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, 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 $\ell_{ab}$ be either the line through $a$ and $b$ or the circle through $a$ with center $b$.
   Likewise, let $\ell_{cd}$ be either the line through $c$ and $d$ or the circle through $c$ with center $d$.
3. If $\ell_{ab}$ and $\ell_{cd}$ 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 $X \subseteq \mathcal{F}(X)$. 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 $i \in \mathbb{Z}_{\geq 1}$, 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.\textsuperscript{14}

\section*{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 \textit{lunes of Hippocrates}\textsuperscript{15} (see Exercise 14).

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

This problem is also known as the \textit{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.

\section*{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.

\section*{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 $2\pi$ 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 $\mathbb{C}$ of complex numbers. Using 25.1, the problems mentioned above can easily be reformulated in terms of numbers constructible from a subset $X \subset \mathbb{C}$. After scaling, we may assume that $X$ contains the two points 0 and 1.

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

\section*{25.6. Proposition.} Let $X \subset \mathbb{C}$ be a set that contains 0 and 1. Then $\mathbb{C}(X)$ is a subfield of $\mathbb{C}$ 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 \( |x| \); the line through 1 parallel to the line through \( |x|/x \) and \( |x| \) now cuts the line through 0 and 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 \( x \in \mathbf{R} \)?

![Diagram](image)

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.

![Diagram](image)

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 \( X \subset \mathbb{C} \) be given, and let \( K = \mathbb{Q}(X, \bar{X}) \) be the subfield of \( \mathbb{C} \) generated by the elements in \( X \) and their complex conjugates. Then every point \( z \in \mathbb{C} \) 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 \( z \in \mathbb{C} \) for which \( (z - a)/(a - b) \) is real. Expanding the identity \( (z - a)/(a - b) = (\bar{z} - \bar{a})/(\bar{a} - \bar{b}) \) gives the following equation for this line:

\[
\ell_{ab} : (\bar{a} - \bar{b})z - (a - b)\bar{z} = \bar{a}b - a\bar{b}.
\]

Intersecting the lines \( \ell_{ab} \) and \( \ell_{cd} \) amounts to solving two linear equations in \( z \) and \( \bar{z} \) with coefficients in \( \mathbb{Q}(a, b, c, d, \bar{a}, \bar{b}, \bar{c}, \bar{d}) \subset K \). If \( \ell_{ab} \) and \( \ell_{cd} \) 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 \( \ell_{ab} \) and \( \ell_{cd} \) 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 \( (z - d)(\bar{z} - \bar{d}) = (c - d)(\bar{c} - \bar{d}) \) or

\[
z\bar{z} - \bar{d}z - d\bar{z} = c\bar{c} - cd - \bar{c}d.
\]

For a point \( z \) on the line \( \ell_{ab} \) that lies on this circle, we can use the equation for \( \ell_{ab} \) to write \( \bar{z} \) 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 \( \bar{z} \) 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. \( \square \)

**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 \( \mathbb{Q} \subset \mathbb{Q}(\sqrt{\mathbb{Q}}) \) is an infinite extension.
25.8. Definition. Let \( K \) be a field of characteristic \( \text{char}(K) \neq 2 \) with algebraic closure \( \overline{K} \). Then the quadratic closure \( K^{\text{quad}} \) of \( K \) in \( \overline{K} \) is the field

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

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 \( X \subset \mathbb{C} \) that contains 0 and 1 is equal to the quadratic closure of the field \( \mathbb{Q}(X, \overline{X}) \) in \( \mathbb{C} \).

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 \( K = \mathbb{Q}(X, \overline{X}) \) 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 \( K = \mathbb{Q}(X, \overline{X}) \) 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 \( K_1 = K(\sqrt{\overline{K}}) \). Note that along with \( K \), the field \( K(\sqrt{\overline{K}}) \) 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 \( K = \mathbb{Q}(X, \overline{X}) \).

