# Chapter 5

# Fields

subfield / extension field vector spaces basis. prome field
focus on number fields and finite fields

## 5.1 First Fields and Automorphisms

**Definition 5.1.1.** A **field** is a set $F$ with two binary operations, $+$ and $*$, called addition and multiplication, two special elements 0 and 1, and two unary operations, $a \longmapsto -a$, and, for all but the 0 element, $a \longmapsto a^{-1}$ such that

- $F$ is an abelian group under $+$ with identity element 0 and additive inverse $a \longmapsto -a$.
- $F^* = F \setminus 0$ is an abelian group under $*$ with identity element 1 and multiplicative inverse $a \longmapsto a^{-1}$.
- Multiplication distributes over addition: $a * (b + c) = a * b + a * c$.

There are a few fields that should be familiar to you. The following were discussed in the first chapter.

- The rational numbers $\mathbb{Q}$. This is the smallest field that contains the integers.
- The prime fields, $\mathbb{F}_p$ for each prime number $p$. A fundamental result from modular arithmetic is that each nonzero element in $\mathbb{Z}/p$, the ring of integers modulo $p$, is invertible. One can compute the inverse of a nonzero element by using the extended Euclidean algorithm. This shows that $\mathbb{Z}/p$ is a field. When studying fields we will write $\mathbb{F}_p$ instead of $\mathbb{Z}/p$.
- The real field, $\mathbb{R}$.

- The field of complex numbers $\mathbb{C}$. The complex numbers also form a vector space of dimension 2 over $\mathbb{R}$ with basis $\{1, i\}$ where $i = \sqrt{-1}$. That is, every element can be written in a unique way as $a + bi$ for $a, b \in \mathbb{R}$, and the properties of a vector space hold for scalar multiplication by a real number. Just as we have $r(a, b) = (ra, rb)$ for $(a, b) \in \mathbb{R}^2$ and $r \in \mathbb{R}$, we have $r(a+bi) = (ra) + (rb)i$.

- Inside the field of complex numbers is the field of Gaussian rationals (see Section 1.2)
$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$$
This is a field, and also a two-dimensional vector space over $\mathbb{Q}$.

**Definition 5.1.2.** Let $K$ be a field and let $F$ be a subset of $K$ such that $F$ is a field using the operations $*_K$ and $+_K$. We say $F$ is a **subfield** of $K$ and $K$ is an **extension field** of $F$. We will write $F \leq K$ and also $K/F$ depending on whether the emphasis is on $F$ being a subfield of $K$ or $K$ an extension of $F$.

*Exercises* 5.1.3. Intersection of fields.

**(a)** Let $F$ and $E$ be subfields of $K$. Show that $F \cap E$ is a subfield of $K$.

**(b)** Let $\mathcal{F}$ be a set of subfields of $K$, then
$$\bigcap_{F \in \mathcal{F}} F$$
is a subfield of $K$.

**(c)** We have a similar property for rings: Let $\mathcal{R}$ be a set of subrings of a ring $S$, then
$$\bigcap_{R \in \mathcal{R}} R$$
is a subring of $S$.

*Exercises* 5.1.4. Field extension as a vector space

A vector space over a field $F$ is an abelian group $V, +$ that also admits a multiplication by elements of $F$, that is called **scalar multiplication**. Scalar multiplication satisfies three properties that coordinate the operations on $F$ with addition on $V$.

- For $a \in F$ and $v \in V$, $av = va$.
- For all $v \in V$, $1_F v = v$.
- For $a, b \in F$ and $v \in V$, $(ab)v = a(bv)$.
- For $a, b \in F$ and $v \in V$, $(a + b)v = av + bv$.

- For $a \in F$ and $v, w \in V$, $a(v+w) = av + aw$.

**(a)** Let $V$ be a vector space over $F$. Verify that the properties above imply that $0_F v = 0_V$ for all $v \in V$. Verify also that $(-1)v$ is the additive inverse of $v$.

**(b)** Let $K$ be an extension field of $F$. Show that $K$ is a vector space over $F$. This involves checking that the properties of a vector space over $F$ are satisfied by $K$.

The previous exercise shows that when $F \leq K$, $K$ is a vector space over $F$.

**Definition 5.1.5.** For $K$ and extension field of $F$, write $[K : F]$ for the dimension when it is finite. It is also called the **degree** of the extension.

We have seen that $[\mathbb{C} : \mathbb{R}] = 2$ and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Our focus in the study of fields is to identify the structure (whatever that means, we will see!) of finite field extensions.

### The Prime Field

For any field $F$, there is a ring homomorphism $\mathbb{Z} \longrightarrow F$ taking 1 to $1_F$, by Theorem 4.2.13. If the kernel is trivial, then $F$ contains a subring isomorphic to the integers. We will simply say that $F$ contains the integers since there is only one ring homomorphism from $\mathbb{Z}$ to $F$. Since $F$ is a field, it must also contain the inverses of all the integers. Thus, it must contain the rationals, $\mathbb{Q}$. [1]

Suppose now that the kernel of $\mathbb{Z} \longrightarrow F$ is not trivial. By the first isomorphism theorem for rings, $F$ contains a subring isomorphic to $\mathbb{Z}/m$ for some integer $m$. Since $F$ is a field, $\mathbb{Z}/m$ cannot have zero-divisors, so $m$ must be prime. We will write this subfield as $\mathbb{F}_p$ ($p$ indicating a prime!) rather than $\mathbb{Z}/p$.

Thus we have two cases, a field $F$ either contains $\mathbb{F}_p$ or it contains $\mathbb{Q}$. This smallest field contained in $F$ is called its **prime field**. We say $F$ has **characteristic** $p$, when $\mathbb{F}_p \leq F$ and $F$ has **characteristic 0** in the case $\mathbb{Q} \leq F$.

### Homomorphisms are just Embeddings

As with groups and with rings, a natural topic to investigate is the functions that respect the structure of fields.

**Definition 5.1.6.** For fields $F$ and $K$, a function $\varphi : F \longrightarrow K$ is a **field homomorphism** when

[1] Strictly speaking, there is a field isomorphic to the rationals inside of $F$. But, as with the integers inside of $F$, there is a unique way for $\mathbb{Q}$ to map to $F$, so we will just think of $F$ containing $\mathbb{Q}$.

(1) $\varphi$ is a homomorphim from the group $F, +_F$ to $K, +_K$, and

(2) $\varphi$ is a homomorphism from the group $F^*, *_F$ to $K^*, *_K$.

Applying Proposition 2.3.2, $\varphi : F \longrightarrow K$ is a homomorphism of fields if it respects addition and multiplication:

$$\varphi(a_1 +_F a_2) = \varphi(a_1) +_K \varphi(a_2), \text{ and}$$
$$\varphi(a_1 *_F a_2) = \varphi(a_1) *_K \varphi(a_2)$$

In these two equations I have emphasized that the addition and multiplication on the left is done in $F$ and the addition and multiplication on the right is in $K$. Generally, we follow standard practice and do *not* write the subscripts on the operation signs to make the equations more legible. But, don't forget the distinction! We will also usually not write the multiplication sign, unless there is some important reason to use it.

It turns out that a homomorphism of fields is always injective!

**Proposition 5.1.7.** *Let $\varphi : F \longrightarrow K$ be a homomorphism of fields. Then $\varphi(a) = \varphi(b)$ implies $a = b$, so $\varphi$ is injective.*

*Proof.* Let $\varphi : F \longrightarrow K$ be a homomorphism. Let $a$ be a nonzero element of $F$. Since $aa^{-1} = 1_F$, applying $\varphi$ we get $\varphi(a)\varphi(a^{-1}) = 1_K$. Since $0_K$ does not have a multiplicative inverse, $\varphi(a)$ cannot be $0_K$. Thus $a \neq 0_F$ implies $\varphi(a) \neq 0_K$.

