## 21 Field extensions

After the zero ring, fields[1] are the commutative rings with the simplest imaginable ideal structure. Because of the absence of non-trivial ideals, all homomorphisms $K \to L$ between fields are injective, and this allows us to view them as *inclusions*.

There can exist multiple inclusions between given fields $K$ and $L$, and it is often useful (see 23.2) to study the entire set $\mathrm{Hom}(K, L)$ of field homomorphisms $K \to L$.

### ▶ Extension Fields

An *extension field* of a field $K$ is a field $L$ that contains $K$ as a subfield. We call $K \subset L$ a *field extension* and also denote it by $L/K$. The classical examples in analysis are the field extensions $\mathbf{Q} \subset \mathbf{R}$ and $\mathbf{R} \subset \mathbf{C}$. Every field $K$ can be viewed as an extension field of a minimal field $k \subset K$.

**21.1. Theorem.** *Let $K$ be a field. Then the intersection $k$ of all subfields of $K$ is again a field, and it is isomorphic to $\mathbf{Q}$ or to a finite field $\mathbf{F}_p$.*

**Proof.** We consider the unique ring homomorphism $\phi : \mathbf{Z} \to K$. The image $\phi[\mathbf{Z}]$ is contained in every subfield of $K$, hence also in $k$. Since $\mathbf{Z}/\ker(\phi) \cong \phi[\mathbf{Z}]$ is a subring of a field and therefore an integral domain, $\ker\phi$ is a prime ideal in $\mathbf{Z}$. If $\phi$ is non-injective, then we have $\ker\phi = p\mathbf{Z}$ for a prime $p$, in which case $\phi[\mathbf{Z}] \cong \mathbf{F}_p$ is a subfield of $k$ and therefore equal to $k$. If $\phi$ is injective, then $k$ contains a subring $\phi[\mathbf{Z}] \cong \mathbf{Z}$. Since every field that contains $\mathbf{Z}$ also contains quotients of elements of $\mathbf{Z}$, we find that, in this case, $k$ contains a subfield isomorphic to $\mathbf{Q}$ and must therefore itself be isomorphic to $\mathbf{Q}$. □

The non-negative generator of $\ker\phi$ in 21.1 is the *characteristic* $\mathrm{char}(K)$ of $K$, and the field $k \subset K$ is the *prime field* of $K$. We have $\mathrm{char}(K) = p$ when $k \cong \mathbf{F}_p$ and $\mathrm{char}(K) = 0$ when $k \cong \mathbf{Q}$.

**Exercise 1.** Do there exist homomorphisms between fields of different characteristics?

For a field extension $K \subset L$, by restriction, the multiplication $L \times L \to L$ gives a scalar product $K \times L \to L$. This makes $L$ into a vector space over $K$.

**Exercise 2.** Determine which ring axioms imply that $L$ is a $K$-vector space.

By 16.6, for every field extension $K \subset L$, we can choose a basis for $L$ as a vector space over $K$; by 16.7, the cardinality of such a basis, the dimension of $L$ over $K$, is independent of the choice.

**21.2. Definition.** *The degree $[L : K]$ of a field extension $K \subset L$ is the dimension of $L$ as a $K$-vector space.*

A field extension of finite degree is called *finite* for short. Finite field extensions of $\mathbf{Q}$ are called *number fields*. Examples are the fields of fractions $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-5})$ of the rings $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{-5}]$ from §12. Extensions of degree 2 and 3 are called *quadratic* and *cubic*, respectively.

In a *chain* $K \subset L \subset M$ of field extensions, also called a *tower* of fields, the degree behaves multiplicatively.

**21.3. Theorem.** *Let $K \subset L \subset M$ be a tower of fields, $X$ a $K$-basis for $L$, and $Y$ an $L$-basis for $M$. Then the set of elements $xy$ with $x \in X$ and $y \in Y$ forms a $K$-basis for $M$, and we have*

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

*In particular, $K \subset M$ is finite if and only if $K \subset L$ and $L \subset M$ are finite.*

**Proof.** Every element $c \in M$ can be written uniquely as $c = \sum_{y \in Y} b_y \cdot y$ with coefficients $b_y \in L$ that are almost all 0. The elements $b_y \in L$ each have a unique representation as $b_y = \sum_{x \in X} a_{xy} x$ with coefficients $a_{xy} \in K$ that are almost all 0. Substituting this in the first representation, we obtain a unique way to write $c$ as a finite $K$-linear combination of the elements $xy$ with $x \in X$ and $y \in Y$:

$$c = \sum_{y \in Y} (\sum_{x \in X} a_{xy} x) y = \sum_{(x,y) \in X \times Y} a_{xy} xy.$$

In particular, the elements $xy$ with $(x, y) \in X \times Y$ form a basis for $M$ over $K$.

Because the cardinality of $X \times Y$ is equal to $\#X \cdot \#Y$, we obtain the product relation $[M : K] = [M : L] \cdot [L : K]$ for the degrees. It is clear that $X \times Y$ is finite if and only if $X$ and $Y$ are finite, because $X$ and $Y$ are non-empty. □

In an extension $K \subset L$, every element $\alpha \in L$ generates a subring

$$K[\alpha] = \{\textstyle\sum_{i \geq 0} c_i \alpha^i : c_i \in K\} \subset L$$

consisting of polynomial expressions in $\alpha$ with coefficients in $K$. Since $K[\alpha]$ is a subring of a field, it is an integral domain; we denote the field of fractions of $K[\alpha]$ by $K(\alpha) \subset L$. This field, which is the smallest subfield of $L$ that contains both $K$ and $\alpha$, is called the extension of $K$ *generated* by $\alpha$.

More generally, given a subset $S \subset L$, we can form the ring $K[S] \subset L$ consisting of polynomial expressions in the elements of $S$ with coefficients in $K$. Since this ring is a subring of $L$, it is again an integral domain; we denote its field of fractions by $K(S) \subset L$. The field $K(S)$ is the smallest subfield of $L$ that contains $K$ and $S$. It is the extension of $K$ *generated by* $S$.

A field extension of $K$ generated by a finite set $S$ is said to be *finitely generated* over $K$. For $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, we write $K[S] = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$ and $K(S) = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. When $S$ consists of a single element, we speak of a *simple* or *primitive* extension of $K$. If $K_1$ and $K_2$ are subfields of $L$ containing $K$, then the subfield $K_1 K_2 \subset L$ generated by $S = K_1 \cup K_2$ over $K$ is called the *compositum* of $K_1$ and $K_2$ in $L$.

**Exercise 3.** Show that a compositum (in $L$) of finitely generated extensions of $K$ is again finitely generated.

**21.4. Example.** In the extension $\mathbf{Q} \subset \mathbf{C}$, the element $\sqrt{2}$ generates the ring

$$\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$$

over $\mathbf{Q}$. Because of the identity $(\sqrt{2})^2 = 2 \in \mathbf{Q}$, no higher powers of $\sqrt{2}$ are needed. The ring $\mathbf{Q}[\sqrt{2}]$ is equal to its field of fractions $\mathbf{Q}(\sqrt{2})$ because every element $a + b\sqrt{2} \neq 0$ has an inverse $\frac{1}{a^2-2b^2}(a - b\sqrt{2}) \in \mathbf{Q}[\sqrt{2}]$.

Similarly, every element $d \in \mathbf{Q}$ that is not a square in $\mathbf{Q}$ leads to a *quadratic field* $\mathbf{Q}(\sqrt{d})$, which is of degree 2 over $\mathbf{Q}$.

For the set $S = \{i, \sqrt{2}\} \subset \mathbf{C}$, we obtain $\mathbf{Q}[S] = \mathbf{Q}(S)$ as a quadratic extension $L(i)$ of the field $L = \mathbf{Q}(\sqrt{2})$. After all, $-1$ is not a square in the real field $L \subset \mathbf{R}$. By 21.3, the field $\mathbf{Q}(\sqrt{2}, i) = L(i)$ is of degree $[L(i) : L] \cdot [L : \mathbf{Q}] = 2 \cdot 2 = 4$ over $\mathbf{Q}$ with basis $\{1, i, \sqrt{2}, i\sqrt{2}\}$.

### ▶ Algebraic and transcendental numbers

An element $\alpha$ in an extension field $L$ of $K$ is said to be *algebraic* over $K$ if there exists a polynomial $f \in K[X] \setminus \{0\}$ with $f(\alpha) = 0$. If such an $f$ does not exist, $\alpha$ is called *transcendental* over $K$. The extension $K \subset L$ is called *algebraic* if every element $\alpha \in L$ is algebraic over $K$. In the case of the extension $\mathbf{Q} \subset \mathbf{C}$, we simply speak of algebraic and transcendental numbers. Examples of algebraic numbers are 3, $\sqrt{2}$, $\sqrt[3]{10}$, and the primitive $n$th root of unity $\zeta_n = e^{2\pi i/n}$ for $n \geq 1$. Polynomials in $\mathbf{Q}[X]$ that have these numbers as zeros are, respectively,

$$X - 3, \qquad X^2 - 2, \qquad X^3 - 10, \qquad X^n - 1.$$

Note that the first three polynomials are irreducible in $\mathbf{Q}[X]$, whereas $X^n - 1$ is not for $n > 1$.

**Exercise 4.** For $1 \leq n < 10$, find irreducible polynomials in $\mathbf{Q}[X]$ with zero $e^{2\pi i/n}$.

Because there are only countably many algebraic numbers (Exercise 21) and $\mathbf{C}$ is uncountable, there are a great many transcendental numbers. The Frenchman Joseph Liouville (1809–1882) already showed around 1850 that very quickly converging series such as $\sum_{k\geq 0} 10^{-k!}$ always have a transcendental value. It is often difficult to prove that a number that "has no reason to be algebraic" is indeed transcendental.

The first proofs of transcendence[2] for the well-known real numbers $e = \exp(1)$ and $\pi$ were given in 1873 and 1882 by the Frenchman Hermite (1822–1901) and the German Lindemann (1852–1939), respectively. Independently of each other, in 1934, the Russian Gelfond (1906–1968) and the German Schneider (1911–1988) found a solution to one of the well-known *Hilbert problems*[3] from 1900: for every pair of algebraic numbers $\alpha \neq 0, 1$ and $\beta \notin \mathbf{Q}$, the expression $\alpha^\beta$ is transcendental.

**Exercise 5.** Use this to deduce that not only $2^{\sqrt{2}}$ but also $\log 3/\log 2$ and $e^\pi$ are transcendental.

Of many real numbers, like Euler's constant $\gamma = \lim_{k\to\infty}(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{k} - \log k)$ and the numbers $2^e$, $2^\pi$, and $\pi^e$, it is not even known whether they are rational.

**21.5. Theorem.** *Let $K \subset L$ be a field extension and $\alpha \in L$ an element.*

1. *If $\alpha$ is transcendental over $K$, then $K[\alpha]$ is isomorphic to the polynomial ring $K[X]$ and $K(\alpha)$ is isomorphic to the field $K(X)$ of rational functions.*
2. *If $\alpha$ is algebraic over $K$, then there is a unique monic, irreducible polynomial $f = f_K^\alpha \in K[X]$ that has $\alpha$ as zero. In this case, there is a field isomorphism*

$$\begin{aligned} K[X]/(f_K^\alpha) &\xrightarrow{\sim} K[\alpha] = K(\alpha) \\ g \bmod (f_K^\alpha) &\longmapsto g(\alpha), \end{aligned}$$

*and the degree $[K(\alpha) : K]$ is equal to $\deg(f_K^\alpha)$.*

**Proof.** We consider the ring homomorphism $\phi : K[X] \to L$ given by $f \mapsto f(\alpha)$. The image of $\phi$ is equal to $K[\alpha]$, and as in the proof of 21.1, we have two possibilities.

If $\alpha$ is transcendental over $K$, then $\phi$ is injective, and we obtain an isomorphism $K[X] \xrightarrow{\sim} K[\alpha]$ of $K[\alpha]$ with the polynomial ring $K[X]$. The field of fractions $K(\alpha)$ is then isomorphic to $K(X)$.

