ALGEBRA III

P. Stevenhagen

2020

TABLE OF CONTENTS ALGEBRA III

First English version: September 2020

Every subsequent version will, hopefully, contain fewer typos and inaccuracies than the present one—please send any comments to psh@math.leidenuniv.nl.

Author's address

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden

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 24.10.

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 $f \in \mathcal{F} = K[X] \setminus K$ 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

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

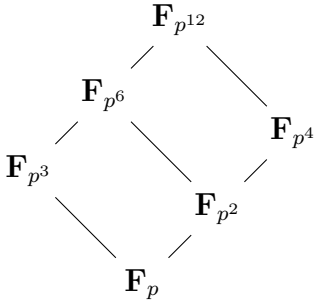
The complete structure of the set of subfields of $\overline{\mathbf{F}}_p$ and the inclusion relations between the subfields can be deduced from this characterization.

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

In 24.4, we generalize this theorem, called the *fundamental theorem of Galois theory* for $K \subset L$, to the case of an *arbitrary* base field K. For finite K, the situation is relatively simple: every finite extension $K \subset L$ is *simple*, of the form $L = K(\alpha)$, and by 22.11, along with $\alpha \in L$, all other zeros of f_K^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.

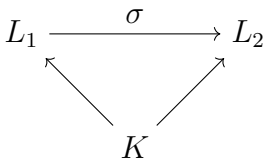
    b. How many reduced commutative rings of order 72 are there, up to isomorphism?

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 $\operatorname{char}(K) = p > 0$, 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 $\alpha, \beta \in \bar{K}$ 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 (1811–1832), 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

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

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

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 $c_i \ne 0$, 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 $[L:K] \le \#G$.

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

$$G = \mathrm{Aut}_K(L) = X_\Omega(L/K). \tag{24.6}$$

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.

24.7. 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. □

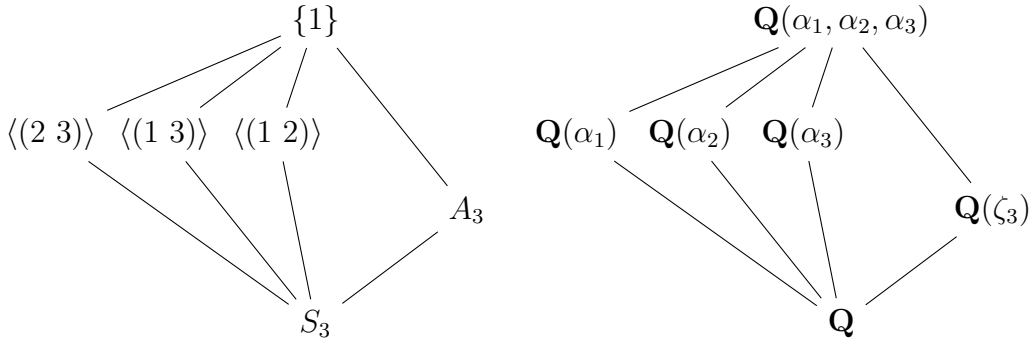
Exercise 3. Prove that $\mathrm{Gal}(f)$ acts transitively on the zeros of a separable polynomial $f \in K[X]$ if and only if f is irreducible.

In view of 24.7, 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.



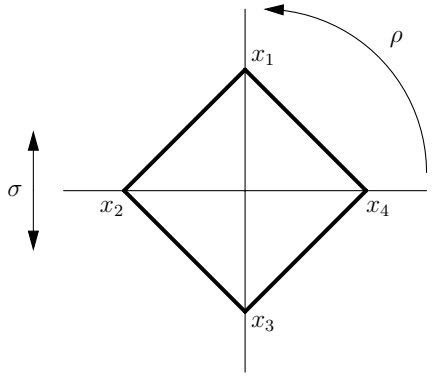
We see that there are no other intermediate fields than the "obvious" ones. The three non-normal extensions $\mathbf{Q}\subset\mathbf{Q}(\alpha_i)$ correspond to the non-normal subgroups of order 2 in S_3. The isomorphic fields $\mathbf{Q}(\alpha_i)$ are conjugate over $\mathbf{Q}$; the subgroups of 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.

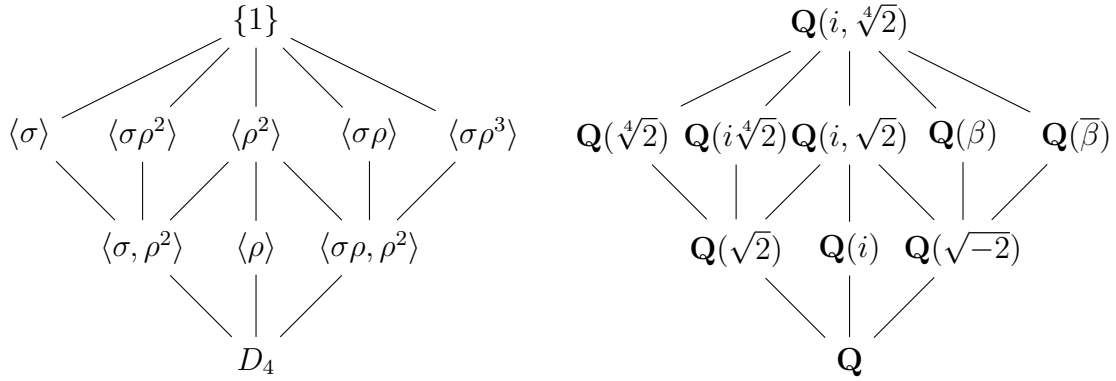
Recall from 10.11 that the subgroups of S_4 of order 8 are the 2-Sylow subgroups and that they are isomorphic to the dihedral group D_4. The isomorphism $\mathrm{Gal}(L/\mathbf{Q})\cong D_4$ can also be discovered by letting σ be the complex conjugation on L and $\rho:L\to L$ an automorphism that satisfies $\rho(x_1)=x_2=ix_1$. 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.

24.8. 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.* □

24.9. 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.

24.10. 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 24.10.2 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 24.7, 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 24.8. 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 24.10 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.

24.11. 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.

24.12. 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 24.12 shows that τ_p is a square root of $p^* = \pm p \equiv 1 \bmod 4$.

▶ Cyclotomic Extensions

Let us see what Theorem 24.10 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 $\mathbf{C}[X]$:

$$\prod_{d \mid n} \Phi_d = X^n - 1. \tag{24.13}$$

This can be used to calculate the polynomials Φ_n inductively. For example, by applying (24.13) 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.

24.14. 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 (24.13) 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 (24.13) 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 24.10, 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*.

24.15. 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 24.7 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 24.10, 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 24.10 (see Exercise 57).

It turns out that the automorphism σ_p constructed in the proof of 24.15 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 24.15 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.

24.16. 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 24.12 without too much trouble (Exercise 29). The proof of 24.16 itself uses techniques from algebraic number theory and falls outside the scope of this syllabus.

As Theorem 24.16 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 24.15 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?

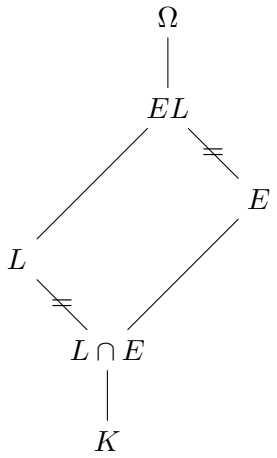
42. Calculate the discriminant of the polynomial $f_{\mathbf{Q}}^{\eta_3} = X^3 + X^2 - 2X - 1$ in Example 24.11.

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 24.15.
    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.

25 Radical extensions

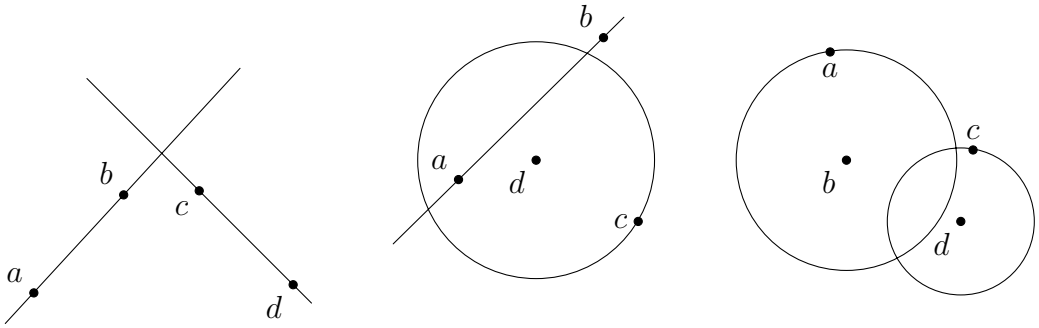
This section contains two classic applications of Galois theory. The first application, the problem of the *constructibility* of points in the plane raised by Greek mathematicians, shows that the underlying questions do not need to refer to field extensions or automorphism groups in any way. The second application, solving polynomial equations by extracting roots, is the problem that, in a way, gave rise to Galois theory.

▶ Construction problems

In Greek mathematics,[13] people used to *construct* figures with a straightedge and compass. Here one repeatedly enlarges a given set X of at least two points in the plane by adding to it those points that can be constructed as intersections of lines and circles defined in terms of the given points. The question is, for given X, whether certain points in the plane can be obtained from X in finitely many construction steps.

More formally, a *construction step* starting out from a subset X of the plane consists of replacing the set X with the set $\mathcal{F}(X)$ of all points P obtained by applying the following algorithm:

1. Pick points $a, b, c, d \in X$ with $a \neq b$ and $c \neq d$.
2. Let ℓ_{ab} be either the line through a and b or the circle through a with center b. Likewise, let ℓ_{cd} be either the line through c and d or the circle through c with center d.
3. If ℓ_{ab} and ℓ_{cd} do not coincide, pick $P \in \ell_{ab} \cap \ell_{cd}$.



In order to perform step 1 of the algorithm, X needs to contain at least two points. In this case, picking $c = a$ and $d = b$ shows that we have $X \subset \mathcal{F}(X)$. As the permissible intersections $\ell_{ab} \cap \ell_{cd}$ consist of 0, 1, or 2 points, $\mathcal{F}(X)$ is finite if X is finite.

25.1. Definition. *Let $X = X_0$ be a subset of the plane containing at least two points, and define, recursively for $i \in \mathbf{Z}_{\geq 1}$, the sets*

$$X_i = \mathcal{F}(X_{i-1}) \supset X_{i-1}.$$

Then $\mathcal{C}(X) = \bigcup_{i=0} X_i$ is called the set of constructible points starting from X.

In addition to constructing points in the plane, we can also speak of constructing lines and circles in the plane. A line is called constructible if it is possible to construct two

distinct points on it, and a circle is called constructible if it is possible to construct its center and a point on it.

As early as the fifth century B.C., Greek mathematics gave rise to several construction problems that the Greeks could not solve and which, for more than two thousand years, defeated many mathematicians, "professional" or not.[14]

25.2. Squaring the circle. *Construct a square whose area is equal to that of a circle with given radius.*

Hippocrates of Chios, who lived around 430 B.C., showed that 25.2 is solvable if instead of the circle, we take certain figures bounded by circular arcs, the so-called *lunes of Hippocrates*[15] (see Exercise 14).

25.3. Doubling the cube. *Construct a line segment that is $\sqrt[3]{2}$ times as long as a given line segment.*

This problem is also known as the *Delian problem*, after the legend in which, through his oracle on the island Delos, the god Apollo decreed that the plague-ridden Athenians should "double" their cubic altar to Apollo.

25.4. Trisecting the angle. *Use a straightedge and compass to divide a given angle into three equal parts.*

For a few angles, such as the right angle, this problem is easy to solve. In most other cases, angle trisection does not seem possible.

25.5. Constructing the n-gon. *For $n \geq 3$, construct a regular n-gon in a given circle.*

Strictly speaking, this problem does not belong to the classical "corpus" of the three unsolved Greek problems. But, as it corresponds to the division of the full angle of 2π radials into n equal parts, it is closely related. Since bisecting an angle using a straightedge and compass is easy, the interesting question in 25.5 is for which *odd* n the problem is solvable. The Greek found solutions for $n = 3$ and $n = 5$ but not, for example, for $n = 7$ or $n = 9$.

To formulate construction problems in terms of field extensions, we identify the plane in the usual way with the field $\mathbf{C}$ of complex numbers. Using 25.1, the problems mentioned above can easily be reformulated in terms of numbers constructible from a subset $X \subset \mathbf{C}$. After scaling, we may assume that X contains the two points 0 and 1.

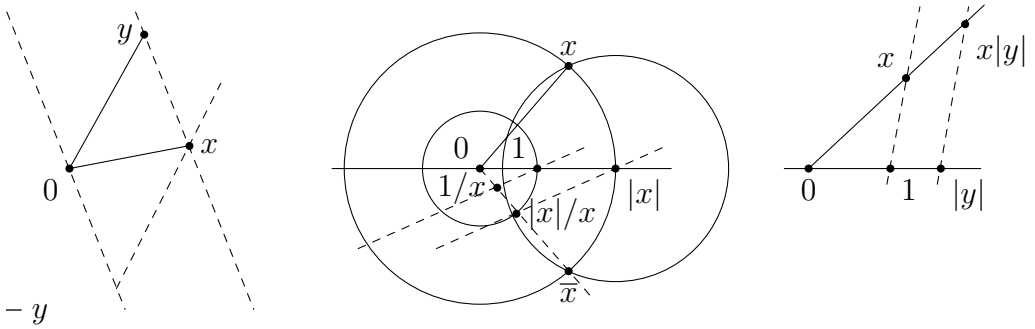
For X equal to $\{0, 1\}$, the set $\mathcal{C} = \mathcal{C}(X)$ is simply called the set of *constructible numbers*. Problems 25.2, 25.3, and 25.5 then correspond to the questions of whether the numbers $\sqrt{\pi}$ and $\sqrt[3]{2}$ and the primitive nth root of unity $\zeta_n = e^{2\pi i/n} \in \mathbf{C}$ are constructible. The question in 25.4 is whether for $\alpha \in \mathbf{C}$ with $|\alpha| = 1$, the set $\mathcal{C}(\{0, 1, \alpha\})$ contains a third root $\sqrt[3]{\alpha}$.

25.6. Proposition. *Let $X \subset \mathbf{C}$ be a set that contains 0 and 1. Then $\mathcal{C}(X)$ is a subfield of $\mathbf{C}$ that contains X. It is closed under complex conjugation and under extracting square roots.*

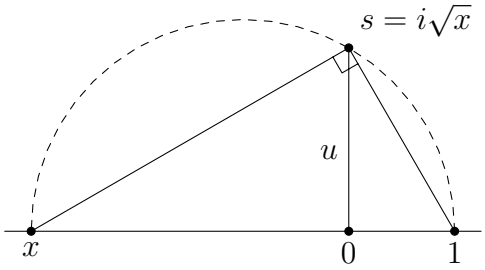
Proof. The proof is an exercise in carrying out elementary constructions. We assume the standard constructions from Exercise 13 known—an exercise we recommend for anyone who has never carried out a construction. It is clear that X, and in particular 0 and 1, are contained in $\mathcal{C}(X)$. It therefore suffices to show that for $x, y \in \mathcal{C}(X)$, the difference $x - y$, the product xy, the inverse $1/x$, the complex conjugate $\overline{x}$, and the square roots $\pm\sqrt{x}$ are constructible from X.

For $x - y$, we mark off the distance $|x - y|$ on the line through 0 parallel to the line through x and y. For $\overline{x}$, we first intersect the circle through x with center 0 with the line through 0 and 1—this gives $|x|$—and then intersect it with the circle through x with center $|x|$. For $x \notin \mathbf{R}$, the point $|x|/x$ is the intersection of the circle through 1 with center 0 with the line through 0 and $\overline{x}$; the line through 1 parallel to the line through $|x|/x$ and $|x|$ now cuts the line through 0 and $\overline{x}$ in $1/x$. A similar figure shows how to multiply x by a real number $|y|$. The product $x|y|$ is then rotated over the angle $\angle y01$ to obtain xy.

Exercise 1. How should the constructions be adjusted for $x \in \mathbf{R}$?



Taking the square root corresponds to constructing $\sqrt{x}$ for $x \in \mathbf{R}_{>0}$. After all, for non-real x, we simply mark off $\sqrt{|x|}$ on the bisector of the angle $\angle x01$. For $x \in \mathbf{R}_{>0}$, we intersect the perpendicular in 0 to the line through 0 and 1 with the circle that has the line segment from $-x$ to 1 as diameter. Let s be an intersection point.



The angle $\angle(-x)s1$ is a right angle (Thales's theorem), so the triangles $(-x)s0$ and $s10$ are similar. The equality of the ratios $x : u = u : 1$ shows that s is equal to $i\sqrt{x}$, and we are done. □

Exercise 2. (For whoever did not know this yet ...) Formulate and prove Thales's theorem.

The main result on constructible numbers is that 25.6 in fact characterizes the field $\mathcal{C}(X)$: it is the *smallest* field that satisfies the conditions of 25.6. To see this, we must show that the construction steps can only lead to quadratic field extensions.

25.7. Proposition. *Let $X \subset \mathbf{C}$ be given, and let $K = \mathbf{Q}(X, \overline{X})$ be the subfield of $\mathbf{C}$ generated by the elements in X and their complex conjugates. Then every point $z \in \mathbf{C}$ that can be obtained from X through a construction step is algebraic over K of degree $[K(z) : K] \leq 2$.*

Proof. Suppose that there exist points $a, b, c, d \in X$ with $a \neq b$ and $c \neq d$. We must show that an intersection point of the line or circle determined by ab and the line or circle determined by cd has degree at most 2 over K. We distinguish between the three possibilities given by the figures before 25.1.

The line through the points a and b consists of the points $z \in \mathbf{C}$ for which $(z-a)/(a-b)$ is real. Expanding the identity $(z-a)/(a-b) = (\overline{z}-\overline{a})/(\overline{a}-\overline{b})$ gives the following equation for this line:

$$\ell_{ab} : (\overline{a}-\overline{b})z - (a-b)\overline{z} = \overline{a}b - a\overline{b}.$$

Intersecting the lines ℓ_{ab} and ℓ_{cd} amounts to solving two linear equations in z and $\overline{z}$ with coefficients in $\mathbf{Q}(a, b, c, d, \overline{a}, \overline{b}, \overline{c}, \overline{d}) \subset K$. If ℓ_{ab} and ℓ_{cd} are not parallel, this system has a unique solution $z \in K$, and we have $K(z) = K$. If the lines are parallel, then because ℓ_{ab} and ℓ_{cd} do not coincide, the system is inconsistent and has no solution.

For the circle through c with center d, the equation is $|z-d| = |c-d|$; we can rewrite this as $(z-d)(\overline{z}-\overline{d}) = (c-d)(\overline{c}-\overline{d})$ or

$$z\overline{z} - \overline{d}z - d\overline{z} = c\overline{c} - c\overline{d} - \overline{c}d.$$

For a point z on the line ℓ_{ab} that lies on this circle, we can use the equation for ℓ_{ab} to write $\overline{z}$ as a linear expression in z with coefficients in K. Substituting this in the equation for the circle gives a quadratic relation with coefficients in K satisfied by z. We find $[K(z) : K] \leq 2$.

In the event that z is a point that lies both on the circle through a with center b and on the circle through c with center d, taking the difference of the equations for the two circles gives a linear relation between z and $\overline{z}$ with coefficients in K. Since the circles do not coincide, this is not the zero relation, and we are back in the previous case. This proves $[K(z) : K] \leq 2$ for all construction steps. □

▶ Quadratic closure

The main result for constructible numbers can be formulated concisely in terms of *quadratic closures*. We first introduce the "maximum square root extension" of a field K (inside an algebraic closure $\overline{K}$) as the subfield $K(S) \subset \overline{K}$ generated by the set

$$S = \{w \in \overline{K} : w^2 \in K\}$$

of square roots of elements of K. For K of characteristic different from 2, this extension, which we symbolically denote by $K(\sqrt{K})$, is an algebraic extension of K that is normal and separable. In many cases, however, it is of infinite degree over K.

Exercise 3. Show that $\mathbf{Q} \subset \mathbf{Q}(\sqrt{\mathbf{Q}})$ is an infinite extension.

25.8. Definition. *Let K be a field of characteristic* $\mathrm{char}(K) \neq 2$ *with algebraic closure $\overline{K}$. Then the quadratic closure K^{quad} of K in $\overline{K}$ is the field*

$$K^{\mathrm{quad}} = \bigcup_{i=0}^{\infty} K_i, \qquad \text{where } K_0 = K \text{ and } K_i = K_{i-1}(\sqrt{K_{i-1}}) \text{ for } i \geq 1.$$

The similarity between 25.8 and 25.1 is more than superficial.