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

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

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

\[
K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_{n-1} \subset E_n \subset \mathbb{C}
\]

of intermediate fields of \( K \subset \mathbb{C} \) 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) \( \Rightarrow \) (1). Let \( V \subset \mathbb{C} \) 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 \( x \in E_n \subset K_n \subset K^{\text{quad}} \). This proves \( V \subset K^{\text{quad}} \).

(1) \( \Rightarrow \) (2). For the inclusion \( K^{\text{quad}} \subset V \) with \( V \) as above, we show that \( V \) is a subfield of \( \mathbb{C} \) 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 \( C \), 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 \( Q(x, y) \subset E_rF_s \) are contained in \( V \). This shows that \( V \) is a field.

(2) \implies (3). If for \( x \in C \), 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 \( M \subset C \) of \( E_n \) over \( K \) and \( \sigma \in Gal(M/K) \) 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 \( \sigma \in Gal(M/K) \) as explained above to one long chain, we obtain a tower of quadratic extensions ending in the compositum \( M \) of the collection of fields \( \{\sigma[E_n]\}_{\sigma \in Gal(M/K)} \). It follows that \( Gal(M/K) \) is a 2-group, and the Galois group \( Gal(f_K^f) \) of the subextension \( \Omega^{f_K}_K \subset M \) over \( K \) is therefore also one.

(3) \implies (2). It follows from 10.17 (“solvability of \( p \)-groups”) that in the 2-group \( G = Gal(f_K^f) \), 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 \( E_i \subset \Omega^{f_K}_K \) give a chain that satisfies the conditions in (2). \( \square \)

**Exercise 4.** Show that 25.10 is correct for any field \( K \) of characteristic different from 2 if, everywhere, we replace \( C \) 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 \( \pi \) is transcendental, then it follows from 25.9 and 25.10.3 that \( \pi \) and \( \sqrt{\pi} \) are not constructible, so we cannot square the circle with a straightedge and compass.

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

For \( \alpha \in C \) with \( |\alpha|^2 = \alpha \overline{\alpha} = 1 \), trisecting the angle \( \angle 10\alpha \) corresponding to \( \alpha \) with a straightedge and compass is not possible if \( X^3 - \alpha \) is irreducible over \( Q(\alpha, \overline{\alpha}) = Q(\alpha) \). This is the case for “most” \( \alpha \), including all transcendental values of \( \alpha \); see Exercises 20 and 21. In the rare reducible case, which occurs, for example, for \( \alpha = \pm 1 \) and \( \alpha = i \), a splitting field \( \Omega^{X^3-\alpha}_Q \) 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 \( Q(\zeta_n) \) over \( Q \) 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 \( n = \prod_{p \mid n} p^{e_p} \), then 6.16 gives the value \( \varphi(n) = \prod_{p \mid n} (p - 1)^{e_p} - 1 \). 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 \( k \)th Fermat number. The first five Fermat numbers \( F_k = 2^{2^k} + 1 \) for \( k \geq 0 \) 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 \( k \)th Fermat number. The \( f \)th Fermat number \( F_k \) is not prime, and neither are the numbers \( F_k \) with \( 6 \leq k \leq 32 \). It is not known 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 24.9.2. 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 \( \mathbb{Q} \) in \( \mathbb{C} \) can also be given for the radical closure \( \mathbb{Q}^{\text{rad}} \) of \( \mathbb{Q} \) in \( \mathbb{C} \). 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 \( K^{\text{rad}} \) of \( K \) in \( \overline{K} \) is the field \( K^{\text{rad}} = \bigcup_{i=0}^{\infty} K_{(i)} \), 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 \( K^{\text{rad}} \) 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 \( p \)th 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

\[
K \subset K^{\text{quad}} \subset K^{\text{rad}} \subset \overline{K}.
\]

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 \( \mathbb{Q}_{\text{rad}} \) is not equal to \( \overline{\mathbb{Q}} \), and in 25.17, we will construct polynomials in \( \mathbb{Q}[X] \) whose zeros are in \( \mathbb{Q} \) but not in \( \mathbb{Q}_{\text{rad}} \).

