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 ϕ 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 ϕ 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 α 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 α, is called the extension of K *generated* by α.

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 α 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, α 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 nth 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 π 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 α^β is transcendental.

Exercise 5. Use this to deduce that not only $2^{\sqrt{2}}$ but also $\log 3/\log 2$ and e^π 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^π, and π^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 α 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 α is algebraic over K, then there is a unique monic, irreducible polynomial $f = f_K^\alpha \in K[X]$ that has α 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 ϕ is equal to $K[\alpha]$, and as in the proof of 21.1, we have two possibilities.

If α is transcendental over K, then ϕ 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 α 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 α 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^α) is a prime ideal in $K[X]$ and f_K^α 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^α), 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^α. If f_K^α 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 α and that α is algebraic over K. □

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

Multiplication in a field such as $M = \mathbf{Q}(\alpha)$ is done by multiplying expressions as polynomials in α and reducing the outcome modulo the relation given by the minimum polynomial of α. 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 α 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 α_i are algebraic over K. The

condition is clearly necessary: a transcendental element generates an infinite extension. It is also sufficient because for algebraic α_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 α_1 and α_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* Ω *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* Ω *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 Ω 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 Ω that contains K. Such an Ω always exists. However, since K can be very large, general constructions of Ω 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 ϕ 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 $K \subset L_1 \subset L_2 \subset L_3 \subset \ldots$ 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 Ω, 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

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

This field, which is of finite degree over K, clearly satisfies the conditions of 21.14. However, the degree of Ω_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 Ω_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 ζ_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 β 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 α, $\alpha\beta$, 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 pth 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 ζ_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 ψ, and there is no "natural choice." For every pair of choices ψ_1 and ψ_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 α and β 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 α to β.

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

We just saw that for $f = X^3-2$ and $K = \mathbf{Q}$, two splitting fields Ω_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 φ 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 under 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 α 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, μ, 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 α in $\overline{K}_1 \setminus E_1$ or in $\overline{K}_2 \setminus E_2$. Then α 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, ϕ, E_2), contradicting the maximality of (E_1, ϕ, 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 ψ 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 α 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 α^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 Ω_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 α 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 Ω_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 pth 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 pth 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* pth 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 β is the only pth root of α. 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

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

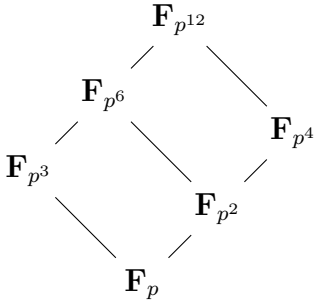
The complete structure of the set of subfields of $\overline{\mathbf{F}}_p$ and the inclusion relations between the subfields can be deduced from this characterization.

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 α 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 α 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 α is a zero of $X^{p^n} - X$, and the latter just means that the minimum polynomial f of α 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 μ:

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

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 α. 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 σ. $\square$

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 σ 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 α 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 $L^H = \{x \in L : \sigma(x) = x$ 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^α 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^α 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 ζ 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 μ the inverse of E in $\mathcal{R}$. Prove that the function μ 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 φ-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 α 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.

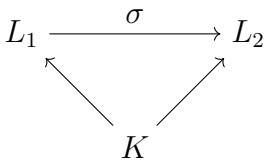
    b. How many reduced commutative rings of order 72 are there, up to isomorphism?

23 Separable and normal extensions

In this section, we treat two properties of algebraic field extensions that play an essential role in Galois theory: *separability* and *normality*. For a large class of base fields, including finite fields and fields of characteristic 0, *all* algebraic extensions turn out to be separable.

▶ Fundamental set

Let L_1 and L_2 be extensions of a field K. We denote by $\mathrm{Hom}_K(L_1, L_2)$ the set of field homomorphisms $L_1 \to L_2$ that are the identity on K. More succinctly: the K-homomorphisms $L_1 \to L_2$. These are the homomorphisms $\sigma : L_1 \to L_2$ that form a commutative diagram



with the inclusion arrows $K \to L_i$.

23.1. Lemma. *Let $K \subset L_1 = K(\alpha)$ be a simple algebraic field extension, $K \subset L_2$ an arbitrary field extension, and S the set of zeros of f_K^α in L_2. Then there is a bijection $\mathrm{Hom}_K(L_1, L_2) \xrightarrow{\sim} S$ given by $\sigma \mapsto \sigma(\alpha)$.*

Proof. A homomorphism $\sigma : K(\alpha) \to L_2$ that is the identity on K is fixed by the choice of the element $\sigma(\alpha) \in L_2$. To see that $\sigma(\alpha)$ is a zero of $f = f_K^\alpha$ in L_2, we write $f = \sum_{i=0}^n a_i X^i \in K[X]$. As in the proof of 22.10, we now have

$$f(\sigma(\alpha)) = \textstyle\sum_{i=0}^n a_i \sigma(\alpha)^i = \sigma\big(\sum_{i=0}^n a_i \alpha^i\big) = \sigma(0) = 0$$

because σ is the identity on the coefficients of f. This proves $\sigma(\alpha) \in S$.

Conversely, for every zero $s \in S$ of f, the map $L_1 \to L_2$ defined by $\sum_i c_i \alpha^i \mapsto \sum_i c_i s^i$ is a K-homomorphism $L_1 \to L_2$ by 21.5.2. □

23.2. Definition. *Let $K \subset L$ be an algebraic extension and Ω an algebraically closed field that contains K. Then*

$$X(L/K) = X_\Omega(L/K) = \mathrm{Hom}_K(L, \Omega)$$

is called a fundamental set for the extension $K \subset L$.

Even though a fundamental set for $K \subset L$ depends on the choice of an algebraically closed field $\Omega \supset K$, we will often write $X(L/K)$ for $X_\Omega(L/K)$.

Lemma 23.1 shows that the image in Ω of an element $\alpha \in L$ under $\sigma \in X(L/K)$ is again algebraic over K. We can therefore identify $X_\Omega(L/K)$ with $\mathrm{Hom}_K(L, \overline{K})$, where $\overline{K}$ is the algebraically closed field obtained by forming the algebraic closure of K in Ω, as in 21.12. We usually simply take $\Omega = \overline{K}$, but for $K = \mathbf{Q}$, it is sometimes also convenient to take $\Omega = \mathbf{C}$.

Exercise 1. Are there algebraic extensions $K \subset L$ for which $X(L/K)$ is the empty set?

If $\overline{K}'$ is another algebraic closure of K, then there exists a K-isomorphism $\psi : \overline{K} \xrightarrow{\sim} \overline{K}'$ by 21.16. Composition with ψ gives a bijection

$$\mathrm{Hom}_K(L, \overline{K}) \xrightarrow{\sim} \mathrm{Hom}_K(L, \overline{K}').$$

We conclude that the cardinality of $X(L/K)$ does not depend on the choice of the field Ω in 23.2. For a simple algebraic extension $L = K(\alpha)$, it follows from 23.1 that we can identify the fundamental set $X(L/K)$ with the set of zeros of f_K^α in an algebraic closure of K. However, this "more explicit" description has the disadvantage that, unlike $X(L/K)$ itself, it depends on the choice of a generating element α.

More generally, for finite extensions $K \subset L$, which are algebraic by 21.6, the fundamental set $X(L/K)$ is always finite. After all, write $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and note that $\sigma \in X(L/K)$ is fixed by its values on the elements α_i. Since $\sigma(\alpha_i)$ is a zero of $f_K^{\alpha_i}$, there are only finitely many possibilities for σ.

▶ Separable extensions

The "separability properties" of an extension $K \subset L$ can be deduced from the fundamental set $X(L/K)$. We call a polynomial in $K[X]$ *separable* if it does not have multiple zeros in an algebraic closure $\overline{K}$ and *inseparable* if it does.

23.3. Definition. *The separable degree $[L : K]_s$ of an algebraic extension $K \subset L$ is the cardinality of a fundamental set $X(L/K)$.*

We have already seen that the cardinality of $X(L/K)$ does not depend on the choice of the algebraically closed field Ω in the definition of $X(L/K)$. For a simple algebraic extension $K \subset L = K(\alpha)$, by 23.1, the degree $[L : K]_s$ is the number of different zeros of f_K^α in $\overline{K}$. We therefore have

$$1 \leq [K(\alpha) : K]_s \leq \deg(f_K^\alpha) = [K(\alpha) : K],$$

and we have equality if and only if f_K^α is separable. In the separable case, we have

$$f_K^\alpha = \prod_{\sigma \in X(K(\alpha)/K)} (X - \sigma(\alpha)).$$

23.4. Lemma. *For every finite field extension $K \subset L$, we have the inequality*

$$1 \leq [L : K]_s \leq [L : K].$$

For a tower $K \subset L \subset M$ of finite extensions, we have

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

Proof. Every embedding $\tau : M \to \Omega$ in $X(M/K)$ is obtained by extending an embedding $\sigma : L \to \Omega$ from $X(L/K)$. Now, for a fixed "inclusion" $\sigma : L \to \Omega$, we can identify the set of extensions $\tau : M \to \Omega$ with $X(M/L)$, and this gives $\#X(M/K) = \#X(L/K) \cdot \#X(M/L)$. The second statement in 23.4 follows.

Now that we know that, like the ordinary degree, the separable degree behaves multiplicatively in towers of extensions, we can deduce the general inequality $[L : K]_s \leq [L : K]$ from the inequality already mentioned for the simple case. After all, an arbitrary finite extension $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ 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. Multiplying the inequalities for these extensions immediately gives $[L : K]_s \leq [L : K]$. □

For an arbitrary algebraic extension $K \subset L$, we say that an element $\alpha \in L$ is *separable* over K if f_K^α has no multiple zeros in $\overline{K}$. The extension $K \subset L$ itself is called separable if every element $\alpha \in L$ is separable over K. An algebraic extension that is not separable is called *inseparable*.

23.5. Theorem. *For a finite extension $K \subset L$, the following are equivalent:*

1. *The extension $K \subset L$ is separable.*
2. *We have $L = K(\alpha_1, \alpha_2, \ldots, \alpha_t)$ for elements $\alpha_1, \alpha_2, \ldots, \alpha_t \in L$ that are separable over K.*
3. *$[L : K]_s = [L : K]$.*

Proof. $(1 \Rightarrow 2)$. This is clear because all $\alpha_i \in L$ are separable over K.

$(2 \Rightarrow 3)$. For a simple extension $K \subset K(\alpha)$, we have already seen that by 23.1, the separability of α implies that $[K(\alpha) : K]_s$ is equal to $\deg(f_K^\alpha) = [K(\alpha) : K]$. For $L = K(\alpha_1, \alpha_2, \ldots, \alpha_t)$, as in the proof of 23.4, we obtain L by successively adjoining the α_i. The elements α_i, which are separable over K, are also separable over every extension E of K because f_E^α is a divisor of f_K^α in $\overline{K}[X]$. Therefore, in every step of the tower, the degree and separable degree are equal. By the multiplicativity of the degree and separable degree, equality also holds for the whole extension $K \subset L$.

$(3 \Rightarrow 1)$. For every $\alpha \in L$, we have a tower $K \subset K(\alpha) \subset L$. Since the separable degree is bounded by the degree, it follows from the equality $[L : K]_s = [L : K]$ and the multiplicativity in towers that for the extension $K \subset K(\alpha)$ too, the equality $[K(\alpha) : K]_s = [K(\alpha) : K]$ holds. By 23.1, this means that f_K^α has exactly $\deg(f_K^\alpha)$ different zeros in $\overline{K}$, so α is separable over K. □

▶ Perfect fields

For many base fields K, *all* algebraic extensions turn out to be separable. Namely, irreducible polynomials only rarely have double zeros.

23.6. Lemma. *Let $f \in K[X]$ be an irreducible polynomial, and suppose that f is inseparable. Then we have $p = \mathrm{char}(K) > 0$ and $f = g(X^p)$ for some $g \in K[X]$. Moreover, not all coefficients of f are pth powers in K.*

Proof. If f has a double zero $\alpha \in \overline{K}$, then α is also a zero of the derivative f' of f. Because (up to multiplication by a unit $c \in K^* = K[X]^*$) f is the minimum polynomial of α over K, the assumption $f'(\alpha) = 0$ implies that f' is divisible is by f. Since f' has a lower degree than f, this is only possible if f' is the zero polynomial in $K[X]$.

For K of characteristic 0, we find that f is constant, which contradicts the assumption that f is irreducible. We therefore have $\mathrm{char}(K) = p > 0$, and by explicitly taking derivatives, we see that we obtain $f' = 0$ for the polynomials in $K[X]$ of the form $f = \sum_i a_i X^{ip} \in K[X]$. For $g = \sum_i a_i X^i$, we then have $f = g(X^p)$.

If all coefficients of f are pth powers in K, say $a_i = c_i^p \in K$, then we have $f = \sum_i a_i X^{ip} = \sum_i c_i^p X^{ip} = (\sum_i c_i X^i)^p$ by the additivity of taking the pth power in characteristic p. However, an irreducible polynomial $f \in K[X]$ cannot be a pth power in $K[X]$, so this leads to a contradiction. □

We conclude from 23.6 that irreducible inseparable polynomials in $K[X]$ can only exist for fields K of characteristic $p > 0$ for which the Frobenius map $F : K \to K$ given by $x \mapsto x^p$ is *not* surjective. Note that, as it is a field homomorphism $K \to K$, the map F is always injective.

23.7. Definition. *A field K is called perfect if it satisfies one of the following two conditions:*

1. *The characteristic of K is 0.*
2. *The characteristic of K is $p > 0$, and the Frobenius map $F : x \mapsto x^p$ is an automorphism of K.*

Note that finite fields and number fields—the most important examples for us—are perfect. However, in the field $\mathbf{F}_p(T)$, the element T is not a pth power, so $\mathbf{F}_p(T)$ is imperfect. Imperfect base fields are common in arithmetic algebraic geometry.

23.8. Theorem. *A field K is perfect if and only if every algebraic extension of K is separable.*

Proof. If K has an inseparable algebraic extension, then there exist inseparable irreducible polynomials in $K[X]$ and K is not perfect by 23.6.

If, conversely, K is not perfect, then there is an element $a \in K$ that is not a pth power in K. Let $\alpha \in \overline{K}$ be a zero of the polynomial $X^p - a$. Then we have

$$X^p - a = (X - \alpha)^p \in \overline{K}[X],$$

so $K \subset K(\alpha)$ is an inseparable extension. □

Exercise 2. Is the polynomial $X^p - a$ above necessarily *irreducible* in $K[X]$?