Now suppose $\varphi(a) = \varphi(b)$. Then $\varphi(a-b) = 0_K$, and the contrapositive of what we showed in the previous paragraph gives $a - b = 0$, so $a = b$. □

A homomorphism of fields $\varphi : F \longrightarrow K$ is often called an **embedding** of $F$ in $K$ since it places an isomorphic copy of $F$, namely $\varphi(F)$ inside of $K$.

The next proposition is completely analogous to results about the composition of homomorphisms of groups, Proposition 2.3.2, and properties of isomorphisms, Proposition 2.3.11.

**Proposition 5.1.8.**

*(1) The composition of two field homomorphisms is a field homomorphism.*

*(2) The composition of two isomorphisms of fields is an isomorphism of fields.*

*(3) Let $\varphi : F \longrightarrow K$ be an isomorphism of fields. The inverse function $\varphi^{-1} : K \longrightarrow F$ is also an isomorphism of fields.*

*Proof.* (1) We have already shown that the composition of group homomorphisms is a group homomorphism. Thus the composition of two field homomorphisms $\alpha : F \longrightarrow H$ and $\beta : H \longrightarrow K$ is both a homomorphism of the additive group $F, +_F$ to $K, +_K$ and a homomorphism of the multiplicative group $F, *_F$ to $K, *_K$. Therefore $\beta \circ \alpha$ is a field homomorphism.

(2) The composition of two bijections is a bijection and the composition of two homomorphisms is a homomorphism.

(3) We can apply the fact that the inverse of an isomorphism of groups is also an isomorphism of groups to prove the result in a similar fashion to the first item.

□

### 5.1.1 The Automorphism Group

And now the culmination of this section!

**Definition 5.1.9.** Let $K$ be a field. The **automorphism group** of $K$ is the set of all isomorphisms from $K$ to itself, with the operation of composition. It is written $\mathrm{Aut}(K)$. Let $F$ be a subfield of $K$. An automorphism $\sigma$ such that $\sigma(a) = a$ for all $a \in F$ is said to **fix** $F$. The set of automorphisms $K$ that **fix** $F$ is denoted $\mathrm{Aut}(K/F)$.

Proposition 5.1.8 shows that the composition of two field isomorphisms is a field isomorphism. When the isomorphism is from $K$ to itself, we call it an automorphism of $K$. Proposition 5.1.8 shows that the composition of two automorphisms of $K$ is an automorphism of $K$ and that the inverse of an automorphism of $K$ is also an automorphism of $K$. Thus, $\mathrm{Aut}(K)$ is a group, which justifies the definition above. It is a simple exercise to show that the composition of two automorphisms that fix $F$ also fixes $F$ and that the inverse of an automorphism that fixes $F$ also fixes $F$. So, $\mathrm{Aut}(K/F)$ is a group.

**Corollary 5.1.10.** *For $K$ a field, $\mathrm{Aut}(K)$ is a group under composition. If $F$ is a subfield of $K$, $\mathrm{Aut}(K/F)$, the automorphisms of $K$ that fix $F$, form a group under composition.*

What can we say about automorphisms of the examples of fields discussed earlier? First, note that any automorphism has to take 1 to itself. Consider an automorphism $\varphi$ of $\mathbb{Q}$. We must have $\varphi(1) = 1$. Since $\varphi$ respects addition,

$$\varphi(\underbrace{1 + \cdots + 1}_{b \text{ terms}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{b \text{ terms}}$$

which shows that $\varphi(b) = b$ for each positive integer $b$. Since $\varphi$ also respects additive inverses, $\varphi(-b) = -b$ for positive integers $b$, so $\varphi$ is the identity map on the integers. Since $\varphi$ respects multiplicative inverses, $\varphi(1/b) = 1/\varphi(b) = 1/b$ for any integer $b$, and since $\varphi$ respects products $\varphi(a/b) = \varphi(a)\varphi(1/b) = a/b$. Thus we have shown that the only automorphism of $\mathbb{Q}$ is the identity map. A similar (shorter argument) shows that the only automorphism of $\mathbb{F}_p$ is the identity map.

Notice also that there can be no homomorphism from $\mathbb{Q}$ to $\mathbb{F}_p$ since any homomorphism must be injective. There can't be a homomorphism from $\mathbb{F}_p$ to $\mathbb{Q}$ since we would have to map $1_{\mathbb{F}_p}$ to $1_{\mathbb{Q}}$, but $\underbrace{1+\cdots+1}_{p \text{ terms}} = 0$ in $\mathbb{F}_p$ while $\underbrace{1+\cdots+1}_{p \text{ terms}} \neq 0$ in $\mathbb{Q}$.

The reals are vastly more complicated, so let's consider automorphims of $\mathbb{C}$ that fix $\mathbb{R}$. That is, we consider automorphisms $\varphi$ such that $\varphi(r) = r$ for $r \in \mathbb{R}$. We know that $i * i = -1$ so $\varphi(i) * \varphi(i) = \varphi(-1) = -1$. We know there are only two square roots of 1 in $\mathbb{C}$, so there are only two possibilities: $\varphi(i)$ is either $i$ itself or $-i$. In the first case $\varphi$ has to be the identity map, $\varphi(a+bi) = \varphi(a) + \varphi(b)\varphi(i) = a + bi$ since $\varphi$ fixes the reals. In the second case $\varphi$ is the conjugation map:

$$\varphi(a + bi) = \varphi(a) + \varphi(b)\varphi(i) = a + b(-i) = a - bi$$

It is clear that the composition of the conjugation map with itself is the identity map. Thus, $\text{Aut}\left(\mathbb{C}/\mathbb{R}\right) \cong \mathbb{Z}_2$.

A similar argument applies to the field $\mathbb{Q}(i)$. The field $\mathbb{Q}$ has to be fixed, and the only non-identity automorphism takes $a + bi$ to $a - bi$. Thus we have $\text{Aut}\left(\mathbb{Q}(i)\right) \cong \mathbb{Z}_2$.

This simple example is the model for much of our work in this chapter. For a field $K$ containing another field $F$, we seek to understand the automorphisms of $K$ that fix $F$, and to use that knowledge to better understand the field $K$.

## 5.2 Constructing Fields

We have three main tools for constructing new fields.

**Construction I**: In Section 1.1 we showed that the ring of integers modulo a prime forms a field, which we write $\mathbb{F}_p$. Similarly, in Section 1.3 we showed that for $F$ a field and $m(x)$ irreducible, $F[x]/m(x)$ is a field (see also Theorem 4.1.9). More generally, for any ring $R$, Theorem 4.6.11 shows that $R/I$ is a field whenever $I$ is a maximal ideal.

**Construction II**: The second method is based on the construction of the rational numbers from the integers. For an integral domain $R$, let $D = R \setminus \{0\}$

and form the ring of fractions $D^{-1}R$ as in Section 4.7. This is a field. For the ring of integers $\mathbb{Z}$, the field thus constructed is $\mathbb{Q}$. For the integral domain $F[x]$ over a field $F$, the resulting field is written $F(x) = \{a(x)/b(x) : a(x), b(x) \in F[x] \text{ with } b(x) \neq 0\}$.

**Construction III**: The third method is to take a subfield of a given field. We did this in Section 1.2 when we introduced the subfield of the complex numbers $\mathbb{Q}(i)$. Given any field $K$ and a subset $S \subseteq K$ we can take the intersection of all subfields of $K$ containing $S$. Exercise 5.1.3 show that this is a field (letting $\mathcal{F}$ be the set of all fields containing $S$). It contains $S$ and it is, by construction, a subfield of every field containing $S$. Thus it makes sense to call it the smallest subfield containing $S$. We often are interested in the smallest subfield of $K$ containing a specific subfield $F$ and some additional set of elements $S \subseteq K \setminus F$. We write this $F(S)$. If no subfield is specificied, we know that this field must contain one of the prime fields $\mathbb{Q}$, or $\mathbb{F}_p$, so we may write it $\mathbb{F}_p(S)$ or $\mathbb{Q}(S)$ as appropriate.