A word of warning is in order when using the notation \( \sqrt[n]{a} \) to indicate an \( n \)th 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 \( \alpha \) of \( X^8 - 16 \) to \( \mathbb{Q} \) would lead to the field \( \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}) \). However, we also have \( 16 = (-2)^4 \), so that \( \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-2}) \) is another field that is as “justifiable.” Similar problems occur when extracting “an” \( n \)th root of 1. Thus, it is better to avoid the notation \( \sqrt[n]{1} \) because not all zeros of \( X^3 - 1 \) generate the same extension of \( \mathbb{Q} \). 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 \( n \)th 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 \( \mathbb{Q}(\zeta_5) \) is a radical extension of \( \mathbb{Q} \) but not an irreducible radical extension.

Although not every radical extension is irreducible, the field \( K_{\text{rad}} \) 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 \( n \in \mathbb{Z}_{\geq 0} \) 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 \( f_K \) over \( K \) is a solvable group.

70
A finite extension $K \subset E$ is called solvable if the Galois group $\text{Gal}(M/K)$ 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

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

in $\text{Gal}(M/K)$ 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 $f_{K}(x) = 0$ 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 $n$th 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 $d$th power in $K$.

Proof. (1) Let $\sigma$ be a generator of $\text{Gal}(L/K)$ and $\zeta \in K$ a primitive $n$th 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 $\sigma$ 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 $\sigma$ to the identity $\sigma(\alpha) = \zeta \alpha$ gives the relation $\sigma^i(\alpha) = \zeta^i \alpha$. It follows that the subgroup $\text{Gal}(L/K(\alpha)) \subset \text{Gal}(L/K)$ of powers of $\sigma$ that fix $\alpha$ 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 $\alpha$ 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 $\tau \in \text{Gal}(L/K)$, we then have $(\tau(\alpha)/\alpha)^n = (\tau(\alpha^n)/\alpha^n) = \tau(a)/a = 1$, so the map

$$\psi : \text{Gal}(L/K) \longrightarrow \langle \zeta \rangle$$

$$\tau \longmapsto \frac{\tau(\alpha)}{\alpha}$$
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 \( \psi \) is injective because a \( K \)-automorphism that fixes \( \alpha \) is the identity on \( L = K(\alpha) \).

We conclude that \( \text{Gal}(L/K) \) is cyclic of degree \( n/d \), where \( d \) is the index of \( \psi[\text{Gal}(L/K)] \) in \( \langle \zeta \rangle \). For all \( \tau \in \text{Gal}(L/K) \), 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 \( d \)th power in \( K \). If, conversely, we have \( a = b^t \) with \( t | n \) and \( b \in K \), then the \( t \)th 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 \( \psi[\text{Gal}(L/K)] \) is annihilated by \( n/t \) and lies in the subgroup of index \( t \) in \( \langle \zeta \rangle \). Consequently, we have \( t \leq d \), so \( d \) is the largest divisor of \( n \) for which \( a \) is a \( d \)th 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 \( K^{\text{rad}} \); it follows that we have \( V = K^{\text{rad}} \).

For (2) \( \Rightarrow \) (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 \( \zeta \) 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 \( E_1(\zeta) \subset E_{i+1}(\zeta) \) are cyclic by 25.16.2. By looking at the corresponding chain of subgroups in \( \text{Gal}(L/K) \), we conclude that \( \text{Gal}(L/K) \) is solvable. It then follows from \( \Omega_{K/K}^{f} \subset L \) that \( \text{Gal}(f) \), as a quotient of \( \text{Gal}(L/K) \), is also solvable.

For (3) \( \Rightarrow \) (2), let \( f = \psi \) have a solvable Galois group \( \text{Gal}(f) = \text{Gal}(\Omega_{K/K}^{f}) \) of order \( N \). If \( \zeta \) is again a primitive root of unity of order \( N \), then the first step in the tower \( K = E_0 \subset E_1 = K(\zeta) \subset \Omega_{K/K}^{f} \) is a radical extension. By (3), the extension \( E_1 = K(\zeta) \subset \Omega_{K/K}^{f} \) 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 \( \mathbb{Q}^{\text{rad}} \) is a proper subfield of \( \overline{\mathbb{Q}} \), we show that there exist polynomials in \( \mathbb{Q}[X] \) 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 \( \mathbb{Q}[X] \) with group \( S_5 \).