▶ Primitive elements

Many of the proofs in this section reduce questions for an arbitrary finite extension $K \subset L$ to the case of a simple extension $K \subset K(\alpha)$. One can wonder whether every finite extension $K \subset L$ is necessarily of this form. In this case, α is called a *primitive element* for the extension $K \subset L$. For explicit calculations, it is often useful to have a

primitive element. Just as we prefer to avoid choosing a basis in (conceptual) proofs in linear algebra, we can, where possible, avoid choosing a primitive element in proofs in field theory.

Some trial and error shows that in many extensions with multiple generators, such as $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}, \sqrt{3})$, we can find a primitive element by considering linear combinations of the generators over the base field.

Exercise 3. Prove: $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\lambda\sqrt{2} + \mu\sqrt{3})$ for all $\lambda, \mu \in \mathbf{Q}^*$.

In separable extensions, there is always a primitive element.

23.9. Primitive element theorem. *Let $K \subset L$ be a finite separable extension. Then there exists an element $x \in L$ with $L = K(x)$.*

Proof. It suffices to show that for every pair of elements $\alpha, \beta \in L$, we can find an element $x \in L$ such that $K(\alpha, \beta) = K(x)$ holds. After all, by successively replacing two generators by a single one, we thus obtain a primitive element for every finitely generated subextension of L over K—and therefore also for L itself.

Now, suppose that $L = K(\alpha, \beta)$ has degree n over K. By the separability of $K \subset L$, the set $X(L/K) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ contains exactly n different embeddings. We are looking for an element $\lambda \in K$ such that the images of $x = \alpha + \lambda\beta$ under the elements σ_i are all different. This means that λ is not a zero of the polynomial

$$f = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} \big(\big(\sigma_i(\beta) - \sigma_j(\beta)\big)X + \big(\sigma_i(\alpha) - \sigma_j(\alpha)\big)\big) \in \overline{K}[X].$$

Since two different elements of $X(L/K)$ cannot agree on both α and β, it follows that f is not the zero polynomial. This means that f has only finitely many zeros, and for infinite K, we find that there exists a $\lambda \in K$ with $f(\lambda) \neq 0$. For finite K, this is not clear, but in that case, 22.5 provides the existence of a primitive element and we are immediately done.

For infinite K, we choose $x = \alpha + \lambda\beta$ as above. Then $K(x)$ has separable degree at least n over K, and therefore also degree $[K(x) : K] \geq n$. On the other hand, we have $[K(x) : K] \leq [L : K] = n$, so that $K(x) = L$ holds, as desired. □

In inseparable extensions, too, it is sometimes possible to find primitive elements, for example when the degree is a prime. If no primitive element exists, we are dealing with an extension with infinitely many *intermediate fields*. For such extensions, there is no *Galois correspondence* in the sense of 24.4.

23.10. Theorem. *Let $K \subset L$ be a finite extension. The following are equivalent:*

1. *There exists an element $\alpha \in L$ with $L = K(\alpha)$.*
2. *There are only finitely many fields E with $K \subset E \subset L$.*

Proof. (1 ⇒ 2). Let α be a primitive element for $K \subset L$, and for every intermediate field E, consider the minimum polynomial $f_E^\alpha \in E[X]$. Since f_E^α is a monic divisor of f_K^α in $\overline{K}[X]$ and a polynomial with coefficients in a field has only finitely many monic

divisors, there are only finitely many possibilities for f_E^α. However, the field E can be deduced from f_E^α: it is the extension of K generated by the coefficients of f_E^α. After all, over the intermediate field $E_0 \subset E$ generated by these coefficients over K, we have $[L : E_0] = \deg(f_{E_0}^\alpha) = \deg(f_E^\alpha) = [L : E]$, and therefore $E_0 = E$.

$(2 \Rightarrow 1)$. Because both statements automatically hold for finite fields K, we assume that K is infinite. As in the proof of 23.9, it suffices to show that every subextension $K \subset K(\alpha, \beta)$ of $K \subset L$ is primitive. Given elements $\alpha, \beta \in L$, we now know that the fields $K(\alpha + \lambda\beta)$ with $\lambda \in K$ are not all different. So, suppose $K(\alpha + \lambda_1\beta) = K(\alpha + \lambda_2\beta)$ with $\lambda_1 \neq \lambda_2$. Then $K(\alpha + \lambda_1\beta)$ contains the elements

$$\alpha = (\lambda_2 - \lambda_1)^{-1}[\lambda_2(\alpha + \lambda_1\beta) - \lambda_1(\alpha + \lambda_2\beta)],$$
$$\beta = (\lambda_1 - \lambda_2)^{-1}[(\alpha + \lambda_1\beta) - (\alpha + \lambda_2\beta)],$$

so $K(\alpha, \beta) = K(\alpha + \lambda_1\beta)$ is a primitive extension. □

Exercise 4. Let V be a vector space over an infinite base field K. Prove that V is *not* the union of a finite number of subspaces $V_i \subsetneq V$. Deduce from this the implication 23.10.2 ⇒ 23.10.1.

Exercise 20 gives an example of an inseparable extension of degree p^2 that is not primitive and therefore has infinitely many intermediate fields.

▶ Normal extensions

For a finite separable extension $K \subset L$, we know that there are $[L : K]$ different ways to embed L in an algebraically closed extension Ω of K. In the case where the image $\sigma[L] \subset \overline{K}$ does not depend on the choice of $\sigma \in X(L/K)$, we can *choose* a fixed K-embedding $\tau : L \subset \Omega$ and view it as an inclusion. The elements of $X(L/K)$ then become *automorphisms* of the field L, and we obtain an identification

$$X(L/K) \xrightarrow{\sim} \mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) : \sigma\big|_K = \mathrm{id}_K\} \tag{23.11}$$

of $X(L/K)$ with the *group* of automorphisms of L that are the identity on K. However, this identification depends on the choice of an element $\tau \in X(L/K)$ that acts as the identity $\mathrm{id}_L \in \mathrm{Aut}_K(L)$; see Exercise 28.

For a finite separable extension $K \subset L$, the images $\sigma[L] \subset \overline{K}$ for $\sigma \in X(L/K)$ are not necessarily equal. Namely, if we write $L = K(\alpha)$ for a primitive element $\alpha \in L$, then the images of L in Ω are the fields $K(\alpha_i)$, with α_i running through the zeros of f_K^α in Ω. The fields $K(\alpha_i)$ coincide if and only if f_K^α has *all* of its zeros in $L = K(\alpha)$ and L therefore is a splitting field of f_K^α over K. In such a case, we call L a *normal* separable extension of K. The general definition of normality is as follows.

23.12. Definition. *An algebraic field extension $K \subset L$ is said to be normal if for every element $\alpha \in L$, the minimum polynomial f_K^α decomposes into linear factors in $L[X]$.*

23.13. Examples. The field $L = \mathbf{Q}(\alpha)$ from 21.15.2 obtained by adjoining a third root α of 2 is not a normal extension of $\mathbf{Q}$: the polynomial $f_{\mathbf{Q}}^\alpha = X^3 - 2$ has only one zero in L.

Every finite extension $\mathbf{F}_p \subset L$ of $\mathbf{F}_p$ is normal. After all, by 22.11, for every $\alpha \in L$, the zeros of $f^{\alpha}_{\mathbf{F}_p}$ are *powers* of α, and those are in L.

The inseparable extension $K = \mathbf{F}_p(T) \subset L = \mathbf{F}_p(T^{1/p})$ is normal. After all, for every $\alpha \in L$, we have $\alpha^p \in K$, and $X^p - \alpha^p \in K[X]$ has a p-tuple linear factor $X - \alpha$ in $L[X]$.

23.14. Theorem. *For a finite extension $K \subset L$ with fundamental set $X(L/K)$, the following are equivalent:*

1. *The extension $K \subset L$ is normal.*
2. *The field L is a splitting field Ω^f_K of a polynomial $f \in K[X]$.*
3. *For all $\sigma, \tau \in X(L/K)$, we have $\sigma[L] = \tau[L]$.*

Proof. $(1 \Rightarrow 2)$. Write $L = K(\beta_1, \beta_2, \ldots, \beta_t)$. Then because of the normality of $K \subset L$, all zeros of $f = f_K^{\beta_1} \cdot f_K^{\beta_2} \cdot \ldots \cdot f_K^{\beta_t} \in K[X]$ are in L. Since they generate L over K, we have $L = \Omega^f_K$.

$(2 \Rightarrow 3)$. Let $L = \Omega^f_K$, and suppose that in $\overline{K}[X]$, the polynomial f decomposes as $f = \prod_{i=1}^n (X - \alpha_i)$. This gives an inclusion $\sigma : L = K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \overline{K}$. For $\tau \in X(L/K)$ arbitrary, we then have $\prod_{i=1}^n (X - \tau(\alpha_i)) = f = \prod_{i=1}^n (X - \alpha_i)$ because τ is the identity on the coefficients of f. We find that τ permutes the zeros of f, and that gives the desired equality $\tau[L] = K(\tau(\alpha_1), \tau(\alpha_2), \ldots, \tau(\alpha_n)) = K(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sigma[L] \subset \overline{K}$.

$(3 \Rightarrow 1)$. Choose an element $\sigma : L \to \overline{K}$ in $X(L/K)$, and take $\alpha \in L$ arbitrary. Suppose that f^{α}_K decomposes as $f^{\alpha}_K = \prod_{i=1}^n (X - \alpha_i)$ in $\overline{K}[X]$. By 23.1, this gives K-isomorphisms $\sigma_i : K(\alpha) \xrightarrow{\sim} K(\alpha_i) \subset \overline{K}$. As in Exercise 21.14, each of the isomorphisms σ_i has an extension to an isomorphism $\sigma_i' : \overline{L} \to \overline{K}$, where $\overline{L}$ is an algebraic closure of L (and therefore of $K(\alpha)$). This isomorphism maps α to $\alpha_i \in \sigma_i'[L]$, and by assumption 3, we have $\sigma_i'[L] = \sigma[L]$ for all σ_i'. It follows that f^{α}_K decomposes into linear factors over $\sigma[L]$ and therefore also over L. □

The proof of 23.14 shows that every finite extension $K \subset L$ fits into a tower of extensions $K \subset L \subset M$ with M finite and normal over K: take the product f of the minimum polynomials of a finite set of elements β_i that generates L over K, and choose $M = \Omega^f_K = \Omega^f_L$. Since every normal extension of K that contains all β_i also contains a subfield isomorphic to M, we find that M is the "smallest" normal extension of K that contains L. Such an extension is called a *normal closure* of L over K.

Exercise 5. Show that a normal closure of L over K is uniquely determined up to K-isomorphism and that in an algebraic closure $\overline{K}$ of K, there exists a *unique* normal closure of L.

▶ Independence of characters

The most important ingredient in the proof of the fundamental theorem of Galois theory, which we formulate in 24.4 for finite *normal* and *separable* field extensions $K \subset L$, is the "linear independence" of the elements of the fundamental set $X(L/K)$. By this, we mean the following.

23.15. Artin–Dedekind lemma. *Let $K \subset L$ be a field extension and $\sigma_1, \sigma_2, \ldots, \sigma_n \in X(L/K) = \mathrm{Hom}_K(L, \Omega)$ an n-tuple of pairwise distinct elements. Suppose that there exist $c_1, c_2, \ldots, c_n \in \Omega$ with*

$$c_1\sigma_1(x) + c_2\sigma_2(x) + \ldots + c_n\sigma_n(x) = 0 \qquad \text{for all } x \in L.$$

Then we have $c_1 = c_2 = \ldots = c_n = 0$.

Proof. We carry out the proof by induction on n. For $n = 1$, it immediately follows from the relation $c_1\sigma_1(x) = 0$ for $x \in L$ that we have $c_1 = c_1\sigma(1) = 0$.

Now, suppose that the lemma is correct for subsets of $X(L/K)$ with fewer than n elements, and suppose given a zero relation as above between $n \geq 2$ elements. Since σ_1 and σ_2 differ on L, there exists an element $y \in L$ with $\sigma_1(y) \neq \sigma_2(y)$. Take such a y, and from the given zero relation, deduce two new relations by, respectively, multiplying the relation by $\sigma_1(y)$ and replacing x in the relation with xy. Since the σ_i are homomorphisms, for arbitrary $x \in L$, this gives

$$\begin{aligned} c_1\sigma_1(x)\sigma_1(y) + c_2\sigma_2(x)\sigma_1(y) + \ldots + c_n\sigma_n(x)\sigma_1(y) &= 0, \\ c_1\sigma_1(x)\sigma_1(y) + c_2\sigma_2(x)\sigma_2(y) + \ldots + c_n\sigma_n(x)\sigma_n(y) &= 0. \end{aligned}$$

Taking the difference of these relations gives a zero relation for the $n-1$ elements $\sigma_2, \sigma_3, \ldots, \sigma_n$ in which the coefficient of σ_2 is equal to $c_2(\sigma_1(y) - \sigma_2(y))$. By the induction hypothesis, this coefficient is equal to 0. The choice of y implies that we have $c_2 = 0$, so the term with σ_2 in the original relation can be left out. If we apply the induction hypothesis again, we see that all c_i are equal to 0. □

The proof given above only uses that the σ_i are *group homomorphisms* $L^* \to \Omega^*$. If, more generally, for an abelian group A and a field F, we define an *F-valued character* on A to be a group homomorphism $\sigma : A \to F^*$, then exactly the same proof shows that there are no F-linear relations between the F-valued characters on A.

Exercise 6. Formulate and prove this more general Artin–Dedekind lemma.

▶ Norm and trace

Let $K \subset L$ be a finite separable extension. Then the *norm* and the *trace* from L to K of an element $x \in L$ are defined by

$$N_{L/K}(x) = \prod_{\sigma \in X(L/K)} \sigma(x) \qquad \text{and} \qquad \mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in X(L/K)} \sigma(x). \tag{23.16}$$

The multiplicative property $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$ of the norm and the additive property $\mathrm{Tr}_{L/K}(x+y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$ of the trace are immediately clear.

