Utrecht University

Master Thesis

Mathematical Sciences

Noether's problem and the existence of generic polynomials

Student:
H.G.J. Tiesinga

Supervisors:
Prof. dr. F. Beukers
Prof. dr. G.L.M. Cornelissen

January 2019

Abstract

The main topics of this thesis are Noether's problem and the existence of generic polynomials. These problems are both related to the inverse Galois problem, which asks the question whether every finite group is isomorphic to the Galois group of a Galois extension over $\mathbb{Q}$. We solved Noether's problem and found generic polynomials for the subgroups of S_n for $n \leq 4$ and the quaternion group of order 8. Moreover, we established generic polyomials for the cyclic groups of odd order and discussed their existence for some other groups such as the dihedral groups of odd order, p-groups and Frobenius groups. We also worked out a counterexample for Noether's problem, namely the cyclic group of order 8.

Acknowledgements

First of all I want to thank Frits Beukers for his pleasant guidance during the work on this thesis. From the first moment I appreciated the comfortable and unforced atmosphere he created during our meetings. He always took time to patiently explain and suggest matters and answer all my questions, for which I am thankful. He closely monitored my work, but also gave me complete freedom to work on the subjects I felt was most interesting. The meeting kept me productive and, most of all, enthusiastic during the entire project.

Furthermore, I would like to thanks Gunther Cornelissen for taking the time to be the second reader of this thesis and for his helpful comments and suggestions.

Finally, I would like to express my gratitude to my friends and family for their support and encouragement over the past year.

Contents

1 Introduction

Mathematicians have studied equations and their solutions through the ages. In the 18th century recipes were known for solving the general quadratic, cubic or quartic equation in radicals. A recipe to solve the general quintic equation in radicals does not exist and the mathematician Abel was in 1824 the first to prove this remarkable statement. A deep insight in the solvability of equations was obtained by the mathematician Evariste Galois in the beginning of the 19th century. He developed a theory, now known as Galois theory, which looks at the symmetry in the solution set of an equation by looking at the permutations of the solutions of an equation that do not change the relations between the solutions. Together, these permutations form a group, the Galois group, for which the structure determines the solvability of an equation.

An interesting problem in Galois theory is the inverse Galois problem, which is generally unsolved. It asks the question whether every finite group is isomorphic to the Galois group of a Galois extension over $\mathbb{Q}$. This problem is the reason for our interest in the two main topics of this thesis: Noether's problem and the problem concerning the existence of generic polynomials. This is because a positive solution for a group G implies for both these problems a positive solution of the inverse Galois problem for G. The next section will treat the different problems and explain and prove the implications between them.

In the third section, the so-called generating invariant polynomials will be determined for cyclic, dihedral and alternating groups. These polynomials are interesting, but also turn out to be a useful tool in the next section.

In the fourth, fifth and sixth section Noether's problem and the existence of generic polynomials will be discussed for several groups. The focus lies in the fourth section on small groups, for which these problems will be investigated explicitly. We use the generating invariant polynomials of the third section there. The fifth section will approach the problems more generally and treats the cyclic groups. Two constructions of a generic polynomial for cyclic groups of odd order will be discussed, after which we will describe the totally different situation for cyclic groups of even order. We finish in the sixth section with an overview of important results concerning some other groups.

2 Preliminaries

This section will describe the main definitions and problems this thesis will deal with. In particular this section describes the inverse Galois problem, Noether's problem and generic polynomials together with the different connections between and implications of these problems. The reader is expected to have some knowledge about rings, fields and Galois theory.

2.1 The inverse Galois problem and generic polynomials

In Galois theory, the following problem is known as the inverse Galois problem. It was posed first in the 19th century and it is unsolved in general. We will first pose the the inverse Galois problem and then describe related problems.

Problem 1 (The Inverse Galois Problem)**.** Let G be a finite group and K a field with characteristic zero. Does there exist a Galois extension $M|K$ such that $\mathrm{Gal}(M|K) \cong G$?

For the rest of this section, let K and G be as in the above problem. A Galois extension $M|K$ with group G is the splitting field of a separable polynomial over K. We will assume from now on that G acts transitively on the roots of this polynomial, which means we assume that this polynomial is irreducible over K. It is interesting to search for this polynomial (or a family of polynomials) over K with Galois group G. The following kind of polynomials are in particular interesting. We write Ω_K^f for the splitting field of a polynomial f over K.

Definition 1. Let $P(\mathbf{x}, X) \in K(\mathbf{x})[X]$ be monic, with $\mathbf{x} = (x_1, ..., x_n)$, where $x_1, ..., x_n$ are algebraically independent over K. Let $\mathbb{M} = \Omega_{K(\mathbf{x})}^{P(\mathbf{x},X)}$. $P(\mathbf{x}, X)$ is a *parametric polynomial of* G *over* K if

1. $\mathbb{M}|K(\mathbf{x})$ is Galois with group G.
2. for every Galois extension $L|K$ with group G we can pick $\mathbf{a} \in K^n$ such that $L = \Omega_K^{P(\mathbf{a},X)}$.

Note that in the definition, n is not the degree of P. One can deduce from condition 1, that if $k > 0$ is the smallest integer such that $G \subset S_k$, then a parametric polynomial P of G over K must be of degree $\geq k$. This will become clear when we discuss proposition 4. We followed [JLY02] in our notation above as we will do for the following definition.

Definition 2. Let $P(\mathbf{x}, X)$ be a parametric polynomial of G over K. $P(\mathbf{x}, X)$ is *generic of* G *over* K if for every field L' containing K and every Galois extension $L|L'$ with group G we can pick $\mathbf{a} \in L'^n$ such that $L = \Omega_{L'}^{P(\mathbf{a},X)}$.

A stronger version of this definition would be to say that a polynomial is generic of G over K if it is parametric of any group $H \subseteq G$ over any field N containing K. However, it was proved in [Led00] that the existence of a generic polynomial in this stronger sense is implied by the existence of a generic polynomial in the sense of definition 2. All examples known to Ledet seem to suggest that a polynomial which is generic in the sense of definition 2 is actually generic in the stronger sense. Nevertheless, this is not proved yet.
One might wonder whether there exist parametric polynomials, which are not generic. We will show below that these exist if $G = C_8$. It is natural to ask the following question.

Problem 2. Does there exist a generic polynomial of G over K?

An interesting fact, proven in [JLY02], is that the existence of generic polynomials over K for the finite groups G and H implies the existence of a generic polynomial for the product $G \times H$ over K. The proof will be skipped, because it is extensive and it relies on the theory of generic extensions of commutative rings, which will need a lot of introduction.

One could wonder whether a solution for some group G for problem 2 implies a solution for the inverse Galois problem for G and $K = \mathbb{Q}$. This is indeed the case and we will discuss this below. For that, we first need to state an important theorem

Theorem 1 (Hilbert's Irreducibility Theorem)**.** Let $\mathbb{K}$ be an algebraic number field and let $f(\mathbf{t}, X) \in \mathbb{K}(\mathbf{t})[X]$ be an irreducible polynomial, with $\mathbf{t} = (t_1, ..., t_n)$ and $t_1, ..., t_n$ are variables that are algebraically independent over $\mathbb{K}$. Then there exist infinitely many $\mathbf{a} = (a_1, ..., a_n) \in \mathbb{K}^n$ such that the specialization $f(\mathbf{a}, X) \in \mathbb{K}[X]$ is well-defined and irreducible over $\mathbb{K}$. The specialization can be chosen to have

$$\mathrm{Gal}(f(\mathbf{t}, X)/\mathbb{K}(\mathbf{t})) \cong \mathrm{Gal}(f(\mathbf{a}, X)/\mathbb{K}).$$

Proof. A proof can be found in [JLY02]. □

We are now ready to prove that if problem 2 is solved for some G and $K = \mathbb{Q}$, then the inverse Galois problem can be solved.

Proposition 1. The existence of a generic polynomial of G over $\mathbb{Q}$ implies a solution for the Inverse Galois problem for G and $K = \mathbb{Q}$

Proof. Let $g(t_1, ..., t_n, X)$ be the generic polynomial of G over $\mathbb{Q}$ and let $L := \Omega^{g(t_1,...,t_n,X)}_{\mathbb{Q}(t_1,...,t_n)}$. Then by definition, $L|\mathbb{Q}(t_1, ..., t_n)$ is Galois with group G. As we assumed G to act transitively on the roots of $g(t_1, ..., t_n, X)$, this means that $g(t_1, ..., t_n, X)$ is irreducible. For $a_1, ..., a_n \in \mathbb{Q}$, let $M := \Omega^{g(a_1,...,a_n,X)}_{\mathbb{Q}}$. With the use of Hilbert's irreducibility theorem, we deduce that there exists infinitely many $a_1, ..., a_n \in \mathbb{Q}$ such that the specializations $g(a_1, ..., a_n, X)$ are irreducible and $M|\mathbb{Q}$ is Galois with group G. □

2.2 Noether's problem

In order to go to Noether's problem, which is one of our main topics, we introduce the following notion.

Definition 3. An extension $L|K$ is *rational* if there exists a subset $\{\beta_i\}_{i \in I}$ of L, which is algebraically independent over K and $L = K(\{\beta_i\})$.

For a rational extension $L|K$ with $L = K(\beta_1, ..., \beta_n)$, for $\beta_1, ..., \beta_n$ being algebraically independent over K, we say that $L|K$ has transcendence degree n. We will now continue with Noether's problem. From now on throughout this whole thesis, on let $x_1, ..., x_n$ be variables, algebraically independent over $\mathbb{Q}$ and define $M := \mathbb{Q}(x_1, ..., x_n)$.

Problem 3 (Noether's problem)**.** Consider G to be a subgroup of S_n. Is $M^G|\mathbb{Q}$ a rational extension with transcendence degree n?

In Noether's problem, we suppose that the elements $\sigma \in G$ act on M by fixing $\mathbb{Q}$ and sending x_i to $x_{\sigma(i)}$. Noether's problem is trivial for $G = S_n$ as then $M^G = \mathbb{Q}(s_1, ..., s_n)$, where $s_1, ..., s_n$ are the elementary symmetric polynomials in the variables $x_1, ..., x_n$. A connection between Noether's problem and the inverse Galois problem is made in the following proposition.

Proposition 2. A solution for a group $G \subseteq S_n$ for Noether's problem implies a solution of the Inverse Galois problem for G and $K = \mathbb{Q}$.

Proof. Suppose Noether's problem is solvable for a group $G \subseteq S_n$, so $M^G = \mathbb{Q}(f_1, ..., f_n)$, where $f_1, ..., f_n$ are algebraically independent over $\mathbb{Q}$. Define $N := M^G$. By the primitive element theorem, $\exists \alpha \in M$ such that $M = N(\alpha)$. Let $g \in N[y]$ be the minimal polynomial of α over N, so $M = \Omega_N^g$. For some $\mathbf{x_0} \in \mathbb{Q}^{\mathbf{n}}$, let $g_{\mathbf{x_0}} \in \mathbb{Q}[y]$ be constructed by substituting the i-th index of $\mathbf{x_0}$ for f_i in g. By the irreducibility theorem of Hilbert, there are infinitely many such $\mathbf{x_0}$ such that $g_{\mathbf{x_0}}$ is irreducible over $\mathbb{Q}$ and $\Omega_{\mathbb{Q}}^{g_{\mathbf{x_0}}}|\mathbb{Q}$ is Galois with group G. $\square$

We can go even further by claiming that a solution to Noether's problem can be used to find a generic polynomial. In order to prove the proposition below, which provides such a construction, we first have to introduce some notation and theory we will use throughout the whole thesis. Let $s_1, ..., s_n$ be the elementary symmetric polynomials in $x_1, ..., x_n$. Define $N := \mathbb{Q}(s_1, ..., s_n)$. As Galois theory tells us, we have $M = \Omega_N^{f(x)}$ for

$$f(x) := \prod_{i=1}^{n}(x - x_i) = x^n - s_1x^{n-1} + ... + (-1)^n s_n.. \tag{$\star$}$$

By the primitive element theorem, for any group $G \subseteq S_n$, we have $M^G = N(h)$ for some element $h \in M$. This element h can always chosen to be in $\mathbb{Q}[x_1, ..., x_n]$, because of the following argument. Let $l(x) \in N[x]$ be the minimal polynomial of h with degree m and let a_m be the coefficient of x^m in $l(x)$. Without loss of generality, we can choose the coefficients of $l(x)$ to lie in $\mathbb{Q}[s_1, ..., s_n]$. Multiply now $l(x)$ with a_m^{m-1} and replace $a_m x$ by y to obtain a monic polynomial $l'(y)$ with coefficients in $\mathbb{Q}[s_1, ..., s_n]$ and root $a_m h$. With the use of the following proposition, which is also explained in [Roe18], the claim that we can always choose h to lie in $\mathbb{Q}[x_1, ..., x_n]$ is justified, because we can take $R = \mathbb{Q}[x_1, ..., x_n]$ and $\beta = a_m h$.

Proposition 3. Let $g(x) = x^m + a_1x^{m-1} + ... + a_m \in R[x]$, where R is a unique factorization domain. If $g(\beta) = 0$ for some $\beta \in Q(R)$ (the quotient field of R), then $\beta \in R$.

Proof. Let $\beta \in Q(R)$ be such that $g(\beta) = 0$. We know we can write $\beta = b/c$ for some $b, c \in R$, such that $\gcd(b, c) = 1$. As $g(b/c) = 0$, we have

$$c^m g(b/c) = b^m + a_1cb^{m-1} + ... + a_{m-1}c^{m-1}b + a_mc^m = 0.$$

This gives $b^m \equiv 0(\mathrm{mod} c)$, which means that $c|b^m$. Because $\gcd(b, c) = 1$, this means c has to be a unit in R, so $\beta = b/c \in R$. $\square$

We now move towards and prove an important proposition.

Proposition 4. Suppose that Noether's problem gives a positive answer for $G \subseteq S_n$. Let $\phi_1, ..., \phi_n \in M^G$ be the algebraically independent set of generators for M^G over $\mathbb{Q}$. Then $f(x)$ in ($\star$) is of the form $f(x) = g(\phi_1, ..., \phi_n, x)$, where $g \in \mathbb{Q}(t_1, ..., t_n)[x]$, with $t_1, ..., t_n$ algebraically independent over $\mathbb{Q}$, and g is a generic polynomial of G over $\mathbb{Q}$.

The easiest non-trivial example of this proposition is when we take $G = C_3$. We refer to section 4.1, where we showed that Noether's problem is solved for this case and where we constructed the generic polynomial of C_3 over $\mathbb{Q}$.

Proof. To prove that g is generic of G over $\mathbb{Q}$, we will first explain that the Galois group of g over $\mathbb{Q}(t_1, ..., t_n)$ is equal to G. As $\mathbb{Q}(t_1, ..., t_n)$ is isomorphic to $M^G = \mathbb{Q}(\phi_1, ..., \phi_n)$, this means that the Galois group of g over $\mathbb{Q}(t_1, ..., t_n)$ is equal to the Galois group of $f(x)$ over M^G. The Galois group of $f(x)$ over M^G is equal to G, because $M = \Omega_{M^G}^{f(x)}$. Therefore, the Galois group of g over $\mathbb{Q}(t_1, ..., t_n)$ is equal to G.

Suppose now that we have a Galois extension $L|L'$ with group G, where $\mathbb{Q} \subseteq L'$. We will show now to satisfy also the second condition of definition 1 that we can pick $a \in L'^n$ such that $L = \Omega_{L'}^{g(a,x)}$. For that we need the following lemma. For the lemma, note that as G is a subgroup of S_n, so we can also let it act on $\mathbb{Q}(x_1, ..., x_n)$ in the way we explained above.

Lemma 1. Let $r(x_1, ..., x_n) \in \mathbb{Q}[x_1, ..., x_n]$ be non-trivial. We can construct $\alpha_1, ..., \alpha_n \in L$ such that

- $L'(\alpha_1, ..., \alpha_n) = L$
- G permutes $\alpha_1, ..., \alpha_n$ in the same way as G permutes $x_1, ..., x_n$.
- $r(\alpha_1, ..., \alpha_n) \neq 0$.

Proof. Define

$$H := \{g \in G | g(x_1) = x_1\} \subsetneq G,$$

which is in the literature called the stabilizer of x_1 by G. It is a proper subgroup of G, because G is assumed to be transitive at the beginning of this section. Also because of transitivity of G, the orbit of x_1 is $\{x_1, ..., x_n\}$. Therefore, by the orbit-stabilizer theorem,

$$[G : H] = \#\{x_1, ..., x_n\} = n.$$

This means we write $G = \cup_{i=1}^n g_i(H)$ for some $g_i \in G$ and we can even choose g_i such that $g_i : x_1 \mapsto x_i$, because G is transitive. Now, let $\alpha_1 \in L$ be such that $L'(\alpha_1) = L^H$ and define $\alpha_i := g_i(\alpha_1)$ for $i = 1, ..., n$. Then, by definition, G permutes $\alpha_1, ..., \alpha_n$ in the same way as $x_1, ..., x_n$. Therefore, combined with the fact that $L'(\alpha_1)|L'$ has degree n, we have $L = L'(\alpha_1, ..., \alpha_n)$.
To satisfy also the last condition, we need to change α_1 a bit. Denote by $L'[x]_{n-1}$, the ring of polynomials in $L'[x]$ with degree $n-1$. We will replace α_1 by $P(\alpha_1)$ for $P \in L'[x]_{n-1}$ satisfying $L'(P(\alpha_1)) = L^H$. It should be clear that G permutes $P(\alpha_1), ..., P(\alpha_n)$ in the same way as $\alpha_1, ..., \alpha_n$, so in the same way as $x_1, ..., x_n$. Therefore, combined with the fact that $L'(P(\alpha_1))|L'$ has degree n, we have $L = L'(P(\alpha_1), ..., P(\alpha_n))$. Polynomials $P \in L'[x]_{n-1}$ that satisfy $L'(P(\alpha_1)) = L^H$ are dense in $L'[x]_{n-1}$, because of the following reasoning.
Let $Q \in L'[x]_{n-1}$ be such that $L'(Q(\alpha_1)) \subsetneq L^H$. Then, because of the fundamental theorem of Galois theory, there exists a subgroup H' such that $H \subsetneq H' \subseteq G$, such that $L'(Q(\alpha_1)) = L^{H'}$. Hence, because $G = \cup_{i=1}^n g_i(H)$, for some $i \neq 1$: $g_i(Q(\alpha_1)) = Q(\alpha_i) = Q(\alpha_1)$. Take now $\epsilon \in L'$, such that $\epsilon > 0$ and define $P = Q + \frac{\epsilon}{2}x \in L'[x]_{n-1}$. Then

$$g_i(P(\alpha_1)) = Q(\alpha_1) + \frac{\epsilon}{2}\alpha_i \neq Q(\alpha_1) + \frac{\epsilon}{2}\alpha_1 = P(\alpha_1)$$

as $\alpha_i \neq \alpha_1$, since $i \neq 1$. If for some j, suddenly

$$g_j(P(\alpha_1)) = Q(\alpha_j) + \frac{\epsilon}{2} \cdot \alpha_j = Q(\alpha_1) + \frac{\epsilon}{2}\alpha_1 = P(\alpha_1),$$

