly independent set to obtain a basis.

Theorem 12.6. *Let V be any vector space over a field F, with $V \neq \{0\}$. Take $v_1, \ldots, v_k \in V$. Then*

1. *if $v_1, \ldots, v_k$ span V, then some subset of $\{v_1, \ldots, v_k\}$ is a basis for V; and*
2. *if $v_1, \ldots, v_k$ are linearly independent, and $\dim V = n < \infty$, then there exist $v_{k+1}, \ldots, v_n \in V$ such that $v_1, \ldots, v_n$ form a basis for V.*

Proof. (1) We proceed by induction on k. If $k = 1$, then since v_1 spans V, and $V \neq \{0\}$, we see that $v_1 \neq 0$, and hence v_1 is linearly independent. (If $av_1 = 0$, and $0 \neq a \in F$, then $0 = a^{-1}av_1 = v_1$.) Thus, v_1 is a basis. Suppose the result is true for k, and let $v_1, \ldots, v_{k+1}$ span V. If they are linearly independent, there is nothing to do. Otherwise, refer to Theorem 12.3. If $v_1 = 0$, then $v_2, \ldots, v_{k+1}$ span V as well. By our inductive hypothesis we are done. Otherwise, some v_l is a linear combination of $v_1, \ldots, v_{l-1}$. Without loss of generality, say $l = k+1$. Write $v_{k+1} = a_1v_1 + \cdots + a_kv_k$. If $v \in V$, we know that

$$v = b_1v_1 + \cdots + b_{k+1}v_{k+1},$$

for some $b_i \in F$. But then

$$v = (b_1 + a_1b_{k+1})v_1 + \cdots + (b_k + a_kb_{k+1})v_k.$$

Thus, $v_1, \ldots, v_k$ span V. Our inductive hypothesis completes the proof.

(2) If $v_1, \ldots, v_k$ span V, there is nothing to do. Otherwise, find $v_{k+1} \in V$ which is not a linear combination of $v_1, \ldots, v_k$. Suppose that $v_1, \ldots, v_{k+1}$ are linearly dependent. Then $a_1v_1 + \cdots + a_{k+1}v_{k+1} = 0$, for some $a_i \in F$. If $a_{k+1} = 0$, then $v_1, \ldots, v_k$ are linearly dependent, which is not the case. Otherwise,

$$v_{k+1} = -a_{k+1}^{-1}a_1v_1 - \cdots - a_{k+1}^{-1}a_kv_k;$$

that is, v_{k+1} is a linear combination of $v_1, \ldots, v_k$, giving us a contradiction. Therefore, $v_1, \ldots, v_{k+1}$ is a linearly independent set. Now repeat. This process must stop, because Lemma 12.1 tells us that V cannot have a linearly independent set with more than n vectors. □

Example 12.19. Let $F = \mathbb{Q}$ and $V = \mathbb{Q}^3$. The vectors $(3, -7, 0)$ and $(1, 2, 0)$ are easily seen to be linearly independent. Furthermore, $(2, 5, 8)$ is not a linearly combination of these two vectors. Thus, since $\dim V = 3$, we see that the vectors $(3, -7, 0)$, $(1, 2, 0)$, $(2, 5, 8)$ form a basis for V.

Exercises

12.11. Let $F = \mathbb{R}$ and $V = \mathbb{R}^3$. Are the following sets of vectors in V linearly dependent or independent over F?

1. $(1, 3, 5)$, $(2, 1, 4)$, $(7, 11, 23)$
2. $(1, 3, 4)$, $(2, 2, 1)$, $(3, 6, 3)$

12.12. Let $F = \mathbb{Z}_7$ and $V = M_2(F)$. Are the following sets of vectors in V linearly dependent or independent over F?

1. $\begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 3 & 2 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}$

12.13. Do the following vectors span $\mathbb{Q}^3$ (as a vector space over $\mathbb{Q}$)?

1. $(1, 0, 2), (2, 5, 3), (3, 5, 5)$
2. $(1, 0, 2), (2, 3, 5), (0, 0, 4)$

12.14. Do the following matrices span $M_2(\mathbb{Z}_5)$ (as a vector space over $\mathbb{Z}_5$), namely $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$?

12.15. Let $V = M_2(\mathbb{C})$. Find the dimension of V as a vector space over $\mathbb{C}$, and as a vector space over $\mathbb{R}$.

12.16. Let $F = \mathbb{Z}_7$ and $V = \{(a, b, c) \in F^3 : c = 3a + 5b\}$. Find the dimension of V over F.

12.17. Let F be a field and V a finite-dimensional vector space. If W is a subspace of V, show that $\dim W \leq \dim V$, with equality if and only if $W = V$. (Do not assume, to begin with, that W is finite-dimensional.)

12.18. Suppose that a vector space V with dimension n has subspaces U and W with dimensions m and k, respectively. If $m + k > n$, show that $U \cap W \neq \{0\}$.

12.19. Let F, V, W and α be as in Exercise 12.5. Suppose that $v_1, \ldots, v_n \in V$ are linearly independent and α is one-to-one. Show that $\alpha(v_1), \ldots, \alpha(v_n)$ are linearly independent.

12.20. Let F be a field and V a finite-dimensional vector space over F. Say $\dim V = n \in \mathbb{N}$. Show that there exists a bijective linear transformation (see Exercise 12.5 for the definition) $\alpha : V \to F^n$.

12.3 Field Extensions

Let us now focus on our main vector space of interest: the field extension.

Definition 12.9. Let K be a field extension of F. Then the **degree** of the extension is the dimension of K over F. We write $[K : F] = \dim_F K$. The extension is **finite** if $[K : F] < \infty$ and, in particular, **quadratic** if $[K : F] = 2$.

Example 12.20. As we observed in Example 12.17, $\mathbb{C}$ is a quadratic extension of $\mathbb{R}$.

Example 12.21. Let $K = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$. We claim that K is a subfield of $\mathbb{R}$ and, therefore, an extension field of $\mathbb{Q}$. All of the properties of a subfield are easy to verify except, perhaps, that nonzero elements have inverses. Take $0 \neq a + b\sqrt[3]{2} + c\sqrt[3]{4} \in K$. Then notice that $(a + bx + cx^2, x^3 - 2)$ divides $x^3 - 2$. But, by Example 11.10, $x^3 - 2$ is irreducible over $\mathbb{Q}$. Thus, the gcd can only be a constant polynomial (in fact, 1, since we assume it to be monic). As $\mathbb{Q}[x]$ is a Euclidean domain, Theorem 10.6 guarantees that we can write

$$1 = u(x)(x^3 - 2) + v(x)(a + bx + c^2),$$

for some $u(x), v(x) \in \mathbb{Q}[x]$. But then $1 = v(\sqrt[3]{2})(a + b\sqrt[3]{2} + c\sqrt[3]{4})$. As it is easy to see that $v(\sqrt[3]{2}) \in K$, we have an inverse for $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ in K, as claimed.