If $\alpha$ is algebraic over $K$, then $\ker \phi$ is a non-trivial ideal of $K[X]$. Since $K[X]$ is a principal ideal domain, there is a unique monic generator $f = f_K^\alpha \in K[X]$ of $\ker \phi$. This is the "smallest" monic polynomial $K[X]$ that has $\alpha$ as zero. The isomorphism theorem gives an isomorphism $K[X]/(f_K^\alpha) \xrightarrow{\sim} K[\alpha] \subset L$ of integral domains, so $(f_K^\alpha)$ is a prime ideal in $K[X]$ and $f_K^\alpha$ is irreducible. Since a prime ideal $(f_K^\alpha) \neq 0$ in a principal ideal domain is maximal (see 15.6), we have that $K[X]/(f_K^\alpha) \cong K[\alpha]$ is a field and therefore equal to $K(\alpha)$. Modulo $(f_K^\alpha)$, every polynomial in $K[X]$ has a unique representative $g$ of degree $\deg(g) < \deg(f_K^\alpha)$: the remainder after dividing by $f_K^\alpha$. If $f_K^\alpha$ has degree $n$, then the residue classes of $\{1, X, X^2, \ldots, X^{n-1}\}$ form a basis for $K[X]/(f_K^\alpha)$ over $K$. In particular, $K[\alpha] = K(\alpha)$ has dimension $[K(\alpha) : K] = n = \deg(f_K^\alpha)$ over $K$. □

**21.6. Corollary.** *Every finite field extension is algebraic.*

**Proof.** For $K \subset L$ finite and $\alpha \in L$ arbitrary, for sufficiently large $n$, the powers $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^n$ are not linearly independent over $K$. But, a dependence relation $\sum_{k=0}^n a_k \alpha^k = 0$ says precisely that the polynomial $f = \sum_{k=0}^n a_k X^k \in K[X] \setminus \{0\}$ has zero $\alpha$ and that $\alpha$ is algebraic over $K$. □

The polynomial $f_K^\alpha$ in 21.5.2 is called the *minimum polynomial* or the *irreducible polynomial* of $\alpha$ over $K$. Every polynomial $g \in K[X]$ with $g(\alpha) = 0$ is divisible by $f_K^\alpha$. Conversely, let us show that every monic, irreducible polynomial in $K[X]$ can be viewed as the minimum polynomial of an element $\alpha$ in an extension field $L$ of $K$.

**21.7. Theorem.** *Let $K$ be a field and $f \in K[X]$ a non-constant polynomial. Then there exists an extension $K \subset L$ in which $f$ has a zero $\alpha$. If $f \in K[X]$ is monic and irreducible, then we moreover have $f = f_K^\alpha$.*

**Proof.** We assume that $f$ is irreducible because for reducible $f$, every zero of an irreducible factor of $f$ in $K[X]$ is also a zero of $f$. The ideal $(f) \subset K[X]$ is then maximal, and $L = K[X]/(f)$ is a field. The composition

$$\varphi : K \to K[X] \to K[X]/(f) = L$$

is a field homomorphism and therefore injective; hence, through $\varphi$, we can view $L$ as an extension field of $K$. The element $\overline{X} = (X \bmod f) \in L$ is now "by definition" a zero of the polynomial $f(Y) \in K[Y] \subset L[Y]$. After all, we have

$$f(\overline{X}) = \overline{f(X)} = \overline{0} \in K[X]/(f) = L.$$

If in addition to being irreducible, $f$ is also monic, then $f$ is the minimum polynomial of $\overline{X}$. □

The field $L = K[X]/(f)$ constructed in the proof of 21.7 for an irreducible polynomial $f \in K[X]$ is the field obtained through the *formal adjunction* of a zero of $f$ to $K$. This important construction allows us to construct a field extension of $K$ in which a given polynomial has a zero.

**21.8. Examples. 1.** The polynomial $f = X^2+1$ is irreducible over $\mathbf{R}$, and the formal adjunction of a zero of $f$ gives the extension field $\mathbf{R}[X]/(X^2+1)$ of $\mathbf{R}$. In this field, which consists of expressions $a+bX$ with $a, b \in \mathbf{R}$, we have, by definition, the relation $X^2 = -1$. Of course, this field constructed through the adjunction of a square root of $-1$ to $\mathbf{R}$ is nothing but the well-known field $\mathbf{C}$: the map $a + bX \mapsto a + bi$ gives an isomorphism. We can also find this isomorphism by applying 21.5.2 to the extension $\mathbf{R} \subset \mathbf{C}$ with $\alpha = i \in \mathbf{C}$. Note that there are numerous polynomials $g \in \mathbf{R}[X]$ for which $\mathbf{R}[X]/(g) \cong \mathbf{C}$ holds, namely all quadratic polynomial without real zeros, such as $X^2 + X + r$ with $r > \frac{1}{4}$.

**2.** If, in the above, we replace the base field $\mathbf{R}$ by $\mathbf{Q}$, then $f = X^2 + 1$ is still irreducible. The field $\mathbf{Q}[X]/(X^2+1)$ is nothing but the number field $\mathbf{Q}(i)$ that we already came across in Theorem 12.19 as the field of fractions of the ring $\mathbf{Z}[i]$ of Gaussian integers. More generally, for an element $d \in \mathbf{Q}$ that is not a square in $\mathbf{Q}$, the polynomial $g = X^2 - d$ gives the quadratic field $\mathbf{Q}(\sqrt{d})$ from 21.4.

Similarly, for every number $d \in \mathbf{Q}$ that is not a third power in $\mathbf{Q}$, by formally adjoining a zero $\sqrt[3]{d}$ of the irreducible polynomial $X^3 - d \in \mathbf{Q}[X]$, we can make an extension $\mathbf{Q}(\sqrt[3]{d})$ of degree 3 over $\mathbf{Q}$. Note that no real or complex numbers are involved in this construction: $\sqrt[3]{d}$ is a *formal zero* of $X^3 - d$ that does not, a priori, lie in $\mathbf{R}$ or $\mathbf{C}$. The question of what the compositum of $\mathbf{R}$ and the cubic field $\mathbf{Q}(\sqrt[3]{d})$ in $\mathbf{C}$ is therefore has no meaning as long as no *choice* has been made of a third root $\sqrt[3]{d}$ of $d$ in $\mathbf{C}$: there are three!

**Exercise 6.** Show that the answer depends on the choice of $\sqrt[3]{d}$ in $\mathbf{C}$.

**3.** The number field $\mathbf{Q}(\zeta_p)$ obtained through the adjunction of a formal zero $\zeta_p$ of the $p$th cyclotomic polynomial $\Phi_p \in \mathbf{Z}[X]$ from Example 13.9.2 to $\mathbf{Q}$ is called the *pth cyclotomic field*. It has degree $\deg(\Phi_p) = p - 1$ over $\mathbf{Q}$. We will study $\mathbf{Q}(\zeta_p)$ further in 24.9.

For a field extension $K \subset L$, we can also consider the evaluation map $K[X] \to L$ in a point $\alpha \in L$ for $n$-tuples of elements from $L$. We call a subset $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset L$

*algebraically independent* over $K$ if the homomorphism

$$\begin{aligned} K[X_1, X_2, \ldots, X_n] &\longrightarrow L \\ f &\longmapsto f(\alpha_1, \alpha_2, \ldots, \alpha_n) \end{aligned}$$

is injective. Informally, this means that there are no algebraic relations between the elements $\alpha_i \in L$. An infinite subset $S \subset L$ is called algebraically independent over $K$ if every one of its finite subsets is so. An extension $K \subset K(S)$ generated by an algebraically independent set $S \subset L$ is called a *purely transcendental extension* of $K$. If a set $S \subset L$ is algebraically independent over $K$ and $K(S) \subset L$ is an algebraic extension, then $S$ is called a *transcendence basis* of $L$ over $K$. It is a "maximal" algebraically independent set in $L$.

**Exercise 7.** Prove that every field extension has a transcendence basis. [Hint: Zorn...]

## ▶ Explicit Calculations

Arithmetic in a finite extension $L$ of $K$ is a fairly direct combination of arithmetic in polynomial rings and techniques from linear algebra and can easily be carried out by present-day[4] computer algebra packages. Nevertheless, it is useful to develop a feeling for the nature of such calculations and be able to carry them out by hand in simple cases. In more complicated cases, packages that can compute with formal zeros offer a solution.

We illustrate the calculations using the extension $\mathbf{Q} \subset M = \mathbf{Q}(i, \sqrt{2})$ from 21.4. Here, we have $[M : \mathbf{Q}] = 4$, and we can take $\{1, i, \sqrt{2}, i\sqrt{2}\}$ as a basis for $M$ over $\mathbf{Q}$. By 21.6, every element $\alpha \in M$ is algebraic over $\mathbf{Q}$. The minimum polynomial of such an element is determined by expressing successive powers of $\alpha$ in the chosen basis until a dependence occurs between these powers. For $\alpha = 1 + i + \sqrt{2}$, sheer perseverance leads to the following representation of the powers of $\alpha$ in the chosen basis:

$$\begin{aligned} \alpha^0 &= (1,\ \ 0,\ \ 0,\ \ 0), \\ \alpha^1 &= (1,\ \ 1,\ \ 1,\ \ 0), \\ \alpha^2 &= (2,\ \ 2,\ \ 2,\ \ 2), \\ \alpha^3 &= (4,\ \ 8,\ \ 2,\ \ 6), \\ \alpha^4 &= (0, 24,\ \ 0, 16). \end{aligned}$$

The fifth vector is the first to depend on the previous ones. Using standard techniques, we find the relation

$$\alpha^4 - 4\alpha^3 + 4\alpha^2 + 8 = 0.$$

When calculating by hand, there are sometimes tricks that shorten the work. By squaring the equality $\alpha - 1 = i + \sqrt{2}$, we find $\alpha^2 - 2\alpha + 1 = 1 + 2i\sqrt{2}$, and squaring $\alpha^2 - 2\alpha = 2i\sqrt{2}$ gives the desired relation

$$\alpha^4 - 4\alpha^3 + 4\alpha^2 = -8.$$

Unlike in the first case, we have no guarantee that this relation is of minimal degree. We must therefore check separately whether $X^4 - 4X^3 + 4X^2 + 8$ is irreducible in $\mathbf{Q}[X]$.

**Exercise 8.** Show that $\frac{1}{8}X^4 f(\frac{2}{X})$ is Eisenstein at 2 in $\mathbf{Z}[X]$. Conclude that $f$ is irreducible.

We conclude from the above that $M = \mathbf{Q}(i, \sqrt{2})$ is equal to the simple extension $\mathbf{Q}(\alpha) = \mathbf{Q}[X]/(X^4 - 4X^3 + 4X^2 + 8)$. The element $\alpha$ is called a *primitive element* for the extension $\mathbf{Q} \subset M$, and $\{1, \alpha, \alpha^2, \alpha^3\}$ is called a *power basis* for $M$ over $\mathbf{Q}$. In 23.9, we will see that many field extensions have a power basis. Since algebra packages prefer to work with a generating element, it can be useful to search for a "small generator."

**Exercise 9.** Show that $\beta = \frac{1}{2}\sqrt{2} + \frac{1}{2}i\sqrt{2}$ satisfies $\beta^4 + 1 = 0$ and that we have $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$. Write $i$ and $\sqrt{2}$ in the basis consisting of powers of $\beta$.

Multiplication in a field such as $M = \mathbf{Q}(\alpha)$ is done by multiplying expressions as polynomials in $\alpha$ and reducing the outcome modulo the relation given by the minimum polynomial of $\alpha$. This means that, as in 12.1, we determine the remainder of the polynomial that describes the expression after dividing by $f = f^{\alpha}_{\mathbf{Q}}$. For a basis that is not a power basis, such as the basis $\{1, i, \sqrt{2}, i\sqrt{2}\}$, we need to know how the product of two elements of the basis looks in the given basis.

The inverse of an element $g(\alpha) \in \mathbf{Q}(\alpha)$ is determined using either linear algebra or the Euclidian algorithm. For example, to determine the inverse of $\alpha^2 + 2\alpha \in M$, for the former, we write the equation

$$(a + b\alpha + c\alpha^2 + d\alpha^3)(\alpha^2 + 2\alpha) = 1$$

in the basis $\{1, \alpha, \alpha^2, \alpha^3\}$, as

$$(-1 - 8c - 48d) + 2(a - 4d)\alpha + (a + 2b - 4c - 24d)\alpha^2 + (b + 6c + 20d)\alpha^3 = 0.$$

The system of linear equations obtained by setting all coefficients equal to 0 can now be solved using standard methods: the solution is $(a, b, c, d) = (-\frac{2}{9}, -\frac{5}{36}, \frac{5}{24}, -\frac{1}{18})$.

