Chapter 5

Galois Theory

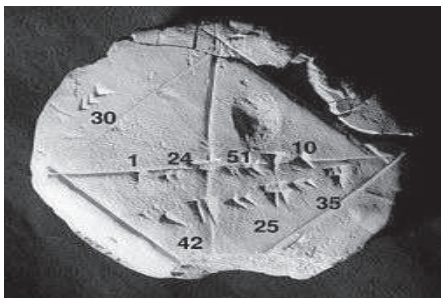
In the work of Galois on roots of polynomials groups appeared for the first time in history. For this reason Galois theory was a very important step in the development of algebra as we know it today. Moreover the theory of Galois provided a striking example of the power of group actions. After the publication of Galois' work (in 1846) his theory has seeen a tremendous development and is now key to understanding various areas of algebra and geometry.

In this chapter we describe some of the basic concepts and constructions of modern Galois theory, focussing on field extensions of finite degree. (The infinite case is very important and interesting as well, but requires a lot more technical tools.) We will use many results from group theory (Chapter 3) and from the theory of field extensions (Chapter 4). From the latter especially the concept of splitting field (Section 4.6) will play a major role.

We start with a very brief description of the historical roots of Galois theory; here we see how the concept and use of symmetry has been developed.

5.1 How it all began

Galois theory is concerned with roots of polynomials. The main problem that led Galois to invent his theory was the one of finding radical expressions for the roots of a polynomial (or proving that no such expressions can be found). This problem has a rather long history as demonstrated by certain clay tablet dating back to at least 1500 BC, and found in current Iraq:



This shows that the ancient Babylonians knew how to solve an equation of degree two, in modern notation: $x^2 + bx + c = 0$. Given this knowledge the question comes up whether we can find formulas for the roots of polynomials of higher degree, for example of degree three: $x^3 + ax^2 + bx + c = 0$. The history regarding those equations starts rather spectacularly in the italian renaissance.

5.1.1 Cardano and the others

In the sixteenth century mathematicians from northern Italy found magnificent formulas for finding the roots of polynomial equations of degree three and four. The main players in this story are Scipione del Ferro (1465-1526, from Bologna), Nicolò Fontana, called il Tartaglia (1499-1557, from Brescia) and Girolamo Cardano (1501-1576, from Milano).

Scipione del Ferro

Nicolò Tartaglia

Girolamo Cardano

Scipione del Ferro was the first to find a formula for the roots of polynomials of degree 3. However, he did not publish it in any form, preferring to keep his discovery to himself, written down in a little notebook. Apparently the mathematicians of those days had a bit of a habit to keep their discoveries to themselves. The reason for this tendency to secrecy was that they often tried to impress other people with their mathematical skill, and even fought mathematical duels between each other. It is clear that the person with more secrets was more likely to excell at such events. However, in the centuries after del Ferro's death his notebook was lost, so we do not know exactly what he discovered.

Before he passed away del Ferro revealed the secret of his formula for the cubic equation to a student of his, Antonio Maria del Fiore. Antionio del Fiore went round in mathematical circles bragging about his knowledge. Tartaglia, who was interested in the problem of solving cubic equations himself, heard about it, and accepted a *cartello di matematica disfida* from Antonio del Fiore. This was a mathematical duel where each contestant gave thirty mathematical problems to his opponent. The winner would be the one who managed to solve more problems. Tartaglia proposed thirty problems of various nature, whereas del Fiore wrote down thirty cubic equations. However, in the meantime Tartaglia had on his own discovered the formula for solving the cubic, so he easily won the contest.

At around that time Girolamo Cardano was writing a book, called the *Ars Magma* (or in full *Artis Magnae, Sive de Regulis Algebraicis Liber Unus*), on algebra. He learned about the contest won by Tartaglia and was very keen on including the formula for the cubic in his book. However, Tartaglia, like Scipione del Ferro, wanted to keep the secret to himself, and only revealed the formula to Cardano when the latter promised not to publish it.

Lodovico Ferrari (1522-1565), who was a collaborator of Cardano, then also found a way to solve equations of degree four. One step of his method consisted in solving an equation of degree 3. So without Tartaglia's formula Cardano and Ferrari could not publish their new discovery either. At this point Cardano and Ferrari recalled the contest with Antionio del Fiore, who had obtained the solution to the cubic from his bolgnese master Scipione del Ferro. They went to Bologna where they found del Ferro's notebook that had been kept by Annibale della Nave, who was his successor at the university of Bologna. Because he had now found the formula also from a different source, Cardano found that he was no longer bound by the promise made to Tartaglia and published the formulas for the cubic and quartic equations in his Ars Magna. Cardano did write that the formulas for the cubic were due to del Ferro and Tartaglia. But the latter was extremely annoyed just the same.

5.1.2 Lagrange

After the publication of the Ars Magna the obvious question arose whether a formula could be found to solve equations of degree 5. The first to systematically investigate this question was Joseph-Louis Lagrange (1736-1813)

who in his great book *Réflexions sur la résolution algébrique des équations* devised a method for solving polynomial equations of arbitrary degree. For degrees 2,3,4 his method yielded the known formulas, but for degree 5 the method failed.

Here we have a short look at Lagrange's method. Consider, for example, an equation of degree 3, $x^3 + ax^2 + bx + c = 0$. Let $\alpha_1, \alpha_2, \alpha_3$ be its solutions. Lagrange considered symmetric expressions in these α_i; these are polynomials in the α_i that remain invariant when we permute the α_i. For example

$$\alpha_1\alpha_2\alpha_3^2 + \alpha_1^2\alpha_2\alpha_3$$

Joseph-Louis Lagrange

is not symmetric because if we interchange α_1, α_2 the expression becomes

$$\alpha_2\alpha_1\alpha_3^2 + \alpha_2^2\alpha_1\alpha_3 = \alpha_1\alpha_2\alpha_3^2 + \alpha_1\alpha_2^2\alpha_3$$

which is not equal to the original expression. On the other hand,

$$\alpha_1^4\alpha_2\alpha_3 + \alpha_1\alpha_2^4\alpha_3 + \alpha_1\alpha_2\alpha_3^4$$

is symmetric. A fundamental fact concerning these symmetric expressions (known before Lagrange) is the following: *a symmetric expression in $\alpha_1, \alpha_2, \alpha_3$ can be computed as a polynomial in a, b, c.* For example,

$$\alpha_1^4\alpha_2\alpha_3 + \alpha_1\alpha_2^4\alpha_3 + \alpha_1\alpha_2\alpha_3^4 = a^3c - 3abc + 3c^2.$$

Now let $\omega = \frac{-1+\sqrt{-3}}{2}$, then $\omega \in \mathbb{C}$ has the property $\omega \neq 1$ but $\omega^3 = 1$. Set

$$\begin{aligned}
z_1 &= \tfrac{1}{3}(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)\\
z_2 &= \tfrac{1}{3}(\alpha_1 + \omega\alpha_3 + \omega^2\alpha_2)\\
z_3 &= \tfrac{1}{3}(\alpha_2 + \omega\alpha_1 + \omega^2\alpha_3)\\
z_4 &= \tfrac{1}{3}(\alpha_2 + \omega\alpha_3 + \omega^2\alpha_3)\\
z_5 &= \tfrac{1}{3}(\alpha_3 + \omega\alpha_1 + \omega^2\alpha_2)\\
z_6 &= \tfrac{1}{3}(\alpha_3 + \omega\alpha_2 + \omega^2\alpha_1),
\end{aligned}$$

and define the so called *resolvent polynomial* $r = (x - z_1)(x - z_2)(x - z_3)(x - z_4)(x - z_5)(x - z_6)$. Because permuting the α_i means that we permute the z_i it follows that the coefficients of r are symmetric expressions in the α_i. In particular, they can be expressed as polynomials in a, b, c. In fact, a small calculation shows that $r = x^6 + qx^3 - \frac{p^3}{27}$ where $q = \frac{2a^3}{27} - \frac{ab}{3} + c$ and $p = -\frac{a^2}{3} + b$. We see that by some miracle r has a form that it makes it easy to find its roots: it is a quadratic polynomial in x^3. So by finding its roots we find the z_j and from there we can find the α_i. This then yields the same formulas as found by del Ferro and Tartaglia.

One of the main reasons why Lagrange's method is important is his use of symmetric expressions. It is one of the the first occasions that *symmetry*, understood as invariance under some transformations (in this case they are permutations of the roots) is used in a systematic way.

5.1.3 Ruffini and Abel

Paolo Ruffini (1765-1822) was an italian mathematician and medical doctor. In 1799 he published a book, entitled *Teoria generale delle equazioni*, with a proof of the impossibility of resolving equations of degree five by radicals. He sent a copy of the book to Lagrange but never received an answer. His argument was a valid attempt at proving the impossibility of resolving the quintic, but in the end it was not quite correct.

Niels Henrik Abel (1802-1829) was a norwegian mathematician who in 1824 gave the first fully accepted proof that it is not possible to solve the quintic by radicals. He used a similar strategy as Ruffini and essentially closed the gap in Ruffini's proof. Abel, like Lagrange, used permutations of the roots of a general equation of degree 5. One essential step in his proof was the following fact (stated in modern language): let the symmetric group S_5 act on the set X, then the orbit of an $x \in X$ cannot have 3 or 4 elements.

Paolo Ruffini

Niels Henrik Abel

5.1.4 Galois

Évariste Galois

Évariste Galois (1811-1832) was a french mathematician and revolutionary. He died in a duel, of which the circumstances are not exactly known, at the age of 20. By that time he had written a paper entitled *Mémoire sur les conditions de résolubilité des équations par radicaux* on the problem of solving polynomial equations by radicals. He submitted several versions of it to the french academy of sciences, but some were lost and the final one, submitted in 1831, was rejected on the grounds that it was hard to read and did not have a criterion that could easily be applied to a given polynomial. (In fact, in order to apply the theory of Galois to a polynomial one first has to compute its splitting field, which can be rather difficult.)

When Galois started to work on solving polynomial equations he probably considered the question as to the solvability of the general equation of degree 5 as closed (and settled by Abel). However, there obviously are polynomials of degree 5 that can be solved by radicals; for a trivial example consider $x^5 - 2$. So Galois considered a different question: when is a given polynomial solvable by radicals? In his solution he went far beyond the mathematics of people such as Lagrange and Abel. For example, Lagrange had considered *all* permutations of the roots of a polynomial, but one of the main results of Galois was that there is a group G_f of permutations of the roots of a polynomial f such that *1) every expression in the roots that is invariant under these permutations is rational* (that is, lies in $\mathbb{Q}$), *2) every expression in the roots that is rational is invariant under these permutations.* It is important to remark here that Galois used a notion of invariance different from Lagrange's: while Lagrange was only considered with the *form* of an expression (that is, he saw them as expressions in formal indeterminates), Galois was concerned with the *value* of the expression (i.e., the exact numerical value).

In 1842, so ten years after Galois' death, Joseph Liouville somehow received Galois' papers and started reading them. A year later he communicated to the french academy that he would publish the work of Galois, which he did in 1846.

5.2 Separable polynomials

Let F be a field and $f \in F[x]$ an *irreducible* polynomial. Then we say that f is *separable* if the roots of f in a splitting field of f all have multiplicity one (in other words, when f has exactly $\deg f$ distinct roots in its splitting field). Because two different splitting field of f are isomorphic via an isomorphism whose restriction to F is the identity (Corollary 4.6.8), this notion does not depend on the choice of

splitting field. More generally we say that a not necessarily irreducible $f \in F[x]$ is separable if its irreducible factors are separable.

Remark 5.2.1 Opinion seems to be divided as to what the best definition of separability for reducible polynomials should be. Many authors use a simpler definition, and define a polynomial to be separable if it has roots of multiplicity one in its splitting field. With this definition the polynomial $x^4 + 2x^3 + 3x^2 + 2x + 1 \in \mathbb{Q}[x]$ is not separable as it is equal to $(x^2 + x + 1)^2$, whereas with our definition it is separable. This difference usually does not lead to confusion, because the only polynomials whose separability is of interest are the irreducible ones.

There is a simple criterion for deciding whether a given polynomial is separable or not based on Lemma 4.7.2. Let $f \in F[x]$ be irreducible and suppose that it is not separable. Then the mentioned lemma says that f and f' have a common root. That means that $\gcd(f, f')$ (which lies in $F[x]$!) has degree at least 1. As f is irreducible that implies that $f = \gcd(f, f')$. Hence f divides f' which, because of their respective degrees, is only possible when $f' = 0$. Write $f = a_0 + a_1x + \cdots + a_mx^m$; then $f' = a_1 + 2a_2x + \cdots + ma_mx^{m-1}$. So $f' = 0$ if and only if $ia_i = 0$ for $i \geq 1$. That implies that the characteristic of F is a prime $p > 0$ and $a_i = 0$ whenever p does not divide i. In other words, we have

$$f = a_0 + a_px^p + \cdots + a_{kp}x^{kp},$$

that is f is a polynomial in x^p. This shows one implication of the following lemma.

Lemma 5.2.2 *Let F be a field and let $f \in F[x]$ be irreducible. Then f is not separable if and only if the characteristic of F is a prime p and f is a polynomial in x^p.*

Proof. We still need to prove the other direction. Suppose that the characteristic of F is a prime p and f is a polynomial in x^p. Then $f' = 0$. Consider a root α of f in a splitting field E. Then $f = (x-\alpha)g$ for some $g \in E[x]$. Hence $f' = g + (x-\alpha)g'$ and as $f' = 0$ it follows that $f = -(x-\alpha)^2g'$, so that f is not separable. □

Remark 5.2.3 We expand a little on remark 5.2.1. Consider $f = x^4 + x^2 + 1 \in \mathbb{F}_2[x]$. This is a polynomial in x^2, but $f = (x^2 + x + 1)^2$ so f is reducible. Now $x^2 + x + 1$ is not a polynomial in x^2 so it is separable. Therefore, according to *our* definition, f is separable as well.

The following rather technical theorem will play an important role for us. In flavour it is similar to the theorem that says that two splitting fields are isomorphic (Theorem 4.6.7). Also in this case we start with two base fields F, $\overline{F}$ that are isomorphic via the map $a \mapsto \bar{a}$. But now, on the left we do not take a splitting field but an extension of F of the form $E = F(\alpha_1, \ldots, \alpha_n)$. On the right we take a field $\overline{L}$ such that the minimal polynomial of each α_i splits into linear factors over $\overline{L}$ (or, equivalently, such that $\overline{L}$ contains a splitting field of the product of these polynomials). The theorem counts the number of injective field homomorphisms $\sigma : E \to \overline{L}$ that extend $a \mapsto \bar{a}$.

From Section 4.6 we recall that the isomorphism $F \to \overline{F}$ extends to an isomorphism $F[x] \to \overline{F}[x]$, $f \mapsto \bar{f}$.

Theorem 5.2.4 *Let $F \subset M$ be fields and let $\alpha_1, \ldots, \alpha_n \in M$ be algebraic over F. Let $f_i \in F[x]$ be the minimal polynomial of α_i. We suppose that each f_i is separable. Let $E = F(\alpha_1, \ldots, \alpha_n)$ and let $\overline{L} \supset \overline{F}$ be an extension such that each $\bar{f}_i$ splits into linear factors over $\overline{L}$. Then the number of injective field homomorphisms $\sigma : E \to \bar{L}$ with $\sigma(a) = \bar{a}$ for $a \in F$ is exactly $|E : F|$.*

Proof. We prove this theorem by induction on n. If $n = 0$ then $E = F$ and $\overline{L} = \overline{F}$ so that the statement is trivial. Now let $\alpha_1, \ldots, \alpha_{n+1} \in M$ be algebraic over F with separable minimal polynomials $f_1, \ldots, f_{n+1}$. Let $E = F(\alpha_1, \ldots, \alpha_{n+1})$ and let $\overline{L} \supset \overline{F}$ be an extension containing a splitting field of $\bar{f}_1 \cdots \bar{f}_{n+1}$.

First note that $\bar{f}_1 \in \overline{F}[x]$ is separable as well (this follows immediately from Lemma 5.2.2). So it has $t = \deg f_1$ distinct roots $\beta_1, \ldots, \beta_t \in \overline{L}$. By Lemma 4.6.6 for $1 \leq i \leq t$ we have a unique injective homomorphism $\psi_i : F(\alpha_1) \to \overline{L}$ with $\psi_i(a) = \bar{a}$ for $a \in F$ and $\psi_i(\alpha_1) = \beta_i$.

Let

$$A = \{\sigma : E \to \overline{L} \mid \sigma \text{ is an injective field homomorphism and } \sigma(a) = \bar{a} \text{ for all } a \in F\}.$$

Let $\sigma \in A$ and write $f_1 = a_0 + a_1x + \cdots + a_tx^t$ with $a_i \in F$. Then

$$\begin{aligned}\bar{f}_1(\sigma(\alpha_1)) &= \bar{a}_0 + \bar{a}_1\sigma(\alpha_1) + \cdots + \bar{a}_t\sigma(\alpha_1)^t \\ &= \sigma(a_0) + \sigma(a_1)\sigma(\alpha_1) + \cdots + \sigma(a_t)\sigma(\alpha_1^t) \\ &= \sigma(a_0 + a_1\alpha_1 + \cdots + a_t\alpha_1^t) = \sigma(f_1(\alpha_1)) = \sigma(0) = 0.\end{aligned}$$

It follows that $\sigma(\alpha_1) = \beta_i$ for a certain i. Therefore the restriction of σ to $F(\alpha_1)$ is equal to a ψ_i. So $A = A_1 \cup \cdots \cup A_t$ (*disjoint* union) where

$$A_i = \{\sigma \in A \mid \sigma|_{F(\alpha_i)} = \psi_i\}.$$

Note that $\overline{L}$ is an extension of $\overline{F}(\beta_i)$ such that the polynomials $\bar{f}_2, \ldots, \bar{f}_{n+1}$ split into linear factors over $\overline{L}$. So by induction we have $|A_i| = |E : F(\alpha_1)|$. Hence

$$\begin{aligned}|A| &= |A_1| + \cdots + |A_t| \\ &= |E : F(\alpha_1)| + \cdots + |E : F(\alpha_1)| \\ &= t|E : F(\alpha_1)| = |E : F(\alpha_1)||F(\alpha_1) : F| = |E : F|\end{aligned}$$

(by the degree formula, Theorem 4.3.3). □

Example 5.2.5 Let $i = \sqrt{-1} \in \mathbb{C}$ and $\omega = \sqrt[4]{2} \in \mathbb{R}$. Using the degree formula (Theorem 4.3.3) one sees that $|\mathbb{Q}(i,\omega) : \mathbb{Q}| = 8$. So by the previous theorem it follows that there are 8 injective field homomorphisms $\sigma : \mathbb{Q}(i,\omega) \to \mathbb{Q}(i,\omega)$ with $\sigma(a) = a$ for all $a \in \mathbb{Q}$. Let σ be such a homomorphism. Viewing $\mathbb{Q}(i,\omega)$ as an 8-dimensional vector space over $\mathbb{Q}$ we have that σ is a linear map. But as σ is injective it has to be surjective as well. It follows that σ is an automorphism.

We can actually describe all these automorphisms. For that note that an automorphism $\sigma : \mathbb{Q}(i,\omega) \to \mathbb{Q}(i,\omega)$ with $\sigma(a) = a$ for $a \in \mathbb{Q}$ is uniquely determined by the values $\sigma(i)$, $\sigma(\omega)$. But $\sigma(i)$ has to be a root of $x^2 + 1$ and $\sigma(\omega)$ is a root of $x^4 - 2$. In other words, $\sigma(i)$ can be $\pm i$ and $\sigma(\omega)$ can be $\pm\omega$, $\pm i\omega$. So we have 8 choices for the pair $(\sigma(i), \sigma(\omega))$. Because we need 8 automorphisms it follows that each of these choices yields an automorphism.

Note that without using Theorem 5.2.4 we would only be able to conclude that we have at most 8 automorphisms. To prove that we have exactly 8 of them (without using the theorem) would involve checking that each choice in fact defines an automorphism, a rather laborious task.

Lemma 5.2.6 *Let $E \supset F$ be a field extension of finite degree. Then E is not equal to the union of a finite number of fields $E_1, \ldots, E_s$ with $F \subset E_i \subsetneq E$.*

Proof. If E is finite then E^* is a cyclic group (Proposition 3.7.9). Also each E_i^* is a cyclic group. Because these are strictly smaller, they cannot contain an element of order $|E^*|$. So the lemma follows in this case.

Now suppose that E is infinite and write $|E : F| = n$. Then E is an n-dimensional vector space over F and the E_i are finite dimensional subspaces. Let $\alpha_1, \ldots, \alpha_n$ be a basis of E over F. Each E_i is contained in a (generally not unique) $(n-1)$-dimensional subspace $V_i \subset E$. Since V_i has codimension 1, there are $e_{i,1}, \ldots, e_{i,n} \in F$ such that

$$V_i = \{a_1\alpha_1 + \cdots + a_n\alpha_n \mid a_i \in F, e_{i,1}a_1 + \cdots + e_{i,n}a_n = 0\}.$$

In other words, if $h_i = e_{i,1}x_1 + \cdots + e_{i,n}x_n \in F[x_1, \ldots, x_n]$, then V_i consists of those $\sum_i a_i\alpha_i$ such that $h_i(a_1, \ldots, a_n) = 0$. let $h = h_1 \cdots h_s$. Then $h(a_1, \ldots, a_s) = 0$ if and only if $\sum_i a_i\alpha_i$ lies in the union of the V_i. But h is not the zero polynomial. So since F is infinite, there are $b_1, \ldots, b_s \in F$ with $h(b_1, \ldots, b_s) \neq 0$. But then $\sum_i b_i\alpha_i$ lies outside the union of the V_i, hence outside the union of the E_i. □

Theorem 5.2.7 (Primitive Element Theorem) *Let $F \subset M$ be fields and $\alpha_1, \ldots, \alpha_n \in M$ algebraic over F. Set $E = F(\alpha_1, \ldots, \alpha_n)$. Suppose that the minimal polynomial of each α_i is separable. Then there is an $\alpha \in E$ such that $E = F(\alpha)$.*

Proof. Let f_i be the minimal polynomial of α_i over F. Let L be the splitting field of $f_1 \cdots f_n$ over E. According to Theorem 5.2.4 there are $t = |E : F|$ injective field homomorphisms $\sigma_i : E \to L$ with $\sigma_i(a) = a$ for $a \in F$ (for $1 \leq i \leq t$). For $1 \leq i < j \leq t$ set

$$E_{i,j} = \{\alpha \in E \mid \sigma_i(\alpha) = \sigma_j(\alpha)\}.$$

These are proper subfields of E. So by Lemma 5.2.6 there is an $\alpha \in E$ lying outside all $E_{i,j}$, i.e., such that $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for $i \neq j$. In other words, $\sigma_1(\alpha), \ldots, \sigma_t(\alpha)$ are all distinct.

Let f be the minimal polynomial of α. Then a small calculation (very similar to the one performed in the proof of Theorem 5.2.4) shows that $\sigma_i(\alpha)$ is a root of f. Hence $\deg(f) \geq t$. So $|F(\alpha) : F| \geq t$. But as $|E : F| = t$ and $F(\alpha) \subset E$ it follows that $F(\alpha) = E$. □

An $\alpha \in E$ as in the theorem is called a *primitive element* of E. Note that in the case of a finite field this term is used for elements with a substantially stronger property (they have to generate the multiplicative group E^*, Section 4.7.3).

Example 5.2.8 Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then also $E = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, so $\sqrt{2} + \sqrt{3}$ is a primitive element of E.

5.3 Separable, normal and Galois extensions

A field extension $E \supset F$ is said to be *algebraic* if every element of E is algebraic over F. We leave it as an exercise to show that extensions of finite degree are automatically algebraic.

Definition 5.3.1 *Let $E \supset F$ be an algebraic field extension. This extension is called*

- separable *if the minimal polynomial of every element of E over F is separable,*
- normal *if every irreducible polynomial in $F[x]$ that has one root in E splits as a product of linear factors over E (that is, has all its roots in E),*
- Galois *if it is both separable and normal.*

Let E be a field then we let $\mathrm{Aut}(E)$ be the set of all field automorphisms of E. This set is called the *automorphism group* of E. We note that with respect to the composition of functions $\mathrm{Aut}(E)$ is indeed a group because

- composition of functions is associative,
- the identity map is an automorphism, and serves as neutral element of $\mathrm{Aut}(E)$,
- if σ, τ are automorphisms of E then $\sigma \circ \tau$ is an automorphism as well (so $\mathrm{Aut}(E)$ is closed under composition),
- if σ is an automorphism of E then so is its inverse σ^{-1} (indeed, let $\alpha, \beta \in E$; then there are $\alpha', \beta' \in E$ with $\alpha = \sigma(\alpha')$, $\beta = \sigma(\beta')$ and hence $\sigma^{-1}(\alpha + \beta) = \sigma^{-1}(\sigma(\alpha') + \sigma(\beta')) = \sigma^{-1}(\sigma(\alpha' + \beta')) = \alpha' + \beta' = \sigma^{-1}(\alpha) + \sigma^{-1}(\beta)$ and in the same way, $\sigma^{-1}(\alpha\beta) = \sigma^{-1}(\alpha)\sigma^{-1}(\beta)$).

Example 5.3.2 Consider the field $\mathbb{Q}(i, \omega)$ as in Example 5.2.5. Let σ be an automorphism of $\mathbb{Q}(i, \omega)$. It is straightforward to see that $\sigma(a) = a$ for $a \in \mathbb{Q}$ (this essentially follows from $\sigma(1) = 1$). So from Example 5.2.5 it follows that $\mathrm{Aut}(\mathbb{Q}(i, \omega))$ has 8 elements. These are described in the mentioned

example. More in detail, we have $\mathrm{Aut}(\mathbb{Q}(i,\omega)) = \{\sigma_1, \ldots, \sigma_8\}$ where $\sigma_j(i)$, $\sigma_j(\omega)$ are as in the following table

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$
ω	ω	$i\omega$	$-\omega$	$-i\omega$	ω	$i\omega$	$-\omega$	$-i\omega$

We can use this to compute product relations between the σ_j. For example, $\sigma_4\sigma_7(i) = \sigma_4(\sigma_7(i)) = \sigma_4(-i) = -i$ and $\sigma_4\sigma_7(\omega) = \sigma_4(\sigma_7(\omega)) = \sigma_4(-\omega) = i\omega$; it follows that $\sigma_4\sigma_7 = \sigma_6$. Also $\sigma_7\sigma_4(i) = \sigma_7(i) = -i$ and $\sigma_7\sigma_4(\omega) = \sigma_7(-i\omega) = \sigma_7(-i)\sigma_7(\omega) = i \cdot -\omega = -i\omega$; so that $\sigma_7\sigma_4 = \sigma_8$. Continuing like this we can complete the multiplication table:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_2	σ_2	σ_3	σ_4	σ_1	σ_6	σ_7	σ_8	σ_5
σ_3	σ_3	σ_4	σ_1	σ_2	σ_7	σ_8	σ_5	σ_6
σ_4	σ_4	σ_1	σ_2	σ_3	σ_8	σ_5	σ_6	σ_7
σ_5	σ_5	σ_8	σ_7	σ_6	σ_1	σ_4	σ_3	σ_2
σ_6	σ_6	σ_5	σ_8	σ_7	σ_2	σ_1	σ_4	σ_3
σ_7	σ_7	σ_6	σ_5	σ_8	σ_3	σ_2	σ_1	σ_4
σ_8	σ_8	σ_7	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

Let E be a field and let $G \subset \mathrm{Aut}(E)$ be a subgroup. Then we set

$$E^G = \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

It is straightforward to see that this is a subfield of E. So we have an extension $E \supset E^G$.

Lemma 5.3.3 *Let E be a field, $G \subset \mathrm{Aut}(G)$ a finite subgroup and $F = E^G$. Furthermore, for $\alpha \in E$ set $A_\alpha = \{\sigma(\alpha) \mid \sigma \in G\}$. Then the minimal polynomial of α over F is*

$$\prod_{\beta \in A_\alpha} (x - \beta).$$

In particular, E/F is algebraic.

Proof. For $\tau \in G$ we define $\tilde{\tau} : E[x] \to E[x]$ by

$$\tilde{\tau}(a_0 + \cdots + a_m x^m) = \tau(a_0) + \cdots + \tau(a_m)x^m.$$

It is straightforward to see that $\tilde{\tau}$ is a ring automorphism (that is, it is bijective and respects multiplication and addition). Let

$$g = \prod_{\beta \in A_\alpha} (x - \beta).$$

Then $\tilde{\tau}(g) = \prod_\beta (x - \tau(\beta))$. As G is a group we have that $\{\tau\sigma \mid \sigma \in G\} = G$. Hence $\{\tau(\beta) \mid \beta \in A_\alpha\} = A_\alpha$. So $\tilde{\tau}(g) = g$, and writing $g = a_0 + \cdots + a_m x^m$ it follows that $\tau(a_i) = a_i$ for all i. As this holds for all $\tau \in G$ we get that $a_i \in E^G = F$. In other words, $g \in F[x]$.