In fact, $[K : \mathbb{Q}] = 3$. To see this, we observe that $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is a basis for K over $\mathbb{Q}$. Clearly, these numbers span K. If they are linearly dependent, then there are rational numbers a, b, c, not all zero, such that $\sqrt[3]{2}$ is a root of $a+bx+cx^2$. But again, $1 = (a+bx+cx^2, x^3-2)$, and we write $1 = u(x)(a+bx+cx^2)+v(x)(x^3-2)$, for some $u(x), v(x) \in \mathbb{Q}[x]$. Evaluating at $\sqrt[3]{2}$, we obtain $1 = 0$, giving a contradiction and establishing that we have a basis.

We are, in fact, engaging in a small abuse of notation here. If K is an extension field of F then, of course, F is also an additive subgroup of K. We could also use the notation $[K : F]$ to mean the index of F in K as additive subgroup. This is not the same as the degree of the extension! For the remainder of the book, when we write $[K : F]$, we will mean the degree of the extension.

In the particular case of a finite field, we can illustrate the difference. By Lagrange's theorem, the index of the additive groups would be $\frac{|K|}{|F|}$. However, the degree is calculated as follows.

Theorem 12.7. *Let K be a field extension of F, such that K is a finite field. Then $[K : F] = \log_{|F|} |K|$.*

Proof. First, we note that K must be finite-dimensional over F. Indeed, the elements of K must span K, and by Theorem 12.6, we can obtain a finite basis. Let $[K : F] = n$, and suppose that $\{v_1, \ldots, v_n\}$ is a basis for K over F. By Theorem 12.4, the elements of K are uniquely of the form $a_1v_1 + \cdots + a_nv_n$, with $a_i \in F$. As there are $|F|$ choices for each a_i, the total number of elements of K is $|F|^n$. Taking the base $|F|$ logarithm, we obtain our result. □

Degrees of extensions behave in a nice way.

Theorem 12.8. *Let K be a finite extension of F and L a finite extension of K. Then $[L : F] = [L : K][K : F]$.*

Proof. Let $\{v_1, \ldots, v_n\}$ be a basis for K over F, and let $\{w_1, \ldots, w_m\}$ be a basis for L over K. We claim that $\{v_iw_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for L over F. This will complete the proof.

Take any $l \in L$. Then $l = a_1w_1 + \cdots + a_mw_m$, for some $a_i \in K$. But $a_i = b_{i1}v_1 + \cdots + b_{in}v_n$, for some $b_{ij} \in F$. Thus,

$$l = b_{11}v_1w_1 + b_{12}v_2w_1 + \cdots + b_{1n}v_nw_1 + \cdots + b_{m1}v_1w_m + \cdots + b_{mn}v_nw_m.$$

That is, the v_iw_j span L over F. Suppose that they are linearly dependent. Then there exist $b_{ij} \in F$, not all zero, such that

$$\begin{aligned} 0 &= b_{11}v_1w_1 + \cdots + b_{1n}v_nw_1 + \cdots + b_{m1}v_1w_m + \cdots + b_{mn}v_nw_m \\ &= (b_{11}v_1 + \cdots + b_{1n}v_n)w_1 + \cdots + (b_{m1}v_1 + \cdots + b_{mn}v_n)w_m. \end{aligned}$$

As each $b_{i1}v_1 + \cdots + b_{in}v_n \in K$, and the w_i are linearly independent over K, we have $b_{i1}v_1 + \cdots + b_{in}v_n = 0$, for all i. But the $b_{ij} \in F$, and the v_j are linearly independent over F. Thus, all of the b_{ij} are zero. The proof is complete. □

Example 12.22. Let $K = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$. By Example 8.30, K is an extension field of $\mathbb{Q}$. Clearly, 1 and $\sqrt{2}$ span K over $\mathbb{Q}$. If they were linearly dependent, then $\sqrt{2}$ would lie in $\mathbb{Q}$, which is not the case. Thus, $[K : \mathbb{Q}] = 2$. Let $L = \{c + d\sqrt{3} : c, d \in K\}$. We claim that L is a subfield of $\mathbb{R}$ and, hence, an extension of K. All of the subfield properties are easy to check except perhaps the existence of inverses. Let $0 \neq c + d\sqrt{3} \in L$. Then $(c + d\sqrt{3})(c - d\sqrt{3}) = c^2 - 3d^2$. Suppose that this is 0. Then $c - d\sqrt{3} = 0$. If $d = 0$, then so is c, giving us a contradiction. Otherwise, $\sqrt{3} = cd^{-1} \in K$. Thus, we can write $a + b\sqrt{2} = \sqrt{3}$, with $a, b \in \mathbb{Q}$. Then $a^2+2b^2+2ab\sqrt{2} = 3$. If $b = 0$, then $\sqrt{3} = a \in \mathbb{Q}$, which is not true. If $a = 0$, then $\sqrt{\frac{3}{2}} = b \in \mathbb{Q}$. But then $2x^2 - 3$ has a rational root which, by Theorem 11.5, is not the case. Thus, $ab \neq 0$, and $\sqrt{2} \in \mathbb{Q}$, giving us a contradiction. Therefore, $(c + d\sqrt{3})^{-1} = \frac{c-d\sqrt{3}}{c^2-3d^2} \in L$. Now, 1 and $\sqrt{3}$ span L over K. If they were linearly dependent, then we would have $\sqrt{3} \in K$ which, as we have just seen, is not the case. Therefore, $[L : K] = 2$. By the theorem above, $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 4$.

One particular type of extension is especially important.

Definition 12.10. Let K be a field extension of F. If $a \in K$, then we write $F(a)$ for the intersection of all subfields of K containing F and a. We say that K is a **simple extension** of F if $K = F(a)$ for some $a \in K$.

By Exercise 8.33, the intersection of some set of fields is a field. Thus, $F(a)$ is always a field. Indeed, it is the smallest subfield of K containing F and a.

Example 12.23. By Example 8.30, $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$. Thus, since any field including $\mathbb{Q}$ and $\sqrt{2}$ would surely contain this field, it is $\mathbb{Q}(\sqrt{2})$.