When the Euclidian algorithm is used as in 6.14, the inverse of an element $g(\alpha)$ can be determined by repeatedly applying division with remainders to the relations $0 \cdot g(\alpha) = f(\alpha)$ and $1 \cdot g(\alpha) = g(\alpha)$. If, for example, we take $g(\alpha) = \alpha^2 + 2\alpha \in M = \mathbf{Q}(\alpha)$, we find

$$\begin{aligned} 0 \cdot (\alpha^2 + 2\alpha) &= f(\alpha) = \alpha^4 - 4\alpha^3 + 4\alpha^2 + 8 \\ 1 \cdot (\alpha^2 + 2\alpha) &= g(\alpha) = \alpha^2 + 2\alpha \\ (-\alpha^2 + 6\alpha - 16) \cdot (\alpha^2 + 2\alpha) &= -32\alpha + 8 \\ (-4\alpha^3 + 15\alpha^2 - 10\alpha - 16) \cdot (\alpha^2 + 2\alpha) &= 72. \end{aligned}$$

The last equation has been multiplied by 128 to get rid of all denominators. We again find $g(\alpha)^{-1} = -\frac{1}{18}\alpha^3 + \frac{5}{24}\alpha^2 - \frac{5}{36}\alpha - \frac{2}{9}$. In larger fields, carrying out such calculations by hand quickly becomes time-consuming.

## ▶ Algebraic Closure

It follows from 21.5 that an element $\alpha$ in an extension field $L$ of $K$ is algebraic over $K$ if and only if $K(\alpha)$ is a finite extension of $K$. More generally, a finitely generated extension $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of $K$ is finite if and only if all $\alpha_i$ are algebraic over $K$. The

condition is clearly necessary: a transcendental element generates an infinite extension. It is also sufficient because for algebraic $\alpha_i$, the extension $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ can be obtained as a tower

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

of $n$ simple finite extensions. By 21.3, this gives a finite extension, and by 21.6, it is algebraic. For $n = 2$, we see that sums, differences, products, and quotients of algebraic elements $\alpha_1$ and $\alpha_2$ are also algebraic over $K$. It follows that for an arbitrary extension $K \subset L$, the set

$$K_0 = \{\alpha \in L : \alpha \text{ is algebraïsch over } K\}$$

is a *subfield* of $L$. It is called the *algebraic closure of $K$ in $L$*. It is the largest algebraic extension of $K$ in $L$.

**21.9. Theorem.** *For a tower $K \subset L \subset M$ of fields, we have*

$$K \subset M \text{ is algebraic} \iff K \subset L \text{ and } L \subset M \text{ are algebraic.}$$

**Proof.** If $K \subset M$ is algebraic, it follows directly from the definition that $K \subset L$ and $L \subset M$ are also algebraic.

Now, assume that $K \subset L$ and $L \subset M$ are algebraic extensions, and let $c \in M$ be arbitrary. Then $c$ has a minimum polynomial $f_L^c = \sum_{i=0}^n b_i X^i \in L[X]$ over $L$. Each of the elements $b_i \in L$ is algebraic over $K$, so $L_0 = K(b_0, b_1, \ldots, b_n)$ is a finite extension of $K$. Because $c$ is also algebraic over $L_0$, the extension $L_0 \subset L_0(c)$ is finite. By 21.3, the extension $K \subset L_0(c)$ is also finite, and by 21.6 it is then algebraic. In particular, it follows that $c$ is algebraic over $K$, and we conclude that $K \subset M$ is algebraic. □

**Exercise 10.** Let $\overline{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. Prove: every element $\alpha \in \mathbf{C} \setminus \overline{\mathbf{Q}}$ is transcendental over $\overline{\mathbf{Q}}$.

Given a field $K$, we are now going to make a "largest possible" algebraic extension $\overline{K}$ of $K$. By 21.9, the field $\overline{K}$ itself can then no longer have any algebraic extensions $\overline{K} \subsetneq M$, and by 21.7, every non-constant polynomial $f \in \overline{K}[X]$ has a zero in $\overline{K}$. Such fields, which we already encountered in §15, are called *algebraically closed*.

**21.10. Definition.** *A field $K$ is called algebraically closed if it has the following equivalent properties:*

1. *For every algebraic extension $K \subset L$, we have $L = K$.*
2. *Every non-constant polynomial $f \in K[X]$ has a zero in $K$.*
3. *Every monic polynomial $f \in K[X]$ can be written as $f = \prod_{i=1}^n (X - \alpha_i)$ for some $\alpha_i \in K$.*

The best-known example of an algebraically closed field is the field $\mathbf{C}$. Proofs of the fact that polynomials of degree $n$ in $\mathbf{C}[X]$ have exactly $n$ complex zeros when counted with multiplicity were already given some 200 years ago by Gauss. At the time, it was not easy to make such a proof precise because all proofs use "topologic properties" of real or complex numbers that were only formulated precisely later in the 19th century. The name of the following theorem, which we already mentioned in §13, is traditional.

**21.11. Fundamental theorem of algebra.** *The field* $\mathbf{C}$ *of complex numbers is algebraically closed.*

Modern proofs often use (complex) analysis. In 26.3, we give a proof using Galois theory that uses only the intermediate value theorem from real analysis.

An algebraic extension $K \subset L$ with the property that $L$ is algebraically closed is called an *algebraic closure* of $K$. Once we know that there is an algebraically closed field that contains $K$, such an algebraic closure is easy to make.

**21.12. Theorem.** *Let* $K$ *be a field and* $\Omega$ *an algebraically closed field that contains* $K$*. Then the algebraic closure*

$$\overline{K} = \{\alpha \in \Omega : \alpha \text{ is algebraic over } K\}$$

*of* $K$ *in* $\Omega$ *is algebraically closed. In particular,*

$$\overline{\mathbf{Q}} = \{\alpha \in \mathbf{C} : \alpha \text{ is algebraic over } \mathbf{Q}\}$$

*is an algebraic closure of* $\mathbf{Q}$*.*

**Proof.** If $f \in \overline{K}[X] \subset \Omega[X]$ is a non-constant polynomial, then by 21.10, it has a zero $\alpha \in \Omega$. The subfield $\overline{K}(\alpha) \subset \Omega$ is algebraic over $\overline{K}$, and $\overline{K}$ is, by definition, algebraic over $K$. By 21.9, the field $\overline{K}(\alpha)$ is again algebraic over $K$ and therefore contained in $\overline{K}$. It follows that $f$ has a zero $\alpha \in \overline{K}$, so $\overline{K}$ is algebraically closed.

For $K = \mathbf{Q}$, by 21.11, we can take the field $\Omega$ equal to $\mathbf{C}$. □

Because $\mathbf{C}$ contains transcendental numbers, the field $\overline{\mathbf{Q}}$ in 21.12 is not equal to $\mathbf{C}$.

For arbitrary $K$, we can use 21.12 to define an algebraic closure of $K$ if there exists an algebraically closed field $\Omega$ that contains $K$. Such an $\Omega$ always exists. However, since $K$ can be very large, general constructions of $\Omega$ rely on the axiom of choice. The German Ernst Steinitz (1871–1928) was the first to give such a construction, in 1910. The proof given below using Corollary 15.12 of Zorn's lemma is by the Austrian Emil Artin (1898–1962).

**21.13. Theorem.** *For every field* $K$*, there exists an algebraically closed extension field* $\Omega \supset K$*.*

***Bewijs.** Let $\mathcal{F}$ be the collection of non-constant polynomials in $K[X]$ and $R = K[\{X_f : f \in \mathcal{F}\}]$ the polynomial ring over $K$ in the (infinitely many) variables $X_f$. In this large ring $R$, we let $I$ be the ideal generated by all polynomials $f(X_f)$ with $f \in \mathcal{F}$. We claim that $I$ is not equal to the entire ring $R$.

After all, every element $x \in I$ can be written as a *finite* sum $x = \sum_f r_f \cdot f(X_f)$ with $r_f \in R$. Only finitely many variables $X_f$ occur in this sum, say those with $f$ in the finite set $\mathcal{F}_x \subset \mathcal{F}$. By repeatedly applying 21.7, we can construct an extension field $K'$ of $K$ in which every polynomial $f \in \mathcal{F}_x$ has a zero $\alpha_f \in K'$. Now, let $\phi : R \to K'$ be the evaluation map defined by $X_f \mapsto \alpha_f$ for $f \in \mathcal{F}_x$ and $X_f \mapsto 0$ for $f \notin \mathcal{F}_x$. Then $\phi$ is a ring homomorphism, and since $\phi(f(X_f)) = f(\alpha_f) = 0$ for $f \in \mathcal{F}_x$, we have $\phi(x) = 0$. It follows that $x$ cannot be the constant polynomial $1 \in R$, so $1 \notin I$.

Now, let $M$ be a maximal ideal of $R$ that contains $I$, as in 15.12, and define $L_1 = R/M$. Then $L_1$ is a field extension of $K$ in which every non-constant polynomial $f \in K[X]$ has a zero $X_f \bmod M$. It does not immediately follow that $L_1$ is algebraically closed, but we can repeat the construction above and thus, inductively, construct a chain $K \subset L_1 \subset L_2 \subset L_3 \subset \dots$ of fields with the property that every non-constant polynomial with coefficients in $L_k$ has a zero in $L_{k+1}$. The union $\Omega = \bigcup_{k\geq 1} L_k$ is then again a field, and, by 21.10.2, this field *is* algebraically closed. After all, any polynomial in $\Omega[X]$ has only finitely many coefficients and is therefore contained in $L_k[X]$ for $k$ sufficiently large. □

***Exercise 11.** Show that the field $L_1$ is in fact already an algebraic closure of $K$.

## ▶ Splitting Fields

It follows from 21.12 and 21.13 that every field $K$ has an algebraic closure $\overline{K}$. The proof of 21.13 gives little information about $\Omega$, and in most cases, the resulting field $\overline{K}$ cannot be "written down explicitly." We therefore usually work with subfields of $\overline{K}$ that are of finite degree over $K$. To every polynomial $f \in K[X] \setminus K$ corresponds such a finite extension, the *splitting field* of $f$ over $K$.

**21.14. Definition.** *Let $K$ be a field and $f \in K[X]$ a non-constant polynomial. An extension $L$ of $K$ is called a splitting field of $f$ over $K$ if the following hold:*

1. *The polynomial $f$ is a product of linear factors in $L[X]$.*
2. *The zeros of $f$ in $L$ generate $L$ as a field extension of $K$.*

A splitting field of $f \in K[X]$ can be made by decomposing $f$ in $\overline{K}[X]$ as a product $f = c\prod_{i=1}^{n}(X - \alpha_i)$ and then taking the field

$$\Omega_K^f = K(\alpha_1, \alpha_2, \dots, \alpha_n) \subset \overline{K}.$$

This field, which is of finite degree over $K$, clearly satisfies the conditions of 21.14. However, the degree of $\Omega_K^f$ over $K$ is not immediately clear.

It is not strictly necessary to first make the algebraic closure $\overline{K}$; it is also possible to use 21.7 to formally adjoin the zeros of $f$ one by one. Given splitting fields $\Omega_K^f$ for all non-constant polynomials $f \in K[X]$, it is, conversely, possible to use these to construct an algebraic closure $\overline{K}$ as in Exercise 45.

**21.15. Examples. 1.** The polynomial $f = X^3 - 2$ is irreducible in $\mathbf{Q}[X]$. It has a real zero $\sqrt[3]{2}$ and a pair of complex conjugate zeros $\zeta_3\sqrt[3]{2}$ and $\zeta_3^2\sqrt[3]{2}$. Here, $\zeta_3 = e^{2\pi i/3} \in \mathbf{C}$ is a primitive third root of unity. The subfield of $\mathbf{C}$ generated over $\mathbf{Q}$ by the zeros of $f$ is

$$\Omega_{\mathbf{Q}}^{X^3-2} = \mathbf{Q}(\sqrt[3]{2}, \zeta_3) \subset \mathbf{C}.$$

Since the minimum polynomial $\Phi_3 = X^2 + X + 1$ of $\zeta_3$ has no zeros in $\mathbf{Q}(\sqrt[3]{2})$ (or in any other subfield of $\mathbf{R}$), the extension $\mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ has degree 2. We conclude that $\Omega_{\mathbf{Q}}^{X^3-2}$ is of degree 6 over $\mathbf{Q}$.

