# Chapter 2

# Field Extensions

This chapter introduces the primary terminology that will be used throughout the module. Galois Theory is essentially the study of fields satisfying $F \subseteq K$; that is, what we call a field extension. We shall present here the basic technology required to work with such extensions.

**Definition 2.1** Let $F$ and $K$ be fields such that $F$ is a subfield of $K$. We then say that $K$ is an *extension* of $F$. We also call $F$ the *base field* of the extension.

In particular, note that every field is an extension of its prime subfield. The point of this definition, though, is a change of perspective. We are not viewing a field extension $F \subseteq K$ as being the situation where we start with a field $K$ and then pass to a subfield $F$. Instead, the philosophy here will be much more starting with a base field $F$ and then creating a bigger field $K$ containing $F$ that is the extension. We shall flesh out this viewpoint initially over the course of the chapter and subsequently over the whole module.

## The degree of an extension

The first observation to make in this setting is that if the field $K$ is an extension of the field $F$, then $K$, in particular, satisfies the following conditions:

- $K$ forms an abelian group under addition;
- we can multiply elements of $K$ by elements of $F$;
- $a(x + y) = ax + ay$ for all $a \in F$ and $x, y \in K$;
- $(a + b)x = ax + bx$ for all $a, b \in F$ and $x \in K$;
- $(ab)x = a(bx)$ for all $a, b \in F$ and $x \in K$;
- $1x = x$ for all $x \in K$.

Thus, we can view $K$ as a *vector space* over the field $F$.

**Definition 2.2** Let the field $K$ be an extension of the field $F$.

(i) The *degree* of $K$ over $F$ is the dimension of $K$ when viewed as a vector space over $F$. We denote this by $|K : F|$. Thus

$$|K : F| = \dim_F K.$$

(ii) If the degree $|K : F|$ is finite, we say that $K$ is a *finite extension* of $F$.

**Warning:** Note that saying $K$ is a finite extension of $F$ does *not* mean that $K$ is a finite field. There are many situations where both fields have infinitely many elements in them. It refers precisely to the dimension of the bigger field over the smaller field.

**Example 2.3** (i) The field $\mathbb{C}$ of complex numbers is an extension of the field $\mathbb{R}$ of real numbers. Every complex number can be written as $x + iy$ where $x, y \in \mathbb{R}$ and it follows that $\{1, i\}$ is a basis for the set of complex numbers when viewed as a real vector space. Hence

$$|\mathbb{C} : \mathbb{R}| = 2;$$

that is, this is a degree 2 extension.

(ii) The field $\mathbb{R}$ of real numbers is an extension of the field $\mathbb{Q}$ of rational numbers. Any finite dimensional vector space $V$ over $\mathbb{Q}$ is countable, since if $\{v_1, v_2, \ldots, v_n\}$ is a basis for $V$ over $\mathbb{Q}$, then there are countably many elements of the form

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

with $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Q}$. Since $\mathbb{R}$ is uncountable, we conclude that $\mathbb{R}$ is not a finite extension of $\mathbb{Q}$; it has infinite degree over $\mathbb{Q}$.

**Theorem 2.4 (Tower Law)** *Let $F \subseteq K \subseteq L$ be field extensions. Then $L$ is a finite extension of $F$ if and only if $L$ is a finite extension of $K$ and $K$ is a finite extension of $F$. In such a case,*

$$|L : F| = |L : K| \cdot |K : F|.$$

PROOF: First suppose that $L$ is a finite extension of $F$. This means that, when viewed as a vector space over $F$, $L$ is finite-dimensional. Now $K \subseteq L$ and $K$ is closed under addition and by multiplication by elements of $F$ (since it is a field). Hence $K$ is a subspace of $L$, when viewed as a vector space over $F$, and so is also finite-dimensional over $F$.

Let $\mathscr{B} = \{x_1, x_2, \ldots, x_k\}$ be a basis for $L$ over $F$. Then every element of $L$ can be written in the form

$$a_1 x_1 + a_2 x_2 + \cdots + a_k x_k \tag{2.1}$$

where $a_1, a_2, \ldots, a_k \in F$. Therefore, every element of $L$ can also be written in the form (2.1) where we choose the coefficients $a_i$ from the field $K$. (We certainly get all the linear combinations built using scalars from $F$ and cannot produce elements outside $L$ since $K$ is a subfield of $L$.) Hence $\mathscr{B}$ spans $L$ when viewed as vector space over $K$ and so we conclude $|L : K| < \infty$.

Conversely, suppose that both $|L : K|$ and $|K : F|$ are finite. Let $\{v_1, v_2, \ldots, v_m\}$ be a basis for $L$ over $K$ and let $\{w_1, w_2, \ldots, w_n\}$ be a basis for $K$ over $F$. We claim that the set of products $\mathscr{B} = \{\, v_i w_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n \,\}$ is a basis for $L$ over $F$.

First note that if $x \in L$, then we can express $x$ in terms of the basis for $L$ over $K$, to deduce that there exist $a_1, a_2, \ldots, a_m \in K$ such that

$$x = \sum_{i=1}^{m} a_i v_i.$$

Now, for each $i$, express $a_i$ in terms of the basis for $K$ over $F$ to find $b_{i1}, b_{i2}, \ldots, b_{in} \in F$ such that

$$a_i = \sum_{j=1}^{n} b_{ij} w_j.$$

Substitute this into the previous sum to conclude

$$x = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} v_i w_j$$

and we conclude that $\mathscr{B}$ does indeed span $L$ as a vector space over $F$.