then replace P by $P = Q + \frac{\epsilon}{2^k}$ for $k = 2, 3, ...$ till for all $l \neq 1$: $g_l(P(\alpha_1)) \neq P(\alpha_1)$. This means that $L'(P(\alpha_1)) = L^H$. Consider $|.|$ to be the l_2-norm on $L'[x]_{n-1}$. As $|P - Q| = \epsilon/2^k < \epsilon$, we conclude that polynomials $P \in L'[x]_{n-1}$ such that $L'(P(\alpha_1)) = L^H$ are dense in $L'[x]_{n-1}$.
Because $L'[x]_{n-1}$ has dimension n and the zero space of r has dimension $n-1$, $L'[x]_{n-1}$ can not be contained in the zero set of r. Choose now some $P' \in L'[x]_{n-1}$ such that

$$r(P'(\alpha_1), ..., P'(\alpha_n)) \neq 0.$$

By a density argument, with respect to the l_2-norm, we can take $P \in L'[x]_{n-1}$, arbitrarily close to P', such that $L'(P(\alpha_1)) = L^H$ and

$$r(P(\alpha_1), ..., P(\alpha_n)) \neq 0.$$

□

Let $p(x_1, ..., x_n)$ be the product of the denominators of $\phi_1, ..., \phi_n \in M$. The denominators of the coefficients (in $\mathbb{Q}(\phi_1, ..., \phi_n)$) of $g(\phi_1, ..., \phi_n, x)$ are polynomials in $\mathbb{Q}[\phi_1, ..., \phi_n]$. Because $\phi_1, ..., \phi_m \in M$, we can express them in $\mathbb{Q}[x_1, ..., x_n]$. Denote the product of these denominators by $q(x_1, ..., x_n)$. Note that the coefficients of $g(\phi_1, ..., \phi_n, x)$ can, by definition of $f(x)$, also be found when expressing $s_1, ..., s_n \in \mathbb{Q}[x_1, ..., x_n]$, in terms of $\phi_1, ..., \phi_n$. Now, let

$$r(x_1, ..., x_n) = p(x_1, ..., x_n) \cdot q(x_1, ..., x_n).$$

and pick, according to the lemma above, $\alpha_1, ..., \alpha_n \in L$ with the properties as explained in the lemma. Let

$$a = (\phi_1(\alpha_1, ..., \alpha_n), ..., \phi_n(\alpha_1, ..., \alpha_n)).$$

The third condition of the lemma makes a well-defined, because $p(\alpha_1, ..., \alpha_n) \neq 0$ and $g(a, x)$ well-defined as $q(\alpha_1, ..., \alpha_n) \neq 0$. Because $\phi_1, ..., \phi_n \in M$ are G-invariant and G permutes $\alpha_1, ..., \alpha_n$ in the same way as $x_1, ..., x_n$, the coefficients of a are G-invariant, so $a \in L'^n$. Furthermore, from the definitions, we see that $g(a, x)$ is the polynomial we obtain when we substitute $\alpha_1, ..., \alpha_n$ for $x_1, ..., x_n$ in $f(x)$. So $\alpha_1, ..., \alpha_n$ are the zeros of $g(a, x)$. Because of the first condition of the lemma, we conclude $L = \Omega_{L'}^{g(a,x)}$. □

The proposition provides a method we will use to find a generic polynomial in the following section. One could wonder whether there exist groups for which Noether's problem has a negative answer. We will prove later on that there does not exist a generic polynomial for C_8 over $\mathbb{Q}$, which implies that Noether's problem has a negative answer for C_8. There are also groups for which a generic polynomial over $\mathbb{Q}$ exists, but for which Noether's problem has a negative answer. Examples are given in [Swa69] and are C_{47}, C_{113} and C_{233}. A proof why there does exist a generic polynomial for these groups is also given later on.

The following will not come back in the rest of this thesis, but is noted for the interested reader. When we consider K to be equal to $\mathbb{Q}$, there is a special version of the inverse Galois problem, which concerns regular extensions. In the following definition, we let $\mathbf{t} = (t_1, ..., t_n)$, where $t_1, ..., t_n$ are variables that are algebraically independent over $\mathbb{Q}$. First we will write out what it means for an extension to be regular.

Definition 4. A finite Galois extension $\mathbb{M}|\mathbb{Q}(\mathbf{t})$ is *regular* if every element in $\mathbb{M}\backslash\mathbb{Q}$ is transcendental over $\mathbb{Q}$.

The special version is the following.

Problem 4 (The Regular Inverse Galois Problem)**.** Does there exist a regular Galois extension $M|\mathbb{Q}(\mathbf{t})$ such that $\mathrm{Gal}(M|\mathbb{Q}(\mathbf{t})) = G$?

As one can show, a solution for problem 2 immediately implies a solution for this problem without the use of Hilbert's irreducibility theorem. Often, a solution for the Inverse Galois problem is found by solving the Regular Inverse Galois problem first.

3 Generating invariant polynomials

In the previous section, we proved that for every finite group $G \subseteq S_n$, there is a polynomial $h_G \in \mathbb{Q}[x_1, ..., x_n]$ such that $M^G = N(h_G)$. From now on, we will call this h_G a generating invariant polynomial of G. In this section we will find generating invariant polynomials for several groups. These generating invariant polynomials will be used later on, when we want to find out whether Noether's problem is solvable and a generic polynomial exists for these specific groups.

3.1 Cyclic groups

Consider the cyclic groups C_n, which we will define as a subgroup of S_n by $C_n := \langle(12...n)\rangle$. Define

$$g_n := x_1x_2^2 + ... + x_{n-1}x_n^2 + x_nx_1^2 \in \mathbb{Q}[x_1, ..., x_n].$$

As one can see immediately, g_n is invariant under C_n. Furthermore, the following proposition holds.

Proposition 5. For all $\sigma \in S_n$: $\sigma(g_n) = g_n$ if and only if $\sigma \in C_n$.

Proof. We already noticed that g_n is mapped to itself by all $\sigma \in C_n$.
Take now any $\sigma \in S_n$ and suppose $\sigma(g_n) = g_n$. We will show in order to complete the proof that $\sigma \in C_n$. Denote for any $a \in \mathbb{Z}$, by $\overline{a} \in \{1, ..., n\}$, the element such that $a \equiv \overline{a}(\text{mod } n)$. For any $i \in \{1, ..., n\}$:

$$\sigma : x_i \cdot x_{\overline{i+1}}^2 \mapsto x_{\sigma(i)} \cdot x_{\sigma(\overline{i+1})}^2.$$

Pick now an arbitrary $i \in \{1, ..., n\}$. We see, from the definition of g_n, that the only term in g_n with x_i and not x_i^2 is the term $x_ix_{\overline{i+1}}^2$. Therefore, combining this with the way σ acts, we deduce that the only term in $\sigma(g_n)$ with $x_{\sigma(i)}$ and not $x_{\sigma(i)}^2$ is the term $x_{\sigma(i)}x_{\sigma(\overline{i+1})}^2$. Also, from the definition of g_n, the only term in g_n with $x_{\sigma(i)}$ and not $x_{\sigma(i)}^2$ is the term $x_{\sigma(i)}x_{\overline{\sigma(i)+1}}^2$. Since we supposed that $\sigma(g_n) = g_n$, we must have

$$\sigma(\overline{i+1}) = \overline{\sigma(i)+1}.$$

Because we looked at an arbitrary $i \in \{1, ..., n\}$, this statement holds for all $i \in \{1, ..., n\}$, hence by induction, for all $i \in \{1, ..., n\}$:

$$\sigma(i) = \overline{\sigma(1) + i - 1}.$$

This means that $\sigma = (12...n)^{\sigma(1)-1} \in C_n$. $\square$

We conclude that $h_{C_n} = g_n$, i.e. g_n is a generating invariant polynomial of C_n.

3.2 Dihedral groups

The dihedral groups will now be discussed. The dihedral groups are often defined as the group presentation

$$\langle \rho, \tau | \text{ord}(\rho) = n, \text{ord}(\tau) = 2, \tau\rho\tau = \rho^{-1}\rangle.$$

We will work with $\langle\rho, \tau\rangle$ as a subgroup of S_n with $\rho = (12...n)$ and

$$\tau = \begin{cases} (2 \quad n)(3 \quad n-1)...(\frac{n+1}{2} \quad \frac{n+1}{2}+1) & \text{if } n \text{ is odd} \\ (2 \quad n)(3 \quad n-1)...(\frac{n}{2} \quad \frac{n}{2}+2) & \text{if } n \text{ is even.} \end{cases}$$

Indeed $\langle \rho, \tau \rangle = D_n$ as the orders of respectively ρ and τ are n and 2 and one can compute that when n is odd and when n is even, $\tau\rho\tau = \rho^{-1}$. Examples of this presentation are $D_4 = \langle (1234), (24) \rangle$ and $D_5 = \langle (12345), (25)(34) \rangle$.
Define

$$l_n := x_1x_2 + ... + x_{n-1}x_n + x_nx_1 \in \mathbb{Q}[x_1, ..., x_n].$$

As one can easily check, l_n is invariant under D_n. Furthermore, the following proposition holds.

Proposition 6. For all $\sigma \in S_n$: $\sigma(l_n) = l_n$ if and only if $\sigma \in D_n$.

Proof. We already noticed that l_n is mapped to itself by all $\sigma \in D_n$.
Take now any $\sigma \in S_n$ and suppose $\sigma(l_n) = l_n$. We will show in order to complete the proof that $\sigma \in D_n$. Denote again for any $a \in \mathbb{Z}$, by $\overline{a} \in \{1, ..., n\}$, the element such that $a \equiv \overline{a} (\text{mod } n)$. For any $i \in \{1, ..., n\}$:

$$\sigma : x_i \cdot x_{\overline{i+1}} \mapsto x_{\sigma(i)} \cdot x_{\sigma(\overline{i+1})}.$$

Pick now an arbitrary $i \in \{1, ..., n\}$. We see, from the definition of l_n, that the only terms in l_n with x_i are the terms $x_i x_{\overline{i+1}}$ and $x_{\overline{i-1}} x_i$. Therefore, combining this with the way σ acts, we deduce that the only terms in $\sigma(l_n)$ with $x_{\sigma(i)}$ are the terms $x_{\sigma(i)} x_{\sigma(\overline{i+1})}$ and $x_{\sigma(\overline{i-1})} x_{\sigma(i)}$. Also, from the definition of l_n, the only terms in l_n with $x_{\sigma(i)}$ are the terms $x_{\sigma(i)} x_{\overline{\sigma(i)+1}}$ and $x_{\overline{\sigma(i)-1}} x_{\sigma(i)}$. Since we supposed that $\sigma(l_n) = l_n$, we must have

$$\sigma(\overline{i+1}) = \overline{\sigma(i)+1} \text{ or } \sigma(\overline{i+1}) = \overline{\sigma(i)-1}.$$

Assume first that $\sigma(\overline{i+1}) = \overline{\sigma(i)+1}$. Then, because we looked at an arbitrary $i \in \{1, ..., n\}$, this statement holds for all $i \in \{1, ..., n\}$, hence by induction, for all $i \in \{1, ..., n\}$:

$$\sigma(i) = \overline{\sigma(1) + i - 1}.$$

This means that $\sigma = (12...n)^{\sigma(1)-1} = \rho^{\sigma(1)-1} \in D_n$.
Assume now that $\sigma(\overline{i+1}) = \overline{\sigma(i)-1}$. Then, because we looked at an arbitrary $i \in \{1, ..., n\}$, this statement holds for all $i \in \{1, ..., n\}$, hence by induction, for all $i \in \{1, ..., n\}$:

$$\sigma(i) = \overline{\sigma(1) - i + 1}.$$

One can check, for all $i \in \{1, ..., n\}$, from the definition of ρ that:

$$\rho^{\sigma(1)-1}\tau : i \mapsto \overline{\sigma(1) + \tau(i) - 1}$$

and from the definition of τ:

$$\tau : i \mapsto \overline{2 - i}.$$

Combining this gives that for all $i \in \{1, ..., n\}$:

$$\rho^{\sigma(1)-1}\tau : i \mapsto \overline{\sigma(1) - i + 1},$$

hence $\sigma = \rho^{\sigma(1)-1}\tau \in D_n$. $\square$

We conclude that $h_{D_n} = l_n$, i.e. l_n is a generating invariant polynomial of D_n.

3.3 Alternating groups

In this section we discuss a generating invariant polynomial of A_n, which is by definition the subgroup of S_n consisting of all even permutations in S_n. We choose a different approach than the previous subsections, because this allows us to use the results later on.
Let $p(x)$ be a monic separable polynomial of degree n in $N[x]$ with roots $a_1, ..., a_n$ and let the G be its Galois group over N. By definition, elements of G are permutations of $a_1, ..., a_n$. Let A be the subgroup of G consisting of all even permutations in G.

Definition 5. *The discriminant of* $p(x)$, denoted by disc(p) is defined by

$$\mathrm{disc}(p) := \prod_{1 \leq i < j \leq n} (a_i - a_j)^2.$$

Define also

$$\delta_n := \prod_{1 \leq i < j \leq n} (a_i - a_j),$$

the square root of disc(p).

One can see immediately that disc(p) is an element of N, because it is invariant under G. For δ_n, this is not the case, as we will see in the following proposition.

Proposition 7. For all $\sigma \in G$: $\sigma(\delta_n) = \delta_n$ if and only if $\sigma \in A$.

Proof. Consider a permutation $\sigma \in G$. If we look at the action of σ on δ_n, we see that $\sigma(\delta) =$sgn$(\sigma)\delta_n$, as σ permutes $a_1, ..., a_n$. Therefore, δ_n is invariant under σ if and only if sgn$(\sigma) = 1$, i.e. $\sigma \in A$. □

If we take $p(x) = f(x)$, then $G = S_n$, $A = A_n$ and $a_i = x_i$ for $i = 1, ..., n$. Hence, by the proposition

$$\delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

is a generating invariant polynomial of A_n.

4 Noether's problem and generic polynomials for small groups

In this section we will give a positive answer to Noether's problem and describe a generic polynomial for all subgroups of S_n for $n \leq 4$ and Q_8 over $\mathbb{Q}$. At the end, we will also have a try at Q_{16}, which is the smallest group for which it is unknown whether Noether's problem is solved, [JLY02]. This section therefore has the purpose of giving examples of the theory above. First we look at the subgroups of S_n for $n \leq 4$. As earlier mentioned Noether's problem is trivial for S_n, so we will look at the subgroups of S_3 and S_4. As explained above, we only have to look at transitive subgroups. So we will cover $A_3 \subseteq S_3$ and $D_4, C_4, V_4, A_4 \subseteq S_4$.

4.1 Alternating group of order 3

We will show that $\mathbb{Q}(x_1, x_2, x_3)^{A_3} = \mathbb{Q}(s_1, t_1, t_2)$ for algebraically independent t_1, t_2 over $\mathbb{Q}(s_1)$, i.e. Noether's problem is solved for A_3. In order to do that, we will use the results from the previous section.

First note that we can transform $f(x) = x^3 - s_1x^2 + s_2x - s_3$ with $x \mapsto x + s_1/3$ to

$$g(x) = x^3 + (s_2 - \frac{s_1^2}{3})x + (\frac{s_1s_2}{3} - s_3 - 2\frac{s_1^3}{27}) = x^3 + ax + b,$$

with $a = s_2 - \frac{s_1^2}{3}$ and $b = \frac{s_1s_2}{3} - s_3 - 2\frac{s_1^3}{27}$. This transformation does not change the splitting field of the polynomial, so the Galois group of $g(x)$ over N is equal to the Galois group of $f(x)$ over N, which is S_n. From the previous section, we now have $\mathbb{Q}(x_1, x_2, x_3)^{A_3} = N(\delta_3)$, where δ_3 is the square root of $\mathrm{disc}(g)$. The question is now whether $s_1, ..., s_3, \delta_3$ can all be expressed as rational functions in 3 algebraic independent variables over $\mathbb{Q}$.

One can now compute that $\delta_3^2 = -4a^3 - 27b^2$. Write $\delta_3 = t_1a$ and $b = t_2a$ and see that this implies that $t_1^2a^2 = -4a^3 - 27t_2^2a^2$, which solves to $a = \frac{-t_1^2 - 27t_2^2}{4}$ (as $a \neq 0$), hence $\delta = t_1\frac{-t_1^2-27t_2^2}{4}$ and $b = t_2\frac{-t_1^2-27t_2^2}{4}$. This gives with the definition of a and b that

$$s_2 = \frac{-t_1^2 - 27t_2^2}{4} + \frac{s_1^2}{3} \text{ and } s_3 = \frac{s_1(-t_1^2 - 27t_2^2)}{12} + \frac{s_1^3}{9} - t_2\frac{-t_1^2 - 27t_2^2}{4} - \frac{2s_1^3}{27}.$$

So, $N(\delta_3) = \mathbb{Q}(s_1, t_2, t_3)$. In particular this implies that that a polynomial over $\mathbb{Q}(s_1, t_1, t_2)$ with group A_3 can be given by

$$x^3 - s_1x^2 + (\frac{-t_1^2 - 27t_2^2}{4} + \frac{s_1^2}{3})x - \frac{s_1(-t_1^2 - 27t_2^2)}{12} - \frac{s_1^3}{9} + t_2\frac{-t_1^2 - 27t_2^2}{4} + \frac{2s_1^3}{27}.$$

By proposition 4 above, this polynomial is generic for A_3 over $\mathbb{Q}$.