Since $\alpha \in A_\alpha$ we see that $g(\alpha) = 0$. Hence α is algebraic over F. Let $f \in F[x]$ be its minimal polynomial. By Proposition 4.3.4, f divides g. Writing $f = b_0 + \cdots + b_m x^m$ with $b_i \in F$, we compute for $\sigma \in G$,

$$f(\sigma(\alpha)) = b_0 + b_1\sigma(\alpha) + \cdots + b_m\sigma(\alpha)^m = \sigma(b_0 + \cdots + b_m\alpha^m) = \sigma(f(\alpha)) = 0.$$

(Where we use that $\sigma(a) = a$ for all $a \in F$.) Hence all $\beta \in A_\alpha$ are roots of f and therefore f divides g. Because both polynomials are monic we have $f = g$. □

Example 5.3.4 Consider the field $\mathbb{Q}(i,\omega)$ as in Examples 5.2.5, 5.3.2. Let $\alpha = i+\omega$. By using the description of the automorphisms in Example 5.2.5 we see that A_α consits of

$$\pm i \pm \omega, \quad \pm i \pm i\omega.$$

So A_α has 8 elements and therefore the minimal polynomial of α has degree 8. In particular α is a primitive element.

Now let $\beta = \omega + i\omega$. Then A_β consists of the elements $\pm\omega \pm i\omega$. It has four elements and therefore the minimal polynomial of $\omega + i\omega$ has degree 4.

Proposition 5.3.5 *Let E be a field, $G \subset \mathrm{Aut}(G)$ a finite subgroup and $F = E^G$. Then E/F is a Galois extension and $|E:F| = |G|$.*

Proof. Let $\alpha \in E$. By Lemma 5.3.3 we see that its minimal polynomial splits into linear factors over E and that its roots all have multiplicity one. It follows that E/F is normal and separable, and hence Galois.

Now we show that $|E:F|$ is finite. Suppose on the contrary that it is infinite. Then there are $\alpha_i \in E$ such that $F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1,\alpha_2) \subsetneq \cdots$ is an infinite series of field extensions. But each field has finite degree over F, so by Theorem 5.2.7 there are $\beta_i \in E$ such that $F(\alpha_1,\ldots,\alpha_i) = F(\beta_i)$. However, by Lemma 5.3.3 the minimal polynomial of β_i has degree at most $|G|$. Hence $|F(\beta_i):F| \leq |G|$ and we see that the infinite series cannot exist.

As $|E:F|$ is finite, and E/F is separable, by Theorem 5.2.7 we have that there is an $\alpha \in E$ such that $E = F(\alpha)$. In the same way as above this implies that $|E:F| \leq |G|$.

In the same way as in the proof of Theorem 5.2.7 we see that there is a $\beta \in F$ such that $\sigma(\beta) \neq \tau(\beta)$ for $\sigma,\tau \in G$, $\sigma \neq \tau$. By Lemma 5.3.3 the minimal polynomial of β has degree $|G|$. It follows that also $|E:F| \geq |G|$. □

For a field extension E/F we define its *Galois group* as

$$\mathrm{Gal}(E/F) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma(a) = a \text{ for all } a \in F\}.$$

Let $\sigma,\tau \in \mathrm{Gal}(E/F)$. It is obvious that $\sigma(\tau(a)) = a$ for $a \in F$, so that $\sigma\tau \in \mathrm{Gal}(E/F)$ as well. Applying σ^{-1} to the equality $\sigma(a) = a$ we see that also $\sigma^{-1} \in \mathrm{Gal}(E/F)$. The identity obviously lies in $\mathrm{Gal}(E/F)$. Hence the latter is a subgroup of $\mathrm{Aut}(E/F)$.

Theorem 5.3.6 *Let E/F be an extension of finite degree and set $G = \mathrm{Gal}(E/F)$. The following are equivalent:*

(i) *E/F is a Galois extension,*

(ii) *E is the splitting field over F of a separable $f \in F[x]$,*

(iii) *$|E:F| = |G|$,*

(iv) *$F = E^G$.*

Proof. Suppose that E/F is Galois, that is, separable and normal. Because E/F is of finite degree there are $\alpha_1,\ldots,\alpha_n \in E$ with $E = F(\alpha_1,\ldots,\alpha_n)$. But then by Theorem 5.2.7 there is an $\alpha \in E$ with $E = F(\alpha)$. Let $f \in F[x]$ be its minimal polynomial. As E/F is normal, f splits into linear factors over E. So E contains a splitting field of f over F. Obviously this splitting field must contain α and therefore is equal to $F(\alpha) = E$.

Next suppose that (ii) holds. We use Theorem 5.2.4 with $\overline{F} = F$, $\bar{a} = a$ for all $a \in F$, $\overline{L} = E$. Note that an injective field homomorphism $E \to E$ is automatically an isomorphism (indeed: we only need to show surjectivity, but the image of the map is a subspace of E of the same dimension as E, therefore it is equal to E). Hence the conclusion of the theorem translates to $|G| = |E:F|$.

Suppose that (iii) holds. Set $K = E^G$. From the definition of Galois group we see that $F \subset K$. By Proposition 5.3.5 we see that $|E:K| = |G|$. So by applying the degree formula (Theorem 4.3.3) we get $|K:F| = 1$ implying $K = F$.

Finally, it is immediate from Proposition 5.3.5 that (iv) implies (i). □

Example 5.3.7 Consider the field $\mathbb{Q}(i,\omega)$ as in Examples 5.2.5, 5.3.2, 5.3.4. From these examples it immediately follows that $|\mathrm{Gal}(\mathbb{Q}(i,\omega)/\mathbb{Q}| = 8 = |\mathbb{Q}(i,\omega) : \mathbb{Q}|$. Hence it is a Galois extension. In fact, $\mathbb{Q}(i,\omega)$ is a splitting field of $x^4 - 2$ over $\mathbb{Q}$.

5.4 The Galois correspondence

The Galois correspondence is the main technical tool for applications of Galois groups, linking, as it does, the intermediate fields of a field extension to the subgroup structure of its Galois group.

Let E/F be an extension of fields. Let K be a field with $F \subseteq K \subseteq E$. Then we say that K is an *intermediate field* of the extension E/F. If it is clear with which extension we are working then we also simply say that K is an intermediate field.

Lemma 5.4.1 *Let E/F be a Galois extension of finite degree and set $G = \mathrm{Gal}(E/F)$.*

(i) *Let $H \subset G$ be a subgroup and set $K = E^H$. Then K is an intermediate field, E/K is a Galois extension and $\mathrm{Gal}(E/K) = H$.*

(ii) *Let K be an intermediate field and set $H = \mathrm{Gal}(E/K)$. Then H is a subgroup of G, E/K is Galois and $K = E^H$.*

Proof. The given inclusions in (i) are obvious. Proposition 5.3.5 immediately gives that E/K is Galois and $|E : K| = |H|$. By Theorem 5.3.6(iii) we see that $|E : K| = |\mathrm{Gal}(E/K)|$. From the definition of Galois group it is immediate that $H \subset \mathrm{Gal}(E/K)$. Hence $|H| = |\mathrm{Gal}(E/K)|$ shows that $H = \mathrm{Gal}(E/K)$.

It is obvious that H in (ii) is a subgroup of G. By Theorem 5.3.6(ii) we have that E is the splitting field over F of a separable $f \in F[x]$. But then also $f \in K[x]$ and E is the splitting field over K of f. Hence by the same theorem E/K is Galois. Now by part (iv) of Theorem 5.3.6 we conclude that $K = E^H$. □

Theorem 5.4.2 (Galois correspondence) *Let E/F be a Galois extension of finite degree and set $G = \mathrm{Gal}(E/F)$. Define*

$$A = \{ \text{ subgroups } H \text{ of } G \}$$
$$B = \{ \text{ fields } K \text{ with } F \subseteq K \subseteq E \}.$$

Then we have bijective maps $\alpha : A \to B$, $\beta : B \to A$ given by $\alpha(H) = E^H$, $\beta(K) = \mathrm{Gal}(E/K)$. We have that α, β are each other's inverses and they invert the inclusion relation, that is

$$H_1 \subset H_2 \Longrightarrow E^{H_1} \supset E^{H_2}$$
$$K_1 \subset K_2 \Longrightarrow \mathrm{Gal}(E/K_1) \supset \mathrm{Gal}(E/K_2).$$

Proof. From Lemma 5.4.1(i) we see that $\beta(\alpha(H)) = H$ and Lemma 5.4.1(ii) states that $\alpha(\beta(K)) = K$. This also immediately implies that α, β are bijective.

For the last statement, suppose that $H_1 \subset H_2$ and let $\alpha \in E^{H_2}$. Then $\sigma(\alpha) = \alpha$ for all $\sigma \in H_2$. Hence $\sigma(\alpha) = \alpha$ for all $\sigma \in H_1$, so that $\alpha \in E^{H_1}$. The second implication is shown in an analogous manner. □

The bijective maps of the theorem are together called the *Galois correspondence*. With this correspondence it is possible to translate field theoretical problems to group theoretical problems. It has proved to be an extremely potent tool in a number of contexts.

An immediate question is the following. Let's fix a property P of (sub-) groups, and take the set of all subgroups of a given Galois group that have P; is it possible to characterize the intermediate

fields corresponding to these subgroups? (An analogous question can be formulated by starting with a property of intermediate fields.) The next proposition has the answer to this question (and a bit more) when P is the property to be a normal subgroup. Subgroups of this kind turn out to correspond to intermediate fields that are stable.

Definition 5.4.3 *Let E/F be a Galois extension and $G = \mathrm{Gal}(E/F)$. An intermediate field K (so we have $F \subseteq K \subseteq E$) is said to be* stable *if for all $\sigma \in G$ and $\alpha \in K$ we have $\sigma(\alpha) \in K$ (in other words, if σ sends K to K).*

Proposition 5.4.4 *Let E/F be a Galois extension of finite degree and $G = \mathrm{Gal}(E/F)$. Let $H \subset G$ be a subgroup and $K = E^H$ the corresponding intermediate field. The following are equivalent*

(i) *H is a normal subgroup,*

(ii) *K is a stable intermediate field,*

(iii) *K/F is a Galois extension.*

Furthermore, if one of these (and hence all three) conditions is satisfied then $\mathrm{Gal}(K/F) \cong G/H$.

Proof. Suppose that H is normal and let $\alpha \in K$, $\sigma \in G$. Then for $\tau \in H$ we have $\sigma^{-1}\tau\sigma \in H$ so that $\sigma^{-1}\tau\sigma(\alpha) = \alpha$, which is the same as $\tau(\sigma(\alpha)) = \sigma(\alpha)$. Since this holds for all $\tau \in H$ it follows that $\sigma(\alpha) \in K$. We conclude that K is stable.

We show that (ii) implies (iii). So suppose that K is stable and set $\mathcal{G} = \mathrm{Gal}(K/F)$. We will show that $K^{\mathcal{G}} = F$. Because K is stable we can restrict a $\sigma \in G$ to K and immediately get that $\sigma|_K : K \to K$ is an element of $\mathcal{G}$. Suppose that $K^{\mathcal{G}} \supsetneq F$ and let $a \in K^{\mathcal{G}}$, $a \notin F$. Then because E/F is a Galois extension it follows that there is a $\sigma \in G$ with $\sigma(a) \neq a$. But then $\sigma|_K$ is an element of $\mathcal{G}$ not leaving invariant a. This is a contradiction and it follows that $K^{\mathcal{G}} = F$. By Theorem 5.3.6 we see that K/F is Galois.

Now suppose that (iii) holds, i.e., K/F is Galois. We want to show (i), but in order to do that we first show (ii). Let $\alpha \in K$ and $\sigma \in G$. Let $f \in F[x]$ be the minimal polynomial of α. Then $\sigma(\alpha)$ is a root of f as well. Now f is an irreducible polynomial in $F[x]$ having a root in K, so as K/F is normal it follows that f splits into linear factors over K. In particular $\sigma(\alpha) \in K$ as well, and we see that K is stable. Because of this we can define a group homomorphism

$$\Psi : G \to \mathrm{Gal}(K/F),\ \Psi(\sigma) = \sigma|_K.$$

(Note that it is obvious that this is a group homomorphism.) We consider its kernel. A $\sigma \in G$ lies in $\ker \Psi$ if and only if $\sigma(\alpha) = \alpha$ for all $\alpha \in K$. But that is the same as saying that $\sigma \in \mathrm{Gal}(E/K)$. By the Galois correspondence the latter is equal to H. We see that $\ker \Psi = H$ and therefore H is a normal subgroup of G (Theorem 3.4.6).

Finally, suppose that the three conditions are satisfied. Again we consider the homomorphism Ψ. Again using Theorem 3.4.6 we see that $\Psi(G) \cong G/N$ so that $|\Psi(G)| = \frac{|G|}{|H|}$. On the other hand, by the degree formula (Theorem 4.3.3) we have $|E : F| = |E : K||K : F|$. Furthermore, $|E : F| = |G|$, $|E : K| = |H|$, $|K : F| = |\mathrm{Gal}(K/F)|$ by Theorem 5.3.6. Hence $|\Psi(G)| = |\mathrm{Gal}(K/F)|$ from which it follows that $\Psi(G) = \mathrm{Gal}(K/F)$. By Theorem 3.4.6 we conclude that $G/H \cong \mathrm{Gal}(K/F)$. □

Example 5.4.5 Consider the field $\mathbb{Q}(i, \omega)$ as in Example 5.3.7. In that example we have observed that it is a Galois extension of degree 8 of $\mathbb{Q}$. In Example 5.3.2 we determined the multiplication table of $\mathrm{Gal}(\mathbb{Q}(i, \omega))$. Now we first find all its subgroups and then the corresponding intermediate fields. For finding the subgroups of a group we use the following observations:

- The order of a subgroup of a finite group G divides the order of G (Corollary 3.2.7).
- Let g be an element of order m of a group. Then $\{1, g, g^2, \ldots, g^{m-1}\}$ is the smallest subgroup containing g (Lemma 3.7.2).

- Let H be a group of prime order p. Let $h \in H$, $h \neq 1$. Then the order of h is p and $H = \{1, h, \ldots, h^{p-1}\}$ (this follows immediately from Proposition 3.7.4).

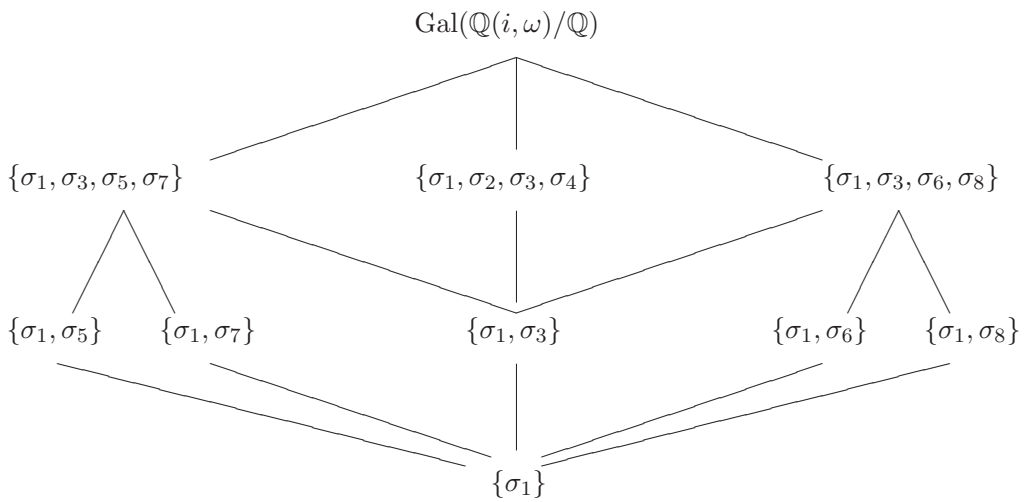
Write $G = \mathrm{Gal}(\mathbb{Q}(i,\omega)/\mathbb{Q})$; then $|G| = 8$ so that a subgroup of G can have order $1, 2, 4, 8$. There is only one subgroup of order 1, namely $\{\sigma_1\}$. Similarly, there is only one subgroup of order 8, namely G itself. For the other subgroups we need to work a bit harder.

First consider the subgroups of order 2. By the observation above they have the form $\{\sigma_1, \tau\}$ where τ is of order 2, i.e., $\tau^2 = \sigma_1$. From the table in Example 5.3.2 we immediately see that we get the subgroups $\{\sigma_1, \sigma_i\}$ for $i = 3, 5, 6, 7, 8$.

Now we look at the subgroups of order 4. We first try to find the cyclic subgroups of order 4. For that we need elements of order 4. From the multiplication table of G we see that σ_2, σ_4 have order 4 (whereas σ_1 has order 1 and all other elements have order 2). But the subgroups generated by these two elements are both equal to $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$. So we find only one cyclic subgroup of order 4. If a subgroup of order 4 is not cyclic then it is of the form $\{\sigma_1, \tau_1, \tau_2, \tau_3\}$ where the elements τ_i have order 2. (Indeed, a τ_i cannot have order 1 as then $\tau_i = \sigma_1$, it cannot have order 3 as 3 does not divide 4, and it cannot have order 4 as then the subgroup would be cyclic.) So we have to find all sets of three elements of order 2 lying in a subgroup of order 4. If we take $\tau_1 = \sigma_3$, $\tau_2 = \sigma_5$ then we see that in fact we get the subgroup $\{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$. If we take $\tau_1 = \sigma_3$, $\tau_2 = \sigma_6$ then we get the subgroup $\{\sigma_1, \sigma_3, \sigma_6, \sigma_8\}$. The choices $\tau_1 = \sigma_3$, $\tau_2 = \sigma_7$ and $\tau_1 = \sigma_3$, $\tau_2 = \sigma_8$ yield the subgroups that we have seen already. If we take $\tau_1 = \sigma_5$, $\tau_2 = \sigma_6$ then because $\sigma_5\sigma_6 = \sigma_4$ we do not get a subgroup of order 4. Continuing like this we see that either we get a subgroup that we have already seen, or we get no subgroup at all.

Concluding, we found one subgroup of order 1, five subgroups of order 2, three subgroups of order 4 and one subgroup of order 8. They are displayed, along with their inclusion relations in Figure 5.3.

Figure 5.3: Subgroups of $\mathrm{Gal}(\mathbb{Q}(i,\omega)/\mathbb{Q})$.



Now we find the intermediate field corresponding to each of these subgroups. Because σ_1 is the identity we obviously have $\mathbb{Q}(i,\omega)^{\{\sigma_1\}} = \mathbb{Q}(i,\omega)$. Because $\mathbb{Q}(i,\omega)$ is a Galois extension of $\mathbb{Q}$ it immediately follows that $\mathbb{Q}(i,\omega)^G = \mathbb{Q}$ (Theorem 5.3.6). For the other subgroups we can always compute the intermediate field by solving a set of linear equations. This is also illustrated below. However, we also have some tricks that sometimes help to find the corresponding intermediate field with much less effort:

- We note the following fact, whose proof we leave as an exercise. Let E/F be a Galois extension, $G = \mathrm{Gal}(E/F)$ and let $H \subset G$ be a subgroup. Let $K \subset E$ be an intermediate field such that

$K \subset E^H$ and $|K : F| = \frac{|G|}{|H|}$. Then $K = E^G$. So if we guess a candidate K for E^G and it happens to be of the correct degree over F then we have our intermediate field.

- We can start from the "field side" and list some obvious intermediate fields, and try and identify the subgroups to which they correspond.

Now we look at the subgroups of order 2, starting with $\{\sigma_1, \sigma_3\}$. By looking at the action of σ_3 it is obvious that i is fixed. But also ω^2 is fixed (as ω is sent to $-\omega$). So a candidate for the intermediate field is $K = \mathbb{Q}(i, \omega^2)$. For its degree we have $|K : \mathbb{Q}| = |K : \mathbb{Q}(\omega^2)| \cdot |\mathbb{Q}(\omega^2) : \mathbb{Q}|$. Now $\omega^2 = \sqrt{2}$ so $|\mathbb{Q}(\omega^2) : \mathbb{Q}| = 2$. Furthermore, $\mathbb{Q}(\omega^2) \subset \mathbb{R}$ so that x^2+1 has no roots in $\mathbb{Q}(\omega^2)$ and hence is irreducible in $\mathbb{Q}(\omega^2)[x]$. It follows that $|K : \mathbb{Q}(\omega^2)| = 2$ and $|K : \mathbb{Q}| = 4$ which is equal to $\frac{|G|}{|H|}$. We conclude that $K = \mathbb{Q}(i, \omega)^{\{\sigma_1, \sigma_3\}}$.

Also the other subgroups of order 2 correspond to intermediate fields of degree 4 over $\mathbb{Q}$. But we also immediately see some intermediate fields of degree 4, namely the fields $\mathbb{Q}(\alpha)$ where α runs over the roots of $x^4 - 2$. However, here $\omega, -\omega$ and $i\omega, -i\omega$ give the same fields. So we immediately have two fields, namely $\mathbb{Q}(\omega)$ and $\mathbb{Q}(i\omega)$. By checking which order 2 subgroups leave these fields fixed we immediately get $\mathbb{Q}(\omega) = \mathbb{Q}(i, \omega)^{\{\sigma_1, \sigma_5\}}$, $\mathbb{Q}(i\omega) = \mathbb{Q}(i, \omega)^{\{\sigma_1, \sigma_7\}}$.

For the remaining two groups of order 2 it is perhaps not immediately clear to which field they belong, so we resort to linear equations. For this we first describe a basis of $\mathbb{Q}(i, \omega)$ over $\mathbb{Q}$. We have that $1, \omega, \omega^2, \omega^3$ is a basis of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$. Since $x^2 + 1$ is irreducible over $\mathbb{Q}(\omega)$ we have that $1, i$ is a basis of $\mathbb{Q}(i, \omega)$ over $\mathbb{Q}(\omega)$. Using the argument in the proof of the degree formula (Proposition 4.3.3) we see that $1, \omega, \omega^2, \omega^3, i, i\omega, i\omega^2, i\omega^3$ is a basis of $\mathbb{Q}(i, \omega)$ over $\mathbb{Q}$. Now consider the subgroup $\{\sigma_1, \sigma_6\}$ and let $a = a_1 + a_2\omega + a_3\omega^2 + a_4\omega^3 + a_5 i + a_6 i\omega + a_7 i\omega^2 + a_8 i\omega^3$ with $a_i \in \mathbb{Q}$ be an element of $\mathbb{Q}(i, \omega)$. Then

$$\sigma_6(a) = a_1 + a_2 i\omega - a_3\omega^2 - a_4 i\omega^3 - a_5 i + a_6\omega + a_7 i\omega^2 - a_8\omega^3.$$

Hence $\sigma_6(a) = a$ if and only if $a_3 = a_5 = 0$, $a_2 = a_6$ and $a_4 = -a_8$. It follows that

$$\mathbb{Q}(i, \omega)^{\{\sigma_1, \sigma_6\}} = \{a_1 + a_2\omega + a_4\omega^3 + a_2 i\omega + a_7 i\omega^2 - a_4 i\omega^3 \mid a_i \in \mathbb{Q}\}.$$

Since the minimal polynomial of $\omega + i\omega$ has degree 4 (Example 5.3.4) we see that this field is equal to $\mathbb{Q}(\omega + i\omega)$.

The subgroup $\{\sigma_1, \sigma_8\}$ is treated similarly. Now we compute

$$\sigma_8(a) = a_1 - a_2 i\omega - a_3\omega^2 + a_4 i\omega^3 - a_5 i - a_6\omega + a_7 i\omega^2 + a_8\omega^3$$

and $\sigma_8(a) = a$ if and only if $-a_2 = a_6$, $a_3 = a_5 = 0$, $a_4 = a_8$. Therefore

$$\mathbb{Q}(i, \omega)^{\{\sigma_1, \sigma_8\}} = \{a_1 + a_2\omega + a_4\omega^3 - a_2 i\omega + a_7 i\omega^2 + a_4 i\omega^3 \mid a_i \in \mathbb{Q}\}.$$

Moreover, in the same way as for $\omega + i\omega$ it is seen that the minimal polynomal of $\omega - i\omega$ has degree 4 and the above field is equal to $\mathbb{Q}(\omega - i\omega)$.

The subgroups of order 4 correspond to intermediate fields of degree 2. For the subgroup $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ we immediately see that its fixed field is $\mathbb{Q}(i)$ (it is fixed, and has degree 2 over $\mathbb{Q}$).

The intermediate fields corresponding to the other two groups of order 4 can be determined by solving a set of linear equations. Consider the subgroup $\{\sigma_1, \sigma_3, \sigma_6, \sigma_8\}$, write a as above and compute

$$\sigma_3(a) = a_1 - a_2\omega + a_3\omega^2 - a_4\omega^3 + a_5 i - a_6 i\omega + a_7 i\omega^2 - a_8 i\omega^3$$
$$\sigma_6(a) = a_1 + a_2 i\omega - a_3\omega^2 - a_4 i\omega^3 - a_5 i + a_6\omega + a_7 i\omega^2 - a_8\omega^3.$$

Because $\sigma_8 = \sigma_3\sigma_6$ we have that $\sigma_3(a) = \sigma_6(a) = a$ implies that $\sigma_8(a) = a$. So

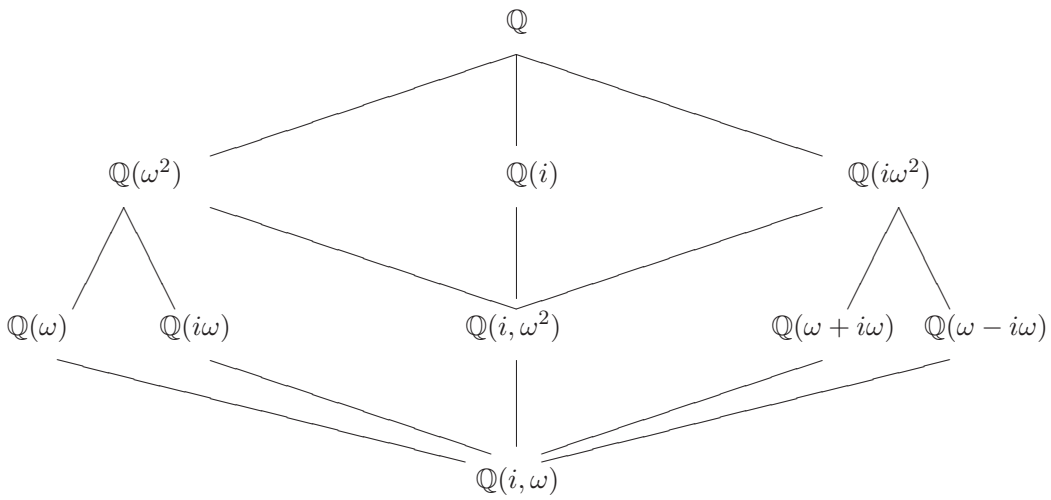
$$\mathbb{Q}(i, \omega)^{\{\sigma_1, \sigma_3, \sigma_6, \sigma_8\}} = \{a \in \mathbb{Q}(i, \omega) \mid \sigma_3(a) = \sigma_6(a) = a\}.$$

Now from the above equations we see that $\sigma_3(a) = a$ if and only if $a_2 = a_4 = a_6 = a_8 = 0$. Secondly, $\sigma_6(a) = a$ if and only if $a_3 = a_5 = 0$, $a_2 = a_6$ and $a_4 = -a_8$. We see that all coefficients are 0 except

a_7 which can be chosen freely. Hence the intermediate field we are after is $\{a_1 + a_7 i\omega^2 \mid a_1, a_7 \in \mathbb{Q}\} = \mathbb{Q}(i\omega^2)$. In the same way we see that the field corresponding to the last remaining group is $\mathbb{Q}(\omega^2)$. Of course, if we had seen that $\mathbb{Q}(i\omega^2)$, $\mathbb{Q}(\omega^2)$ are intermediate fields of degree 2, then we could have associated them directly to these groups.

We can put the intermediate fields in a diagram, see Figure 5.4, obtaing the "same" picture as the one with the subgroups, with the difference that the inclusion relations go the other way. Note that the Galois correspondence implies that this figure contains all subfields of $\mathbb{Q}(i, \omega)$, a result which is not easily obtained otherwise.

Figure 5.4: Intermediate fields of $\mathbb{Q}(i, \omega)/\mathbb{Q}$.



Example 5.4.6 Let $f = x^4 - 4x^2 + 2$. By Eisenstein's criterion (Theorem 2.5.14) f is irreducible. Hence $E = \mathbb{Q}[x]/\langle f \rangle$ is a field (Proposition 4.4.1). Writing $\alpha = [x]$ we have that the elements $1, \alpha, \alpha^2, \alpha^3$ form a basis of E over $\mathbb{Q}$ so that $E = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_i \in \mathbb{Q}\}$.