Now suppose that for some coefficients $c_{ij} \in F$ such that

$$\sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} v_i w_j = 0.$$

First express this as

$$\sum_{i=1}^{m} \Big( \sum_{j=1}^{n} c_{ij} w_j \Big) v_i = 0$$

and use the fact that $\{v_1, v_2, \ldots, v_m\}$ is a basis for $L$ over $K$ to conclude that, for $i = 1, 2, \ldots, m$, the elements

$$\sum_{j=1}^{n} c_{ij} w_j$$

in $K$ are all equal to 0. Now use the fact that $\{w_1, w_2, \ldots, w_n\}$ is a basis for $K$ over $F$ to deduce

$$c_{ij} = 0 \qquad \text{for all } i \text{ and } j.$$

We therefore conclude that $\mathscr{B}$ is indeed a basis for $L$ over $F$. In conclusion, $L$ is a finite extension of $F$ and

$$|L : F| = |\mathscr{B}| = mn = |L : K| \cdot |K : F|.$$

□

**Comment:** We shall need the observation made in the course of the proof later, so we make this explicit: In the setting of the theorem, if $\{v_1, v_2, \ldots, v_m\}$ is a basis for $L$ over $K$ and $\{w_1, w_2, \ldots, w_n\}$ is a basis for $K$ over $F$, then $\{ v_i w_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n \}$ is a basis for $L$ over $F$.

## Algebraic elements and algebraic extensions

The central results presented in this module will concern finite extensions and accordingly we seek to establish detailed information about such extensions. The first step is understand the concept of algebraic elements and their link to polynomial equations. Later in this chapter we shall show that we can characterize finite extensions in terms of algebraic elements.

**Definition 2.5** Let the field $K$ be an extension of the field $F$.

(i) An element $\alpha \in K$ is said to be *algebraic* over $F$ if there exists a non-zero polynomial $f(X) \in F[X]$ such that $f(\alpha) = 0$. When this holds, we shall say that $\alpha$ satisfies the polynomial equation $f(X) = 0$.

(ii) We say that $K$ is an *algebraic extension* of $F$ if every element of $K$ is algebraic over $F$.

Thus to say that an element $\alpha \in K$ is algebraic over the subfield $F$ is to say that there are coefficients $b_0$, $b_1$, …, $b_n$ in $F$ such that

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0.$$

The first observation to make is that every element $\alpha$ of the base field $F$ is algebraic over $F$ since it is a root of the polynomial $X - \alpha$. The interesting question is then which other elements of $K$ also happen to be algebraic over $F$. Indeed in the context of finite extensions, our first, and important, observation is the following.

**Lemma 2.6** *Every finite extension is an algebraic extension.*

PROOF: Let $K$ be an extension of $F$ of degree $n$. Let $\alpha \in K$. Then the $n+1$ elements

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

are linearly independent over $F$, so there exist coefficients $b_0$, $b_1$, ..., $b_n$ in $F$, not all of which are zero, such that

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0.$$

Hence $\alpha$ satisfies a non-zero polynomial over $F$ (namely $f(X) = b_0 + b_1X + \cdots + b_nX^n$), so is algebraic over $F$. □

## Simple extensions

To continue our investigation of finite extensions, we introduce the following notation to describe how a field extension is formed. It enables us to view an extension as formed from a base field by introducing further elements.

**Definition 2.7** Let the field $K$ be an extension of the field $F$ and $\alpha_1$, $\alpha_2$, ..., $\alpha_n$ be elements of $K$. We write

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

for the smallest subfield of $K$ that contains both $F$ and the elements $\alpha_1$, $\alpha_2$, ..., $\alpha_n$.

It is straightforward to verify that the intersection of a collection of subfields of $K$ is again a subfield (see Problem Sheet I, Question 2; one just needs to verify the conditions listed in Chapter 1 on page 7). Consequently, the "smallest subfield" containing $F$ and the elements $\alpha_1$, $\alpha_2$, ..., $\alpha_n$ makes sense: it is the intersection of all the subfields of $K$ that contain this collection of elements. It is possible to describe more explicitly the elements of the field $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ in general, but we shall mainly concentrate on a special case.

**Definition 2.8** We say that the field $K$ is a *simple extension* of the field $F$ if $K = F(\alpha)$ for some $\alpha \in K$. We then also say that $K$ is obtained by *adjoining the element* $\alpha$ to $F$.

Simple extensions will be of great importance. In the case that $\alpha$ is algebraic over $F$, we shall have a precise description of elements in the simple extension $F(\alpha)$ and good knowledge of the degree $|F(\alpha) : F|$ (see Theorem 2.14 below). For a general extension $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ obtained by adjoining a finite collection of elements to a base field $F$, we can view this as a chain of simple extensions,

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

since at each stage $F(\alpha_1, \ldots, \alpha_i)$ is the simple extension obtained by adjoining the element $\alpha_i$ to the previous subfield $F(\alpha_1, \ldots, \alpha_{i-1})$.

**Example 2.9** Let $F$ be a field and $X$ be an indeterminate. The field $F(X)$ of rational functions is a simple extension of $F$.

Indeed, in Proposition 1.27 we observed that $F$ occurs as a subfield of $F(X)$, so $F(X)$ is indeed an extension of $F$. The elements of $F(X)$ has the form $f(X)/g(X)$ where $f(X)$ and $g(X)$

are polynomials with coefficients from $F$. Now if $L$ is any subfield of $F(X)$ that contains the subfield $F$ and the element $X$, then it first contains all polynomials in $X$, since $L$ is closed under multiplication and addition. It is also closed under quotients and hence contains all quotients $f(X)/g(X)$ where $f(X)$ and $g(X)$ are polynomials. Therefore $L = F(X)$. We conclude that $F(X)$ indeed equals its smallest subfield containing $F$ and the indeterminate $X$.