4.2 Dihedral group of order 8

We will now go towards the subgroups of S_4 and start with D_4. Choose without loss of generality for D_4 the presentation $D_4 = \langle(24), (1234)\rangle$. As proved above, $l_4 = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1$ is invariant under D_4. One can check that a permutation of S_4 sends l_4 to itself, $l_4' := x_1x_2 + x_1x_3 + x_3x_4 + x_4x_2$ or $l_4'' := x_2x_4 + x_2x_3 + x_3x_1 + x_4x_1$. Therefore $F(x) = (x - l_4)(x - l_4')(x - l_4'')$ is in $N[x]$ and the minimal polynomial of l_4 over N. In order to have a useful relation in $N(l_4)$, we use the symmetric reduction function of Mathematica (see appendix) to write $F(x)$ in the following way:

$$F(x) = x^3 - 2s_2^2x^2 + (s_2^2 + s_1s_3 - 4s_4)x - (s_1s_2s_3 - s_3^2 - s_1^2s_4),$$

from which we deduce the relation

$$l_4^3 - 2s_2^2l_4^2 + (s_2^2 + s_1s_3 - 4s_4)l_4 - (s_1s_2s_3 - s_3^2 - s_1^2s_4) = 0 \tag{1}$$

in $N(l_4)$. We see that in this relation, for example, s_4 occurs as a linear term. Therefore, we can compute

$$s_4 = \frac{l_4^3 - 2s_2^2l_4^2 + (s_1s_3 + s_2^2)l_4 - s_1s_2s_3 + s_3^2}{4l_4 - s_1^2}.$$

This means that $N(l_4) = \mathbb{Q}(s_1, s_2, s_3, l_4)$ and Noether's problem is solved. In particular, a generic polynomial, by proposition 4, with group D_4 over $\mathbb{Q}$ is given by

$$x^4 - s_1x^3 + s_2x^2 - s_3x + \frac{l_4^3 - 2s_2^2l_4^2 + (s_1s_3 + s_2^2)l_4 - s_1s_2s_3 + s_3^2}{4l_4 - s_1^2} \in \mathbb{Q}(s_1, s_2, s_3, l_4)[x].$$

4.3 Klein four group

In the previous subsection, we discussed the subgroup D_4 of S_4. We continue with discussing the Klein four group $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$, being a subgroup of D_4. This means that $\mathbb{Q}(x_1, x_2, x_3, x_4)^{D_4} \subseteq \mathbb{Q}(x_1, x_2, x_3, x_4)^{V_4}$, so (1) still holds in $\mathbb{Q}(x_1, x_2, x_3, x_4)^{V_4}$. Moreover, $l_4' - l_4'' = (x_1 - x_3)(x_2 - x_4)$ is invariant under V_4, but not under C_4 or D_4, i.e. $\mathbb{Q}(x_1, x_2, x_3, x_4)^{V_4} = N(l_4, l_4' - l_4'')$. As we have that $(l_4' - l_4'')^2$ is invariant under D_4, we must be able to express $(l_4'' - l_4'')^2$ in terms of s_1, s_2, s_3, s_4 and l_4. With the use of Mathematica (see appendix) we derived the expression

$$(l_4' - l_4'')^2 = s_2^2 - 4s_1s_3 + 16s_4 + 2s_2l_4 - 3l_4^2. \tag{2}$$

Because (1) holds, we can substitute the expression derived from (1) for s_4 to obtain

$$(4l_4 + s_1^2)(l_4' - l_4'')^2 = 16(l_4^3 - s_2l_4^2 + s_1s_3l_4 - (s_3^2 - 4s_1s_2)) + (2s_2l_4 - 3l_4^2 + s_2^2 - 4s_1s_3)(4l_4 + s_1^2).$$

Without loss of generality we can assume $s_1 = 0$, because, as we did in the case of A_3 above, we can perform a transformation $x \mapsto x - c$ for some $c \in N$. Therefore, we are left with the relation

$$4l_4(l_4' - l_4'')^2 = 16(l_4^3 - s_2l_4^2 - s_3^2) + 4l_4(2s_2l_4 - 3l_4^2 + s_2^2).$$

Introduce now the parameterization $l_4 = a_1s_2$, $l_4' - l_4'' = a_2s_2$ and $s_3 = a_3s_2$. This gives

$$4a_1a_2^2s_2^3 = (4a_1 - 8a_1^2 + 4a_1^3)s_2^3 - 16a_3^2s_2^2,$$

which solves to $s_2 = \frac{-16a_3^2}{4a_1a_2^2 - 4a_1 + 20a_1^2 - 16a_1^3}$, meaning that s_2, l_4, $l_4' - l_4''$ and s_3 can be expressed in terms of a_1, a_2 and a_3. Combining with the result above for D_4, we have now that

$$\mathbb{Q}(x_1, ..., x_4)^{V_4} = N(l_4, l_4' - l_4'') = \mathbb{Q}(s_1, a_1, a_2, a_3),$$

i.e. $\mathbb{Q}(x_1, ..., x_4)^{V_4}|K$ is rational, so Noether's problem is solved. To be able to come up with a generic polynomial for V_4 over $\mathbb{Q}$, we have to determine how $s_1, ..., s_4$ can be expressed in

$\mathbb{Q}(s_1, a_1, a_2, a_3)$. For s_1 this is trivial and the expressions for s_2 is notated already above. As $s_3 = a_3 s_2$, we can also deduce that $s_3 = \frac{-16a_3^3}{4a_1a_2^2 - 4a_1 + 20a_1^2 - 16a_1^3}$. With the relation of the previous subsection and the fact that $l_4 = a_1 s_2$, we get furthermore

$$\begin{aligned}
s_4 &= \frac{l_4^3 - s_2 l_4^2 + s_1 s_3 l_4 - s_3^2}{4l_4 + s_1^2 - 4s_2} \\
&= \frac{(a_1 s_2)^3 - s_2(a_1 s_2)^2 + s_1 a_3 a_1 s_2^2 - a_3^2 s_2^2}{(4a_1 - 4)s_2 + s_1^2} \\
&= \frac{(a_1^3 - a_1^2)s_2^3 + (s_1 a_3 a_1 - a_3^2)s_2^2}{(4a_1 - 4)s_2 + s_1^2} \\
&= \frac{(a_1^3 - a_1^2)\left(\frac{-16a_3^2}{4a_1a_2^2 - 4a_1 + 20a_1^2 - 16a_1^3}\right)^3 + (s_1 a_3 a_1 - a_3^2)\left(\frac{-16a_3^2}{4a_1a_2^2 - 4a_1 + 20a_1^2 - 16a_1^3}\right)^2}{(4a_1 - 4)\frac{-16a_3^2}{4a_1a_2^2 - 4a_1 + 20a_1^2 - 16a_1^3} + s_1^2} \\
&= \frac{16a_3^6(-1 + a_1 + a_2^2) + a_1 s_1(-1 + 5a_1 - 4a_1^2 + a_2^2)}{a_1(-1 + 5a_1 - 4a_1^2 + a_2^2)^2(16a_3^2(-1 + a_1) + a_1 s_1^2(1 - 5a_1 + 4a_1^2 - a_2^2))}
\end{aligned}$$

This gives the following generic polynomial in $\mathbb{Q}(s_1, a_1, a_2, a_3)[x]$ of V_4 over $\mathbb{Q}$:

$$\begin{aligned}
&x^4 - s_1 x^3 - \frac{16a_3^2}{4a_1a_2^2 - 4a_1 + 20a_1^2 - 16a_1^3} \cdot x^2 + \frac{16a_3^3}{4a_1a_2^2 - 4a_1 + 20a_1^2 - 16a_1^3} \cdot x \\
&+ \frac{16a_3^6(-1 + a_1 + a_2^2) + a_1 s_1(-1 + 5a_1 - 4a_1^2 + a_2^2)}{a_1(-1 + 5a_1 - 4a_1^2 + a_2^2)^2(16a_3^2(-1 + a_1) + a_1 s_1^2(1 - 5a_1 + 4a_1^2 - a_2^2))}.
\end{aligned}$$

4.4 Cyclic group of order 4

We follow the same strategy as above for V_4, but now we use the polynomial $g := (l_4' - l_4'')(x_1 - x_2 + x_3 - x_4)$, which is invariant under C_4 and not under D_4 or V_4 (which can be checked easily). We do not use the generating invariant polynomial, g_4, of the previous section, because its minimal polynomial turns out not to have a term s_i occurring linearly, even after assuming $s_1 = 0$.
Again Mathematica gives the relation

$$g^2 = (s_2^2 - 4s_1 s_3 + 16s_4 + 2s_2 l_4 - 3l_4^2)(s_1^2 - 4s_2 + 4l_4)$$

We assume without loss of generality that $s_1 = 0$ and use (1) to obtain

$$-4l_4 g^2 = 16(l_4^3 - s_2 l_4^2 - s_3^2)(4s_2 - 4l_4) + 4l_4(2s_2 l_4 - 3l_4^2 + s_2^2)(4s_2 - 4l_4).$$

Introduce now the parametrization $l_4 = a_1 s_2$, $g = a_2 s_2$ and $s_3 = a_3 s_2$. Then we obtain the relation

$$-4a_1 a_2^2 s_2^3 = (64(a_1^3 - a_1^2)(1 - a_1) + 16a_1(2a_1 - 3a_1^2 + 1)(1 - a_1))s_2^4 - 64a_3^2(1 - a_1)s_2^3,$$

which solves to $s_2 = \frac{-4a_1a_2^2 + 64a_3^2(1-a_1)}{64(a_1^3 - a_1^2)(1-a_1) + 16a_1(2a_1 - 3a_1^2 + 1)(1-a_1)}$. We conclude

$$\mathbb{Q}(x_1, ..., x_4)^{C_4} = N(l_4, g) = \mathbb{Q}(s_1, a_1, a_2, a_3),$$

i.e. $\mathbb{Q}(x_1,...,x_4)^{C_4}|K$ is rational. Again, we can obtain a generic polynomial by expressing also s_3, s_4 as an element in $\mathbb{Q}(s_1, a_1, a_2, a_3)$. One can check that we get in this case

$$\begin{aligned}
s_3 &= a_3 \cdot \frac{-4a_1a_2^2 + 64a_3^2(1-a_1)}{64(a_1^3-a_1^2)(1-a_1) + 16a_1(2a_1 - 3a_1^2+1)(1-a_1)}, \\
s_4 &= \frac{(a_1^3-a_1^2)\left(\frac{-4a_1a_2^2+64a_3^2(1-a_1)}{64(a_1^3-a_1^2)(1-a_1)+16a_1(2a_1-3a_1^2+1)(1-a_1)}\right)^3}{(4a_1-4)\frac{-4a_1a_2^2+64a_3^2(1-a_1)}{64(a_1^3-a_1^2)(1-a_1)+16a_1(2a_1-3a_1^2+1)(1-a_1)} + s_1^2} \\
&\quad + \frac{(s_1a_3a_1-a_3^2)\left(\frac{-4a_1a_2^2+64a_3^2(1-a_1)}{64(a_1^3-a_1^2)(1-a_1)+16a_1(2a_1-3a_1^2+1)(1-a_1)}\right)^2}{(4a_1-4)\frac{-4a_1a_2^2+64a_3^2(1-a_1)}{64(a_1^3-a_1^2)(1-a_1)+16a_1(2a_1-3a_1^2+1)(1-a_1)} + s_1^2} \\
&= \frac{16(-16a_3^2 + a_1(a_2^2+16a_3^2))^2(16a_3^2 + a_1a_3(95a_3-16s_1) + 47a_1^3a_3s_1 - a_1^2(4a_2^3 + a_3(111a_3+31s_1)))}{(-1+a_1)^4a_1(16+47a_1)^2(256a_3^2 - 31a_1^2s_1^2 + 47a_1^3s_1^2 - 16a_1(a_2^2+16a_3^2+s_1^2))}.
\end{aligned}$$

If we now replace s_2, s_3 and s_4 in the polynomial $x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$ by the complicated expressions above, we get, similar to what we did in previous subsections, a polynomial in $\mathbb{Q}(s_1, a_1, a_2, a_3)$ which is a generic polynomial of C_4 over $\mathbb{Q}$. Because the polynomial gets really large, we will not write it out in full detail.

4.5 Alternating group of order 12

We will use the results above to show now that Noether's problem is also solvable for A_4. We could work with δ_4 as a generating invariant polynomial, but instead we can also work one degree lower, because of the following results. Because V_4 is a normal subgroup of S_4, $\mathbb{Q}(x_1,...,x_4)^{V_4}|N$ is a Galois extension, with Galois group $S_4/V_4 = S_3$. As one can show that $s_2 = l_4 + l_4' + l_4''$, we deduce that $\mathbb{Q}(x_1,...,x_4)^{V_4} = N(l_4, l_4', l_4'')$, so the Galois group S_3 of $\mathbb{Q}(x_1,...,x_4)^{V_4}|N$ is the full permutation group of the polynomials l_4, l_4' and l_4''. As V_4 is a subgroup of A_4, we must have that $\mathbb{Q}(x_1,...,x_4)^{A_4} = (\mathbb{Q}(x_1,...,x_4)^{V_4})^G$ for some subgroup G of S_3. Because A_3 is the only subgroup of S_3 of order 3, we have $G = A_3$. This means that $\mathbb{Q}(x_1,...,x_4)^{A_4} = N(\delta_3)$, with $\delta_3^2 = (l_4 - l_4')(l_4 - l_4'')(l_4' - l_4'')$. An expression in N for δ_3^2 is now given by the discriminant of the minimal polynomial of l_4, l_4' and l_4'', which we recall to be

$$F(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_3^2 - 4s_2s_4 + s_1^2s_4).$$

As we can, without loss of generality, perform a transformation to change F to a polynomial without quadratic term, we have the expression $\delta_3^2 = -4a^3 - 27b^2$ with $a = s_1s_3 - 4s_4$ and $b = s_3^2 - 4s_2s_4 + s_1^2s_4$. Introduce now $\delta_3 = a_1a$ and $b = a_2a$ to obtain, similar to the calculation above, that $a = \frac{-a_1^2-27a_2^2}{4}$ and therefore $\delta_3 = a_1\frac{-a_1^2-27a_2^2}{4}$ and $b = a_2\frac{-a_1^2-27a_2^2}{4}$. With the definition of a and b, we deduce $s_4 = \frac{a_1^2+27a_2^2}{16} + \frac{s_1s_3}{4}$ and

$$s_2 = \frac{a_2(a_1^2+27a_2^2)}{16s_4} + \frac{s_3^2+s_1^2s_4}{4s_4} = \frac{a_2(a_1^2+27a_2^2)}{16s_4} + \frac{s_1^2}{4} + \frac{16s_3^2}{a_1^2+27a_2^2+4s_1s_3}.$$

Therefore we conclude $\mathbb{Q}(x_1, ..., x_4)^{A_4} = N(\delta_3) = \mathbb{Q}(s_1, s_3, a_1, a_2)$ and $\mathbb{Q}(x_1, ..., x_4)^{A_4}|\mathbb{Q}$ is rational. We can also derive the following generic polynomial for A_4 over $\mathbb{Q}$:

$$x^4 - s_1 x^3 + \left(\frac{a_2(a_1^2 + 27a_2^2)}{16 s_4} + \frac{s_1^2}{4} + \frac{16 s_3^2}{a_1^2 + 27 a_2^2 + 4 s_1 s_3} \right) x^2 - s_3 x + \frac{a_1^2 + 27 a_2^2}{16} + \frac{s_1 s_3}{4}.$$

4.6 Quaternion group of order 8

This section will answer the question whether Noether's problem is solvable for Q_8, the quaternion group of order 8, over $\mathbb{Q}$. It was first proved in [Grö34] and this section will describe this method and give a much needed explanation of the several steps. It is interesting to analyze Noether's problem for Q_8, since Noether's problem (even stronger, the question whether there exists a generic polynomial) is unsolved for Q_{16}. The group Q_{16} is in particular one of the smallest groups for which an answer for Noether's problem is not known, as mentioned also in [JLY02].
We begin by describing the group Q_8. First of all, it is a non-abelian group of order eight. It has the following group presentation

$$Q_8 = \langle i, j, k | i^2 = j^2 = k^2 = ijk = e, e^2 = 1 \rangle.$$

In this section, we take the group presentation

$$Q_8 = \langle \sigma_1, \sigma_2, \sigma_3 \rangle \subset S_8,$$

where

$$\begin{aligned} \sigma_1 &= (1458)(2763) \\ \sigma_2 &= (1357)(2468) \\ \sigma_3 &= (1256)(3874). \end{aligned}$$

For this group presentation, we have $e = (15)(26)(37)(48)$. One can check that indeed $\sigma_i^2 = \sigma_1 \sigma_2 \sigma_3 = e$ for $i = 1, 2, 3$. Note that $\sigma_1 = \sigma_2 \sigma_3$, hence $Q_8 = \langle \sigma_2, \sigma_3 \rangle$.
In order to conclude that Noether's problem is solved for Q_8, a priori we have to find elements $t_1, ..., t_8 \in M$, algebraically independent over $\mathbb{Q}$, such that $M^{Q_8} = \mathbb{Q}(t_1, ..., t_8)$. To make this problem manageable, we will use some intermediate steps.
First introduce the following variables

$$\begin{aligned} y_1 &= \frac{1}{2}(x_1 - x_5) & \qquad y_5 &= \frac{1}{2}(x_1 + x_5) \\ y_2 &= \frac{1}{2}(x_2 - x_6) & \qquad y_6 &= \frac{1}{2}(x_2 + x_6) \\ y_3 &= \frac{1}{2}(x_3 - x_7) & \qquad y_7 &= \frac{1}{2}(x_3 + x_7) \\ y_4 &= \frac{1}{2}(x_4 - x_8) & \qquad y_8 &= \frac{1}{2}(x_4 + x_8). \end{aligned}$$

As

$$y_i + y_{i+4} = x_i \text{ for } i = 1, 2, 3, 4 \text{ and } y_i - y_{i-4} = x_i \text{ for } i = 5, 6, 7, 8,$$

we have $M = \mathbb{Q}(y_1, ..., y_8)$. Instead of letting Q_8 act on $x_1, ..., x_8$, we could therefore also let Q_8 act on $y_1, ..., y_8$. This gives

$$\sigma_2 : \begin{cases} y_1 \mapsto y_3 \\ y_2 \mapsto y_4 \\ y_3 \mapsto -y_1 \\ y_4 \mapsto -y_2 \\ y_5 \mapsto y_7 \\ y_6 \mapsto y_8 \\ y_7 \mapsto y_5 \\ y_8 \mapsto y_6 \end{cases} \qquad \sigma_3 : \begin{cases} y_1 \mapsto y_2 \\ y_2 \mapsto -y_1 \\ y_3 \mapsto -y_4 \\ y_4 \mapsto y_3 \\ y_5 \mapsto y_6 \\ y_6 \mapsto y_5 \\ y_7 \mapsto y_8 \\ y_8 \mapsto y_7 \end{cases}$$

Note that $y_5, ..., y_8$ are permuted in the same way as $y_1, ..., y_4$ by σ_2 and σ_3, but without the minus signs. Therefore, something interesting is occurring, which is stated and proved in the following lemma.

Lemma 2. There exists elements $a_0, ..., a_3 \in M^{Q_8}$ such that $\mathbb{Q}(y_1, ..., y_8) = \mathbb{Q}(a_0, ..., a_3, y_1, ..., y_4)$.