We already came across the norm map $N_{\mathbf{Q}(i)/\mathbf{Q}} : \mathbf{Q}(i) \to \mathbf{Q}$, which sends $a + bi$ to $(a+bi)(a-bi) = a^2 + b^2$, just before 12.19. In this case, the norm of x is the product of x with its complex conjugate $\overline{x}$. For an arbitrary separable extension $K \subset L$, it follows from 23.1 that if $x \in L$ generates the field L over K, then the norm $N_{L/K}(x)$ is the product of the zeros of the separable polynomial $f_K^x = \sum_{i=0}^n a_i X^i \in K[X]$ in

an algebraic closure of K and the trace $\mathrm{Tr}_{L/K}(x)$ is the sum of the zeros. These are equal to, respectively, $(-1)^n a_0$ and $-a_{n-1}$ and therefore lie in K. More generally, as in the proof of 23.4, we find the elements of $X(L/K)$ by considering, for every element of $X(K(x)/K)$, the $[L : K(x)]$ different extensions to L; this gives

$$N_{L/K}(x) = N_{K(x)/K}(x)^{[L:K(x)]} \quad \text{and} \quad \mathrm{Tr}_{L/K}(x) = [L : K(x)] \cdot \mathrm{Tr}_{K(x)/K}(x). \tag{23.17}$$

We conclude that the norm induces a group homomorphism $N_{L/K} : L^* \to K^*$ and the trace a group homomorphism $\mathrm{Tr}_{L/K} : L \to K$. For an extension $K \subset L$ of *finite* fields, we already came across these homomorphisms in Exercise 22.32.

Exercise 7. Is the norm map $N_{\mathbf{Q}(i)/\mathbf{Q}} : \mathbf{Q}(i) \to \mathbf{Q}$ surjective?

For an element x in a finite extension L of K, the multiplication

$$\begin{aligned} M_x : L &\longrightarrow L \\ y &\longmapsto xy \end{aligned}$$

by x is a K-linear map of the K-vector space L, and we have the following relationship with the determinants and traces of matrices known from linear algebra.

23.18. Theorem. *Let $K \subset L$ be a finite separable extension and $x \in L$. Then $M_x : L \to L$ is a K-linear map with determinant $N_{L/K}(x)$, trace $\mathrm{Tr}_{L/K}(x)$, and characteristic polynomial $(f_K^x)^{[L:K(x)]}$.*

Proof. We can view $L = \sum_{k=1}^{[L:K(x)]} K(x) \cdot \omega_k$ as a sum of $[L : K(x)]$ one-dimensional vector spaces $K(x) \cdot \omega_k$ over $K(x)$, which are each mapped to themselves by the K-linear map M_x. The characteristic polynomial of M_x is therefore the $[L : K(x)]$th power of the characteristic polynomial of the restriction $M_x : K(x) \to K(x)$.

If we write $f_K^x = \sum_{i=1}^n a_i X^i \in K[X]$, then with respect to the K-basis $\{1, x, x^2, \ldots, x^{n-1}\}$ of $K(x)$, the map M_x is represented by the matrix

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ \vdots & \ddots & & \vdots & \vdots \\ 0 & \ldots & 1 & 0 & -a_{n-2} \\ 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix},$$

which has determinant $(-1)^n a_0 = N_{K(x)/K}(x)$ and trace $-a_{n-1} = \mathrm{Tr}_{K(x)/K}(x)$. For the characteristic polynomial $\det(X \cdot I - A)$, we inductively obtain $f_K^x = \sum_{i=1}^n a_i X^i$ by repeatedly expanding along the last row. By (23.17), the desired result follows. □

Exercise 8. Show that after a "base extension" $K \to \Omega$, on $L \otimes_K \Omega$, the map M_x can be represented by a diagonal matrix with diagonal elements $\{\sigma(x) : \sigma \in X_\Omega(L/K)\}$, and use this to give a "better" proof of 23.18.

Conversely, we can take 23.18 as the *definition* of the norm and trace maps for a finite extension $K \subset L$ and deduce the expression (23.16) for separable extensions; see Exercises 30 and 31.

Exercises.

9. Let $L_1 = K(T)$ be a simple transcendental extension of K and $K \subset L_2$ an arbitrary extension. Prove: the map $\mathrm{Hom}_K(L_1, L_2) \to L_2$ given by $f \mapsto f(T)$ is injective. Describe the image.

10. Let $K \subset L \subset M$ be a tower of algebraic extensions. Prove:

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

11. Let $K \subset L$ be an arbitrary field extension. Prove that

$$K_s = \{x \in L : x \text{ is algebraic and separable over } K\}$$

is a subfield of L. It is called the *separable closure* of K in L.

12. A field F is called *separably closed* if the only separable algebraic extension $F \subset E$ is the trivial extension $E = F$. A *separable closure* of a field K is a separable algebraic extension $K \subset K^{\mathrm{sep}}$ with K^{sep} separably closed. Prove:
    a. Every field K has a separable closure.
    b. Any two separable closures of K are K-isomorphic.
    c. A separable closure K^{sep} of K is algebraically closed if and only if K is perfect.

13. Deduce the primitive element theorem from the vector space argument in Exercise 4. [Hint: consider $\{x \in L : \sigma(x) = \tau(x)\}$ for $\sigma, \tau \in X(L/K)$.]

14. Let K be a field of characteristic $p > 0$ and $f \in K[X]$ an irreducible polynomial. Prove that there exist a separable irreducible polynomial $g \in K[X]$ and an integer $n \in \mathbf{Z}_{\geq 0}$ with $f = g(X^{p^n})$. What is the separable closure of K in $L = K[X]/(f)$?

15. Let $K \subset L$ be a finite extension with $p = \mathrm{char}(K) > 0$ and K_s the separable closure of K in L. Prove: $[L : K]_s = [K_s : K]$ and $[L : K]_s \cdot p^k = [L : K]$ for some $k \in \mathbf{Z}_{\geq 0}$. [The number $[L : K]/[L : K]_s$ is called the *inseparable degree* of L over K.]

16. Let α be algebraic over K. Prove: $f_K^\alpha = \prod_{\sigma \in X(K(\alpha)/K)} (X - \sigma(\alpha))^i$, where i is the inseparable degree of $K(\alpha)$ over K.

17. Let K be a field of characteristic $p > 0$ and $a \in K$ an element that is not a pth power. Prove: $X^{p^k} - a$ is irreducible in $K[X]$ for all $k \geq 0$.

18. Let K be of characteristic $p > 0$ and $f \in K[X]$ monic irreducible. Write $L = K(\alpha)$ with α a zero of f, and denote by K^p and L^p the images of the Frobenius map on, respectively, K and L.
    a. Prove: $\alpha \in L^p \Rightarrow f \in K^p[X]$.
    b. Suppose $f \notin K^p[X]$. Prove: $f(X^{p^k})$ is irreducible in $K[X]$ for $k \in \mathbf{Z}_{\geq 0}$.

19. Let $f \in \mathbf{F}_p[T]$ be an irreducible polynomial and $K = \mathbf{F}_p(T)$ the field of fractions of $\mathbf{F}_p[T]$.
    a. Prove: $X^p - f$ is irreducible in $K[X]$.
    b. Prove: $K \subset L_f = K[X]/(X^p - f)$ is an inseparable extension of degree p, and we have $L_f^p = K$.

c. Let L be the field obtained by taking $f = T$ in part b. Prove: $L_f \cong L$ for all irreducible $f \in \mathbf{F}_p[T]$.

20. Let $L = \mathbf{F}_p(S,T)$ be the field of rational functions in two variables over $\mathbf{F}_p$ and $K = L^p$.
    a. Prove: $K = \mathbf{F}_p(S^p, T^p)$, and $K \subset L$ is a field extension of degree p^2.
    b. Show that $K \subset L$ is not a primitive extension.
    c. Give infinitely many different fields E with $K \subset E \subset L$.

21. For a field K of characteristic $p > 0$, the degree $[K : K^p]$ of the field extension $K^p \subset K$ is called the *degree of imperfection* of K. Prove the following statements:
    a. $[K : K^p] = p^{i(K)}$ with $i(K) \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$.
    b. For every finite extension $K \subset L$, we have $i(L) = i(K)$.
    c. For every algebraic extension $K \subset L$, we have $i(L) \leq i(K)$.
    d. $i(K(T)) = i(K) + 1$.

22. Let $K \subset L$ be a quadratic extension. Prove: $K \subset L$ is normal.

23. Let L be a quadratic extension of a field K of characteristic different from 2. Prove: $L \cong K(\sqrt{x}) \cong K[X]/(X^2 - x)$ for some $x \in K$. Show that the assumption on the characteristic cannot be left out.

24. Let $K \subset L \subset M$ be a tower of finite extensions. For each of the following statements, give a proof or a counterexample:
    a. If $K \subset L$ and $L \subset M$ are normal, then $K \subset M$ is normal.
    b. If $K \subset M$ is normal, then $L \subset M$ is normal.
    c. If $K \subset M$ is normal, then $K \subset L$ is normal.

25. Formulate and prove the analog of 23.14 for arbitrary algebraic extensions.
    [Hint: use a splitting field $\Omega_K^{\mathcal{F}}$ of a family of polynomials $\mathcal{F} \subset K[X]$ over K as in Exercise 21.34.]

26. Determine the degree over $\mathbf{Q}$ of splitting fields of the following polynomials:

$$X^2 + X - 2, \qquad X^2 + 2X - 2, \qquad X^3 + 2X - 2, \qquad X^4 + 2X^2 + 2.$$

27. Define the normal closure of an infinite algebraic extension $K \subset L$, and show that this is uniquely determined up to L-isomorphism.

28. Let $\phi_1, \phi_2 : X(L/K) \xrightarrow{\sim} \mathrm{Aut}_K(L)$ be the identifications in (23.11) for choices $\tau_1, \tau_2 \in X(L/K)$. Show that $\phi_2 \cdot \phi_1^{-1} : \mathrm{Aut}_K(L) \to \mathrm{Aut}_K(L)$ is given by multiplication on the left by $\tau_2^{-1}\tau_1 \in \mathrm{Aut}_K(L)$.

29. Show that in a tower $K \subset L \subset M$ of finite separable extensions, the formulas $N_{L/K} \circ N_{M/L} = N_{M/K}$ and $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$ hold.

30. Define the trace map for a finite extension $K \subset L$ as in 23.18 by $\mathrm{Tr}_{L/K}(x) = \mathrm{trace}(M_x)$. Prove: $\mathrm{Tr}_{L/K} : L \to K$ is a surjective group homomorphism if $K \subset L$ is separable and the zero map if $K \subset L$ is inseparable.

31. Define the norm map for a finite extension $K \subset L$ as in 23.18 by $N_{L/K}(x) = \det(M_x)$. Let K_s be the separable closure of K in L and i the inseparable degree of L over K. Prove: for all $x \in L$, we have $x^i \in K_s$ and $N_{L/K}(x) = N_{K_s/K}(x^i)$.

32. An algebraic field extension $K \subset L$ is called *purely inseparable* if $\#X(L/K) = 1$, and an element $\alpha \in L$ is called purely inseparable over K if $K \subset K(\alpha)$ is purely inseparable. Make Exercises 10, 11, 12 with the word "separable" replaced by "purely inseparable" and "perfect" in 12.c replaced by "separably closed." Also show that in the purely inseparable case, there exists a *unique* K-isomorphism between any two purely inseparable closures of K.

33. Let $K \subset L$ be an algebraic field extension, K_s as in Exercise 11, and K_i the purely inseparable closure of K in L as in the previous exercise.

    a. Prove: $K_s \subset L$ is purely inseparable, and if L is normal over K, then $K_i \subset L$ is separable.
    b. Give an example in which $K_i \subset L$ is not separable.

34. For a field K, denote by $\bar{K}$, K^{sep}, and K^{pi}, respectively, an algebraic closure, a separable closure, and the purely inseparable closure of K. Prove: $\bar{K} \cong_K (K^{\mathrm{sep}})^{\mathrm{pi}} \cong_K (K^{\mathrm{pi}})^{\mathrm{sep}}$ for every K.

35. Let K be a field and $\bar{K}$ an algebraic closure of K.

    a. Let α, $\beta \in \bar{K}$ be such that β is separable over K. Write $f = f_K^{\alpha}$ and $g = f_K^{\beta}$. Moreover, let $\lambda \in K$ and $\vartheta = \alpha + \lambda\beta \in \bar{K}$, and let h be the gcd of $f(\vartheta - \lambda X)$ and g in $K(\vartheta)[X]$. Prove: the degree of h is equal to the number γ of zeros of g in $\bar{K}$ for which $\vartheta - \lambda\gamma$ is a zero of f.
    b. Suppose that $K \subset K(\alpha_1, \ldots, \alpha_t)$ is a finite field extension such that all α_i with the exception of at most one are separable over K. Prove: there is a primitive element for the extension $K \subset K(\alpha_1, \ldots, \alpha_t)$.

36. Let $K \subset L$ be a finite field extension. Prove: there is *no* primitive element for $K \subset L$ if and only if there exists a positive integer m with

$$[L : K] = m \cdot [L : K]_s \cdot \mathrm{char}(K)$$

    such that for every $\alpha \in L$, the element α^m is separable over K. Verify that this is true for the extension in Exercise 20.

37. Let K be a field and $a \in K$ an element.

    a. Let $n \in \mathbf{Z}_{>0}$, and suppose that L is a finite extension of K that contains an element α with $\alpha^n = a$. Prove: there is a $b \in K$ with $a^{[L:K]} = b^n$.
    [Hint: use the norm map.]
    b. Let p be a prime. Prove: $f = X^p - a \in K[X]$ is irreducible in $K[X]$ if and only if f has no zero in K.

38. Let K be a field, $a \in K$, and $n \in \mathbf{Z}_{>0}$. Denote by d the greatest common divisor of the degrees of all irreducible factors of $X^n - a$ in $K[X]$.

    a. Prove: d divides n, and there exists a $b \in K$ with $a^d = b^n$.
    b. Suppose that 1 is the only zero of $X^d - 1$ in K. Prove that $X^n - a$ has an irreducible factor of degree d in $K[X]$.

39. Let K be a field, p a prime for which K contains a primitive pth root of unity, $t \in \mathbf{Z}_{>0}$, and $a \in K$. Prove: the degree of any irreducible factor of $X^{p^t} - a$ in $K[X]$ is a divisor of p^t.

40. Let K, a, n, d be as in Exercise 38. Prove: $X^n - a$ has an irreducible factor of degree d in $K[X]$.
[Hint: first do the case where n is a prime power using the previous exercises.]

41. Let K be a field, $t \in \mathbf{Z}_{>1}$, and $a \in K$.

    a. Suppose that p is an odd prime. Prove: $X^{p^t} - a$ is irreducible in $K[X] \iff X^p - a$ is irreducible in $K[X] \iff$ there is no $b \in K$ with $a = b^p$.
    b. Prove: $X^{2^t} - a$ is irreducible in $K[X] \iff X^4 - a$ is irreducible in $K[X] \iff$ there is no $b \in K$ with $a = b^2$ or $a = -4b^4$.
    c. Let K be a field, n a positive number, and $a \in K$. Prove: $X^n - a$ is reducible in $K[X]$ if and only if there is an element $b \in K$ for which the following holds: either there is a prime factor p of n with $a = b^p$, or 4 divides n and $a = -4b^4$.
    [This is sometimes called *Capelli's theorem*, after the Italian mathematician Alfredo Capelli (1855–1910).]

