university of groningen

faculty of mathematics
and natural sciences

The inverse Galois problem

Bachelor Project Mathematics

July 2016

Student: H.G.J. Tiesinga

First supervisor: prof. dr. J. Top

Second supervisor: dr. A.E. Sterk

Abstract

Some specific field extensions $L|K$ are classified as Galois extensions. We call the group of automorphisms of such $L|K$ the Galois group of $L|K$. The inverse Galois problem asks the question whether every finite group is isomorphic to the Galois group of a Galois extension of $\mathbb{Q}$. We describe the known solutions of this problem for abelian groups, for the symmetric groups S_n and for the alternating groups A_n and even establish specific Galois extensions for the latter two. We conclude with a description of a way to establish some semidirect products as Galois groups.

Contents

Chapter 1

Introduction

Évariste Galois (25 October 1811 - 31 May 1832) was a French mathematician born in Bourg-la-Reine. While still in his teens, he was able to determine a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a problem standing for 350 years. His work laid the foundations for Galois theory. He died at age 20 from wounds suffered in a duel. [1] Galois theory provides a connection between field theory and group theory. Using Galois theory, certain problems in field theory can be reduced to group theory, which is, in some sense, simpler and better understood.[2]

The inverse Galois problem concerns whether every finite group appears as the Galois group of some Galois extension of the field of rational numbers $\mathbb{Q}$. This problem, first posed in the 19th century, is in general unsolved [3]. Despite that, we are able to derive some partial results for this problem. The first systematic approach to a solution of the inverse Galois problem goes back to Hilbert (1892). Using the irreducibility theorem, which he proved for this purpose, he could show that over $\mathbb{Q}$ and more generally over every field generated over $\mathbb{Q}$ there are infinitely many Galois extensions with the symmetric and the alternating group, S_n and A_n [4].

In this thesis we will analyse the inverse Galois problem and we will solve it for some specific groups. In order to fully understand the problem we are dealing with, we will first introduce the notion of a Galois extension and a Galois group and discuss some Galois theory. After that, we will give an elementary proof for the inverse Galois problem when looking at abelian groups. Furthermore, we will solve the problem for the symmetric and the alternating group with the use of Hilbert's irreducibility theorem. For these groups, we will not only prove the existence of a Galois group isomorphic to it, but we will also establish specific Galois extensions with such Galois groups. Finally, using the theory of elliptic curves, we will give an example and describe a way to solve the problem for specific semidirect products.

Chapter 2

Galois theory

We start in this chapter with a short introduction to Galois theory and we discuss some propositions which appear to be useful later on. We assume the reader has some knowledge about fields, rings and automorphisms. If that is not the case we recommend [5], to which we refer often, as a good source of information about these subjects.

2.1 Galois extensions and Galois groups

Before stating the definition of a Galois extension or a Galois group, let us take a look at automorphisms σ of a field $L = K(a_1, ..., a_n)$, with K being a field and $a_1, ..., a_n$ algebraic over K, which have the property that

$$\sigma(a) = a \text{ for any } a \in K.$$

We call these σ, automorphisms of $L|K$ and denote the group of these automorphisms as $\text{Aut}_K(L)$ (see also [6]). We know the group of automorphisms of $K(\alpha)|K$, $\text{Aut}_K(K(\alpha))$, for some algebraic α over K, contains at most $[K(\alpha) : K]$ elements (see [5] for a proof of this fact). If we generalize this, using the well-known Tower rule, for some finite extension $L|K$, we see the group $\text{Aut}_K(L)$ contains at most $[L : K]$ elements. We are now able to state the desired definition which is also in [6].

Definition 1. A *Galois extension* is a finite field extension $L|K$ for which $\#\text{Aut}_K(L) = [L : K]$. If $L|K$ is a Galois extension, we write $\text{Gal}_K(L)$, which we call the Galois group of $L|K$, instead of $\text{Aut}_K(L)$ to denote the group of automorphisms of $L|K$.

In our search for some particular Galois groups, we will most of the time look at splitting fields of polynomials, because the following property allows us to easily check whether such extensions are Galois. A proof is sketched, the details can be found in [5].

Proposition 2. *Let f be a polynomial over some field K without any multiple roots and let L be its (unique [5]) splitting field. Then the extension $L|K$ is Galois and we will often write $Gal_K(f)$ instead of $Gal_K(L)$ to denote its Galois group.*

Proof. Suppose we have a polynomial $f \in K[X]$ of degree m with splitting field L over K and f does not have multiple roots. Write

$$f = g_1 ... g_n$$

for irreducible $g_1, ..., g_n \in K[X]$. Then the splitting field L_1 of g_1 is Galois over K, since the order of $\mathrm{Aut}_K(L_1)$ equals the number of different roots of g_1 in L_1. If f has any irreducible factor of degree $m > 2$ over L_1, then the splitting field L_2 of this factor over L_1 has exactly $[L_2 : K] = [L_2 : L_1] \cdot [L_1 : K]$ automorphisms, since any automorphism of $L_1|K$ extends in exactly $[L_2 : L_1]$ ways to an automorphism of $L_2|K$. Repeating this argument till f splits finishes the proof. □

Remark. Note that for irreducible polynomials over a field of characteristic zero or a finite field it holds that they do not have multiple roots. A full proof of this statement can be found in [6]. We skipped it, because it is a bit involved and highly elementary. Fields with the property that irreducible polynomials over it do not have multiple roots are also called perfect fields.

2.2 Transitivity

We know that an element of the Galois group of a polynomial f over a field K is an identity map if we restrict it to K. Therefore we can say that such an automorphism is uniquely determined by the way it permutes the roots of f. Thus, if f has degree n and we number its roots, then its Galois group is isomorphic to a subgroup of the symmetric group S_n. [6]. The Galois group can be isomorphic to S_n and in the next section we will discuss some propositions that allow us to conclude that. Before we arrive at those propositions, we first have to introduce some notions of a group being transitive and doubly transitive. The following definition is also denoted in [6].

Definition 3. Let G be a group and X be a set on which it acts. Then G is called *transitive* if for every $x, y \in X$, there is a $g \in G$ such that $g(x) = y$.

If we want to know whether a Galois group $G =$Gal$_K(f)$ of a polynomial $f \in K[X]$ acts transitively on the set of roots of f, we use the following proposition from [6]. A proof of the 'if' part is included. For more details concerning the proof, see [6].

Proposition 4. *G acts transitively on the set of roots of a factor of f if and only if that factor of f is irreducible over K.*

Proof. Let α be a root of f and L be the splitting field of f over K. Then the minimal polynomial g of α over K is an irreducible divisor of f. For all $\sigma \in G$ it holds that $\sigma(\alpha)$ is also a root of g, since

$$g(\sigma(\alpha)) = \sigma(g(\alpha)) = \sigma(0) = 0.$$

It also holds that for a root β of g, there is an embedding

$$\tau : K(\alpha) \to L : \alpha \mapsto \beta. \tag{2.1}$$

This is the case, because

$$\pi : K[X] \to K[\alpha] : h \mapsto h(\alpha)$$

is a surjective homomorphism with (g) as its kernel and

$$\rho : K[X] \to L : h \mapsto h(\beta)$$

is a homomorphism with g in its kernel and therefore we can make the homomorphism τ such that $\tau\pi = \sigma$ with

$$\tau(\alpha) = \tau(\pi(X)) = \rho(X) = \beta.$$

So, for any root β of f it holds that β is a root of g if and only if there is an embedding of the form of 2.1. The result follows. □

This means in particular that $\text{Gal}_{\mathbb{Q}}(f)$ acts transitively on the set of roots of $f \in \mathbb{Q}[X]$ if and only if f is irreducible over $\mathbb{Q}$.
Some groups don't just take any element of a set to any other element, but can also do this in pairs. These groups are called doubly transitive and the definition is stronger then the one for it being transitive. We borrowed it from [7]

Definition 5. A group G is called *doubly transitive* if it acts on a non-trivial set X such that for any $x, x', y, y' \in X$ with $x \neq x'$ and $y \neq y'$, we can find a $g \in G$ such that $gx = y$ and $gx' = y'$.

We will furthermore introduce the definition of the stabilizer of an element in order to come up with a useful proposition to determine whether a group is doubly transitive.

Definition 6. Let G be a group and X be a set on which G acts. For $x \in X$, we call the subgroup

$$\text{Stab}_G(x) = \{g \in G | g(x) = x\}$$

of G the *stabilizer* of x in G.

This definition is also in [6]. The following proposition is in [7] together with a proof.

Proposition 7. *Let G be a group and X be a non-trivial set on which G acts. Fix some $x \in X$. Then G acts doubly transitively (on X) if and only if it acts transitively (on X) and $Stab_G(x)$ acts transitively on $X - \{x\}$.*

Proof. The result is clear when $\#X = 2$, so assume the size of X is larger then 2.
If G acts doubly transitively on X, then we can choose for any $x, y_1, y_2 \in X$ with $y_1 \neq x \neq y_2$ a $g \in G$ such that

$$gx = x \text{ and } gy_1 = y_2,$$

so $\mathrm{Stab}_G(x)$ acts transitively on $X - \{x\}$ and furthermore, G acts transitively on X.
Now we assume that $\mathrm{Stab}_G(x)$ acts transitively on $X - \{x\}$ for a fixed $x \in X$ and that G acts transitively on X.
Take a random $y \in X$ and write $y = gx$. Then, using some calculations, one can find out that $\mathrm{Stab}_G(y) = g\mathrm{Stab}_G(x)g^{-1}$. For $z_1, z_2 \in X - \{y\}$, we have $g^{-1}z_1, g^{-1}z_2 \neq g^{-1}y = x$. By hypothesis, some $h \in\mathrm{Stab}_G(x)$ satisfies $hg^{-1}z_1 = g^{-1}z_2$, so $ghg^{-1}z_1 = z_2$. Since $ghg^{-1} \in\mathrm{Stab}_G(y)$, we see the group $\mathrm{Stab}_G(y)$ acts transitively on $X - \{y\}$ for any $y \in X$.
Now consider $x_1, x_2, y_1, y_2 \in X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$ and take elements $g \in\mathrm{Stab}_G(x_1)$ and $g' \in\mathrm{Stab}_G(y_2)$ such that $g(x_2) = y_2$ and $g'(x_1) = y_1$. Then

$$g' \circ g(x_1) = g'(x_1) = y_1 \text{ and } g' \circ g(x_2) = g'(y_2) = y_2$$

as desired.
This recipe works only when $x_1 \neq y_2$, so when $x_1 = y_2$ choose some $z \neq x_1, y_1 \in X$. Now use elements $k \in\mathrm{Stab}_G(x_1)$, $k' \in\mathrm{Stab}_G(z)$ and $k'' \in\mathrm{Stab}_G(y_1)$ with $k(x_2) = z, k'(x_1) = y_1$ and $k''(z) = y_2$ to obtain

$$k''k'k(x_1) = k''k'(x_1) = k''(y_1) = y_1 \text{ and } k''k'k(x_2) = k''k'(z) = k''(z) = y_2.$$

□

2.3 Finding Galois groups

We now arrive at the point where we can state and prove some propositions which ensure us that a subgroup of S_n equals S_n. Proposition 8 and a sketch of the proof of it can be found in [6]. We included a more detailed proof. Note that we mean that the action of some symmetric group S_n is transitive on $\{1, ..., n\}$ if we talk about S_n being transitive.

Proposition 8. *Let p be a prime number and G be a transitive subgroup of S_p which contains a transposition. Then $G = S_p$.*

Proof. Take some $i, j \in \{1, ..., p\}$. Then define the equivalence class

$$i \sim j \iff i = j \text{ or } (i \quad j) \in G.$$

This is obviously an equivalence relation. Note that for $i \sim j$ and $i \sim k$ with $i \neq j \neq k \neq i$ we have

$$(i \quad j)(j \quad k)(i \quad j) = (i \quad k) \in G,$$

so also $i \sim k$. We denote an equivalence class of some i by $[i]$. For $(i \quad j) \in G$ and $\sigma \in G$, it holds that also

$$(\sigma(i) \quad \sigma(j)) = \sigma(i \quad j)\sigma^{-1} \in G,$$

from which we deduce that $\sigma([i]) = [\sigma(i)]$. Since G is transitive, we can deduce that every equivalence class contains the same number of elements, because for any $i, j \in \{1, ..., p\}$ such that $[i] \neq [j]$, we can pick $\sigma \in G$ such that $\sigma(i) = j$, so $\sigma([i]) = [\sigma(i)] = [j]$, hence $\#[i] = \#\sigma([i]) = \#[j]$. We also have that $\#([i])|p$ and that $\#([i]) \neq 1$, since G contains a transposition. Therefore there is only one equivalence class, namely $\{1, ..., p\}$, and G contains all transpositions of S_p. Hence it equals S_p. □

Proposition 8 requires p to be a prime number, so it restricts its possibilities for application. One might wonder whether this proposition also holds when p is not prime.

Example 9. Consider the subgroup $H =< \sigma, \tau >$ of S_4 with

$$\sigma = (13) \text{ and } \tau = (1234).$$

We see

$$\sigma\tau = (13)(1234) = (12)(34) = (1432)(13) = \tau^3\sigma,$$

so

$$\begin{aligned} H &= \{1, \sigma, \tau, \tau^2, \tau^3, \tau\sigma, \tau^2\sigma, \tau^3\sigma\} \\ &= \{1, (13), (1234), (13)(24), (1432), (14)(23), (24), (12)(34)\}. \end{aligned}$$

Now, if we want to map i to j for any given $i, j \in \{1, 2, 3, 4\}$, we can always use τ, τ^2 or τ^3, so H is a transitive subgroup of S_4. It also contains a transposition. We conclude, however, since $\#H = 8 \neq 24 = \#S_4$, that $H \neq S_4$.

We see proposition 8 already does not hold for a subgroup of S_4. Luckily, we are also able to prove a variant of the proposition which requires a stronger condition.