Thus the field $F(X)$ of rational functions is the simple extension of $F$ obtained by adjoining the indeterminate $X$. In particular, the notation $F(X)$ as introduced in Definition 1.26 is consistent with that in Definition 2.8. Moreover, $X$ is not an algebraic element over $F$: if $b_0$, $b_1$, $\ldots$, $b_n$ are elements of $F$, not all of which are zero, then

$$b_0 + b_1X + b_2X^2 + \cdots + b_nX^n$$

is some non-zero polynomial $f(X)$ and so non-zero in the field $F(X)$ of rational functions. The term *transcendental* is used for an element that is not algebraic over the base field. Thus the indeterminate $X$ as used in $F(X)$ is transcendental over the base field $F$. In fact, it turns out — though less central to this module — that if $\alpha$ is any transcendental element over the base field $F$, then the simple extension $F(\alpha)$ is isomorphic to the field $F(X)$ of rational functions.

## Minimum polynomials

We shall be most interested in simple extensions $F(\alpha)$ where $F$ is algebraic over the base field $F$. The most important definition we need in this context is the following:

**Definition 2.10** Let $F$ be a field and $\alpha$ be an element in some field extension of $F$ such that $\alpha$ is algebraic over $F$. The *minimum polynomial* of $\alpha$ over $F$ is the monic polynomial $f(X)$ of least degree in $F[X]$ such that $f(\alpha) = 0$.

Recall that a polynomial is *monic* if its leading term has coefficient 1. (The minimum polynomial is also sometimes called the "minimal polynomial" in some sources.)

One can apply very similar arguments to those used in linear algebra to establish quite directly that the minimum polynomial of an algebraic element exists and is unique. We shall, however, use a more ring-theoretic flavour of argument since that will also set up the technology we shall use to understand the structure of a simple extension.

Let $\alpha$ be an element in some extension of the field $F$ that is algebraic over $\alpha$. Define a map $\phi\colon F[X] \to F(\alpha)$ by evaluating a polynomial at $\alpha$:

$$\phi\colon g(X) \mapsto g(\alpha).$$

We shall first observe that $\phi$ is a ring homomorphism. This is actually quite straightforward and depends upon only the ring axioms holding in the field $F(\alpha)$, but we shall check this explicitly.

Consider two polynomial $g(X), h(X) \in F[X]$, say

$$g(X) = \sum a_iX^i \qquad \text{and} \qquad h(X) = \sum b_iX^i$$

(where we understand that these are finite sums: all but finitely many $a_i$ and $b_i$ are zero). Then

$$\begin{aligned} g(X)\phi + h(X)\phi &= g(\alpha) + h(\alpha) \\ &= \sum a_i\alpha^i + \sum b_i\alpha^i \\ &= \sum (a_i + b_i)\alpha^i \\ &= (g + h)(\alpha) \\ &= \big(g(X) + h(X)\big)\phi \end{aligned}$$

and

$$\begin{aligned} g(X)\phi \cdot h(X)\phi &= g(\alpha)\, h(\alpha) \\ &= \Big(\sum a_i \alpha^i\Big)\Big(\sum b_i \alpha^i\Big) \\ &= \sum c_i \alpha^i, \end{aligned}$$

where $c_i = \sum_{j=0}^{i} a_j b_{i-j}$, by the distributive laws. Note $g(X)\, h(X) = \sum c_i X^i$, by definition, so

$$g(X)\phi \cdot h(X)\phi = \big(g(X)\, h(X)\big)\phi.$$

Hence $\phi$ is a ring homomorphism. The First Isomorphism Theorem (Theorem 1.6) tells us that

$$\frac{F[X]}{\ker \phi} \cong \operatorname{im} \phi$$

and $\operatorname{im} \phi$ is some subring of $F(\alpha)$. (The latter field contains $F$, $\alpha$ and is closed, in particular, under products and sums, so necessarily contains all $g(\alpha)$.) The assumption that $\alpha$ is algebraic ensures there are non-zero polynomials $g(X)$ satisfying $g(\alpha) = 0$; that is, $\ker \phi \neq \mathbf{0}$. The fact that $F[X]$ is a principal ideal domain tells us that

$$\ker \phi = \big(f(X)\big)$$

for some polynomial $f(X)$. Moreover, the proof of Proposition 1.16 tells us that $\deg f(X)$ is minimal amongst all non-zero polynomials $g(X)$ in $\ker \phi$; that is, amongst all non-zero polynomials $g(X)$ satisfying $g(\alpha) = 0$. Finally, note that the scalars are units in $F[X]$, so we may divide by the coefficient of the leading terms of $f(X)$, without changing the ideal generated by $f(X)$, and hence assume $f(X)$ is monic; that is, $f(X)$ is the *minimum polynomial* of $\alpha$ over $F$.

We have therefore established the first two parts of the following lemma that describes the main properties of the minimum polynomial. The others can be deduced quickly, as we now demonstrate, from what we have done.