With the notation of Construction III, given a subset $S$ of $K$ we may also take the intersection of all rings containing $S$ and some subfield $F$, which we write $F[S]$. It is a ring, and is, by construction, the smallest subring of $K$ that contains $F$ and $S$. (See Exercise .)

There is a relationship between Construction III and the other constructions, which we can illustrate with two examples inside the complex field. Before introducing the two examples recall Theorem 4.3.9, which we adapt here as follows.

**Theorem** Let $F$ be a subfield of a field $K$. For any $s \in K$ there is a unique homomorphism from $F[x]$ to $K$ that takes $x$ to $s$, namely

$$\begin{aligned} \overline{\varphi} : F[x] &\longrightarrow K \\ \sum_i a_i x^i &\longmapsto \sum_i a_i s^i \end{aligned}$$

**Definition 5.2.1.** Continuing with the notation as stated above, if the homomorphism is injective we say that $s$ is **transcendental** over $F$. Otherwise, $s$ is **algebraic** over $F$. When $s$ is algebraic, the monic generator of the kernel in the theorem is called the **minimal polynomial** of $s$.

**Proposition 5.2.2.** *If $s$ is algebraic over $F$ then the minimal polynomial of $s$ is an irreducible polynomial. Consequently, the image of $\varphi$ as defined in the theorem is a subfield of $K$. Thus $F[s] = F(s)$. The dimension $[F(s) : F]$ is equal to the degree of the minimal polynomial.*

*Proof.* Suppose by way of contradiction, that the monic generator of the kernel is $m(x)$ and it factors as $m(x) = f(x)g(x) \in F[x]$. Then $f(s)g(s) = 0$ in $K$. Since $K$ is a field either $f(s)$ or $g(s)$ is zero. Without loss of generality, suppose the former. Then $f(x)$ is in the kernel, and is therefore a multiple of $m(x)$. Since $f(x)$ is also a factor of $m(x)$ we must have that $g(x)$ has degree 0, so it is a constant. This shows that $m(x)$ is irreducible.

Alternatively, we can prove the result by applying the First Isomorphism Theorem for rings: $F[x]$ modulo $m(x)$ is isomorphic to its image in $K$. Since $K$ is a field, the image must be an integral domain. Since a reducible polynomial yields a quotient ring with zero divisors by Corollary 4.1.10, the kernel must be generated by an irreducible polynomial. Moreover, the quotient of $F[x]$ by an irreducible polynomial is a field, so the image of $\varphi$ is actually a subfield of $K$.

Note that the image of $\varphi$ consists of polynomials in $s$. Thus the smallest ring containing $F$ and $s$ is also the smallest field containing $F$ and $s$: $F[s] = F(s)$. We note also that this is $\left\{\sum_{i=0}^{n-1} a_i s^i\right\}$ where $n = \deg(m(x))$, since the polynomials of degree less than $n$ form a system of representatives for $F[x]/m(x)$. Since each element of $F[s]$ is uniquely expressed as a polynomial in $s$ of degree less than $\deg(m(x))$, the degree of the extension $F(s)/F$ is equal to $\deg(m(x))$. □

**Proposition 5.2.3.** *If $K$ contains some transcendental element over $F$ then $K/F$ has infinite dimension as a vector space over $F$. Conversely, if $K$ is finite dimensional over $F$ then every element of $K$ is algebraic over $F$.*

*Proof.* Suppose that $\alpha \in K$ is transcendental over $F$. Then $F[\alpha]$ is isomorphic to $F[x]$ since it is the image of the injective homomorphism $\varphi : F[x] \longrightarrow K$ that takes $x$ to $\alpha$ and fixes $F$. In $F[x]$ the powers of $x$, that is $x^i$ for $i \in \mathbb{N}_0$, are linearly independent, so $F[x]$ is infinite dimensional over $F$. Since $F[\alpha]$ is isomorphic to $F[x]$, it is also infinite dimensional over $F$. Since $K$ contains $F[\alpha]$ it is infinite dimensional over $F$. □

*Example* 5.2.4. Consider the homomorphism $\varphi : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ that takes $x$ to $i = \sqrt{-1}$. This is not injective. The kernel is $x^2 + 1$ and the image is $\mathbb{Q}[i]$, the ring of polynomials in $i$ with rational coefficients. It is isomorphic to $\mathbb{Q}[x]/(x^2 + 1)$. This is a field because $x^2 + 1$ is irreducible. Thus the field $\mathbb{Q}(i)$ is the same as the ring $\mathbb{Q}[i]$.

Similarly $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$.

*Example* 5.2.5. For a more subtle example, consider $\mathbb{Q}(\sqrt[3]{2})$. Using the homomorphism $\mathbb{Q}[x] \longrightarrow \mathbb{C}$ that takes $x$ to $\sqrt[3]{2}$, we have $\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[x]/(x^3 - 2)$. There are three cube roots of 2 in $\mathbb{C}$, the others are $\sqrt[3]{(2)}\omega$ and $\sqrt[3]{(2)}\omega^2$ where $\omega = (1 - \sqrt{3}i)/2$. Define $\varphi : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ by $\varphi(x) = \sqrt[3]{(2)}\omega$. This gives $\mathbb{Q}(\sqrt[3]{2}\omega) \cong$

$\mathbb{Q}[x]/(x^3-2)$. We may do the same for $\sqrt[3]{2}\omega^2$, so there are three distinct embeddings of $\mathbb{Q}[x]/(x^3-2)$ in $\mathbb{C}$.

*Example* 5.2.6. Consider the homomorphism $\varphi : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ that takes $x$ to $e$ where $e$ is the Euler number $e \approx 2.71$. It is not obvious, but $e$ is transcendental, not algebraic []. The homomorphism $\varphi$ is therefore an isomorphism of $\mathbb{Q}[x]$ with its image $\mathbb{Q}[e]$. The smallest field containing $\mathbb{Q}[e]$ is

$$\mathbb{Q}(e) = \left\{ \frac{f(e)}{g(e)} : f(e), g(e) \in \mathbb{Q}[e] \text{ and } g(e) \neq 0 \right\}$$

The stipulation that $g(e) \neq 0$ is simply requiring that the coeffiecients of $g$ not all be zero, since no nonzero polynomial in $\mathbb{Q}[x]$ evaluates at $e$ to 0.

The number $\pi \approx 3.14$ is also transcendental [] so there is an isomorphism between $\mathbb{Q}[x]$ and $\mathbb{Q}[\pi]$ and between $\mathbb{Q}(x)$ and $\mathbb{Q}(\pi)$.

The set of algebraic numbers (the complex numbers algebraic over $\mathbb{Q}$) is actually countable, while the complex numbers (and therefore the transcendental numbers) are uncountable.[]

## Adjoining a Root

Our focus henceforth is on Construction I. A critical, and rather subtle, phrase that is used repeatedly in the study of fields is "adjoin a root." We finish the section, with an explanation of this phrase.