Proof. Start by writing

$$\begin{pmatrix} 1 & y_1^2 & y_1^4 & y_1^6 \\ 1 & y_2^2 & y_2^4 & y_2^6 \\ 1 & y_3^2 & y_3^4 & y_3^6 \\ 1 & y_4^2 & y_4^4 & y_4^6 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} y_5 \\ y_6 \\ y_7 \\ y_8 \end{pmatrix}$$

This is a system of 4 equations in 4 unknowns and the determinant of the matrix at the left hand side is nonzero, since the columns are linearly independent. Hence, this system is solvable for $a_0, ..., a_3 \in \mathbb{Q}(y_1, ..., y_8)$. Note that as $y_5, ..., y_8 \in \mathbb{Q}(y_1, ..., y_4, a_0, ..., a_3)$, we have $M = \mathbb{Q}(a_0, ..., a_3, y_1, ..., y_4)$. What is left to prove is that $a_0, ..., a_3 \in M^{Q_8}$. Using Cramer's rule, we obtain

$$a_0 = \begin{vmatrix} y_5 & y_1^2 & y_1^4 & y_1^6 \\ y_6 & y_2^2 & y_2^4 & y_2^6 \\ y_7 & y_3^2 & y_3^4 & y_3^6 \\ y_8 & y_4^2 & y_4^4 & y_4^6 \end{vmatrix} : \begin{vmatrix} 1 & y_1^2 & y_1^4 & y_1^6 \\ 1 & y_2^2 & y_2^4 & y_2^6 \\ 1 & y_3^2 & y_3^4 & y_3^6 \\ 1 & y_4^2 & y_4^4 & y_4^6 \end{vmatrix} \qquad a_1 = \begin{vmatrix} 1 & y_5 & y_1^4 & y_1^6 \\ 1 & y_6 & y_2^4 & y_2^6 \\ 1 & y_7 & y_3^4 & y_3^6 \\ 1 & y_8 & y_4^4 & y_4^6 \end{vmatrix} : \begin{vmatrix} 1 & y_1^2 & y_1^4 & y_1^6 \\ 1 & y_2^2 & y_2^4 & y_2^6 \\ 1 & y_3^2 & y_3^4 & y_3^6 \\ 1 & y_4^2 & y_4^4 & y_4^6 \end{vmatrix}$$

$$a_2 = \begin{vmatrix} 1 & y_1^2 & y_5 & y_1^6 \\ 1 & y_2^2 & y_6 & y_2^6 \\ 1 & y_3^2 & y_7 & y_3^6 \\ 1 & y_4^2 & y_8 & y_4^6 \end{vmatrix} : \begin{vmatrix} 1 & y_1^2 & y_1^4 & y_1^6 \\ 1 & y_2^2 & y_2^4 & y_2^6 \\ 1 & y_3^2 & y_3^4 & y_3^6 \\ 1 & y_4^2 & y_4^4 & y_4^6 \end{vmatrix} \qquad a_3 = \begin{vmatrix} 1 & y_1^2 & y_1^4 & y_5 \\ 1 & y_2^2 & y_2^4 & y_6 \\ 1 & y_3^2 & y_3^4 & y_7 \\ 1 & y_4^2 & y_4^4 & y_8 \end{vmatrix} : \begin{vmatrix} 1 & y_1^2 & y_1^4 & y_1^6 \\ 1 & y_2^2 & y_2^4 & y_2^6 \\ 1 & y_3^2 & y_3^4 & y_3^6 \\ 1 & y_4^2 & y_4^4 & y_4^6 \end{vmatrix}.$$

If we let σ_2 or σ_3 act on these expressions, then the rows of the matrices will interchange. As for both matrices two rows will interchange with two other rows, the sign of the determinants do not change, so the expressions do not change. Therefore, $a_0, ..., a_3$ lie in M^{Q_8}. $\square$

This result reduces our problem a lot. It means that $M^{Q_8} = \mathbb{Q}(y_1, ..., y_4)^{Q_8}(a_0, ..., a_3)$, so we are left with the task of finding $t_1, ..., t_4 \in M^{Q_8}$ such that $\mathbb{Q}(y_1, ..., y_4)^{Q_8} = \mathbb{Q}(t_1, ..., t_4)$.

To establish such $t_1, ..., t_4$, we will need a few steps. The first step is to look at the invariant field $\mathbb{Q}(y_1, ..., y_4)^{\langle\sigma_3\rangle}$ and determine generators for it. After this, we will determine generators $t_1, ..., t_4$

for the invariant field $\left(\mathbb{Q}(y_1,...,y_4)^{\langle\sigma_3\rangle}\right)^{\langle\sigma_2\rangle}$, which is equal to $\mathbb{Q}(y_1,...,y_4)^{Q_8}$ as $\langle\sigma_3\rangle$ is a normal subgroup of Q_8, since it is of index 2.
To prove that some $z_1,...,z_4 \in \mathbb{Q}(y_1,...,y_4)$ have the property $\mathbb{Q}(z_1,...,z_4) = \mathbb{Q}(y_1,...,y_4)^{\langle\sigma_3\rangle}$, we need to check that $z_1,...,z_4$ are σ_3-invariant and furthermore that $\mathbb{Q}(y_1,...,y_4)|\mathbb{Q}(z_1,...,z_4)$ is of degree 4. Choose now

$$\begin{aligned} z_1 &= \frac{y_1y_2}{y_1^2-y_2^2} \\ z_2 &= y_1y_4 + y_2y_3 \\ z_3 &= y_1y_3 - y_2y_4 \\ z_4 &= y_1^2+y_2^2. \end{aligned}$$

One can check from the action of σ_3 on $y_1,...,y_4$ that $z_1,...,z_4$ are invariant under σ_3. We will show now that the extension $\mathbb{Q}(y_1,...,y_4)|\mathbb{Q}(z_1,...,z_4)$ is of degree 4. One can compute that $y_1^2y_2^2 = \frac{z_1^2z_4^2}{1+4z_1^2}$, so the minimal polynomial of y_1 over $\mathbb{Q}(y_1,...,y_4)^{\langle\sigma_3\rangle}$ is

$$\begin{aligned} (x-y_1)(x+y_1)(x+y_2)(x-y_2) &= x^4-(y_1^2+y_2^2)x^2+y_1^2y_2^2 \\ &= x^4 - z_4x^2 + \frac{z_1^2z_4^2}{1+4z_1^2} \in \mathbb{Q}(z_1,...,z_4)[x]. \end{aligned}$$

As

$$\begin{aligned} y_2 &= \frac{z_1(2y_1^2-z_4)}{y_1} \\ y_3 &= (y_1z_3+y_2z_2)z_4^{-1} \\ y_4 &= (y_1z_2-y_2z_3)z_4^{-1}, \end{aligned}$$

we have $\mathbb{Q}(y_1,...,y_4) = \mathbb{Q}(z_1,...,z_4)(y_1)$, hence $\mathbb{Q}(y_1,...,y_4)|\mathbb{Q}(z_1,...,z_4)$ is at most of degree 4. As $\mathbb{Q}(z_1,...,z_4) \subseteq \mathbb{Q}(y_1,...,y_4)^{\langle\sigma_3\rangle}$, we conclude $\mathbb{Q}(y_1,...,y_4)|\mathbb{Q}(z_1,...,z_4)$ is of degree 4 and $\mathbb{Q}(z_1,...,z_4)$ equals $\mathbb{Q}(y_1,...,y_4)^{\langle\sigma_3\rangle}$. We will now determine $t_1,...,t_4$ such that $\mathbb{Q}(t_1,...,t_4) = \mathbb{Q}(z_1,...,z_4)^{\langle\sigma_2\rangle}$.
Once again, we need to check for some $t_1,...,t_4 \in \mathbb{Q}(z_1,...,z_4)$ to have the property $\mathbb{Q}(t_1,...,t_4) = \mathbb{Q}(z_1,...,z_4)^{\langle\sigma_2\rangle}$, that $t_1,...,t_4$ are σ_2-invariant and furthermore that $\mathbb{Q}(z_1,...,z_4)|\mathbb{Q}(t_1,...,t_4)$ is of degree 2. Let

$$\begin{aligned} t_1 &= \frac{z_4-\sigma_2(z_4)}{z_3} && = \frac{y_1^2+y_2^2-y_3^2-y_4^2}{y_1y_3-y_2y_4} \\ t_2 &= z_4+\sigma_2(z_4) && = y_1^2+y_2^2+y_3^2+y_4^2 \\ t_3 &= \frac{z_2}{z_3} && = \frac{y_1y_4+y_2y_3}{y_1y_3-y_2y_4} \\ t_4 &= \frac{z_3(2z_3z_1-z_2)}{2z_1z_2+z_3} && = \frac{(y_1y_3-y_2y_4)(y_1y_4-y_2y_3)}{y_1y_3+y_2y_4}. \end{aligned}$$

One can check (using software such as Mathematica) that the second column of equalities is correct and from the expressions in $\mathbb{Q}(y_1,...,y_4)$ that the t_i's are invariant under σ_2. We are left with the task to show that $\mathbb{Q}(z_1,...,z_4)|\mathbb{Q}(t_1,...,t_4)$ is of degree 2. It is enough to show that

$\mathbb{Q}(t_1,...,t_4)(z_3)|\mathbb{Q}(z_1,...,z_4)$ is of degree 2, because from the definitions, we can see

$$\begin{aligned} z_2 &= t_3 z_3 \\ z_4 &= \frac{t_1 z_3 + t_2}{2} \\ z_1 &= \frac{z_3(z_2+t_4)}{2(z_3^2 - z_2 t_4)}, \end{aligned}$$

As $\sigma_2(z_3) = -z_3$, the minimal polynomial of z_3 over $\mathbb{Q}(y_1,...,y_4)^{Q_8}$ is

$$(x - z_3)(x + z_3) = x^2 - z_3^2.$$

Once we have shown that $z_3^2 \in \mathbb{Q}(t_1,...,t_4)$, then we are done. Since,

$$\sigma_2(z_4) = \sigma_2(y_1^2 + y_2^2) = y_3^2 + y_4^2 = \frac{z_2^2 + z_3^2}{z_4},$$

We know that $z_4\sigma_2(z_4) = z_2^2 + z_3^2$. Therefore,

$$(z_4 + \sigma_2(z_4))^2 = (z_4 - \sigma_2(z_4))^2 + 4z_4\sigma_2(z_4) = (z_4 - \sigma_2(z_4))^2 + 4z_2^2 + z_3^2,$$

hence

$$z_3^2 = z_3^2 \cdot \frac{(z_4 + \sigma_2(z_4))^2}{(z_4 - \sigma_2(z_4))^2 + 4z_2^2 + z_3^2} = \frac{(z_4 + \sigma_2(z_4))^2}{\left(\frac{z_4 - \sigma_2(z_4)}{z_3}\right)^2 + 4\left(\frac{z_2}{z_3}\right)^2 + 4} = \frac{t_2^2}{t_1^2 + 4(t_3^2 + 1)}.$$

We conclude that $\mathbb{Q}(t_1,...,t_4)(z_3)|\mathbb{Q}(z_1,...,z_4)$ is of degree 2, so $\mathbb{Q}(t_1,...,t_4) = \mathbb{Q}(y_1,...,y_4)^{Q_8}$. Combining this with the results above gives

$$M^{Q_8} = \mathbb{Q}(t_1,...,t_4,a_0,...,a_3),$$

i.e. Noether's problem is solved for Q_8 over $\mathbb{Q}$.

Furthermore, this solution provides us with tools to build a generic polynomial for Q_8 over $\mathbb{Q}$. Define

$$g(y) = \prod_{i=1}^{4}(y - y_i)(y + y_i).$$

The action of σ_2 and σ_3 on $y_1,...,y_4$ is described above. One can see that $g(y)$ is invariant under σ_2 and σ_3, so $g(y)$ is an element of

$$M^{Q_8}[y] = \mathbb{Q}(a_0,...,a_3,t_1,...,t_4)[y].$$

We will now explicitly compute the coefficients of $g(y)$ and we will see that the coefficients lie in $\mathbb{Q}(t_1,...,t_4)$. Expanding $g(y)$ gives

$$g(y) = y^8 - p_1y^6 + p_2y^4 - p_3y^2 + p_4,$$

where

$$\begin{aligned}
p_1 &= y_1^2 + y_2^2 + y_3^2 + y_4^2 \\
p_2 &= y_1^2y_2^2 + y_1^2y_3^2 + y_1^2y_4^2 + y_2^2y_3^2 + y_2^2y_4^2 + y_3^2y_4^2 \\
p_3 &= y_1^2y_2^2y_3^2 + y_1^2y_2^2y_4^2 + y_1^2y_3^2y_4^2 + y_2^2y_3^2y_4^2 \\
p_4 &= y_1^2y_2^2y_3^2y_4^2.
\end{aligned}$$

These coefficients can be expressed in terms of $t_1, ..., t_4$ in the following way.

$$\begin{aligned}
p_1 &= \frac{1}{2}t_4 \\
p_2 &= \frac{t_4^2}{64t_5}\left(\frac{8t_1t_2t_3t_4t_5 - (1-t_3^2)(t_4^2 - t_1^2t_5)(t_2^2+t_5)}{(1+t_3^2)(t_4^2+t_1^2t_5)} + 2t_2^2 + 20(t_3^2+1)\right) \\
p_3 &= \frac{t_4^3}{64t_5}\left(\frac{4t_1t_2t_3t_4 - (1-t_3^2)(t_4^2 - t_1^2t_5)}{t_4^2 + t_1^2t_5} + 1 + t_3^2\right) \\
p_4 &= \left(\frac{t_4^2(t_3^2t_4^2 - t_1^2t_5)}{16t_5(t_4^2 + t_1^2t_5)}\right)^2,
\end{aligned}$$

where

$$t_5 = t_2^2 + 4t_3^2 + 4 = \left(\frac{y_1^2 + y_2^2 + y_3^2 + y_4^2}{y_1y_3 - y_2y_4}\right)^2.$$

One can check from the definitions of $t_1, ..., t_4$ that these expressions are correct. Now, transform $g(y) = 0$ with

$$x = a_0 + y + a_1y^2 + a_2y^4 + a_3y^6$$

to the polynomial equation

$$h(x) = x^8 + b_1x^7 + ... + b_7x + b_8 = 0.$$

These kind of transformations are called Tschirnhaus transformations. Note that the coefficients of $h(x)$ lie in $\mathbb{Q}(a_0, ..., a_3, t_1, ..., t_4) = M^{Q_8}$. Because

$$x_i = y_i + y_{i+4} = a_0 + y_i + a_1y_i^2 + a_2y_i^4 + a_3y_i^6$$

for $i = 1, ..., 4$, the variables $x_1, ..., x_4$ are roots of $h(x)$. Because $h(x) \in M^{Q_8}[x]$, we must have that the other 4 roots of $h(x)$ are $x_5, ..., x_8$. This means that $h(x) = f(x)$, where $f(x)$ was defined in ($\star$). By proposition 4, we conclude that $h(x)$ is generic for Q_8 over $\mathbb{Q}$. It will be a mess to express $h(x)$ in $\mathbb{Q}(a_0, ..., a_3, t_1, ..., t_4)[x]$, so instead we will give an example. One can consider

$$\begin{aligned}
t_1 &= -12 \qquad & a_0 &= 15 \\
t_2 &= 8 & a_0 &= -\frac{175}{4} \\
t_3 &= 1 & a_0 &= \frac{80}{3} \\
t_4 &= 144 & a_0 &= -\frac{3}{8}.
\end{aligned}$$

Then, one can compute with the defining definitions that

$$p_1 = 72, p_2 = 180, p_3 = 144, p_4 = 36,$$

so

$$g(y) = y^8 - 72y^6 + 180y^4 - 144y^2 + 36.$$

We use the Tschirnhaus transformation

$$x = 15 + y - \frac{175}{4}y^2 + \frac{80}{3}y^4 - \frac{3}{8}y^6$$

to obtain the polynomial

$$h(x) = x^8 - 92x^6 - 432x^5 - 366x^4 + 864x^3 + 1180x^2 + 48x - 239.$$

This polynomial has Galois group Q_8 over $\mathbb{Q}$, as obtained by Mertens, in [Mer02] and [Mer16]. He did this when the existence of a generic polynomial for Q_8 over $\mathbb{Q}$ was not proved yet.

4.7 Quaternion group of order 16

One might wonder whether the approach of the previous subsection to solve Noether's problem for Q_8 also works for Q_{16}. We will give it a try and reduce Noether's problem to a smaller problem, concerning less variables.

As above, for Q_8, we start by defining the group Q_{16}. It is an example of a dicyclic group and has the presentation

$$Q_{16} = \langle a, b | a^8 = 1, b^2 = a^4, b^{-1}ab = a^{-1} \rangle.$$

As a subgroup of S_{16}, we could take the group presentation

$$Q_{16} = \langle \sigma_1, \sigma_2 \rangle,$$

where

$$\begin{aligned} \sigma_1 &= (1 \quad 2 \quad \dots \quad 8)(9 \quad 10 \quad \dots \quad 16) \\ \sigma_2 &= (1 \quad 10 \quad 5 \quad 14)(11 \quad 4 \quad 15 \quad 8)(2 \quad 9 \quad 6 \quad 13)(3 \quad 16 \quad 7 \quad 12). \end{aligned}$$

We leave it to the reader to check that indeed $\sigma_2^2 = \sigma_1^4$ and $\sigma_2^{-1}\sigma_1\sigma_2 = \sigma_1^{-1}$. We let Q_{16} act on $M = \mathbb{Q}(x_1, \dots, x_{16})$, so Noether's problem wonders whether $M^{Q_{16}}|M$ is a rational extension.

Similar as before, we introduce the expressions $y_1, ..., y_{16}$, which are defined to be

$$\begin{aligned}
y_1 &= \frac{1}{2}(x_1 - x_5) & y_9 &= \frac{1}{2}(x_1 + x_5) \\
y_2 &= \frac{1}{2}(x_2 - x_6) & y_{10} &= \frac{1}{2}(x_2 + x_6) \\
y_3 &= \frac{1}{2}(x_3 - x_7) & y_{11} &= \frac{1}{2}(x_3 + x_7) \\
y_4 &= \frac{1}{2}(x_4 - x_8) & y_{12} &= \frac{1}{2}(x_4 + x_8). \\
y_5 &= \frac{1}{2}(x_9 - x_{13}) & y_{13} &= \frac{1}{2}(x_9 + x_{13}) \\
y_6 &= \frac{1}{2}(x_{10} - x_{14}) & y_{14} &= \frac{1}{2}(x_{10} + x_{14}) \\
y_7 &= \frac{1}{2}(x_{11} - x_{15}) & y_{15} &= \frac{1}{2}(x_{11} + x_{15}) \\
y_8 &= \frac{1}{2}(x_{12} - x_{16}) & y_{16} &= \frac{1}{2}(x_{12} + x_{16}).
\end{aligned}$$

As $y_i + y_{i+8} = x_i$ for $i = 1, ..., 8$ and $y_i - y_{i-8} = x_i$ for $i = 9, ..., 16$, we have that $M = \mathbb{Q}(y_1, ..., y_{16})$. Instead of letting Q_{16} act on $x_1, ..., x_{16}$, we could also let it act on $y_1, ..., y_{16}$. This gives

$$\sigma_1 : \begin{cases} y_1 \mapsto y_2 & y_9 \mapsto y_{10} \\ y_2 \mapsto y_3 & y_{10} \mapsto y_{11} \\ y_3 \mapsto y_4 & y_{11} \mapsto y_{12} \\ y_4 \mapsto -y_1 & y_{12} \mapsto y_9 \\ y_5 \mapsto y_6 & y_{13} \mapsto y_{14} \\ y_6 \mapsto y_7 & y_{14} \mapsto y_{15} \\ y_7 \mapsto y_8 & y_{15} \mapsto y_{16} \\ y_8 \mapsto -y_1 & y_{16} \mapsto y_{13} \end{cases} \qquad \sigma_2 : \begin{cases} y_1 \mapsto y_6 & y_9 \mapsto y_{14} \\ y_2 \mapsto y_5 & y_{10} \mapsto y_{13} \\ y_3 \mapsto -y_8 & y_{11} \mapsto y_{16} \\ y_4 \mapsto -y_7 & y_{12} \mapsto y_{15} \\ y_5 \mapsto -y_2 & y_{13} \mapsto y_{10} \\ y_6 \mapsto -y_1 & y_{14} \mapsto y_9 \\ y_7 \mapsto y_4 & y_{15} \mapsto y_{12} \\ y_8 \mapsto y_3 & y_{11} \mapsto y_{15} \end{cases}$$