Example 12.24. In a similar manner, we note that $\mathbb{Q}(\sqrt[3]{2})$ would have to contain $\sqrt[3]{2}$ and $(\sqrt[3]{2})^2$. Example 12.21 shows us that $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$.

Let us concentrate on simple extensions. In fact, we need to break them down into two types, depending upon one specific property of the element a.

Definition 12.11. Let K be a field extension of F and $a \in K$. We say that a is **algebraic** over F if there exists a nonzero polynomial $f(x) \in F[x]$ such that $f(a) = 0$. Otherwise, a is **transcendental** over F.

Example 12.25. The number $\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$, since it is a root of $x^3 - 2 \in \mathbb{Q}[x]$.

Example 12.26. The number $\sqrt{2}+\sqrt{3}$ is algebraic over $\mathbb{Q}$, since it is a root of x^4-10x^2+1.

Finding examples of real numbers that are transcendental over $\mathbb{Q}$ is a bit tricky. As it happens, the constants e and π are both transcendental. (This is a difficult result. For a proof, see the advanced monograph of Baker [1].) Of course, the underlying field is important! If we let $F=\mathbb{Q}(\pi^2)$, then π is algebraic over F, as π is a root of $x^2-\pi^2\in F[x]$.

We are primarily interested in algebraic elements. However, we can mention one important fact about transcendental elements. If F is a field, then $F[x]$ is an integral domain, and so we can consider its field of fractions. Denote this field of fractions by $F(x)$.

Theorem 12.9. *Let K be an extension field of F, and let $a\in K$ be transcendental over F. Then $F(a)$ is isomorphic to $F(x)$. In particular, $F(a)$ is of infinite degree over F.*

Proof. Define $\alpha: F[x]\to K$ via $\alpha(f(x))=f(a)$. By Lemma 11.1, α is a homomorphism. If $f(x)\in\ker(\alpha)$, then $f(a)=0$. Since a is transcendental, $f(x)$ is the zero polynomial. Thus, α is one-to-one, and $F[x]$ is isomorphic to $\alpha(F[x])$. Also, $f(a)\in F(a)$ for all $f(x)\in F[x]$; thus, $\alpha(F[x])$ is a subring of $F(a)$. By Theorem 9.15, there is a subfield L of $F(a)$ such that L is isomorphic to $F(x)$ and contains $\alpha(F[x])$. Clearly $\alpha(b)=b$ for all $b\in F$ and $\alpha(x)=a$; thus, $\alpha(F[x])$ contains both F and a. But $F(a)$ is the smallest subfield of K containing both F and a; thus, $F(a)=L$.

Suppose that $[F(a):F]=n<\infty$. Then according to Lemma 12.1, the elements $1,a,a^2,\ldots,a^n$ must be linearly dependent over F. But then there exist $c_i\in F$, not all zero, such that a is a root of $c_0+c_1x+\cdots+c_nx^n$. That is, a is algebraic, giving us a contradiction. □

Now suppose that a is algebraic over F. We know that it satisfies a nonzero polynomial in $F[x]$. But one particular such polynomial is key.

Definition 12.12. Let K be an extension field of F and let $a\in K$ be algebraic over F. Then the **minimal polynomial** of a over F is the monic irreducible polynomial $m(x)\in F[x]$ such that $m(a)=0$.

Example 12.27. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is x^3-2. Indeed, $\sqrt[3]{2}$ is a root, and the polynomial is irreducible by Example 11.10.

Example 12.28. The minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ is x^4-10x^2+1. As we noted in Example 12.26, $\sqrt{2}+\sqrt{3}$ is a root. Suppose it were reducible over $\mathbb{Q}$. The Rational Roots Theorem shows us that it has no roots in $\mathbb{Q}$. Thus, it would have to factor as a product of two polynomials of degree 2. By Theorem 11.4, these polynomials may be assumed to be in $\mathbb{Z}[x]$. Looking at the coefficients, we see immediately that (up to multiplying both factors by -1) the only possibilities are $(x^2+ax+1)(x^2-ax+1)$ and $(x^2+ax-1)(x^2-ax-1)$, for some $a\in\mathbb{Z}$. But then $2-a^2=-10$ or $-2-a^2=-10$. Neither of these has a solution in $\mathbb{Z}$.

We were a bit bold in our definition of the minimal polynomial. Indeed, we assumed that such a polynomial exists, and that there is only one. Fortunately, our presumptuousness was justified; in fact, we can say more.

Theorem 12.10. *Let K be an extension field of F, and let $a \in K$ be algebraic over F. Then*

1. *the minimal polynomial $m(x)$ of a over F exists, and is the unique monic polynomial of smallest degree in $F[x]$ of which a is a root; and*
2. *if $f(x) \in F[x]$, then $f(a) = 0$ if and only if $m(x)|f(x)$.*

Proof. Let $I = \{f(x) \in F[x] : f(a) = 0\}$. We claim that I is an ideal of $F[x]$. Surely $0 \in I$. If $f(x), g(x) \in I$, then $f(a) - g(a) = 0$, and hence $f(x) - g(x) \in I$. Also, if $h(x) \in F[x]$, then $f(a)h(a) = 0$, and hence $f(x)h(x) \in I$, proving the claim.

We know that $F[x]$ is a Euclidean domain and hence, by Theorem 10.8, a PID. Thus, let $I = (m(x))$. Since a is algebraic, $m(x)$ is not the zero polynomial. As $(m(x)) = (cm(x))$ if $0 \neq c \in F$, we may as well assume that $m(x)$ is monic. Now, $f(x) \in I$ if and only if $m(x)|f(x)$, as required by (2). As such, $\deg(m(x)) \leq \deg f(x)$, unless $f(x) = 0$. If $\deg(m(x)) = \deg(f(x))$, then $f(x)$ is simply $m(x)$ multiplied by an element of F. If $f(x)$ is also monic, then $f(x) = m(x)$. Thus, $m(x)$ satisfies condition (1) as well.

We must still establish that $m(x)$ is actually the minimal polynomial of a over F. To demonstrate this, we must show that $m(x)$ is irreducible. But if $m(x) = f(x)g(x)$, with $f(x), g(x) \in F[x]$, then $0 = m(a) = f(a)g(a)$. Thus, $f(a) = 0$ or $g(a) = 0$. Without loss of generality, say $f(a) = 0$. Then $m(x)|f(x)$. But also $f(x)|m(x)$. It now follows that $\deg(f(x)) = \deg(m(x))$, and hence $g(x)$ is a constant polynomial. Thus, $m(x)$ is irreducible, and hence a minimal polynomial for a. If $g(x)$ is another minimal polynomial, then $g(x) \in I$, and hence $m(x)|g(x)$. But $g(x)$ is irreducible, and therefore $g(x) = cm(x)$ for some $c \in F$. As $m(x)$ and $g(x)$ are both monic, $m(x) = g(x)$, and the proof is complete. □

We can use the minimal polynomial to describe the simple extension.