Proposition 10. *Let G be a doubly transitive subgroup of S_n for some $n \in \mathbb{Z}_{>1}$, which contains a transposition. Then $G = S_n$.*

Proof. Suppose $(i \quad j) \in G$ for some different $i, j \in \{1, ..., n\}$. Then for any different $k, l \in \{1, ..., n\}$ we have by the fact that G is doubly transitive that there is a $g \in G$ such that $g(i) = k$ and $g(j) = l$. Hence,

$$g(i \quad j)g^{-1} = (g(i) \quad g(j)) = (k \quad l) \in G.$$

This means G contains all transpositions and therefore equals S_n. □

If we look back at example 9, we see H does not contain an element that takes 1 to 2 and 2 to 4, which shows us it is not a doubly transitive subgroup of S_4 in accordance with the proposition above.
One might wonder how to establish the Galois group of a polynomial.

Example 11. Let us consider the polynomial $f(X) = X^3 - 2 \in \mathbb{Q}(X)$. Define $\zeta_3 = e^{\frac{2\pi i}{3}}$. We see f has roots $\zeta_3 \sqrt[3]{2}, \zeta_3^2 \sqrt[3]{2}$ and $\sqrt[3]{2}$ in its splitting field $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. By proposition 2, we know $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)|\mathbb{Q}$ is a Galois extension.
Now, the automorphisms in the Galois group of f are determined by where the send $\sqrt[3]{2}$ and ζ_3 to. Therefore, elements of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3))$ are given by

$$\sigma_{kl} : \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \to \mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \sqrt[3]{2} \mapsto \zeta_3^k \sqrt[3]{2},\ \zeta_3 \mapsto \zeta_3^l,$$

where $k \in \{0, 1, 2\}$ and $l \in \{1, 2\}$. These elements are all the elements of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3))$, since

$$\#\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) = [\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 3 \cdot 2 = 6.$$

Note that this immediately implies that $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) \cong S_3$. We could also see this with the use of proposition 4 and 8 in the following way. We see, since the roots of f are not in $\mathbb{Q}$, that it is irreducible over $\mathbb{Q}$. Therefore, by proposition 4, $\mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to a transitive subgroup of S_3 if we number the roots of f in the way $i = \zeta^i \sqrt[3]{2}$. We see $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains σ_{02}, which can be seen as the transposition $(12) \in S_3$ and therefore, by proposition 8, we conclude that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_3$.

2.4 Reduction modulo a prime

In this section we discuss the very helpful theorem of Dedekind in order to find whether the Galois group of a polynomial contains certain cycle types. The following proposition is derived from a more general proposition in [8]. We use the fact that we can always find prime numbers p such that for f not containing multiple roots, also $\bar{f}$ does not contain multiple roots. The proof of this assumption can be found in [6].

Proposition 12. *Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree n and $\bar{f} = f$ mod p be its reduction modulo a prime number p such that both f and $\bar{f}$ do not have multiple roots. By numbering the roots and building a bijection between these numberings, both $Gal_{\mathbb{F}_p}(\bar{f})$ and $Gal_{\mathbb{Q}}(f)$ are isomorphic to subgroups of S_n. Denote these subgroups as respectively G_p and G. Then $G_p \subseteq G$.*

For details about this proposition and the proof, we recommend [8] or [6]. The proof is not too difficult, but a bit involved, so we skipped it.
Now consider such a polynomial $f \in \mathbb{Z}[X]$ without multiple roots, with degree n, and decompose it into irreducible factors modulo a prime number p

$$\bar{f} = g_1 ... g_h \in \mathbb{F}_p[X]$$

such that this $\bar{f}$ does not have multiple roots. We will take a look at the Galois group of $\bar{f}$ over $\mathbb{F}_p$, but before we do that, we need a lemma from [5]. The proof is sketched and the details can be found in [5].

Lemma 13. *The automorphism group of a finite field is cyclic.*

Proof. Consider the finite field $\mathbb{F}_q$ for some $q = p^n$ with p prime. We know that $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_q$ with minimum polynomial of degree n containing n different roots in $\mathbb{F}_q$. Therefore $\#\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) = n$. Consider the Frobenius-homomorphism

$$\phi : \mathbb{F}_q \to \mathbb{F}_q : x \mapsto x^p.$$

Since $\mathbb{F}_q$ is finite, $\phi \in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$. Moreover, ϕ^k for $0 < k < n$ are all different nontrivial automorphisms of the group $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$. So together with the identity map, they form the whole group and we conclude

$$\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) =< \phi > .$$

□

Using this lemma, we deduce that $\mathrm{Gal}_{\mathbb{F}_p}(\bar{f})$ is cyclic and therefore also the subgroup of S_n isomorphic to it. Consider now the cycle that generates that subgroup of S_n as a product of k disjoint cycles

$$(i_{1,1} \quad i_{1,l_1})(i_{2,1} \quad i_{2,l_2})...(i_{k,1} \quad i_{k,l_k}).$$

Since $\mathrm{Gal}_{\mathbb{F}_p}(\bar{f})$ acts transitively on a factor of $\bar{f}$ if and only if that factor is irreducible by proposition 4, we know that the numbers $l_1, ..., l_k$ must exactly denote the number of roots of respectively the irreducible factors $g_1, ..., g_h$, so we see $k = h$. Because every g_i does not have multiple roots, we see that the numbers $l_1, ..., l_h$ must denote the degrees of respectively $g_1, ..., g_h$. This means $\mathrm{Gal}_{\mathbb{F}_p}(\bar{f})$ contains a cycle of the type $(l_1, ..., l_h)$. Using proposition 12, we have just proven the following wonderful theorem of Dedekind. Parts of this proof are also in [8].

Theorem 14. (Dedekind) *Let f be a polynomial of degree n in $\mathbb{Z}[X]$ without multiple roots. Let p be a prime number such that we can decompose*

$$\bar{f}(X) = g_1(X)...g_h(X) \in \mathbb{F}_p[X],$$

where $\bar{f}$ does not have multiple roots and each g_i is irreducible. Then the subgroup of S_n isomorphic to $Gal_{\mathbb{Q}}(f)$ contains a cycle of the type $(deg(g_1), deg(g_2), ..., deg(g_h))$.

Example 15. Consider the polynomial

$$f(X) = X^4 + 12X^3 + 14X^2 + 14X + 34 \in \mathbb{Z}[X].$$

We want to determine its Galois group $\mathrm{Gal}_{\mathbb{Q}}(f)$. First notice that f does not have multiple roots. This can be checked using the fact that f is irreducible by the well-known Eisenstein criterion for $p = 2$ and the fact that an irreducible polynomial over a field of characteristic zero does not contain any multiple roots (see remark in first section). We now look at the irreducible decompositions of f modulo 3 and modulo 5. We see

$$\begin{aligned}\bar{f}(X) &= X^4 + 2X^2 + 2X + 1 \bmod 3\\ &= (X-1)(X^3 + X^2 + 2) \bmod 3\\ \bar{f}(X) &= X^4 + 2X^3 + 4X^2 + 4X + 4 \bmod 5\\ &= (X-1)(X-2)(X^2-2) \bmod 5.\end{aligned}$$

The factors $X^3 + X^2 + 2$ and $X^2 + 2$ are irreducible in respectively $\mathbb{F}_3[X]$ and $\mathbb{F}_5[X]$, since they have no roots in respectively $\mathbb{F}_3$ and $\mathbb{F}_5$. We see, because these factors are irreducible polynomials over a finite field that these factors do not contain multiple roots (see the remark in the first section). Therefore, the reduction of f modulo 3 and f modulo 5 both do no contain multiple roots and we can apply theorem 14 to conclude that $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains a 2-cycle and a 3-cycle. The fact that it contains a 3-cycle means that the stabilizer of the number in $\{1, 2, 3, 4\}$ that is not in the 3-cycle acts transitively on the remaining numbers. With the use of propositions 4 and 7, we conclude $\mathrm{Gal}_{\mathbb{Q}}(f)$ is doubly transitive. We conclude with proposition 10 that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_4$.

One might wonder whether this theorem can be used to determine the Galois group for all possible polynomials in $\mathbb{Q}[X]$. We will see in the next example that this method is not always sufficient.

Example 16. Consider $f = X^5 - 5X + 12$. Below there are reductions of f into irreducible factors modulo some prime numbers.

$$\begin{aligned}f_2 &= f \bmod 2 = X(X + \bar{1})^4\\ f_3 &= f \bmod 3 = X(X^2 + X - \bar{1})(X^2 - X - \bar{1})\\ f_5 &= f \bmod 5 = (X + \bar{2})^5\\ f_7 &= f \bmod 7 = X^5 + \bar{2}X + \bar{5}.\end{aligned}$$

The fact that these are indeed irreducible factorizations can easily be checked. We left these calculations for the reader.

We see f_2 and f_5 contain multiple roots, so we can not use them with the theorem of Dedekind to deduce which cycles-types appear in $\mathrm{Gal}_{\mathbb{Q}}(f)$. We can look at f_3 and f_7, since they do not contain multiple roots: for f_3 this is clear and for f_7 it is implied by the fact that it is irreducible (which implies that f is irreducible and therefore does not contain multiple roots). With the theorem of Dedekind, we see $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains a product of 2 disjoint transpositions and a 5-cycle.

Keune describes in [6] that if we use theorem 14 with many primes p, we can not ensure the existence of more cycle-types in $\mathrm{Gal}_{\mathbb{Q}}(f)$ and therefore not determine $\mathrm{Gal}_{\mathbb{Q}}(f)$.

Chapter 3

Abelian groups

In this chapter we will prove that for every finite abelian group A, there exists a Galois extension over $\mathbb{Q}$ such that its Galois group is isomorphic to A. Before we are able to do so, we need to introduce a few definitions and propositions.

3.1 Primes equivalent to 1 modulo m

We begin with a special case of the Dirichlet's theorem on arithmetic progressions. This theorem tells us that for every pair of co-prime numbers (m, n), there are infinitely many prime numbers p such that $p = m \bmod n$. The special form of this theorem we want to use in our proof on abelian groups later on is the following.

Theorem 17. *For every positive integer m there are infinitely many prime numbers p such that $p \equiv 1$ mod m.*

Before we are able to prove this theorem, we need to introduce a few definitions we found in [6]. In the following two definitions $\mu_m(K)$ is the set of m-th roots of unity in the field K and o is the order function.

Definition 18. For m being a positive integer, the minimal polynomial of $\zeta_m = e^{2\pi i/m}$ over $\mathbb{Q}$, which we call *the mth-cyclotomic polynomial* Φ_m is defined as

$$\Phi_m(X) = \prod_{\substack{\zeta \in \mu_m(\mathbb{C}) \\ o(\zeta)=m}} (X - \zeta).$$

We can also define similarly

Definition 19. For m being a positive integer, we define

$$\Psi_m(X) = \prod_{\substack{\zeta \in \mu_m(\mathbb{C}) \\ o(\zeta)\neq m}} (X - \zeta).$$

Proposition 20. *For every positive integer m it holds that $\Phi_m(X) \in \mathbb{Z}[X]$ and if $m > 1$ it has constant term equal to* 1.

Proof. The Lemma of Gauss, which can be found in [6], tells us that for a monic polynomial $g \in \mathbb{Z}[X]$ with $g = h \cdot h' \in \mathbb{Q}[X]$ for $h, h' \in \mathbb{Q}[X]$ it holds that $h, h' \in \mathbb{Z}[X]$. Now, since the roots of $\Phi_m(X)$ are roots of $X^m - 1$ and $\Phi_m(X) \in \mathbb{Q}[X]$ as it is a minimal polynomial of ζ_m over $\mathbb{Q}$, a reference for this statement is [6], it follows that $\Phi_m(X) \in \mathbb{Z}[X]$.
For the second claim notice that the constant term equals ± 1, since it is the product of roots of unity and it is in $\mathbb{Z}$. Then see that for $\zeta \in \mu_m(\mathbb{C})$ with order $m > 1$ it holds that ζ^{-1} has the same order m, since:

$$\zeta^m = 1 \text{ and } \zeta^{m-1} = \alpha \neq 1$$

implies

$$(\zeta^{-1})^m = (\zeta^m)^{-1} = 1 \text{ and } (\zeta^{-1})^{m-1} = (\zeta^{m-1})^{-1} = \alpha^{-1} \neq 1.$$

Therefore, since $\zeta \neq \zeta^{-1}$ if ζ has order $m > 2$, we deduce that the constant term of $\Phi_m(X)$ equals the product of the terms $\zeta \cdot \zeta^{-1}$, so it equals 1. If $m = 2$, then $\Phi_2(X) = X + 1$. □

We will now go to the proof of theorem 17.