We have $f(\alpha) = 0$ or $\alpha^4 = 4\alpha^2 - 2$. We claim that $\alpha_1 = \alpha$, $\alpha_2 = -\alpha$, $\alpha_3 = \alpha^3 - 3\alpha$, $\alpha_4 = -(\alpha^3 - 3\alpha)$ are roots of f in E. For α_1 we have already seen this. For α_2 it is also obvious since f involves only even powers of x. For α_3 we first compute $\alpha^6 = \alpha^2 \cdot \alpha^4 = 4\alpha^4 - 2\alpha^2 = 14\alpha^2 - 8$ and

$$(\alpha^3 - 3\alpha)^2 = \alpha^6 - 6\alpha^4 + 9\alpha^2 = -\alpha^2 + 4$$

and

$$(\alpha^3 - 3\alpha)^4 = (-\alpha^2 + 4)^2 = -4\alpha^2 + 14.$$

So we see that indeed $\alpha_3^4 - 4\alpha_3^2 + 2 = 0$. Then immediately $\alpha_4 = -\alpha_3$ is also a root of f.

It follows that E contains a splitting field of f. But since the smallest subfield of E containing $\mathbb{Q}$ and the α_i obviously contains E itself, we see that E is a splitting field of f. Hence $E/\mathbb{Q}$ is a Galois extension (Theorem 5.3.6).

Now we determine the Galois group $\mathrm{Gal}(E/\mathbb{Q})$. First note that a $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ is completely determined by the value of $\sigma(\alpha)$. Secondly, $\sigma(\alpha)$ must be a root of f, so we have at most four possibilities: $\sigma(\alpha) = \alpha_i$, $1 \leq i \leq 4$. On the other hand, because $E/\mathbb{Q}$ is Galois, we have $|\mathrm{Gal}(E/\mathbb{Q})| = |E : \mathbb{Q}| = 4$ (Theorem 5.3.6). It follows that each choice $\sigma(\alpha) = \alpha_i$ must yield an element of $\mathrm{Gal}(E/\mathbb{Q})$. We conclude that $\mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, where $\sigma_i(\alpha) = \alpha_i$.

We can compute products between the α_i. For example, $\alpha_3\alpha_3(\alpha) = \alpha_3(\alpha_3(\alpha)) = \alpha_3(\alpha^3 - 3\alpha) = (\alpha_3 - 3\alpha)^3 - 3(\alpha^3 - 3\alpha)$. As seen above we have $(\alpha^3 - 3\alpha)^2 = -\alpha^2 + 4$, and hence

$$(\alpha^3 - 3\alpha)^3 = (\alpha^3 - 3\alpha)(-\alpha^2 + 4) = -\alpha^5 + 7\alpha^3 - 12\alpha = 3\alpha^3 - 10\alpha.$$

It follows that $\sigma_3\sigma_3(\alpha) = -\alpha$ so that $\sigma_3\sigma_3 = \sigma_2$. In an analogous manner we find the other products, and compute the multiplication table:

	σ_1	σ_2	σ_3	σ_4
σ_1	σ_1	σ_2	σ_3	σ_4
σ_2	σ_2	σ_1	σ_4	σ_3
σ_3	σ_3	σ_4	σ_2	σ_1
σ_4	σ_4	σ_3	σ_1	σ_2

In this case a proper nontrivial subgroup can only have order 2, and must be of the form $\{\sigma_1, \tau\}$ with $\tau^2 = \sigma_1$. We see that we only have $\{\sigma_1, \sigma_2\}$. So together with the obvious subgroups $\{\sigma_1\}$ and $\mathrm{Gal}(E/\mathbb{Q})$ we have three subgroups.

The intermediate fields corresponding to $\{\sigma_1\}$, $\mathrm{Gal}(E/\mathbb{Q})$ are E and $\mathbb{Q}$ respectively (the latter because $E/\mathbb{Q}$ is a Galois extension). It remains to find the intermediate field corresponding to $\{\sigma_1, \sigma_2\}$. Let $a = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \in E$; then

$$\sigma_2(a) = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3.$$

Hence $\sigma_2(a) = a$ if and only if $a_1 = a_3 = 0$. It follows that $E^{\{\sigma_1,\sigma_2\}} = \{a_0 + a_2\alpha^2 \mid a_i \in \mathbb{Q}\} = \mathbb{Q}(\alpha^2)$.

5.5 Cyclotomic fields

Let F be a field and $n \geq 1$ an integer. An $\omega \in F$ with $\omega^n = 1$ is called an *n-th root of unity* in F. It is *primitive* if $\omega^k \neq 1$ for $1 \leq k \leq n-1$. We can reformulate these concepts in group theoretical language by considering the group $F^* = F \setminus \{0\}$. A root of unity is an element of finite order. It is an n-th root of unity if its order divides n. It is a primitive n-th root of unity if its order is exactly n.

Example 5.5.1 Let $\omega = \frac{1}{\sqrt{2}}(1+i) \in \mathbb{C}$. Then

$$\omega^2 = i,\ \omega^3 = \tfrac{1}{\sqrt{2}}(-1+i),\ \omega^4 = -1,\ \omega^5 = \tfrac{1}{\sqrt{2}}(-1-i), \omega^6 = -i,\ \omega^7 = \tfrac{1}{\sqrt{2}}(1-i),\ \omega^8 = 1.$$

Hence ω is a primitive 8-th root of unity.

It is clear that not all fields have primitive n-th roots of unity. For example, the only roots of unity in $\mathbb{Q}$ are ± 1. In order to make a meaningful study of roots of unity we must work with fields that contain enough of them, that is, fields containing a splitting field of $x^n - 1$. Now we have a lemma collecting some immediate properties of the set of n-th roots of unity; in order to prove it we need a little lemma on cyclic groups.

Lemma 5.5.2 *Let G be a group and $g \in G$ of finite order n. Let i be an integer, $i \geq 1$. Then the order of g^i is $\frac{n}{\gcd(n,i)}$.*

Proof. Let k be the order of g^i. Set $d = \gcd(n, i)$ and write $i = i'd$. Then $(g^i)^{n/d} = (g^n)^{i'} = 1$. Hence k divides $\frac{n}{d}$ (Lemma 3.7.6). Also we have $g^{ik} = (g^k)^i = 1$. Hence again by Lemma 3.7.6, n divides ik. But that implies that $\frac{n}{d}$ divides k. It follows that $k = \frac{n}{d}$. □

Lemma 5.5.3 *Let F be a field and let $E \supset F$ be an extension containing a splitting field of $x^n - 1$. Set*

$$U_n(E) = \{\omega \in E \mid \omega^n = 1\}.$$

Suppose that the characteristic of F is 0, or a prime not dividing n.

(i) *$U_n(E)$ is a cyclic subgroup of E^* of order n.*

(ii) *A $\zeta \in U_n(E)$ generates $U_n(E)$ (that is, every element of $U_n(E)$ can be written as a power of ζ) if and only if it is a primitive n-th root of unity.*

(iii) *Let $\zeta \in U_n(E)$ be a primitive n-th root of unity. For $i \geq 1$ we have that ζ^i is also a primitive n-th root of unity if and only if* $\gcd(n, i) = 1$.

Proof. Set $f = x^n - 1$. Then $f' = nx^{n-1}$ which is nonzero because of our hypothesis on the characteristic. The only root of f' is 0, which is not a root of f. Therefore f only has roots of multiplicity 1 in its splitting field (Lemma 4.7.2). Hence $|U_n(E)| = n$. It is obvious that $U_n(E)$ is a subgroup of E^* and it is cyclic by Proposition 3.7.9.

Let $\zeta \in U_n(E)$ and denote its order by $|\zeta|$. The cyclic subgroup of $U_n(E)$ generated by ζ has order exactly $|\zeta|$. So ζ generates $U_n(E)$ if and only if $|\zeta| = n$ if and only if ζ is a primitive n-th root of unity.

The last item follows by (ii) together with Lemma 5.5.2. □

Remark 5.5.4 If the characteristic p divides n then we write $n = p^s n_0$ where p does not divide n_0. Let α be an n-th root of unity in some extension of F. Then by Lemma 4.7.1 we have $0 = \alpha^n - 1 = (\alpha^{n_0})^{p^s} - 1 = (\alpha^{n_0} - 1)^{p^s}$. It follows that α is an n_0-th root of unity. So we lose nothing if we restrict our study to n-th roots of unity where the characteristic of the ground field does not divide n.

5.5.1 Cyclotomic polynomials

Let P_n be the set of *primitive* n-th roots of unity in $\mathbb{C}$. Define

$$\Phi_n = \prod_{\zeta \in P_n} (x - \zeta),$$

which a-priori is a polynomial in $\mathbb{C}[x]$. It is called the *n-th cyclotomic polynomial*. In this section we will describe a method for computing Φ_n without first computing all elements of P_n and evaluating the product. Then we will show that $\Phi_n \in \mathbb{Z}[x]$ and that Φ_n is irreducible in $\mathbb{Q}[x]$.

Lemma 5.5.5 *Let $D(n)$ be the set of all positive divisors of n (including 1 and n). Then*

$$x^n - 1 = \prod_{d \in D(n)} \Phi_d.$$

Proof. Consider the group $U_n(\mathbb{C}) \subset \mathbb{C}^*$ of order n (Lemma 5.5.3). For $d \in D(n)$ we have that P_d is exactly the set of elements of $U_n(\mathbb{C})$ that have order d. So $U_n(\mathbb{C})$ is the disjoint union of the sets P_d where d runs through $D(n)$. Hence

$$x^n - 1 = \prod_{\zeta \in U_n(\mathbb{C})} (x - \zeta) = \prod_{d \in D(n)} \prod_{\zeta \in P_d} (x - \zeta) = \prod_{d \in D(n)} \Phi_d.$$

□

We can use this lemma inductively to compute Φ_n for $n \geq 1$. Indeed, we have $\Phi_1 = x - 1$, $\Phi_2 = x + 1$ and $\Phi_3 = \frac{x^3-1}{x-1} = x^2 + x + 1$. Also $\Phi_1\Phi_2\Phi_4 = x^4 - 1$, and $\Phi_1\Phi_2 = x^2 - 1$ so that $\Phi_4 = \frac{x^4-1}{x^2-1} = x^2 + 1$. For another example, $\Phi_1\Phi_3\Phi_9 = x^9 - 1$ and $\Phi_1\Phi_3 = x^3 - 1$ and therefore $\Phi_9 = \frac{x^9-1}{x^3-1} = x^6 + x^3 + 1$.

Proposition 5.5.6 $\Phi_n \in \mathbb{Z}[x]$.

Proof. We prove this by induction on n. The induction hypothesis is that $\Phi_m \in \mathbb{Z}[x]$ for all $m < n$. Let g be the product of all Φ_d for d a divisor of n, $d \neq n$. By the induction hypothesis $g \in \mathbb{Z}[x]$. By the previous lemma $g\Phi_n \in \mathbb{Z}[x]$. Suppose that $\Phi_n \notin \mathbb{Z}[x]$ and write $\Phi_n = a_0 + \cdots + a_s x^s$, $a_i \in \mathbb{C}$. Let u be maximal with $a_u \notin \mathbb{Z}$. Write $g = b_0 + \cdots + b_t x^t$ where $b_i \in \mathbb{Z}$. Let c be the coefficient of x^{u+t} in $g\Phi_n$. Then

$$c = b_t a_u + (b_{t-1}a_{u+1} + b_{t-2}a_{u+2} + \cdots).$$

The term in brackets lies in $\mathbb{Z}$. So because $c \in \mathbb{Z}$ and $b_t = 1$ it follows $a_u \in \mathbb{Z}$ which is a contradiction. We conclude that $\Phi_n \in \mathbb{Z}[x]$. □

Theorem 5.5.7 *Φ_n is irreducible in $\mathbb{Q}[x]$.*

Proof. Fix a primitive n-th root of unity ζ_0 in $\mathbb{C}$ and let $f \in \mathbb{Q}[x]$ be its minimal polynomial. Then f divides Φ_n by Proposition 4.3.4. So there is a $g \in \mathbb{Q}[x]$ with $\Phi_n = fg$. Because Φ_n, f are monic the same holds for g. By Gauss' lemma (Lemma 2.5.13) there are rational numbers α, β such that αf, βg lie in $\mathbb{Z}[x]$ and $\Phi_n = (\alpha f)(\beta g)$. But f is monic, so $\alpha f \in \mathbb{Z}[x]$ implies $\alpha = \pm 1$. Similarly we get $\beta = \pm 1$. We conclude that $f, g \in \mathbb{Z}[x]$.

Now let $\zeta \in P_n$ be a root of f (there is at least one such ζ). Let p be a prime not dividing n. Then by Lemma 5.5.3(iii) $\zeta^p \in P_n$. We claim that ζ^p is also a root of f. Suppose that this is not the case, then ζ^p is a root of g and hence ζ is a root of $h = g(x^p)$. Therefore f and h have a nontrivial common factor. Consider the homomorphism $\psi_p : \mathbb{Z}[x] \to \mathbb{F}_p[y]$ given by

$$\psi_p(a_0 + \cdots + a_s x^s) = [a_0]_p + [a_1]_p y + \cdots + [a_s]_p y^s.$$

Since f and h have a nontrivial common factor the same holds for $\psi_p(f)$, $\psi_p(h)$. Also $\psi_p(h) = \psi_p(g)(y^p) = (\psi_p(g))^p$ (where the last equality follows from Lemma 4.7.1, along with the fact that $[a]_p^p = [a]_p$ for all $a \in \mathbb{Z}$, see Theorem 2.5.22). Hence $\psi_p(f)$, $\psi_p(g)$ must have a nontrivial common factor. But fg divides $x^n - 1$ so $\psi_p(fg) = \psi_p(f)\psi_p(g)$ implies that $\psi_p(f)\psi_p(g)$ divides $y^n - [1]_p$. Thus the latter polynomial has a root of multiplicity at least 2 in some extension of $\mathbb{F}_p$. But that is excluded by Lemma 4.7.2 as the derivative of $y^n - [1]_p$ is $[n]_p y^{n-1}$ which only has $[0]_p$ as a root because $[n]_p \neq [0]_p$. We conclude that ζ^p must be a root of f.

Finally, let $\omega \in P_n$ and write $\omega = \zeta_0^i$ with $\gcd(n, i) = 1$ (Lemma 5.5.3(iii)). Then $i = p_1 \cdots p_k$, where the p_j are primes not dividing n. By repeatedly applying the claim above we get that

$$\zeta_0^{p_1}, \zeta_0^{p_1 p_2} = (\zeta_0^{p_1})^{p_2}, \ldots, \zeta_0^i = \zeta_0^{p_1 \cdots p_k}$$

are roots of f. In other words, all elements of P_n are roots of f and hence Φ_n divides f. It follows that $f = \Phi_n$ and Φ_n is irreducible. □

5.5.2 The Galois group of a cyclotomic extension

Let F be a field and let $E \supset F$ be a splitting field of $x^n - 1$. Then we say that E is a *cyclotomic extension* of F. By Remark 5.5.4 we may assume that the characteristic of F does not divide n. Then we have that $E = F(\zeta)$, where ζ is any primitive n-th root of unity in E. Indeed, by Lemma 5.5.3(ii) $F(\zeta)$ contains all roots of $x^n - 1$. Furthermore, as $x^n - 1$ has roots of multiplicity 1 in E we have that E/F is Galois (Theorem 5.3.6).

Now we briefly introduce a class of groups that will play an important role in the sequel. For $n \geq 1$ we set

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}.$$

If $\gcd(a, n) = \gcd(b, n) = 1$ then also $\gcd(ab, n) = 1$ so that $[a]_n[b]_n = [ab]_n$ lies in $(\mathbb{Z}/n\mathbb{Z})^*$. Furthermore, if $\gcd(a, n) = 1$ then there exist $u, v \in \mathbb{Z}$ with $ua + vn = 1$. Hence $[u]_n[a]_n = [1]_n$. It follows that $(\mathbb{Z}/n\mathbb{Z})^*$ is a multiplicative group. Its order is denoted $\varphi(n)$; the function $\varphi : \mathbb{N} \to \mathbb{N}$ is called Euler's φ-function.

Theorem 5.5.8 *Let $n \geq 1$. Let F be a field of characteristic 0 or of characteristic $p > 0$ where p is a prime not dividing n. Let E be a splitting field of $x^n - 1$ over F. Then*

(i) *For $\sigma \in \mathrm{Gal}(E/F)$ there is a unique $i_\sigma \in \mathbb{Z}$ with $1 \leq i_\sigma \leq n - 1$, $\gcd(i_\sigma, n) = 1$ such that $\sigma(\omega) = \omega^{i_\sigma}$ for all $\omega \in U_n(E)$.*

(ii) *The map*

$$\psi : \mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^* \text{ defined by } \psi(\sigma) = [i_\sigma]_n$$

is an injective group homomorphism.

(iii) *ψ is surjective if and only if Φ_n is irreducible in $F[x]$.*

Proof. Fix a primitive n-th root of unity $\zeta \in U_n(E)$. Let $\sigma \in \mathrm{Gal}(E/F)$; then $\sigma(\zeta)$ is also a primitive n-th root of unity. Hence by Lemma 5.5.3 $\sigma(\zeta) = \zeta^{i_\sigma}$ for some i_σ with $\gcd(i_\sigma, n) = 1$. Because $\zeta^n = 1$ we may assume that $1 \leq i_\sigma \leq n-1$. Then i_σ is uniquely determined by σ for $\zeta^j = \zeta^{i_\sigma}$ implies that $j \equiv i_\sigma \bmod n$ (because ζ has order n). Finally, if $\omega \in U_n(E)$ then $\omega = \zeta^k$ for a certain k. Hence $\sigma(\omega) = \sigma(\zeta^k) = (\zeta^{i_\sigma})^k = \omega^{i_\sigma}$.

Let $\sigma, \tau \in \mathrm{Gal}(E/F)$. Then $\sigma(\tau(\zeta)) = \sigma\tau(\zeta)$ implies $i_\sigma i_\tau \equiv i_{\sigma\tau} \bmod n$. So $[i_\sigma]_n[i_\tau]_n = [i_\sigma i_\tau]_n = [i_{\sigma\tau}]_n$, which is another way of saying that $\psi(\sigma)\psi(\tau) = \psi(\sigma\tau)$. We see that ψ is a group homorphism. Since $E = F(\zeta)$ we have that a $\sigma \in \mathrm{Gal}(E/F)$ is uniquely determined by the value of $\sigma(\zeta)$. Therefore ψ is injective.

By Lemma 5.5.3(iii) it follows that $|P_n| = \varphi(n)$. Thus $\deg \Phi_n = \varphi(n)$. Secondly, ζ is a root of Φ_n. Indeed: it is a root of $x^n - 1$ so by Lemma 5.5.5 it is a root of a Φ_d for a divisor d of n. But we cannot have $d < n$ as otherwise ζ would be a root of $x^d - 1$ as well, and it therefore would not be primitive. Now ψ is surjective if and only if $|\mathrm{Gal}(E/F)| = \varphi(n)$ if and only if $|E : F| = \varphi(n)$ (Theorem 5.3.6(iii)) if and only if the minimal polynomial of ζ is Φ_n if and only if Φ_n is irreducible in $F[x]$. □

For the base field $\mathbb{Q}$ we summarize our findings in the following corollary.

Corollary 5.5.9 *Let E be the splitting field of $x^n - 1$ over $\mathbb{Q}$. Then $E = \mathbb{Q}(\zeta)$ where ζ is a primitive n-th root of unity. The minimal polynomial of ζ is Φ_n. Furthermore, $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$ and the isomorphism sends $[i]_n \in (\mathbb{Z}/n\mathbb{Z})^*$ to $\sigma_i \in \mathrm{Gal}(E/\mathbb{Q})$ where $\sigma(\zeta) = \zeta^i$.*

Remark 5.5.10 Let $\zeta = e^{\frac{2\pi i}{n}} \in \mathbb{C}$, then ζ is a primitive n-th root of unity. Hence $\mathbb{Q}(\zeta)$ is a splitting field of $x^n - 1$ over $\mathbb{Q}$. By the previous corollary the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ contains an element σ with $\sigma(\zeta) = \zeta^{n-1}$. We have $\sigma^2(\zeta) = \zeta$ so that $\sigma^2 = 1$ and $H = \{1, \sigma\}$ is a subgroup of order 2. Furthermore, since $\sigma(\zeta) = e^{-\frac{2\pi i}{n}}$ we see that σ is the restriction of complex conjugation to $\mathbb{Q}(\zeta)$. Therefore $\mathbb{Q}(\zeta)^H = \mathbb{Q}(\zeta) \cap \mathbb{R}$. So for instance it follows that $|\mathbb{Q}(\zeta) \cap \mathbb{R} : \mathbb{Q}| = \frac{\varphi(n)}{2}$.

Example 5.5.11 Let $\zeta \in \mathbb{C}$ be a primitive 15-th root of unity and consider the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Here we determine its Galois group and explicitly describe its Galois correspondence.

From Theorem 5.5.7 it follows that Φ_{15} is the minimal polynomial of ζ. By Lemma 5.5.5 we see that $x^{15}-1 = \Phi_1\Phi_3\Phi_5\Phi_{15}$. Now $\Phi_1\Phi_5 = x^5-1$ and $\Phi_3 = x^2+x+1$. Furthermore, $x^{15}-1 = (x^5)^3-1 = (x^5-1)((x^5)^2+x^5+1)$, so that $\Phi_{15} = \frac{x^{10}+x^5+1}{x^2+x+1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$. From this it follows that $|\mathbb{Q}(\zeta) : \mathbb{Q}| = 8$, that $1, \zeta, \zeta^2, \ldots, \zeta^7$ is a basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ and $\zeta^8 = \zeta^7 - \zeta^5 + \zeta^4 - \zeta^3 + \zeta - 1$.

Theorem 5.5.8 says that

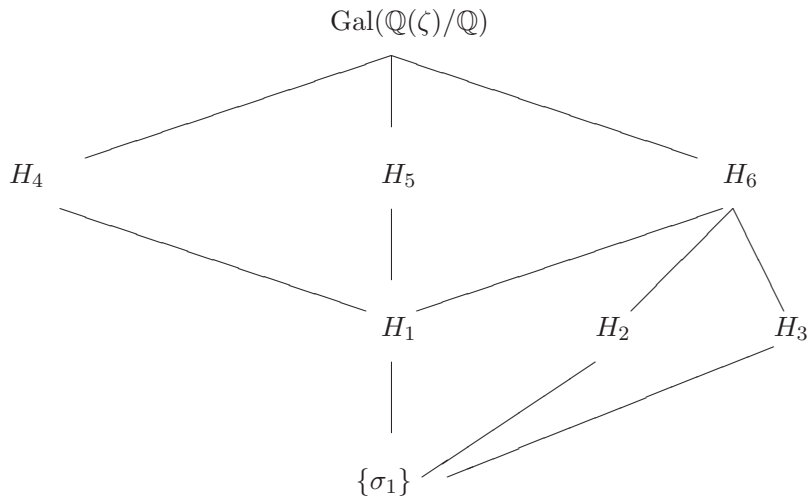
$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_4, \sigma_7, \sigma_8, \sigma_{11}, \sigma_{13}, \sigma_{14}\}$$

where $\sigma_i(\zeta) = \zeta^i$ and $\sigma_i\sigma_j = \sigma_{ij \bmod 15}$. This yields the following multiplication table

	σ_1	σ_2	σ_4	σ_7	σ_8	σ_{11}	σ_{13}	σ_{14}
σ_1	σ_1	σ_2	σ_4	σ_7	σ_8	σ_{11}	σ_{13}	σ_{14}
σ_2	σ_2	σ_4	σ_8	σ_{14}	σ_1	σ_7	σ_{11}	σ_{13}
σ_4	σ_4	σ_8	σ_1	σ_{13}	σ_2	σ_{14}	σ_7	σ_{11}
σ_7	σ_7	σ_{14}	σ_{13}	σ_4	σ_{11}	σ_2	σ_1	σ_8
σ_8	σ_8	σ_1	σ_2	σ_{11}	σ_4	σ_{13}	σ_{14}	σ_7
σ_{11}	σ_{11}	σ_7	σ_{14}	σ_2	σ_{13}	σ_1	σ_8	σ_4
σ_{13}	σ_{13}	σ_{11}	σ_7	σ_1	σ_{14}	σ_8	σ_4	σ_2
σ_{14}	σ_{14}	σ_{13}	σ_{11}	σ_8	σ_7	σ_4	σ_2	σ_1

We determine the subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. The orders of the elements $\sigma_1, \sigma_2, \ldots, \sigma_{14}$ are respectively 1, 4, 2, 4, 4, 2, 4, 2. Hence we have three subgroups of order 2: $H_1 = \{\sigma_1, \sigma_4\}$, $H_2 = \{\sigma_1, \sigma_{11}\}$, $H_3 = \{\sigma_1, \sigma_{14}\}$. A subgroup of order 4 is either cyclic or consists of three elements of order 2 apart from σ_1. We immediately see that we get $H_4 = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8\}$, $H_5 = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{13}\}$ (the cyclic subgroups), and $H_6 = \{\sigma_1, \sigma_4, \sigma_{11}, \sigma_{14}\}$.

Figure 5.5: Subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.



Now we determine the intermediate fields corresponding to these subgroups. First we look around for some obvious intermediate fields. We see that ζ^3 is a primitive fifth root of unity so $\mathbb{Q}(\zeta^3)$ is a field extension of degree 4 of $\mathbb{Q}$. Hence it corresponds to a subgroup of order 2. By looking at the available subgroups of that order we see that it must be H_2, that is, $\mathbb{Q}(\zeta^3) = \mathbb{Q}(\zeta)^{H_2}$. Secondly, ζ^5 is a primitive third root of unity, so that $|\mathbb{Q}(\zeta^5) : \mathbb{Q}| = 2$ and this field corresponds to a subgroup of order 4. By looking at which of those groups leave ζ^5 invariant we see that it must be H_5, i.e., $\mathbb{Q}(\zeta^5) = \mathbb{Q}(\zeta)^{H_5}$.

We deal with the other groups by solving sets of linear equations. First consider H_1. Let $a = a_0 + a_1\zeta + \cdots + a_7\zeta^7$. Then

$$\begin{aligned}\sigma_4(a) =&(a_0 - a_2 - a_6 + a_7) + (a_2 + a_4 - a_7)\zeta + (-a_3 + a_6)\zeta^2 + (-a_2 - a_6)\zeta^3 \\ &+ (a_1 + a_2 - a_7)\zeta^4 + (-a_2 + a_5 + a_7)\zeta^5 - a_6\zeta^6 + (a_2 - a_3 + a_6 - a_7)\zeta^7.\end{aligned}$$

Hence $\sigma_4(a) = a$ if and only if

$$\begin{aligned} -a_2 - a_6 + a_7 &= 0 \\ -a_1 + a_2 + a_4 - a_7 &= 0 \\ -a_2 - a_3 + a_6 &= 0 \\ -a_2 - a_3 - a_6 &= 0 \\ a_1 + a_2 - a_4 - a_7 &= 0 \\ -a_2 + a_7 &= 0 \\ -2a_6 &= 0 \\ a_2 - a_3 + a_6 - 2a_7 &= 0, \end{aligned}$$

which are equivalent to $a_6 = 0$, $a_2 = -a_3 = a_7$, $a_1 = a_4$. Hence

$$\mathbb{Q}(\zeta)^{H_1} = \{a_0 + a_1\zeta + a_2\zeta^2 - a_2\zeta^3 + a_1\zeta^4 + a_5\zeta^5 + a_2\zeta^7 \mid a_i \in \mathbb{Q}\}.$$

The element $\zeta + \zeta^4$ has exactly four different images under $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Therefore its minimal polynomial over $\mathbb{Q}$ has degree 4 (Lemma 5.3.3) and consequently it is a primitive element of $\mathbb{Q}(\zeta)^{H_1}$, that is, $\mathbb{Q}(\zeta)^{H_1} = \mathbb{Q}(\zeta + \zeta^4)$.

The computation for H_3 is analogous, therefore we omit the details. Here the linear equations on

the a_i are equivalent to

$$\begin{aligned} a_1 + a_2 - a_5 - a_6 - a_7 &= 0 \\ a_4 + a_5 + a_6 &= 0 \\ a_2 + a_3 - a_5 &= 0 \\ a_1 + 2a_2 + 2a_3 + a_4 &= 0, \end{aligned}$$

so that

$$\mathbb{Q}(\zeta)^{H_3} = \{a_0+a_1\zeta+a_2\zeta^2+a_3\zeta^3+(-a_1-2a_2-2a_3)\zeta^4+(a_2+a_3)\zeta^5+(a_1+a_2+a_3)\zeta^6+(-a_2-2a_3)\zeta^7 \mid a_i \in \mathbb{Q}\}.$$

Again using Lemma 5.3.3 we see that the minimal polynomial of $\zeta - \zeta^4 + \zeta^6$ has degree 4, so that $\mathbb{Q}(\zeta)^{H_3} = \mathbb{Q}(\zeta - \zeta^4 + \zeta^6)$.