25.9. Theorem. *The set $\mathcal{C}(X)$ of points constructible from a subset $X \subset \mathbf{C}$ that contains* 0 *and* 1 *is equal to the quadratic closure of the field $\mathbf{Q}(X, \overline{X})$ in $\mathbf{C}$.*

Proof. By 25.6, the set $\mathcal{C}(X)$ is a field that contains X and is closed under complex conjugation and extracting square roots, so it is clear that the quadratic closure of $K = \mathbf{Q}(X, \overline{X})$ is contained in $\mathcal{C}(X)$.

Conversely, it follows from 25.7 that the points that can be formed from X through a construction step are contained either in $K = \mathbf{Q}(X, \overline{X})$ itself or in a quadratic extension of K. Every quadratic extension of K is of the form $K \subset K(\sqrt{x})$ and therefore contained in $K_1 = K(\sqrt{K})$. Note that along with K, the field $K(\sqrt{K})$ also maps to itself under complex conjugation. Repeating the previous argument shows that, more generally, the points that can be constructed from X in $i \geq 1$ construction steps are contained in K_i, with K_i as in 25.8. This shows that $\mathcal{C}(X)$ is contained in the quadratic closure of $K = \mathbf{Q}(X, \overline{X})$. □

Even in the simplest case $X = \{0, 1\}$, the field $\mathcal{C}(X) = \mathbf{Q}^{\mathrm{quad}}$ is an infinite field extension of $\mathbf{Q}(X, \overline{X}) = \mathbf{Q}$. The following theorem is therefore very useful to determine whether a complex number is in the quadratic closure of $K \subset \mathbf{C}$.

25.10. Theorem. *Let $K \subset \mathbf{C}$ be a field. Then for an element $x \in \mathbf{C}$, the following statements are equivalent:*

1. *The element x is contained in the quadratic closure of K.*
2. *There exist an $n \in \mathbf{Z}_{\geq 0}$ and a chain*

$$K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_{n-1} \subset E_n \subset \mathbf{C}$$

   of intermediate fields of $K \subset \mathbf{C}$ with $[E_i : E_{i-1}] = 2$ for $1 \leq i \leq n$ and $x \in E_n$.
3. *The element x is algebraic over K, and the Galois group of the polynomial f_K^x over K is a finite 2-group.*

Proof. (2) ⇒ (1). Let $V \subset \mathbf{C}$ be the set of elements that satisfy (2). Then for $x \in V$ with associated chain $K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_n$, every quadratic extension $E_i \subset E_{i+1}$ can be obtained through the adjunction of a square root. It follows that we have $E_i \subset K_i$ for K_i as in 25.8, and therefore $x \in E_n \subset K_n \subset K^{\mathrm{quad}}$. This proves $V \subset K^{\mathrm{quad}}$.

(1) ⇒ (2). For the inclusion $K^{\mathrm{quad}} \subset V$ with V as above, we show that V is a subfield of $\mathbf{C}$ that contains K and is closed under the adjunction of square roots. It is obvious that K is contained in V. It is also clear that along with $x \in V$, we also

have $\sqrt{x} \in V$; in the situation of statement (2), consider the extension $E_n \subset E_n(\sqrt{x})$ of the chain for $\sqrt{x} \notin E_n$. Finally, to see that V is a *subfield* of $\mathbf{C}$, we use the chain $K = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_s$ for $y \in V$ to extend the chain $K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_r$ for $x \in V$ to

$$K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_r = E_rF_0 \subset E_rF_1 \subset E_rF_2 \subset \ldots \subset E_rF_s.$$

This tower consist of successive extensions of degree at most 2, so all elements of $\mathbf{Q}(x, y) \subset E_rF_s$ are contained in V. This shows that V is a field.

(2) $\Rightarrow$ (3). If for $x \in \mathbf{C}$, there exists a chain $K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_n$ as in (2), then x is certainly algebraic over K. We now extend the chain for x so that the last extension is *normal* over K. For this, take the normal closure $M \subset \mathbf{C}$ of E_n over K and $\sigma \in \mathrm{Gal}(M/K)$ arbitrary. Then the chain $K = \sigma[E_0] \subset \sigma[E_1] \subset \ldots \subset \sigma[E_n]$ is a chain as in (2) for $\sigma(x)$. By combining these chains for all $\sigma \in \mathrm{Gal}(M/K)$ as explained above to one long chain, we obtain a tower of quadratic extensions ending in the compositum M of the collection of fields $\{\sigma[E_n]\}_{\sigma \in \mathrm{Gal}(M/K)}$. It follows that $\mathrm{Gal}(M/K)$ is a 2-group, and the Galois group $\mathrm{Gal}(f_K^x)$ of the subextension $\Omega_K^{f_K^x} \subset M$ over K is therefore also one.

(3) $\Rightarrow$ (2). It follows from 10.17 ("solvability of p-groups") that in the 2-group $G = \mathrm{Gal}(f_K^x)$, there exists a chain $G = H_0 \supset H_1 \supset \ldots \supset H_n = 1$ of subgroups for which all indices $[H_i : H_{i+1}]$ are equal to 2. The corresponding subfields $E_i \subset \Omega_K^{f_K^x}$ give a chain that satisfies the conditions in (2). □

Exercise 4. Show that 25.10 is correct for any field K of characteristic different from 2 if, everywhere, we replace $\mathbf{C}$ with an algebraically closed extension of K.

We now return to the problems 25.2–25.5. If we use the result of Lindemann mentioned before 21.5, which says that the number π is transcendental, then it follows from 25.9 and 25.10.3 that π and $\sqrt{\pi}$ are not constructible, so we cannot square the circle with a straightedge and compass.

The number $\sqrt[3]{2}$ is algebraic, but of degree 3 over $\mathbf{Q}$ and therefore not contained in any extension of $\mathbf{Q}$ whose degree is a power of 2. Doubling the cube with a straightedge and compass is therefore also not possible.

For $\alpha \in \mathbf{C}$ with $|\alpha|^2 = \alpha\overline{\alpha} = 1$, trisecting the angle $\angle 10\alpha$ corresponding to α with a straightedge and compass is not possible if $X^3 - \alpha$ is irreducible over $\mathbf{Q}(\alpha, \overline{\alpha}) = \mathbf{Q}(\alpha)$. This is the case for "most" α, including all transcendental values of α; see Exercises 20 and 21. In the rare reducible case, which occurs, for example, for $\alpha = \pm 1$ and $\alpha = i$, a splitting field $\Omega_{\mathbf{Q}(\alpha)}^{X^3-\alpha}$ has degree at most 2 over K and trisection is possible.

In the case of the regular n-gon, we need to determine for what n the degree of the cyclotomic extension $\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$ is a power of 2. This is more of an arithmetic than a geometric problem: for what n is $\varphi(n)$ a power of 2? If such an n has prime decomposition $n = \prod_{p|n} p^{e_p}$, then 6.16 gives the value $\varphi(n) = \prod_{p|n}(p-1)p^{e_p-1}$. This shows that apart from the prime $p = 2$, only primes of the form $p = 2^m + 1$ occur in the decomposition of n and that these primes moreover have exponent $e_p = 1$. Note that $p = 2^m + 1$ can only be prime if m is a power of 2. After all, if m has a proper divisor u for which m/u is *odd*, then $2^m + 1$ is divisible by $2^u + 1$.

25.11. Definition. *A Fermat prime is a prime of the form* $p = 2^{2^k} + 1$.

If we write $F_k = 2^{2^k} + 1$ for $k \geq 0$, then $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$ are prime. Fermat's rash conjecture that all numbers F_k are prime explains the name in 25.11. The number F_k is also called the kth *Fermat number*. The fifth Fermat number $F_5 = 641 \cdot 6700417$ is not prime, and neither are the numbers F_k with $6 \leq k \leq 32$. It is not known[16] whether there exist values $k \geq 5$ for which F_k *is* prime—it is conjectured that this is not the case. Apart from this open question, there is the following complete solution of 25.5.

25.12. Theorem. *Let* $n \geq 3$ *be an integer, and write* $n = 2^k \cdot n_0$ *with* n_0 *odd. Then the regular* n*-gon is constructible if and only if* n_0 *is a product of distinct Fermat primes.* □

The constructibility for n of the given form was already proved by Gauss in 1801 using the cyclotomic periods from 24.10.2. A seventeen-pointed star adorns the Gauss monument in Brunswijk, because a regular 17-gon can only be distinguished from a circle by looking very closely.

▶ Radical closure

A characterization as that given in 25.10 for the quadratic closure of $\mathbf{Q}$ in $\mathbf{C}$ can also be given for the *radical closure* $\mathbf{Q}^{\mathrm{rad}}$ of $\mathbf{Q}$ in $\mathbf{C}$. The definition closely resembles that in 25.8.

25.13. Definition. *Let* K *be of characteristic* 0 *with algebraic closure* $\overline{K}$*. Then the radical closure* K^{rad} *of* K *in* $\overline{K}$ *is the field* $K^{\mathrm{rad}} = \bigcup_{i=0}^{\infty} K_{(i)}$*, where* $K_{(0)} = K$ *and*

$$K_{(i)} = K_{(i-1)}(\{w \in \overline{K} : w^n \in K_{(i-1)} \text{ for some } n \geq 1\})$$

for all $i \geq 1$.

The field K^{rad} is the subfield of $\overline{K}$ consisting of the elements that can be obtained from K by applying the field operations (addition, subtraction, multiplication, and division) and "extracting roots" of arbitrarily high degree. This is the smallest extension of K that is closed under all root extractions.

To avoid separability problems, from now on in this section, we assume that K is of characteristic 0. For fields of positive characteristic p, all results concerning roots of degree n remain valid when n is *not* divisible by p. For $n = p$, we obtain the "correct" generalization by replacing the pth roots of unity, which are zeros of polynomials $X^p - a \in K[X]$, everywhere by zeros of *Artin–Schreier polynomials* $X^p - X - a \in K[X]$. See Exercises 32–34.

Inside the algebraic closure $\overline{K}$ of K, we have a tower of extensions

$$K \subset K^{\mathrm{quad}} \subset K^{\mathrm{rad}} \subset \overline{K}.$$

By definition, $\overline{K}$ consists of all elements that are zeros of a monic polynomial $f \in K[X]$; it is a classical question whether the zeros of a polynomial f can be expressed in the

elements of K "using radicals." For $f \in K[X]$ of degree $n \leq 4$, there exist explicit "radical formulas" to express the zeros of f in the coefficients of f; we will return to this at the end of the section. For polynomials of degree $n \geq 5$, the search for similar formulas continued until into the 19th century. The famous application of Galois theory in this section shows that for $n \geq 5$, such a general formula does *not* exist. The field $\mathbf{Q}^{\mathrm{rad}}$ is not equal to $\overline{\mathbf{Q}}$, and in 25.17, we will construct polynomials in $\mathbf{Q}[X]$ whose zeros are in $\overline{\mathbf{Q}}$ but not in $\mathbf{Q}^{\mathrm{rad}}$.

A word of warning is in order when using the notation $\sqrt[n]{a}$ to indicate an nth root of an element a. The ambiguity in this notation, which for $n = 2$ is restricted to a choice of sign, easily leads to mistakes for general n. For example, because of $16 = 2^4$, it seems logical to expect that adjoining a zero α of $X^8 - 16$ to $\mathbf{Q}$ would lead to the field $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2})$. However, we also have $16 = (-2)^4$, so that $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-2})$ is *another* field that is as "justifiable." Similar problems occur when extracting "an" nth root of 1. Thus, it is better to avoid the notation $\sqrt[3]{1}$ because not all zeros of $X^3 - 1$ generate the same extension of $\mathbf{Q}$. In this last case, even the degree of the extension depends on the choice of the root.

Exercise 5. Show that $1 + i$ and $1 - i$ are also eighth roots of 16.

We can limit the ambiguity in the notation $K \subset K(\sqrt[n]{a})$ for field extensions obtained by adjoining an nth root of $a \in K$ to K by only looking at *irreducible radicals*. In this situation, the additional condition is imposed that only zeros of *irreducible* polynomials $X^n - a \in K[X]$ are adjoined. In many cases, it is easy to avoid the problematic radical notation.

25.14. Definition. *A finite field extension $K \subset L$ is called a radical extension if there exists a primitive element x for $K \subset L$ with $x^n \in K$ for some $n \geq 1$. If x and n can be chosen such that $X^n - x^n$ is irreducible in $K[X]$, then $K \subset L$ is called an irreducible radical extension.*

Exercise 6. Show that the cyclotomic field $\mathbf{Q}(\zeta_5)$ is a radical extension of $\mathbf{Q}$ but not an irreducible radical extension.

Although not every radical extension is irreducible, the field K^{rad} does not depend on the type of radical extension under consideration (Exercise 31). The main result we are going to prove in this section is the following analog of 25.10.

25.15. Theorem. *Let K be a field of characteristic 0 with algebraic closure $\overline{K}$. Then for an element $x \in \overline{K}$, the following statements are equivalent:*

1. *The element x is contained in the radical closure of K in $\overline{K}$.*
2. *There exist an $n \in \mathbf{Z}_{\geq 0}$ and a chain of fields*

$$K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_{n-1} \subset E_n \subset \overline{K}$$

   with $E_{i-1} \subset E_i$ for $1 \leq i \leq n$ a radical extension and $x \in E_n$.
3. *The Galois group of the polynomial f_K^x over K is a solvable group.*

A finite extension $K \subset E$ is called *solvable* if the Galois group $\mathrm{Gal}(M/K)$ of a normal closure M of E over K is a solvable group. By 10.14, this means that there exists a chain of subgroups

$$\mathrm{Gal}(M/K) = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_k = 1$$

in $\mathrm{Gal}(M/K)$ for which every H_{i+1} is normal in H_i and H_i/H_{i+1} is cyclic of prime order. It follows from 25.15 that a finite extension $K \subset K(x)$ of a field K of characteristic 0 is solvable if and only if the equation $f_K^x(X) = 0$ can be "solved" using radicals. This explains the use of the word "solvable" in group theory.

Exercise 7. Show that a subextension of a solvable extension is solvable and that the compositum of two solvable extensions is also solvable.

Before proving 25.15, let us take a closer look at radical extensions. It turns out that such extensions admit an elegant description when the base field contains sufficiently many roots of unity.

25.16. Theorem. *Let $n \geq 2$ be an integer and K a field that contains a primitive nth root of unity.*

1. *Every cyclic extension $K \subset L$ of degree n is of the form $L = K(\sqrt[n]{a})$, with $a \in K$ and $\sqrt[n]{a}$ a zero of $X^n - a \in K[X]$.*
2. *For $a \in K$, the field $L = \Omega_K^{X^n - a}$ is a cyclic extension of K of degree n/d, with d the largest divisor of n for which a is a dth power in K.*

Proof. (1) Let σ be a generator of $\mathrm{Gal}(L/K)$ and $\zeta \in K$ a primitive nth root of unity. We construct an element $\alpha \in L^*$ with $\sigma(\alpha) = \zeta\alpha$ by looking at the so-called *Lagrange resolvent*

$$\alpha = x + \zeta^{-1}\sigma(x) + \zeta^{-2}\sigma^2(x) + \ldots + \zeta^{1-n}\sigma^{n-1}(x),$$

where $x \in L$ is chosen such that we have $\alpha \neq 0$. Note that such an x exists by the Artin–Dedekind lemma 23.15. A simple verification gives $\sigma(\alpha) = \zeta\alpha$. The element $a = \alpha^n$ is now in K because σ leaves a invariant:

$$\sigma(a) = \sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n = a.$$

Since we have $\sigma(\zeta) = \zeta$, repeatedly applying σ to the identity $\sigma(\alpha) = \zeta\alpha$ gives the relation $\sigma^i(\alpha) = \zeta^i\alpha$. It follows that the subgroup $\mathrm{Gal}(L/K(\alpha)) \subset \mathrm{Gal}(L/K)$ of powers of σ that fix α is the trivial subgroup $\langle\sigma^n\rangle = 1$. Consequently, we have $L = K(\alpha)$, with $\alpha = \sqrt[n]{a}$ a zero of $X^n - a$.

(2) If α is a zero of $X^n - a$, then we have $X^n - a = \prod_{i=0}^{n-1}(X - \zeta^i\alpha)$ and $L = \Omega_K^{X^n-a} = K(\alpha)$. For $\alpha = a = 0$, the statement of the theorem is clear, so from now on we assume $a \in K^*$. For $\tau \in \mathrm{Gal}(L/K)$, we then have $(\tau(\alpha)/\alpha)^n = (\tau(\alpha^n)/\alpha^n) = \tau(a)/a = 1$, so the map

$$\begin{aligned} \psi: \quad \mathrm{Gal}(L/K) &\longrightarrow \langle\zeta\rangle \\ \tau &\longmapsto \frac{\tau(\alpha)}{\alpha} \end{aligned}$$

is well defined. It is also a homomorphism; after all, from $\psi(\tau) = \zeta^i$ and $\psi(\tau') = \zeta^j$, we obtain

$$(\tau\tau')(\alpha) = \tau(\zeta^j\alpha) = \zeta^j\tau(\alpha) = \zeta^{i+j}(\alpha),$$

so $\psi(\tau\tau') = \zeta^{i+j} = \psi(\tau)\psi(\tau')$. The homomorphism ψ is injective because a K-automorphism that fixes α is the identity on $L = K(\alpha)$.

We conclude that $\mathrm{Gal}(L/K)$ is cyclic of degree n/d, where d is the index of $\psi[\mathrm{Gal}(L/K)]$ in $\langle\zeta\rangle$. For all $\tau \in \mathrm{Gal}(L/K)$, we then have

$$1 = \psi(\tau)^{n/d} = (\tau(\alpha)/\alpha)^{n/d} = \tau(\alpha^{n/d})/\alpha^{n/d},$$

so $b = \alpha^{n/d}$ is an element of K and $a = b^d$ is a dth power in K. If, conversely, we have $a = b^t$ with $t \mid n$ and $b \in K$, then the tth root of unity $\alpha^{n/t}/b$ is in K, and therefore so is $\alpha^{n/t}$ itself. The identity above (with $d = t$) shows that $\psi[\mathrm{Gal}(L/K)]$ is annihilated by n/t and lies in the subgroup of index t in $\langle\zeta\rangle$. Consequently, we have $t \le d$, so d is the largest divisor of n for which a is a dth power in K. □

Proof of 25.15. The equivalence of (1) and (2) is proved just as in 25.10: the set V of elements that satisfy (2) forms an extension of K that is closed under extracting roots and is contained in K^{rad}; it follows that we have $V = K^{\mathrm{rad}}$.

For (2) ⇒ (3), we first note that as in the proof of 25.10, we may assume—after if necessary extending the chain for x—that the last field E_n of the chain is normal over K. Suppose $E_{i+1} = E_i(x_i)$, with $x_i^{n_i} \in E_i$. Let ζ be a primitive root of unity of order N in $\overline{K}$, where N is a common multiple of all n_i, and take $L = E_n(\zeta)$. Then $K \subset L$ is a normal extension that admits a chain

$$K = E_0 \subset E_0(\zeta) \subset E_1(\zeta) \subset E_2(\zeta) \subset \ldots \subset E_{n-1}(\zeta) \subset E_n(\zeta) = L.$$

In this chain, the first step $E_0 \subset E_0(\zeta)$ is an abelian extension (Exercise 24.46), and the radical extensions $E_i(\zeta) \subset E_{i+1}(\zeta)$ are cyclic by 25.16.2. By looking at the corresponding chain of subgroups in $\mathrm{Gal}(L/K)$, we conclude that $\mathrm{Gal}(L/K)$ is solvable. It then follows from $\Omega_K^{f_K^x} \subset L$ that $\mathrm{Gal}(f)$, as a quotient of $\mathrm{Gal}(L/K)$, is also solvable.

For (3) ⇒ (2), let $f = f_K^x$ have a solvable Galois group $\mathrm{Gal}(f) = \mathrm{Gal}(\Omega_K^f/K)$ of order N. If ζ is again a primitive root of unity of order N, then the first step in the tower $K = E_0 \subset E_1 = K(\zeta) \subset \Omega_K^f(\zeta)$ is a radical extension. By (3), the extension $E_1 = K(\zeta) \subset \Omega_K^f(\zeta)$ can be written as a chain of cyclic extensions of degree a divisor of N. By 25.16, these cyclic extensions are radical extensions; this leads to the desired chain. □

► Unsolvable polynomials

To see that $\mathbf{Q}^{\mathrm{rad}}$ is a proper subfield of $\overline{\mathbf{Q}}$, we show that there exist polynomials in $\mathbf{Q}[X]$ whose Galois group is *not* solvable. Since S_n and its subgroups are solvable for $n < 5$, such a polynomial has degree at least 5. The group S_5 is not solvable, and there exist polynomials in $\mathbf{Q}[X]$ with group S_5.