Proof. For $m = 1$, the statement is trivial, so assume $m > 1$. Suppose for contradiction that there is a finite number of primes p such that $p \equiv 1 \mod m$. Let S be that set of primes and define $P = \prod_{p \in S} p$. If we look at definition 18, we see that $\Phi_m(X) \pm 1$ only has a finite number of zeros. Pick an integer k such that $\Phi_m(kmP) \neq \pm 1$ such that there exists a prime p which divides $\Phi_m(kmP)$. Now, the set $\mu_m(\mathbb{C})$ is the set of roots of $X^m - 1 \in \mathbb{Z}[X]$, so $\Phi_m(X) \cdot \Psi_m(X) = X^m - 1$ and we have

$$\Phi_m(kmP) \cdot \Psi_m(kmP) = (kmP)^m - 1 \equiv -1 \mod p.$$

We deduce $p \nmid m$ and from $p | \Phi_m(kmP)$ we see

$$\overline{\Phi_m}(\overline{kmP}) = \bar{0} \in \mathbb{F}_p.$$

Since, by proposition 20, $\Phi_m(kmP)$ has a constant term 1, we deduce from the fact we just shown that $p \nmid kmP$, hence $p \notin S$.
We determine $\bar{f}'$ of $\bar{f} = X^m - \bar{1} \in \mathbb{F}_p[X]$ to be

$$\bar{f}' = \bar{m}X^{m-1} \in \mathbb{F}_p[X].$$

which is nonzero, since $p \nmid m$. If $\bar{f}$ would have a multiple root α, then α would also be a root of $\bar{f}'$, but then

$$\alpha^m = \alpha^{m-1} \cdot \alpha = \bar{0} \neq \bar{1},$$

so we have a contradiction, so $\bar{f}$ doesn't have multiple roots. Therefore, using $\Phi_m(X) \cdot \Psi_m(X) = X^m - 1$ again, since $\overline{kmP}$ is a root of $\overline{\Phi_m}$, it is not a root of $\overline{\Psi_m}$. Hence $\overline{kmP}$

is a primitive m-th root of unity of $\mathbb{F}_p^*$. By the famous theorem of Lagrange, which can be found in [9], we see

$$m = \# < \overline{kmP} > | \# \mathbb{F}_p^* = p - 1.$$

We conclude that $p \equiv 1 \bmod m$ which contradicts with $p \notin S$. □

Some small parts of this proof are also in [6].

3.2 Group theoretical propositions

This section is devoted to some results from group theory we need for our proof of the inverse Galois problem for abelian groups later on. We will start with a lemma that is in [9] together with its (very detailed) proof.

Proposition 21. *Let A be a finitely generated abelian group. The there exists $r \geq 0$ and a unique sequence $(d_1, ..., d_m) \in \mathbb{Z}_{>1}^m$ with $d_m | d_{m-1} | ... | d_1$ such that*

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_m\mathbb{Z}.$$

We continue with a proposition about cyclic groups we found in [10] together with parts of this proof.

Proposition 22. *If G is cyclic with finite order n, then G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

Proof. Let g be a generator of G and 1 be the identity element. Since G is cyclic of order n it consists of the elements $1, g, g^2, ..., g^{n-1}$. Suppose $g^k = g^l$ for distinct integers k and l between or equal to 0 and $n-1$ and $k > l$. Then $g^{k-l} = 1$ and because G is cyclic it consists of the (at most $k-l$ distinct) elements $1, g, ..., g^{k-l-1}$. But $k - l < n$, so this cannot be true. Therefore the elements $1, g, g^2, ..., g^{n-1}$ of G are distinct.
Now define the map

$$f : \mathbb{Z}/n\mathbb{Z} \to G : \bar{a} \mapsto g^a.$$

We see that for $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$:

$$f(\bar{a} + \bar{b}) = g^{a+b} = f(\bar{a}) f(\bar{b}),$$

so f is a homomorphism. We also see that $\ker(f) = (\bar{0})$, so f is injective. Because of that and the fact that the groups $\mathbb{Z}/n\mathbb{Z}$ and G both contain n elements, the mapping f is an isomorphism. □

We now continue to a more applied proposition about certain groups being cyclic. But in order to proof that proposition, we will first proof the following lemma which can be found in [6]

Lemma 23. *Let a and b be elements of an abelian group with $o(a) = m$, $o(b) = n$ and $gcd(n, m) = 1$. Then $o(ab) = mn$.*

Proof. For an integer k are equivalent

$$\begin{aligned}(ab)^k &= 1,\\ a^k &= b^{-k},\\ a^k &= b^{-k} = 1, \text{ since } o(a^k)|m, o(b^-k)|n \text{ and } \mathrm{ggd}(m,n) = 1\\ m|k &\text{ and } n|k\\ mn|k&, \text{ since } \mathrm{ggd}(m,n) = 1.\end{aligned}$$

So $o(ab) = mn$. □

Now we state the following proposition to end this section. The proof can be found in [5].

Proposition 24. *The multiplicative subgroup of a finite field is cyclic.*

3.3 The fundamental theorem of Galois theory

In this section we discuss a very important theorem in Galois theory and a proposition following from it. The theorem below can be found in [6] together with a detailed proof. We will just state the theorem.

Theorem 25. (The fundamental theorem of Galois theory) *Let $L : K$ be a Galois extension with Galois group G. Then there is the following bijective map between the set X of subextensions of $L : K$ and the set Y of subgroups of G*

$$\phi : X \to Y : K' \mapsto Gal_{K'}(L)$$

with bijective inverse

$$\psi : Y \to X : H \mapsto L^H.$$

Note that L^H denotes the invariants of L under the action of the group H. From this theorem, we also derive the following proposition. The proof can be found in detail in [6].

Proposition 26. *Let $L|K$ be a Galois extension and K' be a subextension of $L|K$. Then $K'|K$ is a Galois extension if and only if $Gal_{K'}(L)$ is a normal subgroup of $Gal_K(L)$. Furthermore, then there is an isomorphism*

$$\frac{Gal_K(L)}{Gal_{K'}(L)} \cong Gal_K(K').$$

3.4 Cyclotomic extensions

If we let K be a field, then we call the extension $L|K$ cyclotomic if L is the splitting field of the polynomial $X^m - 1$ for some positive integer m. If we let $\zeta_m = e^{\frac{2\pi i}{m}}$, then a cyclotomic extension over $\mathbb{Q}$ has the form $\mathbb{Q}(\zeta_m)|\mathbb{Q}$, where $\mathbb{Q}(\zeta_m)$ is the splitting field of $X^m - 1$ over $\mathbb{Q}$. In the proof of theorem 17, we already saw that $X^m - 1$ does not contain multiple roots, so we know by proposition 2 that the extension $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ is Galois. Furthermore we are able to proof the following result. Note that we use here that $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$, see [6] for the proof.

Proposition 27. *For a positive integer m, we have an isomorphism of groups*

$$\phi : Gal_{\mathbb{Q}}(\mathbb{Q}(\zeta_m)) \to (\mathbb{Z}/m\mathbb{Z})^*.$$

Proof. Any automorphism of the extension $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ must send a root of the polynomial $f = X^m - 1 \in \mathbb{Q}[X]$ to another root, which has the same order. Therefore, since ζ_m has order m, it must permute roots ζ_m^k of f with the property that $\text{ggd}(k, m) = 1$. Therefore we can define a group homomorphism between the automorphisms in $\text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m))$ and the elements of $(\mathbb{Z}/m\mathbb{Z})^*$

$$\phi : \text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m)) \to (\mathbb{Z}/m\mathbb{Z})^* : (\sigma : \zeta_m \mapsto \zeta_m^k) \mapsto \bar{k}.$$

This homomorphism is injective, since ϕ only maps the identity map to $\bar{0}$, so its kernel is trivial. It is surjective, since both groups contain the same number of elements. □

Note that the proof is a bit sketched. For another fully elementary proof see [6].

3.5 The inverse Galois problem for abelian groups

In this last section, we can finally prove, using what we established in the previous sections, the following theorem

Theorem 28. *Every finite abelian group A is isomorphic to the Galois group $Gal_{\mathbb{Q}}(K)$ for some Galois extension $K|\mathbb{Q}$.*

Proof. Let A be a finite abelian group. Then, obviously, A is also finitely generated and with the use of proposition 21, we can state that there exists $r \geq 0$ and a unique sequence $(d_1, ..., d_m)$ with all the $d_i \in \mathbb{Z}_{>1}$ and $d_m | d_{m-1} | ... | d_1$ such that

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_m\mathbb{Z}.$$

Note that $r = 0$ in this case, since A is finite and $\mathbb{Z}^r$ is infinite for $r > 0$. Hence

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_m\mathbb{Z}.$$

Choose different $p_i \equiv 1 \bmod d_i$. The existence of such different p_i guaranteed by theorem 17. Now, we see that

$$\phi : \mathbb{Z}/(p_i - 1)\mathbb{Z} \to \mathbb{Z}/d_i\mathbb{Z} : \bar{a} \mapsto \bar{a}$$

is a surjective homomorphism, since:

- ϕ is a homomorphism, since for some $\bar{a}, \bar{b} \in \mathbb{Z}/(p_i - 1)\mathbb{Z}$

$$\phi(\bar{a} + \bar{b}) = \overline{a + b} = \phi(\bar{a}) + \phi(\bar{b}).$$

- for every $\bar{c} \in \mathbb{Z}/d_i\mathbb{Z}$, we can pick $\bar{c} \in \mathbb{Z}/(p_i - 1)\mathbb{Z}$ such that $\phi(\bar{c}) = \bar{c}$, since $p_i - 1 \equiv 0 \bmod d_i$.

Taking products gives a surjective homomorphism

$$\prod_{i=1}^{m} \mathbb{Z}/(p_i - 1)\mathbb{Z} \to A.$$

Furthermore, we see by proposition 24 that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic and with proposition 22

$$\mathbb{Z}/(p_i - 1)\mathbb{Z} \cong (\mathbb{Z}/p_i\mathbb{Z})^*.$$

So if we combine the results, we see by the Chinese remainder theorem, which can also be found in [9] that we have a surjective homomorphism

$$\Phi : (\mathbb{Z}/n\mathbb{Z})^* \to A,$$

for $n = p_1 \cdot ... \cdot p_m$.
What we have proven so far can be displayed as follows

$$\begin{tikzcd}
A \arrow[r, leftrightarrow] & \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_m\mathbb{Z} \\
 & \mathbb{Z}/(p_1 - 1)\mathbb{Z} \times ... \times \mathbb{Z}/(p_m - 1)\mathbb{Z} \arrow[u, two heads, "\phi"] \\
(\mathbb{Z}/n\mathbb{Z})^* \arrow[r, leftrightarrow] \arrow[uu, two heads, "\Phi"] & (\mathbb{Z}/p_1\mathbb{Z})^* \times ... \times (\mathbb{Z}/p_m\mathbb{Z})^* \arrow[u, leftrightarrow]
\end{tikzcd}$$

Define the kernel of Φ to be H. Then we know from basic group theory that

$$A \cong (\mathbb{Z}/n\mathbb{Z})^*/H.$$

We now only have to find a Galois extension with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*/H$ and then we are done.

We know from proposition 27 that the Galois extension $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ has Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. By the fundamental theorem of Galois theory, we can deduce, since H is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ that it corresponds to the subextension $\mathbb{Q}(\zeta_n)^H$ such that

$$\mathrm{Gal}_{\mathbb{Q}(\zeta_n)^H}(\mathbb{Q}(\zeta_n)) = H.$$

Since H is a normal subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ ($(\mathbb{Z}/n\mathbb{Z})^*$ is abelian), we can say by proposition 26 that we found the Galois extension $\mathbb{Q}(\zeta_n)^H|\mathbb{Q}$ with Galois group

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)^H) \cong \frac{\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))}{\mathrm{Gal}_{\mathbb{Q}(\zeta_n)^H}(\mathbb{Q}(\zeta_n))} = \frac{(\mathbb{Z}/n\mathbb{Z})^*}{H} \cong A.$$

This last part of the proof can be displayed in the following diagram containing the discussed Galois extensions of $\mathbb{Q}$ and their Galois groups as a label on the lines between them.

$$\begin{tikzcd}
\mathbb{Q}(\zeta_n) \arrow[dd, dash, "(\mathbb{Z}/n\mathbb{Z})^*"'] \arrow[dr, dash, "H"] & \\
& \mathbb{Q}(\zeta_n)^H \arrow[dl, dash, "(\mathbb{Z}/n\mathbb{Z})^*/H"] \\
\mathbb{Q} &
\end{tikzcd}$$

□

Chapter 4

The symmetric group

So far we were able to solve the inverse Galois problem for abelian groups. In this chapter we will look at the inverse Galois problem for the symmetric group S_n and we will solve it. For n being 1 or 2, this group is abelian, so we will look at the case where $n > 2$. We will first show, given some n, the existence of a polynomial in $\mathbb{Q}[X]$ with S_n as Galois group and after that, using Hilbert's irreducibility theorem, we will proof for the specific polynomial

$$f(X) = X^n - sX - s \in \mathbb{Q}[X]$$

that its Galois group equals S_n for infinitely many $s \in \mathbb{Q}$. This property of $f(X)$ also appears to be useful in the proof of the inverse Galois problem for the alternating group A_n in the next chapter.

4.1 The existence of polynomials with symmetric Galois group

We will show in this section the existence of a polynomial in the polynomial ring $\mathbb{Q}[X]$ with Galois group over $\mathbb{Q}$ equal to S_n for some given $n > 2$. The proof can be used to construct the polynomial for a given n. A part of this proof can be found in [8].

Proposition 29. *For every $n \in \mathbb{Z}_{>2}$, there exists a polynomial $f(X) \in \mathbb{Q}[X]$ such that $Gal_{\mathbb{Q}}(f) \cong S_n$.*

Proof. We are given some $n \in \mathbb{Z}_{>2}$.
As earlier mentioned in the proof of lemma 13, we know that, for any prime number p and any positive integer m, $\mathbb{F}_{p^m} = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_{p^m}$ with minimal polynomial over $\mathbb{F}_p$ of degree m. This shows, for any given integer m and any prime number p, the existence of an irreducible polynomial of degree m in $\mathbb{F}_p[X]$.
Using this result, now choose the following polynomials of degree n

- $f_1(X) \in \mathbb{F}_2[X]$, which is irreducible

- $f_2(X) \in \mathbb{F}_3[X]$, which has irreducible factors of degree $n-1$ and 1
- $f_3(X) \in \mathbb{F}_5[X]$, which has irreducible factors of degree 2 and one or two irreducible factors of odd degree. If n is even, choose the factors to have degree $2, n-3$ and 1 and if n is odd, choose the factors to have degree 2 and $n-2$.