**25.17. Theorem.** Let \( f \in \mathbb{Q}[X] \) be an irreducible polynomial of degree 5 with exactly three real zeros. Then we have \( \text{Gal}(f) \cong S_5 \), and \( f \) has no zeros in \( \mathbb{Q}^{\text{rad}} \).
Proof. By 24.6, the group $\text{Gal}(f)$ is a subgroup of $S_5$ of order divisible by 5. This means that $\text{Gal}(f)$ contains an element of order 5 (Cauchy’s theorem); such an element in $S_5$ is necessarily a 5-cycle. If we view $\mathbb{Q}$ as a subfield of $\mathbb{C}$, then complex conjugation gives an automorphism of $\Omega_{\mathbb{Q}}$ that, because of the assumption, interchanges two zeros of $f$ and fixes the other three. Now, $\text{Gal}(f)$ 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, $\text{Gal}(f)$ is not solvable, and by 25.15, the polynomial $f$ has no zeros in $\mathbb{Q}^{\text{rad}}$. □

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 $f(0) = 2$ 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 of polynomials $\{f_n\}_{n=1}^\infty$ with $\text{Gal}(f_n) \cong S_n$.

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 $aX^2 + bX + c \in \mathbb{R}[X]$. The formula holds not only over $\mathbb{R}$ 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

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

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

\[
\begin{align*}
 u^3 + v^3 &= -q \\
 uv &= -p/3.
\end{align*}
\]

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

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

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.

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

\[(25.20) \quad (Y^2 + s)^2 = (p + 2s)Y^2 + qY + (s^2 + r).\]

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

\[(25.21) \quad (p + 2s)(s^2 + r) = q^2/4,
\]

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 $0, 1 \in \mathbb{C}$ as in the figure, and determine $z = a + bi$.]

16. Let $X \subset \mathbb{C}$ 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 $K \subset \mathbb{C}$ be a field that maps to itself under complex conjugation. Prove that $K_{\text{quad}} \subset \mathbb{C}$ also maps to itself under complex conjugation.

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

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

20. Show that trisecting the angle associated with $\alpha \in \mathbb{C}$ with $|\alpha| = 1$ with a straightedge and compass is not possible if $\alpha$ 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 \( x \in \mathbb{C} \) be a constructible element. Define \( K_i \) as in 25.8 for \( K = K_0 = \mathbb{Q} \). 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:

\[
\sqrt{1+\sqrt{2}}, \quad \sqrt{3-2\sqrt{2}}, \quad \zeta_5, \quad \zeta_{12}, \quad \sqrt{1+2\sqrt{-6}}.
\]

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

24. Define real numbers \( x_i \in \mathbb{R}_{\geq 0} \) recursively by \( x_0 = 0 \) and \( x_{i+1} = \sqrt{2+x_i} \) for \( i \geq 0 \).

a. Prove: \( \mathbb{Q} \subset \mathbb{Q}(x_i) \) 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 \( K^{\text{quad}} \), 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 \( x \in \mathbb{Q}^{\text{rad}} \), and show that the radical depth of \( x \) depends only on \( \text{Gal}(f_{Q\zeta}) \). *Do there exist elements of arbitrarily large radical depth?

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

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

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 \( \mathbb{Q} \).

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

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

30. Show that every extension \( \mathbb{Q} \subset \mathbb{Q}(\zeta_n) \) is solvable by irreducible radicals.

[Hint: induction on \( n \).]

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

\[
K = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_{n-1} \subset E_n \subset \overline{K}
\]

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 \( \alpha \) of an Artin–Schreier polynomial \( f = X^p - X - a \in K[X] \).