24 Galois Theory

For a large class of field extensions $K \subset L$, we can easily describe the set of intermediate fields (and their inclusions) in terms of the group

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

of field automorphisms of L that are the identity on K. This observation, which goes back to Galois (1810–1831), allows us to use group theory to tackle problems for which this is not obvious at first glance.

▶ Galois Extensions

The fundamental idea of Galois theory is to use the automorphisms of a field L to identify the subfields of L. For every collection $G \subset \mathrm{Aut}(L)$ of automorphisms of L, there is a corresponding *field of invariants*

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

It is easy to check that this is a subfield of L. It contains the prime field of L, which allows no non-trivial automorphisms. Note that L^G does not change if we replace G with the subgroup $\langle G\rangle \subset \mathrm{Aut}(L)$ generated by G. We can therefore restrict ourselves to fields of invariants of *subgroups* $G \subset \mathrm{Aut}(L)$. This section treats the classic case where the automorphism group G is *finite*.

24.1. Definition. *A field extension $K \subset L$ is called finite Galois if there exists a finite subgroup $G \subset \mathrm{Aut}(L)$ of automorphisms of L with field of invariants $L^G = K$.*

In the situation of 24.1, we also say that $K \subset L$ is finite Galois with group G. The group G, which is uniquely determined by the extension $K \subset L$ and ensures that the extension $K \subset L$ is finite, as we will see in 24.4.1, is called the *Galois group* of L over K and is denoted by $\mathrm{Gal}(L/K)$.

Non-finite Galois extensions also exist; they are obtained by removing the word "finite" both times in 24.1 for *algebraic* field extensions $K \subset L$. It turns out that for infinite G, extensions $L^G \subset L$ are not automatically algebraic (Exercise 8), and even in the algebraic case, different infinite groups $G \subset \mathrm{Aut}(L)$ can lead to the same field of invariants (Exercise 56). A correct formulation of infinite Galois theory, as we give in §28, will therefore require some topology for Galois groups.

24.2. Example. Every quadratic extension $\mathbf{Q} \subset L = \mathbf{Q}(\sqrt{d})$ with $d \in \mathbf{Q}$ not a square is finite Galois. After all, define $\sigma \in \mathrm{Aut}(\mathbf{Q}(\sqrt{d}))$ by

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}.$$

Then the automorphism group $G = \langle\sigma\rangle$ is cyclic of order 2, and the field of invariants L^G is equal to the base field $\mathbf{Q}$.

More generally, splitting fields of separable polynomials lead to finite Galois extensions.

24.3. Lemma. *Let $K \subset L$ be a finite extension that is normal and separable. Then $K \subset L$ is finite Galois with group $G = \mathrm{Aut}_K(L)$.*

Proof. For a finite field extension $K \subset L$, the group $\mathrm{Aut}_K(L)$ is finite because L is generated over K by finitely many algebraic elements, which each have only finitely many possible images in L under any K-automorphism. It therefore suffices to show that $K = L^G$ holds for $G = \mathrm{Aut}_K(L)$.

The normality and separability of $K \subset L$ give the equality $\#G = \#\,\mathrm{Aut}_K(L) = \#X(L/K) = [L : K]_s = [L : K]$, so there are at least $[L : K]$ automorphisms of L over L^G. The inequality $[L : L^G] \geq [L : K]$ follows from 23.4, and from the inclusions $K \subset L^G \subset L$, we obtain $K = L^G$. □

Exercise 1. Prove the equality $L^G = K$ by giving, for $\alpha \in L \setminus K$, an automorphism $\sigma \in \mathrm{Aut}_K(L)$ with $\sigma(\alpha) \neq \alpha$.

▶ Fundamental Theorem

For a finite Galois extension $K \subset L$, there is the following *Galois correspondence* between subgroups of $\mathrm{Gal}(L/K)$ and intermediate fields of $K \subset L$.

24.4. Fundamental theorem. *Let $K \subset L$ be a finite Galois extension with Galois group G. Then the following statements hold:*

1. *The extension $K \subset L$ is finite, normal, and separable. The Galois group G has order $[L : K]$ and is equal to $G = \mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.*
2. *There is an inclusion-reversing bijection, the Galois correspondence*

$$\begin{array}{rccc} \psi_{L/K}: & \mathcal{T}_{L/K} = \{F : K \subset F \subset L\} & \xrightarrow{\sim} & \mathcal{H}_G = \{H : H \subset G = \mathrm{Aut}_K(L)\} \\ & F & \longmapsto & \mathrm{Aut}_F(L), \end{array}$$

   between the set $\mathcal{T}_{L/K}$ of intermediate fields of $K \subset L$ and the set $\mathcal{H}_G$ of subgroups of G. The inverse is $\psi^{-1}_{L/K} : H \mapsto L^H$.
3. *Let $H = \psi_{L/K}(F)$. Then the extension $F \subset L$ is Galois with group H; we have*

$$[L : F] = \#H \quad \text{and} \quad [F : K] = [G : H].$$

   For every $\sigma \in G$, under $\psi_{L/K}$, the field $\sigma[F] \in \mathcal{T}_{L/K}$ conjugate to F corresponds to the subgroup $\sigma H \sigma^{-1}$ conjugate to H.
4. *An intermediate field $F \in \mathcal{T}_{L/K}$ is normal over K if and only if the subgroup $H = \psi_{L/K}(F)$ is normal in G; for such F, the extension $K \subset F$ is Galois and*

$$\begin{array}{ccc} G/H & \xrightarrow{\sim} & \mathrm{Gal}(F/K) \\ \sigma H & \longmapsto & \sigma\big|_F \end{array}$$

   is a group isomorphism.

When we compare the statements in 24.3 and 24.4.1, we see how Galois extensions can be described in terms of Section 23.

24.5. Corollary. *For a field extension $K \subset L$, we have*

$$K \subset L \text{ is finite Galois} \iff K \subset L \text{ is finite, normal, and separable.} \qquad \square$$

Older proofs of 24.4 often take 24.5 as the *definition* of Galois and the equality for G in 24.4.1 as the definition of the Galois group. Using 23.9, we can then choose a primitive element x for L/K and view G as the permutation group on the zeros of $f = f_K^x$. In this approach, a Galois extension of K is seen as a splitting field $L = \Omega_K^f$ of an irreducible separable polynomial $f \in K[X]$. Our approach, which goes back to E. Artin, is somewhat different. It deduces the fundamental theorem from the Artin–Dedekind lemma from Section 23.

▶ Proof of the Fundamental Theorem

Let $K \subset L$ be a finite Galois extension with Galois group $G \subset \mathrm{Aut}_K(L)$, and view $\mathrm{Aut}_K(L)$ as a subset of $X_\Omega(L/K)$ by choosing a fixed inclusion $L \subset \Omega$. Then by 23.4, we have the inequalities

$$\#G \leq \#X_\Omega(L/K) = [L : K]_s \leq [L : K],$$

and the core of the proof consists of proving the reverse inequality $[L : K] \leq \#G$.

Let G have order n, and suppose that there are $m > n$ elements $\omega_1, \omega_2, \ldots, \omega_m \in L$ that are linearly independent over $K = L^G$. Then the m vectors $v_i = (\sigma(\omega_i))_{\sigma \in G} \in L^n$ for $i \in \{1, 2, \ldots, m\}$ are linearly dependent over L. Let $\sum_{i=1}^m c_i v_i = 0$ be a non-trivial relation with coefficients $c_i \in L$. For every $\sigma \in G$, we then have a relation $\sum_{i=1}^m c_i \sigma(\omega_i) = 0$. By applying σ^{-1} to this relation, we see that we have $\sum_{i=1}^m \sigma^{-1}(c_i)\omega_i = 0$ for every $\sigma \in G$. Taking the sum of these relations over all $\sigma \in G$, we obtain

$$\textstyle\sum_{i=1}^m b_i \omega_i = 0 \qquad \text{with} \quad b_i = \sum_{\sigma \in G} \sigma(c_i).$$

Note that as σ runs through G, the inverses σ^{-1} also do so. For a similar reason, the elements $b_i \in L$ are all contained in the field of invariants $K = L^G$. After all, for $\tau \in G$, the product $\tau\sigma$ runs through G as σ runs through G, and therefore for all $\tau \in G$, we have

$$\tau(b_i) = \textstyle\sum_{\sigma \in G} \tau\sigma(c_i) = \sum_{\sigma \in G} \sigma(c_i) = b_i.$$

Because the elements ω_i are linearly independent over K, it follows that we have $b_i = \sum_{\sigma \in G} \sigma(c_i) = 0$ for $i \in \{1, 2, \ldots, m\}$. However, any prescribed element $x \in L^*$ can occur as one of the coefficients c_i in the dependence relation above: choose an i with $c_i \neq 0$, and multiply the relation by xc_i^{-1}. We see that the map $L \to L$ given by $x \mapsto \sum_{\sigma \in G} \sigma(x)$ is the zero map. This is in contradiction with 23.15, so we have $[L : K] \leq \#G$.

We conclude that $K \subset L$ is finite of degree $\#G$ and that we have

$$G = \mathrm{Aut}_K(L) = X_\Omega(L/K).$$

The other statements in 24.4.1 now immediately follow. After all, the first equality shows that G is of the stated form. The second equality $\mathrm{Aut}_K(L) = X_\Omega(L/K)$ expresses that all embeddings of L in $\overline{K}$ have the same image, so that $K \subset L$ is a normal extension. Since $X_\Omega(L/K)$ has cardinality $\#G = [L : K]$, the extension $K \subset L$ is moreover separable.

Now that we have proved the fundamental property 24.4.1 of Galois extensions, the remainder of the proof of the fundamental theorem 24.4 is a fairly simple verification. If H is a subgroup of G, then L^H is an intermediate field of $K \subset L$, and $L^H \subset L$ is by definition finite Galois. It follows from 24.4.1 that $\psi_{L/K}(L^H) = \mathrm{Aut}_{L^H}(L)$ is equal to H, so the map

$$\begin{array}{ccccc} \mathcal{H}_G & \longrightarrow & \mathcal{T}_{L/K} & \overset{\psi_{L/K}}{\longrightarrow} & \mathcal{H}_G \\ H & \longmapsto & L^H & \longmapsto & \mathrm{Aut}_{L^H}(L) \end{array}$$

is the identity on $\mathcal{H}_G$. Conversely, for every intermediate field F of $K \subset L$, the finite extension $F \subset L$ is separable and normal, hence Galois with group $H = \mathrm{Aut}_F(L)$ of order $\#H = [L : F]$. The equality $L^H = F$ says exactly that the map

$$\begin{array}{ccccc} \mathcal{T}_{L/K} & \overset{\psi_{L/K}}{\longrightarrow} & \mathcal{H}_G & \longrightarrow & \mathcal{T}_{L/K} \\ F & \longmapsto & \mathrm{Aut}_F(L);\ H & \longmapsto & L^H \end{array}$$

is the identity on $\mathcal{T}_{L/K}$. It is clear that $\psi_{L/K}$ and $\psi_{L/K}^{-1}$ reverse inclusions. This proves 24.4.2.

For $H = \psi_{L/K}(F)$, by dividing the order $\#G = [L : K]$ by $\#H = [L : F]$, we obtain the relation $[G : H] = [F : K]$. For $\sigma \in G$, the field isomorphism $F \xrightarrow{\sim} \sigma[F] \subset L$ leads to a group isomorphism $\mathrm{Aut}_F(L) \xrightarrow{\sim} \mathrm{Aut}_{\sigma[F]}(L)$ given by $\tau \mapsto \sigma\tau\sigma^{-1}$: a simple verification. In particular, we see that $\sigma[F]$ corresponds to the conjugate subgroup $\sigma H \sigma^{-1}$. This proves 24.4.3.

Since the restriction map $G = X_\Omega(L/K) \to X_\Omega(F/K)$ is surjective, it follows that all embeddings $F \to \Omega$ have the same image if and only if $\sigma[F] = F$ holds for all $\sigma \in G$. This means that $\sigma H \sigma^{-1} = H$ holds for the corresponding subgroup $H \subset G$, so we see that $K \subset F$ is normal if and only if $H = \psi_{L/K}(F)$ is normal in G. If the extension $K \subset F$ is normal, then it is also Galois because every intermediate field is automatically separable over K. In this case, the surjection $X_\Omega(L/K) \to X_\Omega(F/K)$ leads to a surjective group homomorphism $G \to \mathrm{Gal}(F/K)$ given by $\sigma \mapsto \sigma\big|_F$. This map's kernel is H, so the isomorphism theorem gives a group isomorphism $G/H \xrightarrow{\sim} \mathrm{Gal}(F/K)$. This proves 24.4.4 and concludes the proof. □

▶ Galois Group of a Polynomial

The fundamental theorem tells us that to every finite extension $K \subset L$ that is normal and separable, a finite group $\mathrm{Gal}(L/K)$ is intrinsically attached. Properties of the group "are" properties of the extension, and a Galois extension is therefore called abelian (cyclic, solvable, ...) for short if the corresponding Galois group has this property.

By 23.14, a finite Galois extension L of K can be viewed as a splitting field Ω_K^f of a separable polynomial $f \in K[X]$, which can be chosen irreducible by 23.9.

Consequently, the Galois group $G = \mathrm{Gal}(L/K)$ is sometimes called the Galois group $\mathrm{Gal}(f)$ of the *polynomial* $f \in K[X]$ over K. Because every element $\sigma \in G$ is fixed by its action on the zeros of f in $L = \Omega_K^f$, this gives a description of G as a permutation group on the zeros of f. If f has degree n, we can thus view $\mathrm{Gal}(f)$ as a subgroup of the permutation group S_n on n elements. Since a given extension $K \subset L$ can generally be viewed as a splitting field of numerous different polynomials, this representation is hardly canonical. For example, the quadratic extension $\mathbf{F}_3 \subset \mathbf{F}_9$ as in 22.1 can be viewed as a splitting field of the separable polynomial $X^9 - X \in \mathbf{F}_3[X]$. However, smaller polynomials in $\mathbf{F}_3[X]$ such as $X^2 + 1$ and $X^2 - X - 1$ give the same splitting field.

Exercise 2. Describe the embeddings $\mathrm{Gal}(f) \subset S_2$ and $\mathrm{Gal}(f) \subset S_9$ for $f = X^2 - X - 1$ and $f = X^9 - X \in \mathbf{F}_3[X]$.