Finally choose $f(X) \in \mathbb{Z}[X]$ such that

$$\begin{aligned} f \bmod 2 &= f_1 \\ f \bmod 3 &= f_2 \\ f \bmod 5 &= f_3. \end{aligned}$$

This is always possible. For example, if we define f_1', f_2' and f_3' to be polynomials obtained by changing the coefficients $\bar{\alpha}_i$ in f_1, f_2 and f_3 to $\alpha_i \in \mathbb{Z}$, then

$$f = 15f_1' + 10f_2' + 6f_3'$$

would be sufficient. In this way we constructed a polynomial which is irreducible over $\mathbb{Q}$, since f mod 2 is irreducible over $\mathbb{F}_2$. By the fact that an irreducible polynomial over a field of characteristic zero does not have multiple roots, we know the splitting field of f is a Galois extension of $\mathbb{Q}$. Now by proposition 4, we know the Galois group $\mathrm{Gal}_{\mathbb{Q}}(f)$ is transitive. Furthermore, we see that f_2 and f_3 do not contain any multiple roots. This is the case, since the irreducible factors of the two polynomials do not contain multiple roots, because they are irreducible over a finite field. We now also see, by theorem 14, that $\mathrm{Gal}_{\mathbb{Q}}(f)$ must contain a $(n-1)$-cycle and a $(n-2,2)$-cycle or a $(n-3,2)$-cycle depending on whether n is even or odd. As earlier seen as an example in example 15, the existence of a $(n-1)-$cycle in $\mathrm{Gal}_{\mathbb{Q}}(f)$ together with its transitivity means that $\mathrm{Gal}_{\mathbb{Q}}(f)$ is doubly transitive (by proposition 7). By raising the $(n-2,2)$-cycle or $(n-3,2)$-cycle to respectively the power $n-2$ or $n-3$, we also obtain a transposition in $\mathrm{Gal}_{\mathbb{Q}}(f)$. Therefore, we conclude by proposition 10 that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_n$. □

4.2 Hilbert's irreducibility theorem and Newton's method

Before we are able to prove that the polynomial $f(X) = X^n - sX - s$, as defined earlier in the introduction of this chapter, has Galois group S_n, we will need to introduce two different notions. The first one is a famous theorem of Hilbert. This theorem together with a proof are found in [11]. The proof is extensive and uses material beyond the scope of this thesis, so we skipped it.

Theorem 30. (Hilbert's irreducibility theorem) *Suppose the polynomial $f(X, t_1, ..., t_n) \in \mathbb{Q}[X, t_1, ..., t_n]$ is irreducible. Then there exists an infinite number of n-tuples $(a_1, ..., a_n) \in \mathbb{Q}^n$ such that $Gal_{\mathbb{Q}}(f(X, a_1, ..., a_n) \cong Gal_{\mathbb{Q}(t)}(f(X, t_1, ..., t_n))$. In particular, for such $a_1, ..., a_n$, $f(X, a_1, ..., a_n)$ is irreducible over $\mathbb{Q}$.*

Application 31. As an example of the way we will apply Hilbert's irreducibility theorem later on, we will first look which subgroups of the automorphism group $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$, for transcendental t, appear as Galois groups of subextensions of $\mathbb{Q}(t)|M$ for some ground field M. After that we will discuss an example of the way we can establish a Galois extension with such a subgroup as a Galois group. In the example, we will use Hilbert's irreducibility theorem.
Now,

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t)) = \left\{ \phi_{a,b,c,d} : \mathbb{Q}(t) \to \mathbb{Q}(t) : t \mapsto \frac{at+b}{ct+d} \middle| a,b,c,d \in \mathbb{Q}, \text{ where } ad-bc \neq 0 \right\},$$

so every element in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$ is determined by the constants a, b, c and d. Furthermore, we can introduce the map

$$\psi : \mathrm{GL}_2(\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t)) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \phi_{a,b,c,d},$$

which is surjective. It is also a homomorphism, since for

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}) :$$

$$\begin{aligned}
\psi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) &= \psi \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+c'd & cb'+dd' \end{pmatrix} \\
&= \phi_{aa'+bc',ab'+bd',ca'+c'd,cb'+dd'} : t \mapsto \frac{(aa'+bc')t+ab'+bd'}{(ac'+c'd)t+cb'+dd'} \\
&= \phi_{a,b,c,d} \circ \phi_{a',b',c',d'} : t \mapsto \frac{a\left(\frac{a't+b'}{c't+d'}\right)+b}{c\left(\frac{a't+b'}{c't+d'}\right)+d} \\
&= \psi \begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ \psi \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.
\end{aligned}$$

Note that the kernel of ψ is equal to $\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} | a \in \mathbb{Q}^* \right\}$. Since we are looking for finite subgroups of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$, we are interested in elements in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$ with a finite order. These elements generate such subgroups. Once we know which finite orders are possible in the group $\mathrm{GL}_2(\mathbb{Q})$, we know, because of the existence of ψ, which finite orders are possible in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$. Namely, if $A \in\mathrm{GL}_2(\mathbb{Q})$ has order k, then

$$\mathrm{Id}_{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))} = \psi(I) = \psi(A^k) = \psi(A)^k,$$

so the order of $\psi(A)$ is a divisor of k. Since ψ is surjective, the possible finite orders of elements in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$ are divisors of the possible finite orders of elements in $\mathrm{GL}_2(\mathbb{Q})$. In [12] we found an extensive description of the fact that the only possible finite orders of elements in $\mathrm{GL}_2(\mathbb{Q})$ are 1,2,3,4 and 6. The author uses cyclic decompositions and the similarity of matrices to prove it. We will not repeat his argument. The possible finite orders of elements in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$ are therefore divisors of 1,2,3,4 and 6. The question is whether all divisors appear as order of such an element. Well, one can determine that

$$\phi_{0,1,0,1}\ ,\ \phi_{0,1,1,0}\ ,\ \phi_{0,1,-1,1}\ ,\ \phi_{2,3,-4/3,2} \text{ and } \phi_{3,2,-3/2,3}$$

respectively have order 1,2,3,4 and 6, so that is the case. Let us now consider S_3, which is a subgroup of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$. This group is generated by a 3-cycle and a 2-cycle. We can consider the automorphisms in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$

$$\rho : \mathbb{Q}(t) \to \mathbb{Q}(t) : t \mapsto \frac{1}{1-t}$$
$$\sigma : \mathbb{Q}(t) \to \mathbb{Q}(t) : t \mapsto \frac{1}{t}$$

as respectively the cycles $(0 \quad 1 \quad \infty)$ and $(0 \quad \infty)$ acting on the projective line $\mathbb{P}^1(\mathbb{Q})$. This implies that ρ and σ together generate S_3. By the fundamental theorem of Galois theory, we now know that

$$S_3 \cong Gal_{\mathbb{Q}(t)^{<\rho,\sigma>}}(\mathbb{Q}(t)).$$

We will determine $\mathbb{Q}(t)^{<\rho,\sigma>}$. We compute

$$\rho^2(t) = \rho(\frac{1}{1-t}) = \frac{t-1}{t}$$

and determine the generator of $\mathbb{Q}(t)^{<\rho>}$ to be

$$u := t + \rho(t) + \rho^2(t) = t + \frac{1}{1-t} + \frac{t-1}{t} = \frac{t^3-3t+1}{t^2-t}.$$

We continue with computing the generator of $\mathbb{Q}(t)^{<\rho,\sigma>}$ to be

$$v := u \cdot \sigma(u) = u \cdot \frac{1/t^3 - 3/t + 1}{1/t^2 - 1/t} = u \cdot \left(-\frac{t^3-3t+1}{t^2-t} + \frac{3t^2-3t}{t^2-t} \right) = u \cdot (3-u) = 3u - u^2.$$

This implies that $\mathbb{Q}(t)^{<\rho,\sigma>} = \mathbb{Q}(v)$ and $\mathbb{Q}(t)$ is a Galois extension of $\mathbb{Q}(v)$ obtained by adjoining the roots of the polynomial

$$f(v,X) = X^6 - 3X^5 + (v-3)X^4 + (11-2v)X^3 + (v-3)X^2 - 3X + 1 \in \mathbb{Q}(v)[X],$$

where $f(v, X)$ is obtained by replacing t by X in the factor $3u - u^2 - v$ and rearranging. $f(v, X)$ is irreducible over $\mathbb{Q}(v)$, since otherwise t would be a root of a polynomial with degree lower then 6, but

$$[\mathbb{Q}(t) : \mathbb{Q}(v)] = \#\mathrm{Gal}_{\mathbb{Q}(v)}(\mathbb{Q}(t)) = \#S_3 = 6,$$

since $\mathbb{Q}(t)|\mathbb{Q}(v)$ is Galois.
Now, we will finally use Hilbert's irreducibility theorem to conclude that there is an infinite number of constants $c \in \mathbb{Q}$ we can substitute for v in $f(v, X)$ such that $f(c, X)$ is irreducible over $\mathbb{Q}$. For such a c, this implies that $t \notin \mathbb{Q}$, which is now a root of $f(c, X) \in \mathbb{Q}[X]$. With the use of [11], we can also say that there is an infinite number of values $c \in \mathbb{Q}$ we can substitute for v, such that

$$\mathrm{Gal}_{\mathbb{Q}}(f(c, X)) = \mathrm{Gal}_{\mathbb{Q}(v)}(\mathbb{Q}(t)) \cong S_3,$$

so we found a Galois extension with Galois group isomorphic to S_3.

We will now, surprisingly, continue to a numerical method called Newton's method, used for finding roots of functions, to help us with the upcoming proof. We got this method from [13]. We skipped the rather technical proof of the fact it converges.

Newton's Method. Suppose we have a continuously differentiable function $f : \mathbb{R} \to \mathbb{R}$ for which $f'(x) \neq 0$ with a root and a good approximation z_0 of it. Then, the following iteration, for $n \geq 0$, will converge to the actual root of f

$$z_n = z_{n-1} - \frac{f(z_{n-1})}{f'(z_{n-1})}.$$

4.3 Specific polynomials with symmetric Galois group

Before proving what we want to prove about our specific $f(X, s)$, we will need a lemma about elements in the ring of formal power series

$$\mathbb{Q}[[X]] = \left\{ \sum_{i=0}^{\infty} a_i X^i | a_i \in \mathbb{Q} \right\}$$

concerning the question when those are units.

Lemma 32. *An element $\sum_{i=0}^{\infty} a_i X^i \in \mathbb{Q}[[X]]$ belongs to $(\mathbb{Q}[[X]])^*$ if and only if $a_0 \neq 0$.*

Proof. Take some element $\alpha = \sum_{i=0}^{\infty} a_i X^i \in \mathbb{Q}[[X]]$. We want to construct an inverse of α. We take the element $\beta = \sum_{j=0}^{\infty} b_j X^j \in \mathbb{Q}[[X]]$ and multiply α with it to get

$$\alpha \cdot \beta = \sum_{i=1}^{\infty} a_i X^i \cdot \sum_{j=1}^{\infty} b_j X^j = \sum_{n=0}^{\infty} c_n X^n$$

with

$$c_n = \sum_{\substack{i,j\in\{0,\dots,n\}\\ i+j=n}} a_i b_j.$$

We want to check whether we can find coefficients b_j such that $c_0 = 1$ and $c_n = 0$ for $n \in \mathbb{Z}_{>0}$.
Suppose now $a_0 = 0$. Then we see that

$$c_0 = a_0 b_0 = 0, \text{ so } \alpha \notin (\mathbb{Q}[[X]])^*.$$

Suppose conversely that $a_0 \neq 0$. Then $a_0 \in \mathbb{Q}^*$, so pick

$$b_0 = a_0^{-1}, \text{ to obtain } c_0 = a_0 b_0 = a_0 a_0^{-1} = 1.$$

Furthermore, pick for n not equal to zero:

$$b_n = -a_0^{-1}\Big(\sum_{\substack{i\in\{1,\dots,n\}\\ j\in\{0,\dots,n\}\\ i+j=n}} a_i b_j \Big)$$

to obtain

$$\begin{aligned} c_n &= \sum_{\substack{i,j\in\{0,\dots,n\}\\ i+j=n}} a_i b_j \\ &= a_0 b_n + \sum_{\substack{i\in\{1,\dots,n\}\\ j\in\{0,\dots,n\}\\ i+j=n}} a_i b_j \\ &= a_0 \cdot \Big(- a_0^{-1} \Big(\sum_{\substack{i\in\{1,\dots,n\}\\ j\in\{0,\dots,n\}\\ i+j=n}} a_i b_j \Big)\Big) + \sum_{\substack{i\in\{1,\dots,n\}\\ j\in\{0,\dots,n\}\\ i+j=n}} a_i b_j \\ &= 0. \end{aligned}$$

We conclude that we found an inverse β for α, so $\alpha \in (\mathbb{Q}[[X]])^*$ □

We will now continue to prove the following proposition. A sketch, but incomplete proof of this proposition can be found in [14]. We included a full elaborated proof.