If, above, we replace the base field $\mathbf{Q}$ with $\mathbf{R}$, then $f = X^3 - 2$ is reducible in $\mathbf{R}[X]$, and the splitting field $\Omega_{\mathbf{R}}^{X^3-2} = \mathbf{R}(\zeta_3) = \mathbf{C}$ of $f$ is of degree 2 over $\mathbf{R}$.

**2.** The field $\Omega_{\mathbf{Q}}^{X^3-2}$ can also be constructed without using complex numbers. As in 21.7, first construct the cubic field $\mathbf{Q}[X]/(X^3-2)$. In this field, $\alpha = (X \bmod X^3-2)$ is a zero of $f = X^3-2$. Over $\mathbf{Q}(\alpha)$, the polynomial $f$ decomposes as

$$X^3 - 2 = (X-\alpha)(X^2+\alpha X+\alpha^2) \in \mathbf{Q}(\alpha)[X].$$

To see that the polynomial $g = X^2+\alpha X+\alpha^2$ has no zeros in $\mathbf{Q}(\alpha)$ and is therefore irreducible in $\mathbf{Q}(\alpha)[X]$, we observe that $\alpha^{-2}g(\alpha X) = X^2+X+1$ holds. If $g$ has a zero in $\mathbf{Q}(\alpha)$, then $X^2+X+1$ also has a zero $\beta \in \mathbf{Q}(\alpha)$. This would mean that the quadratic field $\mathbf{Q}(\beta) = \mathbf{Q}[X]/(X^2+X+1)$ is a subfield of the cubic field $\mathbf{Q}(\alpha)$, in contradiction with 21.3. We conclude that $X^2+X+1$ is irreducible over $\mathbf{Q}(\alpha)$, and the formal adjunction of a zero $\beta$ of $X^2+X+1$ to $\mathbf{Q}(\alpha)$ gives a field $\mathbf{Q}(\alpha,\beta)$ of degree 6 over $\mathbf{Q}$. In this field, $X^3-2$ has the zeros $\alpha$, $\alpha\beta$, and $\alpha\beta^2$, so we can take $\Omega_{\mathbf{Q}}^{X^3-2} = \mathbf{Q}(\alpha,\beta)$. Note that this construction does not give a subfield of $\mathbf{C}$.

**3.** The $p$th cyclotomic field $\mathbf{Q}(\zeta_p)$ from 21.8.3 is a splitting field of the polynomial $X^p-1$ over $\mathbf{Q}$. After all, the $p$ zeros of $X^p-1$ in $\mathbf{Q}(\zeta_p)$ are exactly the powers of $\zeta_p$.

The example of $\Omega_{\mathbf{Q}}^{X^3-2}$ shows us that although there may be various ways to make a splitting field, the result is, in a way, independent of the construction. After all, for the fields constructed in 21.15, we have an isomorphism

$$\psi : \mathbf{Q}(\alpha,\beta) \xrightarrow{\sim} \mathbf{Q}(\sqrt[3]{2},\zeta_3)$$

of fields by taking for $\psi(\alpha)$ a complex zero of $X^3-2$ and for $\psi(\beta)$ a zero of $X^2+X+1$ in $\mathbf{C}$. As there are three choices for $\psi(\alpha)$ and two for $\psi(\beta)$, this gives six possibilities for the isomorphism $\psi$, and there is no "natural choice." For every pair of choices $\psi_1$ and $\psi_2$, the composition $\psi_2^{-1} \circ \psi_1$ is an element of the group $\mathrm{Aut}(\mathbf{Q}(\alpha,\beta))$ of field automorphisms.

**Exercise 12.** Show that $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2},\zeta_3))$ is a group of order 6. Is it $S_3$ or $C_6$?

## ▶ Uniqueness Theorems

Two extensions $L_1$ and $L_2$ of $K$ are said to be *isomorphic over* $K$ or $K$*-isomorphic* if there exists a field isomorphism $L_1 \to L_2$ that is the identity on $K$. The fields $L_1$ and $L_2$ are also said to be *conjugate* over $K$. Similarly, elements $\alpha$ and $\beta$ in an algebraic extension of $K$ are said to be *conjugate* over $K$ if there exists a field isomorphism $K(\alpha) \to K(\beta)$ that is the identity on $K$ and sends $\alpha$ to $\beta$.

**Exercise 13.** Prove: elements $\alpha$ and $\beta$ in an algebraic closure $\overline{K}$ of $K$ are conjugate over $K$ if and only if $f_K^\alpha$ and $f_K^\beta$ are equal.

We just saw that for $f = X^3-2$ and $K = \mathbf{Q}$, two splitting fields $\Omega_K^f$ are isomorphic over $K$. This holds for arbitrary $K$ and $f \in K[X]$ and, likewise, an algebraic closure $\overline{K}$ of $K$ is fixed up to $K$-isomorphism.

**21.16. Theorem.** *For a field $K$ and a non-constant polynomial $f \in K[X]$, the following hold:*

1. *Any two splitting fields of $f$ over $K$ are $K$-isomorphic.*
2. *Any two algebraic closures of $K$ are $K$-isomorphic.*

Note that 21.16 only says that, in both cases, there exists *a* $K$-isomorphism. In general, this isomorphism is not unique. The fact that any two isomorphisms "differ" by an automorphism of the splitting field or of the algebraic closure is a fundamental observation that will form the basis for Galois theory in §24. Consequently, we will come across the core of the proof of 21.16, contained in the following lemma, several more times.

**21.17. Lemma.** *Let $\varphi : K_1 \to K_2$ be a field isomorphism, $f_1 \in K_1[X]$ a non-constant polynomial, and $f_2 \in K_2[X]$ the polynomial obtained by applying $\varphi$ to the coefficients of $f_1$. For $i \in \{1, 2\}$, let $L_i$ be a splitting field of $f_i$ over $K_i$.*

*Then there exists an isomorphism $\psi : L_1 \to L_2$ with $\psi\big|_{K_1} = \varphi$.*

**Proof.** The proof is by induction on the degree $d = [L_1 : K_1]$.

For $d = 1$, the polynomial $f_1$ decomposes into linear factors in the polynomial ring $K_1[X]$, say $f_1 = c_1(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$. Since $f_2$ is the image of $f_1$ by the ring isomorphism $\widetilde{\varphi} : K_1[X] \xrightarrow{\sim} K_2[X]$ given by $\sum_i a_i X^i \mapsto \sum_i \varphi(a_i)X^i$, it follows that $f_2$ in turn decomposes in $K_2[X]$, as $f_2 = \widetilde{\varphi}(f_1) = \varphi(c_1)(X - \varphi(\alpha_1))(X - \varphi(\alpha_2))\cdots(X - \varphi(\alpha_n))$. We therefore have $L_2 = K_2$, and we can simply take $\psi = \varphi$.

Now, take $d > 1$, and let $\alpha \in L_1 \setminus K_1$ be a zero of $f_1$. Then the minimum polynomial $h_1 = f^{\alpha}_{K_1} \in K_1[X]$ is an irreducible divisor of $f_1$. By applying the isomorphism $\widetilde{\varphi}$, we see that $h_2 = \widetilde{\varphi}(h_1)$ is an irreducible divisor of $f_2 = \widetilde{\varphi}(f_1)$. Since $f_2$ decomposes completely in $L_2$, this also holds for $h_2$. Let $\beta \in L_2$ be a zero of $h_2$. Then we have $h_2 = f^{\beta}_{K_2}$, so we have a composed isomorphism

$$\chi : K_1(\alpha) \xrightarrow{\sim} K_1[X]/(h_1) \xrightarrow{\sim} K_2[X]/(h_2) \xrightarrow{\sim} K_2(\beta).$$

$$\begin{array}{ccc} L_1 & \xrightarrow{\psi} & L_2 \\ | & & | \\ K_1(\alpha) & \xrightarrow{\chi} & K_2(\beta) \\ | & & | \\ K_1 & \xrightarrow{\phi} & K_2 \end{array}$$

The outside arrows are the known isomorphisms from 21.5.2; the middle arrow is the natural isomorphism induced by $\widetilde{\varphi}$. We have $\chi\big|_{K_1} = \widetilde{\varphi}\big|_{K_1} = \varphi$.

We now note that $L_1$ is a splitting field of $f_1$ over $K_1(\alpha)$ and, likewise, $L_2$ is a splitting field of $f_2$ over $K_2(\beta)$. Because we have chosen $\alpha$ outside of $K_1$, the degree $[L_1 : K_1(\alpha)]$ is strictly less than $[L_1 : K_1] = d$. The induction hypothesis now tells us that $\chi : K_1(\alpha) \xrightarrow{\sim} K_2(\beta)$ can be extended to an isomorphism $\psi : L_1 \to L_2$, and this proves the lemma. □

**Proof of 21.16.** By applying 21.17 with $K_1 = K_2 = K$ and $\varphi = \mathrm{id}_K$, we obtain the statement in 21.16.1.

Now, let $\overline{K}_1$ and $\overline{K}_2$ be algebraic closures of $K$. To prove that $\overline{K}_1$ and $\overline{K}_2$ are isomorphic over $K$, we apply Zorn's lemma to the collection $\mathcal{C}$ of triples $(M_1, \mu, M_2)$. Here, $M_1$ and $M_2$ are subfields of, respectively, $\overline{K}_1$ and $\overline{K}_2$ that contain $K$, and $\mu : M_1 \xrightarrow{\sim} M_2$ is a $K$-isomorphism. We define a partial ordering on $\mathcal{C}$ by setting

$$(M_1, \mu, M_2) \le (\widetilde{M}_1, \widetilde{\mu}, \widetilde{M}_2) \quad \Longleftrightarrow \quad M_1 \subset \widetilde{M}_1,\ M_2 \subset \widetilde{M}_2, \text{ and } \widetilde{\mu}\big|_{M_1} = \mu.$$

The element $(K, \mathrm{id}, K) \in \mathcal{C}$ is an upper bound for the empty chain in $\mathcal{C}$. For non-empty chains, we make an upper bound by taking unions. By 15.11, the collection $\mathcal{C}$ has a maximal element. We prove that such an element is of the form $(\overline{K}_1, \mu, \overline{K}_2)$ and therefore provides the desired $K$-isomorphism.

Let $(E_1, \phi, E_2) \in \mathcal{C}$ be a maximal element, and suppose that there exists an element $\alpha$ in $\overline{K}_1 \setminus E_1$ or in $\overline{K}_2 \setminus E_2$. Then $\alpha$ is algebraic over $K$, so there exists a monic polynomial $f \in K[X]$ with $f(\alpha) = 0$. Now, for $i \in \{1, 2\}$, let $L_i \subset \overline{K}_i$ be the extension of $E_i$ generated by the zeros of $f$. Then $L_i$ is a splitting field of $f$ over $E_i$, and we can apply 21.17 to $\phi : E_1 \to E_2$ and $f_1 = f_2 = f$. This gives a triple $(L_1, \mu, L_2) \in \mathcal{C}$ that is strictly greater than $(E_1, \phi, E_2)$, contradicting the maximality of $(E_1, \phi, E_2)$. □

**Exercise 14.** Let $\overline{K}_1$ and $\overline{K}_2$ be algebraic closures of $K_1$ and $K_2$, respectively. Prove: every isomorphism $K_1 \xrightarrow{\sim} K_2$ admits an extension to an isomorphism $\overline{K}_1 \xrightarrow{\sim} \overline{K}_2$.

As already noted, the $K$-isomorphisms in 21.16 are not, in general, unique. We therefore speak of *a* splitting field of $f$ over $K$ and of *an* algebraic closure of $K$.

EXERCISES.

15. Let $K$ be a field and $\psi : K \xrightarrow{\sim} K$ an automorphism. Prove that $\psi$ is the identity on the prime field of $K$.