25.17. Theorem. *Let $f \in \mathbf{Q}[X]$ be an irreducible polynomial of degree 5 with exactly three real zeros. Then we have $\mathrm{Gal}(f) \cong S_5$, and f has no zeros in $\mathbf{Q}^{\mathrm{rad}}$.*

Proof. By 24.7, the group $\mathrm{Gal}(f)$ is a subgroup of S_5 of order divisible by 5. This means that $\mathrm{Gal}(f)$ contains an element of order 5 (Cauchy's theorem); such an element in S_5 is necessarily a 5-cycle. If we view $\overline{\mathbf{Q}}$ as a subfield of $\mathbf{C}$, then complex conjugation gives an automorphism of $\Omega_{\mathbf{Q}}^f$ that, because of the assumption, interchanges two zeros of f and fixes the other three. Now, $\mathrm{Gal}(f)$ is a subgroup of S_5 that contains a 5-cycle and a 2-cycle, and such a subgroup of S_5 is equal to S_5 (Exercise 2.54). In particular, $\mathrm{Gal}(f)$ is not solvable, and by 25.15, the polynomial f has no zeros in $\mathbf{Q}^{\mathrm{rad}}$. □

Making an irreducible polynomial of degree 5 with exactly three real zeros is not that difficult. For example, if we choose

$$f = (X^2+2)\cdot(X+2)\cdot X\cdot(X-2)+2 = X^5-2X^3-8X+2,$$

then this is an Eisenstein polynomial at 2 that is made by slightly shifting a polynomial with exactly three real zeros. The polynomial f certainly has three real zeros because of $f(0)=2$ and $f(1)=-7$ and the limit values for $x\to\pm\infty$. There are not more because $f' = 5X^4-6X^2-8$ only changes sign twice.

Exercise 8. Show that $f=(X^2+3)(X^2-9)X+3$ also has group S_5.

The construction of an unsolvable polynomial of degree 5 given here can be generalized to any prime degree $p\geq 5$ (Exercise 27). There also exist several families[17] of polynomials $\{f_n\}_{n=1}^{\infty}$ with $\mathrm{Gal}(f_n)\cong S_n$.

▶ Radical formulas

It follows from the fact that S_n and its subgroups are solvable for $n\leq 4$ that the zeros of polynomials of degree at most 4 can be expressed in radicals. The most famous example of a "radical formula" is undoubtedly the "quadratic formula"

$$x_1, x_2 = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

for the zeros x_1 and x_2 of a quadratic polynomial $aX^2+bX+c\in\mathbf{R}[X]$. The formula holds not only over $\mathbf{R}$ but also over every field K of characteristic different from 2. Note that the formula in fact expresses the zeros in b/a and c/a and that we may assume $a=1$ without loss of generality. The proof of the formula by "completing the square" amounts to noticing that when expressed in the shifted variable $X+\frac{b}{2}$, the polynomial

$$X^2+bX+c = \left(X+\tfrac{b}{2}\right)^2-\tfrac{b^2-4c}{4}\in K[X]$$

loses its linear term and can be "solved" by extracting the square root of the *discriminant* b^2-4c of the polynomial X^2+bX+c.

Exercise 9. Show that this discriminant is equal to that from Exercise 24.39.

For polynomials of degree 3, the situation is more complicated. If we write the polynomial as $X^3+aX^2+bX+c\in K[X]$, then if K is not of characteristic 3, the polynomial can be expressed in the variable $Y=X+\frac{a}{3}$, giving

$$Y^3+pY+q,$$

where p and q are polynomial expressions in a, b, and c.

Exercise 10. Express p and q in a, b, and c.

Next, we can use a trick found around 1500 by the Italian Scipione del Ferro (±1465–1526). For this, write $Y = u + v$, and note that the polynomial can now be written as

$$(u+v)^3 + p(u+v) + q = u^3 + v^3 + q + (3uv + p)(u+v).$$

This expression is equal to 0 if we let u and v satisfy

$$\begin{aligned} u^3 + v^3 &= -q \\ uv &= -p/3. \end{aligned} \tag{25.18}$$

Apparently, u^3 and v^3 are zeros of the quadratic polynomial

$$(X - u^3)(X - v^3) = X^2 + qX - (p/3)^3.$$

If we moreover assume that K does not have characteristic 2, then we can express u^3 and v^3 in radicals using the quadratic formula given above, and we find

$$Y = u + v = \sqrt[3]{-q/2 + \sqrt{(q/2)^2 + (p/3)^3}} + \sqrt[3]{-q/2 - \sqrt{(q/2)^2 + (p/3)^3}}. \tag{25.19}$$

We have three choices for each of the third roots u and v of u^3 and v^3, but by (25.18), the root $v = -p/(3u)$ is fixed by the choice of u, and, as expected, we find only three zeros and not nine. See Exercise 37 for notation in terms of third roots that avoids this problem of choice.

Del Ferro did not announce his method to the world, and its publication in 1545 by his compatriot Girolamo Cardano (1501–1576) is dominated by intrigue and priority disputes.[18]

There were also mathematical problems with the solution. If we take a polynomial with three real roots, such as $Y^3 - 7Y + 6 = (Y-1)(Y-2)(Y+3)$, then the Cardano–Del Ferro formula above leads to an expression for the zeros in terms of complex conjugate numbers:

$$\frac{1}{3}\sqrt[3]{-81 + 30\sqrt{-3}} + \frac{1}{3}\sqrt[3]{-81 - 30\sqrt{-3}}.$$

Once we realize that complex numbers were unknown in the sixteenth century and only lost their mysterious halo late in the eighteenth century with Euler, the initial confusion about this *casus irreducibilis* becomes understandable.

Exercise 11. Show how the zeros 1, 2, and -3 follow from the radical representation.
[Hint: $(3 + 2\sqrt{-3})^3 = -81 + 30\sqrt{-3}$.]

The zeros of a general polynomial of degree 4 over a field of characteristic different from 2 and 3 can also be expressed in radicals using a trick. The method, which can be found in Cardano's Ars Magna, goes back to Cardano's student and son-in-law Ludovici Ferrari (1522–1565). Again, we write the general polynomial $X^4 + aX^3 + bX^2 + cX + d$ in terms of $Y = X + \frac{a}{4}$ and solve an equation of the form

$$Y^4 = pY^2 + qY + r$$

by rewriting it as

$$(Y^2+s)^2 = (p+2s)Y^2 + qY + (s^2+r). \tag{25.20}$$

Here, we choose s such that the quadratic polynomial on the right-hand side of (25.20) is the *square* of a polynomial of degree 1:

$$(Y^2+s)^2 = \left(\sqrt{p+2s}\,Y + \frac{q}{2\sqrt{p+2s}}\right)^2.$$

In order to have the constant term equal to s^2+r as in (25.20), we must choose an s that satisfies the cubic equation

$$(p+2s)(s^2+r) = q^2/4, \tag{25.21}$$

and the Cardano–Del Ferro formula gives us a radical expression for s in terms of p, q, and r. We find four values of Y by solving both quadratic equations

$$Y^2 + s = \pm\left(\sqrt{p+2s}Y + \frac{q}{2\sqrt{p+2s}}\right)$$

for a solution s of (25.21). The resulting radical formula is more impressive than practical.

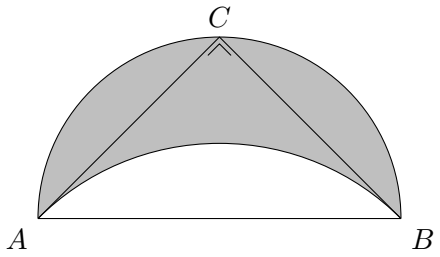
Exercise 12. How should the method be adjusted in the case $p+2s=0$?

Galois theory teaches us that the clever tricks in the Ars Magna cannot be extended to the case of degree 5 or more—not something that is immediately apparent from the manipulations given above. In the next section, we interpret the deduced radical formulas in terms of Galois theory.

See Exercise 37 for a method for the degree 4 equation that is more similar to the trick we applied in the cubic case but also fails to clarify why this method works.

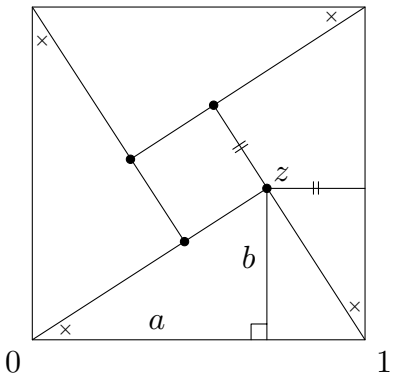
Exercises.

13. *(Construction steps)* Show that the following objects are constructible from three non-collinear points x, y, and z in the complex plane:
    a. the bisector of the line segment xy
    b. the line through x perpendicular to the line through x and y
    c. the line through z perpendicular to the line through x and y
    d. the line through z parallel to the line through x and y
    e. the circle with center z and radius $|x-y|$
    f. the bisector of the angle $\angle xyz$
    g. the circle through x, y, and z
    h. the rotation of a point around y by the angle $\angle xyz$.
14. Let AB be a diagonal of a square and C a third vertex. The *lune of Hippocrates* on ABC is the shaded area in the figure below bounded by the half-circle on AB and the quarter circle tangent to AC and BC.



Prove that the area of this lune is equal to that of the triangle ABC.

15. A figure known in Islamic architecture consists of a small square that, as shown in the figure below, lies in a large square with the same center. The length of the side of the small square is equal to the *distance* from a vertex of the square to the closest side of the large square.



Determine whether the small square is constructible from the large square.
[Hint: choose coordinates $0, 1 \in \mathbf{C}$ as in the figure, and determine $z = a + bi$.]

16. Let $X \subset \mathbf{C}$ be a subset, and suppose that z is constructible from X. Prove that x is constructible from a *finite* subset $X_0 \subset X$.

17. Let $K \subset \mathbf{C}$ be a field that maps to itself under complex conjugation. Prove that $K^{\text{quad}} \subset \mathbf{C}$ also maps to itself under complex conjugation.

18. Show that the quadratic closure K^{quad} of a field K of characteristic $\text{char}(K) \neq 2$ has no quadratic extensions.

19. Give extensions $\mathbf{Q}^{\text{quad}} \subset L$ of degree 3 and degree 5. *Does there also exist an extension of degree 4?

20. Show that trisecting the angle associated with $\alpha \in \mathbf{C}$ with $|\alpha| = 1$ with a straightedge and compass is not possible if α is transcendental.

21. Is trisecting the angles of a triangle ABC with a straightedge and compass possible
    a. when ABC is equilateral?
    b. if the lengths of the sides of ABC are equal to 44, 117, and 125?
    [Hint: $44^2 + 117^2 = 125^2$.]

22. Let K be a field of characteristic different from 2, and define $K_1 = K(\sqrt{K})$ as in 25.8. Prove: $x \in \overline{K}$ is in $K_1 \setminus K$ if and only if $K \subset K(x)$ is a finite Galois extension for which the group $G = \text{Gal}(K(x)/K)$ is abelian of exponent 2.

23. Let $x \in \mathbf{C}$ be a constructible element. Define K_i as in 25.8 for $K = K_0 = \mathbf{Q}$. Then the *root depth* of x is the smallest number $i \geq 0$ for which x is contained in K_i. Determine the root depth of the following elements:

$$\sqrt{1+\sqrt{2}}, \qquad \sqrt{3-2\sqrt{2}}, \qquad \zeta_5, \qquad \zeta_{12}, \qquad \sqrt{1+2\sqrt{-6}}.$$

Does the answer depend on the *choice* of the various roots (of unity) in $\mathbf{C}$?

24. Define real numbers $x_i \in \mathbf{R}_{\geq 0}$ recursively by $x_0 = 0$ and $x_{i+1} = \sqrt{2+x_i}$ for $i \geq 0$.
    a. Prove: $\mathbf{Q} \subset \mathbf{Q}(x_i)$ is cyclic of degree 2^i.
    b. Prove: the root depth of x_i is equal to i for all $i \geq 0$.

25. Let K be a number field. Prove: for the fields K_i in the definition 25.8 of K^{quad}, we have $K_i \neq K_{i+1}$ for all $i \geq 0$.

26. Analogously to the root depth, define the *radical depth* of a number $x \in \mathbf{Q}^{\mathrm{rad}}$, and show that the radical depth of x depends only on $\mathrm{Gal}(f^x_{\mathbf{Q}})$. *Do there exist elements of arbitrarily large radical depth?

27. Let $p = 2k+3 > 3$ be a prime, and define

$$f = (X^2+2)\textstyle\prod_{i=-k}^{k}(X-2i) + 2 \in \mathbf{Q}[X].$$

    a. Prove that f is an irreducible polynomial of degree p.
    b. Prove that f does not have $p-1$ real zeros.
    [Hint: f' is a polynomial in X^2, and the chain of $f'(0)$ is known.]
    c. Prove that f has exactly $p-2$ real zeros. Conclude that f is not solvable by radicals over $\mathbf{Q}$.

28. Give a chain $\mathbf{Q} = E_0 \subset E_1 \subset \cdots \subset E_n$ of *irreducible* radical extensions with $\zeta_{47} \in E_n$. Here, ζ_{47} is a primitive 47th root of unity.

29. Express the real number $x = \cos(2\pi/7)$ in irreducible radicals over $\mathbf{Q}$.

30. Show that every extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_n)$ is solvable by *irreducible* radicals.
[Hint: induction on n.]

31. Let K be a field of characteristic 0 and x an element of $K^{\mathrm{rad}} \subset \overline{K}$. Prove: there exist an $n \in \mathbf{Z}_{\geq 0}$ and a chain of fields

$$K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_{n-1} \subset E_n \subset \overline{K}$$

with $x \in E_n$ and $E_{i-1} \subset E_i$ for $1 \leq i \leq n$ an *irreducible* radical extension.

32. *(Artin–Schreier radicals)* Let K be a field of characteristic $p > 0$ and $K \subset L$ a cyclic extension of degree p. Prove: we have $L = K(\alpha)$ for a zero α of an Artin–Schreier polynomial $f = X^p - X - a \in K[X]$.
[This is the analog of 25.16.1 for $n = p = \mathrm{char}(K)$. Hint: look at the resolvent $\sum_{i=0}^{p-1} i\sigma^i(x)$ for an element $x \in L$ with trace 1.]

33. Let K be a field of characteristic $p > 0$ and $K \subset L$ the extension obtained by adjoining the zeros of the Artin–Schreier polynomial $f = X^p - X - a \in K[X]$ to K. Prove: $K \subset L$ is a cyclic extension of degree 1 or p.
[This is the analog of 25.16.2 for $n = p = \mathrm{char}(K)$. Hint: Exercise 22.30.]

34. Let K be a field of characteristic $p > 0$. The radical closure of K is defined as in 25.13, except that K_i is now obtained from K_{i-1} by adjoining all $w \in \overline{K}$ that satisfy exactly one of the following conditions:
    1. We have $w^n \in K_{i-1}$ for some $n \geq 1$ with $p \nmid n$.
    2. We have $w^p - w \in K_{i-1}$ (informally: w is an Artin–Schreier radical over K).

    Formulate and prove the analog of 25.15 for K.

35. Determine the real solutions of the equation $X^3 = 15X + 4$ using the Cardano–Del Ferro formula.
    [This feat was accomplished by Bombelli in 1572.]

36. Let K be a field with $\mathrm{char}(K) \neq 2, 3$. Show that $Y = \xi\eta(\xi+\eta)$ is a zero of $Y^3+pY+q \in K[Y]$ if ξ and η satisfy
$$\xi^3, \eta^3 = \frac{3q}{2p} \pm \sqrt{\left(\frac{3q}{2p}\right)^2 + \frac{p}{3}}.$$
    Why does this not give nine distinct zeros?
    [Hint: Write $u = \xi^2\eta$ and $v = \xi\eta^2$ in 25.19. This is Cayley's version of the Cardano–Del Ferro formula.]

37. Let K be as in the previous exercise. Show that the degree 4 equation $Y^4 = pY^2+qY+r$ over K has solution $Y = \frac{1}{2}(u + v + w)$ if u^2, v^2, and w^2 are zeros of the cubic resolvent
$$X^3 - 2pX^2 + (p^2 + 4r)X - q^2$$
    and the signs of u, v, and w are chosen such that we have $uvw = q$.

38. Show that the field E_n in 25.10.2 can be chosen such that we have $E_n = K(x)$.

39. Let $F_k = 2^{2^k} + 1$ for $k \in \mathbf{Z}_{\geq 0}$ be the kth Fermat number.
    a. Prove: for $k \in \mathbf{Z}_{\geq 0}$, we have $F_k = 2 + \prod_{i<k} F_i$, and any two distinct Fermat numbers are relatively prime.
    b. Let $S = \{1, 3, 5, 15, \ldots\}$ be the set of integers that can be written as a product of distinct Fermat numbers. Write the first nine elements of S in base 2. What stands out when you compare your result to Pascal's triangle? Give a precise formulation and proof of this observation.

40. Determine all $n \in \mathbf{Z}_{\geq 3}$ for which a regular n-gon, a regular $n+1$-gon, and a regular $n+2$-gon are all constructible.

41. Let $k \in \mathbf{Z}_{\geq 0}$, and let p be a prime factor of F_k.
    a. Prove: the order of $(2 \bmod p)$ in the group $\mathbf{F}_p^*$ is equal to 2^{k+1}, and for $k \geq 2$, the order of $(F_{k-1} \bmod p)$ in $\mathbf{F}_p^*$ is equal to 2^{k+2}.
    b. Prove: for $k \geq 2$, we have $p \equiv 1 \bmod 2^{k+2}$.

42. Let $\mathbf{F}$ be a finite field. Prove that the following two statements are equivalent:
    a. For any two subgroups A and B of $\mathbf{F}^*$, we have $A \subset B$ or $B \subset A$.
    b. Either $\#\mathbf{F}$ is equal to 2, 9, or a Fermat prime, or $\#\mathbf{F} - 1$ is a Mersenne prime.

43. For a group G and $k \in \mathbf{Z}_{\geq 0}$, we define the subgroup $G^{(k)}$ of G recursively by
$$G^{(0)} = G \qquad \text{and} \qquad G^{(k+1)} = [G^{(k)}, G^{(k)}].$$

We call G *solvable* if there is a finite chain of subgroups $G = H_0 \supset H_1 \supset \ldots \supset H_k = \{e\}$ of G such that for every $i > 0$, the group H_i is normal in H_{i-1} with H_{i-1}/H_i abelian.

a. Prove that for finite G, the definition given above is equivalent to Definition 10.14 in the syllabus Algebra 1.
b. Let G be a group and N a normal subgroup of G. Prove: G is solvable $\Leftrightarrow$ every subgroup of G is solvable $\Leftrightarrow$ N and G/N are both solvable $\Leftrightarrow$ there exists a $k \in \mathbf{Z}_{\geq 0}$ with $G^{(k)} = \{e\}$ $\Leftrightarrow$ there exists a finite chain of subgroups $G = H_0 \supset H_1 \supset \ldots \supset H_k = \{e\}$ of G that are all normal in G with H_{i-1}/H_i abelian for all $i > 0$.

44. Let I be a set, G_i a solvable group for every $i \in I$, and $G = \prod_{i \in I} G_i$.

a. Prove: if I is finite, then G is solvable.
b. Is G solvable in general? Give a proof or a counterexample.

45. Let $K \subset L$ be a *cyclic* Galois extension with group $\langle \sigma \rangle$, and let $\alpha \in L^*$. Prove:

$$N_{L/K}(\alpha) = 1 \qquad \Longleftrightarrow \qquad \text{there exists a } \beta \in L^* \text{ with } \alpha = \sigma(\beta)/\beta.$$

[Hint for $\Longrightarrow$: imitate the construction of the Lagrange resolvent.]

The theorem in the previous exercise is called *Hilbert's Theorem 90*, after Satz 90 from the *Zahlbericht* (1897) of David Hilbert (1862–1943). The more general theorem in the next exercise is also called Hilbert's Theorem 90.

46. Let $K \subset L$ be a finite Galois extension with group G, and let $c : G \to L$ be a map.

a. Prove: for all σ, $\tau \in G$, we have $c(\sigma\tau) = c(\sigma) \cdot \sigma(c(\tau))$ if and only if there exists a $\beta \in L^*$ such that for every $\sigma \in G$, we have $c(\sigma) = \sigma(\beta)/\beta$.
b. Show how the previous exercise follows from part (a).

26 Applications of Galois theory

Galois theory is a useful tool that can be utilized in many situations. Nowadays, ideas about the invariance of "symmetric expressions" are common in mathematics, and there also exists, for example, a Galois theory of differential equations.[19] This section gives several unrelated examples and also shows how certain expressions that are rational according to Galois theory can be calculated explicitly.