Note that H_4 is cyclic and generated by σ_2. Hence $a \in \mathbb{Q}(\zeta)^{H_4}$ if and only if $\sigma_2(a) = a$. The linear equations equivalent to that reduce to $a_1 = a_4 = -2a_5$, $a_2 = -a_3 = a_7 = -a_5$, $a_6 = 0$, so that

$$\mathbb{Q}(\zeta)^{H_4} = \{a_0 - 2a_5\zeta - a_5\zeta^2 + a_5\zeta^3 - 2a_5\zeta^4 + a_5\zeta^5 - a_5\zeta^7 \mid a_5 \in \mathbb{Q}\}.$$

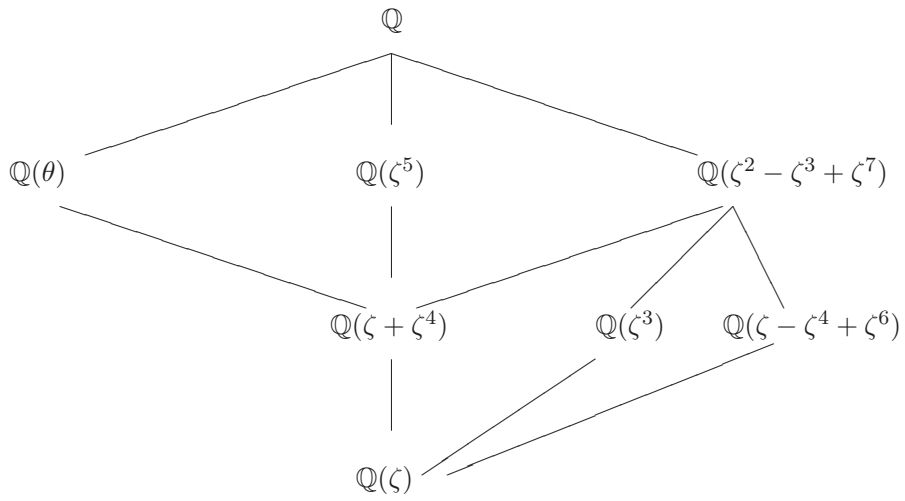
In this case it is obvious that $\mathbb{Q}(\zeta)^{H_4} = \mathbb{Q}(\theta)$ with $\theta = 2\zeta + \zeta^2 - \zeta^3 + 2\zeta^4 - \zeta^5 + \zeta^7$ (in fact, it can be shown the the minimal polynomial of θ is $x^2 - 3x + 6$).

Finally, $\sigma_4\sigma_{14} = \sigma_{11}$ and hence $a \in \mathbb{Q}(\zeta)^{H_6}$ if and only if $\sigma_4(a) = \sigma_{14}(a) = a$. But the linear equations corresponding to $\sigma_4(a) = a$ and $\sigma_{14}(a) = a$ have already been studied above. Together they amount to $a_1 = a_4 = a_5 = a_6 = 0$, $a_2 = -a_3 = a_7$. So

$$\mathbb{Q}(\zeta)^{H_6} = \{a_0 + a_2\zeta^2 - a_2\zeta^3 + a_2\zeta^7 \mid a_2 \in \mathbb{Q}\} = \mathbb{Q}(\zeta^2 - \zeta^3 + \zeta^7).$$

(The minimal polynomial of $\zeta^2 - \zeta^3 + \zeta^7$ is $x^2 - x - 1$.) Figure 5.6 has the subfields together with the inclusions between them.

Figure 5.6: Subfields of $\mathbb{Q}(\zeta)$.



5.6 Solvability of polynomial equations by radicals

In this section we look at Galois' main application of his theory: a criterion for deciding whether the roots of a given polynomial can be expressed by radicals. The criterion says that this happens precisely when the Galois group of the splitting field of the polynomial is *solvable*. The latter is a property of

groups which we study first. Then we derive Galois' criterion and use it to find a polynomial of degree 5 whose roots cannot be expressed by radicals. Then after an intermezzo on discriminants we come to the final topic of this chapter, the so-called irreducible case, which explains why, when expressing the roots of a polynomial of degree 3 by radicals we always need square roots of negative numbers, also if all roots lie in $\mathbb{R}$.

5.6.1 Solvable groups

Definition 5.6.1 *A group G is called* solvable *if there is a series of subgroups $G = G_1 \supset G_2 \supset \cdots \supset G_m = \{1\}$ such that G_{i+1} is a normal subgroup of G_i and G_i/G_{i+1} is abelian for $1 \leq i \leq m-1$.*

For example abelian groups are solvable. Slightly less trivially, the dihedral groups D_n (Section 3.1.2) are solvable. Indeed, let $G_2 \subset D_n$ be the subgroup consisting of the $\sigma_{[i]}$. As seen in Example 3.3.2 this is a normal subgroup. As D_n/G_2 has order 2 it is abelian. Secondly, G_2 is abelian as well, so our series is $D_n \supset G_2 \supset G_3 = \{\sigma_{[0]}\}$.

In order to show that a given group is solvable it suffices to find a series of subgroups as in the definition. Proving that a given group is *not* solvable seems much more difficult. It is our next objective to derive a criterion for doing that.

Let G be a group and $A \subset G$. Let H be the intersection of all subgroups of G that contain A. It is obvious that H is a subgroup of G, and that every subgroup of G that contains A must also contain H. We say that H is the subgroup of G *generated* by A.

Definition 5.6.2 *Let G be a group. For $g, h \in G$ we set $[g,h] = g^{-1}h^{-1}gh$, which is called the* commutator *of g, h. Let A be the set of all commutators of all elements of G then by $[G,G]$ we denote the subgroup of G generated by A. It is called the* commutator subgroup *of G.*

We note that $[g,h] = 1$ if and only if $gh = hg$, i.e., if and only if g, h commute. It follows that G is abelian if and only if $[G,G]$ is the trivial subgroup.

Lemma 5.6.3 *Let G be a group. Then $[G,G]$ is a normal subgroup and the quotient $G/[G,G]$ is abelian. Moreover, for a normal subgroup $N \subset G$ we have that G/N is abelian if and only if N contains $[G,G]$.*

Proof. Let $h \in [G,G]$ and $g \in G$ then $ghg^{-1} = hh^{-1}ghg^{-1} = h[h, g^{-1}]$. We see that $ghg^{-1} \in [G,G]$ and therefore it is a normal subgroup.

Let N be a normal subgroup of G and for $g \in G$ write $\bar{g}$ for the coset gN. The definition of the multiplication in quotient groups implies that $[\bar{g}, \bar{h}] = \overline{[g,h]}$. Furthermore, G/N is abelian if and only if $[\bar{g}, \bar{h}] = \bar{1}$ for all $g, h \in G$. But this is the same as $\overline{[g,h]} = \bar{1}$, which in turn is equivalent to $[g,h] \in N$. We conclude that G/N is abelian if and only if $[g,h] \in N$ for all $g, h \in G$. The latter is obviously equivalent to $[G,G] \subset N$. □

Definition 5.6.4 *Let G be a group and define $G^{(1)} = G$ and for $k \geq 1$, $G^{(k+1)} = [G^{(k)}, G^{(k)}]$. The series $G = G^{(1)} \supset G^{(2)} \supset \cdots$ is called the* derived series *of G.*

Proposition 5.6.5 *Let G be a group. Then G is solvable if and only if there is an $s \geq 1$ with $G^{(s)} = \{1\}$.*

Proof. First of all, if $G^{(s)} = \{1\}$ then using Lemma 5.6.3 we see that the derived series is a series satisfying Definition 5.6.1. Hence G is solvable.

If G is solvable then let $G = G_1 \supset G_2 \supset \cdots \supset G_m = \{1\}$ be a series as in Definition 5.6.1. By induction we show that $G^{(k)} \subset G_k$. This is certainly true for $k = 1$. Suppose it holds for a certain $k \geq 1$. Because G_k/G_{k+1} is abelian we have $[G_k, G_k] \subset G_{k+1}$ by Lemma 5.6.3. Hence

$$G^{(k+1)} = [G^{(k)}, G^{(k)}] \subset [G_k, G_k] \subset G_{k+1}.$$

The conclusion is that $G^{(m)} = \{1\}$. □

Corollary 5.6.6 *Subgroups and quotients of solvable groups are solvable.*

Proof. Let G be a solvable group and H a subgroup. By induction it is straightforward to see that $H^{(k)} \subset G^{(k)}$. So by the previous proposition, H is solvable as well.

Let $N \subset G$ be a normal subgroup. Let $\pi : G \to G/N$ be the surjective homomorphism with $\pi(g) = gN$. We claim that $\pi(G^{(k)}) \supset (G/N)^{(k)}$ for $k \geq 1$. For $k = 1$ this is obvious, so suppose $k \geq 1$ and $\pi(G^{(k)}) \supset (G/N)^{(k)}$. As in the proof of Lemma 5.6.3 we write $\bar{g}$ for the coset gN. Let $\bar{g}, \bar{h} \in (G/N)^{(k)}$; then we may assume that $g, h \in G^{(k)}$. Then $[\bar{g}, \bar{h}] = \overline{[g, h]} = \pi([g, h])$ and hence $[\bar{g}, \bar{h}] \in \pi(G^{(k+1)})$. It follows that $\pi(G^{(k+1)})$ is a subgroup of G/N containing all $[\bar{g}, \bar{h}]$ for $\bar{g}, \bar{h} \in (G/N)^{(k)}$. Hence it contains $(G/N)^{(k+1)}$. Our claim is proved, and it immediately implies that G/N is solvable. □

Now we investigate the solvability of the symmetric groups S_n introduced in Section 3.1.1. As shown there we can write every element of S_n as a product of disjoint cycles. Because

$$(i_1, \ldots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$$

we can also write every element as a product of 2-cycles. However, this way of writing is far from unique. For example $(1, 2)(2, 3)(1, 2) = (1, 3)$. We see that not even the number of 2-cycles that appear in different expressions for a given $\pi \in S_n$ is always the same. But we can prove that the *parity* of the number of 2-cycles is constant. For this we define an *inversion* of a $\pi \in S_n$ to be a pair (i, j) with $i < j$ but $\pi(i) > \pi(j)$. We let $\mathrm{inv}(\pi)$ be the number of inversions of π. For example, $\pi = (1, 2, 3) \in S_3$ has inversions $(1, 3)$, $(2, 3)$ so that $\mathrm{inv}(\pi) = 2$.

Lemma 5.6.7 *Let $\pi, \sigma \in S_n$. Then $\mathrm{inv}(\pi\sigma) \equiv \mathrm{inv}(\pi) + \mathrm{inv}(\sigma) \bmod 2$.*

Proof. Set

$$\begin{aligned}
A &= \{(i, j) \mid 1 \leq i < j \leq n, \sigma(i) < \sigma(j), \pi\sigma(i) < \pi\sigma(j)\} \\
B &= \{(i, j) \mid 1 \leq i < j \leq n, \sigma(i) < \sigma(j), \pi\sigma(i) > \pi\sigma(j)\} \\
C &= \{(i, j) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j), \pi\sigma(i) < \pi\sigma(j)\} \\
D &= \{(i, j) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j), \pi\sigma(i) > \pi\sigma(j)\}.
\end{aligned}$$

Then $\mathrm{inv}(\pi\sigma) = |B| + |D|$, $\mathrm{inv}(\pi) = |B| + |C|$, $\mathrm{inv}(\sigma) = |C| + |D|$. The lemma follows. □

Corollary 5.6.8 *Let $\pi \in S_n$ and write $\pi = \pi_1 \cdots \pi_k = \sigma_1 \cdots \sigma_l$, where the π_i, σ_j are 2-cycles. Then $k \equiv l \bmod 2$.*

Proof. Note that the number of inversions of a 2-cycle is odd. So using the previous lemma we see that $\mathrm{inv}(\pi) \equiv k \bmod 2$ and $\mathrm{inv}(\pi) \equiv l \bmod 2$. □

The elements of S_n that can be written as a product of an even number of 2-cycles are called *even*. The others are called *odd*. It is obvious that the set of even permutations forms a subgroup of S_n. It is called the *alternating group*, and denoted A_n. Consider the 2-cycle $(1, 2)$. It is immediate that S_n is the disjoint union of A_n and $(1, 2)A_n$. Hence $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$. Now we show that $[S_n, S_n] = A_n$. For that we first need a little lemma.

Lemma 5.6.9 *Let $A \subset S_n$ be the set consisting of all 3-cycles. Then A_n is generated by A.*

Proof. Let $H \subset S_n$ denote the group generated by A. We have $(i, j, k) = (i, j)(j, k)$ so that 3-cycles are even and hence H is contained in A_n.

Now consider two 2-cycles, $\pi = (i, j)$, $\sigma = (k, l)$. If $\{i, j\} = \{k, l\}$ then $\pi\sigma = 1$. If $\{i, j\} \cap \{k, l\}$ consists of one element, say $j = k$, then $\pi\sigma = (i, j, l)$. If $\{i, j\}$, $\{k, l\}$ are disjoint then $\pi\sigma = (i, k, j)(k, l, i)$. We conclude that $\pi\sigma$ lies in H. Hence every even permutation lies in H, in other words, $A_n \subset H$. □

Proposition 5.6.10 $[S_n, S_n] = A_n$.

Proof. For $\pi \in S_n$ we have that π and π^{-1} have the same parity. Hence $[\pi, \sigma] = \pi^{-1}\sigma^{-1}\pi\sigma$ is even. It follows that $[S_n, S_n] \subset A_n$. On the other hand,

$$[(i,j),(i,k)] = (i,j)(i,k)(i,j)(i,k) = (i,j,k).$$

Hence $[S_n, S_n]$ contains every 3-cycle and therefore it contains A_n be the previous lemma. □

Theorem 5.6.11 *The group S_n is solvable for $n = 2, 3, 4$ and not solvable otherwise.*

Proof. We have that S_2 is abelian and hence solvable. The group A_3 is of order 3 and abelian, hence $[A_3, A_3] = \{1\}$. Using Propositions 5.6.10, 5.6.5 we conclude that S_3 is solvable. Let

$$V_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

For $\pi \in S_n$ we have $\pi(i,j)(k,l)\pi^{-1} = (\pi(i), \pi(j))(\pi(k), \pi(l))$. It follows that V_4 is a normal subgroup of A_4 (even of S_4). The quotient A_4/V_4 has order 3 and hence is abelian. So $S_4 \supset A_4 \supset V_4 \supset \{1\}$ is a series as in Definition 5.6.1. So S_4 is solvable as well.

Now suppose that $n \geq 5$. Let i, j, k, s, t be distinct elements of $\{1, \ldots, n\}$. Then

$$[(i,s,j),(i,t,k)] = (j,s,i)(k,t,i)(i,s,j)(i,t,k) = (i,j,k).$$

Hence $[A_n, A_n]$ contains every 3-cycle and by Proposition 5.6.10 we see that $[A_n, A_n] = A_n$. By Proposition 5.6.5 S_n is not solvable. □

Now we want to show that a *finite solvable* group has a descending series of subgroups such that the successive quotients have prime order. For this we need a theorem due to Cauchy.

Theorem 5.6.12 (Cauchy) *Let G be a finite group and p a prime dividing $|G|$. Then G has an element of order p.*

Proof. Let T be the set of all p-tuples $(g_1, \ldots, g_p)$ where $g_i \in G$ and $g_1 \cdots g_p = 1$. Note that the first $p-1$ elements of such a p-tuple can be chosen arbitrarily in G, and then the last element is determined by $g_p = (g_1 \cdots g_{p-1})^{-1}$. Hence $|T| = |G|^{p-1}$ and in particular we see that p divides $|T|$.

Let T_0 be the subset of T consisting of the tuples $(g, \ldots, g)$ with $g^p = 1$. Of course T_0 contains $(1, \ldots, 1)$. Hence the theorem is equivalent to the statement $|T_0| > 1$. (Indeed, if $g^p = 1$ and $g \neq 1$ then the order of g is p by Lemma 3.7.6.)

For $(g_1, \ldots, g_p) \in T$ set $\varphi(g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1})$. Because

$$g_p g_1 \cdots g_{p-1} = g_p g_1 \cdots g_{p-1} g_p g_p^{-1} = g_p g_p^{-1} = 1$$

we see that φ maps T to T. Note that it has an obvious inverse and hence φ is a bijection. Furthermore, φ maps T_0 and $T_1 = T \setminus T_0$ to themselves.

Let $t \in T_1$. Observe that $\varphi^p(t) = t$. Let $k \geq 1$ be minimal with $\varphi^k(t) = t$. Then $k \leq p$ and write $p = qk + r$ with $0 \leq r < k$. Then

$$t = \varphi^p(t) = \varphi^r((\varphi^k)^q(t)) = \varphi^r(t),$$

and it follows that $r = 0$ and $k = p$ because p is prime. It follows that the elements $t, \varphi(t), \ldots, \varphi^{p-1}(t)$ are all distinct. So T_1 is the disjoint union of subsets $\{t, \varphi(t), \ldots, \varphi^{p-1}(t)\}$. It follows that p divides $|T_1|$. As p divides $|T|$ we see that it must divide $|T_0|$ as well and wqe are done. □

Remark 5.6.13 We can reformulate this proof using the language of group actions (see Section 3.5). Let $\mathcal{G} = \{1, \varphi, \ldots, \varphi^{p-1}\}$. Then $\mathcal{G}$ is a group of order p (it is a subgroup of the group S_{T_1} of all permutations of T_1). It naturally acts on T_1. The stabilizer of a $t \in T_1$ is a subgroup of $\mathcal{G}$. However, because this group has p elements, its only subgroups are $\{1\}$ and $\mathcal{G}$ itself. Hence the stabilizer of each $t \in T_1$ is trivial. So by the orbit-stabilizer theorem (Corollary 3.5.13) it follows that each orbit of $\mathcal{G}$ on T_1 has p elements.

Theorem 5.6.14 *Let G be a finite solvable group. Then G has a series of subgroups $G = G_1 \supset G_2 \supset \cdots \supset G_m = \{1\}$ such that G_{i+1} is a normal subgroup of G_i and G_i/G_{i+1} is abelian and of prime order.*

Proof. The proof is by induction on $|G|$. The induction hypothesis is that all solvable groups of cardinality less than $|G|$ have a series as in the theorem. Because G is solvable it has a normal subgroup N such that $G \neq N$ and G/N is abelian. Write $H = G/N$. If the order of H is not prime then write $|H| = ps$, where p is a prime and $s > 1$ an integer. By Theorem 5.6.12 H has an element of order p, and thus it has a subgroup M of order p. Since H is abelian, M is automatically normal. Now consider the homomorphisms $\pi_1 : G \to H$, $\pi_1(g) = gN$, and $\pi_2 : H \to H/M$, $\pi_2(h) = hM$ and let $\pi = \pi_2 \circ \pi_1$. Then π is a group homomorphism and let $N' = \ker(\pi)$ be its kernel. Then N' is not all of G because π_1 is surjective and the kernel of π_2 is not all of H. We have that N' strictly contains N and G/N' is abelian as well (this follows for example from Lemma 5.6.3). We can continue this process and eventually we find a normal subgroup N'' of G such that $N'' \neq G$, G/N'' is abelian and G/N''' is of prime order. Set $G_2 = N''$.

By Corollary 5.6.6 we have that G_2 is solvable. So by the induction hypothesis there is a series of subgroups $G_2 \supset G_3 \supset \cdots \supset G_m = \{1\}$ with the properties stated in the theorem. It follows that G has such a series as well. □

5.6.2 Radical extensions

In this section we prove an amazing theorem by Galois: there are expressions for the roots of a given polynomial, involving arithmetic operations and taking n-th roots (for $n \geq 2$) if and only if the Galois group of the spliting field of the polynomial is solvable. In order to be able to do that we first translate the existence of the mentioned expressions into a property of the splitting field.

In this section all fields are of characteristic 0.

Definition 5.6.15 *A field extension E/F is said to be* radical *if there is a tower of fields $F = F_1 \subset F_2 \subset \cdots \subset F_{m+1} = E$ such that for $1 \leq i \leq m$ we have $F_{i+1} = F_i(\alpha_i)$ where $\alpha_i \in F_{i+1}$ satisfies $\alpha_i^{n_i} \in F_i$ for some $n_i > 0$.*

With the notation of this definition write $\beta_i = \alpha_i^{m_i}$. Then $\beta_i \in F_i$ and α_i can be thought of as an n_i-th root of β_i.

Definition 5.6.16 *Let F be a field and $f \in F[x]$. Then f is called* solvable by radicals *if there is a radical extension E/F such that E contains a splitting field of f.*

Note that solvability by radicals exactly means that there are expressions for the roots of f involving the arithmetic operations, elements of F and n-th roots $\sqrt[n]{\ }$. Also we remark that it is not enough to require that the splitting field itself is a radical extension, as there are examples of splitting fields that are contained in radical extensions but are not radical extensions themselves.

Proposition 5.6.17 *Let E/F be a radical extension. Then there is an extension K/E such that K/F is radical and Galois.*

Proof. Because E/F is radical there is a tower as in Definition 5.6.15. In particular $E = F(\alpha_1, \ldots, \alpha_m)$. Let f_i be the minimal polynomial of α_i over F. Set $f = f_1 \ldots f_m$ and let $K \supset E$ be a splitting field of f over E. Since the α_i are roots of f we have that K is also a splitting field of f over F. The extension K/F is Galois by Theorem 5.3.6 (note that f is automatically separable because the characteristic is 0).

Write $\mathrm{Gal}(K/F) = \{\sigma_1, \ldots, \sigma_n\}$, where σ_1 is the identity. Using Lemma 5.3.3 we see that for each root β of f_i there is a σ_j with $\beta = \sigma_j(\alpha_i)$. Hence $K = F(\sigma_j(\alpha_i) \mid 1 \leq i \leq m, 1 \leq j \leq n)$. Set

$$F_{i,j} = F(\sigma_1(\alpha_1), \ldots, \sigma_1(\alpha_m), \sigma_2(\alpha_1), \ldots, \sigma_2(\alpha_m), \sigma_3(\alpha_1), \ldots, \sigma_j(\alpha_1), \ldots, \sigma_j(\alpha_i)).$$

Then for $1 \leq i \leq m-1$ we have $F_{i+1,j} = F_{i,j}(\sigma_j(\alpha_{i+1}))$. Now $\sigma_j(\alpha_{i+1})^{n_{i+1}} = \sigma_j(\alpha_{i+1}^{n_{i+1}})$. But $\alpha_{i+1}^{n_{i+1}} \in F_{i+1} = F(\alpha_1, \ldots, \alpha_i)$. Hence $\alpha_{i+1}^{n_{i+1}}$ can be written in terms of elements of F and $\alpha_1, \ldots, \alpha_i$ (and arithmetic operations). It follows that $\sigma_j(\alpha_{i+1}^{n_{i+1}})$ lies in $F(\sigma_j(\alpha_1), \ldots, \sigma_j(\alpha_i)) \subset F_{i,j}$.

Secondly, for $1 \leq j \leq n-1$ we have $F_{1,j+1} = F_{m,j}(\sigma_{j+1}(\alpha_1))$ and $\sigma_{j+1}(\alpha_1)^{n_1} = \sigma_{j+1}(\alpha_1^{n_1}) = \alpha_1^{n_1} \in F \subset F_{m,j}$. We conclude that we have the tower

$$F \subset F_{1,1} \subset F_{2,1} \subset \cdots \subset F_{m,1} \subset F_{1,2} \subset F_{2,2} \subset \cdots \subset F_{m,2} \subset \cdots \subset F_{m,n} = K$$

and therefore K/F is radical. □

Lemma 5.6.18 *Let K/F be an extension such that there is an $\alpha \in K$ with $K = F(\alpha)$ and $\alpha^n \in F$ for some $n > 0$. Suppose that F contains a primitive n-th root of unity. Then K/F is Galois and* $\mathrm{Gal}(K/F)$ *is abelian.*

Proof. Let $\omega \in F$ be a primitive m-th root of unity. Consider the polynomial $f = x^n - \alpha^n \in F[x]$. The roots of f in K are $\alpha, \omega\alpha, \ldots, \omega^{n-1}\alpha$ and they are all distinct as ω is primitive. Therefore f splits into linear factors in $K[x]$ and we see that K is a splitting field of f over F. So by Theorem 5.3.6 K/F is Galois.

A $\sigma \in \mathrm{Gal}(K/F)$ is uniquely determined by the value of $\sigma(\alpha)$, which has to be a root of f. Hence $\sigma(\alpha) = \omega^i\alpha$ for a certain i with $0 \leq i < n$. Let τ be a second element of $\mathrm{Gal}(K/F)$ and write $\tau(\alpha) = \omega^j\alpha$. Because $\omega \in F$ we have $\sigma(\omega) = \tau(\omega) = \omega$ implying that

$$\sigma\tau(\alpha) = \omega^{i+j}\alpha = \tau\sigma(\alpha).$$

Hence $\mathrm{Gal}(K/F)$ is abelian. □

Proposition 5.6.19 *Let F be a field and $f \in F[x]$. Let E be a splitting field of f over F. If f is solvable by radicals then* $\mathrm{Gal}(E/F)$ *is solvable.*

Proof. By Definition 5.6.16 E is contained in a field K such that K/F is radical. By Proposition 5.6.17 we may assume that K/F is Galois as well. Let $F = F_1 \subset \cdots \subset F_{m+1} = K$ be a tower of extensions such that $F_{i+1} = F_i(\alpha_i)$, $\alpha_i^{n_i} \in F_i$. We now would like to apply the Galois correspondence and obtain a series of subgroups of the Galois group. However, in order to conclude anything on these subgroups we need the previous lemma that assumes that the base field contains certain roots of unity. The trick is to add all needed roots of unity and to put them at the bottom of the tower.

Set $n = n_1 \cdots n_m$ and let L be the splitting field of $x^n - 1$ over K. Since K/F is Galois it is the splitting field of some $h \in F[x]$. Hence L is the splitting field of $h(x^n - 1)$ over F and we see that L/F is Galois. Furthermore, as remarked in Section 5.5.2 we have $L = K(\omega)$ where ω is a primitive n-th root of unity. So $L = F(\alpha_1, \ldots, \alpha_m, \omega)$ and we consider the tower

$$F \subset F(\omega) \subset F(\omega, \alpha_1) \subset F(\omega, \alpha_1, \alpha_2) \subset \cdots \subset F(\omega, \alpha_1, \ldots, \alpha_m) = L.$$

Set $\mathcal{G} = \mathrm{Gal}(L/F)$. To the fields in the tower we apply the Galois correspondence, that is, we set $\mathcal{G}_i = \mathrm{Gal}(L/F(\omega, \alpha_1, \ldots, \alpha_i))$ (so that $\mathcal{G}_0 = \mathrm{Gal}(L/F(\omega))$).

Note that all fields, from $F(\omega)$ onwards, contain a primitive n_i-th root of unity for all i. (Indeed, if we set $s_i = n/n_i$ then ω^{s_i} is a primitive n_i-th root of unity.) For $0 \leq i \leq m-1$ consider the extensions

$$F(\omega, \alpha_1, \ldots, \alpha_i) \subset F(\omega, \alpha_1, \ldots, \alpha_i, \alpha_{i+1}) \subset L.$$

By Lemma 5.6.18 the first of these is Galois with abelian Galois group. So by Proposition 5.4.4 we have that $\mathcal{G}_{i+1}$ is normal in $\mathcal{G}_i$ and the quotient is abelian. Furthermore, $F(\omega)$ is the splitting field of $x^n - 1$ over F so that $F(\omega)/F$ is Galois with abelian Galois group (the latter by Theorem 5.5.8(ii)). Again using Proposition 5.4.4 we see that $\mathcal{G}_0$ is normal in $\mathcal{G}$ with abelian quotient. So we have a series of subgroups

$$\mathcal{G} \supset \mathcal{G}_0 \supset \cdots \supset \mathcal{G}_m = \{1\}$$

satisfying the requirements of Definition 5.6.1. Hence $\mathcal{G}$ is solvable.