**Lemma 2.11** *Let $F$ be a field and $\alpha$ be an element in some field extension of $F$ such that $\alpha$ is algebraic over $F$. Then*

(i) *the minimum polynomial $f(X)$ of $\alpha$ over $F$ exists;*

(ii) *the map $\phi\colon F[X] \to F(\alpha)$ given by $g(X) \mapsto g(\alpha)$ (that is, evaluating each polynomial at $\alpha$) is a ring homomorphism with kernel $\ker \phi = \big(f(X)\big)$;*

(iii) *the minimum polynomial $f(X)$ of $\alpha$ over $F$ is irreducible over $F$;*

(iv) *if $g(X) \in F[X]$, then $g(\alpha) = 0$ if and only if the minimum polynomial $f(X)$ of $\alpha$ over $F$ divides $g(X)$;*

(v) *the minimum polynomial $f(X)$ of $\alpha$ over $F$ is unique;*

(vi) *if $g(X)$ is any monic polynomial over $F$ such that $g(\alpha) = 0$, then $g(X)$ is the minimum polynomial of $\alpha$ over $F$ if and only if $g(X)$ is irreducible over $F$.*

Proof: (iii) Suppose $f(X)$ is reducible over $F$. Then $f(X) = g_1(X)\, g_2(X)$ for some (necessarily non-zero) polynomials $g_1(X)$ and $g_2(X)$ of smaller degree than $f(X)$. Then

$$0 = f(\alpha) = g_1(\alpha)\, g_2(\alpha).$$

Since $F(\alpha)$ is a field, either $g_1(\alpha) = 0$ or $g_2(\alpha) = 0$. However, this then contradicts the assumption that $f(X)$ has smallest degree among polynomials satisfied by $\alpha$.

We conclude that $f(X)$ is indeed irreducible.

(iv) This follows from (ii):

$$\begin{aligned} g(\alpha) = 0 \qquad & \text{if and only if} \qquad g(X) \in \ker \phi = \big(f(X)\big) \\ & \text{if and only if} \qquad f(X) \text{ divides } g(X). \end{aligned}$$

(v) Suppose that $g(X)$ is a polynomial of the same smallest degree as $f(X)$ such that $g(\alpha) = 0$. Then, by (iv), $g(X)$ is a multiple of $f(X)$; say, $g(X) = f(X)\,h(X)$ for some polynomial $h(X)$. However, $\deg g(X) = \deg f(X)$, so we conclude $h(X)$ must be a constant polynomial. Thus $g(X) = c\,f(X)$ for some scalar $c \in F$. Consequently, if $f(X)$ and $g(X)$ are both *monic*, then $c = 1$. Hence the monic polynomial $f(X)$ of least degree such that $f(\alpha) = 0$ is unique.

(vi) This is essentially a corollary of (iii) and (iv).
$\Rightarrow$: If $g(X)$ is not irreducible, then it cannot be the minimum polynomial of $\alpha$ by part (i).
$\Leftarrow$: Conversely suppose $g(X)$ is irreducible. By (iv), $g(X) = f(X)\,h(X)$ for some polynomial $h(X)$. Since $g(X)$ is irreducible and $f(X)$ is not constant, we conclude that $h(X)$ is constant. Hence $g(X) = c\,f(X)$ for some scalar $c$ and the fact that both polynomials are monic forces $c = 1$. Therefore $g(X) = f(X)$ is the minimum polynomial of $\alpha$ over $F$. □

We now have enough of the basic theory of minimum polynomials that we can find them in some of the more straightforward examples. Other examples can be quite difficult, but some of the theory that we develop later in this section will be useful for the problem of determining the degree of a simple extension.

**Example 2.12** *Show that the following complex numbers are algebraic over $\mathbb{Q}$ and determine their minimum polynomials over $\mathbb{Q}$:*

(i) $\sqrt{m}$*, where $m$ is an integer such that $p \mid m$, for some prime $p$, but $p^2 \nmid m$;*
(ii) $\sqrt[3]{2}$*;* (iii) $\mathrm{e}^{2\pi i/3}$.

Solution: (i) First observe that $\sqrt{m}$ is a root of the polynomial $f(X) = X^2 - m$. Hence $\sqrt{m}$ is algebraic over $\mathbb{Q}$ as it satisfies some polynomial with rational coefficients. Moreover, $X^2 - m$ is irreducible (since our choice of $m$ together with the property of the prime $p$ ensures that Eisenstein's Criterion (Theorem 1.23) applies to $f(X)$. Hence $X^2 - m$ is the minimum polynomial of $\sqrt{m}$ over $\mathbb{Q}$.

Note that it also follows from this that $\sqrt{m} \notin \mathbb{Q}$, since otherwise we would be able to factorize $f(X)$ into two linear factors: $X^2 - m = (X - \sqrt{m})(X + \sqrt{m})$, contrary to the quadratic polynomial being irreducible over $\mathbb{Q}$.

(ii) The cube root $\sqrt[3]{2}$ is a root of the polynomial $g(X) = X^3 - 2$. Hence $\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$. Moreover, $X^3 - 2$ is irreducible by Eisenstein's Criterion. Therefore $X^3 - 2$ is the minimum polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.

(iii) Let $\omega = \mathrm{e}^{2\pi i/3}$. Note that $\omega^3 = 1$, so $\omega$ is a root of $X^3 - 1$. Hence $\omega$ is indeed algebraic over $\mathbb{Q}$. However, $X^3 - 1$ is not irreducible: for a start, $1 \in \mathbb{Q}$ is also a root of that polynomial. Instead, observe

$$\omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1),$$

so, since $\omega \neq 1$, we deduce $\omega$ is also a root of the polynomial $h(X) = X^2 + X + 1$. The latter must be irreducible, since if it were not then it would be a product of two linear factors, one of which would have to be $X - \omega$, yet $\omega \notin \mathbb{Q}$ so this is not possible. Hence $X^2 + X + 1$ is the minimum polynomial of $\omega = \mathrm{e}^{2\pi i/3}$ over $\mathbb{Q}$. □

**Comment:** Note that the minimum polynomial of an algebraic element $\alpha$ depends upon the particular base field. For example, a special case of Example 2.12(i) is that $\sqrt{2}$ has minimum polynomial over $X^2 - 2$ over $\mathbb{Q}$, whereas its minimum polynomial over $\mathbb{R}$ is $X - \sqrt{2}$.