Let $m(x)$ be a monic irreducible polynomial of degree $n > 1$ over a field $F$. Let $m(x) = x^n + m_{n-1}x^{n-1} + \cdots + m_1 x + m_0$. Elements of the quotient ring $F[x]/m(x)$ are cosets of $\langle m(x) \rangle$, and each coset is uniquely represented as $a(x) + \langle m(x) \rangle$ for some polynomial $a(x)$ of degree less than $n$. The powers of $x + \langle m(x) \rangle$ are $x^i + \langle m(x) \rangle$ for $i < n$, whereas $x^n + \langle m(x) \rangle$ is represented by $-(m_{n-1}x^{n-1} + \cdots + m_1 x + m_0) + \langle m(x) \rangle$. This is because $m(x) + \langle m(x) \rangle = 0 + \langle m(x) \rangle$. Thus, in the quotient ring $F[x]/m(x)$,

$$\begin{aligned}
&(x + \langle m(x) \rangle)^n + m_{n-1}(x + \langle m(x) \rangle)^{n-1} + m_{n-2}(x + \langle m(x) \rangle)^{n-2} + \cdots \\
&\qquad \cdots + m_2(x + \langle m(x) \rangle)^2 + m_1(x + \langle m(x) \rangle) + m_0(1 + \langle m(x) \rangle \\
&= (x^n + m_{n-1}x^{n-1} + m_{n-2}x^{n-2} + \cdots + m_2 x^2 + m_1 x + m_0) + \langle m(x) \rangle \\
&= 0 + \langle m(x) \rangle
\end{aligned}$$

In other words, we may think of $m(x)$ as having a root in $F[x]/m(x)$, namely the coset $x + \langle m(x) \rangle$.

It is common therefore to give this coset a new symbol, let's call it $\alpha$, and to speak of the quotient ring as follows: We **adjoin a root** $\alpha$ of $m(x)$ to the field

$F$ and obtain the field $F(\alpha)$. Over this field $x - \alpha$ is now a factor of $m(x)$, so $m(x)$ is no longer irreducible. In the polynomial ring $F(\alpha)[x]$, we can then factor $m(x)$ by dividing $m(x)$ by $x - \alpha$. A natural question is whether $m(x)/(x - \alpha)$ is now irreducible, or does it factor completely (into linear factors), or something in between?

The upcoming sections explore this question. It is clear though that if $\deg(m(x)) = 2$ then adjoining a root of $m(x)$ will factor $m(x)$ completely, since the quotient $m(x)/(x - \alpha)$ will be another linear factor.

More generally, over $\mathbb{Q}$, every extension by a root of a quadratic is isomorphic to $\mathbb{Q}(\sqrt{D})$ for some square free integer $D$. The exercise below steps through the proof.

*Exercises* 5.2.7. Quadratic Extensions of $\mathbb{Q}$

Let $m(x) = x^2 + ax + b$ be an irreducible quadratic over $\mathbb{Q}$.

**(a)** Use the quadratic formula to find two distinct embeddings of $\mathbb{Q}[x]/m(x)$ into $\mathbb{C}$.

**(b)** Show that these two embeddings have the same image (although the image of $x + \langle m(x) \rangle$ itself is different in the two cases).

**(c)** Show that there is some square free integer $D$ such that $\mathbb{Q}(\sqrt{D})$ is the same field as the one determined by $\mathbb{Q}[x]/m(x)$.

**(d)** Conclude that every degree 2 extension of $\mathbb{Q}$ is isomorphic to $\mathbb{Q}(\sqrt{D})$ for some square free integer $D$.

**(e)** Conclude also that every degree 2 extension of $\mathbb{Q}$ has one non-trivial automorphism.

Finally, we have this relationship between an automorphim of a field extension and the minimal polynomial of an element in the extension.

**Proposition 5.2.8.** *Let $K$ be an extension of $F$. Let $\alpha \in K$ have minimum polynomial $m(x)$ over $F$. For any $\sigma \in \mathrm{Aut}(F/K)$, $\sigma(\alpha)$ is also a root of $m(x)$.*

*Proof.* Let $m(x) = x^d + m_{d-1}x^{d-1} + \cdots + m_0$ be the mimimum polynomial for $\alpha$

over $F$. Each $m_i \in F$ so

$$\begin{aligned}
\sigma\Big(m(\alpha)\Big) &= \sigma\left(\sum_{i=0}^{n} m_i\alpha\right) \\
&= \sum_{i=0}^{n} \sigma(m_i\alpha) \qquad \text{since } \sigma \text{ respects sums,} \\
&= \sum_{i=0}^{n} m_i\sigma(\alpha) \qquad \text{since } \sigma \text{ respects products and fixes elements of } F \\
&= m\left(\sigma(\alpha)\right)
\end{aligned}$$

Since $m(\alpha) = 0$ we have $m(\sigma(\alpha))$ is also 0. □

## 5.3 Finite Fields

Compared to extension fields of the rationals like $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(i)$, which are somewhat familiar, extensions fields of the field $\mathbb{F}_p$ may seem strange. Yet, the study of finite fields is in many ways much simpler than the study of number fields. We will see in this section that there is a complete classification of finite fields, and that the multiplicative structure is quite simple. Furthermore, for a small finite field, we can write down all the elements and compute by hand (or with computer software) in a way that builds intuition for the structure of a finite field.

Finite fields have become important tools in electrical engineering, specifically in the mathematics of communications systems. Many cryptographic systems and error correction systems are based on finite field arithmetic. The design of hardware to implement finite field arithmetic is also an important area of research and commercial development.

In this section we characterize finite fields by proving the following theorem. It has three main parts. The first identifies several properties that a finite field must hold, and relates these properties to Construction 1 of fields, working in $\mathbb{F}_p[x]$ modulo an irreducible polynomial $m(x)$. The second part establishes the existance and uniqueness of a field of order $p^n$ for any prime $p$ and $n \in \mathbb{N}$. The third part shows that the automorphism group of a finite field (over $\mathbb{F}_p$) is a cyclic group.

Let us start with the smallest example of a finite field that is not a prime field.

*Example* 5.3.1. There are four polynomials of degree 2 in $\mathbb{F}_2[x]$. They are $x^2, x^2+1, x^2+x$ and $x^2+x+1$. The first three all have roots in $\mathbb{F}_2$, so are reducible. Only $x^2+x+1$ is irreducible. Let's use it to construct a field with 4 elements $\mathbb{F}_2[x]/(x^2+x+1)$. Let $\eta$ be the congruence class $x+\langle x^2+x+1\rangle$, then $\eta$ is a root of $x^2+x+1$. We say that we have adjoined $\eta$ to $\mathbb{F}_2$ to create the field $\mathbb{F}_2(\eta)$. The elements of $\mathbb{F}_2(\eta)$ are polynomials in $\eta$ of degree less than 2: $\mathbb{F}_2(\eta) = \{0, 1, \eta, \eta+1\}$. Addition is component-wise (relative to the basis $\{1, \eta\}$). Multiplication must take account of $\eta^2 = \eta + 1$. Here is a multiplication table for this field.

| $*$ | $1$ | $\eta$ | $\eta+1$ |
|---|---|---|---|
| $1$ | $1$ | $\eta$ | $\eta+1$ |
| $\eta$ | $\eta$ | $\eta+1$ | $1$ |
| $\eta+1$ | $\eta+1$ | $1$ | $\eta$ |

We can also see that both $\eta$ and $\eta+1$ generate the multiplicative group. Since $\mathbb{F}_2(\eta)^*$ has 3 elements, any element besides 1 generates.