▶ Fundamental theorem of algebra

As a first application, we prove the fundamental theorem of algebra mentioned in 21.11, which says that the field $\mathbf{C}$ of complex numbers is algebraically closed. There are many proofs, which all use certain "topological arguments." This is not surprising because the construction of $\mathbf{R}$ from $\mathbf{Q}$ using Dedekind cuts or Cauchy sequences is more a topological construction than an algebraic one, and unlike $\mathbf{C} = \mathbf{R}(i)$, the field $\mathbf{Q}(i)$ is not algebraically closed. As a topological argument, we use the *intermediate value theorem* for polynomials in $\mathbf{R}[X]$: a polynomial $f \in \mathbf{R}[X]$ that takes on both a positive and a negative value has a real zero.

26.1. Lemma. *Every polynomial $f \in \mathbf{R}[X]$ of odd degree has a real zero. For every field extension $\mathbf{R} \subset E$ of odd degree, we have $E = \mathbf{R}$.*

Proof. For $f \in \mathbf{R}[X]$ of odd degree, the values $f(x)$ and $f(-x)$ have opposite signs for sufficiently large x; by the intermediate value theorem, f then has a real zero.

For $\mathbf{R} \subset E$ of odd degree and $\alpha \in E$, the degree $[\mathbf{R}(\alpha) : \mathbf{R}]$, as a divisor of $[E : \mathbf{R}]$, is also odd. Now, $f_{\mathbf{R}}^{\alpha}$ is an irreducible polynomial of odd degree. Because it has a zero in $\mathbf{R}$, the polynomial $f_{\mathbf{R}}^{\alpha}$ is of degree 1. We find $\alpha \in \mathbf{R}$ and $E = \mathbf{R}$. □

26.2. Lemma. *There is no field extension $\mathbf{C} \subset E$ with $[E : \mathbf{C}] = 2$.*

Proof. To show that $\mathbf{C}$ does not have any quadratic extensions, it suffices to show that every element $x \in \mathbf{C}$ has a square root in $\mathbf{C}$. If we write $x = s + it$ with $s, t \in \mathbf{R}$, then solving the equation $x = s + it = (c + di)^2$ amounts to finding $c, d \in \mathbf{R}$ with

$$\begin{aligned} c^2 - d^2 &= s \\ 2cd &= t. \end{aligned}$$

For $t = 0$, the value $x = s$ is real and we find $cd = 0$. For $x = s \geq 0$, we then take $d = 0$ and $c = \sqrt{x}$ the real square root of x; for $x = s < 0$, we take $c = 0$ and $d = \sqrt{-x}$ the real square root of $-x$.

For $t \neq 0$, we substitute $d = t/(2c)$ in the first equation, which gives $4c^4 - 4sc^2 - t^2 = 0$. Because the polynomial $4X^4 - 4sX^2 - t^2$ is negative for $X = 0$ and positive for large X, the intermediate value theorem implies that there indeed exists a real zero c of this polynomial. This leads to the desired square root. □

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

Proof. We must prove that $\mathbf{C}$ has no non-trivial algebraic extensions. Let $\mathbf{C} \subset L$ be finite algebraic, and let M be the normal closure of L over $\mathbf{R}$. Then $\mathbf{R} \subset M$ is a finite Galois extension, say with group G. If H is a 2-Sylow subgroup of G in the sense of 10.7, then the field of invariants $E = M^H$ of H is an extension of $\mathbf{R}$ whose degree $[E : \mathbf{R}] = [G : H]$ is odd. By 26.1, we get $E = \mathbf{R}$ and $G = H$, so G is a 2-group. In particular, the subgroup $\mathrm{Gal}(M/\mathbf{C}) \subset G$ is a 2-group. By 10.17, the group $\mathrm{Gal}(M/\mathbf{C})$ is therefore *solvable*. As in 10.14, this means that there exists a chain

$$\mathrm{Gal}(M/\mathbf{C}) = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_k = 1$$

in which each H_{i+1} is a subgroup of index 2 in H_i. Under the Galois correspondence, this gives a chain $\mathbf{C} = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_k = M$ of quadratic field extensions. By 26.2, this chain has length $k = 0$, so $M = L = \mathbf{C}$. □

▶ Quadratic reciprocity

The calculation of the quadratic subfield of $\mathbf{Q}(\zeta_p)$ for prime p carried out in 24.12 allows us to explain a surprising symmetry in the "quadratic character" of primes modulo one another. We already came across a consequence of this phenomenon in Exercises 7.19 and 12.22: if 5 is a primitive root modulo p, then we have $p \equiv \pm 2 \bmod 5$.

If p is an odd prime, then $\mathbf{F}_p^*$ is a cyclic group of even order $p - 1$. The unique subgroup $S_p \subset \mathbf{F}_p^*$ of index 2 consists of the *remainders of squares* modulo p. It is the kernel of the composed homomorphism

$$\begin{array}{rcl} \mathbf{F}_p^* & \longrightarrow & \langle -1 \bmod p \rangle \quad \xrightarrow{\sim} \{\pm 1\} \\ x \bmod p & \longmapsto & x^{(p-1)/2} \bmod p \longmapsto \left(\dfrac{x}{p}\right). \end{array}$$

The symbol $\left(\frac{x}{p}\right)$, which lives in characteristic 0, is the *Legendre symbol* of x modulo p: it is 1 if x is a square in $\mathbf{F}_p^*$ and -1 if x is not a square in $\mathbf{F}_p^*$. There does not seem to be any symmetry in x and p in the definition of $\left(\frac{x}{p}\right)$; nevertheless, around 1744, using numerical examples, Euler discovered a variant of the following result.

26.4. Quadratic reciprocity law. *Let p and q be distinct odd primes. Then we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

In words: if p and q are not both 3 mod 4, then the symbol $\left(\frac{p}{q}\right)$ can be flipped "upside down." For $p \equiv q \equiv 3 \bmod 4$, the sign changes.

Euler was not able to prove this result, and his French colleague Legendre (1752–1833), whose name is attached to the quadratic symbols, mistakenly denied that his own proof published in 1785 was incomplete. Gauss found the first correct proof of 26.4 in 1796 and later gave several "different" proofs of his *theorema aureum*.

Proof. From 24.10 and 24.12, we know that $\mathbf{Q}(\zeta_p)$ is a Galois extension of $\mathbf{Q}$ with group $(\mathbf{Z}/p\mathbf{Z})^* = \mathbf{F}_p^*$ and that the subgroup $S_p \subset \mathbf{F}_p^*$ of squares corresponds with the intermediate field $\mathbf{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$. This gives

$$\left(\frac{q}{p}\right) = 1 \iff (q \bmod p) \in S_p \iff \sigma_q(\sqrt{p^*}) = \sqrt{p^*}.$$

The automorphism σ_q is a type of "lift to characteristic 0" of the Frobenius automorphism F_q on $\overline{\mathbf{F}}_q$. More precisely, if ζ is a primitive pth root of unity in an algebraic closure $\overline{\mathbf{F}}_q$ of $\mathbf{F}_q$, then the reduction map $\mathbf{Z} \to \mathbf{F}_q$ has an extension

$$\begin{array}{rccc} r: & \mathbf{Z}[\zeta_p] & \longrightarrow & \overline{\mathbf{F}}_q \\ & \sum_i a_i\zeta_p^i & \longmapsto & \displaystyle\sum_i \overline{a}_i\zeta^i \end{array}$$

that satisfies $r \circ \sigma_q = F_q \circ r$. The homomorphism r sends the quadratic Gauss sum $\tau_p = \sqrt{p^*} \in \mathbf{Z}[\zeta_p]$ to a zero $w = r(\sqrt{p^*})$ of $X^2 - p^* \in \mathbf{F}_q[X]$. The zeros of $X^2 - p^*$ in $\overline{\mathbf{F}}_q$ are distinct, so σ_q leaves $\sqrt{p^*}$ invariant if and only if F_q leaves the element w invariant. We now have

$$F_q(w) = w \iff w^{q-1} = 1 \iff (p^* \bmod q)^{(q-1)/2} = 1 \iff \left(\frac{p^*}{q}\right) = 1,$$

and we find

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right). \qquad \square$$

Exercise 1. Prove: if 5 is a primitive root modulo a prime $p \neq 2$, then we have $p \equiv \pm 2 \bmod 5$.

▶ Symmetric polynomials

In the main theorem 14.1 for symmetric polynomials, we saw that for $n \in \mathbf{Z}_{\geq 1}$, the "symmetric expressions" in the zeros of the general polynomial

$$F_n = (X - T_1)(X - T_2)\ldots(X - T_n) = X^n + \sum_{k=1}^{n}(-1)^k s_k X^{n-k}$$

of degree n can be written as polynomial expressions in the elementary symmetric polynomials

$$s_k = \sum_{1 \leq i_1 < i_2 < \ldots i_k \leq n} T_{i_1}T_{i_2}\ldots T_{i_k} \in \mathbf{Z}[T_1, T_2, \ldots, T_n]$$

that form the coefficients of that polynomial. Somewhat more precisely, under the natural action of the symmetric group S_n on the ring $\mathbf{Z}[T_1, T_2, \ldots, T_n]$ of polynomials over $\mathbf{Z}$ in the n variables $T_1, T_2, \ldots, T_n$ given by

$$(\sigma f)(T_1, T_2, \ldots, T_n) = f(T_{\sigma(1)}, T_{\sigma(2)}, \ldots, T_{\sigma(n)}) \qquad \text{for } f \in R \text{ and } \sigma \in S_n,$$

the ring of invariants is equal to $\mathbf{Z}[s_1, s_2, \ldots, s_n]$. There is a Galois-theoretic formulation of this result, in terms of the fields of fractions of both rings, and also of the definition of the sign map given in 2.9.

26.5. Theorem. *For every $n \in \mathbf{Z}_{\geq 1}$, the field $\mathbf{Q}(T_1, \ldots, T_n)$ is the splitting field of the general polynomial F_n of degree n over $\mathbf{Q}(s_1, \ldots, s_n)$. The extension*

$$K = \mathbf{Q}(s_1, \ldots, s_n) \subset L = \mathbf{Q}(T_1, \ldots, T_n)$$

is Galois with group $S_n = S(\{T_1, T_2, \ldots, T_n\})$. Over K, the polynomial

$$\delta_n = \prod_{1 \leq i < j \leq n} (T_i - T_j) \in L$$

generates the subfield of L that is invariant under the alternating group A_n.

Proof. Over $K = \mathbf{Q}(s_1, \ldots, s_n)$, the splitting field of the general polynomial $F_n \in K[X]$ of degree n is equal to $L = \mathbf{Q}(T_1, \ldots, T_n)$, so $K \subset L$ is Galois. Because all permutations of the n different zeros of F_n lead to field automorphisms of L over K, it follows that $\mathrm{Gal}(L/K)$ is the entire permutation group S_n of the zero set $\{T_1, T_2, \ldots, T_n\}$.

In 2.9, we used the polynomial δ_n to *define* the sign map $\varepsilon : S_n \to \{\pm 1\}$ by setting $\sigma(\delta_n) = \varepsilon(\sigma) \cdot \delta_n$. The stabilizer of δ_n under the action of S_n is therefore equal to A_n, and $K(\delta_n)$ is the field of invariants L^{A_n}. □

In 14.4, we came across the square of the polynomial δ_n, which is contained in K because it is a symmetric function, as the *discriminant*

$$\delta_n^2 = \Delta_n = \prod_{1 \leq i < j \leq n} (T_i - T_j)^2$$

of the general polynomial F_n of degree n. We can express Δ_n as a polynomial in the elementary symmetric functions $s_1, s_2, \ldots, s_n$ using the method of §14.

▶ Radical formulas in degrees 3 and 4

In terms of 26.5, we can deduce the radical formulas from Section 25 for degree 3 and degree 4 equations without resorting to unexpected clever tricks. After all, for $n \leq 4$, the extension $K \subset L$ in 26.5 is a solvable extension, and as in 25.15, the elements $T_i \in L$ can be obtained as elements in a tower of radical extensions. As a first step in the tower, we can take the extension $K \subset K(\delta_n) = K(\sqrt{\Delta_n})$. By 26.5, the extension $K(\delta_n) \subset L$ is Galois with group A_n.

In the cubic case $n = 3$, the field $L = \mathbf{Q}(T_1, T_2, T_3)$ is cyclic of degree 3 over the quadratic extension of $K = \mathbf{Q}(s_1, s_2, s_3)$ generated by

$$\begin{aligned} \delta_3 = \sqrt{\Delta_3} &= (T_1 - T_2)(T_1 - T_3)(T_2 - T_3) \\ &= (T_1^2 T_2 + T_1 T_3^2 + T_2^2 T_3) - (T_1^2 T_3 + T_1 T_2^2 + T_2 T_3^2). \end{aligned}$$

To obtain a radical expression for T_1 over $K(\delta_3)$, we adjoin a primitive third root of unity $\zeta_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ to $K(\delta_3)$, and as in 25.16, we form both Lagrange resolvents $U, V \in L(\zeta_3)$ from T_1:

$$\begin{aligned} U &= T_1 + \zeta_3 T_2 + \zeta_3^2 T_3 \\ V &= T_1 + \zeta_3^2 T_2 + \zeta_3 T_3. \end{aligned}$$

In terms of these resolvents and $s_1 = T_1 + T_2 + T_3 \in K$, we now have the expressions

$$\begin{aligned} T_1 &= \frac{1}{3}(s_1 + U + V) \\ T_2 &= \frac{1}{3}(s_1 + \zeta_3^2 U + \zeta_3 V) \\ T_3 &= \frac{1}{3}(s_1 + \zeta_3 U + \zeta_3^2 V) \end{aligned} \tag{26.6}$$

because the three third roots of unity add up to $1 + \zeta_3 + \zeta_3^2 = 0$.

Exercise 2. Why do we have $UV \in K$? Express UV in s_1, s_2, s_3.

The elements U^3 and V^3 are in $K(\delta_3, \zeta_3) = K(\sqrt{\Delta_3}, \sqrt{-3})$, and even in $K(\sqrt{-3\Delta_3})$ because the Lagrange resolvents U and V are invariant under the K-automorphism of $L(\zeta_3)$ of order 2 that both interchanges T_2 and T_3 and squares ζ_3. A short calculation now gives

$$U^3, V^3 = \left(s_1^3 - \frac{9}{2}s_1 s_2 + \frac{27}{2}s_3\right) \pm \frac{3}{2}\sqrt{-3\Delta_3}.$$

If we explicitly substitute the third roots of unity for U and V in 26.6, we obtain a radical formula for the T_i in terms of the s_i.

Exercise 3. How does the radical formula (25.19) follow from the obtained formula?

In degree 4, we can also express the zeros of F_4 using radicals.

Exercises.

See the next version of this syllabus.

27 Categories and functors

Much "conceptual mathematics" can be formulated succinctly and precisely in terms of categories and functors. This is more an efficient use of language than a theory in itself, and the arguments sometimes jokingly called "abstract nonsense" are an outstanding embodiment of the faith in clarity and greater applicability through *abstraction* already professed in Section 1. Categorical notions are justified by the large number of concrete examples they have in all parts of mathematics, and knowing such examples facilitates many people's appreciation of categorical abstractions. The mathematical content of this section consists mostly of many examples. The reader should feel free to replace any unappealing example with a better one.

▶ Categories

27.1. Definition. *A category $\mathcal{C}$ consists of objects and, for every ordered pair of objects A, B in $\mathcal{C}$, a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of morphisms from A to B. For any triple of objects A, B, and C in $\mathcal{C}$, there is, moreover, a composition map of morphisms*

$$\begin{aligned} \mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) &\longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, C) \\ (f, g) &\longmapsto g \circ f \end{aligned}$$

such that the following two conditions are satisfied:

1. *For every $A \in \mathcal{C}$, the set $\mathrm{Hom}_{\mathcal{C}}(A, A)$ contains an identity id_A that acts as a unit with respect to composition.*
2. *For morphisms $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, we have $(h \circ g) \circ f = h \circ (g \circ f)$.*

Following the notation used in 27.1.2, the *morphisms* in $\mathcal{C}$ are also called the *arrows* or *maps* in $\mathcal{C}$. Note, however, that elements are not mentioned in the definition of a category; we do not assume by definition that morphisms are maps between sets, or even that objects consist of elements. We also do not rule out that the set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ may be the empty set for some A and B. When the underlying category is clear, we usually write $\mathrm{Hom}(A, B)$ for $\mathrm{Hom}_{\mathcal{C}}(A, B)$.

To avoid set-theoretic paradoxes such as "the set of all sets," we do not require the objects of $\mathcal{C}$ to form a set. They form a *class* in the sense of set theory. We will not further discuss such logical subtleties, which are generally avoided by working in a suitable *universe* with so-called *small categories*.

The existence of an identity for every object allows us to speak of inverses of morphisms and, therefore, of *isomorphisms* (morphisms with a two-sided inverse). Morphisms in $\mathrm{End}(A) = \mathrm{Hom}(A, A)$ are called *endomorphisms* of A, isomorphisms in $\mathrm{Hom}(A, A)$ are called *automorphisms* of A. On the set $\mathrm{Aut}(A) \subset \mathrm{End}(A)$ of automorphisms of A, composition forms a group operation, and $\mathrm{Aut}(A)$ is called the *automorphism group* of A.

Exercise 1. Verify that the morphisms in $\mathrm{Aut}(A)$ form a group under composition.

A category is often referred to in terms of the objects, for example "the category **Ab** of abelian groups" or "the category $\mathbf{Mod}_R$ of R-modules." The reader must then

understand that the morphisms in the category are the "corresponding" maps. In the case of **Ab**, these are group homomorphisms; in the case of $\mathbf{Mod}_R$, they are R-module homomorphisms.

The category **Ab** is, in an obvious way, a *subcategory* of the category **Grp** of all groups. More generally, a category $\mathcal{C}$ is called a subcategory of $\mathcal{D}$ if the objects in $\mathcal{C}$ are also objects in $\mathcal{D}$ and for every ordered pair of objects A, B in $\mathcal{C}$, there is an inclusion $\mathrm{Hom}_{\mathcal{C}}(A,B) \subset \mathrm{Hom}_{\mathcal{D}}(A,B)$. If we always have $\mathrm{Hom}_{\mathcal{C}}(A,B) = \mathrm{Hom}_{\mathcal{D}}(A,B)$, then $\mathcal{C}$ is called a *full subcategory* of $\mathcal{D}$.

27.2. Examples. Before continuing, let us mention some of the countless examples. It can be expanded in various directions, depending on personal taste.

1. The category **Sets** of sets with the "usual" maps as morphisms is a standard example of a category. The subcategory **FSets** of finite sets is a full subcategory of **Sets**. For every group G, we have the category G**-sets** of G-sets in the sense of Definition 5.1. The morphisms in G**-sets** are the G-equivariant maps from Exercise 5.31.

2. The category **Grp** of groups with the group homomorphisms as morphisms contains the category **Ab** of abelian groups as a full subcategory. Likewise, we have **Rng** for rings and ring homomorphisms, with a full subcategory **CRng** of commutative rings. These are "large" categories; people often work in smaller subcategories such as the categories of *finite* abelian groups or *noetherian* rings.

3. The category $\mathbf{Vec}_K$ of vector spaces over a field K has the K-linear maps as morphisms. There is the full subcategory $\mathbf{FVec}_K$ of finite-dimensional K-vector spaces.

4. The modules over a ring R, together with the R-homomorphisms, form a category $\mathbf{Mod}_R$. Many of the "standard constructions" we introduced in Sections 16 and 17 for R-modules (quotients, homomorphism and isomorphism theorem, fibered sums and products) can be carried out purely categorically in so-called *abelian categories*, of which $\mathbf{Mod}_R$ is the generic example.

If R is the group ring $R = K[G]$ of a group G over a field K, then $\mathbf{Mod}_R = \mathbf{Rep}_K(G)$ is the category of K-representations of G. Here, the module homomorphisms are the K-linear maps that respect the G-action in the sense that they are G-equivariant (verify!).

5. The category **Top** of topological spaces has the continuous maps as morphisms. People often work in a full subcategory of topological spaces that have one or more additional properties (connected, Hausdorff, metric, compact, ...). The topology $\mathbf{T}_X$ on a space X is itself also a category. The objects of $\mathbf{T}_X$ are the open sets in X, the morphisms are the inclusions of open sets.

6. For any category $\mathcal{C}$, we can define the *opposite category* $\mathcal{C}^{\mathrm{opp}}$ by "reversing all arrows." More precisely, $\mathcal{C}^{\mathrm{opp}}$ has the same objects as $\mathcal{C}$, and the set of morphisms $\mathrm{Hom}_{\mathcal{C}^{\mathrm{opp}}}(A,B)$ is in bijection with $\mathrm{Hom}_{\mathcal{C}}(B,A)$, say by $f^{\mathrm{opp}} \leftrightarrow f$. The composition of morphisms in $\mathcal{C}^{\mathrm{opp}}$ is then defined by $f^{\mathrm{opp}} \circ g^{\mathrm{opp}} = (g \circ f)^{\mathrm{opp}}$.