Proposition 33. *For an infinite number of rational numbers $s \in \mathbb{Q}$ the polynomial $f(X) = X^n - sX - s \in \mathbb{Q}[X]$ with splitting field L over $\mathbb{Q}$ is such that $L|\mathbb{Q}$ is Galois with $Gal_{\mathbb{Q}}(f) \cong S_n$.*

Proof. We begin this proof with letting s be a transcendental variable over $\mathbb{Q}$. So we have that

$$f(X, s) = X^n - sX - s \in \mathbb{Z}[X, s].$$

By the well-known Eisenstein criterion, we see it is irreducible over $\mathbb{Q}(s)$. For the irreducible element s in $\mathbb{Z}[s]$ divides all but the first coefficient, but $s^2 \nmid (-s)$. Because it is irreducible over a field of characteristic zero, it doesn't have multiple roots and the splitting field of f is a Galois extension of $\mathbb{Q}(s)$ by proposition 2.
We will now prove that $\mathrm{Gal}_{\mathbb{Q}(s)}(f(X, s)) \cong S_n$.
We want to do that with the use of proposition 10, so we need to check that the Galois group is doubly transitive, transitive and contains a transposition. We begin with checking transitivity and doubly transitivity.
By proposition 4, we know immediately that $\mathrm{Gal}_{\mathbb{Q}(s)}(f(X, s))$ is transitive, since it is irreducible. Furthermore, we can rewrite $f(X, s)$ in the way

$$f(X, s) = X^n - X/2 - 1/2 - (s - 1/2)(X + 1)$$

such that for $r = s - 1/2$:

$$f(X, r) = X^n - X/2 - 1/2 - r(X + 1) \in \mathbb{Q}[X, r].$$

We see that if we fill in $r = 0$ in $f(X, r)$ we can factorize

$$f(X, 0) = X^n - X/2 - 1/2 = 1/2(X - 1)(2X^{n-1} + ... + 2X + 1).$$

If we look at the polynomial

$$g(X) = X^{n-1} + 2X^{n-2} + ... + 2X + 2 \in \mathbb{Z}[X],$$

we see that it is irreducible over $\mathbb{Q}$ by the Eisenstein Criterion. Therefore the polynomial

$$h(X) = X^{n-1} \cdot g(1/X) = X^{n-1} \cdot (X^{-n+1} + 2X^{-n+2} + ... + 2X^{-1} + 2) = 1 + 2X + ... + 2X^{n-1},$$

which is the second term of the factorization of $f(X, 0)$, is also irreducible over $\mathbb{Q}$. We see, therefore, that $f(X, 0)$ only has one root, $X = 1$, in $\mathbb{Q}$.
Let's now take a look at the fraction field of the ring of formal power series $\mathbb{Q}[[r]]$, denoted as $\mathbb{Q}((r))$. The polynomial $f(X, r)$ can have at most one root in this ring, since a root of $f(X, r)$ in $\mathbb{Q}((r))$ implies a root of $f(X, 0)$ in $\mathbb{Q}$ and we just saw $f(X, 0)$ only has one root. We are going to find this root with Newton's method for the function

$$f(x) = x^n - 1/2x - 1/2 - r(x + 1)$$

with derivative

$$f'(x) = nx^{n-1} - 1/2 - r.$$

Note that this derivative does not vanish at a point. For if we take $x = a_{-m}r^{-m} + ... \in \mathbb{Q}((r))$, it would mean

$$x^{n-1} = r^{m(n-1)}(a_{-m} + a_{-m+1}r + ...)^{n-1} = \frac{1}{2n} + \frac{1}{n}r,$$

so $m = 0$. But then x^{n-1} is never of degree 1, since $n > 2$.
Our first guess of the root of $f(X,r)$ in $\mathbb{Q}((r))$ is the root $x = 1$ of $f(X,0)$, which is a good guess, since the root we are looking for equals it for $r = 0$. The iteration becomes

$$\begin{aligned}
z_0 &= 1 \\
z_1 &= 1 - \frac{f(1,r)}{f'(1,r)} = 1 + \frac{2r}{n-1/2-r} \\
z_2 &= 1 + \frac{2r}{n-1/2-r} - \frac{f(1+\frac{2r}{n-1/2-r}, r)}{f'(1+\frac{2r}{n-1/2-r}, r)} \\
&= 1 + \frac{2r}{n-1/2-r} - \frac{(1+\frac{2r}{n-1/2-r})^n - 1 - \frac{r+2r^2}{n-1/2-r} - 2r}{n(1+\frac{2r}{n-1/2-r})^n - 1/2 - r} \\
&\vdots
\end{aligned}$$

We see that the denominators of the fractions appearing in the iteration all have a nonzero constant term. This remains unchanged if we iterate further. Therefore, by lemma 32, we conclude all iterations are in the field $\mathbb{Q}((r))$. Thus, since this method converges, we found a root $\alpha \in \mathbb{Q}((r))$ of $f(X,r)$ of the form

$$\alpha = 1 + \sum_{i=1}^{\infty} a_i r^i$$

for some indices $a_i \in \mathbb{Q}$.
We see the polynomial $f(X,r)$ has the form

$$f(X,r) = (X-\alpha)g(X,r) \in \mathbb{Q}((r))[X]$$

for some polynomial $g(X,s)$ of degree $n-1$. This polynomial $g(X,r)$ is irreducible over $\mathbb{Q}((r))$, because we see $g(X,1/2)$ equals $1/2 \cdot h(X)$ for the irreducible polynomial $h(X)$ as earlier defined. Therefore the splitting field of $g(X,r)$ over $\mathbb{Q}((r))$, which we call M is a Galois extension. We call K the splitting field of $f(X,s)$ over $\mathbb{Q}(s)$. Now note that $K \subset M$, since $\mathbb{Q}(s) \subset \mathbb{Q}((r))$. Therefore we can build an injective map

$$\mathrm{Gal}_{\mathbb{Q}((r))}(M) \to \mathrm{Gal}_{\mathbb{Q}(s)}(K) : \sigma \to \sigma|_K,$$

which implies that, since $g(X,r)$ is irreducible of degree $n-1$, that K contains an $(n-1)$-cycle. Therefore, $\mathrm{Gal}_{\mathbb{Q}(s)}(K)$ is doubly transitive.

We will now prove that $\mathrm{Gal}_{\mathbb{Q}(s)}(f(X,s))$ contains a transposition.
We use the scaling $Y = \frac{1-n}{n}X$ to rewrite

$$f(X,s) = \frac{n^n}{(1-n)^n}Y^n - \frac{sn}{1-n}Y - s.$$

This polynomial is a multiple of

$$Y^n - \frac{s(1-n)^{n-1}}{n^{n-1}}Y - \frac{s(1-n)^n}{n^n}.$$

Using the substitution $t = \frac{(1-n)^{n-1}}{n^n}s$ we obtain the polynomial

$$g(Y,t) = Y^n - ntY + (n-1)t$$

which can be written as

$$g(Y,u) = Y^n - Y - (n-1)(Y-1) + u(-nY + n - 1) \in \mathbb{Q}[Y,u]$$

for $u = t - 1$. If we now look at the polynomial

$$g(Y,0) = Y^n - nY + n - 1,$$

we know that if it has multiple roots, then these roots are also roots of the derivative

$$g'(Y,0) = nY^{n-1} - n.$$

Suppose we have a root c of $g'(Y,0)$. This means

$$g'(c,0) = nc^{n-1} - n = 0 \iff c^{n-1} = 1.$$

We now see

$$g(c,0) = c^n - nc + n - 1 = c - nc + n - 1 = (n-1)(1-c) = 0 \iff c = 1,$$

so $g(Y,0)$ only has one multiple root, namely $Y = 1$. If this root would have a higher multiplicity then 2, we know that it should also be a root of $g''(Y,0)$. We compute

$$g''(1,0) = n(n-1)1^{n-2} = n(n-1) \neq 0,$$

which implies that $g(Y,0)$ has one double root at $Y = 1$ and $n-2$ simple roots.
This means that in the splitting field K of $g(Y,0)$ over $\mathbb{Q}$ we have that

$$g(Y,0) = (Y-1)^2(Y-\alpha_1)(Y-\alpha_2)...(Y-\alpha_{n-2})$$

for different roots $\alpha_i \in K$. Now we can use Newton's method again to find the roots corresponding to α_i of the function $g(Y,u)$ in the field $K((u))$. Because $g(Y,u)$ is very similar to $f(X, r)$, for which we proved Newton's method provides a way to find roots in $\mathbb{Q}((r))$, we will not repeat the whole argument about Newtons method for $g(Y, u)$. So we find roots

$$\alpha'_i = \alpha_i + \sum_{j=1}^{\infty} d_j u^j \in K((u))$$

for $g(Y, u) \in K((u))[Y]$. The question remains whether $g(Y, u)$ also has a roots in $K((u))$ corresponding to the double root 1 of $g(Y, 0)$. We know this root should be of the form

$$\gamma = 1 + \sum_{i=1}^{\infty} \delta_i u^i$$

for $\delta_i \in K$. We also know that this root γ of $g(Y, u)$ in $K((u))$ implies the root $\bar{\gamma}$ of $\overline{g(Y, u)}$ in $K((u))/(u^2)$, so let's check whether $\bar{\gamma}$ is a root of $\overline{g(Y, u)} \in K((u))/(u^2)[Y]$:

$$\begin{aligned}
\overline{g(\bar{\gamma}, u)} &= \bar{\gamma}^n - \bar{\gamma} - (n-1)(\bar{\gamma} - 1) + u(-n\bar{\gamma} + n - 1) \\
&= (1 + \delta_1 u)^n - (1 + \delta_1 u) - (n-1)((1 + \delta_1 u) - 1) + u(-n(1 + \delta_1 u) + n - 1) \\
&= 1 + n\delta_1 u - 1 - \delta_1 u - (n-1)\delta_1 u - nu + nu - u \\
&= -u
\end{aligned}$$

It is not the case, hence $g(Y, u)$ does not have a root in $K((u))$ corresponding to the double root 1 of $g(Y, 0)$. Hence, we can write

$$g(Y, u) = h(Y, u)(Y - \alpha'_1)...(Y - \alpha'_{n-2}) \in K((u))[Y]$$

for some quadratic irreducible polynomial $h(Y, u)$. Define the splitting field of $g(Y, u)$ to be L. Then $L|K((u))$ is a Galois extension, since $h(Y, u)$ is irreducible (proposition 4), and therefore $\mathrm{Gal}_{K((u))}(L)$ contains a unique automorphism τ which is the identity map on $K((u))$ (and therefore the identity map on the roots α'_i) and which switches the 2 roots of $h(Y, u)$. Since, by similar arguments as for $\mathbb{Q}((s))$ and $\mathbb{Q}((r))$ and we have that $g(Y, t)$ is just a rescaling of $f(X, s)$, we know now that the transposition τ is also in $\mathrm{Gal}_{\mathbb{Q}(s)}(f(X, s))$. We conclude with proposition 10 that

$$\mathrm{Gal}_{\mathbb{Q}(s)}(f(X, s)) \cong S_n.$$

Now that we have this result, we use Hilbert's irreducibility theorem to derive that there is an infinite number of rational numbers k such that $f(X, k)$ is irreducible. For all such k this means that the roots of the polynomial $f(X) := f(X, k)$ are not in $\mathbb{Q}$ and that f will have Galois group

$$\mathrm{Gal}_{\mathbb{Q}}(f) = \mathrm{Gal}_{\mathbb{Q}(s)}(f(X, s)) \cong S_n.$$

□

Chapter 5

The alternating group

This chapter is devoted to finding polynomials with the alternating Galois group A_n. We found in the previous chapter that for an infinite number of rational numbers t, the polynomial

$$g(Y) = Y^n - ntY - (n-1)t \in \mathbb{Q}[Y]$$

has Galois group over $\mathbb{Q}$ equal to S_n. We will prove in this chapter that there is also an infinite number of rational numbers t such that the Galois group of $g(Y)$ over $\mathbb{Q}$ equals A_n. We will first introduce the notion of the discriminant of a polynomial and the properties it has.

5.1 The discriminant of a polynomial

We will use the following notation in definition 34 and proposition 35.
Let $f(X) \in K[X]$ be a monic polynomial of degree $n \geq 1$ over a field K with splitting field L over K. This means we are talking about a polynomial

$$f(X) = \sum_{i=1}^{n} a_i X^i = \sum_{i=1}^{n} (X - \alpha_i) \in L[X]$$

with $a_i \in K$, $\alpha_i \in L$ and $a_n = 1$. Then we define the discriminant of f to be the following [6].

Definition 34. The *discriminant* of f is

$$\text{disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

We will continue with an important property of the discriminant. The proposition with a proof can be found in [6]. We adapted the proof and added some important details.

Proposition 35. *disc*$(f) \in K$

Proof. It is clear that if f has a multiple root, then disc$(f) = 0 \in K$. We assume f does not, which means $L|K$ is a Galois extension. Now take some nontrivial automorphism $\sigma \in \mathrm{Gal}_K(L)$. Since $\mathrm{Gal}_K(L)$ is isomorphic to a subgroup of S_n, we can see σ as a cycle which permutes the roots, α_i, of f.
We introduce the element

$$\delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)$$

which is the square root of disc(f).
Now, σ can be written as a product of transpositions. Without loss of generality we can assume such a transposition looks like $\tau = (\alpha_k \quad \alpha_l)$ with $k, l \in \{1, ..., n\}$ and $k < l$. It holds that $\tau(\delta(f)) = -\delta(f)$, since

$$\begin{aligned}
&\tau(\alpha_k - \alpha_l) = -(\alpha_k - \alpha_l) \\
&\tau(\alpha_i - \alpha_j) = (\alpha_i - \alpha_j) \text{ for } i \text{ and } j \text{ both different from } k \text{ and } l \\
&\tau(\alpha_i - \alpha_j) = -(\alpha_i - \alpha_j) \text{ when } \{i, j\} = \{k, a\} \text{ or } \{i, j\} = \{l, a\} \text{ for } k < a < l
\end{aligned}$$

and there is an even number of elements $(\alpha_i - \alpha_j)$ in $\delta(f)$ such that $\{i, j\} = \{k, a\}$ or $\{i, j\} = \{l, a\}$ with $k < a < l$. Therefore

$$\sigma(\delta(f)) = \mathrm{sgn}(\sigma)\delta(f),$$

which means that

$$\sigma(\mathrm{disc}(f)) = \sigma(\delta(f)^2) = (\sigma(\delta(f)))^2 = (\mathrm{sgn}(\sigma)\delta(f))^2 = \mathrm{disc}(f).$$

We conclude, since disc(f) is invariant under every automorphism of $\mathrm{Gal}_K(L)$ that disc$(f) \in K$. □

It is not very easy to compute the discriminant of a polynomial. It seems, according to definition 34, that you need to know the roots of the polynomial. However, we found the following formula for computing the discriminant of a trinomial in [15] which only uses the constants appearing in the trinomial. This formula will prove to be useful in the next section. An extensive proof can be found in [15]. It is rather technical and a bit involved so we omitted it.