Here is a "dictionary" between the powers of $\eta$ and the polynomial form of the elements of $\mathbb{F}_2(\eta)$. We will see that this type of dictionary is a useful tool for larger

fields.

| exponential form | polynomial form |
|---|---|
| $1$ | $1$ |
| $\eta$ | $\eta$ |
| $\eta^2$ | $\eta + 1$ |

**Theorem 5.3.2.** *Let $K$ be a field with a finite number of elements.*

*(1) $K$ has $p^n$ elements for some prime $p$ and $n \in \mathbb{N}$.*

*(2) Each element of $K$ is a root of $x^{p^n} - x$, so $x^{p^n} - x$ factors completely, into distinct linear factors, over $K$.*

*(3) There is an element $\eta \in K$ whose powers $\eta^1, \eta^2, \ldots, \eta^{p^n-1} = 1$ give all the nonzero elements of $K$. Consequently, $K^*$ is cyclic of order $p^n - 1$.*

*(4) $K$ is isomorphic to $\mathbb{F}_p[x]/m(x)$ for some irreducible polynomial $m(x)$ of degree $n$ over $\mathbb{F}_p$. Furthermore $m(x)$ is a factor of $x^{p^n} - x$.*

*For any prime $p$ and any positive integer $n$:*

*(4) There exists a field with $p^n$ elements.*

*(5) Any two fields with $p^n$ elements are isomorphic.*

*(6) The field with $p^n$ elements has a subfield with $p^d$ elements if and only if $d$ divides $n$.*

*We use $\mathbb{F}_{p^n}$ to denote the unique field with $p^n$ elements. The automorphism group of $\mathbb{F}_{p^n}$ satisfies:*

*(7) $\mathrm{Aut}(\mathbb{F}_{p^n})$ is generated by the Frobenius map, $\varphi(\beta) = \beta^p$ for $\beta \in \mathbb{F}_{p^n}$.*

*(8) $\mathrm{Aut}(\mathbb{F}_{p^n}) \cong \mathbb{Z}/n$.*

As a first step we prove item (1) of the theorem.

**Proposition 5.3.3.** *A finite field is a vector space over $\mathbb{F}_p$ for some prime $p$. Consequently, the number of elements of $K$ is a power of $p$.*

*Proof.* Suppose that $K$ is a finite field. The smallest field contained in $K$, its prime field, must be $\mathbb{F}_p$ for some prime number $p$.

From the definition of a field, we can see that $K$ satisfies the properties for a vector space over $\mathbb{F}_p$ (This was Exercise 5.1.4.) For example: if $a \in \mathbb{F}_p$ and $\beta, \gamma \in K$ then $a(\beta + \gamma) = a\beta + a\gamma$ follows from the distributive law, but may be also considered as the property concerning scalar multiplication (by $\alpha$) of a sum

of vectors, $\beta+\gamma$. If the dimension of $K$ over $\mathbb{F}_p$ is $n$ then $K$ has a basis $u_1,\ldots,u_n$ and the elements of $K$ are $a_1u_1+\ldots,a_nu_n$ for $a_i\in\mathbb{F}_p$. Thus $K$ must have $p^n$ elements. □

Suppose that $q=p^n$ is the number of elements in $K$. By the definition of a field, the set of nonzero elements of $K$ is a group under multiplication. This group is denoted $K^*$. Recall that the **order** of an element $\alpha$ in a finite group $G$ is the smallest positive integer $r$ such that $\alpha^r$ is the identity. The order of an element divides the order of the group by Lagrange's Theorem 2.7.7.

**Proposition 5.3.4.** *Let $K$ be a field with $p^n$ elements. The polynomial $x^{p^n}-x$ factors completely, into distinct linear factors, over $K$.*

$$x^{p^n-1}-1=\prod_{\alpha\in K^*}(x-\alpha) \quad \textit{and,}$$
$$x^{p^n}-x=\prod_{\alpha\in K}(x-\alpha)$$

*Proof.* The multiplicative group $K^*$ has $p^n-1$ elements, so each element $\alpha\in K^*$ has order dividing $p^n-1$. Thus, each $\alpha\in K^*$ is a root of $x^{p^n-1}-1$. Furthermore, each root corresponds to a factor $x-\alpha$ of $x^{p^n-1}-1$. We have identified $p^n-1$ roots of $x^{p^n-1}-1$, so it factors into linear factors: $x^{p^n-1}-1=\prod_{\alpha\in K^*}(x-\alpha)$. Taking account of the 0 element gives the factorization of $x^{p^n}-x$. □

This establishes item (2) of the theorem.

Before we proceed further, recall the following properties from Theorem 2.1.13 and problems immediately following it.

**Order Theorem** Let $\alpha$ be an element of order $r$ in an group $G$.

(1) $\alpha^i=\alpha^j$ iff $i\equiv j \mod r$.

(2) The order of $\alpha^i$ is $r/d$ where $d=\gcd(i,r)$.

(3) Let $G$ be abelian. Let $\beta\in G$ have order $s$, coprime to $r=\mathrm{ord}(\alpha)$. Then $\mathrm{ord}(\alpha\beta)=rs$.

(4) Let $G$ be abelian. If $\alpha_1,\ldots,\alpha_n$ have orders $r_1,\ldots,r_n$ where the $r_i$ are pairwise coprime, then $\mathrm{ord}(\prod_{i=1}^n\alpha_i)=\prod_{i=1}^n r_i$.

Now we can establish item (3) of the Theorem. The key ideas we exploit are (1) an element of $K^*$ of order $t$ is a root of $x^t-1$, and (2) the polynomial $x^t-1$ has at most $t$ roots.

**Proposition 5.3.5.** *The multiplicative group of a finite field $K$ is cyclic. That is, if $|K| = p^n$, there is some element $\eta \in K$ such that the nonzero elements of $K$ are $1, \eta, \eta^2, \ldots, \eta^{p^n-2}$.*

*Proof.* Let $K$ have $p^n$ elements and let the prime factorization of $p^n - 1$ be $\prod_{i=1}^{r} q_i^{b_i}$. We will show below that for each $i = 1 \ldots, r$ there is an element $\eta_i \in K^*$ of order $q_i^{b_i}$. Let $\eta = \prod_{i=1}^{r} \eta_i$. Since the $q_i^{b_i}$ are coprime to each other, the theorem above shows that the order of $\eta$ is $\prod_{i=1}^{r} q_i^{b_i} = p^n - 1$. Thus $\eta$ generates the multiplicative group of $K$.

Now we prove the claim. Suppose that $q$ is prime and $q^b$ appears in the prime factorization of $p^n - 1$, so $q^b$ divides $p^n - 1$ but $q^{b+1}$ does not. Let $t = (p^n - 1)/q^b$ and consider the set $S = \{\alpha^t : \alpha \in K^*\}$. This set is the image of the left hand map below.

$$\begin{array}{ccccc} K^* & \longrightarrow & K^* & \longrightarrow & K^* \\ \alpha & \longmapsto & \alpha^t & & \\ & & & \beta \longmapsto & \beta^{q^b} \end{array}$$

The set $S$ is also contained in the kernel of the righthand map because

$$(\alpha^t)^{q^b} = \alpha^{p^n-1} = 1$$

This shows that every element of $S$ is a root of $x^{q^b} - 1$. There can be only $q^b$ roots of $x^{q^b} - 1$, so $S$ has at most $q^b$ elements. On the other hand, for any $\beta \in S$ the polynomial $x^t - \beta$ has at most $t$ roots so there can be at most $t$ elements of $K$ whose $t$th power is $\beta$. Therefore the cardinality of $S$ is at least $(p^n - 1)/t = q^b$. We have therefore proven that $|S| = q^b$.

Every element of $S$ is a root of $x^{q^b} - 1$, but at most $q^{b-1}$ of the elements in $S$ can be roots of $x^{q^{b-1}} - 1$. Consequently, there must be at least $q^b - q^{b-1}$ elements of $S$ whose order in $K$ is $q^b$. This shows what we wanted: there is some element of $K$ of order $q^b$.

□

**Definition 5.3.6.** An element of a finite field whose powers generate the nonzero elements of the field is called **primitive**.

Proposition 5.3.5 says that every finite field has a primitive element. Furthermore, from the Order Theorem, if $\eta$ is primitive in a field of $p^n$ elements then $\eta^k$ is also primitive whenever $k$ is coprime to $p^n - 1$. Thus there are $\varphi(p^n - 1)$ primitive elements, where $\varphi$ is the Euler totient function ($\varphi(n)$ is the number of positive integers less than $n$ and coprime to $n$).

To prove item (4) of the Theorem we need to use the minimal polynomial of a primitive element.