As can be seen in the examples above, the sets $\mathrm{Hom}_{\mathcal{C}}(A,B)$ sometimes inherit extra structure from $\mathcal{C}$. For $\mathcal{C} = \mathbf{Ab}$, the group $\mathrm{Hom}_{\mathcal{C}}(A,B)$ is abelian (Exercise 4.41); for

$\mathcal{C} = \mathbf{Mod}_R$, if the ring R is commutative, every abelian group $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is naturally an R-module (Exercise 16.3).

Exercise 2. Show that in both situations above, $\mathrm{End}(A)$ has a natural *ring* structure with group of units $\mathrm{Aut}(A)$. Is this ring necessarily commutative?

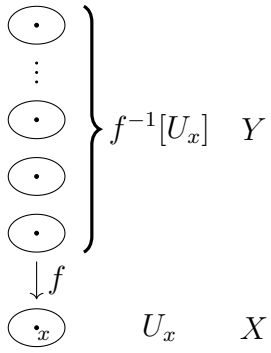
The morphisms in a category $\mathcal{C}$ themselves also form a category, $\mathbf{Mor}(\mathcal{C})$. A morphism $\phi : f \to g$ in $\mathbf{Mor}(\mathcal{C})$ from $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ to $g \in \mathrm{Hom}_{\mathcal{C}}(C, D)$ is an ordered pair $\phi = (\phi_1, \phi_2)$ of morphisms in $\mathcal{C}$ such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\phi_1} & C \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ B & \xrightarrow{\phi_2} & D \end{array}$$

commutes. Also often interesting are the subcategories of $\mathbf{Mor}(\mathcal{C})$ obtained by considering morphisms to or from a fixed object in $\mathcal{C}$. In the first case, we fix $A = C$ in the diagram above and consider only the morphisms $\phi = (\phi_1, \phi_2)$ in $\mathbf{Mor}(\mathcal{C})$ with $\phi_1 = \mathrm{id}_A$. In the second case, we fix $B = D$ and take the morphisms $\phi = (\phi_1, \phi_2)$ with $\phi_2 = \mathrm{id}_B$. This type of category is sometimes called the category of objects over a fixed base object.

27.3. Examples. For every commutative ring R, we can view the category $\mathbf{CAlg}_R$ of commutative R-algebras as the category of "rings over R." After all, a morphism of R-algebras $A_1 \to A_2$ respects the R-algebra structure and is consequently a morphism of the structure maps $f_i : R \to A_i$ in $\mathbf{CRng}$ that is the identity on R.

An interesting example in the topology of objects over a fixed base object is given by the category $\mathbf{Cov}_X$ of *covers* of a topological space X. A map $f : Y \to X$ of topological spaces is called a *cover* if every point $x \in X$ has a neighborhood $U_x \subset X$ such that $f^{-1}[U_x] \xrightarrow{f} U_x$ is a *trivial cover*. This means that the *fiber* $f^{-1}(x)$ over x is discrete in Y and that there is a homeomorphism $f^{-1}(x) \times U_x \to f^{-1}[U_x]$ that gives the projection onto the second coordinate when composed with f. A morphism ϕ from a cover $f_1 : Y_1 \to X$ to $f_2 : Y_2 \to X$ (a *covering transformation*) is a continuous map $\phi : Y_1 \to Y_2$ with $f_2 \circ \phi = f_1$.



▶ Functors

27.4. Definition. *A (covariant) functor $F : \mathcal{C} \to \mathcal{D}$ is a map that takes an object $A \in \mathcal{C}$ to an object $F(A) \in \mathcal{D}$ and a morphism $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ to a morphism $f_* = F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$. Here, we have $(\mathrm{id}_A)_* = \mathrm{id}_{F(A)}$ and $(f \circ g)_* = f_* \circ g_*$.*

For short, the construction of $F(A) \in \mathcal{D}$ from $A \in \mathcal{C}$ is often called "functorial." Such a construction has many pleasant "stability properties" that make functorial concepts considerably more manageable than non-functorial ones.

27.5. Examples. 1. The formation of the commutator subgroup $[G, G]$ of a group G is a functor $\mathbf{Grp} \to \mathbf{Grp}$. The functor $G \mapsto G^{\mathrm{ab}} = G/[G, G]$ that takes any group to its abelianized quotient is a functor $\mathbf{Grp} \to \mathbf{Ab}$. The formation of the center $Z(G)$ of G is *not* a functor $\mathbf{Grp} \to \mathbf{Ab}$ because a group homomorphism $f : G_1 \to G_2$ does not, in general, induce a group homomorphism between the centers.

2. The "group of units functor" $U : \mathbf{Rng} \to \mathbf{Grp}$ takes a ring R to the group of units R^*. For every $n \geq 1$, there are functors $\mathrm{GL}_n : \mathbf{CRng} \to \mathbf{Grp}$ and $\mathrm{Mat}_n : \mathbf{CRng} \to \mathbf{Rng}$ that take a commutative ring R to the group $\mathrm{GL}_n(R)$ of invertible $n \times n$ matrices and to the ring $\mathrm{Mat}_n(R)$ of $n \times n$ matrices with coefficients in R, respectively.

Note that GL_1 and U are "the same" functor.

3. The map $\mathbf{CRng} \to \mathbf{CRng}$ that takes any commutative ring R to the *reduced ring* R/N_R, with N_R the nilradical of R, is a functor. On the subcategory of reduced rings, it is the identity.

4. A *forgetful functor* is a functor that forgets part of an object's structure. For example, there are forgetful functors from most categories mentioned in 27.2 to **Sets** that take a group (ring, vector space, etc.) to the underlying set. The functors from **Rng** and $\mathbf{Vec}_K$ to **Ab** that take a ring or vector space to the underlying abelian additive group, and the functors $\mathbf{Rep}_K(G) \to \mathbf{Vec}_K$ and G-**sets**→**Sets** that forget the G-action, are of the same nature.

5. The formation of the fundamental group $\pi(X)$ of a topological space is *not* a functor $\mathbf{Top} \to \mathbf{Grp}$, not even if we restrict ourselves to path-connected spaces. Let us introduce the category $\mathbf{Top}_*$ of topological spaces X with basepoint $x \in X$ and define a morphism $(X, x) \to (Y, y)$ to be a continuous map $f : X \to Y$ with $f(x) = y$. Note that $\mathbf{Top}_*$ is nothing but the category of "topological spaces over a singleton" in the sense of the second example in 27.3. The formation $(X, x) \mapsto \pi(X, x)$ of the fundamental group with respect to the basepoint x is now a functor $\mathbf{Top}_* \to \mathbf{Grp}$.

6. In every category $\mathcal{C}$, an object $X \in \mathcal{C}$ leads to a *representation functor* $\mathrm{Hom}_{\mathcal{C}}(X, -) : \mathcal{C} \to \mathbf{Sets}$ given by $A \mapsto \mathrm{Hom}(X, A)$. There is also something like a "functor" $\mathrm{Hom}_{\mathcal{C}}(-, X)$ to **Sets**, but this is not a functor in the sense of 27.4 because all arrows are "reversed."

27.6. Definition. *A contravariant functor $F : \mathcal{C} \to \mathcal{D}$ is a map that takes an object $A \in \mathcal{C}$ to an object $F(A) \in \mathcal{D}$ and a morphism $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ to a morphism $f^* = F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(B), F(A))$. Here, we have $(\mathrm{id}_A)^* = \mathrm{id}_{F(A)}$ and $(f \circ g)^* = g^* \circ f^*$.*

27.7. Examples. As we have already seen, the representation functors $\mathrm{Hom}_{\mathcal{C}}(-, X)$ in any category $\mathcal{C}$ are contravariant. Special cases of such functors are several *duality functors* such as $M \mapsto M^* = \mathrm{Hom}_R(M, R)$ for the category $\mathbf{Mod}_R$ of modules over R, or the functor $A \mapsto A^\vee = \mathrm{Hom}(A, \mathbf{Q}/\mathbf{Z})$ on **Ab**.

Slightly more generally, for many categories $\mathcal{C}$, there are contravariant functors that take $A \in \mathcal{C}$ to a set of "R-valued functions on A." Here, R is generally a well-chosen ring, so that the set of R-valued functions inherits additional structure from R. An example is the set $C(X)$ of continuous real-valued functions on a topological space X, which inherits a *ring structure* from $\mathbf{R}$ via the usual pointwise operations.

Exercise 3. Show that the "identity" $\mathcal{C} \to \mathcal{C}^{\mathrm{opp}}$ is a contravariant functor and that the contravariant functors $F : \mathcal{C} \to \mathcal{D}$ correspond bijectively to the functors $F : \mathcal{C} \to \mathcal{D}^{\mathrm{opp}}$.

In category theory, the definition of the objects if always inextricably linked to a definition of morphisms of such objects. The set $\mathbf{Fun}(\mathcal{C}, \mathcal{D})$ of functors $\mathcal{C} \to \mathcal{D}$ itself, in turn, becomes a category if we define *morphisms of functors*, also called *natural transformations*, as follows.

27.8. Definition. *For functors $F, G : \mathcal{C} \to \mathcal{D}$, a natural transformation $F \to G$ is a collection of morphisms $\{\tau_C : F(C) \to G(C)\}_{C \in \mathcal{C}}$ in $\mathcal{D}$ such that for every morphism $f : C \to C'$ in $\mathcal{C}$, the diagram*

$$\begin{array}{ccc} F(C) & \xrightarrow{\tau_C} & G(C) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(C') & \xrightarrow{\tau_{C'}} & G(C') \end{array}$$

commutes. If all morphisms τ_C are isomorphisms, then the functors F and G are said to be naturally equivalent or isomorphic.

27.9. Examples. 1. For the functors $\mathrm{GL}_n : \mathbf{CRng} \to \mathbf{Grp}$ and $U : \mathbf{CRng} \to \mathbf{Grp}$ defined in 27.5.2, the determinant map $\det : \mathrm{GL}_n \to U$ is a natural transformation. For $n = 1$, it is an isomorphism of functors.

2. In the category of finite abelian groups, the formation $G^\vee = \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ of the dual group is a contravariant functor $D : \mathbf{FAb} \to \mathbf{FAb}$ that maps every group to an isomorphic group, but there is no "natural choice" for an isomorphism $G \xrightarrow{\sim} G^\vee$. Such a choice does exist for the formation $G \mapsto G^{\vee\vee}$ of the double dual. After all, an element $x \in G$ defines, in a natural way, a homomorphism $G^\vee \to \mathbf{Q}/\mathbf{Z}$ by taking $f \mapsto f(x)$. Consequently, the covariant functor $\mathbf{FAb} \to \mathbf{FAb}$ given by $G \mapsto G^{\vee\vee}$ is naturally isomorphic to the identity. It is also said that a finite abelian group G is *canonically isomorphic* to its double dual $G^{\vee\vee}$. This means that, for practical purposes, the two groups can usually be identified. Similar remarks hold for the formation of the dual vector space in the category $\mathbf{FVec}_K$ of finite-dimensional vector spaces. As in the case of finite groups, the finiteness condition on the dimension is essential to obtain a canonical isomorphism $V \to V^{**}$. In the infinite-dimensional case, which is studied in functional analysis, additional structure is needed to obtain so-called *reflexive spaces*.

3. The forgetful functor $\mathbf{Rng} \to \mathbf{Sets}$ from rings to sets is isomorphic to the representation functor $\mathrm{Hom}_{\mathbf{Rng}}(\mathbf{Z}[X], -)$. After all, for every ring R, there is a canonical bijection $\mathrm{Hom}_{\mathbf{Rng}}(\mathbf{Z}[X], R) \xrightarrow{\sim} R$ given by $f \mapsto f(X)$. In general, a functor $F : \mathcal{C} \to \mathbf{Sets}$ isomorphic to a representation functor is called a *representable functor*. Since Grothendieck, this concept has been of fundamental importance in arithmetic algebraic geometry. For example, Wiles's proof of Fermat's last theorem consists to a large extent of a proof of the representability of certain functors in the theory of elliptic curves.

27.10. Definition. *The categories $\mathcal{C}$ and $\mathcal{D}$ are called equivalent if there exist functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that $G \circ F$ and $F \circ G$ are isomorphic to the identity on, respectively, $\mathcal{C}$ and $\mathcal{D}$. If there exist contravariant functors with this property, then $\mathcal{C}$ and $\mathcal{D}$ are called anti-equivalent.*

27.11. Examples. 1. Example 27.9.2 shows that the category **FAb** of finite abelian groups is anti-equivalent to itself under the duality functor D.

2. Let L/K be a finite Galois field extension with group G. The *fundamental theorem of Galois theory* says that the category of intermediate fields $\mathbf{Fld}_{L/K}$, with the natural inclusions as morphisms, is anti-equivalent to the category $\mathbf{Sgrp}_G$ of subgroups of G, with again the natural inclusions as morphisms. The functors $\mathbf{Fld}_{L/K} \to \mathbf{Sgrp}_G$ and $\mathbf{Sgrp}_G \to \mathbf{Fld}_{L/K}$ in Definition 27.10 are given by $M \mapsto \mathrm{Aut}(L/M)$ and $H \mapsto L^H$.

3*. The fundamental theorem of Galois theory for topological spaces says that under mild conditions, the category $\mathbf{Cov}_X$ of covers of a path-connected topological space X is anti-equivalent to the category $\pi(X)$**-sets** of sets with an action of the fundamental group $\pi(X)$. For every point $x \in X$, we have the *fiber functor* $F_x : \mathbf{Cov}_X \to \mathbf{Sets}$ that takes a cover $f : Y \to X$ to $f^{-1}(x)$, and the fundamental group $\pi(X, x)$ acts on the fiber $f^{-1}(x)$. Here, the image of $y \in f^{-1}(x)$ by the homotopy class of a path $w \subset X$ in x is defined as the terminal point of the unique path $w^* \subset Y$ with initial point y that is projected onto w by f.

▶ Universal constructions

In Section 17, we already noted that many of the standard constructions for groups, rings, and modules are solutions of certain universal problems in the underlying category. Many of the definitions we already know can therefore be formulated in general categorical terms.

27.12. Definition. *A product of a family of objects $\{A_i\}_{i\in I}$ in $\mathcal{C}$ is an object $P \in \mathcal{C}$ endowed with morphisms $p_i : P \to A_i$ with the property that given an object $T \in \mathcal{C}$ and morphisms $f_i : T \to A_i$, there exists a unique morphism $f : T \to P$ with $p_i \circ f = f_i$.*
A coproduct or sum of $\{A_i\}_{i\in I}$ in $\mathcal{C}$ is an object $S \in \mathcal{C}$ endowed with morphisms $\varepsilon_i : A_i \to S$ with the property that given an object $T \in \mathcal{C}$ and morphisms $g_i : A_i \to T$, there exists a unique morphism $f : S \to T$ with $g \circ \varepsilon_i = g_i$.

We already saw in 17.7 that *if* objects with such a universal characterization exist, they are always determined up to a unique isomorphism. However, the existence of sums and products is not guaranteed in every category. A sum or product may only exist in a "larger" category or not exist at all. The first case often occurs when we try to form sums or products of infinite families of objects in categories with finiteness conditions (finite groups, finite-dimensional vector spaces, finitely generated modules, ...).

We already noted, in 27.2.4, that the category $\mathbf{Mod}_R$ of modules over a commutative ring R is *the* example of a so-called *abelian category*, in which many of the universal standard constructions can be carried out. Theorem 17.8 says, rather unsurprisingly, that sums and products always exist in the category $\mathbf{Mod}_R$ of modules over a ring.

27.13. Examples. 1. In the category **Sets**, the sum of a family of sets is nothing but the *disjoint union*. The product of several sets is the *Cartesian product* of the sets. If the underlying sets are groups or rings, this product has a natural group or ring structure, and we see that products in **Grp** and **Rng** can be constructed in the usual way.

2. In the category of topological spaces, a sum is the same as a disjoint union. For the product, we take the Cartesian product with the known product topology, in which open sets in $\prod_i A_i$ are of the form $\prod_i U_i$, with $U_i \subset A_i$ open and equal to A_i for all but finitely many i.

3. The construction of sums in **Grp** is not that simple. In the category **Ab** of abelian groups, which are $\mathbf{Z}$-modules, we can use the construction of sums of $\mathbf{Z}$-modules from Section 17. In the non-abelian case, we obtain much more complicated groups. For example, the sum of two cyclic groups $\langle\sigma\rangle$ and $\langle\tau\rangle$ of order 2 in **Ab** leads to the Klein four-group, but in **Grp**, it leads to the infinite group in Exercise 2.36 consisting of all finite products of alternating factors σ and τ. We can show[20] that the modular group $\mathrm{SL}_2(\mathbf{Z})/\{\pm 1\}$ is the sum of a subgroup of order 2 with generator $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and a subgroup of order 3 with generator $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. The sum of groups in **Grp** is called a coproduct and often also a *free product*. The sum of a family of infinite cyclic groups $\langle a_i\rangle$ is called the *free group* with generators a_i $(i \in I)$.

4. The product of rings is simply obtained by endowing the Cartesian product with coordinatewise ring operations. In the category **CRng** of commutative rings, which are $\mathbf{Z}$-algebras, the coproduct is the *tensor product* of $\mathbf{Z}$-algebras from Section 17.

5. In the category of objects over a fixed base object A, the product of $X \to A$ and $Y \to A$ is the *fibered product* of X and Y over A. The sum of $A \to X$ and $A \to Y$ is the *fibered sum* of X and Y over A.

Exercise 4. Show that for the category **Ab**, these definitions agree with those in Exercise 9.51.

EXERCISES.

5. Determine which of the following constructions are functorial:
   a. the formation of the automorphism group $\mathrm{Aut}(G)$ of G
   b. the restriction and extension of scalars for modules over a ring
   c. the formation of the algebraic closure of a field
   d. the formation of the normal closure of a field
   e. the formation of the algebraic closure in $\mathbf{C}$ of a subfield $K \subset \mathbf{C}$.

   For the functorial constructions, give the underlying categories.
6. Let G be a group and G-**sets** the category of sets with a G-action. Determine the automorphism group of G viewed as a G-set under the regular action. *Is there a similar direct description if we view G as a G-set under conjugation?
7. Show that every isomorphism $f : A \to B$ in a category induces a group isomorphism $\phi_f : \mathrm{Aut}(A) \to \mathrm{Aut}(B)$ of the corresponding automorphism groups, and that for every ordered pair of isomorphisms $f, f' : A \to B$, there exist inner automorphisms α and β of, respectively, $\mathrm{Aut}(A)$ and $\mathrm{Aut}(B)$ with $\phi_f \circ \alpha = \phi_{f'} = \beta \circ \phi_f$.

8. Give the definition of an automorphism of a functor $F : \mathcal{C} \to \mathcal{D}$, and show that these automorphisms form a group $\mathrm{Aut}(F)$. Determine $\mathrm{Aut}(F)$ for the forgetful functor $F : G\textbf{-sets} \to \textbf{Sets}$.

9. Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be functors. We say that F and G are *adjoint functors* if for every ordered pair of objects $C \in \mathcal{C}$ and $D \in \mathcal{D}$, there is a bijection

$$\mathrm{Hom}_{\mathcal{C}}(C, G(D)) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{D}}(F(C), D)$$

that is natural in C and D. Describe what this means explicitly, and determine the left adjoint F of G for G the forgetful functor $\textbf{Ab} \to \textbf{Grp}$, the forgetful functor $\textbf{Vec}_K \to \textbf{Sets}$, or the forgetful functor $\textbf{Fld} \to \textbf{Dom}$ (from fields to integral domains).

10. Construct left-adjoint functors for the forgetful functors $\textbf{Mod}_R \to \textbf{Sets}$ and $\textbf{Mod}_R \to \textbf{Ab}$.

11. Let F and G be adjoint functors $\textbf{Mod}_R \to \textbf{Mod}_R$ for a commutative ring R. Define left exact and right exact for functors $\textbf{Mod}_R \to \textbf{Mod}_R$, and show that F is right exact if and only if G is left exact.
[Hint: see 17.12 for a concrete example.]

12. An object X in a category $\mathcal{C}$ is called an *initial object* if every object $Y \in \mathcal{C}$ admits a unique morphism $X \to Y$, and a *terminal object* if every object $Y \in \mathcal{C}$ admits a unique morphism $Y \to X$. Show that such objects are determined up to a unique isomorphism *if* they exist. Determine whether they exist in the categories **Sets**, **Grp**, **Rng**, and $\textbf{Mod}_R$.