Note that $y_9, ..., y_{16}$ are permuted in the same way as $y_1, ..., y_8$ by σ_1 and σ_2, but without the minus signs. As in the previous section, in which we proved lemma 2, we know now that there exists elements $a_0, ..., a_7 \in M^{Q_{16}}$ such that $M = \mathbb{Q}(a_0, ..., a_7)(y_1, ..., y_8)$. We could reproduce the proof of lemma 2 for 16 variables instead of 8, but because it is highly similar, we will skip it.
Noether's problem is now reduced to finding $t_1, ..., t_8$ such that $\mathbb{Q}(y_1, ..., y_8)^{\langle\sigma_1,\sigma_2\rangle} = \mathbb{Q}(t_1, ..., t_8)$. Because σ_1 has order 8, we know that $\langle\sigma_1\rangle$ is a normal subgroup of Q_{16}. Therefore, $\mathbb{Q}(y_1, ..., y_8)^{\langle\sigma_1,\sigma_2\rangle} = (\mathbb{Q}(y_1, ..., y_8)^{\langle\sigma_1\rangle})^{\langle\sigma_2\rangle}$, so we will first try to come up with $z_1, ..., z_8$ such that $\mathbb{Q}(y_1, ..., y_8)^{\langle\sigma_1\rangle} = \mathbb{Q}(z_1, ..., z_8)$. One could define

$$\begin{aligned}
z_5 &= y_1y_5 + y_2y_6 + y_3y_7 + y_4y_8 \\
z_6 &= y_1y_6 + y_2y_7 + y_3y_8 - y_4y_5 \\
z_7 &= y_1y_7 + y_2y_8 - y_3y_5 - y_4y_6 \\
z_8 &= y_1y_8 - y_2y_5 - y_3y_6 - y_4y_7.
\end{aligned}$$

It is easy with the action of σ_1, as described above, to check that these $z_5, ..., z_8$ are invariant under σ_1. Furthermore, these $z_5, ..., z_8$ are chosen in a way that makes sure that $y_5, ..., y_8$ lie in $\mathbb{Q}(z_5, ..., z_8)(y_1, ..., y_4)$, because

$$\begin{pmatrix} y_1 & y_2 & y_3 & y_4 \\ -y_4 & y_1 & y_2 & y_3 \\ -y_3 & -y_4 & y_1 & y_2 \\ -y_2 & -y_3 & -y_4 & y_1 \end{pmatrix} \begin{pmatrix} y_5 \\ y_6 \\ y_7 \\ y_8 \end{pmatrix} = \begin{pmatrix} z_5 \\ z_6 \\ z_7 \\ z_8 \end{pmatrix}$$

and the matrix at the left hand side is clearly invertible. This reduces our problem to finding $z_1, ..., z_4$, which must be invariant under the action of σ_1 and make sure that
$\mathbb{Q}(z_1, ..., z_8)(y_1, ..., y_4)|\mathbb{Q}(z_1, ..., z_8)$ is of degree 8. This last property could be analyzed ever further. Since the minimal polynomial of y_1 over $\mathbb{Q}(y_1, ..., y_4)^{\langle\sigma_1\rangle}$ is $\prod_{i=1}^{4}(x + y_i)(x - y_i)$, which is of degree 8, $\mathbb{Q}(y_1, ..., y_4)^{\langle\sigma_1\rangle}(y_1)|\mathbb{Q}(y_1, ..., y_4)^{\langle\sigma_1\rangle}$ is of degree 8.
Therefore, we conclude that we reduced the problem to finding $z_1, ..., z_4 \in \mathbb{Q}(y_1, ..., y_4)^{\langle\sigma_1\rangle}$ such that $\mathbb{Q}(z_1, ..., z_4)(y_1) = \mathbb{Q}(y_1, ..., y_4)$ and $\prod_{i=1}^{4}(x + y_i)(x - y_i) \in \mathbb{Q}(z_1, ..., z_4)[x]$. Unfortunately, despite several attempts, we did not manage to solve this problem yet. A second step would be to find $t_1, ..., t_8$ such that $\mathbb{Q}(z_1, ..., z_8)^{\langle\sigma_2\rangle} = \mathbb{Q}(t_1, ..., t_8)$. Since $\langle\sigma_2\rangle$ is cyclic of order 4, this would be similar to the problem above for Q_8. This together would solve Noether's problem for Q_{16}.

5 Generic polynomials for cyclic groups

In this section we will discuss the existence of generic polynomials for the cyclic groups. It will turn out that for the majority of these groups, a generic polynomial exists. There are, however exceptions, such as the cyclic group of order 8. Two explicit constructions are described for generic polynomials for small cyclic groups, which we will use to give examples.

5.1 Cyclic groups of odd order

As mentioned above in the introduction of this thesis, the existence of generic polynomials for a product of groups $G \times H$ is guaranteed if there exists generic polynomials for G and H. Therefore, we only have to look at cyclic groups C_q of order $q = p^n$, where p is a prime and $n \geq 1$. As the title of this section suggests, we assume that p is odd. This section will explain and prove the existence of generic polynomials for C_q over $\mathbb{Q}$. This means that for every cyclic group of odd order, a generic polynomial over $\mathbb{Q}$ exists. We will discuss two constructions of a generic polynomial and describe the similarity between them.

5.1.1 Elementary construction

We now recall the construction of generic polynomials for C_q as briefly described in [Smi91] added with some necessary details and explanations.
Denote by ζ a primitive q-th root of unity in $\overline{\mathbb{Q}}$. Then, $\mathbb{Q}(\zeta)|\mathbb{Q}$ is the cyclotomic cyclic extension of degree $\varphi(q)$, where φ is Euler's phi function. Denote for any $m \in \mathbb{Z}$ by $\overline{m} \in \{0, ..., q-1\}$ the integer such that $m \equiv \overline{m} (\text{mod } q)$. Define $\{c_i | \gcd(i, q) = 1 \text{ and } 0 < i < q\}$, where the c_i's are $\varphi(q)$ algebraically independent indeterminates over $\mathbb{Q}$. For $c_i \in \{c_i | \gcd(i, q) = 1 \text{ and } 0 < i < q\}$, let $b_i = c_i^q$. Define for $0 \leq i \leq q$:

$$e_i = \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^\times} c_j^{\overline{i/j}}$$

if i is relatively prime to q and $e_i = 0$ otherwise. Let $r_i = \sum_{j=0}^{q-1} e_j \zeta^{ij}$ for $i = 1, ..., q-1$ and consider

$$P(z) = \prod_{i=0}^{q-1} (z - r_i).$$

Proposition 8. The polynomial $P(z)$ has coefficients in $\mathbb{Z}[b_1, ..., b_{q-1}]$.

Proof. By construction, we see that $P(z) \in \mathbb{Z}[c_1, ..., c_{q-1}, \zeta][z]$. Let k be any element in $\{1, ..., q-1\}$ such that $\gcd(k, q) = 1$. We will show that $P(z)$ is invariant under the action $\zeta \mapsto \zeta^k$, to conclude that $P(z) \in \mathbb{Z}[c_1, ..., c_{q-1}][z]$. Furthermore, we will show that $P(z)$ is invariant under $c_k \mapsto \zeta c_k$. This implies that all coefficients of $P(z)$, which are polynomials in $\mathbb{Z}[c_1, ..., c_{q-1}]$, are invariant under $c_k \mapsto \zeta c_k$, hence contain only q-th powers of c_k. As c_k is any element of $\{c_1, ..., c_{q-1}\}$, we can conclude that $P(z) \in \mathbb{Z}[b_1, ..., b_{q-1}][z]$.
The action $\rho : \zeta \mapsto \zeta^k$ gives

$$\rho : r_i = \sum_{j=0}^{q-1} e_j \zeta^{ij} \mapsto \sum_{j=0}^{q-1} e_j \zeta^{ijk} = r_{ik}$$

for $i = 1, ..., q-1$. As $1 \leq k \leq q-1$ and $\gcd(q,k) = 1$, this means that ρ permutes $r_1, ..., r_{q-1}$. Therefore, ρ leaves $P(z)$ invariant.
The action $\lambda : c_k \mapsto \zeta c_k$ gives

$$\lambda : e_i = \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^\times} c_j^{\overline{i/j}} \mapsto \zeta^{i/k} \cdot \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^\times} c_j^{\overline{i/j}} = \zeta^{i/k} e_i,$$

for all $i = 1, ..., q-1$ relatively prime to q. Hence,

$$\lambda : r_i = \sum_{j=0}^{q-1} e_j \zeta^{ij} \mapsto \sum_{j=0}^{q-1} e_j \zeta^{(i+k^{-1})j} = r_{i+k^{-1}}$$

for $i = 1, ..., q-1$. This means that λ permutes $r_1, ..., r_{q-1}$, so λ leaves $P(z)$ invariant. $\square$

Let $\mu_0, ..., \mu_{\varphi(q)-1}$ be a basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$ and let $t_0, ..., t_{\varphi(q)-1}$ be algebraically independent (over $\mathbb{Q}$) indeterminates. Set

$$\widetilde{b_1} = t_0\mu_0 + ... + t_{\varphi(q)-1}\mu_{\varphi(q)-1}$$

and $\widetilde{b_i} = \gamma_i(\widetilde{b_1})$, where $\gamma_i \in$Gal$(\mathbb{Q}(\zeta)|\mathbb{Q})$ is defined by $\gamma_i : \zeta \mapsto \zeta^i$. Replace now the b_i's in $P(z)$ by $\widetilde{b_i}$'s and denote the resulting polynomial by $\widetilde{P(z)}$.

Proposition 9. The polynomial $\widetilde{P(z)}$ has coefficients in $\mathbb{Z}[t_0, ..., t_{\varphi(q)-1}]$.

Proof. From the construction, we see that $\widetilde{P(z)}$ has coefficients in $\mathbb{Z}[t_0, ..., t_{\varphi(q)-1}, \zeta]$. So it is enough to prove that $\widetilde{P(z)}$ is invariant under the action of γ_k, where k is any integer in $\{1, ..., q-1\}$ such that $\gcd(k,q) = 1$. The action of γ_k on the $\widetilde{b_i}$'s is the following:

$$\gamma_k : \widetilde{b_i} = \gamma_i(\widetilde{b_1}) \mapsto \gamma_k(\gamma_i(\widetilde{b_1})) = \gamma_{ki}(\widetilde{b_1}) = \widetilde{b_{\overline{ki}}}.$$

for $i = 1, ..., q-1$ such that $\gcd(i,q) = 1$. Therefore, the polynomial $\gamma_k(\widetilde{P(z)})$ is also obtained when letting $\eta : c_i \mapsto c_{\overline{ki}}$ act on $P(z)$ and after that replacing c_i by $\widetilde{b_i}^{1/q}$ for $i = 1, ..., q-1$. This means it is sufficient, in order to prove the proposition, to show that η leaves $P(z)$ invariant. The action η gives

$$\eta : e_i = \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^\times} c_j^{\overline{i/j}} \mapsto \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^\times} c_{\overline{jk}}^{\overline{i/j}} = \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^\times} c_{\overline{jk}}^{\overline{ik/(kj)}} = e_{ki}$$

for all $i = 1, ..., q-1$ relatively prime to q. Hence,

$$\eta : r_i = \sum_{j=0}^{q-1} e_j \zeta^{ij} \mapsto \sum_{j=0}^{q-1} e_{kj} \zeta^{ij} = \sum_{j=0}^{q-1} e_{kj} \zeta^{i\overline{k}^{-1} \cdot kj} = r_{i \cdot \overline{k}^{-1}}$$

for $i = 1, ..., q-1$. This means that η permutes $r_1, ..., r_{q-1}$, so η leaves $P(z)$ invariant. $\square$

Furthermore, we are able to prove the following proposition.

Proposition 10. The polynomial $\widetilde{P(z)}$ is irreducible over the field $\mathbb{Q}(t_0, ..., t_{\varphi(q)-1})$.

Proof. Consider the specialization of $\widetilde{P(z)}$ with $t_0 = t$, $t_1 = -1$ and $t_i = 0$ for $i > 1$ and denote it by $\widetilde{P(z)}_0$. Also, let $\mu_i = \zeta^i$ for $i \geq 0$. Then, in $\widetilde{P(z)}_0$: $\widetilde{b_i} = t - \zeta^i$, so $\widetilde{P(z)}_0 \in \mathbb{Z}[t][z]$. In order to prove the proposition, it is enough to prove that $\widetilde{P(z)}_0$ is irreducible over $\mathbb{Q}$. In order to prove this, we will check that $\widetilde{P(z)}_0$ is an Eisenstein polynomial with respect to the polynomial

$$\psi := \prod_{i\in(\mathbb{Z}/q\mathbb{Z})^\times} \widetilde{b_i} = \prod_{i\in(\mathbb{Z}/q\mathbb{Z})^\times} (t - \zeta^i).$$

This polynomial ψ is called the q-th cyclotomic polynomial and it is the minimal polynomial of ζ over $\mathbb{Q}$, hence irreducible over $\mathbb{Q}$. Hence, we will check, as $\widetilde{P(z)}_0$ is monic, that ψ is a divisor of all (except the highest) coefficients of $\widetilde{P(z)}_0$ and that it divides the constant term of $\widetilde{P(z)}_0$ only once.

For the first claim, look at $P(z)$. It is enough to show that $\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^\times} b_i$ is a divisor of all (except the highest) coefficients of $P(z)$. By definition, we see that $\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^\times} c_i$ is a divisor of e_i for $i = 1, ..., q-1$. Therefore, $\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^\times} c_i$ is a divisor of r_i for $i = 1, ..., q-1$, hence a divisor of all coefficients of $P(z)$, which are symmetric polynomials in the r_i's. As $P(z) \in \mathbb{Z}[b_1, ..., b_{q-1}][z]$, all (except the highest) coefficients of $P(z)$ are divisible by $\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^\times} b_i$.
For the second claim, note that $\widetilde{P(z)}_0$ can also be obtained when performing the following operation to $P(z)$ (considered to be in $\mathbb{Z}[c_1, ..., c_{q-1}][z]$):

$$c_i \mapsto (t - \zeta^i)^{1/q}$$

for $i = 1, ..., q-1$ relatively prime to q. Then, the e_i's become a

$$\frac{1}{q} \cdot \sum_{i\in(\mathbb{Z}/q\mathbb{Z})^\times} i = \frac{1}{q} \cdot \frac{q}{2} \cdot \varphi(q) = \frac{1}{2}\varphi(q)$$

degree polynomial in t, which means the r_i's are also of degree $\frac{1}{2}\varphi(q)$ in t. The constant term of $\widetilde{P(z)}_0$ is equal to $\prod_{i=0}^{q-1} r_i$, hence a $\frac{q}{2}\varphi(q)$ degree polynomial in t. The degree of ψ^2 clearly is $\varphi(q)^2$. Because q is a power of a prime, $q/2 < \varphi(q)$, hence

$$\deg\left(\prod_{i=0}^{q-1} r_i\right) = \frac{q}{2}\varphi(q) < \varphi(q)^2 = \deg(\psi^2).$$

Therefore, $\prod_{i=0}^{q-1} r_i$ can not be divisible by ψ^2. We conclude that $\widetilde{P(z)}_0$ is Eisenstein, hence irreducible over $\mathbb{Q}$. □

As $\widetilde{P(z)}$ is irreducible over a field of characteristic zero, it is separable. Hence, it generates a Galois extension. The following proposition shows that is has the desired Galois group. The proof of the proposition is also described in a short way in [Den95].

Proposition 11. The polynomial $\widetilde{P(z)}$ has Galois group C_q over the field $\mathbb{Q}(t_0, ..., t_{\varphi(q)-1})$.

Proof. Let $K = \mathbb{Q}(t_0, ..., t_{\varphi(q)-1})$. We will first show that the Galois group of $\widetilde{P(z)}$ over $K(\zeta)$ is equal to C_q. As $\zeta \in \mathbb{Q}(\zeta)$, the matrix $(\gamma_i(\mu_j))_{i,j\in(\mathbb{Z}/q\mathbb{Z})^\times}$, occurring in the formulas for $\widetilde{b_i}$, is invertible over $\mathbb{Q}(\zeta)$, so

$$K(\zeta) = \mathbb{Q}(t_0, ..., t_{\varphi(q)-1}, \zeta) = \mathbb{Q}(\widetilde{b_1}, ..., \widetilde{b_{q-1}}, \zeta).$$

Hence, $\widetilde{b_1}, ..., \widetilde{b_{q-1}}$ are algebraically independent over $\mathbb{Q}(\zeta)$, and so are $\{e_i | 1 \le i \le q-1, \gcd(i,q) = 1\}$. Hence, the splitting field of $\widetilde{P(z)}$ over $K(\zeta)$ is equal to

$$K(\zeta)(r_0, ..., r_{q-1}) = K(\zeta)(e_1, ..., e_{q-1}).$$

Denote this splitting field by N. Let $\sigma \in \mathrm{Gal}_{K(\zeta)}(\widetilde{P(z)})$ be a permutation of $r_0, ..., r_{q-1}$, which sends r_0 to r_l. For any $i \in \{1, ..., q-1\}$ relatively prime to q, we have $e_i^q \in \mathbb{Q}(b_1, ..., b_{q-1}, \zeta) = K(\zeta)$. Hence, $\sigma(e_i)^q = e_i^q$ and there exists a $k_i \in \mathbb{Z}$ such that $\sigma(e_i) = \zeta^{k_i} e_i$. Then,

$$r_l = \sum_{j=0}^{q-1} e_j \zeta^{lj} = \sigma(r_0) = \sum_{j=0}^{q-1} \sigma(e_j) = \sum_{j=0}^{q-1} e_j \zeta^{k_j}.$$

Therefore, for $j = 1, ..., q-1$ relatively prime to q, $k_j = \overline{lj}$. Therefore, $\sigma(r_j) = r_{\overline{j+l}}$ and the Galois group of $\widetilde{P(z)}$ over $K(\zeta)$ is equal to C_q.
Denote the Galois group of $N|K$ by G. Let H be the Galois group of $K(\zeta)|K$ and let $\sigma : \zeta \mapsto \zeta^k$ be an element of H. As $\widetilde{P(z)}$ is fixed by σ, we can extend σ to N by setting $\sigma(r_1) = r_1$. Then,

$$\sigma : e_i^q \mapsto \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^\times} b_{\overline{jk}}^{\overline{i/j}} = \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^\times} b_j^{\overline{ik/j}} = e_{\overline{ik}}^q$$

for $i = 1, ..., q-1$ relatively prime to q. Hence, there exists $l_i \in \mathbb{Z}$ such that $\sigma(e_i) = \zeta^{l_i} e_{\overline{ik}}$. We compute

$$\sigma : r_1 = \sum_{j=0}^{q-1} e_j \zeta^j \mapsto \sum_{j=0}^{q-1} e_{\overline{jk}} \zeta^{l_j} \zeta^{jk} = \sum_{i=0}^{q-1} e_i \zeta^i \zeta^{l_{\overline{i/k}}}.$$

As $\sigma(r_1) = r_1$, we deduce $\zeta^{l_{\overline{i/k}}} = 1$, hence $\sigma(e_i) = e_{\overline{ik}}$ for $i = 1, ..., q-1$ relatively prime to q. Thus,

$$\sigma : r_i = \sum_{j=0}^{q-1} e_j \zeta^{ij} \mapsto \sum_{j=0}^{q-1} e_{\overline{kj}} \zeta^{ijk} = \sum_{j=0}^{q-1} e_j \zeta^{ij} = r_i.$$

for $i = 0, ..., q-1$.
Let $L := K(r_0, ..., r_{q-1})$, which is the splitting field of $\widetilde{P(z)}$ over K. The following figure may clarify the different connections between the fields.

$$\begin{tikzcd} & N \arrow[dl, dash, "C_q"] \arrow[dd, dash, "G"] \arrow[dr, dash] & \\ K(\zeta) \arrow[dr, dash, "H"'] & & L \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Let H' be the set of all extensions of elements of H to N as constructed above. Every element of H' leaves L invariant, by definition, so $L \subseteq N^{H'}$. Hence,

$$[N : L] \geq [N : N^{H'}] = |H'| = |H|.$$

Clearly

$$[L : K] \geq [N : K(\zeta)] = |C_q| = q.$$

We deduce with the tower rule that $N^{H'} = L$ and $[L : K] = q$. As $L|K$ is Galois, H' is a normal subgroup of G and hence a direct complement of C_q in G. Therefore, the Galois group of $L|K$, which is the Galois group of $\widetilde{P(z)}$ over K, is equal to C_q. $\square$

From this proposition, it also follows that $\widetilde{P(z)}_0$ has Galois group C_q over $\mathbb{Q}(t)$, as it is an irreducible specialization of $\widetilde{P(z)}$.