[This is the analog of 25.16.1 for \( n = p = \text{char}(K) \). Hint: look at the resolvent \( \sum_{i=0}^{p-1} \alpha^i(x) \) 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 \( n = p = \text{char}(K) \). 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 \( \text{char}(K) \neq 2, 3 \). Show that \( Y = \xi \eta (\xi + \eta) \) is a zero of \( Y^3 + pY + q \in K[Y] \) if \( \xi \) and \( \eta \) 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 \( k \in \mathbb{Z}_{\geq 0} \) be the \( k \)th Fermat number.

a. Prove: for \( k \in \mathbb{Z}_{\geq 0} \), 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 \( n \in \mathbb{Z}_{\geq 3} \) for which a regular \( n \)-gon, a regular \( n + 1 \)-gon, and a regular \( n + 2 \)-gon are all constructible.

41. Let \( k \in \mathbb{Z}_{\geq 0} \), and let \( p \) be a prime factor of \( F_k \).

a. Prove: the order of \( (2 \mod p) \) in the group \( \mathbb{F}_p^* \) is equal to \( 2^{k+1} \), and for \( k \geq 2 \), the order of \( (F_{k-1} \mod p) \) in \( \mathbb{F}_p^* \) is equal to \( 2^{k+2} \).

b. Prove: for \( k \geq 2 \), we have \( p \equiv 1 \mod 2^{k+2} \).

42. Let \( \mathbb{F} \) be a finite field. Prove that the following two statements are equivalent:

a. For any two subgroups \( A \) and \( B \) of \( \mathbb{F}^* \), we have \( A \subset B \) or \( B \subset A \).

b. Either \( \#\mathbb{F} \) is equal to 2, 9, or a Fermat prime, or \( \#\mathbb{F} - 1 \) is a Mersenne prime.

43. For a group \( G \) and \( k \in \mathbb{Z}_{\geq 0} \), we define the subgroup \( G^{(k)} \) of \( G \) recursively by

\[
G^{(0)} = G \quad \text{and} \quad G^{(k+1)} = [G^{(k)}, G^{(k)}].
\]
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 $\iff$ every subgroup of $G$ is solvable $\iff$ $N$ and $G/N$ are both solvable $\iff$ there exists a $k \in \mathbb{Z}_{\geq 0}$ with $G^{(k)} = \{e\} \iff$ 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 $\alpha \in L^\ast$. Prove:

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

[Hint for $\Rightarrow$: 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 $\sigma, \tau \in G$, we have $c(\sigma \tau) = c(\sigma) \cdot c(\tau)$ if and only if there exists a $\beta \in L^\ast$ such that for every $\sigma \in G$, we have $c(\sigma) = \sigma(\beta)/\beta$.

b. Show how the previous exercise follows from part (a).
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. 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 $\mathbb{C}$ of complex numbers is algebraically closed. There are many proofs, which all use certain “topological arguments.” This is not surprising because the construction of $\mathbb{R}$ from $\mathbb{Q}$ using Dedekind cuts or Cauchy sequences is more a topological construction than an algebraic one, and unlike $\mathbb{C} = \mathbb{R}(i)$, the field $\mathbb{Q}(i)$ is not algebraically closed. As a topological argument, we use the intermediate value theorem for polynomials in $\mathbb{R}[X]$: a polynomial $f \in \mathbb{R}[X]$ that takes on both a positive and a negative value has a real zero.

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

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

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

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

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

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 $\mathbb{C}$ is algebraically closed.
Proof. We must prove that $C$ has no non-trivial algebraic extensions. Let $C \subset L$ be finite algebraic, and let $M$ be the normal closure of $L$ over $R$. Then $R \subset M$ 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 $R$ whose degree $[E : R] = [G : H]$ is odd. By 26.1, we get $E = R$ and $G = H$, so $G$ is a 2-group. In particular, the subgroup Gal$(M/C) \subset G$ is a 2-group. By 10.17, the group Gal$(M/C)$ is therefore solvable. As in 10.14, this means that there exists a chain

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

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

Quadratic reciprocity

The calculation of the quadratic subfield of $\mathbb{Q}(\zeta_p)$ for prime $p$ carried out in 24.11 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 $p \equiv \pm 2 \pmod{5}$.