13. Let R be a commutative ring. Show that a sum of A_1 and A_2 in the category $\textbf{CAlg}_R$ of commutative R-algebras is the tensor product $A_1 \otimes_R A_2$.

14. Show that the group of units functor $R \mapsto R^*$, viewed as a functor $\textbf{Rng} \to \textbf{Sets}$, is isomorphic to the representation functor $\mathrm{Hom}_{\textbf{Rng}}(\mathbf{Z}[X, X^{-1}], -)$.

15. *(Yoneda lemma.)* Show that every natural transformation from the representation functor $F_X = \mathrm{Hom}_{\mathcal{C}}(X, -)$ to $F_Y = \mathrm{Hom}_{\mathcal{C}}(Y, -)$ is induced by a unique morphism $Y \to X$ in $\mathcal{C}$. Conclude that the representation functors F_X and F_Y are isomorphic if and only if the objects X and Y are isomorphic in $\mathcal{C}$.
[Hint: consider the image of $\mathrm{id}_X \in F_X(X)$ in $F_Y(X)$.]

16. Let L/K be a finite Galois extension with group G. Show that there is a contravariant functor $F : \textbf{Fld}_{L/K} \to \textbf{Sets}$ given by $F(M) = \mathrm{Hom}_K(M, L)$ and that there is a natural (right) action of G on $F(M)$. Describe the image of the functor $F : \textbf{Fld}_{L/K} \to G\textbf{-sets}$.
[This is, in fact, a formulation of the fundamental theorem of Galois theory.]

17. Let $\mathcal{C}$ be a subcategory of $\textbf{Mod}_R$ for a ring R. The *Grothendieck group* $K(\mathcal{C})$ of $\mathcal{C}$ is the abelian group with generators the isomorphism classes of the objects in $\mathcal{C}$ and relations $[P] - [Q] + [R] = 0$ for every exact sequence $0 \to P \to Q \to R \to 0$ in $\mathcal{C}$. Show that there are isomorphisms $K(\textbf{FAb}) \cong \mathbf{Z}$ and $K(\textbf{FGAb}) \cong \mathbf{Z}$ that send, respectively, the class of a finite group to its order and the class of a finitely generated group to its free rank.

28 Infinite Galois theory

Given a field K, we can take the union of *all* finite Galois extensions $K \subset L$ inside an algebraic closure $\overline{K}$ of K. This leads to a *separable closure* K^{sep} of K, and we can "bundle" the information on all finite Galois groups $\text{Gal}(L/K)$ into a single automorphism group $G_K = \text{Aut}_K(K^{\text{sep}})$, the *absolute Galois group* of K. The absolute Galois group $G_{\mathbf{Q}}$ takes a central role in modern number theory, and the linear action of $G_{\mathbf{Q}}$ on suitably chosen objects, the so-called *Galois representations*, form the basis of the breakthroughs in recent decades by Faltings, Wiles, and many others.

In the interesting cases where the extension $K \subset K^{\text{sep}}$ has *infinite* degree, the absolute Galois group G_K, which, by construction, has all finite Galois groups $\text{Gal}(L/K)$ as quotient, is an *uncountable* group. To extend the fundamental theorem 24.4 to the situation of infinite field degrees, we need to use the natural *topology* that Galois groups have as "groups of maps."

▶ Topology on automorphism groups

For sets A and B, we often denote the set $\text{Map}(A, B)$ of maps $A \to B$ by B^A. We then think of B^A as the product of a collection of copies of B, one for each element of A, by identifying a map $f : A \to B$ with the "sequence" $(f(x))_{x \in A}$ of elements of B.

We give the non-empty set B the "uninteresting" discrete topology, and note that the corresponding product topology on B^A is *not* discrete for infinite A. Concretely, a set $U \subset B^A$ is open if and only if for every $f \in U$, there is a finite subset $E \subset A$ with the property that every map $g : A \to B$ with $g\big|_E = f\big|_E$ belongs to U. It follows from this definition that the closure of a set $S \subset B^A$ consists of the functions $g : A \to B$ with the property that for every finite subset $E \subset A$, there is an $f \in S$ with $f\big|_E = g\big|_E$. Thus, if we take $A = B = \mathbf{R}$ and for $S \subset \text{Map}(\mathbf{R}, \mathbf{R})$ the "small" set consisting of those functions $f : \mathbf{R} \to \mathbf{R}$ that are only non-zero outside a finite subset of $\mathbf{R}$, then the closure of S is all of $\text{Map}(\mathbf{R}, \mathbf{R})$.

Exercise 1. Verify these statements.

A set $S \subset B^A$ is closed if and only if all $g \in B^A$ that coincide with a map $f \in S$ on every *finite* subset of A are also contained in S. This is often a convenient way to verify that a given S is closed. We can use it, for example, to see that the set of *injective* maps $A \to B$ is closed in B^A (Exercise 4.a) and that if A and B are groups, then $\text{Hom}(A, B)$ is closed in B^A (Exercise 6.a).

Exercise 2. Verify that B^A is a Hausdorff space.

Now, let L be a field, and denote the group of field automorphisms of L by $\text{Aut}\, L$. We have $\text{Aut}\, L \subset L^L$, where L^L has a topology as defined above, with $A = B = L$. The topology on L^L leads to a natural subspace topology on $\text{Aut}(L)$. In this topology, $V \subset \text{Aut}\, L$ is open if and only if there is an open $U \subset L^L$ with $V = U \cap \text{Aut}\, L$.

The group $\text{Aut}\, L$ may not be a *closed* subset of L^L (Exercise 7). To overcome this problem, $\text{Aut}\, L$ is sometimes also viewed as a subset of $L^L \times L^L$ by identifying

$\sigma \in \operatorname{Aut} L$ with $(\sigma, \sigma^{-1}) \in L^L \times L^L$. If we endow $L^L \times L^L$ with the product topology, then $\operatorname{Aut} L$ is a closed subset in $L^L \times L^L$, and the topology induced on $\operatorname{Aut} L$ coincides with the one we just defined (Exercise 8).

A *topological group* is a group G endowed with a topology for which the group operations are continuous. This means that both maps

$$\begin{aligned} G \times G \to G: &\quad (g,h) \mapsto gh \\ G \to G: &\quad g \mapsto g^{-1} \end{aligned}$$

are continuous, where $G \times G$ has the product topology.

As can be expected on categorical grounds, a *homomorphism* $f : G_1 \to G_2$ of topological groups is a continuous map $G_1 \to G_2$ that is a group homomorphism. It is an *isomorphism* of topological groups if it has a two-sided inverse that is also a homomorphism. This means that f is both a group isomorphism and a homeomorphism.

A direct verification, for which we refer to Exercise 8, gives the following conclusion.

28.1. Lemma. *Let L be a field. Then $\operatorname{Aut}(L)$ endowed with the subspace topology of L^L is a topological group. Moreover, $\operatorname{Aut} L$ is Hausdorff.* □

▶ Galois extensions

The correct generalization of 24.1 to arbitrary extensions is the following.

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

In the situation of 28.2, we again say that *$K \subset L$ is Galois with group G.*

Note that a finite subgroup $G \subset \operatorname{Aut} L$ is certainly compact, so a finite Galois extension as in 24.1 is also a Galois extension in the new meaning. Not every compact subgroup of $\operatorname{Aut}(L)$ is necessarily finite, but we are going to prove that an element of L has only finitely many different images under the action of a compact subgroup.

28.3. Lemma. *Let L be a field and $G \subset \operatorname{Aut} L$ a closed subgroup. Then G is compact if and only if for every $\alpha \in L$, the orbit $G\alpha = \{\sigma\alpha : \sigma \in G\}$ of α under G is finite.*

Proof. The orbit $G\alpha$ of an element $\alpha \in L$ is the image of $G \subset \operatorname{Aut} L \subset L^L$ by the projection $\pi_\alpha : L^L \to L$ to the "αth coordinate" given by $f \mapsto f(\alpha)$. Now, π_α is a continuous map, so if G is compact, then the image $\pi_\alpha[G] = G\alpha$ is a compact subspace of L. Since L is discrete, this means that the orbit $G\alpha$ is finite.

For the converse, we view $\operatorname{Aut} L$, and therefore also G, as a subspace of $L^L \times L^L$, as explained above. In fact, G is then a subspace of the subset $F = \prod_{\alpha \in L} G\alpha \times \prod_{\alpha \in L} G\alpha$ of $L^L \times L^L$. If all orbits $G\alpha$ are finite, then F is a product of finite spaces, hence *compact* by Tychonoff's theorem. If G is moreover closed, then as a closed subset of a compact space, G is itself also compact. □

Exercise 3. Why can we not use the natural embedding $G \subset L^L$ in the second part of the proof?

The following theorem describes general Galois extensions in the manner of Lemma 24.3 and part 24.4.1 of the "finite" fundamental theorem.

28.4. Theorem. 1. *Let $K \subset L$ be a field extension that is algebraic, normal, and separable. Then $G = \mathrm{Aut}_K(L)$ is compact, and $K \subset L$ is Galois with group G.*

2. *Let $K \subset L$ be a Galois extension with Galois group G. Then $K \subset L$ is algebraic, normal, and separable, and we have $G = \mathrm{Aut}_K(L)$.*

As in 24.5, this gives a characterization of arbitrary Galois extensions, this time with *algebraic* instead of *finite*.

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

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

Proof of 28.4. (1) We verify that $G = \mathrm{Aut}_K L$ is compact using Lemma 28.3. That $\mathrm{Aut}_K L$ is closed in $\mathrm{Aut}\, L$ follows immediately from the definition of the topology on $\mathrm{Aut}\, L$ (cf. Exercise 6.b). For every $\alpha \in L$, the orbit $G\alpha$ is a subset of the set of zeros of f_K^α in L and therefore finite. The conditions of 28.3 are therefore satisfied, and G is compact. Now, suppose that $\alpha, \beta \in L$ have the same minimum polynomial over K. Then there is a K-isomorphism $\sigma : K(\alpha) \to K(\beta)$ that maps α onto β. If we denote by $\overline{K}$ an algebraic closure of K that contains L, then as in Exercise 21.14, we can extend σ to an isomorphism $\overline{K} \to \overline{K}$, which we still denote by σ. Because L is normal over K, we have $\sigma L = L$; this gives an element $\sigma\big|_L$ of G that maps α onto β. Now, if α belongs to L^G, then we must have $\beta = \alpha$, so f_K^α has only one zero in L. By the normality and separability of L over K, we then have $f_K^\alpha = X - \alpha$, so $\alpha \in K$. This gives $L^G = K$, so $K \subset L$ is Galois with group G.

(2) Take $\alpha \in L$ arbitrary. Then by Lemma 28.3, the orbit $G\alpha$ is finite. We form the monic polynomial $f = \prod_{\beta \in G\alpha}(X - \beta)$. The action of G permutes the factors, so f has coefficients in $L^G = K$. Since f decomposes completely into linear factors in $L[X]$ and has α as zero, this shows that α is separable algebraic over K. Since f_K^α is a divisor of f, the polynomial f_K^α also decomposes completely into linear factors in $L[X]$. It follows that $K \subset L$ is algebraic, separable, and normal. It remains to show $G = \mathrm{Aut}_K L$. The inclusion $\subset$ is clear. For the reverse inclusion, because G is closed, we only need to show that every $\rho \in \mathrm{Aut}_K L$ belongs to the *closure* of G in L^L. To this end, let $E \subset L$ be finite; it suffices to construct $\tau \in G$ with $\rho\big|_E = \tau\big|_E$. The set $GE = \bigcup_{\alpha \in E} G\alpha$ is finite, so the field $F = K(GE)$ is finite over K. Because GE is permuted by G, the restriction of G to F gives a subgroup $G\big|_F$ of $\mathrm{Aut}_K F$ with $F^{G\big|_F} = L^G \cap F = K$. It follows that F is a finite Galois extension of K with group $\mathrm{Gal}(F/K) = G\big|_F$ (this is where we use finite Galois theory!). Every $\rho \in \mathrm{Aut}_K L$ gives an element of this Galois group when restricted to F, so there exists a $\tau \in G$ with $\rho\big|_F = \tau\big|_F$; because of the inclusion $E \subset F$, this gives $\rho\big|_E = \tau\big|_E$, as desired. $\square$

Theorem 28.4 shows that the group G is fixed if we know the Galois extension $K \subset L$, as we have $G = \mathrm{Aut}_K L$. We again write $G = \mathrm{Gal}(L/K)$ and call G the *Galois group*, or *group* for short, of the Galois extension.

28.6. Examples. 1. For an arbitrary field K, a separable closure K^{sep} of K (see Exercise 23.12) is a Galois extension of K by 28.5; moreover, K^{sep} is the "largest" Galois extension of K, in the sense that for every Galois extension L of K, there is a K-isomorphism of L with an intermediate field of $K \subset K^{\mathrm{sep}}$.

2. Let K be a field of characteristic $\mathrm{char}(K) \neq 2$ and $K(\sqrt{K})$ its "maximum square root extension" defined before 25.8. This is the splitting field of the set $\{X^2 - a : a \in K^*\}$ (cf. Exercise 21.34), so it is algebraic, separable, and normal over K. By 28.5, the field $K(\sqrt{K})$ is a Galois extension of K.

▶ Galois correspondence

As in the case of the finite fundamental theorem 24.4, it is relatively easy to deduce the full *Galois correspondence* from the fundamental theorem 28.4. For the collection of subfields of a field L, it reads as follows.

28.7. Theorem. *Let L be a field, $\mathcal{D}$ the set of subfields $K \subset L$ for which L is algebraic, separable, and normal over K, and $\mathcal{C}$ the set of compact subgroups G of $\mathrm{Aut}\, L$. Then there is an inclusion-reversing bijection*

$$\begin{aligned} \psi_L : \mathcal{D} &\xrightarrow{\sim} \mathcal{C} \\ K &\longmapsto \mathrm{Aut}_K L, \end{aligned}$$

with inverse given by $\phi(G) = L^G$.

Proof. From Theorem 28.4, we have, on the one hand, $\phi\psi(K) = \phi(\mathrm{Aut}_K L) = L^{\mathrm{Aut}_K L} = K$, and therefore $\phi\psi = \mathrm{id}_{\mathcal{D}}$. On the other hand, we have $\psi\phi(G) = \psi(L^G) = \mathrm{Aut}_{L^G} L = G$, and therefore $\phi\psi = \mathrm{id}_{\mathcal{C}}$. This shows that ψ_L is a bijection with inverse ϕ_L. For $K, F \in \mathcal{D}$ with $K \subset F$, it immediately follows that we have $\psi_L(K) = \mathrm{Aut}_K L \supset \mathrm{Aut}_F L = \psi_L(F)$; likewise, for $H, G \subset \mathcal{C}$ with $H \subset G$, we have an obvious inclusion $L^H \supset L^H$. □

For an arbitrary Galois extension $K \subset L$, we have the following obvious generalization of 24.4.2. For a topological group G with subgroup H, we endow the set G/H with the quotient topology. If H is a normal subgroup of G, this makes G/H into a topological group (Exercise 10).

28.8. Theorem. *Let $K \subset L$ be a Galois extension with group G.*

1. *There is an inclusion-reversing bijection, the Galois correspondence*

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

   between the set $\mathcal{T}_{L/K}$ of intermediate fields of $K \subset L$ and the set $\mathcal{H}_G$ of closed subgroups of G. The inverse is $\psi_{L/K}^{-1} : H \mapsto L^H$.
2. *Let $F \in \mathcal{T}_{L/K}$. Then the extension $F \subset L$ is Galois with group $H = \psi_{L/K}(F)$, and under $\psi_{L/K}$, for every $\sigma \in G$, the field $\sigma[F] \in \mathcal{T}_{L/K}$ conjugate to F corresponds to the subgroup $\sigma H \sigma^{-1}$ conjugate to H.*

The extension $K \subset F$ is normal 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 there is an isomorphism of topological groups

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

Proof. (1) From Theorem 28.7, we obtain a bijection from the set of all $F \in \mathcal{D}$ with $K \subset F$ to the set of all $H \in \mathcal{C}$ with $H \subset G$. The field L is algebraic, separable, and normal over K, hence also over every $F \in \mathcal{T}_{L/K}$. The first set therefore coincides with $\mathcal{T}_{L/K}$. Since every compact H is closed and, conversely, every closed subgroup of G is compact, the second set coincides with $\mathcal{H}_G$.

(2) The remaining statements are proved as in the finite case of Theorem 24.4; cf. Exercise 9. The fact that the group isomorphism $G/H \to \mathrm{Gal}(F/K)$ with $\sigma H \mapsto \sigma\big|_F$ is a homeomorphism, hence also an isomorphism of *topological* groups, follows from a general theorem in topology; see Exercise 11.a. □

Theorem 28.8 is the fundamental theorem of infinite Galois theory; it was first proved by Wolfgang Krull (German algebraist, 1899–1971) in 1928. If we remove the word "closed" in the definition of $\mathcal{H}_G$, the theorem is wrong (see Exercise 20), so introducing the topology is truly "necessary." The topology defined on $\mathrm{Gal}(L/K)$ is also called the *Krull topology*.

It follows from the fundamental theorem of infinite Galois theory that for given K, we only need to study a single Galois extension, namely a separable closure K^{sep} of K. After all, every other Galois extension L of K has a K-embedding into K^{sep}, and given this embedding, we can "read" $\mathrm{Gal}(L/K)$ from $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. For this reason, the group $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ is also called the *absolute Galois group* of K.

The only ingredient in 24.4 that we do not recover is the correspondence between degrees of fields and group indices in 24.4.3. After all, in the situation of 28.8, these could be infinite. However, we can characterize the intermediate fields of finite degree over K as follows.

28.9. Theorem. *Suppose that, in the notation of Theorem 28.8, the field $F \in \mathcal{T}_{L/K}$ corresponds to the closed subgroup $H \in \mathcal{H}_G$. Then F is finite over K if and only if H has finite index in G, and if and only if H is open in G; for such F, we have $[F : K] = [G : H]$.*

Proof. The fact that a closed subgroup is open if and only if it has finite index is a generality for compact topological groups; see Exercise 12.c. Now, assume that F is finite over K. Because L is normal over K, the field L contains a normal closure M of F over K, and M is finite over K. It follows that M is a finite Galois extension of K. Write $N = \mathrm{Aut}_M L$; then Theorem 28.8 (with M and N in the roles of F and H) gives an isomorphism $G/N \cong \mathrm{Gal}(M/K)$, so N has finite index $[M : K]$ in G. For the same reason, with F as base field, N has index $[M : F]$ in H. It follows that H has finite index $[M : K]/[M : F] = [F : K]$ in G. Finally, assume that F is

not finite over K. Then we can construct, in F, a strictly increasing chain of finite extensions $K = K_0 \subset K_1 \subset K_2 \subset \ldots$ by repeatedly choosing $\alpha_i \in L$ with $\alpha_i \notin K_i$ and taking $K_{i+1} = K_i(\alpha_i)$. By switching to subgroups, we then obtain an infinite chain of subgroups $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset H$, so H has infinite index in G. □

28.10. Example. Let $L = \mathbf{Q}(\sqrt{\mathbf{Q}})$ be the maximum square root extension of $\mathbf{Q}$, as in Example 28.6.2. Let us describe the Galois group $\mathrm{Gal}(L/\mathbf{Q})$. Write $\mathcal{P} = \{-1\} \cup \{p : p \text{ is prime}\}$, and let $\phi : \mathrm{Gal}(L/\mathbf{Q}) \to \{\pm 1\}^{\mathcal{P}}$ be the map that sends each σ to the function $p \mapsto \sigma(\sqrt{p})/\sqrt{p}$. If we endow $\{\pm 1\}^{\mathcal{P}}$ with the product topology in the usual way, then it is easy to verify that ϕ is continuous. It follows from $L = \mathbf{Q}(\sqrt{p} : p \in \mathcal{P})$ that ϕ is injective. With a little more effort, we can show that ϕ is surjective (Exercise 14). It follows that ϕ is a homeomorphism (see Exercise 11.a). If we make $\{\pm 1\}^{\mathcal{P}}$ into a group with componentwise multiplication, then ϕ is also a group homomorphism. The conclusion is that there is an isomorphism $\mathrm{Gal}(L/\mathbf{Q}) \cong \{\pm 1\}^{\mathcal{P}}$ of topological groups.