Proposition 36. *Let K be a field and $f(X) = X^n + AX^k + B \in K[X]$ a trinomial with $A, B \in K$ and $n > k$ both positive integers. Assume the characteristic of K doesn't divide $n(n-k)$ and let d equal gcd$(n, n-k)$. Then the discriminant of f is given by*

$$disc(f) = n^n(-1)^{\frac{n(n-1)}{2}} B^{k-1} \left(B^{\frac{n-k}{d}} - (-1)^{\frac{n}{d}} A^{\frac{n}{d}} \left(1 - \frac{k}{n}\right)^{\frac{n-k}{d}} \left(\frac{k}{n}\right)^{\frac{k}{d}} \right)^d.$$

5.2 Specific polynomials with alternating Galois group

With help of the previous chapter and the previous section we are now able to prove the following proposition. A sketch of this proof can be found in [14] and some small implications in [6]. We included a fully elaborated proof.

Proposition 37. *For an infinite number of rational numbers $t \in \mathbb{Q}$ the polynomial*

$$g(Y) = Y^n - ntY - t(n-1) \in \mathbb{Q}[Y]$$

with splitting field L over $\mathbb{Q}$ is such that $L|\mathbb{Q}$ is Galois with $Gal_{\mathbb{Q}}(g) \cong A_n$.

Proof. Let's begin with looking at the polynomial

$$g = g(Y,t) = Y^n - ntY - t(n-1) \in \mathbb{Q}(t)[Y]$$

for transcendental t over $\mathbb{Q}$. We know by the proof of proposition 33 that for the splitting field L of g over $\mathbb{Q}(t)$ it holds that $L|\mathbb{Q}(t)$ is Galois with Galois group $\mathrm{Gal}_{\mathbb{Q}(t)}(L) \cong S_n$.
We will compute $\mathrm{disc}(g)$ with proposition 36.
In this case $k = 1$, $A = -nt$, $B = t(n-1)$,

$$d = \gcd(n, n-k) = \gcd(n, n-1) = \gcd(n, -1) = 1$$

and the characteristic of $\mathbb{Q}(t)$ which is zero does not divide $n(n-1)$. We see

$$\begin{aligned}\mathrm{disc}(g) &= n^n(-1)^{\frac{n(n-1)}{2}}\left((t(n-1))^{n-1} - (-1)^n(-nt)^n\left(1-\frac{1}{n}\right)^{n-1}\frac{1}{n}\right)\\ &= n^n(-1)^{\frac{n(n-1)}{2}}\left(t^{n-1}(n-1)^{n-1} - n^n t^n \frac{(n-1)^{n-1}}{n^n}\right)\\ &= n^n(-1)^{\frac{n(n-1)}{2}}(n-1)^{n-1}t^{n-1}(1-t).\end{aligned}$$

We will introduce a substitution for t in terms of the variable u^2 depending on whether n is odd or even. This means that $\mathbb{Q}(u^2) = \mathbb{Q}(t)$ and therefore $\mathrm{Gal}_{\mathbb{Q}(u^2)}(L) \cong S_n$. Furthermore, consider the field $\mathbb{Q}(u^2, \delta(g))$ with $\delta(g)$ the square root of the $\mathrm{disc}(g)$ as before in the proof of proposition 35. This field is a subset of L, since $\delta(g)$ is just an expression in terms of the roots of g. By the fundamental theorem of Galois Theory the subextension $\mathbb{Q}(u^2, \delta(g))|L$ is Galois and we claim

Claim 38. *$Gal_{\mathbb{Q}(u^2,\delta(g))}(L) \cong A_n$.*

Proof. For $\sigma \in S_n \cong \mathrm{Gal}_{\mathbb{Q}(u^2)}(L)$ the following statements are equivalent:

$$\begin{aligned}&\sigma \in A_n,\\ &\sigma(\delta(g)) = \delta(g),\\ &\sigma \in \mathrm{Gal}_{\mathbb{Q}(u^2,\delta(g))}(L).\end{aligned}$$

This completes the proof of the claim. □

Now that we know this, let us introduce the expected substitution for t. Let us first consider the case where n is odd. Then substitute

$$t = 1 - (-1)^{\frac{n(n-1)}{2}} nu^2.$$

to obtain the following expression for the discriminant of g:

$$\begin{aligned}
\operatorname{disc}(g) &= n^n(-1)^{\frac{n(n-1)}{2}}(n-1)^{n-1}t^{n-1}(1-t) \\
&= n^n(-1)^{\frac{n(n-1)}{2}}(n-1)^{n-1}t^{n-1}(1-(1-(-1)^{\frac{n(n-1)}{2}}nu^2)) \\
&= n^n(-1)^{\frac{n(n-1)}{2}}(n-1)^{n-1}t^{n-1}(-1)^{\frac{n(n-1)}{2}}nu^2 \\
&= n^{n+1}(n-1)^{n-1}t^{n-1}u^2.
\end{aligned}$$

If n is even, introduce

$$t = \frac{1}{1+(-1)^{\frac{n(n-1)}{2}}(n-1)u^2}$$

to obtain

$$\begin{aligned}
\operatorname{disc}(g) &= n^n(-1)^{\frac{n(n-1)}{2}}(n-1)^{n-1}t^{n-1}(1-t) \\
&= n^n(-1)^{\frac{n(n-1)}{2}}(n-1)^{n-1}t^{n-1}\left(1 - \frac{1}{1+(-1)^{\frac{n(n-1)}{2}}(n-1)u^2}\right) \\
&= n^n(-1)^{\frac{n(n-1)}{2}}(n-1)^{n-1}t^{n-1}\left(\frac{(1+(-1)^{\frac{n(n-1)}{2}}(n-1)u^2)-1}{1+(-1)^{\frac{n(n-1)}{2}}(n-1)u^2}\right) \\
&= n^n(-1)^{\frac{n(n-1)}{2}}(n-1)^{n-1}t^{n-1}\left(\frac{(-1)^{\frac{n(n-1)}{2}}(n-1)u^2}{1+(-1)^{\frac{n(n-1)}{2}}(n-1)u^2}\right) \\
&= n^n(-1)^{\frac{n(n-1)}{2}}(n-1)^{n-1}t^{n-1}(t(-1)^{\frac{n(n-1)}{2}}(n-1)u^2) \\
&= n^n(n-1)^n t^n u^2.
\end{aligned}$$

This means

$$\delta(g) = \begin{cases} \sqrt{n^{n+1}(n-1)^{n-1}t^{n-1}}u & \text{if } n \text{ is odd} \\ \sqrt{n^n(n-1)^n t^n}u & \text{if } n \text{ is even} \end{cases}$$

We see that

$$\begin{aligned}
\sqrt{n^{n+1}(n-1)^{n-1}t^{n-1}} &\in \mathbb{Q}(u^2) \text{ if } n \text{ is odd} \\
\sqrt{n^n(n-1)^n t^n} &\in \mathbb{Q}(u^2) \text{ if } n \text{ is even,}
\end{aligned}$$

so we can conclude that

$$\mathbb{Q}(u^2, \delta(g)) = \mathbb{Q}(u).$$

With claim 38, we have

$$\mathrm{Gal}_{\mathbb{Q}(u)}(L) \cong A_n.$$

The argument can be summarized in a diagram as follows:

$$\begin{tikzcd}
L \arrow[dd, dash, "S_n"'] \arrow[dr, dash, "A_n"] & \\
& \mathbb{Q}(u^2, \delta(g)) = \mathbb{Q}(u) \arrow[dl, dash] \\
\mathbb{Q}(t) = \mathbb{Q}(u^2) &
\end{tikzcd}$$

With the use of Hilbert's irreducibility theorem we see that there is an infinite number of rational numbers we can substitute for u and with that for t such that g is irreducible over $\mathbb{Q}$ and therefore

$$\mathrm{Gal}_{\mathbb{Q}}(g) \cong A_n.$$

□

Chapter 6

Semidirect Products

Throughout this chapter, we will show that some specific semidirect products appear as the Galois group of a Galois extension of $\mathbb{Q}$. We will show this using the theory of elliptic curves, which we will introduce in the first section.

6.1 Elliptic curves

We start this section with defining an elliptic curve and discussing some notations and properties of it. Before that, we remind the reader that $\mathbb{P}^2$ denotes the projective plane containing points (X, Y, Z) for which two points are considered the same when they are a multiple of each other.

Definition 39. An *elliptic curve* E defined over a field K is the set of points $(X, Y, Z) \in \mathbb{P}^2$ such that

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

with $a_i \in K$, taken such that no point satisfies all derivatives as well.

Following [16], we call the equation of definition 39, the Weierstrass equation. Note that if a point (X, Y, Z) satisfies the Weierstrass equation, then a multiple of it also satisfies the Weierstrass equation, so it makes sense to define the points of E to be in $\mathbb{P}^2$.
Now if $Z = 0$, then we see if we look at the Weierstrass equation that also $X = 0$ and because the points in E are in $\mathbb{P}^2$, $Y \neq 0$. This means there is only one point in E such that $Z = 0$, namely $O = (0, 1, 0)$. For $Z \neq 0$, we can set $Z = 1$ and scale $x = X/Z$ and $y = Y/Z$ to obtain the following (affine) form of the the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Points in E can now also be defined as points $(x, y, 1) \in \mathbb{P}^2$ for which the last form of the Weierstrass equation holds together with the point O at infinity.

A very interesting fact about an elliptic curve E is that we can look at it as a group with zero element O. The group operation '+', can be defined as follows.
Let $P, Q \in E$ and let L be the line connecting P and Q (If $P = Q$, let L be the line tangent to E at P). Let R be the third point of intersection of L with E. This point exists, since the equation of E has degree 3 and a special form of Bezout's theorem (see [16]). Introduce another line L' to be the line connecting R and O. We now define $P + Q$ to be the the third point of intersection of L' and E besides the two intersections R and O.
This whole story is a bit technical, so to get a taste of how to add points on an elliptic curve we included a few pictures below, which shows the method for some different cases for some E defined over the real numbers.

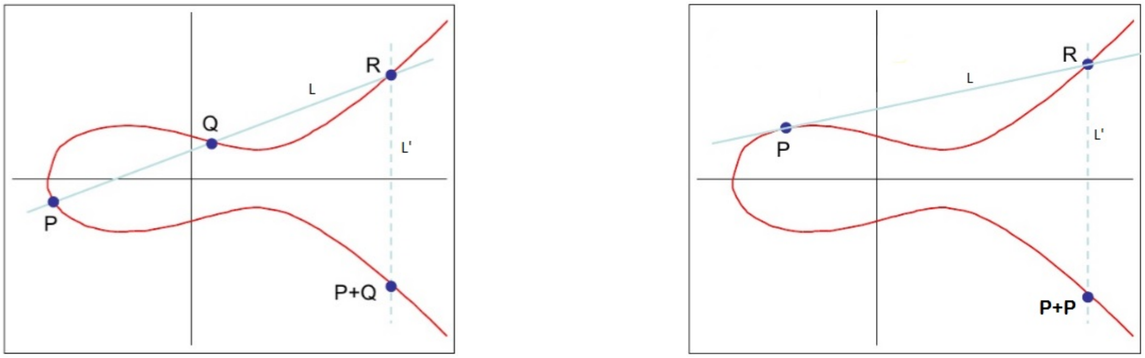


Figure 6.1: Adding points on an elliptic curve

A situation we did not show is the case that L is vertical. Then R equals O, the point at infinity. Furthermore, L' equals the 'line' between O and O and therefore $P + Q = O$. With this group operation, one can deduce that O is indeed the identity element of the group. For let P be a point on E and determine $P + O$. Then we draw a line between P and O and find a third intersection R in E. Now, $P + O$ equals the third intersection of the line between R and O, which is of course again P. So $P + O = P$ and O is the identity element. Furthermore, one can see that $P + (-P) = O$, where we define $-P$ to be the third intersection of the line between P and O, so every element $P \in E$ has an inverse $-P \in E$.
The last thing we need to show in order to conclude that E is a group, is that the group operation is associative. The proof of this statement is a bit involved and we will skip it. For a proof, see [16]. One last interesting observation we can make is that E is a commutative group, since drawing a line between points P and Q is the same as drawing a line between Q and P.

6.2 The m-torsion subgroup of an elliptic curve

In order to discuss the inverse Galois problem for semidirect products, we need to know a bit more about elliptic curves. We start with a definition and continue the section with propositions about a specific elliptic curve which we will use in the next section. In the following definition, let

$$[m]P = P + ...P(m \text{ times}).$$

Definition 40. Let E be an elliptic curve. The *m-torsion subgroup of E* is the subgroup of E containing all points with order equal to m, denoted by

$$E[m] := \{P \in E | [m]P = O\}.$$

It is easy to see this subset forms indeed a subgroup, since $O \in E[m]$ and if $P, Q \in E[m]$, then

$$[m](P + Q) = [m]P + [m]Q = O + O = O$$

and

$$[m](-P) = -[m]P = -O = O,$$

so the inverse of every $P \in E[m]$ is contained in $E[m]$.
Let us take the elliptic curve

$$E : y^2 = x^3 - x.$$

defined over $\mathbb{Q}$ and a prime number $p \equiv 3 \bmod 4$. We will determine $E[p]$ using some lemmas. Fix a point $P = (a, b) \in E[p]$. Now note that we already see for any integer n that $[n]P \in E[p]$, since

$$[p][n]P = [n][p]P = [n]O = O.$$

Therefore,

$$\mathbb{Z}P = \{[n]P | n \in \mathbb{Z}\} \subset E[p].$$

Lemma 41. *The map*

$$\iota : E \to E : (x, y) \mapsto (-x, iy)$$

is an isomorphism

Proof. We start with the remark that this map is well-defined on E, since for $(x, y) \in E$, we see that if we look at the defining equation of E, also $(-x, iy)$ is a point in E.
Proving that ι is a homomorphism requires a lot of effort. We have to distinguish between 5 different situations of addition of points Q and R on E and use a lot of calculations to see whether $\iota(Q + R) = \iota(Q) + \iota(R)$. We refer to [16] to conclude ι is a homomorphism.
We also see that $\ker(\iota) = O$, so ι is a injective and for all $(x, y) \in E$, we can take $(-x, -iy) \in E$ such that

$$\iota(-x, -iy) = (x, y),$$

so ι is surjective. □

Restricting ι to $E[p]$, yields an isomorphism from $E[p]$ to itself, since an isomorphism sends points of a certain order to points with the same order. Therefore $\iota P \in E[p]$.