Theorem 12.11. *Let L be an extension field of F, and let $a \in L$ be algebraic over F. If $m(x)$ is the minimal polynomial of a over F, let $n = \deg(m(x))$. Then*

1. *$[F(a) : F] = n$;*
2. *$\{1, a, a^2, \ldots, a^{n-1}\}$ is a basis for $F(a)$ over F; and*
3. *$F(a)$ is isomorphic to $F[x]/(m(x))$.*

Proof. Of course, (1) follows immediately from (2), so let us prove (2). Suppose that $1, a, \ldots, a^{n-1}$ are linearly dependent. Then there exist $c_0, \ldots, c_{n-1} \in F$, not all zero, such that $c_0 + c_1 a + \cdots + c_{n-1}a^{n-1} = 0$. That is, a is a root of $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. But this polynomial has degree smaller than that of $m(x)$, contradicting Theorem 12.10. Thus, $1, a, \ldots, a^{n-1}$ are linearly independent.

We claim that they span $F(a)$. We know that $F(a)$ is the smallest field containing F and a (and, hence, all of the a^i). Therefore, it is sufficient to show that $K =$

$\{c_0 + c_1a + \cdots + c_{n-1}a^{n-1} : c_i \in F\}$ is a field. Clearly, it contains 1 and is closed under subtraction. To show that it is closed under multiplication, it is enough to show that $a^i \in K$ for all positive integers i. Our proof is by strong induction upon i. If $i < n$, there is nothing to do, so let $i \geq n$ and suppose it is true for smaller exponents. Writing $m(x) = b_0 + \cdots + b_{n-1}x^{n-1} + x^n$, we have $a^i = a^n a^{i-n} = (-b_0 - b_1a - \cdots - b_{n-1}a^{n-1})a^{i-n}$. But this is a linear combination of terms of the form a^j, with $j < i$. Thus, by our inductive hypothesis, $a^i \in K$. Finally, we must check that every nonzero element of K has an inverse in K. But a nonzero element of K has the form $f(a)$, for some $0 \neq f(x) \in F[x]$, with $\deg(f(x)) < n$. Now, $(f(x), m(x))|m(x)$. As $m(x)$ is irreducible, $(f(x), m(x))$ is either 1 or an associate of $m(x)$. However, $\deg(f(x)) < \deg(m(x))$. Thus, $(f(x), m(x)) = 1$. By Theorem 10.6, there exist $u(x), v(x) \in F[x]$ such that $f(x)u(x) + m(x)v(x) = 1$. Since $m(a) = 0$, we have $f(a)u(a) = 1$. Furthermore, as we noted above, $u(a) \in K$, so $f(a)$ has an inverse in K. Therefore, K is a field, and (2) is proved.

(3) Define $\alpha : F[x] \to F(a)$ via $\alpha(f(x)) = f(a)$. By Lemma 11.1, α is a homomorphism. In view of (2), it is onto. The kernel is the set of all polynomials in $F[x]$ of which a is a root. By Theorem 12.10, this is $(m(x))$. Apply the First Isomorphism Theorem. □

Example 12.29. As $x^2 + 1$ is the minimal polynomial of i over $\mathbb{R}$, we see that $\mathbb{C} = \mathbb{R}(i)$ is isomorphic to $\mathbb{R}[x]/(x^2 + 1)$.

Example 12.30. As we saw in Example 12.28, the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ is $x^4 - 10x^2 + 1$. Therefore, $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ is isomorphic to

$$\mathbb{Q}[x]/(x^4 - 10x^2 + 1).$$

Furthermore, letting $a = \sqrt{2} + \sqrt{3}$, the elements of $\mathbb{Q}(a)$ are precisely $c_0 + c_1a + c_2a^2 + c_3a^3$, with $c_i \in \mathbb{Q}$. Addition works in the obvious way. To demonstrate multiplication, let us try $(2 - 3a + 4a^2)(5 + a - 6a^2 + 2a^3)$. We get $10 - 13a + 5a^2 + 26a^3 - 30a^4 + 8a^5$. Now, $a^4 = 10a^2 - 1$ and $a^5 = 10a^3 - a$. Thus, our product is $40 - 21a - 295a^2 + 106a^3$.

Our last theorem has an interesting immediate consequence.

Corollary 12.1. *Let K be an extension field of F. If $a, b \in K$, and a and b have the same minimal polynomial over F, then $F(a)$ is isomorphic to $F(b)$.*

Proof. If $m(x)$ is the minimal polynomial, then by Theorem 12.11, both $F(a)$ and $F(b)$ are isomorphic to $F[x]/(m(x))$. □

Example 12.31. Let ω be a primitive cube root of unity in $\mathbb{C}$. (That is, $\omega^3 = 1$ but $\omega \neq 1$.) Then $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$ are both roots of $x^3 - 2 \in \mathbb{Q}[x]$. As we have observed, $x^3 - 2$ is irreducible over $\mathbb{Q}$, so it is the minimal polynomial of both $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$. Thus, $\mathbb{Q}(\sqrt[3]{2})$ is isomorphic to $\mathbb{Q}(\omega\sqrt[3]{2})$. These fields are clearly distinct, as $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of $\mathbb{R}$, but $\omega\sqrt[3]{2} \notin \mathbb{R}$.

Exercises

12.21. Find the minimal polynomial of $\sqrt{5}+\sqrt{7}$ over $\mathbb{Q}$.

12.22. Find the minimal polynomial of $\sqrt[3]{3}+\sqrt[3]{9}$ over $\mathbb{Q}$.

12.23. Let K be a finite extension field of F. Show that every element of K is algebraic over F.

12.24. Let K be an extension field of F and L an extension field of K. If $a \in L$ is algebraic over F, show that $[K(a) : K] \leq [F(a) : F]$.

12.25. Suppose that we have subfields F_n of K with $F_1 \subseteq F_2 \subseteq F_3 \subseteq \cdots$. Show that $\bigcup_{n=1}^{\infty} F_n$ is a field.

12.26. For each positive integer n, let $a_n = \sqrt[2^n]{2}$. If $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(a_n)$, show that K is an infinite field extension of $\mathbb{Q}$, but every element of K is algebraic over $\mathbb{Q}$.