But that is not the group that we were interested in! Consider the extensions $F \subset E \subset L$. Here E/F is Galois, so that $N = \mathrm{Gal}(L/E)$ is a normal subgroup and $\mathrm{Gal}(E/F) \cong \mathcal{G}/N$ (again by Proposition 5.4.4). Now with Corollary 5.6.6 we conclude that $\mathrm{Gal}(E/F)$ is solvable. □

Lemma 5.6.20 *Let K/F be a Galois extension of prime degree p. Suppose that F contains a primitive p-th root of unity. Then there is an $\alpha \in K$ such that $K = F(\alpha)$ and $\alpha^p \in F$.*

Proof. Write $H = \mathrm{Gal}(K/F)$ then $|H| = p$ by Theorem 5.3.6. Let $\sigma \in H$ be different from the identity. Then σ has order p by Proposition 3.7.4. Hence σ generates H, that is

$$H = \{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}\}.$$

Now we view K as a vector space over F and $\sigma : K \to K$ as a linear map. Let λ be an eigenvalue of σ (this λ could lie in an extension of F). Then $\sigma^p = 1$ implies that $\lambda^p = 1$ and because of the assumption on F we see that F contains all eigenvalues of σ. Now suppose that the only eigenvalue of σ is 1. Then the characteristic polynomial of σ is $f = (x-1)^p$. The Cayley-Hamilton theorem now implies that $f(\sigma) = 0$, that is, $(\sigma - I_K)^p = 0$, where I_K is the identity map on K. Because $\sigma^p = 1$ we also have that $g(\sigma) = 0$ with $g = x^p - 1$. Furthermore $\gcd(f, g) = x - 1$ so there are $u, v \in F[x]$ with $uf + vg = x - 1$ (Theorem 2.3.11). But that implies that $\sigma = 1$, which is not the case. Hence σ has an eigenvalue λ not equal to 1. Let $\alpha \in E$ be a corresponding eigenvector, i.e., $\sigma(\alpha) = \lambda\alpha$. Then $\alpha \notin F$ (as otherwise $\sigma(\alpha) = \alpha$). Because $|K : F| = p$ there are no intermediate fields other than F and K. Hence $K = F(\alpha)$. Finally, $\sigma(\alpha^p) = (\lambda\alpha)^p = \lambda^p\alpha^p = \alpha^p$ and as σ generates H we have that $\alpha^p \in K^H = F$. □

Proposition 5.6.21 *Let F be a field and $f \in F[x]$. Let E be a splitting field of f over F. Suppose that* $\mathrm{Gal}(E/F)$ *is solvable. Then f is solvable by radicals.*

Proof. Write $G = \mathrm{Gal}(E/F)$. By Theorem 5.6.14 G has a normal subgroup N such that G/N is abelian of prime order p. Let $E' \supset E$ be a splitting field of $x^p - 1$. In the same way as in the proof of Proposition 5.6.19 we see that $E' = E(\omega)$ where ω is a primitive p-th root of unity and that E'/F is Galois. Since also E/F is Galois we have that $\sigma(E) = E$ for all $\sigma \in \mathrm{Gal}(E'/F)$ (Proposition 5.4.4). So we can define the homomorphism

$$\psi : \mathrm{Gal}(E'/F(\omega)) \to G \text{ with } \psi(\sigma) = \sigma|_E.$$

(Note that $\mathrm{Gal}(E'/F(\omega))$ is a subgroup of $\mathrm{Gal}(E'/F)$.)

We have that ψ is injective. Indeed, let $\sigma \in \mathrm{Gal}(E'/F(\omega))$ be such that $\psi(\sigma) = 1$. Then $\sigma(\alpha) = \alpha$ for $\alpha \in E$. Furthermore, $\sigma(\omega) = \omega$ is automatic from $\sigma \in \mathrm{Gal}(E'/F(\omega))$. Hence σ is the identity on E'. So the kernel of ψ is trivial and hence ψ is injective. It follows that $\mathrm{Gal}(E'/F(\omega))$ is isomorphic to a subgroup of G.

We prove the theorem by induction on $|G|$. The induction hypothesis is that for all Galois extensions L/K with $\mathrm{Gal}(L/K)$ solvable and of order less than $|G|$ we have that L is contained in a radical extension of K. We consider two cases.

In the first case we have $|\mathrm{Gal}(E'/F(\omega))| < |G|$. By the induction hypothesis E' is contained in a radical extension M of $F(\omega)$. But since $F \subset F(\omega)$ is radical, M is also a radical extension of F.

In the second case we have $|\mathrm{Gal}(E'/F(\omega))| = |G|$. Then $\mathrm{Gal}(E'/F(\omega))$ is isomorphic to G and it follows that $\mathrm{Gal}(E'/F(\omega))$ also has a normal subgroup H' such that the quotient is abelian of order p. Let M be the corresponding intermediate field, that is,

$$M = E'^{H'} = \{\alpha \in E' \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H'\}.$$

By the Galois correspondence (more precisely Lemma 5.4.1(i)) we have that $H' = \mathrm{Gal}(E'/M)$. Now we apply Proposition 5.4.4 and find that $M/F(\omega)$ is a Galois extension with Galois group isomorphic to $\mathrm{Gal}(E'/F(\omega))/H'$ which has p elements. Hence $|M : F(\omega)| = p$ and from Lemma 5.6.20 we see that there is an $\alpha \in M$ with $M = F(\omega, \alpha)$ and $\alpha^p \in F(\omega)$.

As $|\mathrm{Gal}(E'/M)| = |H'| < |G|$ we infer by induction that there is a radical extension R of M with $E' \subset R$. But we have just seen that M is a radical extension of F, so that R is also a radical extension of F. Because it contains E the theorem is proved. □

We unite the two previous propositions in the following theorem due to Galois.

Theorem 5.6.22 (Galois) *Let F be a field and let $f \in F[x]$ have splitting field E over F. Then f is solvable by radicals if and only if* $\mathrm{Gal}(E/F)$ *is solvable.*

Example 5.6.23 We can use the strategy of the proof of Proposition 5.6.21 to find radical expressions for the roots of a given $f \in F[x]$ such that the Galois group G of its splitting field E is solvable. This works especially well when we have a series of subgroups $G = G_1 \supset G_2 \supset \cdots \supset G_s = \{1\}$ with G_{i+1} normal in G_i and G_i/G_{i+1} abelian of order 2. Ideed, let $F_i = E^{G_i}$; then $E = F_s \supset F_{s-1} \supset \cdots \supset F_1 = F$ where $|F_i : F_{i-1}| = 2$. Write $\mathrm{Gal}(F_i/F_{i-1}) = \{\tau_0, \tau_1\}$ where τ_0 is the identity and $\tau_1^2 = \tau_0$. Note that F_{i-1} contains a primitive second root of unity, namely -1. So by Lemma 5.6.20, $F_i = F_{i-1}(\alpha_{i-1})$ with $\alpha_{i-1}^2 \in F_{i-1}$. Finally, by the proof of the mentioned lemma, finding such an α_{i-1} amounts to solving the equation $\tau_1(\alpha_{i-1}) = -\alpha_{i-1}$. So we can construct a radical tower and in the end find an expression for a root of f using only square roots.

We illustrate this in the case of $f = x^{15} - 1 \in \mathbb{Q}[x]$. The Galois correspondence for its slitting field is described in Example 5.5.11. Consider the subgroups

$$G \supset H_5 = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{13}\} \supset H_1 = \{\sigma_1, \sigma_4\} \supset \{\sigma_1\}$$

corresponding to the chain of subfields $\mathbb{Q} \subset \mathbb{Q}(\zeta^5) \subset \mathbb{Q}(\zeta + \zeta^4) \subset \mathbb{Q}(\zeta)$. By Proposition 5.4.4 we have $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^4)/\mathbb{Q}) \cong G/H_1$. The cosets of H_1 in G are $\sigma_1 H_1$, $\sigma_2 H_1$, $\sigma_7 H_1$ and $\sigma_{11} H_1$. So $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^4)/\mathbb{Q}) = \{\bar\sigma_1, \bar\sigma_2, \bar\sigma_7, \bar\sigma_{11}\}$, where $\bar\sigma_i$ is the restriction of σ_i to $\mathbb{Q}(\zeta + \zeta^4)$. Furthermore, $\mathbb{Q}(\zeta^5) = \mathbb{Q}(\zeta + \zeta^4)^{\{\bar\sigma_1, \bar\sigma_7\}}$ so that $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^4)/\mathbb{Q}(\zeta^5)) = \{\bar\sigma_1, \bar\sigma_7\}$. That also means that $\mathrm{Gal}(\mathbb{Q}(\zeta^5)/\mathbb{Q}) = \{\hat\sigma_1, \hat\sigma_2\}$, where $\hat\sigma_i$ is the restriction of σ_i to $\mathbb{Q}(\zeta^5)$.

Now we write the chain of subfields as a radical tower. We start with $\mathbb{Q}(\zeta^5) \supset \mathbb{Q}$. Finding $\alpha \in \mathbb{Q}(\zeta^5)$ with $\mathbb{Q}(\zeta^5) = \mathbb{Q}(\alpha)$ and $\alpha^2 \in \mathbb{Q}$ amounts to solving $\hat\sigma_2(\alpha) = -\alpha$. Write $\alpha = a + b\zeta^5$ with $a, b \in \mathbb{Q}$. Then $\hat\sigma_2(\alpha) = a + b\zeta^{10} = a - b - b\zeta^5$. So $\hat\sigma_2(\alpha) = -\alpha$ is the same as $2a = b$. We choose $a = 1$, $b = 2$ and hence $\alpha = 1 + 2\zeta^5$. (Then $\alpha^2 = -3$.)

Next we consider $\mathbb{Q}(\zeta + \zeta^4) \supset \mathbb{Q}(\zeta^5)$. Write $\theta = \zeta + \zeta^4$ then $\bar\sigma_7(\theta) = \zeta^7 + \zeta^{28} = 1 - \zeta - \zeta^4 + \zeta^5 = 1 + \zeta^5 - \theta$. To find a $\beta \in \mathbb{Q}(\theta)$ with $\mathbb{Q}(\theta) = \mathbb{Q}(\beta)$ and $\beta^2 \in \mathbb{Q}(\zeta^5)$ amounts to finding a $\beta \in \mathbb{Q}(\theta)$ with $\bar\sigma_7(\beta) = -\beta$. Write $\beta = a + b\theta$ with $a, b \in \mathbb{Q}(\zeta^5)$. Then $\bar\sigma_7(\beta) = a + (1 + \zeta^5)b - b\theta$. So $\bar\sigma_7(\beta) = -\beta$ amounts to $2a + (\zeta^5 + 1)b = 0$. We choose $a = \zeta^5 + 1$ and $b = -2$ so that $\beta = 1 + \zeta^5 - 2(\zeta + \zeta^4)$. (Then $\beta^2 = 5\zeta^5$.)

Finally we look at $\mathbb{Q}(\zeta) \supset \mathbb{Q}(\zeta + \zeta^4)$. We first compute the minimal polynomial of ζ over the second field. According to Lemma 5.3.3 the minimal polynomial of ζ is $(x - \zeta)(x - \sigma_4(\zeta))$, which is equal to $x^2 - (\zeta + \zeta^4)z + \zeta^5$. In particular we have the relation $\zeta^2 = (\zeta + \zeta^4)\zeta - \zeta^5$. (Which, of course, is also easy to see directly.) Write $\gamma = a + b\zeta$ with $a, b \in \mathbb{Q}(\zeta + \zeta^5)$. Then $\sigma_4(\gamma) = a + b\zeta^4 = a + b((\zeta + \zeta^4) - \zeta)$. So $\sigma_4(\gamma) = -\gamma$ amounts to $2a + (\zeta + \zeta^4)b = 0$. We choose $a = \zeta + \zeta^4$, $b = -2$ so that $\gamma = (\zeta + \zeta^4) - 2\zeta$. (Then $\gamma^2 = (\zeta + \zeta^4)^2 - 4\zeta(\zeta + \zeta^4) + 4\zeta^4 = (\zeta + \zeta^4)^2 - 4\zeta^5$.)

Now we construct an injective homomorphism $Q(\zeta) \to \mathbb{C}$ in the following way. We start with the identity homomorphism $\psi_0 : \mathbb{Q} \to \mathbb{C}$. By Lemma 4.6.6 there exists a unique injective homomorphism $\psi_1 : \mathbb{Q}(\alpha) \to \mathbb{C}$ with $\psi_1(a) = a$ for $a \in \mathbb{Q}$ and $\psi_1(\alpha) = \sqrt{-3}$. Note that $\zeta^5 = \frac{\alpha - 1}{2}$, so that $\psi_1(\zeta^5) = \frac{\sqrt{-3} - 1}{2}$. So by the same lemma there exists an injective homomorphism $\psi_2 : \mathbb{Q}(\alpha, \beta) \to \mathbb{C}$ such that $\psi_2(a) = \psi_1(a)$ for all $a \in \mathbb{Q}(\alpha)$ and $\psi_2(\beta) = \sqrt{\frac{5}{2}(\sqrt{-3} - 1)}$. We have $\zeta + \zeta^4 = \frac{1}{2}(\zeta^5 + 1 - \beta) = \frac{\alpha + 1 - 2\beta}{4}$ and therefore

$$\psi_2(\zeta + \zeta^4) = \frac{1 + \sqrt{-3} - 2\sqrt{\frac{5}{2}(\sqrt{-3} - 1)}}{4}.$$

Again by Lemma 4.6.6 we get an injective homomorphism $\psi_3 : \mathbb{Q}(\alpha, \beta, \gamma) \to \mathbb{C}$ with $\gamma_2(a) = a$ for all $a \in \mathbb{Q}(\alpha, \beta)$ and

$$\psi_2(\gamma) = \sqrt{\left(\frac{1 + \sqrt{-3} - 2\sqrt{\frac{5}{2}(\sqrt{-3} - 1)}}{4}\right)^2 - 2(\sqrt{-3} - 1)}.$$

We have $\zeta = \frac{1}{2}(\zeta + \zeta^4 - \gamma)$. So we also get a radical expression for $\psi_3(\zeta)$. After some manipulation it

is seen to be

$$\frac{1}{8}\left(1+\sqrt{-3}-\sqrt{10(\sqrt{-3}-1)}-\sqrt{20-20\sqrt{-3}-2\sqrt{-3}\sqrt{10(\sqrt{-3}-1)}-2\sqrt{10(\sqrt{-3}-1)}}\right).$$

(Here we have to be a bit careful as something like $\sqrt{u}$ can indicate two complex numbers. With ψ_1 we fix a choice for $\sqrt{-3}$; with ψ_2 we fix $\sqrt{10(\sqrt{-3}-1)}$. Then $\sqrt{-3}\sqrt{10(\sqrt{-3}-1)}$ is the product of these two. If we would write this as $\sqrt{-30(\sqrt{-3}-1)}$ then we would introduce another choice, not necessarily compatible with the first two.)

5.6.3 A polynomial not solvable by radicals

Here we give a polynomial of degree five whose roots are not expressible by radicals. By Theorem 5.6.22 along with Theorem 5.6.11 a polynomial whose splitting field has Galois group isomorphic to S_5 has this property. The main problem now is to show that the splitting field of a given polynomial has this Galois group. Indeed, because $|S_5| = 120$ we cannot simply list its elements and compute a multiplication table. We need to resort to some tricks to show that the Galois group is isomorphic to S_5. For this we first show how to identify a Galois group with a permutation group, a construction that is of wider interest.

Let F be a field, $f \in F[x]$ a separable polynomial and $E \supset F$ its splitting field. Let $\alpha_1, \ldots, \alpha_n \in E$ be the roots of f without repetitions (that is, we just take the roots of the irreducible factors of f). Then by definition $E = F(\alpha_1, \ldots, \alpha_n)$ (Definition 4.6.1). Let $\sigma \in \mathrm{Gal}(E/F)$. For $1 \leq i \leq n$ we have that $\sigma(\alpha_i)$ is a root of f, hence equal to an α_j. Moreover, for $i_1 \neq i_2$ we cannot have $\sigma(\alpha_{i_1}) = \sigma(\alpha_{i_2})$ because σ is injective. It follows that there is a $\pi_\sigma \in S_n$ with

$$\sigma(\alpha_i) = \alpha_{\pi_\sigma(i)} \text{ for } 1 \leq i \leq n.$$

Define a map $\psi : \mathrm{Gal}(E/F) \to S_n$ by $\psi(\sigma) = \pi_\sigma$.

Lemma 5.6.24 *ψ is an injective group homomorphism.*

Proof. Let $\sigma, \tau \in \mathrm{Gal}(E/F)$. Then $\sigma\tau(\alpha_i) = \sigma(\tau(\alpha_i))$ translates to

$$\alpha_{\pi_{\sigma\tau}(i)} = \alpha_{\pi_\sigma \pi_\tau(i)}$$

so that $\pi_{\sigma\tau}(i) = \pi_\sigma\pi_\tau(i)$ for all i. In other words, $\pi_{\sigma\tau} = \pi_\sigma\pi_\tau$, which just means that ψ is a group homomorphism.

If $\psi(\sigma) = \psi(\tau)$ then $\sigma(\alpha_i) = \tau(\alpha_i)$ for all i, and because $E = F(\alpha_1, \ldots, \alpha_n)$ this implies that $\sigma = \tau$. We see that ψ is injective. □

Let $H = \psi(\mathrm{Gal}(E/F))$. Then H is a subgroup of S_n and $\psi : \mathrm{Gal}(E/F) \to H$ is an isomorphism. So $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of S_n.

Now let $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ with splitting field $E \subset \mathbb{C}$. By Eisenstein's criterion (Theorem 2.5.14) f is irreducible. So it has five distinct roots in $\mathbb{C}$ and by the above construction we have that $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to a subgroup H of S_5. With a few steps we prove that this subgroup is equal to S_5.

H contains a 5-cycle. Let $\alpha \in E$ be a root of f then $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 5$, so since $|E : \mathbb{Q}| = |E : \mathbb{Q}(\alpha)||\mathbb{Q}(\alpha) : \mathbb{Q}|$ (Theorem 4.3.3) we have that $|E : \mathbb{Q}|$ is divisible by 5. Because $|\mathrm{Gal}(E/\mathbb{Q})| = |E : \mathbb{Q}|$ we have the same for the order of the Galois group. Hence by Theorem 5.6.12 H contains an element of order 5. Now the order of a k-cycle in S_n is k. By listing the various possible decompositions of an element of S_5 as a product of disjoint cycles and using Proposition 3.7.7 it is seen that an element of order 5 must be a 5-cycle, denote it π_5.

H contains a 2-cycle. By computing the derivative of f we see that the graph of f (seen as a function $\mathbb{R} \to \mathbb{R}$) has one positive maximum and one negative minimum. Therefore f has exactly three real roots, denoted $\alpha_3, \alpha_4, \alpha_5$, and hence exactly two non-real roots, denoted α_1, α_2. The latter

are complex conjugates. Let $\sigma : \mathbb{C} \to \mathbb{C}$ be complex conjugation, i.e., $\sigma(x+iy) = x - iy$ for $x, y \in \mathbb{R}$. Then σ permutes the roots of f and therefore maps E to itself. Furthermore, σ is an automorphism of $\mathbb{C}$ and hance its restriction to E is as well. We have $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_1$, $\sigma(\alpha_i) = \alpha_i$ for $i = 3, 4, 5$. Hence $\pi_\sigma = (1, 2)$.

Write $\pi_5 = (1, i_2, i_3, i_4, i_5)$. Then $\pi_5^2 = (1, i_3, i_5, i_2, i_4)$, $\pi_5^3 = (1, i_4, \ldots)$, $\pi_5^4 = (1, i_5, \ldots)$. We see that H contains the 5-cycle $(1, 2, j_3, j_4, j_5)$. By relabelling the α_i for $i = 3, 4, 5$ we now may assume that $j_k = k$ and that H contains $(1, 2, 3, 4, 5)$.

Finally, $(1, 2)$ and $(1, 2, 3, 4, 5)$ generate S_5 (we leave this verification as an exercise). The conclusion is that $H = S_5$.

5.6.4 The discriminant of a polynomial

Let F be a field and $f \in F[x]$. Let E be a splitting field of f and write $f = \gamma(x - \alpha_1) \cdots (x - \alpha_n)$ where $\gamma \in F$ and $\alpha_i \in E$. Then

$$D(f) = \gamma^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

is the *discriminant* of f. (The γ^{2n-2} is a normalizing factor to make some formulas work out better.)

As an immediate property we mention that $D(f) = 0$ if and only if f has a root of multiplicity at least 2.

Example 5.6.25 Let $f = ax^2 + bx + c = a(x - \alpha_1)(x - \alpha_2)$. Then $\alpha_1 + \alpha_2 = -\frac{b}{a}$, $\alpha_1\alpha_2 = \frac{c}{a}$. Hence

$$(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = \frac{b^2}{a^2} - 4\frac{c}{a}.$$

It follows that $D(f) = a^2(\alpha_1 - \alpha_2)^2 = b^2 - 4ac$.

Example 5.6.26 The discriminant of a polynomial is a *symmetric polynomial* in the roots of f (this means that it is unchanged when we permute the roots in any way). It can be shown that this implies that the discriminant of a monic polynomial can be expressed as a polynomial in the coefficients of f. For example, if $f = x^3 + ax^2 + bx + c$ then

$$D(f) = a^2b^2 - 4a^3c + 18abc - 4b^3 - 27c^2.$$

So it is possible to decide whether f has a root of multiplicity at least 2 without computing any of the roots explicitly!

Proposition 5.6.27 *Let f be a field and $f \in F[x]$. Suppose that f is separable and square-free. Let $\alpha_1, \ldots, \alpha_n$ be the (necessarily distict) roots of f in its splitting field E. Consider the injective group homomorphism $\psi : \mathrm{Gal}(E/F) \to S_n$ constructed in Section 5.6.3. Then*

(i) *$D(f) \in F$,*

(ii) *$\psi(\mathrm{Gal}(E/F))$ is contained in the alternating group A_n if and only if $D(f)$ is a square in F.*

Proof. Let $P = \{(i, j) \mid 1 \le i < j \le n\}$. For $\pi \in S_n$ define the map $\tilde{\pi} : P \to P$ by

$$\tilde{\pi}(i, j) = \begin{cases} (\pi(i), \pi(j)) & \text{if } \pi(i) < \pi(j) \\ (\pi(j), \pi(i)) & \text{if } \pi(i) > \pi(j) \end{cases}.$$

The inverse of $\tilde{\pi}$ is $\tilde{\tau}$, where $\tau = \pi^{-1}$. In particular it follows that $\tilde{\pi}$ is bijective. For $(i, j) \in P$ we set $\delta_{(i,j)} = \alpha_i - \alpha_j$. Then $\delta_{\tilde{\pi}(i,j)} = \alpha_{\pi(i)} - \alpha_{\pi(j)}$ if (i, j) is *not* an inversion of π and it is equal to $-(\alpha_{\pi(i)} - \alpha_{\pi(j)})$ if (i, j) is an inversion of π.

Now let $\sigma \in \mathrm{Gal}(E/F)$ and write $\psi(\sigma) = \pi_\sigma$. Let $\Delta = \prod_{(i,j) \in P} \delta_{(i,j)}$. Then

$$\sigma(\Delta) = \prod_{(i,j) \in P} (\alpha_{\pi_\sigma(i)} - \alpha_{\pi_\sigma(j)}) = (-1)^{\mathrm{inv}(\pi_\sigma)} \prod_{(i,j) \in P} \delta_{\tilde{\pi}_\sigma(i,j)} = (-1)^{\mathrm{inv}(\pi_\sigma)} \Delta.$$

(Where $\mathrm{inv}(\pi)$ is the number of inversions of π, see Section 5.6.1.)

Hence

$$\sigma(\Delta^2) = \sigma(\Delta)^2 = ((-1)^{\mathrm{inv}(\pi_\sigma)}\Delta)^2 = \Delta^2.$$

We conclude that Δ^2 is fixed under all $\sigma \in \mathrm{Gal}(E/F)$ so that $\Delta^2 \in F$. So the same holds for $D(f) = \gamma^{2n-2}\Delta^2$ where γ is the leading coefficient of f.

Secondly it follows that $\sigma(\Delta) = \Delta$ if and only if $\mathrm{inv}(\pi_\sigma)$ is even. By definition that is the same as $\pi_\sigma \in A_n$. It follows that $\psi(\mathrm{Gal}(E/F)) \subset A_n$ if and only if $\Delta \in F$. But the latter is obviously equivalent to $D(f)$ being a square in F. □

Remark 5.6.28 Note that when f has roots of multiplicity at least 2 then $D(f) = 0$ and in particular, $D(f) \in F$.

5.6.5 Casus irreducibilis

Let $f \in \mathbb{Q}[x]$ be of degree 3 with real roots. Then when using the known formulas for finding a root of f one invariably finds square roots of negative numbers along the way. This phenomenon was extensively studied by the bolognese mathematician Rafael Bombelli, who in the 1572 edition of his book *L'Algebra* looks at the following example. Let $f = x^3 - 15x - 4$. The roots of f are 4 and $-2 \pm \sqrt{3}$. However, the formulas give as one of the solutions

$$\sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}.$$

Bombelli noticed that $(2 + i)^3 = 2 + 11i$, $(2 - i)^3 = 2 - 11i$ so that the sum above reduces to $(2 + i) + (2 - i) = 4$. As Bombelli put it: "Somma 4; e tanto vale la Cosa." (The sum is 4 and that is the value of the thing.)

Here we prove the "irreducible case": if f is irreducible then there always must appear square roots of negative numbers in a radical expression for a root of f.

Lemma 5.6.29 *Let F be a field of characteristic 0 and $f \in F[x]$ be monic and irreducible of degree 3. Let $E \supset F$ be a splitting field and write $D = D(f)$. Let $\alpha \in E$ be one of the roots of f. Then $E = F(\alpha, \sqrt{D})$.*

Proof. Let $\beta, \gamma \in E$ be the other two roots of f. Of course, $\alpha \in E$ and

$$\sqrt{D} = \pm(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$$

also lies in E. Hence $F(\alpha, \sqrt{D}) \subset E$.

Let $K = F(\alpha, \sqrt{D})$. We now show that $\beta, \gamma \in K$. First of all, in $K[x]$ we have a factorization $f = (x - \alpha)g$, where $g \in K[x]$ is of degree 2. But $g = (x - \beta)(x - \gamma)$. Hence $\beta + \gamma \in K$. Next we observe that $g(\alpha) = (\alpha - \beta)(\alpha - \gamma)$ also lies in K. So K contains

$$\frac{\sqrt{D}}{g(\alpha)} = \frac{\pm(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)}{(\alpha - \beta)(\alpha - \gamma)} = \pm(\beta - \gamma).$$

Since $\beta + \gamma$ and $\beta - \gamma$ both lie in K, so do β, γ.

So K is a subfield of E containing F and the roots of f. It follows that $K = E$. □

Lemma 5.6.30 *Let F be a field and p a prime. Let $a \in F$. If the polynomial $x^p - a$ is reducible in $F[x]$ then it has a root in F.*

Proof. We may assume $a \neq 0$.

Let $E \supset F$ be a splitting field of $f = x^p - a$. Let $\alpha \in E$ be a root of f. Let $\beta \in E$ be a second root of f. Then $\left(\frac{\beta}{\alpha}\right)^p = 1$ so that $\beta = \alpha\omega$ where $\omega \in E$ satisfies $\omega^p = 1$. It follows that $\alpha\omega_1, \ldots, \alpha\omega_p$ are the roots of f where $\omega_i^p = 1$.

Suppose that $f = gh$ with $g, h \in F[x]$ and $\deg(g), \deg(h) \geq 1$. Write $k = \deg(g)$; hence

$$g = (x - \omega_{i_1}\alpha) \cdots (x - \omega_{i_k}\alpha).$$

Let $\zeta = \omega_{i_1} \cdots \omega_{i_k}$ then $\zeta^p = 1$ and the constant coefficient of g is $\pm\zeta\alpha^k$. So $\zeta\alpha^k \in F$.

Moreover, $\gcd(p, k) = 1$ and hence there are integers u, v with $up + vk = 1$ (Theorem 2.2.3). But $(\zeta\alpha^k)^p = (\alpha^p)^k = a^k$ hence

$$a = a^1 = (a^u)^p (a^k)^v = (a^u)^p (\zeta\alpha^k)^p = (a^u \zeta\alpha^k)^p.$$

We conclude that $a = \beta^p$ for a $\beta \in F$ and f has a root in F. □

Theorem 5.6.31 (Casus irreducibilis) *Let $f \in \mathbb{Q}[x]$ be of degree 3 and irreducible. Suppose that f has three real roots. Let $E \subset \mathbb{R}$ be a splitting field of f. Let $K \supset E$ be a radical extension of $\mathbb{Q}$ contained in $\mathbb{C}$. Then K is not contained in $\mathbb{R}$.*

Note that the radical extension K exists by Theorem 5.6.22. Indeed, by the construction in Section 5.6.3 we see that the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to a subgroup of S_3 which is solvable.

Proof. Suppose that $K \subset \mathbb{R}$. We will derive a contradiction from that.

By definition we have a tower $\mathbb{Q} = F_1 \subset F_2 \subset \cdots \subset F_{m+1} = K$ with $F_{i+1} = F_i(\alpha_i)$ and $\alpha_i^{m_i} \in F_i$ for $1 \leq i \leq m$. We observe that we may assume that each m_i is prime. Indeed, suppose that $m_i = ps$ where p is a prime and $s > 1$. Then we replace $F_i \subset F_{i+1}$ in the tower by $F_i \subset F_i(\beta) \subset F_{i+1}$ where $\beta = \alpha_i^s$: we have $\beta^p \in F_i$ and $F_{i+1} = F_i(\beta, \alpha_i)$ with $\alpha_i^s \in F_i(\beta)$. Continuing this process we arrive at a longer tower where all exponents are prime.