If we concentrate our efforts on simple extensions $F(\alpha)$ with $\alpha$ algebraic over the base field $F$, there are two questions that naturally arise and whose answers will enable us to make progress:

(i) Given an irreducible polynomial $f(X)$ over the field $F$, can we construct a simple extension $F(\alpha)$ such that the minimum polynomial of $\alpha$ over $F$ is $f(X)$?

(ii) If $\alpha$ is algebraic over $F$, what is the structure of the simple extension $F(\alpha)$ and in what way is this determined by the minimum polynomial of $\alpha$ over $F$?

These questions essentially boil down to the existence of simple extensions and to then investigating their properties (and essentially establishing uniqueness as a consequence). Note that in answering the first question in the affirmative, as we do in the following theorem, we are showing that we can always *adjoin a root $\alpha$ of an irreducible polynomial to a field $F$* to construct some simple extension $F(\alpha)$.

**Theorem 2.13** *Let $F$ be a field and $f(X)$ be a monic irreducible polynomial over $F$. Then there exists a simple extension $F(\alpha)$ of $F$ such that $\alpha$ is algebraic over $F$ with minimum polynomial $f(X)$.*

The ideas discussed when establishing Lemma 2.11 give us a hint as to how to construct the simple extension. We shall construct it using the quotient ring $F[X]/(f(X))$ of the polynomial ring $F[X]$ by the ideal generated by $f(X)$.

PROOF: Let $I = (f(X))$, the ideal of the polynomial ring $F[X]$ generated by $f(X)$, and let $K = F[X]/I$, the quotient ring of $F[X]$ by the ideal $I$. Certainly $K$ is a commutative ring with a 1. Note that the multiplicative identity is $I + 1$. Since $f(X)$ is irreducible, non-zero constant polynomials are not divisible by $f(X)$ (irreducibles are not units) and so $1 \notin I$; that is, the multiplicative identity $I + 1$ is non-zero.

Now if $g(X)$ is any polynomial such that $I + g(X)$ is non-zero (that is, $g(X) \notin I$), consider the greatest common divisor $h(X)$ of $f(X)$ and $g(X)$. Since $f(X)$ is irreducible, $h(X)$ is either a constant polynomial or a scalar multiple of $f(X)$. However, $f(X)$ does not divide $g(X)$, by assumption, so we conclude that $h(X)$ a constant. It follows therefore by the Euclidean Algorithm (Theorem 1.18) that there are polynomials $u(X), v(X) \in F[X]$ such that

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

Hence, in the quotient ring,

$$I + 1 = (I + u(X))(I + g(X)).$$

We conclude that every non-zero element of $K$ has a multiplicative inverse and thus $K$ is indeed a field.

Define the map $\iota\colon F \to K$ by

$$\iota\colon \lambda \mapsto I + \lambda.$$

The definition of addition and multiplication in the quotient ring $K$ ensures that $\iota$ is a homomorphism. It is injective, since if $\lambda\iota = \mu\iota$, then $\lambda - \mu \in I$, which forces $\lambda = \mu$ (as the only constant polynomial in $I = (f(X))$ is 0). Hence $\operatorname{im}\iota = \{\, I + \lambda \mid \lambda \in F \,\}$ is a subring of $K$ isomorphic to $K$; that is, $K$ is a field extension of a subfield isomorphic to $F$. Identifying $F$ with this isomorphic copy via $\iota$, we view $K$ as a field extension of $F$.

Finally, write $\alpha = I + X \in K$. Since every element of $K$ has the form $I + g(X)$, where $g(X) \in F[X]$, we see, using the definition of addition and multiplication in $K$, that every element

of $K$ is expressible as a sum $b_0 + b_1\alpha + \cdots + b_n\alpha^n$ for some non-negative integer $n$ and some $b_0, b_1, \ldots, b_n \in F$. Thus, the smallest subfield of $K$ containing the subfield $F$ and the element $\alpha$ is the whole field $K$; that is, $K = F(\alpha)$. Moreover, applying this to the polynomial $f(X)$, we calculate

$$f(\alpha) = f(I + X) = I + f(X) = I + 0;$$

that is, $\alpha$ satisfies the polynomial $f(X)$, so $\alpha$ is algebraic and, by Lemma 2.11(vi), the minimum polynomial of $\alpha$ is $f(X)$. □

**Comments:** There are two comments to make placing the above existence result for simple extensions in context.

(i) Although not stated in Chapter 1, the Correspondence Theorem for rings tells us that there is a one-one correspondence between ideals in the quotient ring $F[X]/I$, where $I = (f(X))$, and ideals in the polynomial ring $F[X]$ that contain $I$. We have shown that when $f(X)$ is irreducible, the quotient $K = F[X]/I$ is a field; that is, it has only two ideals $\mathbf{0}$ and $K$ itself. Therefore, via the correspondence, $I = (f(X))$ is a maximal ideal of the polynomial ring: there are no ideals $J$ satisfying $I < J < F[X]$. Consequently, we are observing above that $(f(X))$ is a maximal ideal when $f(X)$ is irreducible. (The implication also reverses, as follows quite easily, but we omit the proof.)