16. Let $\mathbf{C}(X)$ be the field of rational functions with complex coefficients. Prove that a $\mathbf{C}$-basis of $\mathbf{C}(X)$ is given by

$$\{X^i\}_{i=0}^{\infty} \cup \left\{ \frac{1}{(X-\alpha)^k} : \alpha \in \mathbf{C}, k \in \mathbf{Z}_{>0} \right\}.$$

[This *partial fraction decomposition* is useful for integrating rational functions.]

*17. Formulate and make the analog of the previous exercise for the field $K(X)$ of rational functions with coefficients in an arbitrary field $K$.

18. Let $K \subset L$ be an algebraic extension. For $\alpha, \beta \in L$, prove that we have

$$[K(\alpha,\beta) : K] \leq [K(\alpha) : K] \cdot [K(\beta) : K].$$

Show that equality does not always hold. Does equality always hold if $[K(\alpha) : K]$ and $[K(\beta) : K]$ are relatively prime?

19. Let $K \subset K(\alpha)$ be an extension of odd degree. Prove: $K(\alpha^2) = K(\alpha)$.

20. Prove: an algebraically closed field is of infinite degree over its prime field.

21. Show that there are only countably many algebraic numbers. Conclude that $\mathbf{C}$ is not algebraic over $\mathbf{Q}$ and that there exist uncountably many transcendental numbers.

22. Let $B$ be a basis for $\mathbf{C}$ over $\mathbf{Q}$. Is $B$ countable?

23. Show that every quadratic extension of $\mathbf{Q}$ is of the form $\mathbf{Q}(\sqrt{d})$ with $d \in \mathbf{Z}$. For what $d$ do we obtain the cyclotomic field $\mathbf{Q}(\zeta_3)$?

24. Is every cubic extension of $\mathbf{Q}$ of the form $K = \mathbf{Q}(\sqrt[3]{d})$ for some $d \in \mathbf{Q}$?

25. Take $M = \mathbf{Q}(i, \sqrt{2})$ and $\alpha = 1 + i + \sqrt{2}$. Prove: $G = \mathrm{Aut}(M)$ is isomorphic to $V_4$, and $f = \prod_{\sigma \in G}(X - \sigma(\alpha))$ is the minimum polynomial of $\alpha$ over $\mathbf{Q}$.
[This method works very generally: Exercises 13 and 14.]

26. Define $\sqrt{2}, \sqrt{3} \in \mathbf{R}$ in the usual way, and set $M = \mathbf{Q}(\alpha) \subset \mathbf{R}$ with $\alpha = 1 + \sqrt{2} + \sqrt{3}$. Prove that $M$ is of degree 4 over $\mathbf{Q}$, determine $f_{\mathbf{Q}}^{\alpha}$, and write $\sqrt{2}$ and $\sqrt{3}$ in the basis $\{1, \alpha, \alpha^2, \alpha^3\}$.

27. Show that $f = X^4 - 4X^3 - 4X^2 + 16X - 8$ is irreducible in $\mathbf{Q}[X]$, and determine the degree of a splitting field of $f$ over $\mathbf{Q}$. [Hint: previous exercise...]

28. Prove: $\mathbf{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbf{Q}(\sqrt{2} \cdot \sqrt[3]{3}) = \mathbf{Q}(\sqrt{2} + \sqrt[3]{3})$. Determine the minimum polynomials of $\sqrt{2} \cdot \sqrt[3]{3}$ and $\sqrt{2} + \sqrt[3]{3}$ over $\mathbf{Q}$.

29. Take $K = \mathbf{Q}(\alpha)$ with $f_{\mathbf{Q}}^{\alpha} = X^3 + 2X^2 + 1$.
    a. Determine the inverse of $\alpha + 1$ in the basis $\{1, \alpha, \alpha^2\}$ of $K$ over $\mathbf{Q}$.
    b. Determine the minimum polynomial of $\alpha^2$ over $\mathbf{Q}$.

30. Define the cyclotomic field $\mathbf{Q}(\zeta_5)$ as in 21.8.3, and write $\alpha = \zeta_5^2 + \zeta_5^3$.
    a. Show that $\mathbf{Q}(\alpha)$ is a quadratic extension of $\mathbf{Q}$, and determine $f_{\mathbf{Q}}^{\alpha}$.

b. Prove: $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{5})$.

c. Prove: $\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$ and $\sin(2\pi/5) = \sqrt{\frac{5+\sqrt{5}}{8}}$.

31. Let $\overline{K}$ be an algebraic closure of $K$ and $L \subset \overline{K}$ a field that contains $K$. Prove that $\overline{K}$ is an algebraic closure of $L$.

32. Let $K \subset L$ be a field extension and $K_0$ the algebraic closure of $K$ in $L$. Prove that every element $\alpha \in L \setminus K_0$ is transcendental over $K_0$.

33. Give a construction of a splitting field $\Omega_K^f$ from 21.14 that uses only 21.7 and not the existence of an algebraic closure $\overline{K}$ of $K$.

34. Let $K$ be a field and $\mathcal{F}$ a family of polynomials in $K[X]$. Define a splitting field $\Omega_K^{\mathcal{F}}$ of the family $\mathcal{F}$ over $K$, and show that $\Omega_K^{\mathcal{F}}$ exists and is unique up to $K$-isomorphism.

35. Let $f \in K[X]$ be a polynomial of degree $n \geq 1$. Prove: $[\Omega_K^f : K]$ divides $n!$.

36. Let $d \in \mathbf{Z}$ be an integer that is not a third power in $\mathbf{Z}$. Prove that a splitting field $\Omega_{\mathbf{Q}}^{X^3-d}$ has degree 6 over $\mathbf{Q}$. What is the degree if $d$ *is* a third power?

37. Determine the degree of a splitting field of $X^4 - 2$ over $\mathbf{Q}$.

38. Answer the same question for $X^4 - 4$ and $X^4 + 4$. Explain why the notation $\mathbf{Q}(\sqrt[4]{4})$ and $\mathbf{Q}(\sqrt[4]{-4})$ is not used for the fields obtained through the adjunction of a zero of, respectively, $X^4 - 4$ and $X^4 + 4$ to $\mathbf{Q}$.

39. Let $K \subset L = K(\alpha)$ be a simple field extension of degree $n$, and define $c_i \in L$ by

$$\sum_{i=0}^{n-1} c_i X^i = \frac{f_K^\alpha}{X - \alpha} \in L[X].$$

Prove: $\{c_0, c_1, \ldots, c_{n-1}\}$ is a $K$-basis for $L$.

40. Let $K \subset E \subset L = K(\alpha)$ be a tower of field extensions, with $\alpha$ algebraic over $K$.

a. Prove that as an extension of $K$, the field $E$ is generated by the coefficients of the polynomial $f_E^\alpha \in E[X]$.

b. Prove that as a $K$-vector space, $E$ is generated by the coefficients of the polynomial $f_K^\alpha / f_E^\alpha \in E[X]$.
[Hint: use $f_K^\alpha/(X-\alpha) = (f_K^\alpha/f_E^\alpha) \cdot (f_E^\alpha/(X-\alpha))$ and the previous exercise.]

41. What is the cardinality[5] of a transcendence basis for $\mathbf{C}$ over $\mathbf{Q}$?

42. Let $\overline{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. Is $\mathbf{C}$ purely transcendental over $\overline{\mathbf{Q}}$?

*43. Show that $\mathbf{C}$ has uncountably many automorphisms and that the cardinality of $\mathrm{Aut}(\mathbf{C})$ is even greater than that of $\mathbf{C}$.

44. Show that $\mathbf{C}$ has exactly two *continuous* automorphisms.
[Hint: prove that such an automorphism is the identity on $\mathbf{R}$.]

45. Let $K$ be a field, and suppose given for every $f \in \mathcal{F} = K[X]\backslash K$ a splitting field $\Omega_K^f$ of $f$ over $K$.

a. Let $R$ be the ring $\prod_{f\in\mathcal{F}} \Omega_K^f$, with componentwise ring operations, and for $g \in \mathcal{F}$, write

$$I_g = \{(x_f)_{f\in\mathcal{F}} \in R : x_f = 0 \text{ if } g \mid f\}.$$

Prove: $I = \bigcup_{g\in\mathcal{F}} I_g$ is an ideal of $R$ different from $R$.

b. Prove that $R$ has a maximal ideal $M$ with $I \subset M$, that $R/M$ can be viewed as an extension field of $K$, and that the algebraic closure of $K$ in $R/M$ (as defined for 21.9) is an algebraic closure of $K$.

46. Prove that for any two fields of equal characteristic, one of the two is isomorphic to a subfield of an algebraic closure of the other.

47. Let $K \subset L$ and $K \subset M$ be two field extensions. Prove that there is a field extension $K \subset N$ such that $L$ and $M$ are both $K$-isomorphic to a subfield of $N$.

48. Let $K \subset L$ be a field extension of degree $n$ and $V, W \subset L$ two sub-$K$-vector spaces with $\dim_K V + \dim_K W > n$.

    a. Prove: every $x \in L$ can be written as $x = v/w$ with $v \in V$ and $w \in W$.
    b. Suppose $L = K(\alpha)$, and let $a, b \in \mathbf{Z}_{\geq 0}$ satisfy $a + b = n - 1$. Prove: for every element $x \in L$, there exist polynomials $A, B \in K[X]$ of degree $\deg(A) \leq a$ and $\deg(B) \leq b$ for which $x = A(\alpha)/B(\alpha)$ holds.

49. Let $K \subset L$ and $V, W \subset L$ be as in the previous exercise. Prove: every $x \in L$ can be written as a finite sum of elements of the form $vw$ with $v \in V$ and $w \in W$.
    [Hint: show that every $K$-linear map $L \to K$ that vanishes on all elements $vw$ is the zero map.]

## 22 Finite fields

In this section, we apply the theory of field extensions in the case of *finite* fields. Since the prime field of a finite field cannot be the infinite field $\mathbf{Q}$, for every finite field $\mathbf{F}$, the prime field is a field $\mathbf{F}_p$ with $p$ elements, with $p = \mathrm{char}(\mathbf{F}) > 0$ the characteristic of $\mathbf{F}$. Finite fields are therefore nothing but finite extensions of the prime fields $\mathbf{F}_p$.

Since for a prime $p$, all binomial coefficients $\binom{p}{i}$ with $0 < i < p$ are divisible by $p$, the binomial theorem in fields (or commutative rings) of characteristic $p$ leads to the much-used identity $(x + y)^p = x^p + y^p$: taking the $p$th power is *additive* in characteristic $p$.

### ▶ The field $\mathbf{F}_{p^n}$

Unlike in the case of the prime field $\mathbf{Q}$, the finite extensions of $\mathbf{F}_p$ can be easily classified: for every $n \in \mathbf{Z}_{\geq 1}$, up to isomorphism, there is exactly one extension $\mathbf{F}_p \subset \mathbf{F}_{p^n}$ of degree $n$.

**22.1. Theorem.** *Let $\mathbf{F}$ be a finite field and $\mathbf{F}_p$ the prime field of $\mathbf{F}$. Then $\mathbf{F}$ is an extension of $\mathbf{F}_p$ of finite degree $n$, and $\mathbf{F}$ has $p^n$ elements.*

*Conversely, for every prime power $q = p^n > 1$, there exists, up to isomorphism, a unique field $\mathbf{F}_q$ with $q$ elements; it is a splitting field of $X^q - X$ over $\mathbf{F}_p$.*

*Proof.* If $\mathbf{F}$ is finite, then $\mathbf{F}$ is of finite degree over its prime field $\mathbf{F}_p$. If this degree is equal to $n$, then $\mathbf{F}$, as an $n$-dimensional vector space over $\mathbf{F}_p$, has exactly $p^n$ elements. The group of units $\mathbf{F}^*$ then has order $p^n - 1$, and it follows that the elements of $\mathbf{F}^*$ are exactly the $p^n - 1$ zeros of the polynomial $X^{p^n-1} - 1 \in \mathbf{F}[X]$. In particular, we have

$$\textstyle\prod_{\alpha \in \mathbf{F}} (X - \alpha) = X^{p^n} - X \in \mathbf{F}_p[X].$$

It follows that $\mathbf{F}$ is a splitting field of $X^{p^n} - X$ over $\mathbf{F}_p$, and from 21.16, it follows that, up to isomorphism, there can exist at most one field with $p^n$ elements.