**Proposition 5.3.7.** *Let $K$ be a finite field of $p^n$ elements. Let $\eta$ be any primitive element of $K$, let $\varphi : \mathbb{F}_p[x] \longrightarrow K$ take $x$ to $\eta$ and let $m(x)$ generate the kernel (so $m(x)$ is the minimal polynomial of $\eta$ over $\mathbb{F}_p$). Then $K$ is isomorphic to $\mathbb{F}_p[x]/m(x)$ and $\deg m(x) = n$. Furthermore, $m(x)$ divides $x^{p^n} - x$ and $m(x)$ factors completely in $K$.*

*Proof.* From the First Isomorphism Theorem for rings, $\varphi$ gives rise to an isomorphism from $\mathbb{F}_p[x]/m(x)$ to its image in $K$. Proposition 5.2.2 shows that $m(x)$ must be irreducible, since $K$ has no zero divisors. But, the image of $\varphi$ contains $\eta$ and therefore all of its powers. Thus the image is all of $K$ and we have $K \cong \mathbb{F}_p[x]/m(x)$. The dimension of $K$ over $\mathbb{F}_p$ is $n$ and the dimension of $\mathbb{F}_p[x]/m(x)$ is $\deg(m(x))$, so the degree of $m(x)$ is $n$.

By Proposition 5.3.4, $x^{p^n} - x$ factors into linear factors in $K$ and $\eta$ is one of the roots. This implies that $x^{p^n} - x$ is in the kernel of $\varphi$, so $m(x)$ divides $x^{p^n} - x$. Since $x^{p^n} - x$ factors completely in $K$ so to does $m(x)$. □

We have established items (1)-(4) of the theorem which identify the fundamental properties that a finite field must satisfy. We can now prove existence and uniqueness for fields of prime power order. We will need one more property, the "Freshman's dream":

**Proposition 5.3.8.** *Let $\alpha, \beta$ be elements of a field of characteristic $p$. Then $(\alpha + \beta)^p = \alpha^p + \beta^p$.*

*Proof.* Expanding $(\alpha + \beta)^p$ using the binomial theorem we get terms like

$$\binom{p}{k} \alpha^k \beta^{p-k}$$

The binomial coefficient really means 1 added to itself $\binom{p}{k}$ times. Since $p$ divides the binomial coefficient when $1 < k < p$ the coefficient is 0 unless $k = 0$ or $k = p$. That gives the result. □

We can now prove items (5)-(6) of the theorem.

**Proposition 5.3.9.** *For any prime power there exists a unique field of that order.*

*Proof.* Uniqueness: Let $K$ and $K'$ be two fields with $p^n$ elements. Let $\eta$ be a primitive element in $K$ and let $m(x)$ be its minimal polynomial over $\mathbb{F}_p$. The previous proposition showed that $\eta$ is a root of $x^{p^n} - x$, and $m(x)$ divides $x^{p^n} - x$.

By Proposition 5.3.7, $x^{p^n} - x$ factors into distinct linear factors in both $K$ and $K'$ so there must be a root of $m(x)$ in $K'$. Call this root $\eta'$. Then the homomorphism from $\mathbb{F}_p[x]$ to $K'$ that takes $x$ to $\eta'$ must have image that is a subfield of dimension $n$ in $K'$, and is therefore all of $K'$. By Proposition 5.3.7, both $K$ and $K'$ are isomorphic to $\mathbb{F}_p[x]/m(x)$ so they are isomorphic to each other.

Existence: By successively factoring $x^{p^n} - x$ and adjoining roots of a nonlinear irreducible factor, we can, after a finite number of steps, arrive at a field in which $x^{p^n} - x$ factors completely. I show below that the roots of $x^{p^n} - x$ form a field. Since the derivative of $x^{p^n} - x$ is $-1$, $x^{p^n} - x$ does not have multiple roots, so by the roots-factors theorem it has exactly $p^n$ roots. Thus we have a field of $p^n$ elements.

To show the roots of $x^{p^n} - x$ form a field, we need to show that the sum of two roots is a root, that the additive inverse of a root is a root, that the product of two roots is a root and that the multiplicative inverse of a root is a root. These are straightforward and left as an exercise. □

*Exercises* 5.3.10. THE ROOTS OF $x^{p^n} - x$ FORM A FIELD.

Let $\alpha, \beta$ be roots of $x^{p^n} - x$ in some finite field $K$.

**(a)** Show that $-\alpha$ is also a root of $x^{p^n} - x$.

**(b)** Show that $\alpha + \beta$ is a root of $x^{p^n} - x$, using the "Freshman's dream."

**(c)** Show that $\alpha^{-1}$ is a root of $x^{p^n} - x$.

**(d)** Show that $\alpha\beta$ is a root of $x^{p^n} - x$.

We are now justified in using $\mathbb{F}_{p^n}$ to denote the *unique* field of order $p^n$. We can now identify the possibilities for one finite field to contain another finite field, which is item (7) of the theorem.

**Proposition 5.3.11.** *The field $\mathbb{F}_{p^d}$ is contained in $\mathbb{F}_{p^n}$ if and only if $d$ divides $n$.*

*Proof.* See Exercise 5.3.21. □

**Definition 5.3.12.** Let $m(x) \in \mathbb{F}_p[x]$ be a polynomial over $\mathbb{F}_p$. If $m(x)$ is irreducible and the coset $x + \langle m(x) \rangle$ is primitive in $\mathbb{F}_p[x]/m(x)$, then we say $m(x)$ is a **primitive polynomial**.

The following example shows that there can be many ways to construct a given field.

*Example* 5.3.13. Let $p = 2$. We can construct the field $\mathbb{F}_{2^3}$ by adjoining to $\mathbb{F}_2$ a root $\eta$ of the irreducible polynomial $m(x) = x^3 + x + 1$. Since the degree of $m(x)$ is 3, the elements of the field will be polynomials of degree less than 3 in $\eta$. Since $\mathbb{F}_3^*$ has 7 elements, any element, other than 1 generates the multplicative group. Thus we know that $\eta$ is primitive.

Here is the "dictionary" between powers of $\eta$ and corresponding polynomials in $\eta$. We use $\eta^3 = \eta + 1$ to compute successive rows in the table.

| exponential form | polynomial form |
|---|---|
| $1$ | $1$ |
| $\eta$ | $\eta$ |
| $\eta^2$ | $\eta^2$ |
| $\eta^3$ | $\eta + 1$ |
| $\eta^4$ | $\eta^2 + \eta$ |
| $\eta^5$ | $\eta^2 + \eta + 1$ |
| $\eta^6$ | $\eta^2 + 1$ |

The next line in the table would be

$$\eta^7 = \eta^3 + \eta = \eta + 1 + \eta = 1$$

This is to be expected, since $\mathbb{F}_8^*$ is a cyclic group of order 7.

We can use this table to verify that $\eta^2$ is another root of $x^3 + x + 1$.

$$\begin{aligned}(\eta^2)^3 + \eta^2 + 1 &= \eta^6 + \eta^2 + 1 \\ &= 0\end{aligned}$$

Similarly $\eta^4$ is also a root.

$$\begin{aligned}(\eta^4)^3 + \eta^4 + 1 &= \eta^{12} + \eta^4 + 1 \\ &= \eta^5 + \eta^4 + 1 \\ &= (\eta^2 + \eta + 1) + (\eta^2 + \eta) + 1 \\ &= 0\end{aligned}$$

The Finite Field Theorem says that there is a unique field of order 8 so every irreducible polynomial of degree 3 over $\mathbb{F}_2$ must have roots in the field that we constructed. There are 2 monic irreducible polynomials of degree 3 over $\mathbb{F}_2$: $x^3 + x + 1$, which we used to construct this field, and $x^3 + x^2 + 1$. As an exercise, show that $\eta^3$, $\eta^5$ and $\eta^7$ are the roots of $x^3 + x^2 + 1$.