The task of determining the Galois group $\mathrm{Gal}(f)$ over K of a separable polynomial $f \in K[X]$ is not easy, and even already non-trivial in the special case $K = \mathbf{Q}$. The conjecture that for the base field $K = \mathbf{Q}$, *every* finite group occurs as the Galois group of a polynomial $f \in \mathbf{Q}[X]$ remains unproven: this is the *inverse problem*[6] of Galois theory.

An important step in determining $\mathrm{Gal}(f)$ is determining the degree of the field Ω_K^f obtained through the adjunction of the zeros of f to K. This degree is equal to the order of $G = \mathrm{Gal}(L/K)$. Through its action on the zeros of f, the group G can be viewed as a finite permutation group. In the fundamental case where f is irreducible of degree n, not all subgroups of S_n occur as Galois groups.

24.6. Theorem. *Let $f \in K[X]$ be an irreducible separable polynomial with zeros $\alpha_1, \alpha_2, \ldots, \alpha_n \in \overline{K}$, and view $G = \mathrm{Gal}(f) = \mathrm{Gal}(K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K)$ as a subgroup of S_n through its action on the zeros of f. Then G is a transitive subgroup of S_n, and $\#G$ is a divisor of $n!$ that is divisible by n.*

Proof. Since f is irreducible, there exists, for any $i, j \in \{1, 2, \ldots, n\}$, an isomorphism $\varphi : K(\alpha_i) \xrightarrow{\sim} K(\alpha_j)$ that sends α_i to α_j. When we apply 21.17 to this isomorphism with $f_1 = f_2 = f$, we see that φ can be extended to an automorphism σ of $L = \Omega_K^f = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. We have $\sigma(\alpha_i) = \alpha_j$, so G acts transitively on the zeros of f. The stabilizer of α_1 in G has index n in G by 5.3. It follows that the order of G, which is a divisor of $\#S_n = n!$, is divisible by n. □

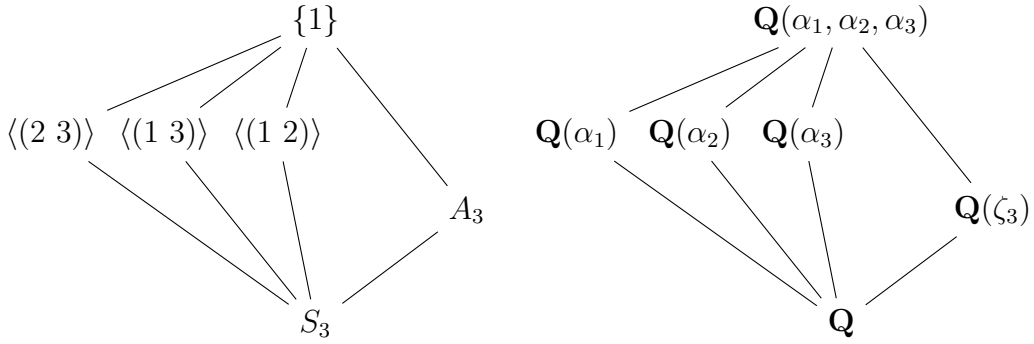
Exercise 3. Prove that $\mathrm{Gal}(f)$ acts transitively on the zeros of a separable polynomial $f \in K[X]$ if and only if f is irreducible.

In view of 24.6, it is interesting to determine, for given n, which (isomorphism types of) transitive subgroups S_n has. For $n \leq 5$, this is not too much work (Exercises 43 and 44); for somewhat larger n, lists can be used made by certain computer algebra packages[7]. However, the complexity of the problem increases rapidly with n.

▶ Two Examples

Let us determine the Galois groups of the polynomials X^3-2 and X^4-2 in $\mathbf{Q}[X]$, in part to illustrate the statement of the fundamental theorem, w

For $f=X^3-2$, we constructed a splitting field $L=\Omega_{\mathbf{Q}}^{X^3-2}$ in two different ways in 21.15. We can view L as a subfield of $\mathbf{C}$ by taking a real third root $\sqrt[3]{2}$ and a primitive third root of unity $\zeta_3\in\mathbf{C}$: we then have $L=\mathbf{Q}(\zeta_3,\sqrt[3]{2})$, and X^3-2 has zeros $\alpha_1=\sqrt[3]{2}$, $\alpha_2=\zeta_3\sqrt[3]{2}$, and $\alpha_3=\zeta_3^2\sqrt[3]{2}$. Through its action on the zeros of f, the Galois group $\mathrm{Gal}(f)=\mathrm{Gal}(L/\mathbf{Q})$ is a subgroup of S_3. We already found $[L:\mathbf{Q}]=6$ in 21.15, so we have $\#\,\mathrm{Gal}(f)=6$ and $\mathrm{Gal}(L/\mathbf{Q})\cong S_3$. The *lattice* of subgroups of S_3 is not difficult to find; it corresponds to the lattice of intermediate fields of $\mathbf{Q}\subset L$ given below. Note that the inclusion in the left and right diagrams go in opposite directions.



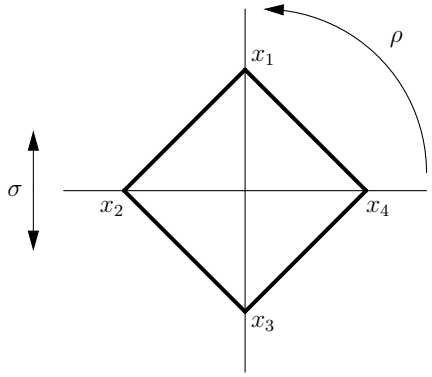
We see that there are no other intermediate fields than the "obvious" ones. The three non-normal extensions $\mathbf{Q}\subset\mathbf{Q}(\alpha_i)$ correspond to the non-normal subgroups of order 2 in S_3. The isomorphic fields $\mathbf{Q}(\alpha_i)$ are conjugate over $\mathbf{Q}$; the subgroups of order 2 are conjugate in S_3. The quadratic field $\mathbf{Q}(\zeta_3)$, which is normal over $\mathbf{Q}$, corresponds to the normal subgroup $A_3\lhd S_3$. The extension $\mathbf{Q}\subset\mathbf{Q}(\zeta_3)$ is Galois, and $\mathrm{Gal}(\mathbf{Q}(\zeta_3)/\mathbf{Q})\cong S_3/A_3$ is cyclic of order 2.

Exercise 4. Prove: for every irreducible polynomial $f=X^3-k\in\mathbf{Q}[X]$, we have $\mathrm{Gal}(f)\cong S_3$.

Next, we determine the subgroup $G\subset S_4$ that occurs as the Galois group of the irreducible polynomial $f=X^4-2\in\mathbf{Q}[X]$ over $\mathbf{Q}$. As in the previous case, we can use the zeros of f in $\mathbf{C}$. If $x=\sqrt[4]{2}$ is the positive real fourth root of 2, then we obtain the other zeros of f by multiplying x by the powers of $i=\sqrt{-1}$. Setting $x_k=i^kx$ for $k\in\mathbf{Z}$, we have $\Omega_{\mathbf{Q}}^f=\mathbf{Q}(x_1,x_2,x_3,x_4)=\mathbf{Q}(x,i)$, where $x=x_4=\sqrt[4]{2}$ is as above. This is an extension of degree 8 because $i=\sqrt{-1}$ is not contained in the real field $\mathbf{Q}(x)$. The group $\mathrm{Gal}(f)$ is apparently a subgroup of S_4 of order 8. Hence, not all permutations of the zeros of f are realized by automorphisms $L=\Omega_{\mathbf{Q}}^f$. Because of the equalities $x_3=-x_1$ and $x_4=-x_2$, this is not surprising.

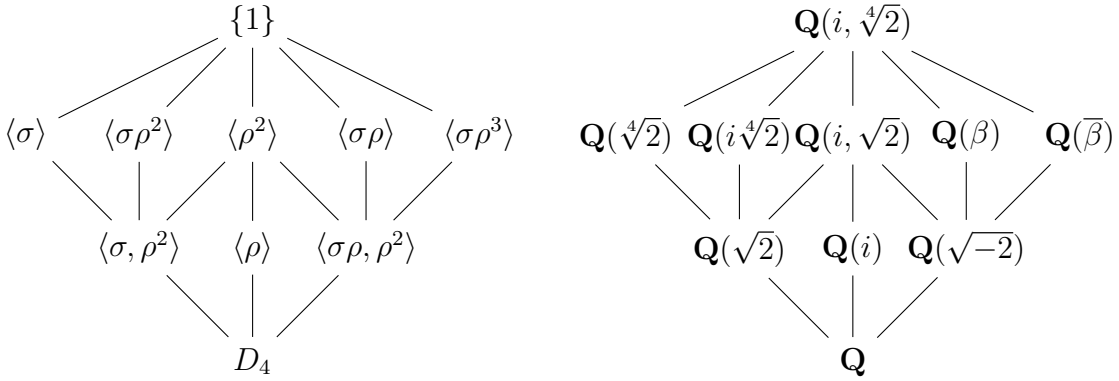
Recall from 10.11 that the subgroups of S_4 of order 8 are the 2-Sylow subgroups and that they are isomorphic to the dihedral group D_4. The isomorphism $\mathrm{Gal}(L/\mathbf{Q})\cong D_4$ can also be discovered by letting σ be the complex conjugation on L and $\rho:L\to L$ an automorphism that satisfies $\rho(x_1)=x_2=ix_1$. By replacing ρ with $\sigma\rho$ if necessary, we may assume that we have $\rho(i)=i$ and therefore $\rho(x_k)=x_{k+1}$. The action of ρ and σ on the zeros of f, drawn in the complex plane as the vertices of a square, is then,

respectively, the quarter turn and the reflection in the real axis. Do note that ρ does not act on $\mathbf{Q}(x_1, x_2, x_3, x_4) \subset \mathbf{C}$ as a quarter turn!



We already know from 1.4 that the quarter turn ρ and the reflection σ generate the group D_4. This knowledge is also useful in making the lattice of subgroups of D_4. The central element ρ^2 and the four reflections $\sigma\rho^k$ each generate a subgroup of order 2. The subgroups of D_4 of order 4 are the subgroups generated by ρ^2 and a reflection—these are isomorphic to the Klein four-group V_4—and the unique cyclic subgroup $\langle\rho\rangle$ of order 4.

We obtain intermediate fields corresponding to the various subgroups of $\mathrm{Gal}(L/\mathbf{Q}) \cong D_4$ by writing down the obvious subfields and—if these are not all intermediate fields—constructing invariant elements in terms of the x_k.



Subfields of degree 4 are $\mathbf{Q}(x_4) = \mathbf{Q}(x_2) = \mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(x_3) = \mathbf{Q}(x_1) = \mathbf{Q}(i\sqrt[4]{2})$. The non-trivial symmetries of order 2 that fix the corresponding vertices of the square are the complex conjugation σ and the automorphism $\sigma\rho^2$ that fixes x_1 and x_3. The field $\mathbf{Q}(\sqrt{2})$ generated by the square of a zero of f is invariant under both these symmetries: it is the intersection of $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(i\sqrt[4]{2})$ and corresponds to the subgroup of D_4 generated by σ and ρ^2.

The field $\mathbf{Q}(i)$ is invariant under ρ, hence corresponds to the subgroup $\langle\rho\rangle$ of order 4. The *compositum* $\mathbf{Q}(i, \sqrt{2})$ of the subfields $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{2})$ corresponds to the intersection $\langle\rho^2\rangle$ of the subgroups $\langle\rho\rangle$ and $\langle\sigma, \rho^2\rangle$. This field contains the subfield $\mathbf{Q}(\sqrt{-2})$, and since x_1x_4 is a square root of -2, it is not difficult to see that ρ^2 and the reflections $\sigma\rho$ and $\sigma\rho^3$ leave this field invariant.

It turns out that we are still missing two fields of degree 4, corresponding to the groups generated by each of the two reflections we just mentioned. Since $\sigma\rho$ exchanges

the elements x_1 and x_2, the sum $\beta = x_1 + x_2 = (-1+i)\sqrt[4]{2}$ is an element of the corresponding field of invariants. We have $\beta^2 = -2\sqrt{-2}$, so $\mathbf{Q}(\beta)$ contains $\mathbf{Q}(\sqrt{-2})$. Because of $\rho^2(\beta) = -\beta$, the element β is not in $\mathbf{Q}(\sqrt{-2})$, so $\mathbf{Q}(\beta)$ is the field of degree 4 corresponding to $\langle\sigma\rho\rangle$. Conjugation with σ sends the subgroup $\langle\sigma\rho\rangle$ to $\langle\sigma\rho^3\rangle$. The field corresponding to $\langle\sigma\rho^3\rangle$ is therefore the field $\sigma[\mathbf{Q}(\beta)] = \mathbf{Q}(\overline{\beta})$ generated by the complex conjugate $\overline{\beta} = (-1-i)\sqrt[4]{2}$ of β. We have $f_{\mathbf{Q}}^{\beta} = X^4 + 8$.

The reader may determine, as an exercise, which intermediate fields of $\mathbf{Q} \subset L$ are normal over $\mathbf{Q}$ and what the corresponding Galois groups are.

▶ Cyclic Extensions

A finite Galois extension $K \subset L$ is called *cyclic* if $\mathrm{Gal}(L/K)$ is a cyclic group. For cyclic groups, the lattice of subgroups is very easy to describe. After all, if $G = \langle x\rangle$ is a cyclic group of order n with generator x, then for every divisor $d \mid n$, the subgroup $\langle x^d\rangle \subset G$ has index d in G. Conversely, every subgroup $H \subset G$ of index $d \mid n$ contains the element x^d; after all, x^d mod H is the unit element in G/H, so we have $H = \langle x^d\rangle$. We conclude that for every divisor $d \mid n$, the group G has a unique subgroup $H_d \subset G$ of index d. The corresponding quotient group G/H_d is also cyclic and of order d.

Exercise 5. Is, conversely, every group of order n that has a unique subgroup of order d for every divisor $d \mid n$ a cyclic group?

For cyclic field extensions, we obtain the following result.