Since $\sqrt{D} \in K$ (by Lemma 5.6.29) we can also consider the intermediate fields $L_i = \mathbb{Q}(\sqrt{D}, \alpha_1, \ldots, \alpha_i)$ for $0 \leq i \leq m$ (so $L_0 = \mathbb{Q}(\sqrt{D})$). This yields the tower

$$\mathbb{Q} \subset L_0 \subset L_1 \subset \cdots \subset L_m = K.$$

We note that f is irreducible in $L_0[x]$. Indeed, otherwise f has a root β in L_0 because f is of degree 3. But $|\mathbb{Q}(\beta) : \mathbb{Q}| = 3$ because f is irreducible. Since $D \in \mathbb{Q}$ we have that $|\mathbb{Q}(\sqrt{D}) : \mathbb{Q}| \leq 2$, and that is a contradiction (a field extension of degree 2 cannot contain an extension of degree 3).

Now f is reducible in $L_m[x]$. Hence there is an $i \geq 0$ such that f is irreducible in $L_i[x]$ but reducible in $L_{i+1}[x]$. Writing $\alpha = \alpha_{i+1}$, $p = m_{i+1}$ we have $L_{i+1} = L_i(\alpha)$ with $\alpha^p \in L_i$ where p is prime.

Set $h = x^p - \alpha^p \in L_i[x]$. The roots of h in $\mathbb{C}$ are $\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{p-1}\alpha$, where $\zeta \in \mathbb{C}$ is a primitive p-th root of unity. If $p = 2$ then these are $\alpha, -\alpha$ which are not contained in L_i. If $p > 2$ then except α none of the roots of h are real, so that again we conclude that L_i contains no root of h. By Lemma 5.6.30 we see that h is irreducible in $L_i[x]$. Hence h is the minimal polynomial of α and $|L_{i+1} : L_i| = p$. In particular, there are no intermediate fields M with $L_i \subsetneq M \subsetneq L_{i+1}$.

Because f is reducible in $L_{i+1}[x]$ we have that L_{i+1} contains a root γ of f. But since $E = \mathbb{Q}(\sqrt{D}, \gamma)$ (Lemma 5.6.29) we see that E is contained in L_{i+1}. In particular, L_{i+1} contains all three roots of f, and therefore L_{i+1} contains a splitting field of f over L_i. From the remark on the intermediate fields it now follows that L_{i+1} is a splitting field of f over L_i.

Also $L_i(\gamma)$ is an intermediate field and as $\gamma \notin L_i$ it follows that $L_{i+1} = L_i(\gamma)$. As f is irreducible in $L_i[x]$ it is the minimal polynomial of γ over L_i. Hence $|L_{i+1} : L_i| = 3$ and we have that $p = 3$.

Now we turn back to h. Its roots in $\mathbb{C}$ are $\alpha, \zeta\alpha, \zeta^2\alpha$. By hypothesis α is real, also implying that the other two are not real. But L_{i+1} is the splitting field of f over L_i, and in particular the extension L_{i+1}/L_i is normal. Because h is irreducible and has a root in L_{i+1} it must have all its roots in L_{i+1}. But that contradicts our assumption that K is contained in $\mathbb{R}$.

So we have obtained a contradiction, and it follows that K cannot be contained in $\mathbb{R}$. □

5.7 Applications of Galois theory

5.7.1 The fundamental theorem of algebra

The so-called fundamental theorem of algebra states that every polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$ (or, in other words, that $\mathbb{C}$ is algebraically closed). This theorem has a long history and many proofs exist. Here we describe a proof using Galois theory.

First we show that it is enough to prove that every polynomial in $\mathbb{R}[x]$ has a root in $\mathbb{C}$. For $z = x+iy \in \mathbb{C}$ (with $x, y \in \mathbb{R}$) let $\bar{z} = x-iy$ denote its complex conjugate. Then $z \mapsto \bar{z}$ is an automorphism of $\mathbb{C}$. We extend this to an autmorphism of $\mathbb{C}[x]$ by mapping a polynomial $a_0 + a_1x + \cdots + a_mx^m$ to $\bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_mx^m$. Let $f \in \mathbb{C}[x]$; then $\overline{f\bar{f}} = \bar{f}f = f\bar{f}$ so that $f\bar{f} \in \mathbb{R}[x]$. But if $\alpha \in \mathbb{C}$ is a root of $f\bar{f}$ then it has to be a root of f or of $\bar{f}$. In the second case $\bar{\alpha}$ is a root of f. So if we know that every polynomial in $\mathbb{R}[x]$ has a root in $\mathbb{C}$ then the same follows for every polynomial in $\mathbb{C}[x]$.

Secondly we remark that every polynomial of degree 2 in $\mathbb{C}[x]$ has a root in $\mathbb{C}$. Because of the quadratic formula this is equivalent to each element of $\mathbb{C}$ having a square root in $\mathbb{C}$. So let $z = x + iy \in \mathbb{C}$, where $x, y \in \mathbb{R}$. Then $z = (u + iv)^2 = (u^2 - v^2) + 2uvi$; hence we have to solve the equations $u^2 - v^2 = x$, $2uv = y$ over $\mathbb{R}$. Because $\sqrt{x^2 + y^2} \geq |x|$ there are $u, v \in \mathbb{R}$ with

$$u^2 = \frac{1}{2}x + \frac{1}{2}\sqrt{x^2 + y^2},\ v^2 = -\frac{1}{2}x + \frac{1}{2}\sqrt{x^2 + y^2}.$$

If we choose u to be positive and the sign of v equal to the sign of y then these u, v are solutions to the original equations, and hence $z = (u + iv)^2$.

Now let $f \in \mathbb{R}[x]$ and suppose that it has no roots in $\mathbb{C}$. Let $E/\mathbb{C}$ be its splitting field over $\mathbb{C}$. Hence $|E : \mathbb{C}| > 1$. Then $E/\mathbb{R}$ is the splitting field of the polynomial $f(x^2 + 1)$. Let $\mathcal{G} = \mathrm{Gal}(E/\mathbb{R})$ and write $|\mathcal{G}| = 2^s m$ with m odd. Now by Sylow's theorem in group theory (see for example [DF04], §4.5, Theorem 18) there is a subgroup $\mathcal{H}$ of $\mathcal{G}$ of order 2^s. Set $K = E^{\mathcal{H}}$. Then $|K : \mathbb{R}| = m$ which is odd. Let $\alpha \in K$, then the degree of the minimal polynomial of α over $\mathbb{R}$ is $|\mathbb{R}(\alpha) : \mathbb{R}|$ which must be odd as well by the degree formula. It is an elementary fact of analysis that every polynomial of odd degree in $\mathbb{R}[x]$ has a root in $\mathbb{R}$. Therefore we must have $m = 1$ and $|\mathcal{G}| = 2^s$.

Write $G = \mathrm{Gal}(E/\mathbb{C})$. Then G is a subgroup of $\mathcal{G}$ so that $|G| = 2^t$ for some $t > 0$. It can be shown that groups of prime power order are solvable (let P be such a group; one first shows that the centre Z of P is non-trivial ([DF04], §6.1, Theorem 1); then P/Z is solvable by induction, and as Z is solvable the same follows for P). Hence by Theorem 5.6.14 G has a normal subgroup H with $[G : H] = 2$. Set $L = E^H$. Then $|L : \mathbb{C}| = 2$. Let $\alpha \in L \setminus \mathbb{C}$. Then its minimal polynomial over $\mathbb{C}$ has degree 2. As we have seen above, each such a polynomial has a root in $\mathbb{C}$. Hence we have a contradiction and it follows that f has a root in $\mathbb{C}$.

5.7.2 Proving that certain primitive functions are not elementary

We know, for example, that $\int x^3\,\mathrm{d}x = \frac{1}{4}x^4$, $\int \sin(x)\,\mathrm{d}x = -\cos(x)$, $\int xe^{x^2}\,\mathrm{d}x = \frac{1}{2}e^{x^2}$. However, we have never seen a nice expression for $\int e^{x^2}\,\mathrm{d}x$. Of course, we can define the function $p : \mathbb{R}_{\geq 0} \to \mathbb{R}$ by $p(x) = \int_0^x e^{t^2}\,\mathrm{d}t$ with which we have $\int e^{x^2}\,\mathrm{d}x = p(x)$ (or, in other words, $p'(x) = e^{x^2}$). But by doing it this way we do not feel that we have really solved the problem because we define the solution in terms of an integral. Indeed, by writing $\int f(x)\,\mathrm{d}x$ we ask for a primitive function of $f(x)$, or, in other words, a function whose derivative is $f(x)$. By using the function p we say nothing other than "a primitve of e^{x^2} exists and it is called p". In fact, we could use this "method" also in other cases, for example defining $q(x) = \int_0^x x^3\,\mathrm{d}t$ we also have that $q'(x) = x^3$. Here it is obvious that the expression $q(x) = \frac{1}{4}x^4$ gives much more information on the function q.

Here we will show that for $\int e^{x^2}\,\mathrm{d}x$ there does not exist a "nice" expression. In order to prove this, and to arrive at a satisfactory definition of what a "nice" expression is, we will consider functions as formal objects, that is as elements of a field to which we can apply arithmetical operations. The only extra property, not generally satisfied by field elements, is that we have a notion of derivative, which also is a formal operation.

For convenience *all fields that we consider in this section are of characteristic 0.*

Definition 5.7.1 *A* differential field *is a field F together with an operation $' : F \to F$ (called the* derivation *of F) such that $(a+b)' = a' + b'$ and $(ab)' = a'b + ab'$ for all $a, b \in F$.*

Example 5.7.2 Let z be an indeterminate over $\mathbb{C}$ and consider the field

$$\mathbb{C}(z) = \left\{ \frac{p}{q} \mid p, q \in \mathbb{C}[z], q \neq 0 \right\}.$$

For $'$ we can take the "normal" $\frac{\mathrm{d}}{\mathrm{d}z}$, i.e.,

$$\left(\frac{p}{q}\right)' = \frac{p'q - pq'}{q^2},$$

where $p'q'$ are defined as in Section 4.7.1.

We remark that it is possible to consider also other derivations, such as $z\frac{\mathrm{d}}{\mathrm{d}z}$.

Lemma 5.7.3 *Let F be a differential field with derivation $'$. Then we have the following (for $a, b, a_1, \ldots, a_n \in F^*$)*

(i) $1' = 0$,

(ii) $(\frac{1}{a})' = -\frac{a'}{a^2}$,

(iii) $(\frac{a}{b})' = \frac{a'b - ab'}{b^2}$,

(iv) $(a^n)' = na'a^{n-1}$ *for* $n \in \mathbb{Z}$,

(v) $\frac{(a_1^{\nu_1} \cdots a_n^{\nu_n})'}{a_1^{\nu_1} \cdots a_n^{\nu_n}} = \nu_1 \frac{a_1'}{a_1} + \cdots + \nu_n \frac{a_n'}{a_n}$ *for all* $\nu_1, \ldots, \nu_n \in \mathbb{Z}$.

Proof. Using Definition 5.7.1 we see that $1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1' = 1' + 1'$ implying that $1' = 0$. Therefore $0 = 1' = (a \cdot \frac{1}{a})' = a' \cdot \frac{1}{a} + a \cdot (\frac{1}{a})'$ which implies (ii).

Continuing, $(\frac{a}{b})' = (a \cdot \frac{1}{b})' = a' \cdot \frac{1}{b} + a \cdot (-\frac{b'}{b^2})$ from which we get (iii).

The proof of (iv) for $n > 0$ is a straightforward induction. For $n < 0$ we write $a^n = (\frac{1}{a})^{-n}$. Since $-n > 0$ we see that $(a^n)' = -n(\frac{1}{a})^{-n-1}(-\frac{a'}{a^2}) = na'a^{n-1}$.

The last statement is perhaps best proved first for $n = 2$. Then we have $(a_1^{\nu_1} a_2^{\nu_2})' = \nu_1 a_1' a_1^{\nu_1 - 1} a_2 + \nu_2 a_1^{\nu_1} a_2' a_2^{\nu_2 - 1}$ immediately implying the formula. The general case works in the same way. Alternatively it can be shown by induction on n. □

Keep the notation of the previous lemma and set

$$C = \{a \in F \mid a' = 0\}.$$

The lemma immediately implies that this is a subfield of F. It is called the *field of constants* of F.

Let E, F be differential fields with $F \subset E$. Then we say that E is a *differential field extension* of F if E/F is a field extension and the restriction of the derivation of E to F is equal to the derivation of F (so, denoting the derivations of F and E by $'$ and ∂ respectively, we have $\partial(a) = a'$ for all $a \in F$).

Let F be a differential field and E a differential field extension of F. Let $t \in E$. Then we say that t is the *logarithm* of $a \in F$ if $t' = \frac{a'}{a}$ and we say that t is the *exponential* of $a \in F$ if $t' = a't$. Furthermore, E is said to be an *elementary extension* of F if there is a tower of differential field extensions

$$F = F_1 \subset F_2 \subset \cdots \subset F_{m+1} = E \tag{5.7.1}$$

with $F_{i+1} = F_i(t_i)$ where $t_i \in F_{i+1}$ is algebraic over F_i or the logarithm of an element of F_i or the exponential of an element of F_i (note the similarity with Definition 5.6.15).

Let $F = \mathbb{C}(z)$ with derivation $' = \frac{\mathrm{d}}{\mathrm{d}z}$ (see Example 5.7.2). Let $\Omega \subset \mathbb{C}$ be open and connected. A function $f : \Omega \to \mathbb{C}$ is said to be *meromorphic* if its singularities in Ω are poles, and every singularity is isolated. If f and g are two meromorphic functions on Ω then the sum $f + g$, product fg and quotient

f/g are meromorphic again, the latter of course only if $g \neq 0$. Hence the set of meromorphic functions on Ω forms a field denoted $M(\Omega)$ (see [J$\ddot{9}$3], §4.2). If f is holomorphic on Ω then so is its derivative f'. Hence $M(\Omega)$ is a differential field. Moreover, the elements of $F = \mathbb{C}(z)$ are holomorphic on $\mathbb{C}$ so that $M(\Omega)$ is a differential extension of F.

An *elementary function* is a meromorphic function $\delta : \Omega \to \mathbb{C}$ where Ω is a connected open subset of $\mathbb{C}$, such that $F(\delta)$ is an elementary extension of F (note that $F(\delta)$ is a well-defined subfield of $M(\Omega)$).

Example 5.7.4 Here are some examples of elementary functions

$$e^{\sqrt{\frac{1}{z^2+1}}}, \ \log(z^3 - z - 1), \ \sin(z).$$

Here the first function is meromorphic on $\mathbb{C} \setminus \{\pm i\}$. For the last one note that $\sin(z) = \frac{e^{iz} - e^{-iz}}{2i}$.

Now we have some technical facts on differential extensions.

Lemma 5.7.5 *Let F be a differential field of characteristic 0 with derivation $'$. Let E be an extension of F of finite degree. Then there exists a unique derivation ∂ of E with $\partial(a) = a'$ for all $a \in F$.*

Proof. Let x be an indeterminate and consider the polynomial ring $F[x]$. Define two maps $D_0, D_1 : F[x] \to F[x]$ by

$$D_0(\sum_{i=0}^{m} a_i x^i) = \sum_{i=0}^{m} a_i' x^i$$
$$D_1(\sum_{i=0}^{m} a_i x^i) = \sum_{i=1}^{m} i a_i x^{i-1}.$$

First suppose that a derivation ∂ as in the lemma exists. Then for $f \in F[x]$ and $\alpha \in E$ we have $\partial(f(\alpha)) = D_0(f)(\alpha) + D_1(f)(\alpha)\partial(\alpha)$. Now let f be the minimal polynomial of α, then $D_1(f)(\alpha) \neq 0$ (as $D_1(f)$ has smaller degree) and hence

$$\partial(\alpha) = -\frac{D_0(f)(\alpha)}{D_1(f)(\alpha)}.$$

We see that ∂ is uniquely determined.

Now we prove the existence of ∂. By the theorem of the primitive element (Theorem 5.2.7) we have $E = F(\alpha)$ for a certain $\alpha \in E$. Let $g \in F[x]$ and define $D_g : F[x] \to F[x]$ by $D_g(f) = D_0(f) + gD_1(f)$. Then for $f_1, f_2 \in F[x]$ we have

$$D_g(f_1 + f_2) = D_g(f_1) + D_g(f_2), \ D_g(f_1 f_2) = D_g(f_1)f_2 + f_1 D_g(f_2),$$

because these relations hold with D_0 and D_1 in place of D_g. Now let $f \in F[x]$ be the minimal polynomial of α and set $\beta = -\frac{D_0(f)(\alpha)}{D_1(f)(\alpha)}$. Because $E = F(\alpha)$ there is a $g_0 \in F[x]$ with $g_0(\alpha) = \beta$. But then $D_{g_0}(f)(\alpha) = 0$.

Let $\gamma \in E$ then $\gamma = h(\alpha)$ for a certain $h \in F[x]$. Then we set $\partial(\gamma) = D_{g_0}(h)(\alpha)$. We need to check that this is independent of the choice of h. So let $\hat{h} \in F[x]$ be a second polynomial with $\hat{h}(\alpha) = \gamma$. Then $(h - \hat{h})(\alpha) = 0$ so that f divides $h - \hat{h}$ (Proposition 4.3.4), or $h = \hat{h} + qf$ for some $q \in F[x]$. But then $D_{g_0}(h) = D_{g_0}(\hat{h}) + D_{g_0}(q)f + qD_{g_0}(f)$ and it follows that $D_{g_0}(h)(\alpha) = D_{g_0}(\hat{h})(\alpha)$. So ∂ is well-defined. The relations satisfied by D_{g_0} show that ∂ is a derivation of E. It obviously satisfies the required property. □

Lemma 5.7.6 *Let F be a differential field and E a differential extension of F of finite degree. Denote the derivation of both fields by $'$. Let $\sigma \in \mathrm{Gal}(E/F)$. Then $\sigma(\alpha') = \sigma(\alpha)'$ for all $\alpha \in E$.*

Proof. Fix $\sigma \in \mathrm{Gal}(E/F)$. Define $\partial : E \to E$ by $\partial(\alpha) = \sigma^{-1}(\sigma(\alpha)')$. It is straightforward to check that ∂ is a derivation of E. For $a \in F$ we have $\partial(a) = a'$, so that by the uniqueness part of Lemma 5.7.5 it follows that $\partial = '$. Hence $\alpha' = \sigma^{-1}(\sigma(\alpha)')$ for all $\alpha \in E$. By applying σ to both sides we get the result. □

Proposition 5.7.7 *Let E be a differential extension of the differential field F, and let the derivation of both fields be denoted $'$. We suppose that the field of constants of E is equal to the field of constants of F. Let $\alpha \in E$ be* transcendental *over F.*

(i) *Suppose that $\alpha' \in F$. Let $f = a_n x^n + \cdots + a_0 \in F[x]$ be a polynomial of degree $n > 0$. There is a $g \in F[x]$ with $f(\alpha)' = g(\alpha)$. Moreover $\deg(g) = n$ if a_n is not a constant and $\deg(g) = n - 1$ if a_n is a constant.*

(ii) *Suppose that $\frac{\alpha'}{\alpha} \in F$. Let $f \in F[x]$ be of degree > 0. Then there is a $g \in F[x]$ with $\deg(g) = \deg(f)$ and $f(\alpha)' = g(\alpha)$. Moreover, $g = \mu f$ for a certain $\mu \in F$ if and only if $f = a_n x^n$, $a_n \in F$.*

Proof. We start with (i). Using Lemma 5.7.3 we see that $f(\alpha)' = a_n'\alpha^n + (na_n\alpha' + a_{n-1}')\alpha^{n-1} + \cdots$. Hence g exists. If $a_n' \neq 0$ (that is, a_n is not a constant) then $\deg(g) = n$. Suppose that $a_n' = 0$. If $na_n\alpha' + a_{n-1}' = 0$ as well then $(na_n\alpha + a_{n-1})' = 0$ and by the hypothesis on the fields of constants it follows that $na_n\alpha + a_{n-1} \in F$. But that implies $\alpha \in F$ contrary to the hypothesis that α is transcendental over F. Hence $na_n\alpha' + a_{n-1}' \neq 0$ and we have $\deg(g) = n - 1$.

For (ii) write $\frac{\alpha'}{\alpha} = \gamma \in F$. Then for $a \in F$, $a \neq 0$ we have

$$(a\alpha^n)' = (a' + na\gamma)\alpha^n.$$

If $a' + na\gamma = 0$ then $(a\alpha^n)' = 0$ and $a\alpha^n \in F$ contrary to the hypothesis on α. Hence $(a\alpha^n)' = b\alpha^n$ for a certain $b \in F$. Hence g exists. It is also obvious that if $f = a_n x^n$ then $g = \mu f$. Conversely, suppose that $g = \mu f$ and that f has more than one monomial. Then we can write $f = a_k x^k + a_l x^l + \cdots$ where $a_k, a_l \neq 0$. Also from the above it follows that $g = (a_k' + ka_k\gamma)x^k + (a_l' + la_l\gamma)x^l + \cdots$. So $a_k' + ka_k\gamma = \mu a_k$ and $a_l' + la_l\gamma = \mu a_l$, so that $\frac{a_k'}{a_k} + k\frac{\alpha'}{\alpha} = \frac{a_l'}{a_l} + l\frac{\alpha'}{\alpha}$. A small computation shows that this is entails

$$\left(\frac{a_k\alpha^k}{a_l\alpha^l}\right)' = 0.$$

But that implies that the term in brackets lies in F, contrary to the hypothesis on γ. We conclude that $f = a_n x^n$. □

Now we have a short intermezzo on partial fraction decompositions of rational functions. We start with a lemma treating a special case, followed by the main theorem.

Lemma 5.7.8 *Let F be a field and $f, p \in F[x]$ with $\deg(p) > 0$ and $\deg(f) < s\deg(p)$ for some $s > 0$. Then there are unique $a_i \in F[x]$ with $\deg(a_i) < \deg(p)$ and $\frac{f}{p^s} = \frac{a_1}{p} + \frac{a_2}{p^2} + \cdots + \frac{a_s}{p^s}$.*

Proof. The existence of the a_i follows from the division with remainder theorem (Proposition 2.3.8). Indeed, define $q_0 = f$, and for $i \geq 1$, supposing that $q_0, \ldots, q_{i-1}$ have been defined, let q_i, a_{s+1-i} be the unique elements of $F[x]$ with $q_{i-1} = q_i p + a_{s+1-i}$ and $\deg(a_{s+1-i}) < \deg(p)$. The sequence stops when $i = m$ with $q_m = 0$. Then for $j \geq 1$ we have

$$f = q_j p^j + \sum_{k=0}^{j-1} a_{s-k} p^k.$$

Let $0 \leq t < s$ be such that $t\deg(p) \leq \deg(f) < (t+1)\deg(p)$. Then $q_{t+1} = 0$ and $f = a_s + a_{s-1}p + \cdots + a_{s-t}p^t$. Dividing by p^s we see that the a_i exist.

Secondly, if we have a_i as in the lemma, then it is clear that a_{s+1-i} is the remainder of q_{i-1} upon division by p. Therefore it is uniquely determined. □

Theorem 5.7.9 *Let $f, g \in F[x]$ with $\deg(g) > 0$. Write $g = p_1^{n_1} \cdots p_r^{n_r}$, where the p_i are irreducible and distinct. Then there are unique $h, a_{i,j} \in F[x]$ with $\deg(a_{i,j}) < \deg(p_i)$ and*

$$\frac{f}{g} = h + \sum_{i=1}^{r} \sum_{j=1}^{n_i} \frac{a_{i,j}}{p_i^j}.$$

Proof. Let $g_1, g_2 \in F[x]$ be such that $\gcd(g_1, g_2) = 1$. Then there are $a, b \in F[x]$ with $ag_1 + bg_2 = 1$ (Theorem 2.3.11). Hence $\frac{f}{g_1 g_2} = \frac{fb}{g_1} + \frac{fa}{g_2}$. Applying this repeatedly we see that there are $f_i \in F[x]$ with $\frac{f}{g} = \frac{f_1}{p_1^{n_1}} + \cdots + \frac{f_r}{p_r^{n_r}}$. Write $f_i = h_i p_i^{n_i} + v_i$, where $h_i, v_i \in F[x]$ and $\deg(v_i) < n_i \deg(p_i)$. Setting $h = h_1 + \cdots + h_r$ and applying the previous lemma to the quotients $\frac{v_i}{p_i^{n_i}}$ we see that the polynomials of the theorem exist.

Now we come to the uniqueness part. Note that $g\frac{a_{i,j}}{p_i^j}$ is a polynomial of degree $< \deg(g)$. So multiplying by g we see that h is a quotient of f upon division by g. Hence h is uniquely determined. By taking all terms with denominator equal to a power of p_i together and putting them in a single fraction we get $b_i \in F[x]$ with $\deg(b_i) < \deg(p_i)$ and

$$\frac{f}{g} - h = \sum_{i=1}^{r} \frac{b_i}{p_i^{n_i}}.$$

We first show that these b_i are uniquely determined. Suppose that

$$\sum_{i=1}^{r} \frac{b_i}{p_i^{n_i}} = \sum_{i=1}^{r} \frac{c_i}{p_i^{n_i}}.$$

Fix j with $1 \leq j \leq r$ and set $q = \frac{g}{p_j^{n_j}}$. Then

$$\sum_{i=1}^{r} \frac{b_i}{p_i^{n_i}} = \frac{b_j}{p_j^{n_j}} + \sum_{i \neq j} \frac{b_i}{p_i^{n_i}} = \frac{b_j}{p_j^{n_j}} + \frac{u}{q}$$

for some $u \in F[x]$. Similarly, $\sum_{i=1}^{r} \frac{c_i}{p_i^{n_i}} = \frac{c_j}{p_j^{n_j}} + \frac{v}{q}$ for some $v \in F[x]$. Then $(b_j - c_j)q = (v - u)p_j^{n_j}$. But since $\gcd(p_j^{n_j}, q) = 1$ this implies that $p_j^{n_j}$ divides $b_j - c_j$ which, because of the degrees, implies that $b_j - c_j = 0$.

It follows that the b_i are uniquely determined. We now get the uniqueness of the $a_{i,j}$ by applying the previous lemma to the quotient $\frac{b_i}{p_i^{n_i}}$. □

Theorem 5.7.10 *Let F be a differential field with derivation $'$. Let $a \in F$ and suppose that there exists an elementary extension E of F, with the same field of constants, and such that there exists a $y \in E$ with $y' = a$. Then there are $c_1, \ldots, c_n$, $u_1, \ldots, u_n, v$ in F, where $c_1, \ldots, c_n$ are constants and such that*

$$a = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + v'.$$

Proof. By definition there exists a tower of differential extensions $F = F_1 \subset \cdots \subset F_{m+1} = E$ as in (5.7.1). We use induction on $m \geq 0$. If $m = 0$ then $E = F$ and we can take $c_i = 0$, $u_i = 1$, $v = y$. Now suppose $m \geq 1$ and and that the theorem holds when the tower consists of m fields. Applying the induction hypothesis to the tower $F_2 \subset \cdots \subset F_{m+1} = E$ we see that there are $c_1, \ldots, c_n$, $u_1, \ldots, u_n, v \in F_2$ such that $a = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + v'$. Moreover $F_2 = F(\alpha)$ where α is algebraic over F or it is the logarithm or the exponential of an element of F. Accordingly we distinguish three cases.

Case I: α is algebraic over F. Then there exist $f_1, \ldots, f_n, g \in F[x]$ with $u_i = f_i(\alpha)$, $v = g(\alpha)$. (Note that $c_i \in F$ because they are constants.) Let $K \supset F_2$ be the splitting field of the minimal polynomial of α. By Lemma 5.7.5 there exists a unique derivation (which we also denote $'$) of K

extending the derivation of F. Write $G = \mathrm{Gal}(K/F)$ and let $\beta_1, \ldots, \beta_s$ be the distinct elements of $\{\sigma(\alpha) \mid \sigma \in G\}$. Fix a β_j and let $\sigma \in G$ be such that $\sigma(\alpha) = \beta_j$. Using Lemma 5.7.6 we see that $\sigma(f_i(\alpha)') = \sigma(f_i(\alpha))' = f_i(\beta_j)'$. So because $\sigma(a) = a$ we get

$$a = \sum_{i=1}^{n} c_i \frac{f_i(\beta_j)'}{f_i(\beta_j)} + g(\beta_j)'.$$

Applying $\frac{1}{s}\sum_{j=1}^{s}$ to both sides and using Lemma 5.7.3(v) we obtain

$$\alpha = \sum_{i=1}^{n} \frac{c_i}{s} \frac{(f_i(\beta_1)\cdots f_i(\beta_s))'}{f_i(\beta_1)\cdots f_i(\beta_s)} + \left(\frac{g(\beta_1) + \cdots + g(\beta_s)}{s}\right)'.$$

As $f_i(\beta_1)\cdots f_i(\beta_s)$ and $g(\beta_1)+\cdots+g(\beta_s)$ are fixed by all elements of G they lie in F. Hence we have found an expression of the required form.