12.27. Let K be a field extension of F. Show that for every $a \in K$, $F(a^2) \subseteq F(a)$. Also, give an explicit example illustrating that we do not have $F(a^2) = F(a)$ in general.

12.28. Let K be a field extension of F and $a \in K$. Show that a is algebraic over F if and only if a^2 is algebraic over F.

12.29. Let K be an extension field of $\mathbb{C}$. If $a \in K$ is algebraic over $\mathbb{C}$, show that $a \in \mathbb{C}$.

12.30. Let K be a finite extension of F. If R is a subring of K containing F, show that R is a field.

12.4 Splitting Fields

Let us now take a slightly different perspective from the preceding section. Given a field F, instead of looking at elements of extension fields and finding their minimal polynomials, let us instead take a nonconstant polynomial $f(x) \in F[x]$ and see if we can find a field containing F and a root of $f(x)$. For instance, suppose that we only knew about the rational numbers, and we wanted to construct a field having a root of $x^2 - 2$.

Definition 12.13. Let F be a field and let $f(x) \in F[x]$ be a nonconstant polynomial. If K is an extension field of F, then we say that $f(x)$ **splits** over K if there exist $a, a_1, \ldots, a_n \in K$ such that $f(x) = a(x - a_1) \cdots (x - a_n)$. In particular, K is a **splitting field** for $f(x)$ if $f(x)$ splits over K, and if L is any subfield of K with $F \subseteq L \subsetneq K$, then $f(x)$ does not split over L.

To put this another way, if K is an extension field of F and $b_1, \ldots, b_n \in K$, write $F(b_1, \ldots, b_n)$ for the intersection of all subfields of K containing F and all of the b_i. If $f(x) \in F[x]$ splits over K, and $a_1, \ldots, a_n$ are the roots of $f(x)$ in K, then K is a splitting field of $f(x)$ if and only if $K = F(a_1, \ldots, a_n)$.

But how to construct such a field? The following observation is helpful.

Lemma 12.2. *Every nonzero prime ideal in a PID is maximal.*

Proof. Let I be a nonzero prime ideal in a PID R. Then $I = (a)$, for some $a \in I$. By Lemma 10.2, a is prime. In particular, by Theorem 10.10, a is irreducible. Since I is prime, $I \neq R$. Suppose that J is an ideal of R with $I \subsetneq J \subsetneq R$. Let $J = (b)$. Then $a \in (b)$, so $b|a$. As a is irreducible, b is a unit or an associate of a. In the former case, $J = R$. In the latter, $a|b$, and hence $J = I$. Either way, we have a contradiction. □

The next lemma is the key to our construction.

Lemma 12.3. *Let F be a field and $f(x)$ an irreducible polynomial in $F[x]$. Let $K = F[x]/(f(x))$. Then K is a field containing (an isomorphic copy of) F and a root a of $f(x)$. In fact, $K = F(a)$.*

Proof. We know that $F[x]$ is a Euclidean domain and hence, by Theorem 10.8, a PID. By Theorem 10.11, $f(x)$ is prime. Thus, by Lemma 10.2, $(f(x))$ is a prime ideal. The preceding lemma tells us that $(f(x))$ is maximal. By Theorem 9.20, K is indeed a field. Define $\alpha : F \to K$ via $\alpha(b) = b + (f(x))$. It is immediate that α is a homomorphism. If $\alpha(b) = 0$, then $b \in (f(x))$, which means that $f(x)|b$. As b is a constant, $b = 0$, and hence α is one-to-one. Thus, K contains an isomorphic copy of F, namely $\alpha(F)$. Finally, let us show that K contains a root of $f(x)$. But this root is $a = x + (f(x))$. Indeed, $f(a) = f(x) + (f(x)) = 0 + (f(x))$, as required. Clearly, $F(a)$ would have to contain $x^n + (f(x))$ for all $n \geq 0$. Thus, $K = F(a)$. □

Let us combine the preceding lemma with Theorem 12.11. We see that if $f(x) \in F[x]$ is irreducible of degree n, then the field K has, as a basis over F, the terms $x^i + (f(x))$, with $0 \leq i < n$. This allows us for the first time to create finite fields other than $\mathbb{Z}_p$, where p is a prime.

Example 12.32. Suppose we wish to construct a field of order 125. In view of Theorem 12.7, we would need an extension of degree 3 of $\mathbb{Z}_5$. Consider $f(x) = x^3 + 3x^2 + x + 2 \in \mathbb{Z}_5[x]$. By Corollary 11.2, it is irreducible over $\mathbb{Z}_5$ if it has no roots in $\mathbb{Z}_5$. There are only five possible roots, and none of them work. Therefore, $f(x)$ is irreducible and $F[x]/(f(x))$ is a field of order 125. The elements are $a_0 + a_1x + a_2x^2 + (f(x))$, with $a_i \in \mathbb{Z}_5$. Addition works in the obvious way. As an example of multiplication, we have (letting $I = (f(x))$)

$$\begin{aligned}(2 + 4x + 3x^2 + I)(1 + 4x + I) &= 2 + 2x + 4x^2 + 2x^3 + I \\ &= 2 + 2x + 4x^2 + 2(-3x^2 - x - 2) + I \\ &= 3 + 3x^2 + I.\end{aligned}$$

We can now construct splitting fields.

Theorem 12.12. *Let F be a field and $f(x) \in F[x]$ a nonconstant polynomial. Then there is a splitting field of $f(x)$ over F.*

Proof. First, let us prove the existence of a field extension in which $f(x)$ splits. We proceed by induction on $n = \deg(f(x))$. If $n = 1$, then F will suffice. Assume that $n \geq 2$ and the $n-1$ case holds. We know that $F[x]$ is a UFD. Thus, write $f(x) = g_1(x) \cdots g_k(x)$, where the $g_i(x)$ are irreducible in $F[x]$. By Lemma 12.3, there is an extension field K of F in which $g_1(x)$ has a root, a. Then by Theorem 11.2, $g_1(x) = (x-a)h_1(x)$, for some $h_1(x) \in K[x]$. Thus, in $K[x]$, we have $f(x) = (x-a)h_1(x)g_2(x) \cdots g_k(x)$. Now, $h_1(x)g_2(x) \cdots g_k(x)$ has degree $n-1$. Thus, by our inductive hypothesis, it splits in some extension field L of K. Hence, L is an extension field of F, and $f(x)$ splits over L.