Lemma 42. *$\iota P \notin \mathbb{Z}P$.*

Proof. Note first of all that

$$\iota^2 P = \iota^2(a,b) = (a,-b) = -P.$$

Suppose now for contradiction that the point ιP is inside $\mathbb{Z}P$ and therefore equals $[n]P$ for some $n \in \mathbb{Z}$. Then we see

$$-P = \iota^2 P = \iota[n]P = [n]\iota P = [n^2]P,$$

which implies that

$$n^2 = -1 \bmod p,$$

since p is the order of P. This means that

$$n^4 \equiv 1 \bmod p$$

and since $n^2 \not\equiv 1 \bmod p$, the order of n equals 4. Just as we did in the proof of theorem 17, we use Lagrange's theorem here to conclude that

$$4 = \# < \bar{n} > | \#(\mathbb{Z}/p\mathbb{Z})^* = p - 1.$$

This means that $p \equiv 1 \bmod 4$, which is a contradiction with our assumption that $p \equiv 3 \bmod p$. □

We are now almost able to prove our final result for this chapter. But before we do that, we denote the following very interesting result we found in [16]: for any nonzero integer m and an elliptic curve E defined over the field K with $\mathrm{char}(K) \nmid m$, we have that

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

This result holds for our elliptic curve E, since p is nonzero and the characteristic of $\mathbb{Q}$ is zero. The proof of the statement is highly involved and can be found in [16].

Proposition 43. *$E[p] \cong \mathbb{Z}[\iota]P \cong (\mathbb{F}_{p^2}, +, \bar{0})$.*

Proof. Because of lemma 41 and the remarks above and below that lemma, we know that $\mathbb{Z}[\iota]P \subset E[p]$. Now, introduce the map

$$\eta : \mathbb{Z}[i] \to \mathbb{Z}[\iota]P : a + bi \mapsto ([a] + [b]\iota)P.$$

It is a group homomorphism, since for $a + bi, c + di \in \mathbb{Z}$:

$$\eta(a+bi+c+di) = ([a+c]+[b+d]\iota)P = ([a]+[b]\iota)P + ([c]+[d]\iota)P = \eta(a+bi) + \eta(c+di).$$

It is also surjective, since for any $([a]+[b]\iota)P \in \mathbb{Z}[\iota]P$, we can pick $a+bi \in \mathbb{Z}[i]$ such that $\eta(a+bi) = ([a]+[b]\iota)P$. The kernel of η equals $(p) = p \cdot \mathbb{Z}[i]$, since for the elements $p(a+bi) \in (p)$:

$$\eta(p(a+bi)) = ([pa]+[pb]\iota)P = ([a]+[b]\iota)[p]P = ([a]+[b]\iota)O = O.$$

and for elements $a+bi \in$ker(η) it holds, by lemma 42, that both a and b are multiples of p. This gives

$$\mathbb{Z}[\iota]P \cong \mathbb{Z}[i]/(p) = \{\bar{a}+\bar{b}i | \bar{a}, \bar{b} \in \mathbb{F}_p\}. \tag{6.1}$$

Furthermore, by the result of [16] we discussed above, it holds that

$$E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}. \tag{6.2}$$

Because we see that both sets in equations 6.1 and 6.2 are abelian groups containing p^2 elements, they are, due to proposition 21, both isomorphic to $(\mathbb{F}_{p^2}, +, \bar{0})$. □

6.3 Establishing semidirect products

In this section, we will show, using the facts we obtained in the previous section, that we can can establish some semidirect products as Galois groups. We will not solve the inverse Galois problem for these type of groups, but we will sketch a method to find specific semidirect products and give an example of this method. We will still be talking about the same elliptic curve E, the prime number p and the point $P = (a,b) \in E[p]$ as in the previous sections. For simplicity, we will now notate $[n]P$ by nP for some integer n.
The extension we will look at is $\mathbb{Q}(E[p])|\mathbb{Q}$. Note that extending $\mathbb{Q}$ with $E[p]$ means that we extend $\mathbb{Q}$ with all the x- and y-coordinates of the points in $E[p]$.

Proposition 44. *The extension $\mathbb{Q}(E[p])|\mathbb{Q}$ is Galois.*

Proof. Look at a field homomorphism

$$\sigma : \mathbb{Q}(E[p]) \to \mathbb{C}.$$

If we can show that σ is an automorphism, then this means $\mathbb{Q}(E[p])|\mathbb{Q}$ is a Galois extension, because there are $[\mathbb{Q}(E[p]) : \mathbb{Q}]$ different field homomorphisms $\mathbb{Q}(E[p]) \to \mathbb{C}$. For details and a proof of this statement, we refer to [6].
We can define for $Q \in E$

$$\sigma(Q) = \begin{cases} (\sigma(x), \sigma(y)) & \text{if } Q = (x,y) \\ O & \text{if } Q = O \end{cases}$$

to see that for $Q = (x,y) \in E$:

$$\sigma(y)^2 = \sigma(y^2) = \sigma(x^3 - x) = \sigma(x)^3 - \sigma(x),$$

so $\sigma(Q) \in E$.
With similar arguments, one can prove that for any $Q, R \in E$:

$$\sigma(Q+R) = \sigma(Q) + \sigma(R),$$

since the coefficients of $Q+R$ can be determined by equations with rational coefficients. We will show this now for the case that $Q \neq \pm R$ and leave the other cases for the reader to check.
Write

$$Q = (x_1, y_1), R = (x_2, y_2) \text{ and } Q+R = (x_3, y_3).$$

Then one can calculate the line between Q and R

$$y = \lambda x + v, \text{ with } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } v = y_1 - \lambda x_1$$

and intersect it with E to get

$$y^2 = (\lambda x + v)^2 = x^3 - x$$

which means

$$x^3 - \lambda^2 x^2 - v^2 - (2\lambda v + 1)x = 0,$$

so

$$x^3 - \lambda^2 x^2 - v^2 - (2\lambda v + 1)x = (x - x_1)(x - x_2)(x - x_3),$$

hence it yields, if we look at the terms before x^2, that

$$-\lambda^2 = -x_1 - x_2 - x_3,$$

which implies

$$x_3 = \lambda^2 - x_1 - x_2 \text{ and } y_3 = -\lambda x_3 - v.$$

Therefore

$$\sigma(x_3) = \left(\frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)} \right)^2 - \sigma(x_1) - \sigma(x_2)$$

and

$$\sigma(y_3) = \frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)}(\sigma(x_1) - \sigma(x_3)) - \sigma(y_1).$$

Hence

$$\sigma(Q+R) = (\sigma(x_3), \sigma(y_3)) = (\sigma(x_1), \sigma(y_1)) + (\sigma(x_2), \sigma(y_2)) = \sigma(Q) + \sigma(R).$$

We now see, for any $Q \in E[p]$, that

$$p\sigma(Q) = \sigma(pQ) = \sigma(O) = O,$$

so $\sigma(Q) \in E[p]$. Therefore $\sigma(\mathbb{Q}(E[p])) \subset \mathbb{Q}(E[p])$ and since the kernel of σ is trivial

$$\sigma(\mathbb{Q}(E[p])) = \mathbb{Q}(E[p]).$$

□

We will determine the Galois group of $\mathbb{Q}(E[p])|\mathbb{Q}$. We remind the reader that if $C_2 =< \sigma >$ and $C_k =< \tau >$ are subgroups of some group G such that $G =< \sigma, \tau >$ and $C_2 \cap C_k = \{1\}$ and $\sigma\tau\sigma^{-1} = \tau^m$ for coprime k and m, so C_k is normal in G, then G is a semidirect product of C_2 and C_k determined by the relation $\sigma\tau\sigma^{-1} = \tau^m$. It can be written as

$$G = C_2 \rtimes C_k.$$

First we need a lemma.

Lemma 45. *Let E and p be as before. Then there exists an injective homomorphism*

$$\rho : Gal_{\mathbb{Q}}(\mathbb{Q}(E[p])) \to GL_2(\mathbb{F}_p).$$

Proof. We know the points P and ιP are generators of $\mathbb{Z}[\iota] \cong E[p]$ by the previous section. Therefore, any $\sigma \in$Gal$_{\mathbb{Q}}(\mathbb{Q}(E[p]))$ is uniquely determined by where it sends P and ιP to (it permutes non-trivial points in $E[p]$ as noticed in the proof of proposition 44). Therefore,

$$\sigma(P) = aP + b\iota P$$
$$\sigma(\iota P) = cP + d\iota P,$$

for some $a, b, c, d \in \mathbb{F}_p$ with a and b not both zero and c and d not both zero. It also holds that $(a, b) \neq \lambda(c, d)$ for $\lambda \in \{1, ..., p\}$, because otherwise σ would not be injective. Now build

$$\rho : \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[p])) \to GL_2(\mathbb{F}_p) : \sigma \mapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix},$$

where a, b, c and d are determined by the definition of $\sigma(P)$ and $\sigma(\iota P)$ as above. We see because of the earlier described restrictions on a, b, c and d that every $\rho(\sigma) \in \mathrm{GL}_2(\mathbb{F}_p)$. We see this is a group homomorphism, since for $\sigma, \tau \in$Gal$_{\mathbb{Q}}(\mathbb{Q}(E[p]))$ with

$$\sigma(P) = aP + b\iota P \qquad \tau(P) = a'P + b'\iota P$$
$$\sigma(\iota P) = cP + d\iota P \qquad \tau(\iota P) = c'P + d'\iota P,$$

we can compute

$$\sigma \circ \tau(P) = \sigma(a'P + b'\iota P) = a'(aP + b\iota P) + b'(cP + d\iota P) = (a'a + b'c)P + (a'b + b'd)\iota P$$
$$\sigma \circ \tau(\iota P) = \sigma(c'P + d'\iota P) = c'(aP + b\iota P) + d'(cP + d\iota P) = (c'a + d'c)P + (c'b + d'd)\iota P,$$

hence
$$\rho(\sigma \circ \tau) = \begin{pmatrix} a'a + b'c & c'a + d'c \\ a'b + b'd & c'b + d'd \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \rho(\sigma) \cdot \rho(\tau).$$
Furthermore, for any $\sigma \in \ker(\rho)$ it holds that $\sigma(P) = P$ and $\sigma(\iota P) = \iota P$, so it is the identity map on $E[p]$ and therefore the identity map in $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[p]))$. We conclude ρ is injective. □

Note that ρ is not always surjective. Every element in $\mathrm{GL}_2(\mathbb{F}_p)$ clearly defines an automorphism on $E[p]$ and, moreover, an automorphism on $\mathbb{Q}(E[p])$, but such an automorphism is not always an automorphism of $\mathbb{Q}(E[p])|\mathbb{Q}$.

Proposition 46. *Let E, p and P be as before. Then $Gal_{\mathbb{Q}}(\mathbb{Q}(E[p])) \cong C_2 \rtimes C_n$ given by $\sigma\tau\sigma^{-1} = \tau^k$ for some coprime n and k, where $n|p^2 - 1$.*

Proof. We will first prove that $\mathbb{Q}(i)$ is a subextension of $\mathbb{Q}(E[p])|\mathbb{Q}$, which is Galois with Galois group C_2.
By lemma 41, we know ι is an automorphism on $E[p]$. Therefore, as we used before, since $P = (a, b) \in E[p]$, also $\iota P = (-a, ib) \in E[p]$. Now note that adding points on an elliptic curve to $\mathbb{Q}$, means that we add the x- and y-coordinates of those points to $\mathbb{Q}$. So $b, bi \in \mathbb{Q}(E[p])$ and therefore $i \in \mathbb{Q}(E[p])$, which means $\mathbb{Q}(i)$ is a subextension of $\mathbb{Q}(E[p])|\mathbb{Q}$. We know $\mathbb{Q}(i)$ is the splitting field over $\mathbb{Q}$ of the irreducible polynomial $f = X^2 + 1$, so by proposition 2, $\mathbb{Q}(i)|\mathbb{Q}$ is Galois with Galois group C_2. Notice that
$$\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i) : a + bi \mapsto a - bi,$$
which is complex conjugation, is an automorphism of $\mathbb{Q}(i)$ which sends elements of $\mathbb{Q}$ to itself, so $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(i)) =< \sigma >$.
Because, by proposition 43, $E[p] \cong \mathbb{Z}[\iota]P$, we know that $\mathbb{Q}(E[p]) = \mathbb{Q}(i, P)$. Therefore, every automorphism μ of $\mathrm{Gal}_{\mathbb{Q}(i)}(\mathbb{Q}(E[p]))$ is uniquely determined by where it sends P to. We can also see this if we note that when $\mu(P) = aP + b\iota P$, then $\mu(\iota P) = -bP + a\iota P$, since $\mu(i) = i$. Therefore, if we restrict ρ from the lemma before, we see
$$\rho : \mathrm{Gal}_{\mathbb{Q}(i)}(\mathbb{Q}(E[p])) \to \mathrm{GL}_2(\mathbb{F}_p) : \mu \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$
for a and b defined by $\mu(P)$. Clearly, it also holds that
$$\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \right\} \cong \mathbb{F}_p^*(i)$$
if we identify $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ with $a + bi \in \mathbb{F}_p^*(i)$. Since ρ is injective, $\mathrm{Gal}_{\mathbb{Q}(i)}(\mathbb{Q}(E[p]))$ is isomorphic to a subgroup of $\mathbb{F}_p^*(i)$. We know $\mathbb{F}_p(i) \cong \mathbb{F}_{p^2}$, because every two finite fields

containing the same number of elements are isomorphic. By proposition 24, we conclude that $\mathbb{F}_{p^2}^* \cong C_{p^2-1}$. Since every subgroup of a cyclic group with order q is a cyclic group with order dividing q, we deduce that

$$\mathrm{Gal}_{\mathbb{Q}(i)}(\mathbb{Q}(E[p])) \cong C_n =< \tau > \text{ for some } \tau \text{ with order } n|p^2-1.$$

Therefore, since $\sigma \notin C_n$, because it does not fix i:

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[p])) \cong < \sigma, \tau >= C_2 \rtimes C_n.$$

given by $\sigma\tau\sigma^{-1} = \tau^k$ for some integer k. To see k and n are coprime, note that if, for some integers a, l and m with $a > 1$, we would have that $k = al$ and $n = am$, then

$$1 = (\tau^n)^l = (\tau^k)^m = (\sigma\tau\sigma^{-1})^m = \sigma\tau^m\sigma^{-1} \implies \tau^m = 1,$$

which is a contradiction. □

This result allows us to determine Galois groups isomorphic to non-abelian semidirect products if for the generators σ and τ it holds that $\sigma\tau\sigma^{-1} = \tau^k$ for $k > 1$.