24.7. Theorem. *Let $K \subset L$ be a cyclic Galois extension of degree n. Then for every divisor $d \mid n$, there is a unique intermediate field K_d of $K \subset L$ of degree d over K. The extension $K \subset K_d$ is cyclic of degree d.* □

24.8. Example. Every extension $K \subset L$ of finite fields is cyclic, and in this special case, we already proved the Galois correspondence in 22.12. If we write $K = \mathbf{F}_q$ and $L = \mathbf{F}_{q^n}$, then we have

$$\mathrm{Gal}(L/K) = \langle F_K\rangle \cong \mathbf{Z}/n\mathbf{Z}$$

with $F_K : L \to L$ the *Frobenius automorphism* associated with the base field $K = \mathbf{F}_q$, defined by $F_K(x) = x^q$. For every divisor d of the degree $n = [L : K]$ of the extension, $K_d = \mathbf{F}_{q^d}$ is the intermediate field of degree d over K. It corresponds to the subgroup $\langle F_K^d\rangle$ of index d in $\mathrm{Gal}(L/K)$.

Over $\mathbf{Q}$, the pth cyclotomic field defined in 21.8.3 is an example of a cyclic extension.

24.9. Theorem. *Let p be a prime and $\zeta_p \in \overline{\mathbf{Q}}$ a zero of Φ_p. Then we have the following:*

1. *For every element $k \in (\mathbf{Z}/p\mathbf{Z})^*$, there is an automorphism $\sigma_k \in \mathrm{Aut}(\mathbf{Q}(\zeta_p))$ with $\sigma_k(\zeta_p) = \zeta_p^k$, and the map*

$$\begin{aligned} \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) &\xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^* \\ \left[\sigma_k : \zeta_p \mapsto \zeta_p^k\right] &\longmapsto (k \bmod p) \end{aligned}$$

is an isomorphism of cyclic groups of order $p-1$.

2. *For every divisor $d \mid p-1$, there is a unique subfield $K_d \subset \mathbf{Q}(\zeta_p)$ with $[K_d : \mathbf{Q}] = d$. If $H_d \subset (\mathbf{Z}/p\mathbf{Z})^*$ is the subgroup of index d in $(\mathbf{Z}/p\mathbf{Z})^*$, then we have $K_d = \mathbf{Q}(\eta_d)$ with*

$$\eta_d = \sum_{k \in H_d} \zeta_p^k.$$

The element η_d in 24.9.2 is called the *Gaussian period of degree d* in $\mathbf{Q}(\zeta_p)$. The *number* of terms of η_d is $\frac{p-1}{d}$.

Proof. The field $\mathbf{Q}(\zeta_p)$, as a splitting field of the irreducible polynomial Φ_p, is a finite Galois extension of $\mathbf{Q}$. Every automorphism $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ is fixed by its action on the *group* $\mu_p = \langle \zeta_p \rangle$ of pth roots of unity. Since the automorphisms of μ_p are the kth power maps $\sigma_k : \zeta_p \mapsto \zeta_p^k$ with $p \nmid k$, this leads to an injective homomorphism

$$\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \longrightarrow \mathrm{Aut}(\mu_p) = (\mathbf{Z}/p\mathbf{Z})^*.$$

By 24.6, all possible k mod p are realized by elements of $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$, so this map is an isomorphism. We know from 7.7 and 12.5 that $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic.

The first statement in part 2 is a special case of 24.7. To show that the Gaussian period η_d associated with the subgroup $H_d \subset (\mathbf{Z}/p\mathbf{Z})^*$ of index d generates the field of invariants $K_d = \mathbf{Q}(\zeta_p)^{H_d}$, we observe that the element σ_a acts on η_d by

$$\sigma_a(\eta_d) = \textstyle\sum_{k \in H_d} \zeta_p^{ak} = \sum_{k \in aH_d} \zeta_p^k.$$

For $a \in H_d$, we have $aH_d = H_d$ and $\sigma_a(\eta_d) = \eta_d$, so we have $\eta_d \in K_d$. The elements ζ_p^k for $k \in \{1, 2, \ldots, p-1\}$ are linearly independent over $\mathbf{Q}$—after all, they form a basis for $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$—so the elements $\sigma_a(\eta_d)$ associated with different rest classes aH_d are also different. This shows that η_d has exactly $d = [(\mathbf{Z}/p\mathbf{Z})^* : H_d]$ conjugates in $\mathbf{Q}(\zeta_p)$. The field $\mathbf{Q}(\eta_d)$ is therefore of degree d over $\mathbf{Q}$, and we find $\mathbf{Q}(\eta_d) = K_d$. □

The proof of 24.9 uses the fact that $\mathbf{Q}(\zeta_p)$ has a $\mathbf{Q}$-basis that consists of the conjugates of the element ζ_p. More generally, we call a K-basis for a Galois extension $K \subset L$ consisting of the set $\{\sigma(x)\}_{\sigma \in \mathrm{Gal}(L/K)}$ of conjugates of an element $x \in L$ a *normal basis* for L over K.

24.10. Example. For $p = 7$, we have $p - 1 = 6$, so the non-trivial subfields of $\mathbf{Q}(\zeta_7)$ have degree 2 and 3 over $\mathbf{Q}$. The corresponding subgroups of index 2 and 3 in $(\mathbf{Z}/7\mathbf{Z})^*$ are $H_2 = \langle \overline{2} \rangle = \{\overline{1}, \overline{2}, \overline{4}\}$ and $H_3 = \langle -\overline{1} \rangle$. For $\zeta = \zeta_7$, we obtain $\eta_2 = \zeta + \zeta^2 + \zeta^4$ and $\eta_3 = \zeta + \zeta^{-1}$ as generators of $K_2 = \mathbf{Q}(\eta_2)$ and $K_3 = \mathbf{Q}(\eta_3)$. The quadratic period η_2 has a conjugate $\sigma_{-1}(\eta_2) = \zeta^{-1} + \zeta^{-2} + \zeta^{-4} = \zeta^6 + \zeta^5 + \zeta^3$, and a short calculation gives the polynomial

$$f_{\mathbf{Q}}^{\eta_2} = (X - \eta_2)(X - \sigma_{-1}(\eta_2)) = X^2 + X + 2$$

with zeros $-\frac{1}{2} \pm \frac{1}{2}\sqrt{-7}$. We find $K_2 = \mathbf{Q}(\sqrt{-7})$.

The cubic Gaussian period $\eta_3 = \zeta + \zeta^{-1}$ has conjugates $\sigma_2(\eta_3) = \zeta^2 + \zeta^{-2}$ and $\sigma_3(\eta_3) = \zeta^3 + \zeta^{-3}$. Multiplying out the brackets gives

$$f_{\mathbf{Q}}^{\eta_3} = (X - \eta_3)(X - \sigma_2(\eta_3))(X - \sigma_3(\eta_3)) = X^3 + X^2 - 2X - 1.$$

Exercise 6. Show that, in addition to η_3, the polynomial $f_{\mathbf{Q}}^{\eta_3}$ has the zeros $\eta_3^2 - 2$ and $-\eta_3^2 - \eta_3 + 1$.

There is a general description of the quadratic subfield $\mathbf{Q}(\eta_2) \subset \mathbf{Q}(\zeta_p)$ generated by the quadratic Gaussian period.

24.11. Theorem. *Let p be an odd prime and η_2 the quadratic Gaussian period in $\mathbf{Q}(\zeta_p)$. Then we have*

$$f_{\mathbf{Q}}^{\eta_2} = X^2 + X + \frac{1 - p^*}{4} \qquad \text{with } p^* = (-1)^{(p-1)/2} p.$$

In particular, we have $\mathbf{Q}(\eta_2) = \mathbf{Q}(\sqrt{p^*})$.

Proof. Let $S \subset (\mathbf{Z}/p\mathbf{Z})^*$ be the subgroup of squares in $(\mathbf{Z}/p\mathbf{Z})^*$, and write $T = (\mathbf{Z}/p\mathbf{Z})^* \setminus S$. Then $\eta_2 = \sum_{s \in S} \zeta_p^s$ and $\widetilde{\eta}_2 = \sum_{t \in T} \zeta_p^t$ are the zeros of $f_{\mathbf{Q}}^{\eta_2}$.

Because of the equality $\eta_2 + \widetilde{\eta}_2 = \sum_{i=1}^{p-1} \zeta_p^i = -1$, the linear coefficient of $f_{\mathbf{Q}}^{\eta_2}$ is equal to 1. The constant coefficient $\eta_2 \widetilde{\eta}_2 = \sum_{s \in S, t \in T} \zeta_p^{s+t}$ is a sum of $\#S \cdot \#T = (\frac{p-1}{2})^2$ roots of unity.

For $p \equiv 1 \bmod 4$, we observe, as in the proof of 12.20, that we have $-1 \in S$; hence, along with $s \in S$, we also have $-s \in S$. For $s \in S$ and $t \in T$, we then have $s + t \neq 0$, so $\eta_2 \widetilde{\eta}_2$ is a sum of $(\frac{p-1}{2})^2$ conjugates of ζ_p. These conjugates form a basis of $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$. Because $\eta_2 \widetilde{\eta}_2$ is rational and therefore invariant under the action of the Galois group, this means that each of the $p - 1$ different roots of unity occur *equally often* in the sum: $\frac{p-1}{4}$ times. We find

$$\eta_2 \widetilde{\eta}_2 = \tfrac{p-1}{4} \cdot \left(\sum_{i=1}^{p-1} \zeta_p^i \right) = \tfrac{p-1}{4} \cdot (-1) = \tfrac{1-p}{4}.$$

Now, suppose $p \equiv -1 \bmod 4$. Then we have $-1 \notin S$, so for every $s \in S$, there is a unique element $t = -s \in T$ with $s + t = 0$. This leads to $\#S = \frac{p-1}{2}$ terms $\zeta_p^0 = 1$ in the sum for $\eta_2 \widetilde{\eta}_2$. The remaining $(\frac{p-1}{2})^2 - \frac{p-1}{2} = (p-1) \cdot \frac{p-3}{4}$ roots of unity in the sum are conjugates of ζ_p and add up to a rationale sum. As above, we conclude that each of the $p - 1$ roots of unity occurs $\frac{p-3}{4}$ times. This gives

$$\eta_2 \widetilde{\eta}_2 = \tfrac{p-1}{2} + \tfrac{p-3}{4} \cdot (-1) = \tfrac{1+p}{4}.$$

Since $f_{\mathbf{Q}}^{\eta_2}$ has zeros $-\frac{1}{2} \pm \frac{1}{2}\sqrt{p^*}$, the equality $\mathbf{Q}(\eta_2) = \mathbf{Q}(\sqrt{p^*})$ is clear. □

The element $\tau_p = \eta_2 - \widetilde{\eta}_2$ is the quadratic *Gauss sum* in $\mathbf{Q}(\zeta_p)$. The proof of 24.11 shows that τ_p is a square root of $p^* = \pm p \equiv 1 \bmod 4$.

▶ Cyclotomic Extensions

Let us see what Theorem 24.9 looks like for the extension $\mathbf{Q} \subset \mathbf{Q}(\zeta)$ obtained through the adjunction of an arbitrary root of unity to $\mathbf{Q}$ or to another base field. Such extensions, which occur frequently, are called *cyclotomic extensions*.

For a field K, the torsion subgroup $\mu_K \subset K^*$ of K^* is called the group of *roots of unity* in K. This group consists of the elements $x \in K$ for which $x^n = 1$ holds for

some $n \in \mathbf{Z}_{\geq 1}$. We have $\mu_{\mathbf{Q}} = \mu_{\mathbf{R}} = \{\pm 1\}$ and $\mu_K = K^*$ for every finite field K. An element $x \in \mu_K$ is called an nth root of unity if $x^n = 1$ holds and a *primitive* nth root of unity if the order of x in K^* is equal to n.

In a field K of characteristic $p > 0$, there are no primitive pth roots of unity because $X^p - 1$ then decomposes as $(X-1)^p$ in $K[X]$. We therefore assume that $n \geq 1$ is not divisible by the characteristic of K. This is, in particular, the case for $\mathrm{char}(K) = 0$. The polynomial $f = X^n - 1 \in K[X]$ is then a separable polynomial because the derivative $f' = nX^{n-1}$ has no common zeros with f in an algebraic closure $\overline{K}$. It follows that the n different zeros of $X^n - 1$ in $\overline{K}$ form a subgroup $\mu_n \subset \overline{K}^*$ of order n. By 12.4, this group is cyclic. Since every cyclic group of order n has exactly $\varphi(n)$ generators, with φ Euler's φ-function, there are $\varphi(n)$ primitive nth roots of unity in $\overline{K}$.

In the case $\mathrm{char}(K) = 0$, the nth roots of unity lie in $\overline{\mathbf{Q}}$, and we can visualize μ_n in $\overline{\mathbf{Q}} \subset \mathbf{C}$ as the set of n points in the complex plane that divide the complex unit circle $T = \{z \in \mathbf{C} : |z| = 1\}$ into n equal parts, starting at the point $z = 1$. This explains the word *cyclotomy*, which is Greek for circle division. In $\mathbf{C}$, the number $\zeta_n = \exp(2\pi i/n) = \cos(2\pi/n) + i\sin(2\pi/n)$ is a primitive nth root of unity, and the nth cyclotomic polynomial is defined by

$$\Phi_n = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^*} (X - \zeta_n^k).$$

The zeros of Φ_n in $\mathbf{C}$ are the $\varphi(n)$ primitive nth roots of unity. For $n = p$ a prime, we have $X^p - 1 = (X-1)\Phi_p$, so this definition agrees with that in 13.9. More generally, we can group the zeros of $X^n - 1$ in $\mathbf{C}$ according to their exact order $d \mid n$. This gives the following product relation in $\mathbf{C}[X]$:

$$\prod_{d \mid n} \Phi_d = X^n - 1. \tag{24.12}$$

This can be used to calculate the polynomials Φ_n inductively. For example, by applying (24.12) successively to the divisors of 6, we find

$$\begin{aligned}
\Phi_1 &= X - 1; \\
\Phi_1 \cdot \Phi_2 &= X^2 - 1, \quad \text{so} \quad \Phi_2 = X + 1; \\
\Phi_1 \cdot \Phi_3 &= X^3 - 1, \quad \text{so} \quad \Phi_3 = X^2 + X + 1; \\
\Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_6 &= X^6 - 1, \quad \text{so} \quad \Phi_6 = (X^6 - 1)/(\Phi_1 \cdot \Phi_2 \cdot \Phi_3) = X^2 - X + 1.
\end{aligned}$$

The Möbius inversion formula 22.9 applied with the multiplicative group $\mathbf{C}(X)^*$ in the role of the additive group $\mathbf{C}$ gives the identity

$$\Phi_n = \textstyle\prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)}.$$

However, to calculate Φ_n, it is better to use the formulas in Exercise 30.