Smith proved in [Smi91] the strong statement that $\widetilde{P(z)}$ is generic for C_q over $\mathbb{Q}$. This means that apart from the proposition above, he proved that for all Galois extensions $L|L'$ with Galois group C_q and $\mathbb{Q} \subseteq L'$, there exists a specialization of $\widetilde{P(z)}$ with splitting field L over L'. His proof is very extensive, so we will not give it here. We refer to [Smi91]. For the interested reader, the proof combines theory about Stickelberger elements, Lagrange resolvents and convolution algebras.

Let us consider an example of this construction. In [Smi91] the example for $q = 3$ is written out. We will show the method for $q = 5$. Then $e_0 = 0$ and

$$\begin{aligned}
e_1 &= c_1 c_2^3 c_3^2 c_4^4 \\
e_2 &= c_1^2 c_2 c_3^4 c_4^3 \\
e_3 &= c_1^3 c_2^4 c_3 c_4^2 \\
e_4 &= c_1^4 c_2^2 c_3^3 c_4,
\end{aligned}$$

hence we can compute

$$\begin{aligned}
r_0 &= c_1 c_2^3 c_3^2 c_4^4 + c_1^2 c_2 c_3^4 c_4^3 + c_1^3 c_2^4 c_3 c_4^2 + c_1^4 c_2^2 c_3^3 c_4 \\
r_1 &= c_1 c_2^3 c_3^2 c_4^4 \zeta + c_1^2 c_2 c_3^4 c_4^3 \zeta^2 + c_1^3 c_2^4 c_3 c_4^2 \zeta^3 + c_1^4 c_2^2 c_3^3 c_4 \zeta^4 \\
r_2 &= c_1 c_2^3 c_3^2 c_4^4 \zeta^2 + c_1^2 c_2 c_3^4 c_4^3 \zeta^4 + c_1^3 c_2^4 c_3 c_4^2 \zeta + c_1^4 c_2^2 c_3^3 c_4 \zeta^3 \\
r_3 &= c_1 c_2^3 c_3^2 c_4^4 \zeta^3 + c_1^2 c_2 c_3^4 c_4^3 \zeta + c_1^3 c_2^4 c_3 c_4^2 \zeta^4 + c_1^4 c_2^2 c_3^3 c_4 \zeta^2 \\
r_4 &= c_1 c_2^3 c_3^2 c_4^4 \zeta^4 + c_1^2 c_2 c_3^4 c_4^3 \zeta^3 + c_1^3 c_2^4 c_3 c_4^2 \zeta^2 + c_1^4 c_2^2 c_3^3 c_4 \zeta.
\end{aligned}$$

Expanding the polynomial $P(z)$ gives the following expression

$$\begin{aligned}
P(z) = z^5 &- 10 c_1^5 c_2^5 c_3^5 c_4^5 z^3 - 5 c_1^5 c_2^5 c_3^5 c_4^5 (c_1^5 c_2^5 + c_3^5 c_4^5 + c_1^5 c_3^5 + c_2^5 c_4^5) z^2 \\
&+ (5(c_1^5 c_2^5 c_3^5 c_4^5)^2 - 5 c_1^5 c_2^5 c_3^5 c_4^5 (c_1^{10} c_2^5 c_3^5 + c_1^5 c_2^{10} c_4^5 + c_1^5 c_3^{10} c_4^5 + c_2^5 c_3^5 c_4^{10})) z \\
&- c_1^5 c_2^5 c_3^5 c_4^5 (c_1^{15} c_2^5 c_3^{10} + c_1^{10} c_2^{15} c_4^5 + c_1^5 c_3^{15} c_4^{10} + c_2^{10} c_3^5 c_4^{15}).
\end{aligned}$$

The expression was obtained using Mathematica, see the appendix for details. Expressed in b_i's, this is equal to

$$\begin{aligned}
P(z) = z^5 &- 10 b_1 b_2 b_3 b_4 z^3 - 5 b_1 b_2 b_3 b_4 (b_1 b_2 + b_3 b_4 + b_1 b_3 + b_2 b_4) z^2 \\
&+ (5(b_1 b_2 b_3 b_4)^2 - 5 b_1 b_2 b_3 b_4 (b_1^2 b_2 b_3 + b_1 b_2^2 b_4 + b_1 b_3^2 b_4 + b_2 b_3 b_4^2)) z \\
&- b_1 b_2 b_3 b_4 (b_1^3 b_2 b_3^2 + b_1^2 b_2^3 b_4 + b_1 b_3^3 b_4^2 + b_2^2 b_3 b_4^3).
\end{aligned}$$

Now, let $\mu_i = \zeta^{i+1}$ for $\mu_0, ..., \mu_3$ be our choice of a basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$ which means that

$$\begin{aligned}
\widetilde{b_1} &= t_0\zeta + t_1\zeta^2 + t_2\zeta^3 + t_3\zeta^4 \\
\widetilde{b_2} &= t_0\zeta^2 + t_1\zeta^4 + t_2\zeta + t_3\zeta^3 \\
\widetilde{b_3} &= t_0\zeta^3 + t_1\zeta + t_2\zeta^4 + t_3\zeta^2 \\
\widetilde{b_4} &= t_0\zeta^4 + t_1\zeta^3 + t_2\zeta^2 + t_3\zeta.
\end{aligned}$$

We obtain $\widetilde{P(z)}$ by replacing b_i by $\widetilde{b_i}$ in $P(z)$ for $i = 1, ..., q-1$. With the use of Mathematica, we can compute $\widetilde{P(z)}$, but it gets very large, so we will not display it here.
As one can verify,

$$\gamma_2 : \widetilde{b_1} \mapsto \widetilde{b_2} \mapsto \widetilde{b_4} \mapsto \widetilde{b_3} \mapsto \widetilde{b_1}.$$

So, if we take a look at the coefficients of $P(z)$, we can verify that $\widetilde{P(z)}$ is invariant under γ_2. As γ_2 is the generator of the Galois group of $\mathbb{Q}(\zeta)|\mathbb{Q}$, we deduce that $\widetilde{P(z)}$ must lie in $\mathbb{Z}[t_0, t_1, t_2, t_3][z]$, which is what we claimed.
One might wonder whether Noether's problem is solvable for C_5. In fact it is, according to the results in [JLY02] (with references to [Fur25]). This however does not follow straightforward from the construction above, since the elements $r_0, ..., r_4$ become very complicated once the c_i's are replaced by $\sqrt[5]{\widetilde{b_i}}$'s and the $\widetilde{b_i}$'s are replaced by the expressions above in $\mathbb{Z}[t_0, ..., t_3, \zeta]$.

5.1.2 Construction using the field trace

In this section we give a detailed and extended version of what is written in [Nak00] and refer to [Coh12] in some parts. We will claim and prove the existence of a generic polynomial for a cyclic group of odd prime order over the rational numbers.
Let l be an odd prime and C_l be the cyclic group of order l. As said, in this section we will work towards a generic polynomial for C_l over $\mathbb{Q}$. By Kummer Theory, in particular implied by corollary 10.2.7 of [Coh12], we have that $X^l - T$ is generic for C_l over k if k contains an l-th root of unity. As $\mathbb{Q}$ does not contain a primitive l-th root of unity, it will not be that easy. Furthermore, let ζ be a primitive l-th root of unity and $F := \mathbb{Q}(\zeta)$. Now let $V := F^\times/(F^\times)^l$ be regarded as vector space over $\mathbb{F}_l$. Explicitly, this means that V has multiplication as operation and that it consists of all elements $\overline{\alpha}$, with $\alpha \in F^\times$, where $\overline{\alpha} = \overline{\beta} \in V$ if and only if $\alpha = \beta \cdot \lambda^l$ for some $\lambda \in F^\times$. $\mathbb{F}_l$ acts on V explicitly by

$$\mathbb{F}_l \times V \to V : (\overline{a}, \overline{\alpha}) \mapsto \overline{\alpha^a}$$

which can easily be checked to be well-defined. From basic Galois theory we know that the Galois group G of $F|\mathbb{Q}$ is isomorphic to $\mathbb{F}_l^\times$ as we have an injective groupisomorphism

$$\chi : G \to \mathbb{F}_l^\times : (\sigma : \zeta \mapsto \zeta^m) \mapsto \overline{m}.$$

Also note that the size of G is $l-1$. G acts on V in the following canonical way

$$G \times V \to V : (\sigma, \overline{\alpha}) \mapsto \overline{\sigma(\alpha)}$$

for which it is again not hard to see that it is well-defined. Combining these actions of $\mathbb{F}_l$ and G on V gives V a $\mathbb{F}_l[G]$-module structure. Let now

$$\varepsilon = \overline{l-1}^{-1} \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma \in \mathbb{F}_l[G].$$

The following computation shows that ε is idempotent.

$$\begin{aligned}
\varepsilon^2 &= \overline{l-1}^{-2} \sum_{\sigma,\tau\in G} \chi((\sigma\tau)^{-1})\sigma\tau, \text{ by definition} \\
&= \overline{l-1}^{-2} \sum_{\sigma,\tau\in G} \chi(\sigma^{-1})\sigma, \text{ if we transform } \sigma \mapsto \sigma\tau^{-1} \\
&= \varepsilon, \text{ as the summation over } \tau \text{ gives a factor } \overline{l-1}.
\end{aligned}$$

As ε is an element of $\mathbb{F}_l[G]$, it acts on V. Denote the image of ε by V^ε. For elements of V^ε the following interesting property holds.

Proposition 12. Let $\overline{\alpha} \in V$. Then, $\overline{\alpha} \in V^\varepsilon$ if and only if $\sigma(\overline{\alpha}) = \overline{\alpha}^{\chi(\sigma)}$ for all $\sigma \in G$.

Proof. If we assume that $\overline{\alpha} \in V^\varepsilon$, then this means that

$$\overline{\alpha} = \varepsilon(\overline{\beta}) = \left(\prod_{\tau\in G} \overline{\tau(\beta)^{\chi(\tau^{-1})}} \right)^{\overline{l-1}^{-1}}$$

for some $\overline{\beta} \in V$. Then, for any $\sigma \in G$:

$$\sigma(\overline{\alpha}) = \left(\prod_{\tau\in G} \overline{\sigma\tau(\beta)^{\chi(\tau^{-1})}} \right)^{\overline{l-1}^{-1}} = \left(\prod_{\sigma\tau\in G} \overline{\sigma\tau(\beta)^{\chi(\sigma(\sigma\tau)^{-1})}} \right)^{\overline{l-1}^{-1}} = \left(\prod_{\tau\in G} \overline{\tau(\beta)^{\chi(\sigma\tau^{-1})}} \right)^{\overline{l-1}^{-1}} = \overline{\alpha}^{\chi(\sigma)}.$$

Conversely, if $\sigma(\overline{\alpha}) = \overline{\alpha}^{\chi(\sigma)}$ for all $\sigma \in G$, then $\overline{\alpha} = \overline{\sigma(\alpha)}^{\chi(\sigma^{-1})}$ for all $\sigma \in G$. As $\#G = l-1$, we now have that

$$\overline{\alpha} = \left(\prod_{\sigma\in G} \overline{\sigma(\alpha)^{\chi(\sigma^{-1})}} \right)^{\overline{d}^{-1}} = \varepsilon(\overline{\alpha}),$$

i.e. $\overline{\alpha} \in V^\varepsilon$. □

Now that we know these things it is time to explore an arbitrary cyclic extension, so let $K|\mathbb{Q}$ be a Galois extension with group $C_l = \langle\tau\rangle$. Let σ be the generator of G. This means that we have the following diagram of extensions.

$$\begin{tikzcd}
K \arrow[r, dash] \arrow[d, dash, "\langle\tau\rangle"] & K(\zeta) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash, "\langle\sigma\rangle"'] & F = \mathbb{Q}(\zeta)
\end{tikzcd}$$

Note that as l is an odd prime, K can not contain a proper subextension of $F|\mathbb{Q}$, i.e. $F \cap K = \mathbb{Q}$. Therefore, with elementary Galois theory, for example proposition 5.54 of [Keu15], we can deduce that $K(\zeta)|\mathbb{Q}$ is a Galois extension with group isomorphic to

$$\mathrm{Gal}(F|\mathbb{Q}) \times \mathrm{Gal}(K|\mathbb{Q}) = \langle (1,\tau), (\sigma,1) \rangle \cong \langle \tau, \sigma \rangle,$$

where we extended on the right hand side τ to $\mathbb{Q}(\zeta)$ by saying that τ leaves F invariant and σ to K by saying that σ leaves K invariant. Note that we immediately see that σ and τ commute from these observations.

Furthermore, we have that $K(\zeta)|K$ and $K(\zeta)|F$ are Galois with group isomorphic to respectively $\langle\sigma\rangle$ and $\langle\tau\rangle$. By Kummer theory, again corollary 10.2.7 of [Coh12], we have that $K(\zeta) = F(\sqrt[l]{\alpha})$ for some α in $F^\times$.

For such an α: as $(\sigma(\sqrt[l]{\alpha}))^l = \sigma(\alpha)$, we have $\sigma(\sqrt[l]{\alpha}) = \zeta^n \sqrt[l]{\sigma(\alpha)}$ for some integer n between 0 and $l-1$. If $n \neq 0$, then if we assume that $\sigma : \zeta \mapsto \zeta^m$, as $\sigma^l(\sqrt[l]{\alpha}) = \sqrt[l]{\alpha}$: $n^l m^{l-1} \equiv 0(\text{mod } l)$. This however, as l is a prime number, can not be the case, since we assumed that m and n are not multiples of l. Thus, $n = 0$ and $\sigma : \sqrt[l]{\alpha} \mapsto \sqrt[l]{\sigma(\alpha)}$.

The following proposition describes more properties of this α we work with. This proposition actually implies that there is a bijection between cyclic extensions over $\mathbb{Q}$ of degree l and one-dimensional subspaces of V^ε.

Proposition 13. If K is a Galois extension with group C_l and $\alpha \in F^\times$ is an element such that $K(\zeta) = F(\sqrt[l]{\alpha})$, then $\overline{\alpha} \in V^\varepsilon$. Conversely, if $\alpha \in F^\times$ such that $\overline{\alpha} \in V^\varepsilon\backslash\{1\}$, then $F(\sqrt[l]{\alpha})|\mathbb{Q}$ is an abelian extension of degree $l(l-1)$ containing a unique cyclic extension $K|\mathbb{Q}$ of degree l.

Proof. For the first part of this proposition, we will first prove that $\sigma(\alpha) = \lambda^l\alpha^e$ for some $e \in \mathbb{Z}$ and $\lambda \in F$, where $l \nmid e$ if all assumptions of the proposition are satisfied. We already know that $F(\sqrt[l]{\alpha}) = F(\sqrt[l]{\sigma(\alpha)})$, so $\sqrt[l]{\sigma(\alpha)} = \sum_{i=0}^{l-1} \lambda_i \sqrt[l]{\alpha}^i$ for some $\lambda_i \in F$. Assume now that $\tau(\sqrt[l]{\alpha}) = \zeta^a\sqrt[l]{\alpha}$ and $\tau(\sqrt[l]{\sigma(\alpha)}) = \zeta^b\sqrt[l]{\sigma(\alpha)}$. Then $\zeta^b\sqrt[l]{\sigma(\alpha)}$ can be expressed as $\sum_{i=0}^{l-1}\lambda_i\zeta^{ai}\sqrt[l]{\alpha}^i$ and $\sum_{i=0}^{l-1}\lambda_i\zeta^{b}\sqrt[l]{\alpha}^i$ using the above expressions. If we subtract these expressions from each other then we end up with the expression $\sum_{i=0}^{l-1}\lambda_i(\zeta^{ai}-\zeta^b)\sqrt[l]{\alpha}^i = 0$, which implies that $\lambda_i(\zeta^{ai}-\zeta^b) = 0$ for $i = 0, ..., l-1$. Choose now i such that $\zeta^{ai}-\zeta^b = 0$. Then for all $j \neq i$, we have that $\lambda_j = 0$, so $\sigma(\alpha) = \lambda^l\alpha^e$.

Now assume that $\sigma : \zeta \mapsto \zeta^m$, i.e. $\chi(\sigma) = \overline{m}$. Then we compute that

$$\sigma \circ \tau : \sqrt[l]{\alpha} \mapsto \lambda\sqrt[l]{\alpha^e} \mapsto \lambda\zeta^{ae}\sqrt[l]{\alpha^e}$$
$$\tau \circ \sigma : \sqrt[l]{\alpha} \mapsto \zeta^a\sqrt[l]{\alpha} \mapsto \lambda\zeta^{am}\sqrt[l]{\alpha^e}$$

and because σ and τ commute, we have now that $e = m$. We can now conclude that

$$\sigma(\overline{\alpha}) = \overline{\lambda^l\alpha^m} = \overline{\alpha^m} = \overline{\alpha}^{\chi(\sigma)},$$

so $\overline{\alpha} \in V^\varepsilon$.

For the second part of the proposition, note that again directly from corollary 10.2.7 of [Coh12], we have that $F(\sqrt[l]{\alpha})|F$ is cyclic of degree l (because $\overline{\alpha} \neq 1$ and l is prime). As earlier said, $F(\sqrt[l]{\alpha})|\mathbb{Q}$ has Galois group isomorphic to $\langle\sigma,\tau\rangle$, which is abelian and of degree $l(l-1)$. By the fundamental theorem of Galois theory, there is a unique subextension $K|\mathbb{Q}$ of $F(\sqrt[l]{\alpha})|\mathbb{Q}$ of degree l which is cyclic, namely the subextension corresponding to the subgroup $\langle\sigma\rangle$ of $\langle\sigma,\tau\rangle$. □

In the following proposition the arbitrary cyclic extension $K|\mathbb{Q}$ will be investigated even more.

Proposition 14. If $K|\mathbb{Q}$ is a Galois extension with group C_l and $\alpha \in F^\times$ is such that $K(\zeta) = F(\sqrt[l]{\alpha})$, then $K = \mathbb{Q}(Tr_{L/K}(A))$ for $L = K(\zeta)$ and $A = \sqrt[l]{\alpha}$. The conjugates of $Tr_{L/K}(A)$ are precisely $Tr_{L/K}(\zeta^i A)$ for $i = 0, ..., l-1$.