Here is a multiplication table (omitting 0) for the representation of $\mathbb{F}_8$ using $x^3 + x + 1$.

| $*$ | $1$ | $\eta$ | $\eta+1$ | $\eta^2$ | $\eta^2+1$ | $\eta^2+\eta$ | $\eta^2+\eta+1$ |
|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $\eta$ | $\eta+1$ | $\eta^2$ | $\eta^2+1$ | $\eta^2+\eta$ | $\eta^2+\eta+1$ |
| $\eta$ | $\eta$ | $\eta^2$ | $\eta^2+\eta$ | $\eta+1$ | $1$ | $\eta^2+\eta+1$ | $\eta^2+1$ |
| $\eta+1$ | $\eta+1$ | $\eta^2+\eta$ | $\eta^2+1$ | $\eta^2+\eta+1$ | $\eta^2$ | $1$ | $\eta$ |
| $\eta^2$ | $\eta^2$ | $\eta+1$ | $\eta^2+\eta+1$ | $\eta^2+\eta$ | $\eta$ | $\eta^2+1$ | $1$ |
| $\eta^2+1$ | $\eta^2+1$ | $1$ | $\eta^2$ | $\eta$ | $\eta^2+\eta+1$ | $\eta+1$ | $\eta^2+\eta$ |
| $\eta^2+\eta$ | $\eta^2+\eta$ | $\eta^2+\eta+1$ | $1$ | $\eta^2+1$ | $\eta+1$ | $\eta$ | $\eta^2$ |
| $\eta^2+\eta+1$ | $\eta^2+\eta+1$ | $\eta^2+1$ | $\eta$ | $1$ | $\eta^2+\eta$ | $\eta^2$ | $\eta+1$ |

Now we consider the automorphism group of a finite field. Recall that any automorphism has to take 1 to itself, and must therefore fix the subfield $\mathbb{F}_p$.

**Proposition 5.3.14.** *The automorphism group of $\mathbb{F}_{p^n}$ is cyclic of order $n$, generated by the Frobenius map $\varphi : \alpha \longmapsto \alpha^p$.*

*Proof.* The Frobenius map respects addition, by the Freshman's dream, and it clearly respects multiplication: $\varphi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \varphi(\alpha)\varphi(\beta)$. Thus $\varphi$ is a homomorphism of fields. Since a homomorphism of fields must be injective, and since an injective function on a finite set is also surjective, we conclude that $\varphi$ is an automorphism.

Repeatedly composing the Frobenius with itself gives other automorphims and one can inductively establish the formula: $\varphi^t(\alpha) = \alpha^{p^t}$. Since $\mathbb{F}_{p^n}^*$ has order $p^n - 1$ we have for $\alpha \neq 0$, $\varphi^n(\alpha) = \alpha^{p^n} = \alpha^{p^n-1} * a = 1 * \alpha = \alpha$. Thus $\varphi^n$ is the identity map.

I claim no lower power of $\varphi$ is the identity map. Suppose that $\varphi^r$ is the identity automorphism and let $\eta$ be primitive in $\mathbb{F}_{p^n}$. Then $\eta = \varphi^r(\eta) = \eta^{p^r}$, so $\eta^{p^r-1} = 1$. Since $\eta$ is primitive it has order $p^n - 1$, so we see $r \geq n$ as claimed.

We need to show that there are no other automorphisms of $\mathbb{F}_{p^n}$. Let $\eta$ be primitive, and let $m(x) = x^n + m_{n-1}x^{n-1} + \cdots + m_0$ be its mimimum polynomial. The lemma showed that $\varphi^r(\eta) = \eta^{p^r}$ is another root of $m(x)$. Since $\eta$ is primitive, $\eta, \ldots, \eta^{p^{n-1}}$ are all distinct and thus they form the complete set of roots of $m(x)$.

Let $\sigma$ be an arbitrary automorphim of $\mathbb{F}_{p^n}$. Then $\sigma$ must take $\eta$ to one of these other roots of $m(x)$. The action of $\sigma$ on $\eta$ determines $\sigma$ completely, so if $\sigma(\eta) = \eta^{p^r}$ then $\sigma = \varphi^r$.

In conclusion $\mathrm{Aut}(\mathbb{F}_{p^n})$ is cyclic of order $n$, and is generated by $\varphi$. □

## Constructing Finite Fields

To construct the field $\mathbb{F}_p^n$ we need an irreducible polynomial of degree $n$ (which we may assume to be monic). How can we identify a monic irreducible? The analogous question for the integers (as compared to $\mathbb{F}_p[x]$ is: How can we identify prime numbers? Neither problem is easy to address. Since we are not concerned here developing the most efficient methods to find irreducibles, we will fall back on something akin to the Sieve or Eratosthenes, which is a method for finding primes.

The process proceeds iteratively. Assume that we have identified all monic irreducibles of degree less than $n$. We show how to find all monic irreducibles of degree $n$. We list all polynomials of degree $n$. Then eliminate all products of the irreducibles of degree less than $n$ that give a polynomial of degree $n$ (which will, by construction, be reducible). The polynomials of degree $n$ remaining after this process are irreducible.

For $n = 3$ one must consider a product of 3 linear factors and a product of a linear and an irreducible quadratic. For degree 4 one must consider a product of 4 linear factors, a product of two linear factors and an irreducible quadratic, a product of one linear and an irreducible cubic, and a product of two irreducible quadratics.

*Exercises* 5.3.15. Irreducible polynomials over $\mathbb{F}_2$.

We have seem that there is one irreducible of degree 2 over $\mathbb{F}_2$, $x^2 + x + 1$.

**(a)** Find all irreducible polynomials over $\mathbb{F}_2$ of degree at most 4. You should justify your list.

**(b)** Find all all irreducible polynomials over $\mathbb{F}_2$ of degree 5. Use the list from part (a) to explain your result. Notice any patterns in the list of polynomials.

**(c)** Determine how many irreducible polynomials of degree 6 there are over $\mathbb{F}_2$ based on part (a). Justify your answer briefly.

*Example* 5.3.16. Consider now the degree 3 extension of $\mathbb{F}_3$, the field with 27 elements, $\mathbb{F}_{27}$. In this field there is just one subfield $\mathbb{F}_3$, so there are 24 elements that have a minimal polynomial of degree 3. Each of these minimal polynomials factors completely in $\mathbb{F}_{27}$ by Proposition 5.3.7. Thus we have $24/3 = 8$ monic irreducible polynomials of degree 3 over $\mathbb{F}_3$.

Let's count the number of irreducible monic polynomials of degree 3 over $\mathbb{F}_3$ using the method related to the Sieve of Eratosthenes. The monic polynomials of degree 3 over $\mathbb{F}_3$ are all of the form $x^3 + a_2x^2 + a_1x + a_0$ for $a_i \in \mathbb{F}_3$. Thus there are 27 monic polynomials of degree 3. A reducible polynomial is either the product of 3 linear factors or the product of a linear and a quadratic irreducible. There are 3 monic linear polynomials, and 3 monic quadratic irreducibles, so 9 possible products. For a product of linear monic polynomials we choose 3 factors with replacement from the 3 linear polynomials, so there are $\binom{3+2}{3} = 10$ possibilites. Thus the number of irreducibles shoule be $27 - 9 - 10 = 8$. That checks with our computation from the previous paragraph.

The multiplicative group $\mathbb{F}_{27}^*$ is cyclic of order 26. In $\mathbb{Z}/26$ the odd numbers, other than 13, are all generators for the group so there are 12 generators. Consequently in $\mathbb{F}_{27}^*$ there are 12 primitive elements. Each is a root of one of the monic irreducible polynomials of degree 3, so we expect $12/3 = 4$ different primitive monic polynomials of degree 3.