Now we have a small intermezzo concerning some generalities on the case where α is transcendental over F. In that case for each $w \in F(\alpha)$ there are $f, g \in F[x]$ with $\gcd(f, g) = 1$ and $w = \frac{f(\alpha)}{g(\alpha)}$. A small calculation shows that $\frac{w'}{w} = \frac{f(\alpha)'}{f(\alpha)} - \frac{g(\alpha)'}{g(\alpha)}$. So we may assume that there exist polynomials $f_i \in F[x]$ such that $u_i = f_i(\alpha)$. Furthermore, because of Lemma 5.7.3(v) we may assume that the f_i are irreducible and monic. By the partial fractions theorem (Theorem 5.7.9) there are $h, p_j, q_j \in F[x]$ with q_j monic and irreducible, $\deg(p_j) < \deg(q_j)$ and

$$v = h(\alpha) + \sum_{j=1}^{t} \frac{p_j(\alpha)}{q_j^{r_j}(\alpha)}.$$

We say that this is the partial fractions expansion of v.

Case II: α is transcendental and the logarithm of $b \in F$. The latter means that $\alpha' = \frac{b'}{b}$. In particular $\alpha' \in F$. So by Proposition 5.7.7(i) we have that there is a $k_i \in F[x]$ with $\deg(k_i) = \deg(f_i) - 1$ and $f_i(\alpha)' = k_i(\alpha)$. Hence $\frac{u_i'}{u_i} = \frac{k_i(\alpha)}{f_i(\alpha)}$. Moreover, the partial fractions expansion of $\frac{k_i}{f_i}$ is simply $\frac{k_i}{f_i}$. Now if $\frac{p_j(\alpha)}{q_j^{r_j}(\alpha)}$ appears in the partial fractions expansion of v, then the partial fractions expansion of v' contains a fraction with denominator $q_j^{r_j+1}(\alpha)$. But $r_j + 1 \geq 2$ so such a fraction can never cancel against a a $\frac{k_i(\alpha)}{f_i(\alpha)}$. Furthermore $\sum_i \frac{u_i'}{u_i} + v' \in F$. Hence the partial fractions expansion of v cannot have such terms, whence $v = h(\alpha)$. But then we cannot have $\deg(f_i) > 0$ as otherwise the fraction $\frac{k_i(\alpha)}{f_i(\alpha)}$ does not cancel. It follows that $u_i \in F$ for all i. But then also $v' \in F$ so that $v = d\alpha + e$ for certain $d, e \in F$. Hence $\alpha = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + d\frac{b'}{b} + e'$ is an expression of the required form.

Case III: α is transcendental and the exponential of $b \in F$. Then $\frac{\alpha'}{\alpha} = b'$. From Proposition 5.7.7(ii) we get that if $f \in F[x]$ is monic, irreducible, and $f \neq x$ then $f(\alpha)'$ is a polynomial in α of the same degree, and it is not a scalar multiple of $f(\alpha)$. Hence $\frac{u_i'}{u_i} = \frac{k_i(\alpha)}{f_i(\alpha)}$ where in this case $\deg(k_i) = \deg(f_i)$. So if $f_i \neq x$ then the partial fractions expansion of $\frac{k_i}{f_i}$ is of the form $m_i + \frac{l_i}{f_i}$ where $m_i \in F$ and $l_i \in F[x]$, $\deg(l_i) < \deg(f)$. On the other hand, if $f_i = x$ then $\frac{u_i'}{u_i} = b' \in F$. Again, if in the partial fractions decomposition of v we have a term $\frac{p_j(\alpha)}{q_j^{r_j}(\alpha)}$ with $q_j \neq x$, then in the partial fractions decomposition of v' we will have a term with denominator $q_j^{r_j+1}(\alpha)$, which cannot cancel against any of the $\frac{u_i'}{u_i}$. It follows that we can only have $q_j = x$ and therefore $v = \sum_{j\in\mathbb{Z}} a_j t^j$ where $a_j \in F$. But then we also must have $u_i \in F$ if $f_i \neq x$. In particular $\frac{u_i'}{u_i} \in F$ for all i so that $v' \in F$ as well. Note that $(a_j\alpha^j)' = b_j\alpha^j$ for a certain $b_j \in F$ which cannot be zero because α is transcendental. Therefore we must have $v \in F$. If every u_i lies in F then we are done. But if one u_i, say u_1, is equal to α then we have $\alpha = c_1\frac{\alpha'}{\alpha} + \sum_{i=2}^{n} c_i\frac{u_i'}{u_i} + v' = \sum_{i=2}^{n} c_i\frac{u_i'}{u_i} + (c_1 b + v)'$ and again we have the required expression. □

Theorem 5.7.11 (Liouville) *Let $f, g \in \mathbb{C}(z)$. Then $\int f e^g \,\mathrm{d}z$ is elementary if and only if there is an $a \in \mathbb{C}(z)$ with $f = a' + ag'$.*

Proof. Firstly, if such an a exists then $\int fe^g \,\mathrm{d}z = ae^g$.

For the other implication let $E = \mathbb{C}(z,t)$ where $t = e^g$. Suppose that $\int fe^g \,\mathrm{d}z$ is elementary. By definition that means that there exists an elementary extension of E containing an element y with $y' = ft$. By the previous theorem it follows that there are $c_1, \ldots, c_n \in \mathbb{C}$, $u_1, \ldots, u_n, v \in E$ with

$$tf = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + v'.$$

Set $F = \mathbb{C}(z)$. Then $E = F(t)$ and $t' = gt$. We now perform exactly the same analysis as in the third case of the proof of Theorem 5.7.10. Again we obtain that $v = \sum_{j\in\mathbb{Z}} b_j t^j$ and $u_i \in F$ or $u_i = t$ for precisely one i. Then $v' = \sum_{j\in\mathbb{Z}} (b_j' + jg'b_j)t^j$ and $\sum_{i=1}^{n} c_i \frac{u_i'}{u_i} \in F$. Hence

$$tf = (\sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + b_0') + \sum_{j\neq 0} (b_j' + jg'b_j)t^j.$$

It follows that the first term has to be zero, whereas each term in the second summation is zero except for $j = 1$. Hence $tf = (b_1' + g'b_1)t$ from which it follows $f = b_1' + b_1 g'$ and we see that we can take $a = b_1$. □

Corollary 5.7.12 *$\int e^{z^2} \,\mathrm{d}z$ is not elementary.*

Proof. We apply the previous theorem with $f = 1$, $g = z^2$. According to the theorem the integral is elementary if and only if there is an $a \in \mathbb{C}(z)$ with $1 = a' + 2az$. Write $a = \frac{p}{q}$ with $p, q \in \mathbb{C}[z]$ and $\gcd(p,q) = 1$. Then $a' + 2az = 1$ amounts to $p'q - q'p + 2zpq = q^2$. It follows that $q|q'p$, which because p, q are coprime, implies that $q|q'$ and hence $q = 1$. So $a = p$ is a polynomial. But then we cannot have $a' + 2az = 1$ because $\deg(2az) = \deg(a') + 2$. □

5.7.3 Galois descent

In this section we let E/F be a Galois extension of finite degree. Let V be a vector space over E. Then V is also a vector space over F. A $U \subset V$ is said to be an F-subspace if $u+v \in U$ for all $u, v \in U$ and $\alpha u \in U$ for all $\alpha \in F$, $u \in U$ (that is, if U is a subspace of V when the latter is considered as a vector space over F).

Example 5.7.13 Let $E = \mathbb{C}$, $F = \mathbb{R}$, $V = \mathbb{C}^2$, whose elements we write as row vectors. Let U_1 be the $\mathbb{R}$-subspace spanned by $(1,i)$, $(1,-i)$. Let U_2 be the $\mathbb{R}$-subspace spanned by $(1,1)$, (i,i). Both spaces (as vector spaces over $\mathbb{R}$) have dimension 2. For $i = 1, 2$ let $\mathbb{C}U_i$ denote the vector space over $\mathbb{C}$ spanned by the same vectors as U_i. Then we see that $\dim \mathbb{C}U_1 = 2$ whereas $\dim \mathbb{C}U_2 = 1$. We express this by saying that U_1 is an $\mathbb{R}$-form of V, whereas U_2 is not.

Definition 5.7.14 *The F-subspace U of V is called an* F-form *of V if there is a basis of U that is also a basis of V.*

By the next lemma, if there is a basis of U that is not a basis of V then U is not an F-form of V.

Lemma 5.7.15 *Let V be a vector space over E and U an F-form of V. Then every basis of U is also a basis of V.*

Proof. Let $u_1, u_2, \ldots$ be a basis of U that is also a basis of V. Let $v_1, v_2, \ldots$ be a second basis of U. Let $v \in V$ then v is a linear combination (with coefficients in E) of some of the u_i. Writing these as linear combinations of the v_j we see that v is a linear combination of the v_j.

Consider $v_1, \ldots, v_m$ for some $m \geq 1$. There is an n such that each v_i lies in the space (over F) spanned by $u_1, \ldots, u_n$. Write $v_i = \sum_{j=1}^{n} c_{ij} u_j$ with $c_{ij} \in F$. Set $c_i = (c_{i1}, \ldots, c_{in})$. Then the vectors

c_i are linearly independent over F. By elementary linear algebra that implies that they are linearly independent over E. But that means that $v_1, \ldots, v_m$ is linearly indepedent over E. It follows that $v_1, v_2, \ldots$ is a basis of V. □

Constructing F-forms of V is called *descent*. The main question is which F-forms a given V can have. Of course, this depends very strongly on the given data (E, F, V). This question is most interesting if the vector spaces have an extra structure, for example that of an algebra. But for the moment we will just focus on vector spaces.

Let V be a vector space over E and let U be an F-form of V. Let $u_1, u_2, \ldots$ be a basis of U over F. Then by Lemma 5.7.15 this is a basis of V as well. Write $G = \mathrm{Gal}(E/F)$. Then for $\sigma \in G$ we define a map $T_\sigma : V \to V$ by $T_\sigma(\sum_i \alpha_i u_i) = \sum_i \sigma(\alpha_i) u_i$ (where, if the set of u_i is infinite, all but a finite number of the α_i are zero). This map does not depend on the choice of the basis. Indeed, let $v_1, v_2, \ldots$ be a second basis of U over F and let T'_σ be the corresponding map. There are $\delta_{ij} \in F$ with $u_i = \sum_j \delta_{ij} v_j$. Hence

$$T'_\sigma(\sum_i \alpha_i u_i) = T'_\sigma(\sum_j (\sum_i \alpha_i \delta_{ij}) v_j) = \sum_j \sum_i \sigma(\alpha_i \delta_{ij}) v_j = \sum_j \sum_i \sigma(\alpha_i) \delta_{ij} v_j = \sum_i \sigma(\alpha_i) u_i = T_\sigma(\sum_i \alpha_i u_i).$$

The maps T_σ have the following properties:

$$\begin{aligned} T_\sigma(u+v) &= T_\sigma(u) + T_\sigma(v) \text{ for } \sigma \in G, u, v \in V \\ T_\sigma(\alpha u) &= \sigma(\alpha) T_\sigma(u) \text{ for } \sigma \in G, u \in V, \alpha \in E \\ T_\sigma \circ T_\tau &= T_{\sigma\tau} \text{ for } \sigma, \tau \in G \\ T_1 &= I_V. \end{aligned} \tag{5.7.2}$$

(Here I_V denotes the identity map on V.) Moreover, we obviously have $U = \{u \in V \mid T_\sigma(u) = u \text{ for all } \sigma \in G\}$. Hence we have the following lemma.

Lemma 5.7.16 *Let V be a vector space over E and let U be an F-form of V. Then there is a set of maps $\{T_\sigma : V \to V \mid \sigma \in G\}$ with (5.7.2) such that $U = \{u \in V \mid T_\sigma(u) = u \text{ for all } \sigma \in G\}$.*

We also have the converse of this. In order to prove it we need a lemma on Galois extensions that is of independent interest.

Lemma 5.7.17 *Let E/F be a Galois extension of finite degree n. Write $\mathrm{Gal}(E/F) = \{\sigma_1, \ldots, \sigma_n\}$ and let $\alpha_1, \ldots, \alpha_n \in E$ be a basis of E over F. Then the matrix $(\sigma_i(\alpha_j))_{1 \le i,j \le n}$ is invertible.*

Proof. Consider the system of linear equations

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_n)x_n = 0 \\ \sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \cdots + \sigma_2(\alpha_n)x_n = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_n)x_n = 0 \end{cases}$$

The given matrix is invertible if and only if this system only has the trivial solution. So suppose that there are nontrivial solutions, and let $(\lambda_1, \ldots, \lambda_n)$ be such a solution with the minimal number of nonzero coordinates. We may assume that $\lambda_1, \ldots, \lambda_r \neq 0$, $\lambda_{r+1}, \ldots, \lambda_n = 0$. After dividing we may assume that $\lambda_1 = 1$. Not all λ_i are in F as otherwise the α_i are linearly dependent over F (note that there is a j such that σ_j is the identity). So we may assume that $\lambda_2 \notin F$. As E/F is Galois there is a σ_j with $\sigma_j(\lambda_2) \neq \lambda_2$. We have the equations

$$\sigma_i(\alpha_1) + \sigma_i(\alpha_2)\lambda_2 + \cdots + \sigma_i(\alpha_r)\lambda_r = 0 \text{ for } 1 \le i \le n. \tag{5.7.3}$$

To thse equations we apply σ_j and use the fact that $\sigma_j \sigma_i = \sigma_k$ and σ_k runs over $\mathrm{Gal}(E/F)$ if σ_i does so. Therefore we also have

$$\sigma_k(\alpha_1) + \sigma_k(\alpha_2)\sigma_j(\lambda_2) + \cdots + \sigma_k(\alpha_r)\sigma_j(\lambda_r) = 0 \text{ for } 1 \le k \le n. \tag{5.7.4}$$

Now we subtract (5.7.4) for $k = i$ from (5.7.3) and we see that we get a nontrivial solution with fewer nonzero coordinates. This is a contradiction and the lemma is proved. □

Lemma 5.7.18 *Let V be a vector space over E. Let $\{T_\sigma \mid \sigma \in G\}$ be a set of maps $T_\sigma : V \to V$ satisfying* (5.7.2)*. Set $U = \{u \in V \mid T_\sigma(u) = u \text{ for all } \sigma \in G\}$. Then U is an F-form of V.*

Proof. It is immediate that U is an F-subspace of V.

Let $v \in V$. Then for $\alpha \in E$ we set $v_\alpha = \sum_{\sigma\in G} \sigma(\alpha)T_\sigma(v)$. Then $v_\alpha \in U$ because for $\tau \in G$ we have $T_\tau(v_\alpha) = \sum_{\sigma\in G} \tau\sigma(\alpha)T_{\tau\sigma}(v)$, which is equal to v_α. Let $\alpha_1, \ldots, \alpha_n \in E$ be a basis of E over F. Write $G = \{\sigma_1, \ldots, \sigma_n\}$. By Lemma 5.7.17 the matrix $A = (\sigma_j(\alpha_i))_{1\le i,j\le n}$ is invertible. Furthermore we have $v_{\alpha_i} = \sum_{j=1}^n \sigma_j(\alpha_i)T_{\sigma_j}(v)$, so the inverse of the matrix A allows us to express the $T_{\sigma_i}(v)$ as E-linear combinations of the v_{α_i}. Since there is an i with $\sigma_i = 1$ we see in particular that v itself is an E-linear combination of the v_{α_i}. But the latter lie in U. Hence V is spanned by the elements of U.

Let $u_1, u_2, \ldots$ be a basis of U and suppose that it is linearly dependent over E. Let $v_1, \ldots, v_r$ be a E-linearly dependent subset of the u_i of smallest cardinality. (In other words, there are no sets of u_i of cardinality $< r$ that are E-linearly dependent.) By hypothesis there are $\lambda_i \in E$ such that $\lambda_1 v_1 + \cdots + \lambda_r v_r = 0$. By the minimality of r no λ_i can be zero, and after dividing we have $\lambda_1 = 1$. At least one λ_i does not lie in F; we may assume that $\lambda_2 \notin F$. Then there is a $\sigma \in G$ with $\sigma(\lambda_2) \neq \lambda_2$. After applying T_σ to the above relation we get

$$v_1 + \sigma(\lambda_2)v_2 + \sigma(\lambda_3)v_3 + \cdots + \sigma(\lambda_r)v_r = 0.$$

So after subtracting we get a nontrivial linear dependency $(\lambda_2 - \sigma(\lambda_2))v_2 + \cdots + (\lambda_r - \sigma(\lambda_r))v_r = 0$. But this involves fewer than r elements, and hence we have a contradiction. □

Theorem 5.7.19 *Let V be a vector space over E. There is a bijection between the set of F-forms of V and the set of sets of maps $\{T_\sigma : V \to V \mid \sigma \in G\}$ satisfying* (5.7.2)*.*

Proof. The maps between these sets are given by Lemma's 5.7.16, 5.7.18. Lemma 5.7.16 also says that if we start with an F-form U and consider the corresponding set of transformations $\{T_\sigma\}$, then the F-form corresponding to that set is precisely U. Secondly, let $\{T_\sigma\}$ be a set of transformations with (5.7.2) and let U be the corresponding F-form. Let $u_1, u_2, \ldots$ be a basis of U. Then the transformations corresponding to U are defined by $T'_\sigma(\sum_i \alpha_i u_i) = \sum_i \sigma(\alpha_i)u_i$. But then obviously $T'_\sigma = T_\sigma$. □

As an application we sketch the a theorem from algebraic geometry. Let $R = E[x_1, \ldots, x_n]$, $V = E^n$. Then for a subset $A \subset R$ we consider the set of the common zeros

$$\mathcal{V}(A) = \{v \in V \mid f(v) = 0 \text{ for all } f \in A\}.$$

This is called an *affine variety*. It is clear that $\mathcal{V}(A) = \mathcal{V}(I)$, where I is the ideal of R generated by A. Secondly, given a set $X \subset V$ we define its *vanishing ideal*

$$\mathcal{I}(X) = \{f \in R \mid f(v) = 0 \text{ for all } v \in X\}.$$

An affine variety $X = \mathcal{V}(A)$ is said to be *defined over F* if $\mathcal{I}(X)$ is generated (as ideal) by polynomials in $F[x_1, \ldots, x_n]$. Note that G acts on V by $\sigma \cdot (v_1, \ldots, v_n) = (\sigma(v_1), \ldots, \sigma(v_n))$.

Theorem 5.7.20 *$X = \mathcal{V}(A)$ is defined over F if and only if $\sigma(X) \subset X$ for all $\sigma \in G$.*

Proof. Suppose that X is defined over F. Set $I = \mathcal{I}(X)$; then also $X = \mathcal{V}(I)$. Let $f \in F[x_1, \ldots, x_n]$ be a generator of I. Because f has coefficients in F we see that for $\sigma \in G$ and $v \in V$ we have $f(\sigma \cdot v) = \sigma(f(v))$. Hence if $v \in X$ we get $f(\sigma(v)) = \sigma(f(v)) = \sigma(0) = 0$. Because this holds for all $f \in I$ we obtain $\sigma(v) \in X$.

Now suppose that $\sigma(X) \subset X$ for all $\sigma \in G$. As $\sigma \in G$ is invertible this implies that $\sigma(X) = X$ for all $\sigma \in G$. For $\sigma \in G$ and $f \in R$ we let $T_\sigma(f)$ be the polynomial obtained from f by letting σ act

on the coefficients of f. Then the maps $\{T_\sigma\}$ satisfy (5.7.2). Furthermore, for $v \in V$ and $f \in R$ we have $\sigma(f(v)) = T_\sigma(f)(\sigma \cdot v)$. Let $v \in X$ and $\sigma \in G$ and let $w \in X$ be such that $w = \sigma(v)$. Then for $f \in I$ we have $0 = \sigma(f(v)) = T_\sigma(f)(w)$. So since w runs through all of X if v does so, we see that $T_\sigma(f) \in I$. Because the T_σ are invertible we get that $T_\sigma(I) = I$ for all $\sigma \in G$. Hence by Theorem 5.7.19, $\{f \in I \mid T_\sigma(f) = f \text{ for } \sigma \in G\}$ is an F-form of I. On the other hand it is clear that this is $I \cap F[x_1, \ldots, x_n]$. In particular it follows that $I \cap F[x_1, \ldots, x_n]$ generates I, and therefore X is defined over F. □

Now we have a look at F-forms of algebras. An *algebra* over a field K is a vector space A over K together with a bilinear map $m : A \times A \to A$. The map m is called the multiplication and often we write $a \cdot b$ (or simply ab) instead of $m(a, b)$. The algebra A is called *associative* if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in A$. One of the main examples of associative algebras are the matrix algebras $M_n(K)$ consisting of the $n \times n$-matrices with coefficients in K. Here the product is the ordinary matrix product.

Let A be an algebra over E. An F-form of A is an F-form of the vector space A that is closed under taking products.

Example 5.7.21 Consider the algebra $M_2(\mathbb{C})$. Then $M_2(\mathbb{R})$ is a $\mathbb{R}$-form of it. Let $\mathcal{H}$ be the $\mathbb{R}$-span of the following matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

It is straightforward to show that $\mathcal{H}$ is closed under taking products (it is enough to check that the product of two basis elements again lies in $\mathcal{H}$). Moreover, the given matrices obviously form a basis of $M_2(\mathbb{C})$. So $\mathcal{H}$ is another $\mathbb{R}$-form of $M_2(\mathbb{C})$. We have that $\mathcal{H}$ is the algebra of *quaternions*. It is not isomorphic to $M_2(\mathbb{R})$ (that is, there is no bijective linear map $\psi : M_2(\mathbb{R}) \to \mathcal{H}$ with $\psi(XY) = \psi(X)\psi(Y)$ for all $X, Y \in M_2(\mathbb{R})$). This can be proved by showing that every nonzero element in $\mathcal{H}$ has a multiplicative inverse, whereas $M_2(\mathbb{R})$ obviously does not have that property.

Let $U \subset A$ be an F-form of A. Let $u_1, u_2, \ldots$ be a basis of U, then there are $\gamma_{ij}^k \in F$ with $u_i \cdot u_j = \sum_k \gamma_{ij}^k u_k$ (where, as always, only a finite number of the γ_{ij}^k are non-zero). For $\sigma \in G$ define, as before, $T_\sigma : A \to A$ by $T_\sigma(\sum_i c_i u_i) = \sum_i \sigma(c_i) u_i$. Let $a = \sum_i \alpha_i u_i$, $b = \sum_j \beta_j u_j$ be two elements of A (so $\alpha_i, \beta_j \in E$); then $a \cdot b = \sum_k \left(\sum_{i,j} \alpha_i \beta_j \gamma_{ij}^k \right) u_k$ and therefore

$$T_\sigma(a \cdot b) = \sum_k \left(\sum_{i,j} \sigma(\alpha_i)\sigma(\beta_j)\gamma_{ij}^k \right) u_k = \left(\sum_i \sigma(\alpha_i) u_i \right) \cdot \left(\sum_j \sigma(\beta_j) u_j \right) = T_\sigma(a) \cdot T_\sigma(b).$$

So the T_σ corresponding to U are multiplicative, that is, they satisfy $T_\sigma(a \cdot b) = T_\sigma(a) \cdot T_\sigma(b)$ for all $a, b \in A$.

Conversely, let $\{T_\sigma\}$ be a set of multiplicative maps $A \to A$ with (5.7.2). Let $U = \{a \in A \mid T_\sigma(a) = a \text{ for all } \sigma \in G\}$ (i.e., U is the vector space F-form of A corresponding to $\{T_\sigma\}$). From the multiplicativity of the T_σ it now immediately follows that U is closed under taking products, and therefore is an F-form of A. We conclude that the F-forms of A correspond bijectively to the sets of multiplicative maps $\{T_\sigma\}$ satisfying (5.7.2).

Now let U, V be two F-forms of A corresponding to the maps $\{T_\sigma\}$, $\{S_\sigma\}$ respectively. Let $\psi : U \to V$ be an isomorphism; that is ψ is a bijective F-linear map respecting the multiplication. Extend ψ to a map $\psi : A \to A$ by $\psi(\sum_i \gamma_i u_i) = \sum_i \gamma_i \psi(u_i)$, where $\gamma_i \in E$. Set $S'_\sigma = \psi T_\sigma \psi^{-1}$. Then the S'_σ satisfy (5.7.2) and are multiplicative. Hence $V' = \{a \in A \mid S'_\sigma(a) = a \text{ for all } \sigma \in G\}$ is an F-form of A. But $S'_\sigma(a) = a$ (for all σ) is equivalent to $T_\sigma(\psi^{-1}(a)) = \psi^{-1}(a)$ (for all σ), which is equivalent to $\psi^{-1}(a) \in U$, which in turn is equivalent to $a \in V$. We see that $V' = V$ and therefore $S'_\sigma = S_\sigma$ by Theorem 5.7.19. Conversely, if ψ is an automorphism of A with $S_\sigma = \psi T_\sigma \psi^{-1}$ for all $\sigma \in G$ then it is immediate that ψ maps U onto V and therefore restricts to an isomorphism $\psi : U \to V$. The conclusion is that the F-forms U, V are isomorphic if and only if there is an automorphism ψ of A such that $S_\sigma = \psi T_\sigma \psi^{-1}$ for all $\sigma \in G$.

5.7.4 Galois cohomology

Galois cohomology offers another perspective on classification problems like the one considered at the end of the previous section. There it is shown that classfying all F-forms of a given algebra A over E up to isomorphism is equivalent to classifying, up to conjugacy by the group $\mathrm{Aut}(A)$, all sets of maps $\{T_\sigma \mid \sigma \in G\}$ that are multiplicative and satisfy (5.7.2). However, dealing with these maps is not so easy because they are not linear, indeed, we have $T_\sigma(\alpha a) = \sigma(\alpha)T_\sigma(a)$ for $\sigma \in G$, $\alpha \in E$, $a \in A$. Galois cohomology provides a way of dealing with sets like the ones above, with the difference that the elements are automorphisms.

Example 5.7.22 Consider the set up of Example 5.7.21. Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and write $G = \{1, \gamma\}$, where γ denotes complex conjugation, $\gamma(z) = \bar{z}$ for $z \in \mathbb{C}$. Let $\Gamma : M_2(\mathbb{C}) \to M_2(\mathbb{C})$ be the map defined by

$$\Gamma \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}.$$

Then G acts on $\mathrm{Aut}(M_2(\mathbb{C}))$ by $\gamma \cdot \psi = \Gamma\psi\Gamma$ (indeed, we have $\gamma \cdot (\gamma \cdot \psi) = \Gamma\Gamma\psi\Gamma\Gamma = \psi$). Let $\{T_1, T_\gamma\}$ be a set of multiplicative maps with (5.7.2) and define $\alpha : G \to \mathrm{Aut}(M_2(\mathbb{C}))$ by $\alpha(1) = \mathrm{Id}$, $\alpha(\gamma) = T_\gamma\Gamma$. Then it is straightforward to see that

$$\alpha(\sigma\tau) = \alpha(\sigma)(\sigma \cdot \alpha(\tau)) \text{ for all } \sigma, \tau \in G. \tag{5.7.5}$$

Conversely, let $\alpha : G \to \mathrm{Aut}(M_2(\mathbb{C}))$ satisfy (5.7.5). Then $\alpha(1) = \alpha(1 \cdot 1) = \alpha(1)1 \cdot \alpha(1) = \alpha(1)^2$, implying that $\alpha(1) = \mathrm{Id}$. Secondly, from $\alpha(\gamma\gamma) = \alpha(\gamma)\gamma \cdot \alpha(\gamma)$ it follows that $(\alpha(\sigma)\Gamma)^2 = \mathrm{Id}$. Therefore putting $T_1 = \mathrm{Id}$, $T_\gamma = \alpha(\gamma)\Gamma$ we obtain a set of multiplicative maps $\{T_\sigma : M_2(\mathbb{C}) \to M_2(\mathbb{C}) \mid \sigma \in G\}$ with (5.7.2).

Furthermore, if $\alpha' : G \to \mathrm{Aut}(M_2(\mathbb{C}))$ is the map corresponding to the set $\{\psi T_1\psi^{-1}, \psi T_\gamma\psi^{-1}\}$ (where $\psi \in \mathrm{Aut}(M_2(\mathbb{C}))$) then

$$\alpha'(\sigma) = \psi\alpha(\sigma)(\sigma \cdot \psi^{-1}) \text{ for all } \sigma \in G. \tag{5.7.6}$$

Conversely, let $\alpha, \alpha' : G \to \mathrm{Aut}(M_2(\mathbb{C}))$ be two maps with (5.7.5) and suppose that the relation (5.7.6) holds. Set $T_1 = T_1' = \mathrm{Id}$ and $T_\gamma = \alpha(\gamma)\Gamma$, $T_\gamma' = \alpha'(\gamma)\Gamma$. Then $T_\sigma' = \psi T_\sigma \psi^{-1}$ for all $\sigma \in G$.