(ii) Recall that the prime subfields are constructed from the ring of integers $\mathbb{Z}$. We observed, in Theorem 1.12, that the prime subfield of any field is either isomorphic to $\mathbb{Q}$ (which is the field of fractions of the Euclidean domain $\mathbb{Z}$) or to a finite field $\mathbb{F}_p$ (which occurs as the quotient $\mathbb{Z}/(p)$ by the ideal generated by some prime $p$, the primes being the irreducible elements in $\mathbb{Z}$). An analogous observation is being made here. If $F$ is a field, the simple extensions of $F$ are constructed from the Euclidean domain $F[X]$ as follows:

- If $\alpha$ is transcendental, then $F(\alpha)$ is isomorphic to the field of fractions, $F(X)$, of $F[X]$.
- If $\alpha$ is algebraic, then $F(\alpha)$ can be constructed as the quotient $F[X]/(f(X))$ by an ideal generated by an irreducible polynomial $f(X)$.

Having established the existence of simple extensions with any specified minimum polynomial, we now establish the main result concerning the structure of such simple extensions $F(\alpha)$ with $\alpha$ algebraic. We determine the degree of the extension and establish a uniqueness result showing that $F(\alpha)$ is always constructed as in Theorem 2.13.

**Theorem 2.14** *Let $F$ be a field and $\alpha$ be an element in some extension of $F$. The simple extension $F(\alpha)$ over $F$ is a finite extension if and only if $\alpha$ is algebraic over $F$. Moreover, in this case,*

$$|F(\alpha) : F| = \deg f(X),$$

*the degree of the minimum polynomial $f(X)$ of $\alpha$ over $F$. Furthermore,*

$$F(\alpha) \cong \frac{F[X]}{(f(X))}$$

*(as rings).*

We shall use the various parts, particularly the first two, throughout the module. The final conclusion of the theorem will be particularly significant as a technical tool in a number of proofs.

PROOF: If $F(\alpha)$ is a finite extension of $F$, then all its elements, in particular $\alpha$, are algebraic over $F$ by Lemma 2.6.

Conversely, suppose $\alpha$ is algebraic over $F$. Let $f(X)$ be the minimum polynomial of $\alpha$ over $F$ and let $n$ be the degree of $f(X)$. We make use of the technology developed when proving Lemma 2.11. Recall the ring homomorphism $\phi\colon F[X] \to F(\alpha)$ is defined by evaluating polynomials at $\alpha$:

$$\phi\colon g(X) \mapsto g(\alpha).$$

The kernel of $\phi$ is $\ker\phi = \big(f(X)\big)$. Let $L = \operatorname{im}\phi$. This is a subring of $F(\alpha)$ and it contains all the elements of $F$ (as the images of the constant polynomials under $\phi$) and $\alpha$ (as the image of $X$). We shall show that $L$ is a field.

If $g(\alpha) \neq 0$, then $g(X)$ is not a multiple of $f(X)$ by Lemma 2.11(iv). Since $f(X)$ is irreducible, the greatest common divisor of $f(X)$ and $g(X)$ must be a constant. (It cannot be $f(X)$ as $f(X)$ does not divide $g(X)$.) Hence by Theorem 1.18 there exist polynomials $u(X), v(X) \in F[X]$ such that

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

We now substitute $\alpha$ to conclude

$$1 = u(\alpha)\, g(\alpha).$$

Hence $g(\alpha)$ has a multiplicative inverse in $L$ and we conclude that $L$ is indeed a field. We then conclude $F(\alpha) = L$ from the definition of $F(\alpha)$ as the smallest field containing $F$ and $\alpha$. The last part of the theorem is now established

$$F(\alpha) = \operatorname{im}\phi \cong \frac{F[X]}{\ker\phi} = \frac{F[X]}{(f(X))}$$

by the First Isomorphism Theorem.

It remains to establish $F(\alpha)$ is a finite extension of $F$ and to determine the degree of the extension. If $b \in F(\alpha)$, then $b = g(\alpha)$ for some polynomial $g(X) \in F[X]$. Since $F[X]$ is a Euclidean domain, we can write

$$g(X) = q(X)\, f(X) + r(X)$$

where either $r(X) = 0$ or $\deg r(X) < \deg f(X) = n$. Then

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

Hence every element of $F(\alpha)$ is the image of a polynomial of degree at most $n-1$ under $\phi$ and we conclude that $F(\alpha)$ is spanned by the set $\mathscr{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ as a vector space over $F$. In fact, $\mathscr{B}$ is linearly independent, for if we had a linear dependence relation

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$$

then $g(X) = b_0 + b_1 X + \cdots + b_{n-1}X^{n-1}$ would be a polynomial of degree smaller than $f(X)$ satisfying $g(\alpha) = 0$. The definition of the minimum polynomial forces

$$b_0 = b_1 = \cdots = b_{n-1} = 0.$$

Hence $\mathscr{B}$ is a basis for $F(\alpha)$ over $F$. We conclude that $F(\alpha)$ is indeed a finite extension of $F$ and that the degree is

$$|F(\alpha) : F| = |\mathscr{B}| = n = \deg f(X).$$

This completes the proof of the theorem. □

We record the following observation that was made during the towards the end of the proof:

**Corollary 2.15** *Suppose that $\alpha$ is algebraic over $F$ with minimum polynomial of degree $n$. Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for the simple extension $F(\alpha)$ over $F$.* □

It will be important to interpret the isomorphism appearing in the proof of Theorem 2.14 in various proofs that follow. When observing that $F[X]/(fX))$ is isomorphic to the simple extension $F(\alpha)$, we applied the First Isomorphism Theorem. Recall that the specific isomorphism $\bar{\phi}$ establishing the two rings are isomorphic is given by

$$\bar{\phi}\colon (\ker \phi) + g(X) \mapsto g(X)\phi = g(\alpha)$$

for any $g(X) \in F[X]$. (See the sketch proof of Theorem 1.6 above.) In particular, the effect on specific elements in the quotient ring are as follows:

$$\bar{\phi}\colon (f(X)) + a \mapsto a$$

for any element $a$ in the base field $F$, and

$$\bar{\phi}\colon (f(X)) + X \mapsto \alpha.$$

We shall now use the Theorem, and its corollary, to give a description of a variety of fields that we can construct. We shall make use of the minimum polynomials calculated in Example 2.12.