Let us write $f(x) = b(x-b_1) \cdots (x-b_n)$, with $b, b_1, \ldots, b_n \in L$. Then $F(b_1, \ldots, b_n)$ is a splitting field for $f(x)$ over F. □

But we can go one step further. We want to show that splitting fields are unique up to isomorphism. (The proof is a bit technical, but the result will pay dividends when we classify the finite fields.) To this end, we need to sharpen Corollary 12.1 a bit. If $\alpha : R \to S$ is a ring homomorphism, and $f(x) = c_0 + \cdots + c_n x^n \in R[x]$, then we write $\alpha(f(x)) = \alpha(c_0) + \cdots + \alpha(c_n)x^n \in S[x]$.

Lemma 12.4. *Let $\alpha : F \to K$ be an isomorphism of fields. Let $f(x) \in F[x]$ be an irreducible polynomial. Suppose that a is a root of $f(x)$ in some extension field of F and b is a root of $\alpha(f(x))$ in some extension field of K. Then there exists an isomorphism $\beta : F(a) \to K(b)$ such that $\beta(c) = \alpha(c)$ for all $c \in F$ and $\beta(a) = b$.*

Proof. Define $\gamma : F[x] \to F(a)$ via $\gamma(g(x)) = g(a)$. By Lemma 11.1, γ is a homomorphism. By Theorem 12.10, $\ker(\gamma) = (f(x))$. (We assumed that $f(x)$ was monic in that theorem, but that is immaterial here.) In view of Theorem 12.11, γ is onto. Thus, the proof of the First Isomorphism Theorem shows us that the map $\rho : F[x]/(f(x)) \to F(a)$ given by $\rho(g(x) + (f(x))) = g(a)$ is an isomorphism. We also note that if $c \in F$, then $\rho(c + (f(x))) = c$ and $\rho(x + (f(x))) = a$. In precisely the same manner, the map $\tau : K[x]/(\alpha(f(x))) \to K(b)$ given by $\tau(h(x) + (\alpha(f(x)))) = h(b)$ is an isomorphism, $\tau(d + (\alpha(f(x)))) = d$ for all $d \in K$ and $\tau(x + (\alpha(f(x)))) = b$.

Now, the function from $F[x]$ to $K[x]$ mapping each $u(x)$ to $\alpha(u(x))$ is easily seen to be an isomorphism. Composing that with the obvious homomorphism from $K[x]$ to $K[x]/(\alpha(f(x)))$, we obtain a homomorphism from $F[x]$ onto $K[x]/(\alpha(f(x)))$ with kernel $(f(x))$. In view of the First Isomorphism Theorem, we have an isomorphism $\sigma : F[x]/(f(x)) \to K[x]/(\alpha(f(x)))$ given by

$$\sigma(u(x) + (f(x))) = \alpha(u(x)) + (\alpha(f(x))).$$

Notice that $\sigma(c + (f(x))) = \alpha(c) + (\alpha(f(x)))$ for all $c \in F$, and $\sigma(x + (f(x))) = x + (\alpha(f(x)))$.

From Theorem 9.12, we learn that $\tau\sigma\rho^{-1} : F(a) \to K(b)$ is an isomorphism. Furthermore, if $c \in F$, then

$$\tau\sigma\rho^{-1}(c) = \tau\sigma(c + (f(x))) = \tau(\alpha(c) + (\alpha(f(x)))) = \alpha(c),$$

and

$$\tau\sigma\rho^{-1}(a) = \tau\sigma(x + (f(x))) = \tau(x + (\alpha(f(x)))) = b.$$

Letting $\beta = \tau\sigma\rho^{-1}$, we are done. □

This allows us to prove the uniqueness of splitting fields.

Theorem 12.13. *Let $\alpha : F \to K$ be a field isomorphism, and let $f(x) \in F[x]$ be a nonconstant polynomial. If L is a splitting field of $f(x)$ over F, and M is a splitting field of $\alpha(f(x))$ over K, then there is an isomorphism $\beta : L \to M$ such that β and α agree on F.*

Proof. We proceed by induction on $n = \deg(f(x))$. If $n = 1$, then we can only have $L = F$ and $M = K$. Thus, letting $\beta = \alpha$ will suffice. Assume that the result is true for polynomials of degree $n - 1$. As $f(x)$ is a product of irreducibles in $F[x]$, let us say that $f(x) = g(x)h(x)$, where $g(x)$ is irreducible and $h(x) \in F[x]$. Let a be a root of $g(x)$ in L and b a root of $\alpha(g(x))$ in M. By the preceding lemma, there is an isomorphism $\gamma : F(a) \to K(b)$ such that γ agrees with α on F and $\gamma(a) = b$. We have $f(x) = (x - a)u(x)$, for some $u(x) \in F(a)[x]$, by Theorem 11.2. Also, $\gamma(f(x)) = (x - \gamma(a))\gamma(u(x)) = (x - b)\gamma(u(x))$ in $K(b)[x]$. Now, L is a splitting field for $u(x)$ over $F(a)$ and M is a splitting field for $\gamma(u(x))$ over $K(b)$. Since $\deg(u(x)) = n - 1$, our inductive hypothesis completes the proof. □

Corollary 12.2. *Let F be a field and $f(x) \in F[x]$ a nonconstant polynomial. Then any two splitting fields of $f(x)$ over F are isomorphic.*

Proof. In the preceding theorem, let $\alpha : F \to F$ be the identity automorphism. □

Exercises

12.31. Construct an extension field F of $\mathbb{Z}_7$ having order 7^3. In particular, if $F = \mathbb{Z}_7(a)$, what do all of the elements of F look like? To which of these elements is $(a^2 + 5a + 4)(3a^2 + 6)$ equal?

12.32. Construct an extension field F of $\mathbb{Z}_3$ having order 81. In particular, if $F = \mathbb{Z}_3(a)$, what do all of the elements of F look like? To which of these elements is $(a^3 + 2a^2 + 2)(2a^2 + a + 1)$ equal?

12.33. Show that $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting field of $x^3 - 2$ over $\mathbb{Q}$, where $\omega \in \mathbb{C}$, $\omega^3 = 1$, but $\omega \neq 1$.

12.34. Let F be a field and $f(x) \in F[x]$ a nonconstant polynomial. If K is a splitting field of $f(x)$ over F and L is any extension field of F, suppose that $\alpha : K \to L$ is a homomorphism satisfying $\alpha(c) = c$ for all $c \in F$. If $a \in K$ is a root of $f(x)$, show that $\alpha(a)$ is also a root of $f(x)$.

12.35. Find every automorphism of $\mathbb{Q}(\sqrt{2})$.

12.36. Construct a splitting field for $x^3 + 2x + 1$ over $\mathbb{Z}_3$. Show that it has degree 3 over $\mathbb{Z}_3$.