We now prove that, conversely, for every prime power $q = p^n > 1$, a splitting field of $X^q - X \in \mathbf{F}_p[X]$ over $\mathbf{F}_p$ is a field with $q$ elements. Because the derivative $f' = -1$ of $f = X^q - X$ has no zeros, $f$ has no double zeros in an algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$. The zero set

$$\mathbf{F}_q = \{\alpha \in \overline{\mathbf{F}}_p : \alpha^{p^n} = \alpha\} \subset \overline{\mathbf{F}}_p \tag{22.2}$$

of $f$ therefore has $q = p^n$ elements. By Fermat's little theorem, we have $\mathbf{F}_p \subset \mathbf{F}_q$. It is clear that $\mathbf{F}_q$ is closed under multiplication and division by non-zero elements. The additivity of taking the $p$th power implies

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

so $\mathbf{F}_q$ is also an additive subgroup of $\overline{\mathbf{F}}_p$. It follows that $\mathbf{F}_q$ is a subfield of $\overline{\mathbf{F}}_p$ and therefore a splitting field of $f$ over $\mathbf{F}_p$. □

Perhaps needless to say, let us mention that for $n > 1$, the field $\mathbf{F}_q = \mathbf{F}_{p^n}$ in (22.2) is *not* equal to the ring $\mathbf{Z}/q\mathbf{Z}$.

▶ Frobenius automorphism

The proof of Theorem 22.1 is based on the fact that the *Frobenius map*

$$\begin{aligned} F: \quad \overline{\mathbf{F}}_p &\longrightarrow \overline{\mathbf{F}}_p \\ x &\longmapsto x^p \end{aligned}$$

is an *automorphism* of the algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$. The fundamental property $F(x+y) = F(x) + F(y)$ is a peculiarity in fields of characteristic $p$ that has no equivalent for fields of characteristic 0. The injectivity of $F$ means that elements in $\overline{\mathbf{F}}_p$ have a *unique* $p$th root. It indeed follows from $\beta^p = \alpha \in \overline{\mathbf{F}}_p$ that we have

$$(X-\beta)^p = X^p - \beta^p = X^p - \alpha,$$

and this shows that $\beta$ is the only $p$th root of $\alpha$. We further discuss this *inseparability property* in 23.6.

By repeatedly applying the Frobenius automorphism to $\overline{\mathbf{F}}_p$, we obtain the automorphism $F^n : x \mapsto x^{p^n}$. The proof of 22.1 shows that for every $n \geq 1$, the field $\overline{\mathbf{F}}_p$ contains exactly one subfield with $p^n$ elements and that, in terms of $F$, it can be characterized as

$$\mathbf{F}_{p^n} = \{\alpha \in \overline{\mathbf{F}}_p : F^n(\alpha) = \alpha\}. \tag{22.3}$$

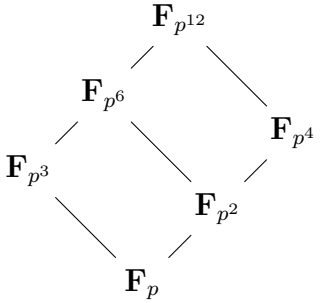
The complete structure of the set of subfields of $\overline{\mathbf{F}}_p$ and the inclusion relations between the subfields can be deduced from this characterization.

**22.4. Theorem.** *Let $\mathbf{F}_q$ and $\mathbf{F}_r$ be subfields of $\overline{\mathbf{F}}_p$ with, respectively, $q = p^i$ and $r = p^j$ elements. The following are equivalent:*

1. *$\mathbf{F}_q$ is a subfield of $\mathbf{F}_r$.*
2. *$r$ is a power of $q$.*
3. *$i$ is a divisor of $j$.*

*Proof.* If $\mathbf{F}_r$ is an extension field of $\mathbf{F}_q$ of degree $d$, then we have $r = q^d$ and therefore $j = di$. This proves $1 \Rightarrow 2 \Rightarrow 3$. Finally, if $i$ is a divisor of $j$, then for $\alpha \in \overline{\mathbf{F}}_p$, we have the implication $F^i(\alpha) = \alpha \Rightarrow F^j(\alpha) = \alpha$. This is, however, equivalent to the inclusion relation $\mathbf{F}_q = \mathbf{F}_{p^i} \subset \mathbf{F}_{p^j} = \mathbf{F}_r$. □

It follows from 22.4 that the inclusion relation of finite subfields of $\overline{\mathbf{F}}_p$ corresponds to the divisibility relation of their degrees over $\mathbf{F}_p$. For $n = 12$, we obtain the following *lattice* of subfields of $\mathbf{F}_{p^{12}}$.



Such a lattice is also called a *Hasse diagram*, after the German Helmut Hasse (1898–1979). A line connecting two fields in such a lattice must be viewed as an inclusion in the upward direction of the line. In our figure, the short connecting lines represent quadratic extensions and the long ones cubic extensions.

### ▶ Irreducible polynomials over $\mathbf{F}_p$

The description of $\mathbf{F}_q$ we have given so far is characteristic for *Galois theory*: it is the subfield of $\overline{\mathbf{F}}_p$ consisting of the elements that are invariant for certain powers of the Frobenius automorphism. To do arithmetic in finite fields, we need a description of $\mathbf{F}_q$ as an extension of $\mathbf{F}_p$ obtained through the formal adjunction of a zero of an explicit polynomial $f \in \mathbf{F}_p[X]$.

**22.5. Theorem.** *The group of units $\mathbf{F}_q^*$ of $\mathbf{F}_q$ is a cyclic group of order $q-1$. For every generator $\alpha \in \mathbf{F}_q^*$, we have $\mathbf{F}_q = \mathbf{F}_p(\alpha) \cong \mathbf{F}_p[X]/(f^\alpha_{\mathbf{F}_p})$.*

*Proof.* The group of units $\mathbf{F}_q^*$ is cyclic by 12.5. If we have $\mathbf{F}_q^* = \langle\alpha\rangle$, then we have $\mathbf{F}_q \subset \mathbf{F}_p(\alpha)$ and therefore $\mathbf{F}_q = \mathbf{F}_p(\alpha)$. The isomorphism $\mathbf{F}_p(\alpha) \cong \mathbf{F}_p[X]/(f^\alpha_{\mathbf{F}_p})$ is a special case of 21.5.2. □

**22.6. Corollary.** *Let $p$ be a prime and $n \geq 1$ an integer. Then there exists an irreducible polynomial of degree $n$ in $\mathbf{F}_p[X]$.*

*Proof.* Write $\mathbf{F}_{p^n} = \mathbf{F}_p(\alpha)$ and take $f = f^\alpha_{\mathbf{F}_p}$. □

**Exercise 1.** Is every element $\alpha \in \mathbf{F}_q^*$ with $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ necessarily a generator of $\mathbf{F}_q^*$?

"Constructing" a field of order $q = p^n$ "explicitly" corresponds to finding an irreducible polynomial of degree $n$ in $\mathbf{F}_p[X]$. For small values of $n$ and $p$, such a polynomial can be found through trial and error. For $n = p = 2$, the only possibility is $X^2 + X + 1$, which gives

$$\mathbf{F}_4 \cong \mathbf{F}_2[X]/(X^2 + X + 1).$$

Through this, we obtain $\mathbf{F}_4$ as an explicit $\mathbf{F}_2$-vector space $\mathbf{F}_4 = \mathbf{F}_2 \cdot 1 \oplus \mathbf{F}_2 \cdot \alpha$ with multiplication based on the rule $\alpha^2 = \alpha + 1$. The group $\mathbf{F}_4^*$ has order 3 and is generated by $\alpha$ or by $\alpha^{-1} = \alpha + 1$.

**Exercise 2.** Give a complete multiplication table for $\mathbf{F}_4$.

In most cases, there is much choice for an irreducible polynomial of degree $n$ in $\mathbf{F}_p[X]$. For example, because 2 and 3 are not squares in $\mathbf{F}_5$, we have

$$\mathbf{F}_{25} \cong \mathbf{F}_5(\sqrt{2}) = \mathbf{F}_5[X]/(X^2 - 2) \qquad \text{and} \qquad \mathbf{F}_{25} \cong \mathbf{F}_5(\sqrt{3}) = \mathbf{F}_5[X]/(X^2 - 3).$$

In particular, there is an isomorphism $\mathbf{F}_5(\sqrt{2}) \xrightarrow{\sim} \mathbf{F}_5(\sqrt{3})$. Because of the equality $(2\sqrt{3})^2 = 2 \in \mathbf{F}_5$, an explicit choice for this isomorphism is the map $a+b\sqrt{2} \mapsto a+2b\sqrt{3}$.

**Exercise 3.** Show that there is *no* field isomorphism $\mathbf{Q}(\sqrt{2}) \to \mathbf{Q}(\sqrt{3})$.

Because, by (22.2), the elements of $\mathbf{F}_{p^n}$ are zeros of $X^{p^n} - X$, we can, in principle, find the irreducible polynomials of degree $n$ by decomposing this polynomial into irreducible factors.

**22.7. Theorem.** *For $p$ a prime and $n \geq 1$, the following relation holds in $\mathbf{F}_p[X]$:*

$$X^{p^n} - X = \prod_{\substack{f \text{ monic, irreducible} \\ \deg(f) | n}} f.$$

*In particular, the number $x_d$ of monic, irreducible polynomials of degree $d$ in $\mathbf{F}_p[X]$ satisfies the identity $\sum_{d|n} d \cdot x_d = p^n$.*

*Proof.* Let $f \in \mathbf{F}_p[X]$ be a monic, irreducible polynomial of degree $d$. A zero $\alpha$ of $f$ in $\overline{\mathbf{F}}_p$ then generates an extension $\mathbf{F}_p(\alpha)$ of degree $d$. By (22.4), we have $\mathbf{F}_p(\alpha) \subset \mathbf{F}_{p^n}$ if and only if $d$ is a divisor of $n$. By (22.2), we have $\mathbf{F}_p(\alpha) \subset \mathbf{F}_{p^n}$ if and only if $\alpha$ is a zero of $X^{p^n} - X$, and the latter just means that the minimum polynomial $f$ of $\alpha$ is a divisor of $X^{p^n} - X$. We conclude that $f$ is a divisor of $X^{p^n} - X$ if and only if $\deg(f)$ is a divisor of $n$. Because $X^{p^n} - X$ has no multiple zeros, this leads to the desired decomposition in $\mathbf{F}_p[X]$. Comparing degrees gives $\sum_{d|n} d \cdot x_d = p^n$. □

By applying 22.7 successively for $n = 1, 2, 3, \ldots$, we can calculate the values of $x_n$ inductively. For $n = 1$, we find, predictably, that there are $x_1 = p$ monic, linear polynomials in $\mathbf{F}_p[X]$. If $n$ is a prime, then the relation $x_1 + nx_n = p^n$ leads to $x_n = (p^n - p)/n$. By Fermat's little theorem—modulo the prime $n$, not $p$—this is indeed an integer. For $n = 2$ or $n = 3$, this formula can be verified directly (Exercise 24).

A general formula for $x_n$ in terms of $p$ can be obtained from 22.7 using *Möbius inversion*. This is a general method that allows us, for any two functions $f, g : \mathbf{Z}_{>0} \to \mathbf{C}$ related through the formula $\sum_{d|n} f(d) = g(n)$, to express the values of $f$ in those of $g$. To do so, we define the *Möbius function* $\mu : \mathbf{Z}_{>0} \to \mathbf{Z}$, named after the German August Ferdinand Möbius (1790–1868),

$$\mu(n) = \begin{cases} 0 & \text{if there is a prime } p \text{ with } p^2 \mid n, \\ (-1)^t & \text{if } n \text{ is the product of } t \text{ different primes.} \end{cases}$$

We have $\mu(1) = 1$; after all, 1 is the product of $t = 0$ primes. The Möbius function is uniquely determined by its value in 1 and the fundamental property

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if n=1,} \\ 0 & \text{if } n > 1. \end{cases} \tag{22.8}$$

We refer to Exercise 26 for the details.