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

$$\mathbb{F}_p^* \rightarrow \langle -1 \pmod{p} \rangle \xrightarrow{\sim} \{ \pm 1 \}$$

$$x \pmod{p} \mapsto x^{(p-1)/2} \pmod{p} \mapsto \left( \frac{x}{p} \right).$$

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 $\mathbb{F}_p^*$ and $-1$ if $x$ is not a square in $\mathbb{F}_p^*$. 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

$$\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4}.$$

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 $p \equiv q \equiv 3 \pmod{4}$, 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 24.9 and 24.11, we know that \( \mathbb{Q}(\zeta_p) \) is a Galois extension of \( \mathbb{Q} \) with group \( (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^* \) and that the subgroup \( S_p \subset \mathbb{F}_p^* \) of squares corresponds with the intermediate field \( \mathbb{Q}(\sqrt{p^r}) \), where \( p^r = (-1)^{(p-1)/2}p \). This gives

\[
\left( \frac{q}{p} \right) = 1 \iff (q \mod p) \in S_p \iff \sigma_q(\sqrt{p^r}) = \sqrt{p^r}.
\]

The automorphism \( \sigma_q \) is a type of “lift to characteristic 0” of the Frobenius automorphism \( F_q \) on \( \mathbb{F}_q \). More precisely, if \( \zeta \) is a primitive \( p \)th root of unity in an algebraic closure \( \overline{\mathbb{F}}_q \) of \( \mathbb{F}_q \), then the reduction map \( \mathbb{Z} \to \mathbb{F}_q \) has an extension

\[
r : \mathbb{Z}[\zeta_p] \to \mathbb{F}_q
\]

\[
\sum_i a_i \zeta_p^i \mapsto \sum_i a_i \zeta^i
\]

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

We now have

\[
F_q(w) = w \iff w^{q-1} = 1 \iff (p^r \mod q)^{(q-1)/2} = 1 \iff \left( \frac{p^r}{q} \right) = 1,
\]

and we find

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

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

Symmetric polynomials

In the main theorem 14.1 for symmetric polynomials, we saw that for \( n \in \mathbb{Z}_{\geq 1} \), 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

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

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

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

the ring of invariants is equal to \( \mathbb{Z}[s_1, s_2, \ldots, s_n] \). 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 $n \in \mathbb{Z}_{\geq 1}$, the field $\mathbb{Q}(T_1, \ldots, T_n)$ is the splitting field of the general polynomial $F_n$ of degree $n$ over $\mathbb{Q}(s_1, \ldots, s_n)$. The extension

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

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 $K = \mathbb{Q}(s_1, \ldots, s_n)$, the splitting field of the general polynomial $F_n \in K[X]$ of degree $n$ is equal to $L = \mathbb{Q}(T_1, \ldots, T_n)$, 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 $\text{Gal}(L/K)$ 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 $\delta_n$ to define the sign map $\varepsilon : S_n \to \{\pm 1\}$ by setting $\sigma(\delta_n) = \varepsilon(\sigma) \cdot \delta_n$. The stabilizer of $\delta_n$ 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 $\delta_n$, 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 $\Delta_n$ 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 $L = \mathbb{Q}(T_1, T_2, T_3)$ is cyclic of degree 3 over the quadratic extension of $K = \mathbb{Q}(s_1, s_2, s_3)$ generated by

$$\delta_3 = \sqrt{\Delta_3} = (T_1 - T_2)(T_1 - T_3)(T_2 - T_3) = (T_1^2T_2 + T_1T_3^2 + T_2^2T_3) - (T_1^2T_3 + T_1T_2^2 + T_2T_3^2).$$

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

$$U = T_1 + \zeta_3T_2 + \zeta_3^2T_3$$
$$V = T_1 + \zeta_3^2T_2 + \zeta_3T_3.$$
In terms of these resolvents and $s_1 = T_1 + T_2 + T_3 \in K$, we now have the expressions

\begin{align*}
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{align*}

(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 $\zeta_3$. 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.