**Example 2.16** (i) The field $\mathbb{Q}(\sqrt{2})$ is the extension of $\mathbb{Q}$ obtained by adjoining $\sqrt{2}$. We know from Example 2.12 that the minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $f(X) = X^2 - 2$. Since this has degree 2, we conclude

$$|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2.$$

Moreover, as noted in Corollary 2.15, $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Thus every element of $\mathbb{Q}(\sqrt{2})$ can be expressed *uniquely* in the form

$$a + b\sqrt{2}$$

where $a, b \in \mathbb{Q}$. The addition, subtraction, multiplication and division can now be explicitly determined in terms of this form. Addition can be performed simply by adding the coefficients in front of each basis element (after all, the addition is part of the vector space structure). To multiply use the distributive laws:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

for any $a, b, c, d \in \mathbb{Q}$. Division can be obtained by a process similar to "complex conjugation":

$$\begin{aligned}\frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\end{aligned}$$

for any $a, b \in \mathbb{Q}$. We know that the denominator is non-zero if $a$ and $b$ are not both 0, since $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

Note here that if $a, b \neq 0$, then $a^2 - 2b^2 \neq 0$ since otherwise $\sqrt{2} = |a/b|$, which would be a contradiction as $\sqrt{2} \notin \mathbb{Q}$.

(ii) The previous example has much in common to the behaviour of the complex numbers. Indeed, note that $\mathbb{C} = \mathbb{R}(i)$, the field obtained by adjoining the imaginary number $i$ to the real numbers and the minimum polynomial of $i$ over $\mathbb{R}$ is $X^2 + 1$. This is consistent, via the Theorem, with the fact that $|\mathbb{C} : \mathbb{R}| = 2$ (the degree of the minimum polynomial) and $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.

(iii) Similarly, we know that the minimum polynomial of $\alpha = \sqrt[3]{2}$ is $X^3 - 2$, which has degree 3. Hence

$$|\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$$

and $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$. Consequently, elements of $\mathbb{Q}(\alpha)$ can be uniquely expressed in the form

$$a + b\alpha + c\alpha^2,$$

where $a, b, c \in \mathbb{Q}$, and multiplication of two such elements can be achieved by exploiting the fact that $\alpha^3 = 2$.

(iv) Finally, turning to the final part of Example 2.12, recall that the minimum polynomial of $\omega = \mathrm{e}^{2\pi i/3}$ over $\mathbb{Q}$ is $X^2 + X + 1$. Hence

$$|\mathbb{Q}(\omega) : \mathbb{Q}| = 2,$$

$\{1, \omega\}$ is a basis for $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, and consequently every element of $\mathbb{Q}(\omega)$ is uniquely expressed in the form

$$a + b\omega$$

where $a, b \in \mathbb{Q}$. We multiply two such expression by exploiting the fact that $\omega^2 = -\omega - 1$. Thus

$$\begin{aligned}(a + b\omega)(c + d\omega) &= ac + (ad + bc)\omega + bd\omega^2 \\ &= (ac - bd) + (ad + bc - bd)\omega.\end{aligned}$$

The theory we have developed so far enables us to give a good description of finite extensions of a base field.

**Theorem 2.17** *Let $K$ be an extension of a field $F$. Then $K$ is a finite extension of $F$ if and only if $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some finite collection $\alpha_1$, $\alpha_2$, …, $\alpha_n$ of elements of $K$ each of which is algebraic over $F$.*

Proof: First suppose that $K$ is a finite extension of $F$. Then $K$ has some finite basis, say $\mathscr{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, over $F$. Necessarily then $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ since the smallest field containing $F$ and the elements $\alpha_i$ necessarily contains all *$F$-linear combinations* of the $\alpha_i$ (that is, all expression $b_1\alpha_1 + \cdots + b_n\alpha_n$ where the $b_i$ are selected from $F$). Lemma 2.6 tells us that every element of $K$ is algebraic over $F$, so in particular each of the $\alpha_i$ is algebraic over $F$.

Conversely, suppose $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where each $\alpha_i$ is algebraic over the base field $F$. We shall show, by induction on $n$, that $|K : F|$ is finite. The base case is $n = 0$, when $K = F$ and then $|K : F| = 1$ since $\{1\}$ is a basis for $F$ as a vector space over itself $F$.