**22.9. Möbius inversion formula.** *Let $f, g : \mathbf{Z}_{>0} \to \mathbf{C}$ satisfy the following equality for all $n \in \mathbf{Z}_{>0}$:*

$$\textstyle\sum_{d|n} f(d) = g(n).$$

*Then for all $n \in \mathbf{Z}_{>0}$, we have the inversion formula*

$$f(n) = \textstyle\sum_{d|n} \mu(d) g(n/d).$$

*Proof.* Express $g$ in the second formula in $f$ and use the fundamental property (22.8) of $\mu$:

$$\sum_{d|n}\mu(d)g(n/d)=\sum_{d|n}\sum_{k|\frac{n}{d}}\mu(d)f(k)=\sum_{k|n}\left(\sum_{d|\frac{n}{k}}\mu(d)\right)f(k)=f(n). \qquad \square$$

If we apply 22.9 with $f:n\mapsto nx_n$ and $g:n\mapsto p^n$, then using 22.7, we find the relation

$$x_n=\tfrac{1}{n}\textstyle\sum_{d|n}\mu(d)p^{n/d}.$$

It follows (Exercise 21) that for large $n$ or $p$, an arbitrary monic polynomial of degree $n$ in $\mathbf{F}_p[X]$ is irreducible with probability approximately $\frac{1}{n}$.

### ▶ Automorphisms of $\mathbf{F}_q$

We already observed that the Frobenius automorphism $F:x\mapsto x^p$ plays a central role in the theory of the finite fields. There are, essentially, no other automorphisms of finite fields.

**22.10. Theorem.** *Let $\mathbf{F}_q$ be the extension of degree $n$ of $\mathbf{F}_p$. Then $\mathrm{Aut}(\mathbf{F}_q)$ is a cyclic group of order $n$ generated by the Frobenius automorphism $F:x\mapsto x^p$.*

*Proof.* We already know that $F$ is an automorphism of $\mathbf{F}_q$, and we are going to prove that $F$ has order $n$ in $\mathrm{Aut}(\mathbf{F}_q)$. By (22.3), the power $F^n$ is the identity on $\mathbf{F}_q=\mathbf{F}_{p^n}$, so the order of $F$ divides $n$. For every positive integer $d<n$, the power $F^d$ is not the identity on $\mathbf{F}_{p^n}$ because the polynomial $X^{p^d}-X$ has no more than $p^d$ zeros in $\mathbf{F}_{p^n}$.

To prove that the cyclic group $\langle F\rangle$ of order $n$ is the entire group $\mathrm{Aut}(\mathbf{F}_q)$, we show that there can be no more than $n$ automorphisms of $\mathbf{F}_q$. To do this, write $\mathbf{F}_q=\mathbf{F}_p(\alpha)$ as in 22.5, and let $f=\sum_{i=0}^n a_iX^i$ be the minimum polynomial of $\alpha$. Every automorphism $\sigma:\mathbf{F}_p(\alpha)\to\mathbf{F}_p(\alpha)$ is the identity on the prime field $\mathbf{F}_p$, hence is fixed by the value $\sigma(\alpha)$. Because $f$ has coefficients in $\mathbf{F}_p$, we have

$$\begin{aligned}f(\sigma(\alpha))&=\textstyle\sum_{i=0}^n a_i\sigma(\alpha)^i=\sum_{i=0}^n\sigma(a_i\alpha^i)=\sigma(\sum_{i=0}^n a_i\alpha^i)\\&=\sigma(f(\alpha))=\sigma(0)=0.\end{aligned}$$

It follows that $\sigma(\alpha)$ is a zero of $f$, and because $f$ has no more than $\deg(f)=n$ zeros in $\mathbf{F}_q$, there are at most $n$ possibilities for $\sigma$. $\square$

The proof of 22.10 shows that the zeros of the minimum polynomial over $\mathbf{F}_p$ of an element $\alpha\in\overline{\mathbf{F}}_p$ are exactly the elements $\sigma(\alpha)$, where $\sigma$ runs over the elements of the automorphism group $\mathrm{Aut}(\mathbf{F}_p(\alpha))$. Because $\mathrm{Aut}(\mathbf{F}_p(\alpha))$ consists of the powers of the Frobenius automorphism, this gives the following result.

**22.11. Corollary.** *Let $f\in\mathbf{F}_p[X]$ be a monic, irreducible polynomial of degree $d$. Then every zero $\alpha$ of $f$ in $\overline{\mathbf{F}}_p$ satisfies the equality*

$$f=\prod_{i=0}^{d-1}(X-\alpha^{p^i})\in\overline{\mathbf{F}_p}[X]. \qquad \square$$

**Exercise 4.** Formulate and prove the analog of 22.11 for an irreducible polynomial $f\in\mathbf{F}_q[X]$.

For an arbitrary extension $K \subset L$ of finite fields, we can easily determine, in the automorphism group $\mathrm{Aut}(L)$ given by 22.10, the subgroup

$$\mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) : \sigma\big|_K = \mathrm{id}_K\}$$

of automorphisms of $L$ *over* $K$. If we write $K = \mathbf{F}_q$ with $q = p^m$ and $L = \mathbf{F}_{q^n} = \mathbf{F}_{p^{mn}}$, then $\mathrm{Aut}_K(L)$ is the subgroup of $\mathrm{Aut}(L) = \langle F \rangle$ generated by $F_K = F^m$, the Frobenius automorphism $F_K : x \mapsto x^{\#K}$ associated with $K$.

**Exercise 5.** Show that $F^k$ is the identity on $\mathbf{F}_{p^m}$ if and only if $k$ is a multiple of $m$.

The group $\mathrm{Aut}_K(L)$ is apparently a cyclic group of order $n$. For every divisor $d$ of $n$, there is a subgroup $H \subset \mathrm{Aut}_K(L)$ of index $d$ and order $n/d$ generated by $F_K^d = F^{dm}$. To this subgroup corresponds a *field of invariants*

$$L^H = \{x \in L : \sigma(x) = x \quad \text{for all } \sigma \in H\}$$

that is equal to $\mathbf{F}_{q^d} = \mathbf{F}_{p^{md}}$. When we compare this with the statement in 22.4, we see that we have the following *Galois correspondence* between subgroups of $\mathrm{Aut}_K(L)$ and *intermediate fields* $E$ of $K \subset L$.

**22.12. Galois theory for finite fields.** *Let $K \subset L$ be an extension of finite fields of degree $n$. Then $\mathrm{Aut}_K(L)$ is a cyclic group of order $n$ generated by the Frobenius automorphism $F_K : x \mapsto x^{\#K}$, and there is a bijection*

$$\begin{aligned} \{E : K \subset E \subset L\} &\longrightarrow \{H : H \subset \mathrm{Aut}_K(L)\} \\ E &\longmapsto \mathrm{Aut}_E(L) \end{aligned}$$

*between the set of intermediate fields $E$ of $K \subset L$ and the set of subgroups $H$ of $\mathrm{Aut}_K(L)$. Under this bijection, $H \subset \mathrm{Aut}_K(L)$ corresponds to the field of invariants $L^H = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in H\}$.* □

In 24.4, we generalize this theorem, called the *fundamental theorem of Galois theory* for $K \subset L$, to the case of an *arbitrary* base field $K$. For finite $K$, the situation is relatively simple: every finite extension $K \subset L$ is *simple*, of the form $L = K(\alpha)$, and by 22.11, along with $\alpha \in L$, all other zeros of $f_K^\alpha$ are also in $L$. There are exactly $[L : K]$ different zeros, and the generator $F_K$ of $\mathrm{Aut}_K(L)$ permutes them cyclically.

For infinite $K$, there often is no Frobenius automorphism, and several other problems also come up. For example, it is unclear whether all finite extensions of $K$ are of the form $K(\alpha)$, whether $f_K^\alpha$ always has $\deg(f_K^\alpha)$ different zeros in $\overline{K}$, and whether these zeros are necessarily in $K(\alpha)$. These problems are treated in the next section. Only for finite extensions $K \subset L$ called *separable* and *normal* in the terminology introduced there is there an analog of 22.12.

Exercises.

6. Give an explicit isomorphism $\mathbf{F}_5[X]/(X^2 + X + 1) \xrightarrow{\sim} \mathbf{F}_5(\sqrt{2})$.

7. Show that $f = X^2 + 2X + 2$ and $g = X^2 + X + 3$ are irreducible in $\mathbf{F}_7[X]$, and give an explicit isomorphism $\mathbf{F}_7[X]/(f) \xrightarrow{\sim} \mathbf{F}_7[X]/(g)$.
8. Calculate the orders of $1 - \sqrt{2}$, $2 - \sqrt{2}$, and $3 - \sqrt{2}$ in $\mathbf{F}_5(\sqrt{2})^*$.
9. Let $\alpha \in \overline{\mathbf{F}}_7$ be a zero of $X^3 - 2 \in \mathbf{F}_7[X]$. Prove that $\mathbf{F} = \mathbf{F}_7(\alpha)$ is a field with 343 elements and that in $\mathbf{F}[X]$, the polynomial $X^3 - 2$ decomposes as $X^3 - 2 = (X - \alpha)(X - 2\alpha)(X - 4\alpha)$. What are the degrees of the irreducible factors of $X^{19} - 1$ in $\mathbf{F}[X]$ and in $\mathbf{F}_7[X]$?
10. Determine the degrees of the irreducible factors of $X^{13} - 1$ in $\mathbf{F}_5[X]$, in $\mathbf{F}_{25}[X]$, and in $\mathbf{F}_{125}[X]$.
11. Let $p$ be a prime. Show that $\mathbf{F}_p[X]/(X^2 + X + 1)$ is a field if and only if $p$ is congruent to 2 mod 3.
12. Let $q$ be a prime power.
    a. For what $q$ is the quadratic extension $\mathbf{F}_{q^2}$ of $\mathbf{F}_q$ of the form $\mathbf{F}_q(\sqrt{x})$ with $x \in \mathbf{F}_q$?
    b. For what $q$ is the cubic extension $\mathbf{F}_{q^3}$ of $\mathbf{F}_q$ of the form $\mathbf{F}_q(\sqrt[3]{x})$ with $x \in \mathbf{F}_q$?
13. Let $p$ be an odd prime.
    a. Show that $\mathbf{F}_{p^2}$ contains a primitive eighth root of unity $\zeta$ and that $\alpha = \zeta + \zeta^{-1}$ satisfies $\alpha^2 = 2$.
    b. Prove: $\alpha \in \mathbf{F}_p \Leftrightarrow p \equiv \pm 1 \bmod 8$. Conclude that 2 is a square modulo $p$ if and only if $p \equiv \pm 1 \bmod 8$ holds.
14. Determine for what primes $p$ the polynomial $X^2 + 2 \in \mathbf{F}_p[X]$ is reducible. [This is the star of Exercise 12.49.]
15. Determine all primes $p$ for which $\mathbf{F}_p[X]/(X^4 + 1)$ is a field.
16. Prove: $f = X^3 + 2$ is irreducible in $\mathbf{F}_{49}[X]$. Is $f$ irreducible over $\mathbf{F}_{7^n}$ for all even $n$?
17. Prove: $f = X^4 + 2$ is irreducible in $\mathbf{F}_{125}[X]$. Is $f$ irreducible over $\mathbf{F}_{5^n}$ for all odd $n$?
18. Let $i \in \overline{\mathbf{F}}_3$ be a zero of $X^2 + 1$. Prove that $\mathbf{F} = \mathbf{F}_3(i)$ is a field with nine elements, and determine $f^{\alpha}_{\mathbf{F}_3}$ for all $\alpha \in \mathbf{F}$. Decompose $X^9 - X$ into irreducible factors in $\mathbf{F}_3[X]$.
19. Let $\mathbf{F} = \mathbf{F}_{32}$ be the field with 32 elements.
    a. Prove: for all $x \in \mathbf{F} \setminus \mathbf{F}_2$, we have $\mathbf{F}^* = \langle x \rangle$.
    b. For how many polynomials $f \in \mathbf{F}_2[X]$ do we have $\mathbf{F}_2[X]/(f) \cong \mathbf{F}$?
20. Formulate and prove the analog of 22.7 for monic, irreducible polynomials in $\mathbf{F}_q[X]$ with $q = p^k$ a prime power.
21. Show that the number $x_n$ of monic, irreducible polynomials of degree $n$ in $\mathbf{F}_p[X]$ satisfies the inequalities
$$p^n - \frac{p}{p-1} p^{n/2} < n x_n \leq p^n.$$
Let $\delta_p(n)$ be the probability that an arbitrarily chosen monic polynomial of degree $n$ in $\mathbf{F}_p[X]$ is irreducible. Prove: $\lim_{n\to\infty} n \cdot \delta_p(n) = 1$ and $\lim_{p\to\infty} \delta_p(n) = \frac{1}{n}$.
22. Formulate and prove the analog of the previous exercise for $\mathbf{F}_q[X]$ with $q = p^k$ a prime power.