12.37. Let F be any field and $f(x) \in F[x]$ a nonconstant polynomial. If we let $g(x) = f(x + 1)$, show that $f(x)$ and $g(x)$ have the same splitting fields over F.

12.38. Let F be a field and $f(x) \in F[x]$ a polynomial with $\deg(f(x)) = n \in \mathbb{N}$. Show that $f(x)$ has a splitting field K over F with $[K : F] \leq n!$.

12.5 Applications to Finite Fields

Let us see what we can deduce about finite fields. If F is a finite field, we know that its prime subfield must be isomorphic to $\mathbb{Z}_p$, for some prime p. By Theorem 12.7, F must have order p^n, for some positive integer n. We will construct a field of order p^n and show that, up to isomorphism, there is only one such field.

The following concept looks suspiciously like calculus, but is not.

Definition 12.14. Let F be a field and $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$. Then the **formal derivative** of $f(x)$ is $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$.

Note that this has nothing whatsoever to do with limits, as limits do not necessarily make sense in an arbitrary field. The formula happens to agree with the one used for the derivative of real polynomials. We will also not be disturbed by the fact that the following lemma extends the similarity to calculus.

Lemma 12.5. *Let F be a field, $f(x), g(x) \in F[x]$ and $a \in F$. Then*

1. $(af(x))' = af'(x)$;
2. $(f(x) + g(x))' = f'(x) + g'(x)$; *and*
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Proof. The first two parts follow immediately from the definition. The third is left as Exercise 12.40. □

Definition 12.15. Let F be a field, $f(x) \in F[x]$ and $a \in F$. We say that a is a **multiple root** of $f(x)$ if $(x - a)^2 | f(x)$.

Example 12.33. In $\mathbb{Q}[x]$, 2 is a multiple root of $x^5 - 4x^4 + 7x^3 - 7x^2 - 8x + 20$, since the polynomial factors as $(x - 2)^2(x^3 + 3x + 5)$.

Theorem 12.14. *Let F be a field, $f(x) \in F[x]$ and let $a \in F$ be a root of $f(x)$. Then a is a multiple root of $f(x)$ if and only if $f'(a) = 0$.*

Proof. Suppose that a is a multiple root of $f(x)$, say $f(x) = (x-a)^2 g(x)$, with $g(x) \in F[x]$. Then by Lemma 12.5, $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x)$. Thus, $f'(a) = 0$. Conversely, suppose that $f'(a) = 0$. By Theorem 11.2, $f(x) = (x-a)h(x)$, for some $h(x) \in F[x]$. Thus, $f'(x) = h(x) + (x-a)h'(x)$. As $f'(a) = 0$, we have $0 = h(a) + (a-a)h'(a) = h(a)$. By Theorem 11.2, $(x-a) | h(x)$, and hence $(x-a)^2 | f(x)$. □

Corollary 12.3. *Let F be a field and let $f(x) \in F[x]$ be irreducible. Let K be a splitting field of $f(x)$ over F. If $f(x)$ has a multiple root in K, then $f'(x)$ is the zero polynomial.*

Proof. Let a be the multiple root. Then (multiplying $f(x)$ by a suitable element of F to make it monic), we see that $f(x)$ is the minimal polynomial of a over F. By Theorem 12.10, $f(x) | f'(x)$. But if $f'(x) \neq 0$, then $\deg(f'(x)) < \deg(f(x))$, which is impossible. Therefore, $f'(x)$ is the zero polynomial. □

Definition 12.16. A field F is said to be **perfect** if no irreducible $f(x) \in F[x]$ has multiple roots in any splitting field of $f(x)$ over F.

We digress from our discussion of finite fields to mention the following.

Theorem 12.15. *Every field of characteristic zero is perfect.*

Proof. If $f(x) = a_0 + \cdots + a_n x^n$, with $a_n \neq 0$ and $n \geq 1$, then $f'(x) = a_1 + \cdots + n a_n x^{n-1}$ has leading coefficient $n a_n \neq 0$. Thus, $f'(x)$ is not the zero polynomial. Apply Corollary 12.3. □

Actually, finite fields are perfect too! Let us see why.

Lemma 12.6. *Let F be a finite field of characteristic p. Then the function $\alpha : F \to F$ given by $\alpha(a) = a^p$ is an automorphism.*

Proof. Since F is commutative, $\alpha(ab) = (ab)^p = a^p b^p = \alpha(a)\alpha(b)$, for all $a, b \in F$. By Theorem 8.14, $\alpha(a+b) = (a+b)^p = a^p + b^p = \alpha(a) + \alpha(b)$. If $a^p = 0$, then since F is a field, $a = 0$. Thus, α is one-to-one. Since F is finite, α is onto as well. □

Theorem 12.16. *Every finite field is perfect.*

Proof. Suppose that F has characteristic p. Let $f(x) \in F[x]$ be irreducible. Suppose that $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. If $f(x)$ has multiple roots in a splitting field, then by Corollary 12.3, $f'(x) = 0$. Thus, $k a_k = 0$, for $1 \leq k \leq n$. If $p \nmid k$, then as $(k, p) = 1$, we may write $ku + pv = 1$, for some $u, v \in \mathbb{Z}$. Therefore, $a_k = uka_k + pva_k = 0 + 0 = 0$. Thus,

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{mp} x^{mp}.$$

In view of the preceding lemma, there exist $b_i \in F$ such that $b_i^p = a_{ip}$. But now Theorem 8.14 tells us that

$$\begin{aligned}(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m)^p &= b_0^p + b_1^p x^p + \cdots + b_m^p x^{mp} \\ &= a_0 + a_p x^p + \cdots + a_{mp}x^{mp} \\ &= f(x).\end{aligned}$$

That is, $f(x)$ is reducible. This contradiction completes the proof. □

What would an imperfect field look like? Clearly, it would have to be an infinite field of prime characteristic. Exercise 12.44 shows how to construct an imperfect field.

Back to the finite fields!

Lemma 12.7. *Let F be a field of prime characteristic p and let n be a positive integer. If $K = \{a \in F : a^{p^n} = a\}$, then K is a subfield of F.*

Proof. See Exercise 8.40.