6.4 The structure of the group $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[3]))$

As the title of this section suggests, we will now look at an example of what we did in the previous section. We will look at the Galois extension $\mathbb{Q}(E[3])|\mathbb{Q}$ for the same elliptic curve E as before and we will determine its Galois group. First we will see that coordinates of the point P in the the 3-torsion group

$$E[3] = \{(a,b) \in E|(a,b) + (a,b) + (a,b) = O\}.$$

can be determined as roots of a polynomial.
For the point $P = (a,b) \in E[p]$, we deduce from the definition that $-(P+P) = P$. First we calculate $P+P$. According to the first section in this chapter, we must therefore find the third intersection of E with the tangent line of E at P. We determine the slope of E:

$$\begin{aligned} y^2 &= x^3 - x, \text{ which is the equation for points } (x,y) \text{ on } E \\ 2ydy &= (3x^2-1)dx, \text{ after differentiating both sides} \\ \frac{dy}{dx} &= \frac{3x^2-1}{2y}, \text{ after rearranging} \end{aligned}$$

So the tangent line of E at P is given by

$$y - b = \left.\frac{dy}{dx}\right|_{(x,y)=(a,b)}(x-a) = \frac{3a^2-1}{2b}(x-a).$$

Now, we intersect this line with E to obtain the following equation for the x-coordinate of the points of intersection:

$$x^3 - x - \left(\frac{3a^2-1}{2b}(x-a)+b\right)^2 = 0. \tag{6.3}$$

This polynomial must have $x = a$ as a root with multiplicity 2, since the tangent line of E at (a, b) has an intersection with E at P with multiplicity 2. Therefore (6.3) reduces to

$$(x-a)(x-a)(x-\alpha) \tag{6.4}$$

for some α depending on a and b. This α is the x-coordinate of the third intersection we want to determine. Since (6.3) equals (6.4), we know both factors before the x^2 are equal. Therefore

$$2a + \alpha = \left(\frac{3a^2-1}{2b}\right)^2$$

and if we notice that $b^2 = a^3 - a$, since $P \in E$, we have

$$\alpha = \frac{(3a^2-1)^2}{4(a^3-a)} - 2a.$$

From this we conclude that the x-coordinate of $P + P$ equals $-\alpha$, so the x-coordinate of $-(P + P)$ equals α.

As earlier said, for P it must hold that $-(P + P) = P$. So we are left with the equation for a:

$$\alpha = \frac{(3a^2-1)^2}{4(a^3-a)} - 2a = a,$$

which arranges to

$$3a^4 - 6a^2 - 1 = 0.$$

This means $\mathbb{Q}(E[3]) = \mathbb{Q}(a, b, i)$ for a root a such that the equation above holds and $b^2 = a^3 - a$.

We described the extension $\mathbb{Q}(E[3])$ and what is left is to determine the Galois group.

We see the minimal polynomials for i, a and b over respectively $\mathbb{Q}$,$\mathbb{Q}(i)$ and $\mathbb{Q}(i, a)$ are equal to

$$\begin{aligned}
f_1 &= X^2 + 1 \in \mathbb{Q}[X] \\
f_2 &= 3X^4 - 6X^2 - 1 \in \mathbb{Q}(i)[X] \\
f_3 &= X^2 - a^3 - a \in \mathbb{Q}(i, a)[X],
\end{aligned}$$

since these polynomials have respectively i, a and b as a root and are irreducible: f_1 does not have roots in $\mathbb{Q}$ and f_2 and f_3 are irreducible by Eisenstein's criterion for respectively

$p = 3$ (after reversing the order of the coefficients as we did for $h(X)$ in the proof of proposition 33) and $p = a$.
This implies that

$$\mathbb{Q}(E[3]) : \mathbb{Q}] = 2 \cdot 4 \cdot 2 = 16,$$

which means that $\#\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[p])) = 16 = 2^4$. Now, $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[p]))$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$, because of lemma 45. Notice that $\mathrm{GL}_2(\mathbb{F}_3)$ is a group containing $8 \cdot 6 = 48 = 2^4 \cdot 3$ elements, because for every element there are 8 nontrivial first column vectors possible and 6 options for the second column vector such that the first and second column are linearly independent. Hence, $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[p]))$ is isomorphic to the (unique up to isomorphism) Sylow 2-subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. We also see, because of the size, that $\mathrm{Gal}_{\mathbb{Q}(i)}(\mathbb{Q}(E[p]))$ equals C_8. So the Sylow 2-subgroup we will look for is generated by an element of order 2 and an element of order 8. One can compute that

$$\sigma = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_3)$$

have respectively order 2 and 8. We also leave it as an exercise for the reader to check that

$$\sigma\tau\sigma^{-1} = \tau^3.$$

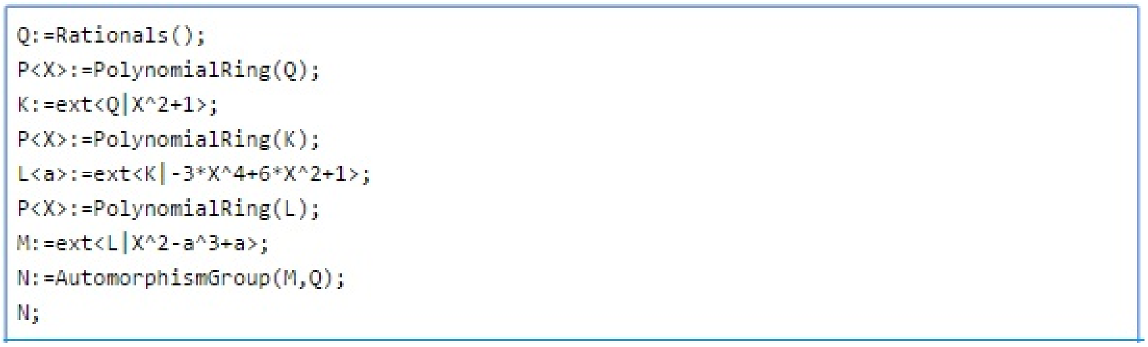
Hence,

$$\# < \sigma, \tau > = \#\{1, \sigma, \tau, \tau^2, \tau^3, \tau^4, \tau^5, \tau^6, \tau^7, \sigma\tau, \sigma\tau^2, \sigma\tau^3, \sigma\tau^4, \sigma\tau^5, \sigma\tau^6, \sigma\tau^7\} = 16,$$

so

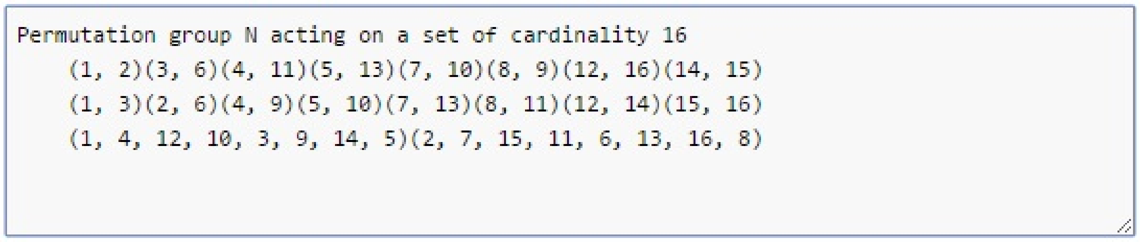
$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[p])) \cong < \sigma, \tau > = C_2 \rtimes C_8 = SD_8,$$

where SD_8 denotes the semi-dihedral group of order 16.
Alternatively, if the minimal polynomials of a and b are known, one can can use the Magma code



```
Q:=Rationals();
P<X>:=PolynomialRing(Q);
K:=ext<Q|X^2+1>;
P<X>:=PolynomialRing(K);
L<a>:=ext<K|-3*X^4+6*X^2+1>;
P<X>:=PolynomialRing(L);
M:=ext<L|X^2-a^3+a>;
N:=AutomorphismGroup(M,Q);
N;
```

with the output



```
Permutation group N acting on a set of cardinality 16
    (1, 2)(3, 6)(4, 11)(5, 13)(7, 10)(8, 9)(12, 16)(14, 15)
    (1, 3)(2, 6)(4, 9)(5, 10)(7, 13)(8, 11)(12, 14)(15, 16)
    (1, 4, 12, 10, 3, 9, 14, 5)(2, 7, 15, 11, 6, 13, 16, 8)
```

to see that the generators for the subgroup of S_{16} isomorphic to $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[p]))$ are

$$\begin{aligned} \sigma &= (1\quad 2)(3\quad 6)(4\quad 11)(5\quad 13)(7\quad 10)(8\quad 9)(12\quad 16)(14\quad 15) \\ \tau &= (1\quad 4\quad 12\quad 10\quad 3\quad 9\quad 14\quad 5)(2\quad 7\quad 15\quad 11\quad 6\quad 13\quad 16\quad 8), \end{aligned}$$

since the second output cycle of Magma equals $(\sigma\tau)^2$. One can now see with some calculations that

$$\sigma\tau\sigma^{-1} = \tau^3,$$

so we can conclude the same result.

Chapter 7

Conclusion

We started with the notion of a Galois group and presented some tools to determine this group. By presenting some examples, we illustrated that these tools, especially the theorem of Dedekind, appeared to be very useful in order to determine the Galois group of a polynomial over $\mathbb{Q}$. We also saw, with an example of a polynomial for which the Galois group could not be determined, that they are not always sufficient.

In the third chapter we introduced some important theorems such as the theorem of Dirichlet on arithmetic progressions and the fundamental theorem of Galois theorem to help us with the proof that every finite abelian group is isomorphic to a Galois group over $\mathbb{Q}$. In particular we proved that every finite abelian group is isomorphic to the Galois group of a subextension of $\mathbb{Q}(\zeta_n)|\mathbb{Q}$.

The fourth and fifth chapter were devoted to the proof of the inverse Galois problem for the symmetric and the alternating group. With the use of the irreducibility theorem of Hilbert, we even managed to establish specific polynomials with the desired Galois groups.

In chapter six we did not come up with a proof of the inverse Galois problem for semidirect products. However, we described a method to find a lot of these groups and showed in an example that we could find SD_8.

Of course there is a lot more known about this problem then we could show in our thesis. If one wants to read more about this problem, we recommend [4] or [11], although these books are not very accessible for undergraduate students.

Bibliography

[1] https://en.wikipedia.org/wiki/%C3%89variste_Galois, visited on 09-06-2016.

[2] https://en.wikipedia.org/wiki/Galois_theory, visited on 09-06-2016.

[3] https://en.wikipedia.org/wiki/Inverse_Galois_problem, visited on 09-06-2016.

[4] G. Malle and B.H. Matzat. *Inverse Galois Theory.* Springer, Berlin Heidelberg, 1999.

[5] B. van Geemen, H.W. Lenstra, F. Oort, with additions of J. Top. Algebraische structuren. http://www.math.rug.nl/~top/dic.pdf, Groningen: 2014.

[6] Frans Keune. *Galoistheorie.* Epsilon Uitgaven, Amsterdam, 2015.

[7] Keith Conrad. Course notes on transitive group actions. http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/transitive.pdf.

[8] B.L. van der Waerden. *Modern Algebra.* Frederick Ungar Publishing CO, New York, 1949.

[9] J. Top. Groepentheorie. http://www.math.rug.nl/~top/alg1.pdf, Groningen, 2013.

[10] Lecture notes on Abstract Algebra 1 by Bülent Köklüce. http://www.fatih.edu.tr/~bkokluce/alg/notes1.pdf, 2006.

[11] Jean-Pierre Serre. *Topics in Galois theory*, Course at Harvard University(Notes written by Henri Darmon), Fall 1988.

[12] Reginald Koo. *A Classification of Matrices of Finite Order over C, R and Q*, Mathematics Magazine, Vol 76, No. 2, Mathematical Association of America, Washington, April 2003.

[13] Richard L. Burden and J. Douglas Faires. *Numerical Analysis.* Cengage Learning, Boston, 2010.

[14] Manoj Kumar, Gyan Shekhar, Lata Misra. *A Study on the Inverse Galois Problem in Galois Theory*, International Journal of Modern Electronics and Communication Engineering, Volume No.-3, Issue No.-3, September 2015.

[15] Fernando Barrera Mora et al. *The discriminant of a trinomial*, International Journal of Pure and Applied Mathematics, Volume 74, No. 1, 43-54, 2012.

[16] Joseph H. Silverman. *The arithmetic of elliptic curves.* Springer Verlag, New York, 1986.