23. Show that the fraction $\delta_p(n)$ of monic polynomials of degree $n$ that are irreducible in $\mathbf{F}_p[X]$ satisfies $\delta_p(n) \geq \frac{1}{2n}$.

24. Show that there exist $(p^2+p)/2$ monic polynomials of degree 2 in $\mathbf{F}_p[X]$ that are *reducible*. Conclude: $x_2 = (p^2-p)/2$. Also determine $x_3$ without using Theorem 22.7.

*25. For $n \in \mathbf{Z}_{\geq 1}$, we denote by $\Sigma_T(n)$ the set of monic polynomials of degree $n$ in $\mathbf{Z}[X]$ whose coefficients all have absolute values bounded by $T \in \mathbf{R}_{>0}$, and by $\Sigma_T^{\mathrm{irr}}(n) \subset \Sigma_T(n)$ the subset of irreducible polynomials.

Prove the following statements:

a. If $T = p_1 p_2 \dots p_k$ is the product of $k$ different primes, then of the $T^n$ monic polynomials of degree $n$ with coefficients in $\{0, 1, \dots T-1\} \subset \mathbf{Z}$, at most $(1-\frac{1}{2n})^k T^n$ are reducible in $\mathbf{Z}[X]$.

b. For all $n \in \mathbf{Z}_{\geq 1}$, we have

$$\lim_{T\to\infty} \frac{\#\Sigma_T^{\mathrm{irr}}(n)}{\#\Sigma_T(n)} = 1.$$

[This shows that a "random" monic polynomial in $\mathbf{Z}[X]$ is irreducible "with probability 1."]

26. The ring $\mathcal{R}$ of *arithmetic functions* is the set of functions $f : \mathbf{Z}_{\geq 1} \to \mathbf{C}$ endowed with pointwise addition and the so-called *convolution product*:

$$(f_1 + f_2)(n) = f_1(n) + f_2(n)$$
$$(f_1 \star f_2)(n) = \textstyle\sum_{d|n} f_1(d) f_2(n/d).$$

The subset $\mathcal{M} \subset \mathcal{R}$ of *multiplicative* arithmetic functions consists of the $f \in \mathcal{R} \setminus \{0\}$ that satisfy $f(mn) = f(m)f(n)$ for all relatively prime $m, n \in \mathbf{Z}_{\geq 1}$.

a. Show that $\mathcal{R}$ is an integral domain with as unit element $e$ the characteristic function of $\{1\}$ given by $e(1) = 1$ and $e(n) = 0$ for $n > 1$.

b. Prove: $\mathcal{R}^* = \{f : f(1) \neq 0\}$, and $\mathcal{M}$ is a subgroup of $\mathcal{R}^*$.

c. Show that an element $f \in \mathcal{M}$ is fixed by its values on the prime powers in $\mathbf{Z}_{>1}$. Can these values be chosen independently?

d. Let $E$ be the arithmetic function that is constant, equal to 1, and $\mu$ the inverse of $E$ in $\mathcal{R}$. Prove that the function $\mu$ satisfies the identity (22.8) and is equal to the Möbius function.

27. Let $f, g : \mathbf{Z}_{>0} \to \mathbf{C}$ satisfy the inversion formula

$$f(n) = \textstyle\sum_{d|n} \mu(d) g(n/d)$$

for all $n \in \mathbf{Z}_{>0}$. Prove: $\sum_{d|n} f(d) = g(n)$ for all $n \in \mathbf{Z}_{>0}$.

28. Show that Euler's $\varphi$-function and the functions $\sigma_k : n \mapsto \sum_{d|n} d^k$, for $k \in \mathbf{Z}$, are multiplicative arithmetic functions. Prove: $\sum_{d|n} \mu(d)/d = \varphi(n)/n$.

*29. Let $x_d$ be the number of monic, irreducible polynomials of degree $d$ in $\mathbf{F}_p[X]$.

a. Prove the following power series identity in $\mathbf{Z}[[T]]$:

$$\prod_{n=1}^{\infty} \left(\frac{1}{1-T^n}\right)^{x_n} = \frac{1}{1-pT}.$$

[Hint: use the geometric series $(1-aT)^{-1} = \sum_{k=0}^{\infty} (aT)^k \in \mathbf{Z}_p[[T]]$ and unique factorization in $\mathbf{F}_p[X]$.]

b. Deduce the identity $\sum_{d|n} d \cdot x_d = p^n$ by calculating the logarithmic derivative $(\log f)' = f'/f$ in the above.

30. Prove that the *Artin–Schreier polynomial* $X^p - X - a \in \mathbf{F}_p[X]$ is irreducible of degree $p$ for all $a \in \mathbf{F}_p^*$. How does the polynomial $X^q - X - a \in \mathbf{F}_q[X]$ decompose into irreducible factors for an arbitrary finite field $\mathbf{F}_q$?
[Hint: how does the Frobenius automorphism act on the roots?]

31. Let $K \subset L$ be an extension of finite fields and $G = \mathrm{Aut}_K(L)$ the associated automorphism group. Prove: for $\alpha \in L$ with $L = K(\alpha)$, we have $f_K^\alpha = \prod_{\sigma \in G}(X - \sigma(\alpha))$. What is the corresponding statement for arbitrary $\alpha \in L$?

32. Take $K \subset L$ and $G = \mathrm{Aut}_K(L)$ as in the previous exercise. Define the *norm* and the *trace* of an element $x \in L$ by $N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x)$ and $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x)$.

a. Prove: $N_{L/K} : L^* \to K^*$ and $\mathrm{Tr}_{L/K} : L \to K$ are surjective group homomorphisms.
b. Let $f = \sum_{i=0}^m a_i X^i \in K[X]$ be an irreducible polynomial of degree $m = [L : K]$ and $\alpha$ a zero of $f$ in $L$. Prove the identities

$$N_{L/K}(\alpha) = (-1)^m a_0 a_m^{-1} \quad \text{and} \quad \mathrm{Tr}_{L/K}(\alpha) = -a_{m-1} a_m^{-1}.$$

c. Prove that for $\alpha \neq 0$ in part b, we have $\mathrm{Tr}_{L/K}(\alpha^{-1}) = -a_1 a_0^{-1}$.

*33. Let $f = \sum_{i=0}^m a_i X^i \in \mathbf{F}_p[X]$ be an irreducible polynomial of degree $m \geq 1$ with

$$a_m a_{m-1} \neq 0 \neq a_1 a_0.$$

Let $g = \sum_{i=0}^n b_i X^i \in \mathbf{F}_p[X]$ be the polynomial of degree $n$ that arises from $f$ by subsequently replacing $X$ with $X^p - X$, forming the reciprocal polynomial, and replacing $X$ with $X - 1$ in the latter.

Prove: $g \in \mathbf{F}_p[X]$ is irreducible of degree $n = pm$, and we have $b_n b_{m-1} \neq 0 \neq b_1 b_0$.

34. Let $K \subset L$ be a field extension and $G = \mathrm{Aut}_K(L)$.

a. Show that $L^*$ has a natural structure of module over the group ring $\mathbf{Z}[G]$.
b. Show that $L$ has a natural structure of module over the group ring $K[G]$.
c. Prove: for $K$ finite and $K \subset L$ of finite degree $n$, the group rings in parts a and b are isomorphic to, respectively, $\mathbf{Z}[X]/(X^n - 1)$ and $K[X]/(X^n - 1)$.

*35. Let $K \subset L$ be a degree $n$ extension of finite fields and $G = \mathrm{Aut}_K(L)$ as in the previous exercise. View $L$ as a $K[X]$-module by letting $X$ act as the Frobenius automorphism $F_K$. Prove the following statements:

a. The field $L$ is a finitely generated torsion module over $K[X]$ annihilated by $X^n - 1$.
b. The exponent of $L$ as a $K[X]$-module is $X^n - 1$.
c. There exists an $x \in L$ of order $X^n - 1$, and for such an $x$, the field $L$ is a free $K[G]$-module with basis $\{x\}$.
[Hint: Theorem 16.5.]
d. There exists a $K$-basis for $L$ of the form $\{\sigma(x)\}_{\sigma \in G}$, a so-called *normal basis* for $L$ over $K$.

36. Let $q > 3$ be a prime power. Prove: every element $\alpha \in \mathbf{F}_q^* \setminus \{1\}$ is a generator of the multiplicative group $\mathbf{F}_q^*$ if and only if $q - 1$ is a Mersenne prime (as in Exercise 6.28).

37. Let $f \in \mathbf{F}_q[X] \setminus \{0\}$ be a polynomial and $t$ the number of different monic, irreducible factors of $f$.

    a. Show that the *Berlekamp subalgebra* $B \subset \mathbf{F}_q[X]/(f)$ given by

    $$\{a \in \mathbf{F}_q[X]/(f) : a^q - a = 0\}$$

    is a subring of $\mathbf{F}_q[X]/(f)$ and that as a ring, $B$ is isomorphic to the product of $t$ copies of $\mathbf{F}_q$.

    b. Show: $f$ is irreducible if and only if $\dim_{\mathbf{F}_q} B = 1$ and $\mathrm{ggd}(f, f') = 1$.

38. View $\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$ as a ring with componentwise ring operations, and define

    $$\widehat{\mathbf{Z}} = \{(a_n)_{n\geq 1} \in \textstyle\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z} : a_n \equiv a_d \bmod d \text{ for all } n \geq 1 \text{ and } d \mid n\}.$$

    a. Show that $\widehat{\mathbf{Z}}$ is a subring of $\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$.

    b. Show that $\widehat{\mathbf{Z}}$ is a ring of uncountable cardinality that contains $\mathbf{Z}$ as a proper subring.

    c. Prove: for $m \in \mathbf{Z}_{\geq 1}$, the ring $\widehat{\mathbf{Z}}/m\widehat{\mathbf{Z}}$ is isomorphic to $\mathbf{Z}/m\mathbf{Z}$.

    [The ring $\widehat{\mathbf{Z}}$ is called the *profinite completion of* $\mathbf{Z}$ or the *ring of profinite integers*.]

39. Let $\overline{\mathbf{F}}_p$ be an algebraic closure of $\mathbf{F}_p$. Prove that there exists a group isomorphism

    $$\mathrm{Aut}(\overline{\mathbf{F}}_p) \xrightarrow{\sim} \widehat{\mathbf{Z}}$$

    to the additive group of $\widehat{\mathbf{Z}}$ that maps the Frobenius automorphism to $1 \in \widehat{\mathbf{Z}}$.

40. Let $\mathbf{F}_q \subset L$ be a field extension and $V \subset L$ a finite subset. Prove: $V$ is a sub-$\mathbf{F}_q$-vector space of $L$ if and only if the polynomial $f = \prod_{v\in V}(X - v) \in L[X]$ is of the form $f = X^{q^n} + \sum_{i=0}^{n-1} a_i X^{q^i}$ for some $n \in \mathbf{Z}_{\geq 0}$ and $a_0, \ldots, a_{n-1} \in L$.

41. Let $G = \mathbf{F}_q \rtimes \mathbf{F}_q^*$ be the affine group over $\mathbf{F}_q$, defined as in 8.14.1, and $n$ a positive integer.

    a. Prove: $G$ has a subgroup of order $n$ if and only if we have $n = am$ with $a$ and $m$ positive divisors of, respectively, $q$ and $q - 1$ that satisfy $a \equiv 1 \bmod m$.

    b. Assume that $n$ is not a prime power. Prove: there exists a group of order divisible by $n$ that does not have a subgroup of order $n$.

42. A commutative ring is said to be *reduced* if its nilradical (see 15.14) is the zero ideal.

    a. Let $R$ be a ring. Prove: $R$ is a finite, reduced, commutative ring if and only if $R$ is isomorphic with the product of a finite set of finite fields, with componentwise ring operations.

    b. How many reduced commutative rings of order 72 are there, up to isomorphism?