Theorem 12.17. *Let p be a prime and n a positive integer. Then a field F has order p^n if and only if it is a splitting field of $x^{p^n} - x$ over the prime subfield, (an isomorphic copy of) $\mathbb{Z}_p$.*

Proof. Let F have order p^n. Then $U(F)$ has order $p^n - 1$. Thus, if $0 \neq a \in F$, then $a^{p^n-1} = 1$, and hence $a^{p^n} - a = 0$. Clearly, $0^{p^n} - 0 = 0$ as well. Thus, every element of F is a root of $x^{p^n} - x$. By Corollary 11.3, $x^{p^n} - x$ can only have p^n roots. Thus, $x^{p^n} - x$ splits over F, and surely it cannot split over any smaller field, as all of the roots must be present. Therefore, F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Conversely, let F be a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. By Lemma 12.7, the roots of $x^{p^n} - x$ form a subfield K of F. Since $x^{p^n} - x$ splits over K, we must have $F = K$. Furthermore, the formal derivative of $x^{p^n} - x$ is -1, which has no roots. Therefore, by Theorem 12.14, $x^{p^n} - x$ has no multiple roots. In particular, $|F| = p^n$, as required. □

Theorem 12.18. *If k is a positive integer, then there is a field of order k if and only if $k = p^n$ for some prime p and positive integer n. All fields of order p^n are isomorphic.*

Proof. By Theorem 12.7, a finite field must have order p^n. Theorem 12.12 tells us that $x^{p^n} - x$ has a splitting field over $\mathbb{Z}_p$. By Theorem 12.17, this splitting field has order p^n. But Theorem 12.17 also says that every field of order p^n is such a splitting field. By Corollary 12.2, these splitting fields are isomorphic. □

The unique (up to isomorphism) field of order p^n is called the **Galois field** of order p^n.

We can also determine the subfields of a finite field. In order to do so, we will need the following theorem, which is of interest on its own.

Theorem 12.19. *Let F be a field. Then any finite subgroup G of $U(F)$ is cyclic.*

Proof. Since G is a finite abelian group, Theorem 5.3 tells us that it is a direct product of cyclic groups. If all of these cyclic groups have relatively prime orders, then by Theorem 5.4, G is cyclic, and we are done. Otherwise, we may assume that G has a subgroup $\langle a\rangle \times \langle b\rangle$, and there exists a prime p dividing the orders of a and b. By Cauchy's theorem, $\langle a\rangle$ and $\langle b\rangle$ each contain an element of order p. Thus, G has a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. But every element of $\mathbb{Z}_p \times \mathbb{Z}_p$ has order 1 or p. That is, we have at least p^2 roots for the polynomial $x^p - 1 \in F[x]$, which has degree p, giving us a contradiction and completing the proof. □

Theorem 12.20. *Let F be a field of order p^n, for some prime p and positive integer n. Then every subfield of F has order p^m, for some positive divisor m of n. Furthermore, for each positive divisor m of n, F has exactly one subfield of order p^m, namely $\{a \in F : a^{p^m} = a\}$.*

Proof. Let K be a subfield of F. Then K and F have the same prime subfield, (an isomorphic copy of) $\mathbb{Z}_p$. By Theorems 12.7 and 12.8,

$$n = [F : \mathbb{Z}_p] = [F : K][K : \mathbb{Z}_p].$$

In particular, if $[K : \mathbb{Z}_p] = m$, then $|K| = p^m$ and $m|n$.

Let m be a divisor of n and let $K = \{a \in F : a^{p^m} = a\}$. By Lemma 12.7, K is a subfield of F. Furthermore, the preceding theorem tells us that $U(F)$ is cyclic of order $p^n - 1$. In addition,

$$p^n - 1 = (p^m - 1)(1 + p^m + p^{2m} + p^{3m} + \cdots + p^{n-m}).$$

Thus, $(p^m - 1)|(p^n - 1)$. By Corollary 3.3, $U(F)$ has a subgroup G of order $p^m - 1$. But every element a of G satisfies $a^{p^m - 1} = 1$, and hence $a^{p^m} = a$. That is $G \subseteq K$. Also, $0 \in K$, and therefore K has at least p^m elements. But every element of K is a root of $x^{p^m} - x$, and therefore K can have at most p^m elements.

To prove the uniqueness of this subfield, suppose that L is another subfield of F with p^m elements. Then $U(K)$ and $U(L)$ are both subgroups of order $p^m - 1$ in $U(F)$. However, Corollary 3.3 tells us that $U(F)$ has only one such subgroup. Therefore, $U(K) = U(L)$. As the unit group of a field consists of everything except 0, we have $K = L$, as required. □

Exercises

12.39. Find the smallest field containing exactly 3 proper subfields.

12.40. Let F be a field and $f(x), g(x) \in F[x]$. Show that $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

12.41. Let $f(x) \in \mathbb{Z}_5[x]$ be an irreducible polynomial of degree 3. If K is a splitting field of $f(x)$ over $\mathbb{Z}_5$, show that $|K| = 5^3$ or 5^6.

12.42. Let K be a field of order p^n for some prime p and positive integer n, having subfields F and L of orders p^m and p^r, respectively. Find the order of $F \cap L$.

12.43. Let F be a field and $f(x) \in F[x]$ an irreducible polynomial having a multiple root in some extension field of F. Show that char $F = p$ for some prime p, $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{mp} x^{mp}$ for some $a_i \in F$, and that at least one of the a_i is transcendental over the prime subfield of F.

12.44. Let $\mathbb{Z}_2[t]$ be a polynomial ring over $\mathbb{Z}_2$ and $F = \mathbb{Z}_2(t)$ its field of fractions. Show that the polynomial $x^2 - t \in F[x]$ is irreducible over F, but that it has a multiple root in some extension field of F. In particular, conclude that F is not a perfect field.

12.45. Theorem 12.19 tells us that the unit group of a finite field is cyclic. If char $F \neq 2$, show that the unit group of an infinite field is not cyclic.

12.46. Suppose char $F = 2$. Let us prove that the preceding exercise still holds. Suppose, to the contrary, that $U(F)$ is cyclic. Let $U(F) = \langle a \rangle$.

1. Show that $F = \mathbb{Z}_2(a)$.
2. If a is algebraic over $\mathbb{Z}_2$, show that F is finite, and we are done.
3. If a is transcendental over $\mathbb{Z}_2$, show that there exists an integer n such that $a^n = a + 1$, and obtain a contradiction.

12.47. Suppose we wrote $x^{125} - x$ as a product of irreducibles over $\mathbb{Z}_5$. Show that each of these irreducible polynomials has degree 1 or 3. (Please do not actually write the polynomials!)

12.48. Show that for every prime p and positive integer n, there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.

Reference

1. Baker, A.: Transcendental Number Theory, 2nd edn. Cambridge University Press, Cambridge (1990)