Proof. As noted above, we have

$$\mathrm{Gal}(L|K) = \mathrm{Gal}(K(\zeta)|K) \cong \langle\sigma\rangle = G.$$

Now identify an integer $x_\sigma \in \{1, ..., l-1\}$ with $\chi(\sigma) = x_\sigma (\mathrm{mod}\, l)$ for each $\sigma \in G$, i.e. $\sigma : \zeta \mapsto \zeta^{x_\sigma}$. As $\overline{\alpha} \in V^\varepsilon$ by the previous proposition, we have that $(A^{\sigma - x_\sigma})^l = \alpha^{\sigma - x_\sigma} \in (F^\times)^l$ for any $\sigma \in G$. Thus there exists a $\gamma_\sigma \in F^\times$ such that $\sigma(A) = \gamma_\sigma A^{x_\sigma}$ for $\sigma \in G$. Therefore, $Tr_{L|K}(A) = \sum_{\sigma\in G} \gamma_\sigma A^{x_\sigma} \notin \mathbb{Q}$, because $\{x_\sigma\}_{i=0,...,l-1} \subseteq \{1, ..., l-1\}$ and $1, A, A^2, ..., A^{l-1}$ are linearly independent over F. Because $K|\mathbb{Q}$ is of prime degree l, we must have now that $K = \mathbb{Q}(Tr_{L|K}(A))$. The conjugates of $Tr_{L|K}(A)$ are clearly $Tr_{L|K}(\zeta^i A)$ for $i = 0, ..., l-1$, as these are the images of $Tr_{L|K}(A)$ under τ, which is also described above. As $\#\langle\tau\rangle = l$, those $Tr_{L|K}(\zeta^i A)$ are distinct for $i = 0, ..., l-1$ and are precisely the conjugates of $Tr_{L|K}(A)$. $\square$

This means that our arbitrary Galois extension $K|\mathbb{Q}$ with group C_l is the splitting field of the polynomial

$$f(X; \alpha) = \prod_{i=0}^{l-1}(X - Tr_{L|K}(A\zeta^i)).$$

To come up with a generic polynomial for C_l over $\mathbb{Q}$, we need to do a few steps. First we transform $f(X; \alpha)$ to a more general form using a substitution for α. Let

$$\mathcal{E} = \{e \in \mathbb{Z}[G] | s\varepsilon = e \bmod l \text{ for some } s \in \mathbb{F}_l^\times\}.$$

Then for any $e \in \mathcal{E}$ and any $\beta \in F^\times$, we can define $f(X; \beta^e)$. As $\overline{\beta^e} = \varepsilon(\overline{\beta^s}) \in V^\varepsilon$, we know from proposition 14 that $F(\sqrt[l]{\beta^e})|\mathbb{Q}$ is cyclic of degree $l(l-1)$ if $\beta^e \notin (F^\times)^l$, containing a unique subfield K of $F(\sqrt[l]{\beta^e})$ which is cyclic over $\mathbb{Q}$ of degree l, which is the splitting field of $f(X; \beta^e)$. Note that the cyclic extension generated by $f(X, \beta^e)$ is independent of the choice of $e \in \mathcal{E}$, as shown by the following reasoning. If $e', e \in \mathcal{E}$ and $e' \equiv e (\mathrm{mod}\, l)$, then $e' = e + kl$ for some $k \in \mathbb{Z}$. Then,

$$F(\sqrt[l]{\beta^{e'}}) = F(\sqrt[l]{\beta^e}\beta^k) = F(\sqrt[l]{\beta^e}).$$

If $e', e \in \mathcal{E}$ and $e' \not\equiv e (\mathrm{mod}\, l)$, then $e' (\mathrm{mod}\, l) = s'\varepsilon$ and $e (\mathrm{mod}\, l) = s\varepsilon$ for distinct $s, s' \in \mathbb{F}_l^\times$. So $s^{-1}s'e (\mathrm{mod}\, l) = e' (\mathrm{mod}\, l)$. We conclude

$$F(\sqrt[l]{\beta^{e'}}) = F(\sqrt[l]{\beta^e}^{\,s^{-1}s'}) = F(\sqrt[l]{\beta^e}),$$

since l is prime and $s^{-1}s' \in \mathbb{F}_l^\times$.
Now is the time to actually describe the polynomial $g(X; \mathbf{T})$ for which we will later prove that it is generic for C_l over $\mathbb{Q}$. From now on, let $e \in \mathcal{E}$ be fixed and define $(w_\sigma)_{\sigma\in G}$ to be the basis of $F/\mathbb{Q}$ and let $\mathbf{T} = (T_\sigma)_{\sigma\in G}$ be algebraically independent transcendental variables over $\mathbb{Q}$ indexed by G. The Galois group $F(\mathbf{T})|\mathbb{Q}(\mathbf{T})$ is canonically isomorphic to G. So apply the previous explanation to define

$$g(X; \mathbf{T}) = f(X; \beta'(\mathbf{T})^e),$$

where $\beta'(\mathbf{T}) = \sum_{\sigma\in G} w_\sigma T_\sigma \in F(\mathbf{T})$.
Because $(w_\sigma)_{\sigma\in G}$ is a basis for $F/\mathbb{Q}$, we can pick $\mathbf{t} \in \mathbb{Q}^{l-1}$ for any $\beta \in F^\times$ such that $\beta = \beta'(\mathbf{t})$. Then we get again $f(X; \beta^e) = g(X; \mathbf{t}) \in \mathbb{Q}[X]$. This gives the following important property of $g(X; \mathbf{T})$.

Proposition 15. Any Galois extension $K|\mathbb{Q}$ with group C_l can be obtained as the splitting field of $g(X;\mathbf{t})$ over $\mathbb{Q}$ for some $\mathbf{t} \in \mathbb{Q}^{l-1}$.

Before proving that $g(X;\mathbf{T})$ is generic for C_l over $\mathbb{Q}$, we will analyze the roots of $g(X;\mathbf{T})$. We will use a similar method as in proposition 3 and derive similar results. Let $A' = \sqrt[l]{\beta'(\mathbf{T})^e}$ and let $L' = F(\mathbf{T})(A')$. Let K' be the subfield of $L'|\mathbb{Q}(\mathbf{T})$ such that $[L' : K'] = l-1$. Then the Galois group of $L'|K'$ can be identified with G. Again there exists rational functions $\gamma'_\sigma(\mathbf{T}) \in F(\mathbf{T})$ determined by $A'^\sigma = \gamma'_\sigma(\mathbf{T})A'^{x_\sigma}$ for $\sigma \in G$. So the roots of $g(X;\mathbf{T})$ are of the form

$$Tr_{L'|K'}(A'\zeta^j) = \sum_{\sigma\in G} \gamma'_\sigma(\mathbf{T})A'^{x_\sigma}\zeta^{jx_\sigma}$$

for $j = 0, ..., l-1$. For simplicity denote

$$B_\sigma(\mathbf{T}) = \beta'(\mathbf{T})^\sigma = \sum_{\tau\in G} w^\sigma_\tau T_\tau,$$

which gives if we write $e = \sum_{\sigma\in G} e_\sigma\sigma$ (with $e_\sigma \in \mathbb{Z}$):

$$A'^l = \beta'(\mathbf{T})^e = \prod_{\sigma\in G} B_\sigma(\mathbf{T})^{e_\sigma}.$$

In [Coh12] a proof of the following statement can be found. Because the proof is very extensive and technical, we will skip it.

Proposition 16. Any coefficient of $g(X;\mathbf{T})$ is given in the form of a finite sum $\sum q_i\beta'(\mathbf{T})^{u_i}$, where q_i are elements of $\mathbb{Q}$ and $u_i \in \mathbb{Z}[G]$.

In order to prove that $g(X;\mathbf{T})$ is generic for C_l over $\mathbb{Q}$, we have to prove two things. First that the Galois group of $g(X;\mathbf{T})$ over $\mathbb{Q}(\mathbf{T})$ is C_l and that for any field k_1 containing $\mathbb{Q}$ as a subfield: any Galois extension $K_1|k_1$ with group C_l is the splitting field of $g(X;\mathbf{t})$ for some $\mathbf{t} \in k_1^{l-1}$. So consider such a k_1 and K_1. We first note that the coefficients of $g(X;\mathbf{T})$ can be defined at $\mathbf{t} \in k_1^{l-1}$. This follows from the above proposition, because the prime field of k_1 is the same as that of $\mathbb{Q}$. Also the function $\gamma'_\sigma(\mathbf{T})$ (for each $\sigma \in G$) can be defined at $\mathbf{t} \in k_1^{l-1}$. This is because of the following. Since $e(\sigma - x_\sigma)(\alpha) = (\alpha^\varepsilon)^{s(\sigma-x_\sigma)} \equiv 1 \in V$, we have that $e(\sigma - x_\sigma) = 0(\text{mod } l)$. Therefore, because $\gamma'_\sigma(\mathbf{T})^l = A'^{l(\sigma-x_\sigma)} = \beta'(\mathbf{T})^{e(\sigma-x_\sigma)}$, there exists $j_\sigma \in \mathbb{F}_l^\times$ and $v_\sigma \in \mathbb{Z}[G]$ such that $\gamma'_\sigma(\mathbf{T}) = \zeta^{j_\sigma}\beta'(\mathbf{T})^{v_\sigma}$. So it is clear that we can define this function if $\mathbf{t} \in k_1^{l-1}$. Also note that $\gamma'_\sigma(\mathbf{T}) \neq 0$. The last thing we want to mention is that it follows directly from the description above that if A_1 is an element in the algebraic closure of k_1 such that $A_1^l = \prod_{\sigma\in G} B_\sigma(\mathbf{t})^{e_\sigma}$, then the roots of $g(X;\mathbf{T})$ are given by

$$\sum_{\sigma\in G} \gamma'_\sigma(\mathbf{T})A'^{x_\sigma}\zeta^{jx_\sigma}, 0 \le j \le l-1.$$

Theorem 2. $g(X;\mathbf{T})$ is generic for C_l over $\mathbb{Q}$.

Proof. Let W be the matrix $(w^\sigma_\tau)_{\sigma,\tau\in G}$, where the rows are indexed by σ and the columns by τ. As $F|\mathbb{Q}$ is separable , W is invertible. Thus, the $l-1$ linear forms $B_\sigma(\mathbf{T})$ ($\sigma \in G$) are distinct from each other. This means that $\beta'(\mathbf{T})^e = \prod B_\sigma(\mathbf{T}) \notin F^\times(\mathbf{T})^l$ as $e(\text{mod } l) \neq 0(\text{mod } l)$. This implies, by a generalization of proposition 14 and the description of the roots of $g(X;\mathbf{T})$ above that the

Galois group of $g(X;\mathbf{T})$ over $\mathbb{Q}(\mathbf{T})$ is isomorphic to C_l.
For the second property of a generic polynomial we have to find some $\mathbf{t} \in k_1^{l-1}$ such that K_1 is the splitting field of $g(X;\mathbf{t})$ over $\mathbb{Q}(\mathbf{t})$. Let $F_1 = k_1(\zeta)$ and $L_1 = K_1(\zeta)$. Now, the Galois group H of $F_1|k_1$ can be regarded as a subgroup of G. Define $e(H) = \sum_{\sigma\in H} e_\sigma \sigma$. Since L_1 is abelian over k_1, there is an $\beta_1 \in F_1^\times$ such that $L_1 = F_1(\sqrt[l]{\beta_1^{e(H)}})$, by proposition 14. For $\sigma \in G$, set $b_\sigma = \beta_1^\sigma$ if $\sigma \in H$ and $b_\sigma = 1$ if $\sigma \notin H$. Let $b = (b_\sigma)_{\sigma\in G}$ and let $\mathbf{t} = W^{-1}\mathbf{b}$. We will show in what follows that $\mathbf{t} \in k_1^{l-1}$. To see this, first write $\mathbf{t} = (W^T W)^{-1}(W^T\mathbf{b})$. One can check easily that the entries of $W^T W$ are invariant under G, so belong to $\mathbb{Q}$. Moreover, the entries of $W^T\mathbf{b}$ belong to k_1, because

$$\begin{aligned}\sum_{\tau\in G} w_\sigma^\tau b_\tau &= \sum_{\tau\in H} w_\sigma^\tau \beta_1^\tau + \sum_{\tau\notin H} w_\sigma^\tau \\ &= \sum_{\tau\in H} w_\sigma^\tau(\beta_1^\tau - 1) + \sum_{\tau\in G} w_\sigma^\tau \\ &= Tr_{F_1/k_1}(w_\sigma(\beta_1 - 1)) + Tr_{F/\mathbb{Q}}(w_\sigma).\end{aligned}$$

The relation $W\mathbf{t}=\mathbf{b}$ shows directly that $B_\sigma(\mathbf{t}) = b_\sigma$ for $\sigma \in G$. Moreover,

$$\beta_1^{e(H)} = \prod_{\sigma\in G} b_\sigma^{e_\sigma} = \prod_{\sigma\in G} B_\sigma(\mathbf{t})^{e_\sigma}.$$

Therefore, by our discussion above the theorem, $\gamma'_\sigma(\mathbf{t}) \neq 0$ and all the roots of $g(X;\mathbf{t})$ are given by

$$\theta_j = \sum_{\sigma\in G} \gamma'_\sigma(\mathbf{t}) A_1^{x_\sigma} \zeta^{jx_\sigma},\ 0 \le j \le l-1.$$

where $A_1 = \sqrt[l]{\beta_1^{e(H)}}$. Since $\gamma'_\sigma(\mathbf{t}) \neq 0$ and $1, A_1, A_1^2, ..., A_1^{l-1}$ are linearly independent over F_1, we obtain $L_1 = F_1(\theta_j)$, which yields

$$l = [L_1 : F_1] = [F_1(\theta_j) : F_1] \le [k_1(\theta_j) : k_1] \le \deg(g(X;\mathbf{t})) = l.$$

We conclude that $[k_1(\theta_j) : k_1] = l$, hence $K_1 = k_1(\theta_j)$ for any j and the proof is complete. $\square$

Now that we proved the above statement, it is interesting to see what such a $g(X;\mathbf{T})$ looks like, so we will consider a few examples.

Example 1. Let $l = 3$. A basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$ is given by $\{\zeta, \zeta^2\}$, so let $w_1 = \zeta$ and $w_2 = \zeta^2$. Then $\beta'(\mathbf{T}) = \zeta T_1 + \zeta^2 T_2$. Now, $G =$Gal$(\mathbb{Q}(\zeta)|\mathbb{Q}) = \{id, \sigma\}$, where id is the identity map and $\sigma : \zeta \mapsto \zeta^2$, so

$$\varepsilon = \overline{2}^{-1}(\overline{1}\cdot id + \overline{2}\cdot\sigma) = \overline{2}\cdot id + \overline{1}\cdot\sigma.$$

Therefore

$$\mathcal{E} = \{e \in \mathbb{Z}[G] | e(\text{mod } 3) \in \{\overline{2}\cdot id + \overline{1}\cdot\sigma, \overline{1}\cdot id + \overline{2}\cdot\sigma\}\}$$

Pick now $e = id + 2\cdot\sigma \in \mathcal{E}$. Then

$$A' = \sqrt[3]{\beta(\mathbf{T})^e} = \sqrt[3]{(\zeta T_1 + \zeta^2 T_2)(\zeta^2 T_1 + \zeta T_2)^2},$$

which means that the roots of $g(X;\mathbf{T})$ are of the form

$$\zeta^j A' + \zeta^{2j}\sigma(A') \text{ for } j = 0, 1, 2.$$

With the use of Mathematica, see the Appendix below, we could obtain the following expression for $g(X, \mathbf{T})$:

$$g(X; \mathbf{T}) = X^3 - A'\sigma(A')X - A'^3 - \sigma(A')^3.$$

With the definition of A', we can determine

$$\begin{aligned} A'\sigma(A') &= \sqrt[3]{(\zeta T_1 + \zeta^2 T_2)(\zeta^2 T_1 + \zeta T_2)^2} \cdot \sqrt[3]{(\zeta^2 T_1 + \zeta T_2)(\zeta T_1 + \zeta^2 T_2)^2} \\ &= (\zeta T_1 + \zeta^2 T_2)(\zeta^2 T_1 + \zeta T_2) \\ &= T_1^2 - T_1 T_2 + T_2^2. \end{aligned}$$

Furthermore, an easy computation shows that

$$\begin{aligned} -A'^3 - \sigma(A')^3 &= -(\zeta T_1 + \zeta^2 T_2)(\zeta^2 T_1 + \zeta T_2)^2 - (\zeta^2 T_1 + \zeta T_2)(\zeta T_1 + \zeta^2 T_2)^2 \\ &= T_1^3 + T_2^3. \end{aligned}$$

Hence, we see that $g(X; \mathbf{T}) \in \mathbb{Q}(\mathbf{T})[X]$. So a generic polynomial for C_3 over $\mathbb{Q}$ is given by

$$g(X; \mathbf{T}) = X^3 - (T_1^2 - T_1 T_2 + T_2^2)X + T_1^3 + T_2^3.$$

This is the same polynomial as the resulting polynomial of the procedure of section 5.1.1. (for $q = 3$). We will see in the following section that this is not a coincidence.

5.1.3 Connection between the two constructions

In the above sections we described two constructions of a generic polynomial of a cyclic group. Both constructions have different assumptions, but we will show in this section that the two produce the same polynomial in the part where the assumptions overlap. This means that we will look at the situation where q is an odd prime and we will show that the polynomial $P(z)$ (as constructed in 5.1.1.) equals $g(X; \mathbf{T})$ (with $l = q$), as constructed in 5.1.2. For that, we will rewrite the construction of $P(z)$ in the terminology of section 5.1.2.
We see in the last step of the construction in 5.1.1. that we replace b_i by $\widetilde{b_i}$. We see directly that $\widetilde{b_i} = \beta'(\mathbf{T})^{\sigma_i}$, where $\sigma_i : \zeta \mapsto \zeta^i$. This also means that b_1 is replaced by $\beta'(\mathbf{T})$ and b_i by $\sigma_i(\widetilde{b_1})$. Furthermore, this is the same as replacing c_1 by $\sqrt[l]{\beta'(\mathbf{T})}$ and c_i by $\sigma_i(\sqrt[l]{\beta'(\mathbf{T})})$. Using the terminology of 5.1.2., this gives that e_1 turns into

$$e_1' = \prod_{\sigma \in G} \sigma(\sqrt[l]{\beta'(\mathbf{T})})^{\chi(\sigma)^{-1}} = \sqrt[l]{\beta'(\mathbf{T})}^e,$$

where we choose $e \in \mathcal{E}$ to be such that $e = \sum_{\sigma \in G} e_\sigma \sigma$, with $e_\sigma \in \mathbb{Z}$ such that $e_\sigma \in [1, l-1]$ and $\chi(\sigma^{-1}) = e_\sigma (\text{mod } l)$. This means that e_i turns into $(\sqrt[l]{\beta'(\mathbf{T})}^e)^{\chi(\sigma_i^{-1})}$, which equals $(\sqrt[l]{\beta'(\mathbf{T})}^e)^{\sigma_i^{-1}}$, by proposition 2. Therefore, r_0 turns into $Tr_{L/K}(\sqrt[l]{\beta'(\mathbf{T})}^e)$ and r_i into $Tr_{L/K}(\sqrt[l]{\beta'(\mathbf{T})}^e \zeta^{-i})$. Therefore, $P(z)$ equals the polynomial $f(X; \alpha)$, when A^l is replaced by $\beta'(\mathbf{T})^e$, which is exactly the polynomial $g(X; \mathbf{T})$.