24.13. Lemma. *For all $n \geq 1$, the nth cyclotomic polynomial Φ_n is a monic polynomial in $\mathbf{Z}[X]$.*

Proof. It is clear that Φ_n is monic. By induction on n, it follows from (24.12) that Φ_n is the quotient of the monic polynomials $X^n - 1$ and $\prod_{d|n, d\neq n} \Phi_d \in \mathbf{Z}[X]$. By 12.1, or alternatively by the Gauss lemma 13.5, this quotient is an element of $\mathbf{Z}[X]$. □

We are going to prove that Φ_n is irreducible in $\mathbf{Q}[X]$ for all n, so that (24.12) gives the factorization of $X^n - 1$ in $\mathbf{Q}[X]$. For this, it suffices to show that the nth cyclotomic field $\mathbf{Q}(\mu_n) = \mathbf{Q}(\zeta_n)$ obtained by adjoining a zero ζ_n of Φ_n to $\mathbf{Q}$ has degree $\deg(\Phi_n) = \varphi(n)$.

For every field K whose characteristic does not divide n, the splitting field $K(\mu_n) = K(\zeta_n)$ of $X^n - 1$ over K is a Galois extension of K, and we can view the elements of $\mathrm{Gal}(K(\mu_n)/K)$ as automorphisms of the group $\mu_n = \langle \zeta_n \rangle$ of nth roots of unity. The automorphisms of μ_n are the kth power maps $\sigma_k : \zeta_n \mapsto \zeta_n^k$ with $\gcd(k, n) = 1$, and as in 24.9, this leads to an injective group homomorphism

$$\mathrm{Gal}(K(\mu_n)/K) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^*.$$

The irreducibility of Φ_n in $\mathbf{Q}[X]$ boils down to the statement that for $K = \mathbf{Q}$, this injection is an *isomorphism*.

24.14. Theorem. *The Galois group of the nth cyclotomic field $\mathbf{Q}(\mu_n) = \mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$ is described by the group isomorphism*

$$\begin{aligned} \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) &\xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^* \\ \left[\sigma_k : \zeta_n \mapsto \zeta_n^k\right] &\longmapsto (k \bmod n). \end{aligned}$$

In particular, $\mathbf{Q}(\zeta_n)$ has degree $\varphi(n)$ over $\mathbf{Q}$, and Φ_n is the minimum polynomial of ζ_n over $\mathbf{Q}$.

Proof. We only need to show that the given homomorphism is *surjective*; we do this by showing that for every prime $p \nmid n$, the extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_n)$ admits a *field* automorphism $\sigma_p : \zeta_n \mapsto \zeta_n^p$. Let f be the minimum polynomial of ζ_n over $\mathbf{Q}$ and g the minimum polynomial of ζ_n^p over $\mathbf{Q}$. Then f and g are irreducible divisors of $X^n - 1$ in $\mathbf{Q}[X]$, and by the Gauss lemma 13.5, they have integer coefficients. Since ζ_n is a zero of $g(X^p)$, the polynomial f is also a divisor of $g(X^p) \in \mathbf{Z}[X]$. If we consider this divisibility modulo p, we see that $\overline{f} = f \bmod p$ is a divisor of $\overline{g}(X^p) = \overline{g}(X)^p \in \mathbf{F}_p[X]$. It follows that f and g are *equal* in $\mathbf{Q}[X]$. After all, if this is not the case, then f and g are different irreducible factors of $X^n - 1$ in $\mathbf{Q}[X]$ and fg is also a divisor of $X^n - 1$. However, modulo p, the polynomial $X^n - 1$ is *separable* in $\mathbf{F}_p[X]$: because of $p \nmid n$, the derivative nX^{n-1} is relatively prime to $X^n - 1$. The factors $\overline{f} = f \bmod p$ and $\overline{g} = g \bmod p$ are therefore relatively prime in $\mathbf{F}_p[X]$, This contradicts the divisibility relation $\overline{f} \mid \overline{g}^p$ we just proved.

Now that we know that for all primes $p \nmid n$, the power ζ_n^p is also a zero of $f = f_{\mathbf{Q}}^{\zeta_n}$, it follows from 24.6 that for such p, the group $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ contains an automorphism $\sigma_p : \zeta_n \mapsto \zeta_n^p$. By composing such automorphisms, we obtain all elements $\sigma_k : \zeta_n \to \zeta_n^k$ with $k \in (\mathbf{Z}/n\mathbf{Z})^*$, and the desired surjectivity follows. □

Unlike in 24.9, it is not always so that the $\varphi(n)$ primitive nth roots of unity form a normal basis for the extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_n)$. Already for $n = 4$, we see that, for example,

$\zeta_4 = i$ and $-i$ are linearly dependent over $\mathbf{Q}$. This makes it more complicated to write down explicitly the field of invariants associated with $H \subset (\mathbf{Z}/n\mathbf{Z})^*$ than in the case of 24.9 (see Exercise 57).

It turns out that the automorphism σ_p constructed in the proof of 24.14 for all primes $p \nmid n$, which is a type of "lift to characteristic 0" of the Frobenius automorphism, can be constructed much more generally for extensions of number fields. In modern number theory, where such Frobenius automorphisms play an important role, the isomorphism in 24.14 is viewed as a special case of the so-called *Artin map* for abelian extensions of number fields[8].

The extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_n)$ has an abelian Galois group, so for every subfield $F \subset \mathbf{Q}(\zeta_n)$, the extension $\mathbf{Q} \subset F$ is also Galois with abelian Galois group. It is rather surprising that a converse of this statement also holds. This converse was already formulated in 1853 by the German Leopold Kronecker (1823–1891). His incomplete proof was corrected in 1886 by Heinrich Weber (1842–1913), who became known, among other things, as the author of *the* algebra textbook[9] of the early 20th century.

24.15. Kronecker–Weber theorem. *Let $\mathbf{Q} \subset F$ be a finite Galois extension with abelian Galois group. Then there is a cyclotomic field $\mathbf{Q}(\zeta_n)$ that contains F as a subfield.*

For *quadratic* extensions $\mathbf{Q} \subset F$, this theorem can be deduced from 24.11 without too much trouble (Exercise 29). The proof of 24.15 itself uses techniques from algebraic number theory and falls outside the scope of this syllabus.

As Theorem 24.15 already suggests, the Galois group of a polynomial $f \in \mathbf{Q}[X]$ being abelian is a strong condition: there are only "few" abelian extensions of $\mathbf{Q}$. More precisely, for an "arbitrary" monic polynomial $f \in \mathbf{Z}[X]$ of degree $n > 2$, it is not only true that f has "probability 1" of being irreducible (Exercise 22.24), it *also* has "probability 1" of having non-abelian Galois group $\mathrm{Gal}(f) \cong S_n$[10].

Exercise 7. Make this statement precise for $n = 2$ and give a proof for it.

Abelian extensions of $\mathbf{Q}$ are also called *abelian number fields*. Because of their simple characterization, they have a richer arithmetic structure[11] than "ordinary" number fields. It is an open problem whether *arbitrary* algebraic extensions of $\mathbf{Q}$, or even the algebraic extensions with a fixed non-abelian group G, can be described as "explicitly" as the abelian extensions. The difficulty is related to our relatively poor understanding[12] of the infinite group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) = \mathrm{Aut}(\overline{\mathbf{Q}})$, the *absolute Galois group* of $\mathbf{Q}$. The idea underlying 24.14 of obtaining extensions with "explicit" Galois groups by adjoining "torsion points" of suitable groups such as $\mathbf{C}^*$ knows many generalizations. Torsion points of elliptic curves have led to beautiful results in the 20th century. More generally, the natural action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on all sorts of algebraic structures leads to what are called *Galois representations*.

Exercises.

8. Let $L = \mathbf{Q}(X)$ be the field of rational functions over $\mathbf{Q}$ and $\sigma \in \mathrm{Aut}(L)$ the unique automorphism with $\sigma(X) = X + 1$. Prove that $G = \langle \sigma \rangle$ is an infinite subgroup of

$\mathrm{Aut}(L)$ and that $L^G \subset L$ is *not* an algebraic extension. Also show that, in this case, the map $H \mapsto L^H$ from the set of subgroups of G to the set of subfields of L is neither injective nor surjective.

9. Let $L = \mathbf{Q}(X)$ be as above, and define $\sigma_i \in \mathrm{Aut}(L)$ by

$$\sigma_1(X) = -X, \qquad \sigma_2(X) = 1/X, \qquad \sigma_3(X) = 1 - X.$$

Determine the field of invariants $L^{\langle \sigma_i \rangle}$ for $i \in \{1, 2, 3\}$.

10. Define σ_i as in the previous exercise.
    a. Show that $\rho = \sigma_2\sigma_3$ has order 3 in $\mathrm{Aut}(L)$, and determine $L^{\langle \rho \rangle}$.
    b. Show that $G = \langle \sigma_2, \sigma_3 \rangle$ has order 6 and is isomorphic to S_3. Determine $f \in \mathbf{Q}(X)$ with $L^G = \mathbf{Q}(f)$.

11. Let $L = K(X)$ be the field of rational functions over a field K of characteristic $p > 0$ and $\sigma \in \mathrm{Aut}_K(L)$ the automorphism with $\sigma(X) = X + 1$. Show that $G = \langle \sigma \rangle$ is finite, and determine a generator of L^G over K.

12. Let K be a field and $f = \frac{p}{q} \in K(X)$ the quotient of relatively prime polynomials $p, q \in K[X]$ of degree, respectively, m and n. Prove: if f is not constant, then $K(f) \subset K(X)$ is an algebraic extension of degree $\max(m, n)$.

13. Let $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ be a set of $n \geq 1$ algebraic numbers that are pairwise conjugate over $\mathbf{Q}$, and suppose that $f = \prod_{i=1}^{n}(X - \alpha_i)$ is a polynomial with rational coefficients. Prove: f is irreducible in $\mathbf{Q}[X]$.
    [Example: the monic polynomial with the four zeros $1 \pm i \pm \sqrt{2}$ from Exercise 25.]

14. Let $K \subset K(\alpha)$ be a Galois extension with group G. Prove that the minimum polynomial of α over K is equal to $f_K^\alpha = \prod_{\sigma \in G}(X - \sigma(\alpha))$.

15. Let $K \subset L$ be a Galois extension of degree n. Show that L is a splitting field Ω_K^f for a polynomial $f \in K[X]$ of degree n. Is such an f necessarily irreducible?

16. Determine the Galois group of $f = X^3 - 2$ over $\mathbf{F}_3$, $\mathbf{F}_5$, and $\mathbf{F}_7$.

17. Let K be of characteristic different from 2 and $K \subset L$ a quadratic extension.
    a. Prove: there exists an element $m \in K^* \setminus K^{*2}$ with $L = K(\sqrt{m})$, and the subgroup $\langle \overline{m} \rangle \subset K^*/K^{*2}$ is uniquely determined by L.
    b. Prove: there is a bijection between the set of quadratic extensions of K (inside an algebraic closure $\overline{K}$) and the set of non-trivial elements of K^*/K^{*2}, given by $L \longmapsto (L^{*2} \cap K^*) \setminus K^{*2}$.

18. Let K be of characteristic 2 and $K \subset L$ a separable quadratic extension. Write $\wp(F) = \{x^2 + x : x \in F\}$ for a field F. Prove:
    a. There exists an element $m \in K \setminus \wp(K)$ such that $L = K(\alpha)$ holds for a zero α of $X^2 + X + m \in K[X]$, and the subgroup $\langle \overline{m} \rangle \in K/\wp(K)$ is uniquely determined by L.
    b. There is a bijection between the set of separable quadratic extensions of K (inside an algebraic closure $\overline{K}$) and the set of non-trivial elements of $K/\wp(K)$, given by $L \longmapsto (\wp(L) \cap K) \setminus \wp(K)$.

19. Let L be a splitting field of the polynomial $f = X^4 + 20 \in \mathbf{Q}[X]$. Determine $\mathrm{Gal}(f)$ and the diagram of intermediate fields of the extension $\mathbf{Q} \subset L$.

20. Do likewise for $f = X^4 - 4X^2 + 5$ and $f = X^4 - 5X^2 - 5$.

21. Let K be a field of characteristic different from 2 and $L = K(\sqrt{m})$ a quadratic extension of K. Let $\delta = a + b\sqrt{m} \in L \setminus K$ be an element that is not a square in L, and take $M = L(\sqrt{\delta})$. Write $\delta' = a - b\sqrt{m}$. Prove:
    a. We have $f_K^{\sqrt{\delta}} = X^4 - 2aX^2 + a^2 - mb^2$ and $\Omega_K^f = L(\sqrt{\delta}, \sqrt{\delta'})$.
    b. The following are equivalent:
        1. The extension $K \subset M$ is normal.
        2. $N_{L/K}(\delta) = a^2 - mb^2 \in L^{*2} \cap K^* = \langle m, K^{*2} \rangle$.
        3. $\delta/\delta' = \gamma^2$ with $\gamma \in L$.
    c. For $N_{L/K}(\delta) \in K^{*2}$, we have $\mathrm{Gal}(M/K) \cong C_2 \times C_2$, and for $N_{L/K}(\delta) \in m \cdot K^{*2}$, we have $\mathrm{Gal}(M/K) \cong C_4$.
    d. For $\gamma \in L$ as in part b, we have $N_{L/K}(\gamma) = \pm 1$, and $N_{L/K}(\gamma) = -1$ holds if and only if $K \subset M$ is *cyclic* of degree 4.

22. Determine $\mathrm{Gal}(f)$ for each of the following polynomials $f \in \mathbf{Q}[X]$:

$$X^4 - 4X^2 + 2, \qquad X^4 - 2X^2 + 4, \qquad X^4 - 2X^2 + 2.$$

23. Does there exist a quadratic extension of $K = \mathbf{Q}(i)$ that is cyclic over $\mathbf{Q}$? Answer the same question for $K = \mathbf{Q}(\sqrt{17})$.

24. Show that $\mathbf{Q} \subset \mathbf{Q}(\zeta_{11})$ has exactly two non-trivial intermediate fields, and for both fields, determine the minimum polynomial of a primitive element.

25. Determine the minimum polynomials for generators of the subfields of the cyclotomic field $\mathbf{Q}(\zeta_{13})$.

26. Let d be a divisor of 16 and K_d the subfield of $\mathbf{Q}(\zeta_{17})$ of degree d over $\mathbf{Q}$.
    a. Prove: $K_2 = \mathbf{Q}(\sqrt{17})$.
    b. Determine the minimum polynomial of a generator of K_4 over K_2.