Here are the monic irreducibles of degree 3 over $\mathbb{F}_3$ that are not primitive

$$x^3 + 2x^2 + 2x + 2,$$
$$x^3 + x^2 + x + 2$$
$$x^3 + 2x + 2$$
$$x^3 + x^2 + 2,$$

and here are the ones that are primitive.

$$x^3 + 2x + 1$$
$$x^3 + 2x^2 + x + 1$$
$$x^3 + x^2 + 2x + 1$$
$$x^3 + 2x^2 + 1$$

*Exercises* 5.3.17. The field $\mathbb{F}_{2^3}$.

**(a)** Construct the multiplication table for the field $\mathbb{F}_8$ using $x^3 + x^2 + 1$.

**(b)** Make a table showing the powers of the primitive element, call it $\eta$, and the corresponding vector form, using the basis $\{1, \eta, \eta^2\}$.

**(c)** Show that the polynomial $x^3 + x + 1$ also has roots in your construction of $\mathbb{F}_8$.

*Exercises* 5.3.18. The field $\mathbb{F}_{16}$.

**(a)** One of the irreducible polynomials of degree 4 in Exercise 5.3.15 has roots which are not primitive. Which one?

**(b)** Construct the field with 16 elements using one of the primitive irreducible polynomials of degree 4: Make a table showing the powers of the primitive element, call it $\eta$, and the corresponding vector form, using the basis $\{1, \eta, \eta^2, \eta^3\}$. Give also the multiplicative order of each element and its minimal polynomial.

**(c)** Identify the subfield $\mathbb{F}_4$.

**(d)** Factor over $\mathbb{F}_4$ the irreducible polynomial that you chose to construct $\mathbb{F}_{16}$.

**(e)** How many elements of $\mathbb{F}_{16}$ are primitive?

*Exercises* 5.3.19. The field $\mathbb{F}_{3^2}$.

**(a)** Write a multiplication table for $\mathbb{F}_3[x]/\langle x^2 + x + 2\rangle$. [You may omit 0. It may be easier to take the elements in the order $1, x, x+1, x+2$ followed by twice each.]

**(b)** Find all irreducible polynomials of degree 2 over $\mathbb{F}_3$ and find their roots in the table you constructed.

*Exercises* 5.3.20. Factoring a polynomial over different fields.

**(a)** Factor $x^9 - x$ over $\mathbb{F}_3$.

**(b)** Factor $x^5 + x^4 + 1$ over $\mathbb{F}_2$ (it is reducible!), $\mathbb{F}_4$ and $\mathbb{F}_8$.

**(c)** Factor $x^{16} - x$ over $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$ and $\mathbb{F}_{16}$.

*Exercises* 5.3.21. Subfields of a Finite Field

Let $n > m$ be positive integers and $d = \gcd(n, m)$. Show that the intersection of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ is $\mathbb{F}_{p^d}$ as follows.

**(a)** Recall that the remainder $x^n - 1$ divided by $x^m - 1$ is $x^r - 1$ where $r$ is the remainder when $n$ is divided by $m$.

**(b)** Show that the gcd of $x^n - 1$ and $x^m - 1$ is $x^d - 1$.

**(c)** Combine the previous results and the theorem that the roots of $x^{p^n} - x$ are the elements of $\mathbb{F}_{p^n}$ to conclude that $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$ iff $d$ divides $n$. (Strictly speaking $\mathbb{F}_{p^n}$ has a subfield isomorphic to $\mathbb{F}_{p^d}$. See 11.10.)

*Exercises* 5.3.22. Subfields and (multiplicative) order of an element.

**(a)** Make a table showing the possible multiplicative orders and the number of elements of each order for $\mathbb{F}_{64}$, $\mathbb{F}_{128}$, and $\mathbb{F}_{256}$. Relate this information to subfields (refer to the previous problem).

*Exercises* 5.3.23. The Field $\mathbb{F}_{81}$.

**(a)** The polynomials $x^2+x+2$ and $x^2+2x+2$ are both irreducible over $\mathbb{F}_3$. Can you construct $\mathbb{F}_{81}$ by using one of these polynomials and then the other?

**(b)** In a computer algebra system use $m(x) = x^4 + x + 2$ and $r(x) = x^4 + 2x + 2$ to construct two versions of $\mathbb{F}_{81}$. Using a brute force search, find a root of $m(x)$ in the second field and a root of $r(x)$ in the first field. These give isomorphisms between the two fields. Check by hand that each composition is an automorphism of the appropriate version of $\mathbb{F}_{81}$.

**(c)** Factor $x^{80} - 1$ over $\mathbb{F}_3$. For each irreducible factor $a(x)$, find the roots of $a(x)$ in $\mathbb{F}_3[x]/m(x)$.

*Exercises* 5.3.24. The field $\mathbb{F}_{64}$.

**(a)** The polynomials $m(x) = x^6 + x + 1$ and $r(x) = x^6 + x^5 + x^4 + x + 1$ are both irreducible over $\mathbb{F}_2$. Using a computer algebra system construct two versions of $\mathbb{F}_{64}$, using $m(x)$ for one and $r(x)$ for the other. Using a brute force search, find a root of $m(x)$ in the second field and a root of $r(x)$ in the first field. These give isomorphisms between the two fields. Check by hand that each composition of the two isomorphisms is an automorphism of the appropriate version of the field.

**(b)** Factor $x^{63} - 1$ over $\mathbb{F}_2$. For each irreducible factor $a(x)$, find the roots of $a(x)$ in $\mathbb{F}_2[x]/m(x)$. Use Sage, but also use your understanding of the theory.

**(c)** The field $\mathbb{F}_{64}$ can also be constructed as an extension of $\mathbb{F}_4$. Construct $\mathbb{F}_4$, then factor $x^{63}-1$ in $\mathbb{F}_4[x]$. Choose one of the factors of degree 3 to construct $\mathbb{F}_{64}$.

**(d)** Now create $\mathbb{F}_8$ using an irreducible polynomial of degree 3 over $\mathbb{F}_2$, then factor $x^{63}-1$, then create $\mathbb{F}_{64}$ using an irreducible polynomial of degree 2 in $\mathbb{F}_8[x]$.

*Exercises* 5.3.25. The algebraic closure of $\mathbb{F}_p$.

This problem extends Exercise 5.3.21, which showed that we may consider $\mathbb{F}_{p^d}$ as contained in $\mathbb{F}_{p^n}$ if and only if $d|n$.

**(a)** Let $\overline{\mathbb{F}}_p = \bigcup_{t\geq 1} \mathbb{F}_{p^t}$. Prove that $F$ is a field.

**(b)** Prove that $\overline{\mathbb{F}}_p$ is algebraically closed.

**(c)** Prove that every element of $\overline{\mathbb{F}}_p$ is algebraic over $\mathbb{F}_p$ so there is no algebraically closed field properly contained in $\overline{\mathbb{F}}_p$.

**(d)** Conclude that $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_{p_n}$ for any $n$.

*Exercises* 5.3.26. Irreducible polynomials over $\mathbb{F}_p$.

Suppose you have formulas for the number of irreducible monic polynomials of degree $m$ over $\mathbb{F}_p$ for each $m < n$. Using some combinatorial arguments you can then compute the number of monic reducible polynomials of degree $n$. Subtracting this from the number of monic polynomials of degree $n$ yields the number of monic irreducible polynomials of degree $n$.

**(a)** Show that the number of monic irreducible quadratics over $\mathbb{F}_p$ is $(p^2-p)/2$.

**(b)** Show that the number of monic irreducible cubics over $\mathbb{F}_p$ is $(p^3-p)/3$.

**(c)** You might want to guess at a general formula. A different counting method yields the result more easily than the one above. Try this if you want, noting:

- For $a \in \mathbb{F}_{p^n}$, $a$ is in no proper subfield iff the minimal polynomial for $a$ has degree $n$.
- Each monic irreducible of degree $n$ has $n$ distinct roots in $\mathbb{F}_{p^n}$.