We conclude that the $\mathbb{R}$-forms of $M_2(\mathbb{C})$ correspond to maps $\alpha : G \to \mathrm{Aut}(M_2(\mathbb{C}))$ with (5.7.5). Furthermore, two $\mathbb{R}$-forms, corresponding to the maps α, α', are isomorphic if and only if the relation (5.7.6) holds.

Now we take a step back and consider a more general situation. Let G be a finite group. Let A be a group on which G acts by homomorphisms. That means that we have a map $G \times A \to A$, $(\sigma, a) \mapsto \sigma \cdot a$ as in Section 3.5, and for each $\sigma \in G$ the map $A \to A$, $a \mapsto \sigma \cdot a$ is a group homomorphsim (i.e., $\sigma \cdot (ab) = (\sigma \cdot a)(\sigma \cdot b)$ for all $a, b \in A$). Then a 1-*cocyle* with values in A is a map $\alpha : G \to A$ with

$$\alpha(\sigma\tau) = \alpha(\sigma)(\sigma \cdot \alpha(\tau)) \text{ for all } \sigma, \tau \in G. \tag{5.7.7}$$

By $Z^1(G, A)$ we denote the set of all 1-cocycles with values in A.
We remark the following:

- If α is a 1-cocycle then $\alpha(1) = \alpha(1 \cdot 1) = \alpha(1)(1 \cdot \alpha(1)) = \alpha(1)^2$ implying $\alpha(1) = 1$ (where the second 1 denotes the neutral element of A).

- The map $\alpha : G \to A$ with $\alpha(\sigma) = 1$ for all $\sigma \in G$ is a 1-cocycle, called the *trvial cocycle*. In the sequel we denote it by 1.

- Let $\alpha \in Z^1(G, A)$ and $a \in A$. Define $\alpha^a : G \to A$ by $\alpha^a(\sigma) = a\alpha(\sigma)(\sigma \cdot a^{-1})$ (compare (5.7.6)). Then a short calculation shows that α^a is a 1-cocycle as well.

Two 1-cocycles $\alpha, \alpha' \in Z^1(G, A)$ are said to be *cohomologous* if there is an $a \in A$ with $\alpha' = \alpha^a$. In this situation we write $\alpha \sim \alpha'$. This is an equivalence relation. (Indeed: $\alpha = \alpha^1$. If $\alpha' = \alpha^a$ then $\alpha = (\alpha')^{a^{-1}}$. If $\alpha' = \alpha^a$, $\alpha'' = (\alpha')^b$, then $\alpha'' = \alpha^{ba}$.) The set of equivalence classes is denoted $H^1(G, A)$ and called the *first cohomology set of G with coefficients in A*.

One problem with these cohomolgy sets is that they are difficult to compute. A generalization of a famous theorem of Hilbert gives these sets for an important class of groups.

Theorem 5.7.23 (Hilbert 90) *Let E/F be a Galois extension of finite degree, $G = \mathrm{Gal}(E/F)$. Note that G acts naturally on the matrix group $\mathrm{GL}(n, E)$ (by letting a $\sigma \in G$ act on the coefficients of a matrix in $\mathrm{GL}(n, E)$). We have that $H^1(G, \mathrm{GL}(n, E)) = 1$ (where the latter denotes the set consisting of the class of the trivial coclycle only).*

Proof. Set $U = E^n$. Let $u \in U$ and write $u = (u_1, \ldots, u_n)$. Then for a $\sigma \in G$ we set $\sigma \cdot u = (\sigma(u_1), \ldots, \sigma(u_n))$. Let $\alpha \in Z^1(G, \mathrm{GL}(n, E))$ and for $\sigma \in G$ define the map $T^\alpha_\sigma : U \to U$ by $T^\alpha_\sigma(u) = \alpha(\sigma)(\sigma \cdot u)$. It is straightforward to see that the set $\{T^\alpha_\sigma \mid \sigma \in G\}$ satisfies (5.7.2). Hence

$$U^\alpha = \{u \in U \mid T^\alpha_\sigma(u) = u \text{ for all } \sigma \in G\}$$

is an F-form of U (Lemma 5.7.18). Let $v_1, \ldots, v_n$ be an F-basis of U^α. Let $P \in \mathrm{GL}(n, E)$ be the matrix with columns $v_1, \ldots, v_n$. For $\sigma \in G$ the matrix $\sigma \cdot P$ has columns $\sigma \cdot v_1, \ldots, \sigma \cdot v_n$. But $v_i \in U^\alpha$, so that for $\sigma \in G$ we have

$$v_i = T^\alpha_\sigma(v_i) = \alpha(\sigma)(\sigma \cdot v_i),$$

which implies that $P = \alpha(\sigma)(\sigma \cdot P)$ (a product of two elements in $\mathrm{GL}(n, E)$). But then

$$\alpha^{P^{-1}}(\sigma) = P^{-1}\alpha(\sigma)(\sigma \cdot P) = P^{-1}P = I_U.$$

We conclude that α is cohomologous to the trivial cocycle. □

Definition 5.7.24 *A* pointed set *is a set S with a fixed distinguished element $s \in S$, which is called the* base point *of S. Let S, T be pointed sets with base points s, t respectively. A* map of pointed sets *is a map $f : S \to T$ with $f(s) = t$. Its* kernel *is* $\ker(f) = \{x \in S \mid f(x) = t\}$.

Our main example of a pointed set is the first cohomology set $H^1(G, A)$ whose base point is the class of the trivial cocycle. In the next bit we describe a construction of maps of pointed sets between cohomology sets.

Definition 5.7.25 *Let G, G' be finite groups acting by homomorphisms on the groups A, A' respectively. Let $\varphi : G' \to G$, $f : A \to A'$ be group homomorphisms. Then we say that φ and f are* compatible *if*

$$f(\varphi(\sigma') \cdot a) = \sigma' \cdot f(a) \text{ for all } a \in A, \sigma' \in G'.$$

Remark 5.7.26 We use the notation from the previous definition and suppose φ, f are compatible. Write

$$A^G = \{a \in A \mid \sigma \cdot a = a \text{ for all } \sigma \in G\}.$$

The obviously $f(A^G) \subset (A')^G$.

Proposition 5.7.27 *We use the notation from Definition 5.7.25 and suppose that φ, f are compatible. Let $\alpha, \alpha' \in Z^1(G, A)$ and define $\beta : G' \to A'$ by $\beta(\sigma') = f(\alpha(\varphi(\sigma')))$ and define β' similarly using α'. Then $\beta, \beta' \in Z^1(G', A')$. Moreover, if $\alpha \sim \alpha'$ then $\beta \sim \beta'$.*

Proof. We have

$$\begin{aligned}
\beta(\sigma'\tau') = f(\alpha(\varphi(\sigma')\varphi(\tau'))) &= f(\alpha(\varphi(\sigma'))(\varphi(\sigma') \cdot \alpha(\varphi(\tau')))) \\
&= f(\alpha(\varphi(\sigma')))f(\varphi(\sigma') \cdot \alpha(\varphi(\tau'))) \\
&= f(\alpha(\varphi(\sigma'))) \left(\sigma' \cdot f(\alpha(\varphi(\tau')))\right) \\
&= \beta(\sigma')(\sigma' \cdot \beta(\tau')).
\end{aligned}$$

Suppose that there is an $a \in A$ such that $\alpha' = \alpha^a$, i.e., $\alpha'(\sigma) = a\alpha(\sigma)(\sigma \cdot a^{-1})$. We write this with $\varphi(\sigma')$ in place of σ and apply f to obtain

$$\beta'(\sigma') = f(a)\beta(\sigma')(\sigma' \cdot f(a)^{-1}).$$

So we see that $\beta' = \beta^{f(a)}$. □

By the previous proposition we get a map

$$f_* : H^1(G, A) \to H^1(G', A')$$

by $f_*([\alpha]) = [\beta]$. The proposition states that this map is well-defined. It obviously maps the class of the trivial cocycle to the class of the trivial cocycle. Hence it is a map of pointed sets.

Consider a sequence of maps of pointed sets

$$\ldots \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} A_{i+2} \xrightarrow{f_{i+2}} \ldots$$

The sequence is said to be *exact at* A_i if $\mathrm{im}(f_{i-1}) = \ker(f_i)$. The sequence is *exact* if it is exact at each A_i.

In the next part we work with three pointed sets A, B, C on which G acts. The distinguished element will in all cases be denoted 1. We suppose further

- A, B are groups on which G acts by homomorphisms,
- we have an exact sequence of pointed sets

$$1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1 \tag{5.7.8}$$

  (that is, $\ker(f) = \{1\}$, $\mathrm{im}(f) = \ker(g)$, g is surjective),
- f is a group homomorphism (so that it is injective),
- f, g commute with the action of G, that is $f(\sigma \cdot a) = \sigma \cdot f(a)$ for all $a \in A$, $\sigma \in G$, and similarly for g,
- for all $b, b' \in B$ we have $g(b) = g(b')$ if and only if $b' = bf(a)$ for a certain $a \in A$ (that is, g is constant on the cosets $bf(A)$ - note that $f(A)$ is a subgroup of B- and takes different values on different cosets).

We write A^G, B^G, C^G for the subsets of A, B, C respectively, consisting of all elements that are fixed under all $\sigma \in G$. So A^G consists of all $a \in A$ with $\sigma \cdot a = a$ for all $\sigma \in G$. Because f, g commute with the action of G we have $f(A^G) \subset B^G$ and $f(B^G) \subset C^G$.

Now let $c \in C^G$. As g is surjective there exist $b \in B$ with $g(b) = c$; fix such a b. Then $g(\sigma \cdot b) = g(b)$ for all $\sigma \in G$. By the assumption on g this implies that for each $\sigma \in G$ there exists an $a_\sigma \in A$ with $\sigma(b) = bf(a_\sigma)$. But this is the same as $f(a_\sigma) = b^{-1}\sigma(b)$. Note that a_σ is uniquely determined by b because f is injective.

Lemma 5.7.28 *Define $\alpha : G \to A$ by $\alpha(\sigma) = a_\sigma$. Then $\alpha \in Z^1(G, A)$ and its class in $H^1(G, A)$ does not depend on the choice of b.*

Proof. Let $\sigma, \tau \in G$. On the one hand we have $f(a_{\sigma\tau}) = b^{-1}(\sigma\tau \cdot b)$. On the other hand,

$$f(a_\sigma(\sigma \cdot a_\tau)) = f(a_\sigma)(\sigma \cdot f(a_\tau)) = b^{-1}(\sigma \cdot b)(\sigma \cdot (b^{-1}(\tau \cdot b))) = b^{-1}(\sigma \cdot (\tau \cdot b)).$$

As f is injective it follows that $a_{\sigma\tau} = a_\sigma(\sigma\tau \cdot a_\tau)$ and $\alpha \in Z^1(G, A)$.

Let $b' \in B$ be a second element with $g(b') = c$. This yields an $a'_\sigma \in A$ with $f(a'_\sigma) = (b')^{-1}\sigma \cdot b'$. Since $g(b') = g(b)$, the assumption on g provides an $a' \in A$ with $b' = bf(a')$. But then

$$(b')^{-1}\sigma \cdot b' = f(a')^{-1}b^{-1}(\sigma \cdot b)(\sigma \cdot f(a')) = f((a')^{-1}a_\sigma(\sigma \cdot a')).$$

Because f is injective it follows that $a'_\sigma = (a')^{-1}a_\sigma(\sigma \cdot a')$. But that means that the cocycles defined by b and b' are cohomologous. □

By the previous lemma we get a well-defined map

$$\delta^0 : C^G \to H^1(G, A)$$

with $\delta^0(c) = [\alpha]$, where $\alpha \in Z^1(G, A)$ is defined by $f(\alpha(\sigma)) = b^{-1}\sigma \cdot b$, where $b \in B$ is any element with $\mathfrak{g}(b) = c$.

Theorem 5.7.29 *The following sequence is exact*

$$1 \to A^G \xrightarrow{f} B^G \xrightarrow{g} C^G \xrightarrow{\delta^0} H^1(G, A) \xrightarrow{f_*} H^1(G, B).$$

Proof. The exactness at A^G immediately follows from the fact that the kernel of the homomorphism $f : A \to B$ is $\{1\}$.

We have $f(A^G) \subset \ker(g)$ by the exactness of (5.7.8). Let now $b \in B^G$ be such that $g(b) = 1$. Then again by the exactness of (5.7.8) there is an $a \in A$ with $b = f(a)$. For $\sigma \in G$ we have $f(a) = b = \sigma \cdot b = \sigma \cdot f(a) = g(\sigma \cdot a)$, so that $a \in A^G$ as f is injective. Hence $b \in f(A^G)$.

Now we consider the exactness of the sequence at C^G. Let $b \in B^G$ and set $c = g(b)$. For $\sigma \in G$ let $a_\sigma \in A$ be the element determined by b as above. Then $f(a_\sigma) = b^{-1}\sigma \cdot b = b^{-1}b = 1$. Hence $\delta^0(c)$ is the class of the trivial cocycle and we have shown that $g(B^G) \subset \ker(\delta^0)$. Now let $c \in C^G$, set $\alpha = \delta^0(c)$ and suppose that $\alpha \sim 1$. Let $b \in B$ be such that $g(b) = c$; then $f(\alpha(\sigma)) = b^{-1}\sigma \cdot b$ for all $\sigma \in G$. Furthermore, $\alpha \sim 1$ means that there is an $a \in A$ with $\alpha(\sigma) = a\sigma \cdot a^{-1}$. Then $b^{-1}\sigma \cdot b = f(\alpha(\sigma)) = f(a\sigma \cdot a^{-1}) = f(a)\sigma \cdot f(a)^{-1}$, which is equivalent to $f(a)^{-1}b^{-1} = \sigma \cdot (f(a)^{-1}b^{-1})$. We see that $f(a)^{-1}b^{-1}$ and therefore also $bf(a)$ lie in B^G. But $g(f(a)) = 1$ by exactness of (5.7.8), so $g(bf(a)) = g(b) = c$ and we have shown that $\ker(\delta^0) \subset f(B^G)$.

Finally we deal with exactness at $H^1(G, A)$. Let $c \in C^G$ and set $\alpha = \delta^0(c)$. Let $b \in B$ be such that $g(b) = c$; then $f(\alpha(\sigma)) = b^{-1}\sigma \cdot b$ for all $\sigma \in G$. Set $\beta = f_*(\alpha)$; then $\beta(\sigma) = f(\alpha(\sigma)) = b^{-1}\sigma \cdot b$. It follows that $\beta \sim 1$. Now let $\alpha \in Z^1(G, A)$ and set $\beta = f_*(\alpha)$, i.e., $\beta(\sigma) = f(\alpha(\sigma)$ for $\sigma \in G$. Suppose that $\beta \sim 1$, that is, there is a $b \in B$ with $\beta(\sigma) = b^{-1}\sigma \cdot b$ for all $\sigma \in G$. Let $\sigma \in G$. Then $b^{-1}\sigma \cdot b = f(\alpha(\sigma))$ whence $\sigma \cdot b = bf(\alpha(\sigma))$. Therefore $\sigma \cdot g(b) = g(\sigma \cdot b) = g(bf(\alpha(\sigma))) = g(b)$ (again by exactness of (5.7.8)). We see that $g(b) \in C^G$. Moreover, because $f(\alpha(\sigma)) = b^{-1}\sigma \cdot b$ and $g(b) = c$ we have by definition of δ^0 that $\delta^0(c) = [\alpha]$. □

As an application of this theorem we have the followwing result.

Proposition 5.7.30 *Let the notation be as in Theorem 5.7.23. Let* $\mathrm{SL}(n, E)$ *be the subgroup of* $\mathrm{GL}(n, E)$ *consisting of the matrices of determinant 1. Then* $H^1(G, \mathrm{SL}(n, E)) = 1$.

Proof. We have the following exact sequence

$$1 \to \mathrm{SL}(n, E) \xrightarrow{i} \mathrm{GL}(n, E) \xrightarrow{\det} E^* \to 1$$

(here i simply maps a matrix to itself) and the maps satisfy all our hypotheses. Then by the previous theorem

$$\mathrm{GL}(n, F) \xrightarrow{\det} F^* \xrightarrow{\delta^0} H^1(G, \mathrm{SL}(n, E)) \xrightarrow{f_*} H^1(G, \mathrm{GL}(n, E))$$

is exact. But by Theorem 5.7.23 the last set in this sequence is trivial. Hence $\delta^0(F^*) = H^1(G, \mathrm{SL}(n, E))$. Furthermore, $\det : \mathrm{GL}(n, F) \to F^*$ is surjective, so that $\ker(\delta^0) = F^*$. In other words, $\delta^0(F^*) = \{[1]\}$. Putting the two things together proves the proposition. □

We have already seen how classification of real forms of a complex algebra is equivalent to computing a Galois cohomology set (Example 5.7.22). Now we show how Galois cohomology can also be of interest in certain situations for the classification of orbits.

We define an action of B^G on C^G. Let $b \in B^G$ and $c \in C^G$. There is a $b' \in B$ with $g(b') = c$. We define

$$b \cdot c = g(bb').$$

Lemma 5.7.31 *We have that $g(bb')$ does not depend on the choice of b'. This indeed defines an action of B^G on C^G.*

Proof. Let $b'' \in B$ be such that $g(b'') = c$. Then by hypothesis $b'' = b'f(a)$ for a certain $a \in A$. Hence $g(bb'') = g(bb'f(a)) = g(bb')$.

We show that $b \cdot c \in C^G$. Let $\sigma \in G$, then $\sigma \cdot g(bb') = g((\sigma \cdot b)(\sigma \cdot b')) = g(b\sigma \cdot b')$. But $g(\sigma \cdot b') = \sigma \cdot g(b') = \sigma \cdot c = c$, so by the first part of the proof, $g(b\sigma \cdot b') = g(bb')$. It follows that $b \cdot c \in C^G$.

Let $b_1, b_2 \in B$. We show that $b_1 \cdot (b_2 \cdot c) = (b_1b_2) \cdot c$. Let $b_2' \in B$ be such that $g(b_2') = c$, so that $b_2 \cdot c = g(b_2b_2')$. Let $b_1' \in B$ be such that $g(b_1') = g(b_2b_2')$, which is equivalent to $b_1' = b_2b_2'f(a)$ for a certain $a \in A$. We now infer $b_1 \cdot (b_2 \cdot c) = g(b_1b_1') = g(b_1b_2b_2'f(a)) = g(b_1b_2b_2') = (b_1b_2) \cdot c$. □

Theorem 5.7.32 *Let C^G/B^G denote the set of orbits of B^G on C^G. Sending $B^G \cdot c$ to $\delta^0(c)$ yields a well-defined map from C^G/B^G to $\ker(f_*) \subset H^1(G, A)$. Moreover, this map is a bijection.*

Proof. We first show that the map is well-defined. Suppose that $c, c' \in C^G$ lie in the same B^G-orbit, that is, there is a $b \in B^G$ with $c' = b \cdot c = g(bb')$, where $b' \in B$ is such that $g(b') = c$. Then $\delta^0(c) = [\alpha]$ where $f(\alpha(\sigma)) = (b')^{-1}\sigma \cdot b'$ and $\delta^0(c') = [\alpha']$ where $f(\alpha'(\sigma)) = (bb')^{-1}\sigma \cdot (bb')$. But $\sigma \cdot b = b$ and therefore $(bb')^{-1}\sigma \cdot (bb') = (b')^{-1}b^{-1}\sigma \cdot b\sigma \cdot b' = (b')^{-1}\sigma \cdot b' = f(\alpha(\sigma))$. As f is injective it follows that $\alpha = \alpha'$.

Theorem 5.7.29 directly shows that the map is surjective. So it remains to show injectivity. Let $c, c' \in C^G$, write $\delta^0(c) = \alpha$, $\delta^0(c') = \alpha'$ and suppose that $\alpha \sim \alpha'$, that is, there is an $a \in A$ with $\alpha'(\sigma) = a\alpha(\sigma)\sigma \cdot a^{-1}$ for all $\sigma \in G$. Let $b, b' \in B$ be such that $g(b) = c$, $g(b') = c'$. Then $f(\alpha(\sigma)) = b^{-1}\sigma \cdot b$, $f(\alpha'(\sigma)) = (b')^{-1}\sigma \cdot b'$ for all $\sigma \in G$. Let $\sigma \in G$, then

$$(b')^{-1}\sigma \cdot b' = f(\alpha'(\sigma)) = f(a)f(\alpha(\sigma))f(\sigma \cdot a^{-1}) = f(a)b^{-1}(\sigma \cdot b)(\sigma \cdot f(a)).$$

But this is equivalent to $b'f(a)b^{-1} = \sigma \cdot (b'f(a)b^{-1})$. So if we set $\hat{b} = b'f(a)b^{-1}$ then we have $\hat{b} \in B^G$. Furthermore $b'f(a) = \hat{b}b$, so that $c' = g(b') = g(b'f(a)) = g(\hat{b}b) = \hat{b} \cdot c$. We conclude that c and c' lie in the same B^G-orbit. □

Example 5.7.33 Let F be a field. We consider the space $M_2(F)$ consisting of the 2×2-matrices with coefficients in F. Let $\mathrm{GL}(2, F)$ be the group consisting of the invertible elements of $M_2(F)$. Furthermore, $\mathrm{SL}(2, F)$ is the group consisting of the elements of $M_2(F)$ of determinant 1. Both these groups act on $M_2(F)$ by conjugation, that is, for $T \in \mathrm{GL}(2, F)$ (respectively $\mathrm{SL}(2, F)$) and $M \in M_2(F)$ we set $T \cdot M = TMT^{-1}$.

An $N \in M_2(F)$ is said to be nilpotent if there is an $m > 0$ with $N^m = 0$; it can be shown that this is the case if and only if $N^2 = 0$. Let $N \in M_2(F)$ be nilpotent and nonzero. Then there is a nonzero $v \in F^2$ such that $Nv \neq 0$. We have that v, Nv is a basis of F^2 with respect to which the linear map corresponding to N has matrix

$$N_0 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

It follows that N is $\mathrm{GL}(2, F)$-conjugate to N_0. In other words, the set of nonzero nilpotent elements of $M_2(F)$ is a single $\mathrm{GL}(2, F)$-orbit.

When we consider the group $\mathrm{SL}(2, F)$ the situation is a bot different. First let $F = \mathbb{C}$ and let $T \in \mathrm{GL}(2, \mathbb{C})$ be such that $TNT^{-1} = N_0$. Set $\lambda = \frac{1}{\sqrt{\det(T)}}$ and $S = \lambda T$. Then $S \in \mathrm{SL}(2, \mathbb{C})$ and $SNS^{-1} = N_0$. So also in this case there is a single orbit of nonzero nilpotent matrices. Second, let $F = \mathbb{R}$. Then if $\det(T) > 0$ we can do the same thing. However, if $\det(T) < 0$ then we set $\lambda = \frac{1}{\sqrt{-\det(T)}}$ and

$$S = \lambda \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} T.$$

Then again $S \in \mathrm{SL}(2,\mathbb{R})$, but this time $SNS^{-1} = -N_0$. Furthermore it is straightforward to see that N_0 and $-N_0$ are not $\mathrm{SL}(2,\mathbb{R})$-conjugate. So here we get two orbits of nilpotent nonzero matrices.

Now we reinterpret this in terms of Galois cohomology. Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \gamma\}$. Here γ is complex conjugation and acts on $M_2(\mathbb{C})$ by the map Γ from Example 5.7.22. $B = \mathrm{SL}(2,\mathbb{C})$, $A = \{T \in B \mid T \cdot N_0 = N_0\}$ (that is, A is the stabilizer of N_0 in $\mathrm{SL}(2,\mathbb{C})$), $C = B \cdot N_0 = \{T \cdot N_0 \mid T \in B\}$ (that is, C is the orbit of N_0). Then a small calculation shows that

$$A = \left\{ \begin{pmatrix} \varepsilon & 0 \\ c & \varepsilon \end{pmatrix} \mid \varepsilon = \pm 1, c \in \mathbb{C} \right\}.$$

Moreover, if we let $f : A \to B$ be the inclusion map (so simply $f(T) = T$ for $T \in A$) and define $g : B \to C$ by $g(T) = T \cdot N_0$ then we get an exact sequence as in (5.7.8). Furthermore, all hypotheses on the sequence (5.7.8) are satisfied. For the last one suppose that $g(S) = g(T)$. This is equivalent to $S \cdot N_0 = T \cdot N_0$, which amounts to $S^{-1}T \in A$, or $T = SU$ for a $U \in A$.

We have $B^G = \mathrm{SL}(2,\mathbb{R})$ and $C^G = \mathrm{SL}(2,\mathbb{C}) \cdot N_0 \cap M_2(\mathbb{R})$, so C^G is the set of nonzero nilpotent elements of $M_2(\mathbb{R})$. We now look at the action of B^G on C^G defined above. Let $T \in B^G$ and $M \in C^G$ then we denote this action by $T \circ M$. Let $T' \in B$ be such that $T' \cdot N_0 = M$. Then by definition $T \circ M = g(TT')$. But the latter is equal to $g(TT') = TT' \cdot N_0 = T \cdot (T' \cdot N_0) = T \cdot M$ (which by definition equals TMT^{-1}). So we see that the $\circ$ action of B^G on C^G is nothing other than the action we had already defined. We see that the orbits of B^G on C^G are the orbits of $\mathrm{SL}(2,\mathbb{R})$ on the set of nonzero nilpotent elements of $M_2(\mathbb{R})$.

By Proposition 5.7.30 we have that $H^1(G, B) = 1$. Therefore by Theorem 5.7.29, $\ker f_* = H^1(G, A)$. We conclude by Theorem 5.7.32 that the orbits of $\mathrm{SL}(2,\mathbb{R})$ on the set of nonzero nilpotent elements of $M_2(\mathbb{R})$ are in bijection with $H^1(G, A)$.

Now we compute $H^1(G, A)$. Let $\alpha : G \to A$ be a cocycle. Then $\alpha(1) = I_2$ (the 2×2-identity matrix) and $\alpha(\gamma) = T$ with

$$T = \begin{pmatrix} \varepsilon & 0 \\ c & \varepsilon \end{pmatrix}$$

with $\varepsilon = \pm 1$. We have that α is a cocycle if and only if $T\overline{T} = I_2$. A straightforward computation shows that this happens if and only if $c + \bar{c} = 0$, that is, when $c = iu$ for some $u \in \mathbb{R}$. Now let $S \in A$ and write

$$S \begin{pmatrix} \delta & 0 \\ c_0 & \delta \end{pmatrix}$$

where $\delta = \pm 1$. Then $\alpha^S(\gamma) = ST\overline{S}^{-1}$, which is equal to

$$\begin{pmatrix} \varepsilon & 0 \\ \delta\varepsilon(c_0 - \bar{c}_0) + iu & \varepsilon \end{pmatrix}.$$

We see that by choosing $c_0 = -\frac{1}{2}\delta\varepsilon ui$ the term in the $(2,1)$ position vanishes. So we have two cocycles, the trivial one, and the one sending γ to $-I_2$. Therefore we recover the fact that there are two $\mathrm{SL}(2,\mathbb{R})$-orbits in the set of nonzero nilpotent elements of $M_2(\mathbb{R})$.

Remark 5.7.34 In the previous example it may seem that Galois cohomology is a way to transform easy problems into more difficult ones. However, there are also situations, analogous to the one considered in the example, where it is not possible to list the real orbits directly. In those cases the approach via Galois cohomology can be very useful. We refer to [Djo83] for an example.

Index

Bibliography

[Cla94] David A. Clark. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.*, 83(3-4):327–330, 1994.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.

[Djo83] Dragomir Ž. Djokovic. Classification of trivectors of an eight-dimensional real vector space. *Linear and Multilinear Algebra*, 13(1):3–39, 1983.

[Edw77] Harold M. Edwards. *Fermat's last theorem*, volume 50 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1977. A genetic introduction to algebraic number theory.

[Gal78] Steven Galovich. Unique factorization rings with zero divisors. *Math. Mag.*, 51(5):276–283, 1978.

[JÖ93] Klaus Jänich. *Funktionentheorie*. Springer-Lehrbuch. [Springer Textbook]. Springer-Verlag, Berlin, third edition, 1993. Eine Einführung. [An introduction].

[Mig83] Maurice Mignotte. How to share a secret. In *Cryptography (Burg Feuerstein, 1982)*, volume 149 of *Lecture Notes in Comput. Sci.*, pages 371–375. Springer, Berlin, 1983.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[Sie13] Aaron N. Siegel. *Combinatorial game theory*, volume 146 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2013.

[Ste07] Ian Stewart. *Why beauty is truth*. Basic Books, New York, 2007. A history of symmetry.