27. Let $\zeta_9 \in \mathbf{C}$ be a primitive ninth root of unity.
    a. Prove: $f_{\mathbf{Q}}^{\zeta_9} = \Phi_9 = X^6 + X^3 + 1$.
    b. Show that $\mathbf{Q} \subset \mathbf{Q}(\zeta_9)$ has exactly two non-trivial intermediate fields, and for both fields, determine the minimum polynomial of a primitive element.

28. Determine all intermediate fields of the extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_{15})$, and indicate which subgroups of $(\mathbf{Z}/15\mathbf{Z})^*$ they correspond to.

29. Let $d \in \mathbf{Z}$ be an integer that is not a square. Prove: the cyclotomic field $\mathbf{Q}(\zeta_{4|d|})$ contains the quadratic field $\mathbf{Q}(\sqrt{d})$ as a subfield.

30. Let p be a prime and $n \in \mathbf{Z}_{\geq 1}$ an integer. Prove:
    a. We have $\Phi_{pn} = \Phi_n(X^p)$ if p is a divisor of n.
    b. We have $\Phi_{pn} = \Phi_n(X^p)/\Phi_n$ if p is not a divisor of n.
    c. For $n > 1$ odd, we have $\Phi_{2n} = \Phi_n(-X)$.

31. Calculate Φ_n for all composite numbers $n \leq 30$.

32. Calculate the values $\Phi_n(0)$ and $\Phi_n(1)$ for all $n \geq 1$.

33. Prove that for $n > 1$, the polynomial Φ_n is symmetric: $X^{\varphi(n)} \cdot \Phi_n(1/X) = \Phi_n$.

34. Let $n \geq 1$ be integer and $p \nmid n$ prime. Prove: $\Phi_{np^k} = (\Phi_n)^{\varphi(p^k)} \in \mathbf{F}_p[X]$.

35. Let $n \geq 1$ be integer and $p \nmid n$ prime. Suppose that $p \in (\mathbf{Z}/n\mathbf{Z})^*$ has order d. Prove that $\Phi_n \in \mathbf{F}_p[X]$ is the product of $\varphi(n)/d$ irreducible factors of degree d.
[Hint: what is $[\mathbf{F}_p(\alpha) : \mathbf{F}_p]$ for a zero $\alpha \in \overline{\mathbf{F}}_p$ of Φ_n?]

36. Decompose the polynomial Φ_7 in $\mathbf{F}_p[X]$ for $p \in \{2, 3, 5, 7, 13, 29\}$.

37. Let $n \in \mathbf{Z}_{>1}$. Prove that there exist infinitely many primes $p \equiv 1 \bmod n$.
[Hint: Imitate Euclid's proof 6.5. What primes divide $\Phi_n(N)$?]

38. Show that for every finite *abelian* group G, there exists a Galois extension K of $\mathbf{Q}$ with group G.
[Hint: use the previous exercise and the structure theorem 9.12 for finite abelian groups.]

39. Let K be a field and $f \in K[X]$ of degree n with decomposition $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $\overline{K}[X]$. Deduce from 24.4 that the *discriminant*

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

of f is an element of K.

40. Let $f \in \mathbf{Q}[X]$ be monic irreducible, and view $\mathrm{Gal}(f)$ as a subgroup of S_n through its action on the zeros of f. Prove:

$$\mathrm{Gal}(f) \subset A_n \iff \Delta(f) \text{ is a square in } \mathbf{Q}^*.$$

Is the choice of the base field $\mathbf{Q}$ important?

41. Let $f \in \mathbf{Q}[X]$ be monic irreducible of degree 3. Prove: for every zero $\alpha \in \mathbf{C}$ of f, the field $\mathbf{Q}(\alpha, \sqrt{\Delta(f)}) \subset \mathbf{C}$ is a splitting field of f. Is it necessary for f to be irreducible?

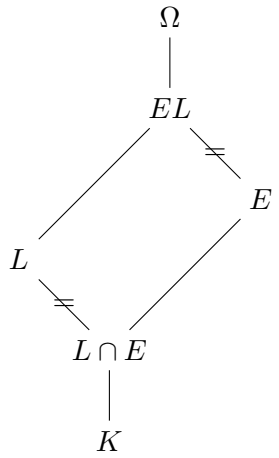
42. Calculate the discriminant of the polynomial $f_{\mathbf{Q}}^{\eta_3} = X^3 + X^2 - 2X - 1$ in Example 24.10.

43. Let K be a field and $f \in K[X]$ an irreducible separable polynomial of degree 4. Show that up to isomorphism, there are no more than five possibilities for the group $\mathrm{Gal}(f)$.

44. Let K be a field and $f \in K[X]$ an irreducible separable polynomial of degree 5.

    a. Prove: $\mathrm{Gal}(f)$ contains an element σ of order 5.
    b. Prove: $\mathrm{Gal}(f)$ is isomorphic to C_5, D_5, or the affine group $\mathrm{Aff}(\mathbf{Z}/5\mathbf{Z})$ of order 20 from 8.14.4 if the subgroup $\langle\sigma\rangle \subset \mathrm{Gal}(f)$ (with σ as in part a) is normal, and isomorphic to A_5 or S_5 if this is not the case.

45. Let $K \subset \Omega$ be an arbitrary field extension and L and E intermediate fields of the extension $K \subset \Omega$. Suppose that $K \subset L$ is a finite Galois extension. Prove: EL is a finite Galois extension of E, and the natural restriction map $\mathrm{Gal}(EL/E) \to \mathrm{Gal}(L/(L \cap E))$ is an isomorphism.



[Question: is there a relation to the diagram of groups after Theorem 8.2?]

46. Let $K \subset K(\zeta)$ be the cyclotomic extension obtained by adjoining a primitive nth root of unity ζ to K. Prove: $K \subset K(\zeta)$ is Galois with group $G \subset (\mathbf{Z}/n\mathbf{Z})^*$. Can every subgroup of $(\mathbf{Z}/n\mathbf{Z})^*$ be obtained as a Galois group for a suitable K?

47. Let $f \in K[X]$ be a polynomial of degree n with Galois group S_n. Let $L = K(\alpha)$ be the extension of K obtained through the adjunction of a zero of f and E be an intermediate field of the extension $K \subset L$. Prove: $E = K$ or $E = L$.

48. Let $K \subset \Omega$ be a field extension, and let E_1 and E_2 be intermediate fields of $K \subset \Omega$ that are finite over K.

    a. Prove that the compositum E_1E_2 is finite over K of degree

    $$[E_1E_2 : K] \leq [E_1 : K] \cdot [E_2 : K].$$

    Is $[E_1E_2 : K]$ necessarily a *divisor* of $[E_1 : K] \cdot [E_2 : K]$?

    b. Prove that E_1E_2 is normal over K if E_1 and E_2 are. Does the converse hold?

    c. Prove that E_1E_2 is abelian over K if E_1 and E_2 are. Does the converse hold?

49. Suppose that the fields E_1 and E_2 in the previous exercise are K-isomorphic and that $L \subset \Omega$ is a field that contains E_1 and is finite Galois over K. Prove: there exists an element $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma[E_1] = E_2$.

50. Let $K \subset M$ be a finite Galois extension with Galois group G and L an intermediate field of $K \subset M$ corresponding to a normal subgroup $N \triangleleft G$. Prove that the exact sequence $1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$ splits if and only if there exists an intermediate field E of $K \subset M$ with $E \cap L = K$ and $EL = M$.

51. Let $L = \Omega_{\mathbf{Q}}^{X^5-2}$ be a splitting field of $X^5 - 2$ over $\mathbf{Q}$. Prove that there exists an exact sequence of groups

    $$0 \longrightarrow \mathbf{Z}/5\mathbf{Z} \longrightarrow \mathrm{Gal}(L/\mathbf{Q}) \longrightarrow (\mathbf{Z}/5\mathbf{Z})^* \longrightarrow 1.$$

    Show that this sequence splits and that $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to the affine group $\mathrm{Aff}(\mathbf{Z}/5\mathbf{Z})$ from Exercise 44.

52. Show that the Galois group of the polynomial $X^n - a \in \mathbf{Z}[X]$ is isomorphic to a subgroup of $\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ from 8.14.4.

53. Define an action of the affine group $G = \mathrm{Aff}(\mathbf{F}_q) = \mathbf{F}_q \rtimes \mathbf{F}_q^*$ on the field of rational functions $L = \mathbf{F}_q(X)$ by viewing $(b, a) \in \mathbf{F}_q \rtimes \mathbf{F}_q^*$ as the automorphism induced by $X \mapsto aX + b$.
    a. Prove that $L^G \subset L$ is a finite Galois extension with group G, and determine a generator of L^G over $\mathbf{F}_q$.
    b. What intermediate fields correspond to the subgroups $\mathbf{F}_q^*$ and $\mathbf{F}_q$ of G?

54. Let $K(X)$ be the field of rational functions over a field K.
    a. Prove that every automorphism σ of $K(X)$ over K satisfies $\sigma(X) = \frac{aX+b}{cX+d}$ with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ and that this induces an isomorphism $G = \mathrm{Aut}_K(K(X)) \cong \mathrm{PGL}_2(K)$. (Here, $\mathrm{PGL}_2(K) = \mathrm{GL}_2(K)/K^*$ is the group obtained by taking the quotient of $\mathrm{GL}_2(K)$ by the normal subgroup $K^* = K^* \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ of scalar matrices.)
    b. Prove that we have $L^G = K$ if and only if K is infinite.

55. Let $K \subset L$ be finite Galois with group G and $X(L/K)$ a fundamental set. Show that the map
$$\begin{aligned} X(L/K) \times G &\longrightarrow X(L/K) \\ (\phi, \sigma) &\longmapsto \phi \circ \sigma \end{aligned}$$
defines a right action of G on $X(L/K)$ that is faithful and transitive.

56. Let $L = \overline{\mathbf{F}}_p$ be an algebraic closure of $\mathbf{F}_p$ and $H \subset G = \mathrm{Aut}(L)$ the cyclic subgroup generated by the Frobenius automorphism. Prove: we have $H \subsetneq G$ but $L^G = L^H = \mathbf{F}_p$. [Hint: use Exercises 22.38 and 22.39]

57. Let $H \subset (\mathbf{Z}/n\mathbf{Z})^*$ be a subgroup and $L \subset \mathbf{Q}(\zeta_n)$ the intermediate field that corresponds to H under the identification 24.14.
    a. Show that $\eta_H = \sum_{\sigma \in H} \sigma(\zeta_n)$ is contained in L.
    b. Show that we have $L = \mathbf{Q}(\eta_H)$ for $H = \{\pm 1 \bmod n\}$.
    c. Show that we have $\eta_H = 0$ if $H \subset (\mathbf{Z}/p^2\mathbf{Z})^*$ is the subgroup of prime order p.

58. Formulate and make the analog of Exercise 4 (page 49) for irreducible polynomials of the form $X^4 - k$ or $X^6 - k$, with $k \in \mathbf{Q}_{>0}$.

59. Let K be a field, and denote the group of roots of unity in K by μ_K. Prove: we have $\mu_K = K^*$ if and only if there is a prime p such that K is an algebraic extension of $\mathbf{F}_p$.

60. Let V be a vector space over a field L and $G \subset \mathrm{Aut}\, L$ a finite subgroup. Let a *semilinear* action of G on V be given, that is, an action with the property that for all $c \in L$, v, $w \in V$, and $\sigma \in G$, we have $\sigma(v + w) = \sigma v + \sigma w$ and $\sigma(cv) = (\sigma c)(\sigma v)$. Define $S : V \to V$ by $S(v) = \sum_{\sigma \in G} \sigma v$.
    a. Suppose that $\varphi : V \to L$ is an L-linear map with $S(V) \subset \ker \varphi$. Prove: $\varphi = 0$. (*Hint*: use $\varphi(S(cv)) = 0$ for all $c \in L$ and $v \in V$.)
    b. Prove that as an L-vector space, V is spanned by $S(V)$.
    c. Prove that V has a G-invariant L-basis, i.e., a basis $(b_i)_{i \in I}$ such that we have $\sigma\left(\sum_{i \in I} c_i b_i\right) = \sum_{i \in I} (\sigma c_i) b_i$ for all $\sigma \in G$ and coefficients $c_i \in L$, almost all of which are 0.

61. Let L be a field. We call a subset U of $\mathrm{Aut}\, L$ *open* if for every $\sigma \in U$, there is a finite subset $E \subset L$ such that U contains every $\tau \in \mathrm{Aut}\, L$ with $\tau\big|_E = \sigma\big|_E$.

a. Prove that this defines a topology on $\operatorname{Aut} L$ and that $\operatorname{Aut} L$ is Hausdorff.
b. Prove that $\operatorname{Aut} L$ is a *topological* group in the sense that the maps $\operatorname{Aut} L \times \operatorname{Aut} L \to \operatorname{Aut} L$ and $\operatorname{Aut} L \to \operatorname{Aut} L$ defined by $(\sigma, \tau) \mapsto \sigma\tau$ and $\sigma \mapsto \sigma^{-1}$ are continuous when $\operatorname{Aut} L \times \operatorname{Aut} L$ is endowed with the product topology.

62. Suppose that the rings $\hat{\mathbf{Z}}$ and $\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$ from Exercise 22.38 are endowed with a topology by giving each $\mathbf{Z}/n\mathbf{Z}$ the discrete topology, $\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$ the product topology, and $\hat{\mathbf{Z}}$ the subspace topology. Prove that the group isomorphism from Exercise 22.39 is in fact an *isomorphism of topological groups*, that is, both a group isomorphism and a homeomorphism.

63. The *maximal cyclotomic extension* $\mathbf{Q}^{\mathrm{cycl}}$ of $\mathbf{Q}$ is obtained by adjoining to $\mathbf{Q}$, inside an algebraic closure $\bar{\mathbf{Q}}$, all roots of unity in $\bar{\mathbf{Q}}$. Prove: as a topological group, $\operatorname{Aut} \mathbf{Q}^{\mathrm{cycl}}$ is isomorphic to the group of units $\hat{\mathbf{Z}}^*$ of $\hat{\mathbf{Z}}$, where $\hat{\mathbf{Z}}^* \subset \hat{\mathbf{Z}}$ is endowed with the induced subspace topology.

64. Let L be a field and $G \subset \operatorname{Aut} L$ a subgroup. Prove: G is compact if and only if G is closed and, moreover, for every $c \in L$, the orbit Gc of c under G is finite.
[Hint: use Tychonoff's theorem.]

65. Let $K \subset L$ be a field extension.
a. Prove: $\operatorname{Aut}_K L$ is a closed subgroup of $\operatorname{Aut} L$.
b. Prove: if L is algebraic over K, then $\operatorname{Aut}_K L$ is compact.