28.11. Example. Let $\mathbf{F}_q$ be a field with q elements and $\overline{\mathbf{F}}_q$ an algebraic closure. Because finite fields are perfect, $\mathbf{F}_q \subset \overline{\mathbf{F}}_q$ is a Galois extension. The Galois group $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ contains the Frobenius automorphism F that maps each $\alpha \in \overline{\mathbf{F}}_q$ to α^q. It follows from $\mathbf{F}_q = \{\alpha \in \overline{\mathbf{F}}_q : \alpha^q = \alpha\}$ that we have $\mathbf{F}_q = \overline{\mathbf{F}}_q^{\langle F \rangle}$. Consequently, $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ is generated *topologically* by F in the sense that $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ is equal to the *closure* of $\langle F \rangle$ (see Exercise 13). It follows from the general fact that an infinite Galois group can never be countable (Exercise 19) that $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ is not equal to $\langle F \rangle$ itself; we can also deduce this from the explicit description of $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ we give below.

For every $n \in \mathbf{Z}_{>0}$, the field $\overline{\mathbf{F}}_q$ has a unique subfield $\mathbf{F}_{q^n} = \{x \in \overline{\mathbf{F}}_q : x^{q^n} = x\}$ with q^n elements, and by restriction, every $\sigma \in \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ gives an element of $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$; this latter group is cyclic of order n, generated by the restriction of F to $\mathbf{F}_{q^n}$. Therefore, for every $\sigma \in \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ and every n, there is an integer $a_n(\sigma)$, uniquely determined modulo n, such that σ and $F^{a_n(\sigma)}$ coincide on $\mathbf{F}_{q^n}$. This leads to a map

$$\phi : \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) \to \prod_{n>0} \mathbf{Z}/n\mathbf{Z}, \qquad \sigma \mapsto (a_n(\sigma) \bmod n)_{n>0}\,.$$

This is a group homomorphism, and it follows from $\overline{\mathbf{F}}_q = \bigcup_{n>0} \mathbf{F}_{q^n}$ that ϕ is injective. If we endow every $\mathbf{Z}/n\mathbf{Z}$ with the discrete topology and $\prod_{n>0} \mathbf{Z}/n\mathbf{Z}$ with the product topology, then ϕ is moreover continuous. Using Exercise 11, we can now conclude that ϕ induces an isomorphism of $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ with the image of ϕ.

We have $\phi(F) = (1, 1, 1, \ldots)$, and the closure of the subgroup of $\prod_{n>0} \mathbf{Z}/n\mathbf{Z}$ generated by this element is equal to the image of ϕ. This follows from $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) = \overline{\langle F \rangle}$ and the fact that the image of ϕ is closed in $\prod_{n>0} \mathbf{Z}/n\mathbf{Z}$ (Exercise 11.b).

▶ Projective limits

The description of $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ given above may not be very enlightening, but the basic idea that an infinite Galois group G can be described in terms of its finite quotients G/N can be made more explicit. After all, since every Galois extension $K \subset L$ can be

viewed as the "union" of all its finite normal subextensions $K \subset L_0$, an automorphism $\sigma \in G$ is uniquely determined by the collection of its images $\sigma_N = (\sigma \bmod N)$ in all finite quotients G/N of G. It is almost a tautology to say that the elements of G can be viewed as the elements $(\sigma_N)_N \in \prod_{G/N \text{ finite}} G/N$ that are "compatible" under the inclusion of normal subgroups or, equivalently, normal subextensions.

This intuitive idea is made more precise through the notion of *projective limit*, which can be defined in any category. As in the formulation of Zorn's lemma (15.11), we can include the compatibility under inclusions in the notion of *partial ordering*.

A *partially ordered set* is a set I endowed with a relation $\leq$ such that for all i, j, $k \in I$, the implications $i \leq j \wedge j \leq k \Rightarrow i \leq k$ and $i \leq j \wedge j \leq i \Leftrightarrow i = j$ hold. We call such a partially ordered set *directed* if for any two i, $j \in I$, there exists an element $k \in I$ with $i \leq k \wedge j \leq k$. A *projective system* consists of three things: first, a directed partially ordered set I; second, a set A_i for every $i \in I$; and third, for any two elements i, $j \in I$ with $i \leq j$, a map $f_i^j : A_j \to A_i$ such that for all $i \in I$, we have $f_i^i = \mathrm{id}_{A_i}$ and for all i, j, $k \in I$ with $i \leq j$ and $j \leq k$, we moreover have the equality $f_i^k = f_i^j \circ f_j^k$. This is, more precisely, a projective system of *sets*. We can obtain a projective system in another category such as that of groups, rings, topological spaces, ..., by taking all A_i to be groups, rings, topological spaces, ..., and requiring that every f_i^j is a group homomorphism, a ring homomorphism, a continuous map, ...

A projective system is often given by only stating what the A_i are; it is then generally clear what I, the partial ordering on I, and the "transition maps" f_i^j are, and if this is not the case, they are given explicitly.

28.12. Examples. The projective system (of sets, and of groups and rings) $(\mathbf{Z}/2^i\mathbf{Z})_{i\geq 0}$ has $I = \mathbf{Z}_{\geq 0}$ with the usual ordering, and the map $f_i^j : \mathbf{Z}/2^j\mathbf{Z} \to \mathbf{Z}/2^i\mathbf{Z}$ sends $(a \bmod 2^j)$ to $(a \bmod 2^i)$. The projective system $(\mathbf{Z}/n\mathbf{Z})_{n>0}$ is somewhat more subtle because a natural map (and group and ring homomorphism) $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$, $(a \bmod m) \mapsto (a \bmod n)$ only exists if n is a *divisor* of m; so here we take $I = \mathbf{Z}_{>0}$, with a partial ordering $\preceq$ defined by $n \preceq m \Leftrightarrow n \mid m$.

Suppose given a projective system as defined above. The *(projective) limit* of the system, denoted by $\lim_{\leftarrow} A_i$ or $\lim_{\leftarrow i\in I} A_i$, is by definition equal to the subset $\{(x_i)_{i\in I} \in \prod_{i\in I} A_i$: for all i, $j \in I$ with $i \leq j$, we have $f_i^j(x_j) = x_i\}$ of $\prod_{i\in I} A_i$. In the case of a projective system of groups or rings, this is a subgroup or subring, respectively, of the product group or ring $\prod_{i\in I} A_i$; in the case of projective system of topological spaces, $\prod_{i\in I} A_i$ is given the product topology and $\lim_{\leftarrow} A_i$ the subspace topology. In Galois theory, we often consider a system of compact topological groups that are Hausdorff, with continuous group homomorphisms as transition maps; the projective limit is then again a compact topological group that is Hausdorff (Exercise 16). (In general categories, we must be more careful when defining projective limits as they do not always exist.)

▶ Profinite groups

Suppose given a projective system consisting of finite groups and group homomorphisms. If we endow each of these groups with the discrete topology, then by the

above, the projective limit is automatically a topological group. A *profinite group* is a topological group that is isomorphic to a topological group obtained this way. Every profinite group is compact and Hausdorff, and moreover *totally disconnected* (a topological space X is called totally disconnected if X has no connected subspaces of more than one element). Conversely, it can be proved[21] that every totally disconnected compact topological group is profinite. Analogously to profinite groups, we can define *profinite rings*. Every compact topological ring that is Hausdorff turns out to be profinite.[22]

28.13. Example. In 28.12, we considered the projective system $(\mathbf{Z}/n\mathbf{Z})_{n>0}$. We denote its projective limit by $\hat{\mathbf{Z}}$ (pronunciation: zee-hat; in British: zed-hat). This is a profinite ring, and its additive group is an abelian profinite group. The unit element of $\hat{\mathbf{Z}}$ is the element $(1, 1, 1, \ldots)$ of $\prod_{n>0} \mathbf{Z}/n\mathbf{Z}$. The ring $\hat{\mathbf{Z}}$ is closed in $\prod_{n>0} \mathbf{Z}/n\mathbf{Z}$, so $\hat{\mathbf{Z}}$ contains the closure of the additive subgroup of $\prod_{n>0} \mathbf{Z}/n\mathbf{Z}$ generated by $(1, 1, 1, \ldots)$, which was considered in 28.12. In fact, $\hat{\mathbf{Z}}$ is *equal* to that closure (cf. Exercise 17.c). Combining this with the result from 28.12, we see that we have

$$\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) \cong \hat{\mathbf{Z}}$$

for every finite field $\mathbf{F}_q$, with an isomorphism that maps the Frobenius automorphism F onto the unit element of $\hat{\mathbf{Z}}$. Since $\hat{\mathbf{Z}}$ is the projective limit of $(\mathbf{Z}/n\mathbf{Z})_{n>0}$ and every $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$, it follows that the infinite Galois group $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ can be identified with the projective limit of the system $\left(\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)\right)_{n>0}$. The following theorem says that this is a completely general way to describe infinite Galois groups. In particular, all Galois groups are profinite.

28.14. Theorem. *Let $K \subset L$ be a Galois extension, and let I be a set of intermediate fields F of $K \subset L$ such that every $F \in I$ is finite Galois over K and $\bigcup_{F\in I} F = L$. Then $(\mathrm{Gal}(F/K))_{F\in I}$ together with the restriction maps $\mathrm{Gal}(F/K) \to \mathrm{Gal}(F'/K)$ (for F', $F \in I$, $F' \subset F$) is a projective system, and there is an isomorphism $\mathrm{Gal}(L/K) \to \lim_{\leftarrow F\in I} \mathrm{Gal}(F/K)$ of topological groups.*

Proof. We first show that I is directed under inclusion. Take F', $F'' \in I$. Then $F' \cdot F''$ is finite separable over K, so $F' \cdot F'' = K(\alpha)$ for some α (Theorem 23.9). It follows from $\bigcup_{F\in I} F = L$ that there exists an $F \in I$ with $\alpha \in F$, and then we have $K(\alpha) \subset F$, and therefore $F' \subset F$ and $F'' \subset F$, as desired. It is easy to verify that there exists a well-defined group homomorphism $\phi : \mathrm{Gal}(L/K) \to \prod_{F\in I} \mathrm{Gal}(F/K)$ with $\sigma \mapsto (\sigma\big|_F)_{F\in I}$, that ϕ is continuous, and that the image of ϕ is contained in $\lim_{\leftarrow F\in I} \mathrm{Gal}(F/K)$. It follows from $\bigcup_{F\in I} F = L$ that ϕ is injective. To prove the surjectivity, we take an element $(\sigma_F)_{F\in I}$ from the projective limit. We then define $\sigma : L \to L$ as follows: for $x \in L$, we choose an $F' \in I$ with $x \in F'$ and set $\sigma(x)$ equal to $\sigma_{F'}(x)$; if $F'' \in I$ also contains x and $F \in I$ satisfies $F' \subset F$ and $F'' \subset F$, then it follows from $\sigma_F\big|_{F'} = \sigma_{F'}$ and $\sigma_F\big|_{F''} = \sigma_{F''}$ that $\sigma_{F'}(x) = \sigma_F(x) = \sigma_{F''}(x)$, so $\sigma(x)$ does not depend on the choice of F'. Consequently, σ is well defined. The verification that σ is a field homomorphism $L \to L$ is similar. It is the identity on K, so σ belongs to $\mathrm{Gal}(L/K)$, and we have

$\phi(\sigma) = (\sigma_F)_{F\in I}$. Therefore, ϕ is a bijection. That it is an isomorphism of topological groups follows, in turn, from Exercise 11. □

28.15. Example. The *maximal cyclotomic extension* $\mathbf{Q}^{\mathrm{cycl}}$ of $\mathbf{Q}$ is obtained by adjoining to $\mathbf{Q}$ all roots of unity from an algebraic closure of $\mathbf{Q}$. It is the union of the fields $\mathbf{Q}(\zeta_n)$ for $n \in \mathbf{Z}_{>0}$. Every extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_n)$ is Galois with group isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$ (see Theorem 24.15), so $\mathrm{Gal}(\mathbf{Q}^{\mathrm{cycl}}/\mathbf{Q})$ is isomorphic to the projective limit of all groups $(\mathbf{Z}/n\mathbf{Z})^*$, which in turn is isomorphic to the group of units $\hat{\mathbf{Z}}^*$ of the ring $\hat{\mathbf{Z}}$.

Exercises.

4. Let A, B be two sets. Endow B with the discrete topology and B^A with the product topology.
   a. Prove that the set of injective maps $A \to B$ is closed in B^A.
   b. Suppose that A and B are countably infinite, and let $S \subset B^A$ be the set of surjective maps. Prove that S is not closed in B^A and that S is dense in B^A.

5. a. Let A, B, C be three sets. Prove that the map $C^B \times B^A \to C^A$, $(g, f) \mapsto g \circ f$, is continuous.
   b. Let A and B be two sets, and endow $A^B \times B^A$ with the product topology. Prove that $\{(g, f) \in A^B \times B^A : g \circ f = \mathrm{id}_A \text{ and } f \circ g = \mathrm{id}_B\}$ is closed in $A^B \times B^A$.

6. a. Let A and B be groups. Prove that $\mathrm{Hom}(A, B)$ is closed in B^A.
   b. Let A and B be field extensions of a field K. Prove that the set of field homomorphisms $A \to B$ that are the identity on K is closed in B^A.

7. a. Prove that the set $\mathrm{Aut}\,\mathbf{C}$ of field automorphisms of $\mathbf{C}$ is not closed in $\mathbf{C}^{\mathbf{C}}$. What is the closure of $\mathrm{Aut}\,\mathbf{C}$ in $\mathbf{C}^{\mathbf{C}}$?
   b. Prove that $\mathrm{Aut}\,\overline{\mathbf{Q}}$ is closed in $\overline{\mathbf{Q}}^{\overline{\mathbf{Q}}}$. Does this also hold with $\overline{\mathbf{Q}}$ replaced by $\overline{\mathbf{Q}(t)}$ if t is transcendental over $\mathbf{Q}$?

8. Let L be a field.
   a. Prove that the map $\mathrm{Aut}\,L \to \mathrm{Aut}\,L$, $\sigma \mapsto \sigma^{-1}$ is continuous.
   b. Prove Lemma 28.1.
   c. Prove that the maps $\mathrm{Aut}\,L \to L^L \times L^L \to L^L$ defined by $\sigma \mapsto (\sigma, \sigma^{-1})$ and $(f, g) \mapsto f$ are continuous, and conclude that the first map is a homeomorphism from $\mathrm{Aut}\,L$ to its image in $L^L \times L^L$. Also show that the image of $\mathrm{Aut}\,L$ in $L^L \times L^L$ is closed.

9. Let L, $\mathcal{D}$, $\mathcal{C}$ be as in Theorem 28.7, and suppose that $K \in \mathcal{D}$ corresponds to $G \in \mathcal{C}$. Prove: for every $\sigma \in \mathrm{Aut}\,L$, the element $\sigma K \in \mathcal{D}$ corresponds to $\sigma G \sigma^{-1} \in \mathcal{C}$.

10. Let G be a topological group and $H \subset G$ a normal subgroup. Prove that G/H, endowed with the quotient topology, is a topological group.

11. a. Prove that every continuous bijection from a compact topological space to a Hausdorff space is a homeomorphism.
    b. Let $f : X \to Y$ be a continuous map from a compact topological space X to a Hausdorff space Y. Define an equivalence relation $\sim$ on X by $x \sim y \Leftrightarrow f(x) = f(y)$. Endow $X/\sim$ with the quotient topology and $f(X) \subset Y$ with the subspace

topology. Prove that f induces a homeomorphism $X/\sim \to f(X)$ and that $f(X)$ is closed in Y.

12. Let G be a topological group, and let H be a subgroup of G.
    a. Let $a \in G$. Prove: H is open if and only if aH is open, and H is closed if and only if aH is closed.
    b. Prove: if H is open, then H is closed; and if H is closed and has finite index, then H is open.
    c. Assume that G is compact. Prove: H is open if and only if H is closed and has finite index.
13. Let $K \subset L$ be a Galois extension with group G. Prove that for every subgroup H of G, the closure $\overline{H}$ is also a subgroup of G and that we have $\overline{H} = \mathrm{Gal}(L/L^H)$.
14. In this exercise, we endow $\mathrm{Hom}(\mathbf{Q}^*, \{\pm 1\}) \subset \{\pm 1\}^{\mathbf{Q}^*}$ with the subspace topology, and we write $\mathcal{P} = \{-1\} \cup \{p : p \text{ is prime}\}$.
    a. Show that $\mathrm{Hom}(\mathbf{Q}^*, \{\pm 1\})$ is a compact topological group, that there is an isomorphism of topological groups $\mathrm{Hom}(\mathbf{Q}^*, \{\pm 1\}) \cong \{\pm 1\}^{\mathcal{P}}$, and that $\{\pm 1\}^{\mathcal{P}}$ has a subgroup of index 2 that is not open.
    b. Let $G \subset \mathrm{Hom}(\mathbf{Q}^*, \{\pm 1\})$ be a closed subgroup with the property that for every $a \in \mathbf{Q}^*$ with $a \notin \mathbf{Q}^{*2}$, there exists an $f \in G$ with $f(a) = -1$. Prove: $G = \mathrm{Hom}(\mathbf{Q}^*, \{\pm 1\})$.
    c. Let $\mathbf{Q} \subset L$ be the Galois extension from Example 28.10. Show that there exists an isomorphism $\mathrm{Gal}(L/\mathbf{Q}) \cong \mathrm{Hom}(\mathbf{Q}^*, \{\pm 1\})$ of topological groups.
15. Let $K \subset L$ be a Galois extension with group G, and let $I \subset H$ be two subgroups of G with $(H : I) < \infty$.
    a. Prove: if I is closed in G, then H is also closed in G, and we then have $[L^I : L^H] = (H : I)$.
    b. Prove that, in general, we have $[L^I : L^H] \leq (H : I)$.
    c. Construct an example with $[L^I : L^H] < (H : I)$ and H closed in G.
16. Suppose given a projective system of compact topological groups that are Hausdorff, with continuous group homomorphisms as transition maps. Prove: the projective limit is also a compact topological group that is Hausdorff.
17. Let G be a group, and let I_G be the set of normal subgroups of G of finite index, ordered by $N \leq N' \Leftrightarrow N \supset N'$. The *profinite completion* $\hat{G}$ of G is the limit of the projective system $(G/N)_{N \in I_G}$.
    a. Prove that the profinite completion of the additive group of $\mathbf{Z}$ is the additive group of $\hat{\mathbf{Z}}$. What is the profinite completion of $\mathbf{R}^*$?
    b. Show that there exists exactly one group homomorphism $G \to \hat{G}$ with the property that for every $M \in I_G$, the canonical map $G \to G/M$ is equal to the composition of $G \to \hat{G}$ with the inclusion $\hat{G} \subset \prod_{N \in I_G} G/N$ and the projection $\prod_{N \in I_G} G/N \to G/M$ onto the Mth coordinate.
    c. Show that the image of the group homomorphism from part b is dense in $\hat{G}$.
18. Let $K \subset L$ be a Galois extension, and let I be a set of intermediate fields, all Galois over K, that is directed under inclusion. Assume $\bigcup_{F \in I} F = L$. Prove that, as a topological group, $\mathrm{Gal}(L/K)$ is isomorphic to the projective limit of the system $(\mathrm{Gal}(F/K))_{F \in I}$

of topological groups. (Note that, unlike in Theorem 28.14, we do not assume that all $F \in I$ are finite over K.)

19. Let G be an infinite profinite group. Prove that G is not countable.

20. Let $K \subset L$ be a Galois extension that is not finite, with group G. Prove that G has countably many infinite subgroups and that none of these are closed.

21. Let K, L, M be subfields of a field Ω, with $K \subset L$ and $K \subset M$. Assume that $K \subset L$ is Galois. Prove that $M \subset L \cdot M$ is Galois and that there is an isomorphism $\mathrm{Gal}(L \cdot M/M) \cong \mathrm{Gal}(L/L \cap M)$ of topological groups.

22. Prove that every profinite group is isomorphic to the Galois group of a suitably chosen Galois extension.

23. Let p be a prime. Define the ring $\mathbf{Z}_p$ of p-adic numbers as the projective limit of the system of rings $(\mathbf{Z}/p^n\mathbf{Z})_{n\geq 0}$. Prove: $\mathbf{Z}_p$ is a principal ideal domain of characteristic 0, with $p\mathbf{Z}_p$ as only maximal ideal, and every non-zero ideal of $\mathbf{Z}_p$ is of the form $p^n\mathbf{Z}_p$, with $n \in \mathbf{Z}_{\geq 0}$ uniquely determined by the ideal.

24. Use the Chinese remainder theorem to prove that, as a topological ring, $\hat{\mathbf{Z}}$ is isomorphic to the product ring $\prod_{p\,\mathrm{prime}} \mathbf{Z}_p$, where the topological ring $\mathbf{Z}_p$ is as in Exercise 23 and the product has the product topology.