Assume then that $n \geqslant 1$ and, by induction, that the subfield $L = F(\alpha_1, \ldots, \alpha_{n-1})$ is a finite extension of $F$. Note that $L(\alpha_n) = K$, since the smallest subfield of $K$ containing $L$ and the element $\alpha_n$ necessarily contains $F$ and all the $\alpha_i$. Now the minimum polynomial of $\alpha_n$ over $F$ has coefficients in $F$, so these coefficients also belong $L$. Hence $\alpha_n$ is algebraic over $L$ and Theorem 2.14 tells us that $|L(\alpha) : L|$ is finite. Therefore, by the Tower Law (Theorem 2.4),

$$|K : F| = |L(\alpha) : F| = |L(\alpha) : L| \cdot |L : F|$$

is finite. This completes the induction and establishes the theorem. □

**Example 2.18** *Determine the degree of* $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ *over* $\mathbb{Q}$.

SOLUTION: We shall first make use of the Tower Law (Theorem 2.4) in the form

$$|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| = |\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}):\mathbb{Q}|.$$

Now $\sqrt{2}$ has minimum polynomial $X^2-2$ over $\mathbb{Q}$ (note this polynomial is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion), so

$$|\mathbb{Q}(\sqrt{2}):\mathbb{Q}| = 2.$$

The element $\sqrt{3}$ is algebraic over $\mathbb{Q}(\sqrt{2})$ since it is a root of the polynomial $X^2-3$. Hence

$$|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})| \leqslant 2.$$

(Note at this stage, we do not know that the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is $X^2-3$. This polynomial is irreducible over $\mathbb{Q}$, but we need more work to determine whether or not it is irreducible over $\mathbb{Q}(\sqrt{2})$.) If it were the case that $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})| = 1$, then these two fields would be equal and $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Thus we would be able to write

$$\sqrt{3} = a + b\sqrt{2}$$

for some $a, b \in \mathbb{Q}$ (since the proof of Theorem 2.14 tells us that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$). Note that both $a$ and $b$ must be non-zero, as if $b = 0$ then $\sqrt{3} = a \in \mathbb{Q}$ while if $a = 0$ then $\sqrt{6} = 2b \in \mathbb{Q}$, both of which are false as $\sqrt{3}$ and $\sqrt{6}$ are irrational. Upon squaring this equation, we conclude that

$$3 = a^2 + 2ab\sqrt{2} + 2b^2;$$

that is,

$$\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}.$$

This is again a contradiction. We conclude that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ and hence $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})| = 2$. We conclude, therefore, from the Tower Law, that

$$|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| = 4.$$

Note also that the Tower Law tells us that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$ (see the comment after the proof of Theorem 2.4).

Now apply the Tower Law to the inclusions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ (note that $\sqrt{2}+\sqrt{3}$ is an element of the larger field, so these inclusions hold):

$$4 = |\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| = |\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3})| \cdot |\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}|,$$

so $|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}|$ divides 4.

Note $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}$ because $\{1, \sqrt{2}, \sqrt{3}\}$ is linearly independent over $\mathbb{Q}$. Hence $|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}| = 2$ or 4. Suppose the minimum polynomial of $\alpha = \sqrt{2}+\sqrt{3}$ is quadratic, say $X^2 + bX + c$ for some $b, c \in \mathbb{Q}$. Thus

$$\begin{aligned} 0 = \alpha^2 + b\alpha + c &= (\sqrt{2}+\sqrt{3})^2 + b(\sqrt{2}+\sqrt{3}) + c \\ &= 2 + 2\sqrt{6} + 3 + b\sqrt{2} + c\sqrt{3} + c \\ &= (5+c) + b\sqrt{2} + c\sqrt{3} + 2\sqrt{6}. \end{aligned}$$

This contradicts the fact that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is linearly independent. Hence $\alpha$ is not a root of a quadratic polynomial over $\mathbb{Q}$. We conclude therefore

$$|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}| = 4.$$

□

**Example 2.19** Let us write $\mathbb{A}$ for the set of all elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. We call $\mathbb{A}$ the *field of algebraic numbers* over $\mathbb{Q}$. In this example, we show that $\mathbb{A}$ is indeed a subfield of $\mathbb{C}$ and determine the degree $|\mathbb{A} : \mathbb{Q}|$.

Certainly $\mathbb{A}$ is non-empty since it contains $\mathbb{Q}$ (these are the roots of linear equations $X - a$ for $a \in \mathbb{Q}$) plus lots of elements considered already, e.g., $\sqrt{2}$, $\sqrt{3}$, $i$, etc. Let $\alpha, \beta \in \mathbb{A}$. Note that

$$|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}| = |\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)| \cdot |\mathbb{Q}(\alpha) : \mathbb{Q}|$$

and here $|\mathbb{Q}(\alpha) : \mathbb{Q}|$ is finite because $\alpha$ is algebraic over $\mathbb{Q}$ and $|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)|$ is finite because $\beta$ is algebraic over $\mathbb{Q}$, so also algebraic over $\mathbb{Q}(\alpha)$. Hence $|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}|$ is finite, so every element of $\mathbb{Q}(\alpha, \beta)$ is algebraic over $\mathbb{Q}$ by Lemma 2.6. Now $\mathbb{Q}(\alpha, \beta)$ is a field, so it contains $\alpha + \beta$, $-\alpha$, $\alpha\beta$ and, provided $\alpha \neq 0$, also $1/\alpha$. Therefore the elements $\alpha + \beta$, $-\alpha$, $\alpha\beta$ and $1/\alpha$ are algebraic over $\mathbb{Q}$, so belong to $\mathbb{A}$. This establishes that $\mathbb{A}$ is a subfield of $\mathbb{C}$.

Finally, note also that $\sqrt[n]{2} \in \mathbb{A}$ and this has minimum polynomial $X^n - 2$ over $\mathbb{Q}$ (the latter polynomial being irreducible by Eisenstein's Criterion). Hence $|\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}| = n$ and applying the Tower Law to the inclusion $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{A}$, we conclude that $|\mathbb{A} : \mathbb{Q}| \geqslant n$ for all positive integers $n$. Therefore $\mathbb{A}$ is an infinite degree extension of $\mathbb{Q}$ consisting entirely of algebraic elements. (As a consequence, this tells us that the converse of Lemma 2.6 is false: there are algebraic extensions that are not finite extensions.)