25. a. Let $n \in \mathbf{Z}_{>0}$. Prove that the inclusion $\mathbf{Z} \subset \hat{\mathbf{Z}}$ induces a ring isomorphism $\mathbf{Z}/n\mathbf{Z} \to \hat{\mathbf{Z}}/n\hat{\mathbf{Z}}$ and that $n\hat{\mathbf{Z}}$ is open in $\hat{\mathbf{Z}}$.
    b. Prove that every subgroup of $\hat{\mathbf{Z}}$ of finite index is open.

26. A *Steinitz number* or *supernatural number* is a formal expression $a = \prod_{p\,\mathrm{prime}} p^{a(p)}$ with $a(p) \in \{0, 1, 2, \ldots, \infty\}$ for every p (Ernst Steinitz, German algebraist, 1871–1928). For a Steinitz number a, we write $a\hat{\mathbf{Z}}$ for the intersection of all subgroups $n\hat{\mathbf{Z}}$ of $\mathbf{Z}$, where n runs through the set of positive integers that "divide" a (in the sense that for every prime p, the number of factors p in n is at most $a(p)$). Prove that there is a bijection from the set of Steinitz numbers to the set of closed subgroups of $\hat{\mathbf{Z}}$, with $a \mapsto a\hat{\mathbf{Z}}$.

27. Let G be a profinite group. We call G *procyclic* if there is an element $g \in G$ with $G = \overline{\langle g \rangle}$. Prove that the following four properties are equivalent:
    (i) The group G is procyclic.
    (ii) The group G is isomorphic to the limit of a projective system consisting of finite cyclic groups.
    (iii) For any two open subgroups H, $I \subset G$ with $(G : H) = (G : I)$, we have $H = I$.
    (iv) There is a Steinitz number a (see Exercise 26) with $G \cong \hat{\mathbf{Z}}/a\hat{\mathbf{Z}}$.

    Also prove that the Steinitz number in part (iv) is uniquely determined if it exists.

28. a. Prove that $\hat{\mathbf{Z}}$ is isomorphic to the limit of the projective system $(\mathbf{Z}/n!\mathbf{Z})_{n>0}$.
    b. Prove that there is a homeomorphism $\prod_{n>0}\{0.1, \ldots, n\} \to \hat{\mathbf{Z}}$ that maps a sequence $(c_n)_{n>0}$ of "numbers" to the infinite sum $\sum_{n>0} c_n n!$; here, every $\{0.1, \ldots, n\}$ has the discrete topology, and the product has the product topology.

29. a. Given $b \in \mathbf{Z}_{\geq 0}$, we define a sequence $(a_n)_{n=0}^{\infty}$ of non-negative integers by $a_0 = b$, $a_{n+1} = 2^{a_n}$. Prove that the sequence $(a_n)_{n=0}^{\infty}$ has a limit in $\hat{\mathbf{Z}}$ and that this limit is independent of b.

b. Write the limit from part a as $\sum_{n>0} c_n n!$, with $c_n \in \{0.1, \ldots, n\}$ (see Exercise 28). Calculate c_n for $1 \leq n \leq 10$.

30. Prove that the field L from Example 28.10 is contained in $\mathbf{Q}^{\mathrm{cycl}}$, and give an explicit description of the map $\hat{\mathbf{Z}}^* \to \{\pm 1\}^{\mathcal{P}}$ obtained by composing the isomorphisms $\mathrm{Gal}(\mathbf{Q}^{\mathrm{cycl}}/\mathbf{Q}) \cong \hat{\mathbf{Z}}^*$ (see 28.15) and $\mathrm{Gal}(L/\mathbf{Q}) \cong \{\pm 1\}^{\mathcal{P}}$ (see 28.10) and the restriction map $\mathrm{Gal}(\mathbf{Q}^{\mathrm{cycl}}/\mathbf{Q}) \to \mathrm{Gal}(L/\mathbf{Q})$.

References

1. Most algebra books cover not only groups and rings but also fields. This holds, in particular, for the books of Artin, Shafarevich, Lang, Gallian, and Van der Waerden already mentioned in the syllabus Algebra II.

2. Liouville's construction of transcendental numbers and transcendence proofs of e and π can be found in Chapter 6 of Stewart's book, or in Chapter 11 of Hardy and Wright's book. Recently, transcendence results were proved for values of modular functions, by, among others, the Russian Nesterenko (Ostrowski Prize 1998). For example, we recently learned that $\sum_{n=0}^{\infty} 2^{-n^2}$ is transcendental and that π and e^{π} are not only both transcendental, they are also *algebraically independent*. The latter means that the map $\mathbf{Q}[X, Y] \to \mathbf{C}$ given by $f \mapsto f(\pi, e^{\pi})$ is injective.

- I. Stewart, *Galois theory*, 2nd edition, Chapman and Hall, 1989.
- G. H. Hardy, E. M. Wright, *An Introduction to the Theory or Numbers*, Oxford, 1938.

3. In a now-famous lecture at the International Congress of Mathematicians in Paris in 1900, the German mathematician David Hilbert (1862–1943) presented twenty-three open problems that he considered important for the development of mathematics in the 20th century. The transcendence conjecture for α^{β} was one of them.

- D. Hilbert, *Mathematische Probleme*, Gesammelte Abhandlungen, Band III, 290–329. Springer, 1970.

See www.mathematik.uni-bielefeld.the/~kersten/hilbert/rede.html for an online version, or Yandell's book to see how work on the problems has progressed.

- B. H. Yandell, *The Honors Class: Hilbert problems and their solvers*, AK Peters, 2003.

4. There exist many computer algebra packages, each with its own strengths and weaknesses. Known commercial systems are Magma, Maple, Mathematica, and Matlab. In addition, there are several open-source packages, which have, for a large part, collectively found a home in William Stein's package SAGE. See the webpage www.sagemath.org.

5. It is, in general, true that the *cardinality* of a transcendence basis of a field extension does not depend on the chosen transcendence basis. This is called the *transcendence degree* of the extension. There is a direct relation between the *dimension* of "geometric rings" such as $K[X_1, X_2, \ldots, X_n]$ over a field K and the transcendence degree of their fields of fractions over K. See, for example, Chapter VIII in Lang's Algebra or Matsumura's book already mentioned in [Algebra II, note **14**].

6. The inverse Galois problem remains unsolved, but much progress has been made in the last fifty years. Shafarevich proved that every finite solvable group occurs as a Galois group over $\mathbf{Q}$, and in the past decades, most simple groups have been successfully realized as Galois groups over $\mathbf{Q}$.

- G. Malle, B. Matzat, *Inverse Galois theory*, Springer, 1999.

7. Lists of transitive subgroups of S_n for $n \leq 22$ are now routinely included in computer algebra packages such as Magma and GAP. The number of isomorphism types of such subgroups

is still only 16 for $n = 6$, but for $n = 16$, it is already 1954. The number does not grow regularly with n: for $n = 19$, there are only 8 isomorphism types.

8. There is a reasonably accessible paper about the Artin map that places the proof of Theorem 24.15 and the remarks following it in a broader context.

- H. W. Lenstra, Jr, P. Stevenhagen, *Artin reciprocity and Mersenne primes*, Nieuw Archief voor Wiskunde **18** (1), 44–54 (2000).

9. It is interesting to see how an algebra textbook looked a century ago and to realize how what is seen as "basic knowledge" for a mathematician has developed over time.

- H. Weber - *Lehrbuch der Algebra*, 3 volumes (1894, 1896, 1908). Reprinted by Chelsea.

10. The remark that the Galois group of a polynomial $f \in \mathbf{Z}[X]$ has group S_n with "probability 1" is due to Van der Waerden. This is a refinement of an argument given in his algebra book to make polynomials with group S_n. The most important ingredient here is the useful fact that the decomposition of a polynomial $f \in \mathbf{Z}[X]$ modulo primes p can be used to see which *cycle types* occur among the permutations in $\mathrm{Gal}(f) \subset S_n$.

- B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109**, 13–16 (1934).

11. All proofs of the Kronecker–Weber theorem, such as that in Chapter 6 of Long's book, use some algebraic number theory. Washington's book, which contains much modern wisdom about the fields $\mathbf{Q}(\zeta_n)$, has a proof in an appendix.

- R. L. Long, *Algebraic number theory*, Marcel Dekker, 1977.
- L. C. Washington, *Introduction to cyclotomic fields*, Springer GTM, 1982. Second edition 1997.

12. The "description" of the absolute Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ of $\mathbf{Q}$ is seen by some as a "holy grail" of number theory. An unpublished manuscript of the French mathematician Alexander Grothendieck already mentioned in Section 15, "*Esquisse d'un programme*," underlies a recent theory that attempts to describe this group through an action on so-called "dessins d'enfants."

- L. Schneps (ed.), *The Grothendieck theory of dessins d'enfants*, LMS Lecture Note Series **200**, Cambridge University Press, 1994.

13. For those who wish to take a look at Greek mathematics, the two parts of the well-known bilingual Loeb series with classical Greek and Roman texts is a good place to start.

- *Greek Mathematical Works*, Loeb Classical Library, vols 335 & 362, Harvard University Press, 1939–1941. Several reprints.

14. Sir Thomas Heath's classic text on Greek mathematics has a separate chapter *Special problems* devoted to these famous problems and their history.

- T. L. Heath, *A history or Greek mathematics*, 2 parts, Oxford University Press, 1921.

15. An extensive discussion of Hippocrates's squaring of lunes and the question "which lunes can be squared," can be found in Heath's book. It was not until 1948 that the Russian mathematician N. G. Chebotarëv—who became known for a very general density theorem about primes—solved this using methods from Galois theory. The article below contains the necessary details on both the lunes and the relation between the density theorem mentioned

above and the determination of Galois groups of polynomials $\mathrm{Gal}(f)$ from the decomposition of $(f \bmod p)$ mentioned in note 10?[23]

- P. Stevenhagen, H. W. Lenstra, Jr., *Chebotarëv and his density theory*, Math. Intelligencer **18**(2), 26–37 (1996).

16. The most current information on Fermat numbers changes annually and can therefore best be looked up on the internet. The website *The Prime Pages* primes.utm.edu mentioned in [Algebra I, note **25**] has links to pages with information on Fermat numbers.

17. There are classic results of Schur on the Galois groups of polynomials that occur in analysis as truncated power series. For example, the nth partial sum $\sum_{i=0}^{n} X^i/i!$ of the exponential sequence is a polynomial in $\mathbf{Q}[X]$ with group S_n if n is not divisible by 4. For $4 \mid n$, the group becomes A_n. The nth Laguerre polynomial $\sum_{i=0}^{n} \binom{n}{i}(-X)^i/i!$ has group S_n for all $n \geq 1$. The polynomial $X^n - X - 1$ also has group S_n for all $n > 1$.

- I. Schur, *Gleichungen ohne Affekt*, Sitzungsber. der Preuß. Akad. der Wiss., Phys.-Math. Kl., 443–449 (1930).

18. The review (in Dutch) in the Nieuw Archief voor Wiskunde of Dieter Jörgenson's historical novel *The Mathematician* gives a good idea of the circumstances under which the radical formulas were found and spread. You can, of course, also read the novel itself.

- N. S. Hekster, *Boekbespreking van 'De Rekenmeester'*, Nieuw Archief voor Wiskunde **5/1**(3), 310–313 (2000).

19. The Galois theory of differential equations is treated in, among others, a classic book of Kaplansky, and in the more recent short book of Magid.

- I. Kaplansky, *An introduction to differential algebraic*, Hermann, 1952.
- A. R. Magid, *Lectures on Differential Geometry*, AMS University Lecture Series **7**, 1994.

20. That the modular group $\mathrm{SL}_2(\mathbf{Z})/\{\pm 1\}$ is the sum of cyclic subgroups of orders 2 and 3 generated by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $W = \left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ follows directly from Theorem 8 in Chapter 2, Section 1 of the following book—although the matrix W in the theorem has a typing error.

- H. Maass, *Lectures on Modular Functions of One Complex Variable*, Tata Institute or Fundamental Research, Bombay, 1964.

21. Corollary 1.2.4 of the following book states that every totally disconnected compact topological group is profinite.

- John S. Wilson, *Profinite groups*, Oxford University Press, 1998.

22. It turns out that it is not easy to prove that every Hausdorff compact topological ring is profinite. Proposition 5.1.2 of the following book gives a sketch of a proof.

- Luis Ribes, Pavel Zalesskii, *Profinite groups*, Springer-Verlag, Berlin, 2000.

Mathematical Institute
Leiden University

Algebra 3 Exam, May 22, 2002, 14:00–17:00

1. Give an element $\alpha \in K = \mathbf{Q}(\sqrt{2}, \sqrt{5})$ with $K = \mathbf{Q}(\alpha)$, and determine the minimum polynomial $f_{\mathbf{Q}}^{\alpha}$.

2. Show that $K_1 = \mathbf{F}_3[X]/(X^3 - X - 1)$ and $K_2 = \mathbf{F}_3[Y]/(Y^3 - Y - 2)$ are isomorphic fields, and give an explicit isomorphism $\phi : K_1 \xrightarrow{\sim} K_2$.

3. Can the angles of an equilateral triangle be trisected with a straightedge and compass? (Explain your answer and give the statements of the theorems you use.)

4. Let $L = \Omega_{\mathbf{Q}}^{X^4-3}$ be the splitting field of $X^4 - 3$ over $\mathbf{Q}$.
   a. Show that $\mathrm{Gal}(L/\mathbf{Q})$ is a non-abelian group.
   b. Show that there exists a subfield $K \subset L$ such that $\mathrm{Gal}(L/K)$ is abelian of order 4.
   c. Is the field K in part b uniquely determined?

5. Define K_2 and K_4 as the unique subfields of $\mathbf{Q}(\zeta_{13})$ of degrees 2 and 4, respectively, over $\mathbf{Q}$. These fields are ordered as follows: $\mathbf{Q} \subset K_2 \subset K_4 \subset \mathbf{Q}(\zeta_{13})$.
   a. Prove: $K_2 = \mathbf{Q}(\sqrt{13})$.
   b. Determine an element $\alpha \in K_2$ such that $K_4 = K_2(\sqrt{\alpha})$.
   c. Does there exist an element $\beta \in \mathbf{Q}$ such that $K_4 = \mathbf{Q}(\sqrt[4]{\beta})$? Explain your answer.

Mathematical Institute
Leiden University

Algebra 3 Exam, June 1, 2004, 14:00–17:00

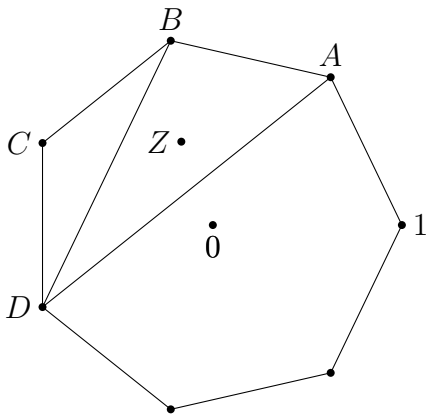
This is an open book exam.
Explain all your answers, if necessary with references to theorems from the syllabus.

1. Determine the following field degrees:
   a. $[\mathbf{Q}(\sqrt{-2},\sqrt{3}):\mathbf{Q}]$
   b. $[\mathbf{R}(\sqrt{-2},\sqrt{3}):\mathbf{R}]$
   c. $[\mathbf{F}_7(\sqrt{-2},\sqrt{3}):\mathbf{F}_7]$
   d. $[\mathbf{F}_{11}(\sqrt{-2},\sqrt{3}):\mathbf{F}_{11}]$.

2. Define polynomials $f_1, f_2, f_3 \in \mathbf{F}_2[X]$ by $f_1 = X^2+1$, $f_2 = X^2+X$, and $f_3 = X^2+X+1$. Answer the following questions for $i \in \{1,2,3\}$:
   a. Is f_i a separable polynomial?
   b. Is $\mathbf{F}_2[X]/(f_i)$ a separable field extension of $\mathbf{F}_2$?

3. a. Prove that the ring $K = \mathbf{Q}[X]/(X^6+3)$ is a field. We also denote this field by $K = \mathbf{Q}(\sqrt[6]{-3})$.
   b. Is K a Galois extension of $\mathbf{Q}$? If so, determine the Galois group. If not, determine the normal closure.
   c. Is the ring $K = \mathbf{Q}[X]/(X^6-72)$ a field? If so, is this field normal over $\mathbf{Q}$? If not, give a maximal ideal of this ring.

4. Consider the regular 7-gon in $\mathbf{C}$ with center 0 and vertex 1, and name the vertices A, B, C, D as indicated. Determine which of the following points are constructible from the set $\{0,1\}$ using a straightedge and compass:
   a. the point A
   b. the middle of the line segment CD
   c. the centroid (geometric center) Z of triangle ABD.



Mathematical Institute
Leiden University

Algebra 3 Exam, June 12, 2006, 10:00–13:00

This is an open book exam.
Write your name and student number on all pages you turn in.
Explain all your answers.

1. Let $K \subset L$ be a field extension, and let α, β in L be transcendental over K.
   a. Give examples that show that $\alpha + \beta$ and $\alpha \cdot \beta$ can be algebraic over K.
   b. Is it possible for $\alpha + \beta$ and $\alpha \cdot \beta$ to both be algebraic over K *at the same time*?

2. Let $K = \mathbf{Q}(\sqrt{3}, \sqrt{7})$.
   a. Give an element α in K such that $K = \mathbf{Q}(\alpha)$.
   b. Determine the minimum polynomial of α over $\mathbf{Q}$.
   c. Determine the subfields of K.

3. Let K be the field $\mathbf{Q}(\sqrt{-3}, \sqrt[3]{5})$.
   a. Determine the degree $[K : \mathbf{Q}]$.
   b. Give a polynomial f in $\mathbf{Q}[X]$ such that K is the splitting field of f over $\mathbf{Q}$.
   c. Determine the field automorphisms of K.
   d. Determine the degree over $\mathbf{Q}$ of the elements

$$\sqrt{-3} \cdot \sqrt[3]{5} \quad \text{and} \quad (\sqrt{-3} + 1) \cdot \sqrt[3]{5}$$

   of K.

4. Let $K = \mathbf{Q}(\zeta_{15})$ with ζ_{15} a primitive 15th root of unity in $\mathbf{C}$.
   a. Prove that K is a Galois extension of $\mathbf{Q}$.
   b. Prove that K contains a primitive fifth root of unity ζ_5.
   c. Determine $[K : \mathbf{Q}(\zeta_5)]$ and $\mathrm{Gal}(K/\mathbf{Q}(\zeta_5))$.

   Let $\alpha = \zeta_{15}^2 + \zeta_{15}^7$.
   d. Prove: $\alpha \in \mathbf{Q}(\zeta_5)$.
   e. Determine the degree of α over $\mathbf{Q}$.

5. Let Φ_n be the nth cyclotomic polynomial.
   a. Decompose Φ_5 and Φ_{12} into irreducible factors in $\mathbf{F}_2[X]$.
   b. For both polynomials, determine the degree of the splitting field over $\mathbf{F}_2$.
   c. Let p be a prime that does not divide n, and let K be a field of characteristic p. Prove: every zero of Φ_n in K is a primitive nth root of unity.

Mathematical Institute
Leiden University

Algebra 3 Exam, June 11, 2007, 10:00–13:00

This is an open book exam: you may use the syllabus, your notes, and (corrected) homework.
You may not use any electronic devices.
Write your name and student number on all pages you turn in.
Explain all your answers, and refer to the theorems you use. You may not refer to results from homework or exercises.

1. Let $\alpha \in \mathbf{R}$ be the unique real zero of $X^3 - 2$. Determine all possible values of $[K(\alpha) : K]$, where K is a subfield of $\mathbf{C}$. For each value, give an example of a K for which this value is assumed.

2. Let $f = X^4 + 9 \in \mathbf{Q}[X]$, and let α be a zero of f in $\overline{\mathbf{Q}}$.
   a. Show that f is irreducible over $\mathbf{Q}$.
   b. Determine the minimum polynomial of $\alpha^3 - 3\alpha + 1$ over $\mathbf{Q}$.
   c. Show that $K = \mathbf{Q}(\alpha)$ is Galois over $\mathbf{Q}$, and determine $\mathrm{Gal}(K/\mathbf{Q})$.
   d. Give all subfields of K.

3. Let Φ_n be the nth cyclotomic polynomial.
   a. Show that Φ_3 and Φ_5 split into linear factors in $\mathbf{F}_{16}$.
   b. Let p be a prime and k a field of characteristic different from p. Let $\zeta \in k$ be a zero of Φ_p. Show that ζ has order p in k^*.
   c. Show that every field over which Φ_3 and Φ_5 split into linear factors has at least 16 elements.

4. Let $\vartheta \in \mathbf{C}$ be defined as in the figure.
   a. Show that $[\mathbf{Q}(\vartheta) : \mathbf{Q}] = 3$.
   b. Given the points 0, 1, and ϑ, is it possible to construct a regular 13-gon using a straightedge and compass?