Example 2. To see an example of this procedure, consider $q = 5$. Then, similar to example 1, a basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$ is given by $\{\zeta, ..., \zeta^4\}$, so let $w_i = \zeta^i$ for $i = 1, ..., 4$. Then $\beta'(\mathbf{T}) = \zeta T_1 + ... + \zeta^4 T_4$, which is equal to $\widetilde{b_1}$ as computed in section 5.1.1. Now, $G=$Gal$(\mathbb{Q}(\zeta)|\mathbb{Q}) = \{\sigma_i | i = 1, ..., 4\}$, where $\sigma_i : \zeta \mapsto \zeta^i$, so

$$\varepsilon = \overline{4}^{-1}(\overline{1}\cdot\sigma_1 + \overline{3}\cdot\sigma_2 + \overline{2}\cdot\sigma_3 + \overline{4}\cdot\sigma_4) = \overline{4}\sigma_1 + \overline{2}\cdot\sigma_2 + \overline{3}\cdot\sigma_3 + \overline{1}\cdot\sigma_4.$$

Pick now $e = \sigma_1 + 3\sigma_2 + 2\sigma_3 + 4\sigma_4 \in \mathcal{E}$. Then,

$$A' = \sqrt[5]{\beta(\mathbf{T})^e} = \sqrt[5]{\widetilde{b_1}\widetilde{b_2}^3\widetilde{b_3}^2\widetilde{b_4}^4},$$

which we see now is equal to e_1 (of section 5.1.1.) after replacing c_i by $\sqrt[5]{\widetilde{b_i}}$. This means that

$$\begin{aligned}\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\sqrt[5]{\beta'(\mathbf{T})}^e) &= \sigma_1(A') + ... + \sigma_4(A')\\ &= \sqrt[5]{\widetilde{b_1}\widetilde{b_2}^3\widetilde{b_3}^2\widetilde{b_4}^4} + \sqrt[5]{\widetilde{b_2}\widetilde{b_4}^3\widetilde{b_1}^2\widetilde{b_3}^4} + \sqrt[5]{\widetilde{b_3}\widetilde{b_1}^3\widetilde{b_4}^2\widetilde{b_2}^4} + \sqrt[5]{\widetilde{b_4}\widetilde{b_3}^3\widetilde{b_2}^2\widetilde{b_1}^4},\end{aligned}$$

which is equal to the computed r_0 (in 5.1.1.) after replacing c_i by $\sqrt[5]{\widetilde{b_i}}$. This means that the polynomial $\widetilde{P(z)}$, for which the zeros are the expressions obtained after replacing c_i by $\sqrt[5]{b_i}$ in r_i for $i = 0, ..., 4$, is the same as the polynomial $g(X; \mathbf{T})$ with roots $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\sqrt[5]{\beta'(\mathbf{T})}^e\zeta^i)$ as claimed.

5.2 Cyclic groups of even order

In this section we will write about the existence of generic polynomials for C_{2^n} with $n \geq 1$. Above we described a generic polynomial for $C_2 = S_2$ and C_4, so we will now look at the situation where $n = 3$. In the end we will prove the non-existence of a generic polynomial over $\mathbb{Q}$ for the group C_8, which is the one of the few groups for which this fact is known and proven. Actually, because our proof can be used for C_{2^n} if $n \geq 3$, we can claim the non-existence of a generic polynomial over $\mathbb{Q}$ for the cyclic groups of order 2^n for $n \geq 3$. This means moreover that there does not exist a generic polynomial over $\mathbb{Q}$ for the cyclic groups with order divisible by 8.
Before we arrive at this point, we need to introduce a few concepts and denote some important propositions. We begin by introducing the p-adic numbers. We follow the notation as in [Kob77].

Definition 6. Let p be a prime number. For any nonzero $a \in \mathbb{Z}$, let the p-adic ordinal, denoted by $ord_p(a)$, be the highest power of p which divides a, i.e. the greatest m such that $a \equiv 0(\text{mod } p^m)$. For $x = a/b \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$, define $ord_p(x) = ord_p(a) - ord_p(b)$. Define the map $|.|_p$ on $\mathbb{Q}$ as follows

$$|x|_p = \begin{cases} p^{-ord_p(x)} & \text{, if } x \neq 0 \\ 0 & \text{, if } x = 0. \end{cases}$$

It can be proven from the definition that $|.|_p$ is a norm on $\mathbb{Q}$. Define now $\mathbb{Q}_p$, the p-adic numbers, as the completion of $\mathbb{Q}$ with respect to $|.|_p$.

We expect the reader to be familiar with algebraic number theoretical concepts such as ramification. For a detailed description of this concept in the case of p-adic numbers, we refer to [Kob77]. A more algebraic way of defining this can be found in [Ste17]. The following propositions can be found in [Kob77] and are denoted here, because they will be used later on.

Proposition 17. There is exactly one unramified extension L_f^{unram} of some degree f of $\mathbb{Q}_p$. It can be obtained by adjoining a primitive (p^f-1)th root of 1.

Proposition 18 (Krasner's lemma)**.** Let $a, b \in \overline{\mathbb{Q}_p}$, and assume that b is chosen closer to a than all conjugates a_i of a ($a_i \neq a$), i.e.

$$|b - a|_p < |a_i - a|_p,$$

then $\mathbb{Q}_p(a) \subseteq \mathbb{Q}_p(b)$.

The following corollary of Krasner's lemma can be found in some more generality in [Sut17] and will turn out to be useful in the upcoming proof.

Corollary 1. Let $f \in \mathbb{Q}_p[x]$ be a monic irreducible separable polynomial. There exists $\delta \in \mathbb{R}_{>0}$, depending on f, such that for every monic polynomial $g \in \mathbb{Q}_p[x]$ with $|f - g|_p < \delta$ the following holds: For every root β of g there exists a root α of f such that $K(\beta) = K(\alpha)$.
In particular, every such g is separable, irreducible and has the same splitting field as f.

In order to prove the proposition that there does not exist a generic polynomial for C_8 over $\mathbb{Q}$, we will need the following proposition. The statement and a sketch of the proof can be found in [Wan48], [JLY02](p.56) and [Bor+12]. We will give a more explained proof, sometimes referring to basic algebraic number theoretical facts or other steps in the references.

Proposition 19. Let $L|\mathbb{Q}$ be a Galois extension with group C_8 and define $L_2 := L \cdot \mathbb{Q}_2$. If $L_2|\mathbb{Q}_2$ is an unramified extension, then $\mathrm{Gal}(L_2|\mathbb{Q}_2) \neq C_8$.

Proof. We assume that $L_2|\mathbb{Q}_2$ is unramified and $\mathrm{Gal}(L_2|\mathbb{Q}_2) = C_8$ and we will look for a contradiction. Let $\mathbb{Q}(\sqrt{D})|\mathbb{Q}$ be a quadratic subextension of $L|\mathbb{Q}$, with D being a square-free integer. Because L_2 is an unramified extension of $\mathbb{Q}_2$, we know that the prime ideal $2\mathcal{O}_{L_2}$ is unramified, so $2\mathcal{O}_L$ is unramified. Hence $2\mathcal{O}_L = P_1 \cdots P_n$ for $n \leq 8$. We will show now that $2\mathcal{O}_L$ is inert.
From algebraic number theory, for example proposition 2.7.16 of [Hus], we know that, for $i = 1, ..., n$: $[L_{P_i} : \mathbb{Q}_2] = e_{P_i} f_{P_i}$, where L_{P_i} is the completion of L with respect to the norm $|.|_{P_i}$, defined similarly to the p-adic norm. Because $L = \mathbb{Q}(\alpha)$ for some $\alpha \in L$, we have for $i = 1, ..., n$: $L_{P_i} = (\mathbb{Q}(\alpha))_2$, which is equal to $\mathbb{Q}_2(\alpha)$, as can be verified from the definition. So we have $L_{P_i} = \mathbb{Q}_2(\alpha) = L_2$ and we end up with $8 = [L_2 : \mathbb{Q}_2] = f_{P_i}$ for $i = 1, ..., n$. Therefore, as $\sum_{i=1}^n e_{P_i} f_{P_i} = 8$, we deduce that $n = 1$, i.e. $2\mathcal{O}_L$ is inert. We will now prove that this implies that $D \not\equiv 1(\text{mod } 8)$.
Note that the ring of integers of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Z}[\frac{d+\sqrt{d}}{2}]$, where d is the discriminant of $\mathbb{Q}(\sqrt{D})$. The minimal polynomial of $\frac{d+\sqrt{d}}{2}$ is

$$\left(x - \frac{d+\sqrt{d}}{2}\right)\left(x - \frac{d-\sqrt{d}}{2}\right) = x^2 - dx + \frac{d^2 - d}{4}.$$

We know that $d = D$ if $D \equiv 1(\text{mod } 4)$ and $d = 4D$ if $D \equiv 2, 3(\text{mod } 4)$. This means that if we suppose $D \equiv 1(\text{mod } 8)$, then $d = D \equiv 1(\text{mod } 8)$. Then, we also see that $d^2 - d \equiv 1 - 1(\text{mod } 8) = 0(\text{mod} 8)$, so $\frac{d^2-d}{4} \equiv 0(\text{mod } 2)$. Hence,

$$x^2 - dx + \frac{d^2 - d}{4} \equiv x^2 + x(\text{mod } 2) = x(x+1)(\text{mod } 2),$$

so $2\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = (2, \frac{d+\sqrt{d}}{2})(2, \frac{d+\sqrt{d}}{2} + 1)$ is a totally split, which is a contradiction to the earlier derived result that $2\mathcal{O}_L$ is inert. We conclude that $D \not\equiv 1(\text{mod } 8)$.

If the prime factorization of D would contain only primes that are equivalent to 1 modulo 8, then D would be equivalent to 1 modulo 8, which is not the case. So there exists a prime number p which divides D and $p \not\equiv 1 (\text{mod } 8)$. Pick now such a prime p. We will now show that we can also deduce that $p \equiv 1 (\text{mod } 8)$ from our assumptions, which means that we have our desired contradiction. For that we will first show that p is totally ramified in L.
Let $\mathfrak{r}$ be a prime ideal in L above p and $I(\mathfrak{r}/p)$ the group of inertia, i.e.

$$I(\mathfrak{r}/p) = \{\sigma \in \text{Gal}(L|\mathbb{Q}) | \sigma(x) = x(\text{ mod } \mathfrak{r}) \text{ for all } x \in \mathcal{O}_L\}.$$

We have $e_{L|\mathbb{Q}}(p) = |I(\mathfrak{r}/p)|$. Let $\mathfrak{s}$ be the prime ideal $\mathfrak{r} \cap \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ in $\mathbb{Q}(\sqrt{D})$. Then it follows from the definition that $I(\mathfrak{r}/\mathfrak{s}) = H \cap I(\mathfrak{r}/p)$, where $H = \text{Gal}(L|\mathbb{Q}(\sqrt{D})) = C_4$. If $I(\mathfrak{r}/p)$ would be contained in H, then $|I(\mathfrak{r}/p)| = |I(\mathfrak{r}/\mathfrak{s})|$, so $e_{L|\mathbb{Q}}(p) = e_{L|\mathbb{Q}(\sqrt{D})}(p)$ and p would not be ramified in $\mathbb{Q}(\sqrt{D})$. However, p is ramified in $\mathbb{Q}(\sqrt{D})$ as $p|D$. So $I(\mathfrak{r}/p)$ can not be contained in H. Because $\text{Gal}(L|\mathbb{Q}) = C_8$, the only subgroup of $\text{Gal}(L|\mathbb{Q})$ not contained in H is $\text{Gal}(L|\mathbb{Q})$ itself, hence $e_{L|\mathbb{Q}}(p) = |I(\mathfrak{r}/p)| = 8$, i.e. p is totally ramified in L.
Since $I(\mathfrak{r}/p) = C_8$ is a subgroup of $\mathcal{O}^\times_{L/\mathfrak{r}} = \mathbb{F}_p^\times$, which follows from well-known algebraic number theory, it follows that $8|p-1$, hence $p \equiv 1(\text{mod } 8)$. ☐

It is now time to go to our main claim.

Proposition 20. There does not exist a generic polynomial for C_8 over $\mathbb{Q}$.

Proof. We will prove this proposition with contradiction, so assume that there does exist a generic polynomial $f(X, \mathbf{T}) \in \mathbb{Q}(\mathbf{T})[X]$ for C_8 over $\mathbb{Q}$ with $\mathbf{T}$ being a tuple consisting of algebraically independent transcendental indeterminates. Let L_2 be the unique unramified C_8-extension of $\mathbb{Q}_2$, which exists because of proposition 18. Then L_2 is the splitting field of some specialization $f(X, \mathbf{a})$ of $f(X, \mathbf{T})$ over $\mathbb{Q}_2$. We may assume here without loss of generality that $f(X, \mathbf{a})$ and $f(X, \mathbf{T})$ are irreducible. The corollary of Krasner's lemma, as described above, gives us the possibility to slightly change the coefficients of $f(X, \mathbf{a})$ without changing its splitting field. If we consider the definition of the norm $|.|_2$ on $\mathbb{Q}_2$, then we deduce that we can even assume in this case $\mathbf{a}$ to be a tuple of rational numbers. Because $\Omega^{f(X,\mathbf{T})}_{\mathbb{Q}(\mathbf{T})}|\mathbb{Q}(\mathbf{T})$ has Galois group C_8, we know that $\Omega^{f(X,\mathbf{a})}_{\mathbb{Q}}|\mathbb{Q}$ has Galois group at most C_8. Therefore, because $\mathbb{Q}_2\Omega^{f(X,\mathbf{a})}_{\mathbb{Q}} = L_2$, we know $\Omega^{f(X,\mathbf{a})}_{\mathbb{Q}}|\mathbb{Q}$ has Galois group equal to C_8. We conclude that L_2 is the composition of a C_8 extension of $\mathbb{Q}$ and $\mathbb{Q}_2$, which is a contradiction with the proposition above. ☐

Note that the proof above works for C_{2^n} extensions when $n \geq 3$.
In general, one could wonder why the construction of 5.1.1. doesn't work for an even prime number. That is because for $n \geq 3$, $\mathbb{Q}(\zeta)|\mathbb{Q}$ is not cyclic in general anymore. Therefore, the proof in 5.1.1. does not hold and as we saw above, counterexamples can be found.

In [Sch92], an explicit construction is given of a parametric polynomial of C_8 over a field K, whenever K satisfies certain conditions. For the reader that has some knowledge about Brauer groups, it might be interesting to know that the condition is that for all $d \in K$ such that $(-1, d) = 0$ in $Br_2(K)$ and $(2, d) = 0$ in $Br_2(K(i))$, we have $(2, d) = 0$ in $Br_2(K)$. In this condition, $Br_2(K)$ denotes the kernel of multiplication by 2 in the Brauer group of K (written additively) and (a, b) is the class of the quaternion algebra (a, b) for $a, b \in K$. Examples of fields that satisfy this condition are $\mathbb{Q}$ and fields containing $\sqrt{2}$, i or $i\sqrt{2}$. See [Sch92] for more examples. Over $\mathbb{Q}$ an example of a parametric polynomial of C_8, which is not generic, is

$$X^8 - 8(1+t^2)(1+t^4)X^6 + 8t^2(4+t^2)(1+t^4)^2X^4 - 32t^4(1+t^4)^3X^2 + 16t^8(1+t^4)^3.$$

6 Noether's problem and generic polynomials for several groups

In the previous sections we discussed Noether's problem and the existence of generic polynomials for small groups and the cyclic groups of odd order. In this section, we will give an overview of some results concerning other groups. We start with a table, which denotes the groups for which a generic polynomial exists over the field corresponding to these groups in the table. Afterwards, we will give examples of generic polynomials for groups noted in this table. We end this section with some results concerning Noether's problem. Let p be a prime number, q an odd prime power and l a positive integer such that $l|p-1$.

Group	Field	Reference
Dihedral groups D_q	$\mathbb{Q}$	[Sal82]
p-groups	Infinite fields of characteristic p	[Gas59]
Frobenius groups $F_{pl} = C_p \rtimes C_l$, where $8 \nmid l$	$\mathbb{Q}$	[Sal82]

As noted in the previous section, the above result concerning dihedral groups is enough to claim that for every dihedral group of odd order, a generic polynomial over $\mathbb{Q}$ exists.
As an example, we consider $q = 3$. Then the construction from the proof of Saltman gives the generic polynomial:

$$f(s_1, s_2, t_1, t_2, u, x) = x^3 - 9x^2 + \frac{324(s_1t_2 - s_2t_1)^2u}{S^2 - T^2u} \in \mathbb{Q}(s_1, s_2, t_1, t_2, u)[x]$$

for D_3 over $\mathbb{Q}$. Here,

$$S = s_1^2 + s_1s_2 + s_2^2 + u(t_1 + t_1t_2 + t_2^2)$$
$$T = 2s_1t_1 + s_1t_2 + s_2t_1 + 2s_2t_2.$$

One can deduce from this that also $x^3 + x^2 + t \in \mathbb{Q}(t)[x]$ is generic for D_3 over $\mathbb{Q}$.

The following example is that of a generic polynomial for a p-group over $\mathbb{F}_p$. As described in [JLY02], the polynomial

$$\sum_{i=0}^{d} \binom{d}{i} (-1)^{d-i} x^{i(p-1)/d+1} - s \in \mathbb{F}_p(s)[x]$$

is generic for the group $C_p \rtimes C_d$ over $\mathbb{F}_p$, where $d|p-1$. In particular,

$$x^p - 2x^{(p+1)/2} + x - s \in \mathbb{F}_p(s)[x]$$

is generic for D_4 over $\mathbb{F}_p$.
Over fields with characteristic $\neq p$, it is not known yet whether there exists a generic polynomial for all p-groups. However, for some specific p-groups, these generic polynomials are already found, namely for the following ([JLY02]): over a field with characteristic $\neq 2$, there exists a generic

polynomial for the groups

$$QC_8 = \langle i, j, \rho | i^2 = j^2 = \rho^2 = -1, ji = -ij, \rho i = i\rho, \rho j = j\rho \rangle.$$
$$QD_8 = \langle u, v | u^8 = 1, v^2 = u^4, vu = u^3 v \rangle.$$

and over a field with characteristic $\neq p$, there exists a generic polynomial for the group

$$H_{p^3} = \langle u, v, w | u^p = v^p = w^p = 1, vu = uvw, wu = uw, wv = vw \rangle.$$

A construction of a generic polynomial for F_{pl} over $\mathbb{Q}$ should be possible to build, as a contruction is mentioned in the proof. It however turns out to be hopelessly involved. An explicit construction of polynomials with group $F_{p(p-1)/2}$ is given in [JLY02], but these polynomials are unfortunately neither parametric nor generic.

We conclude this section with some remaining results concerning Noether's problem for some groups which are not named yet.

Proposition 21. Noether's problem is solvable for the following groups:

- solvable transitive subgroups of S_p for $p = 3, 5, 7, 11$.
- transitive subgroups of S_5
- transitive subgroups of S_7 which are not equal to $PSL_2(\mathbb{F}_7)$ or A_7
- the groups $\mathbb{Q}D_8$, D_8 and M_{16}, which is the smallest group containing C_8.
- transitive subgroups of S_6 containing $C_3 \times C_3$, without being equal to A_6.
- the alternating group A_5.

A reference for the first three claims is [JLY02]. For the fourth, fifth and sixth claim, we refer to respectively [HHR08], [Zho15], [Mae89].
For the alternating groups A_n with $n \geq 6$, it is not known yet whether Noether's problem is solvable. Moreover, the existence of a generic polynomial for A_n with $n \geq 6$ is not guaranteed. To make clear how hard to handle this group appears to be, it is also not possible to build a parametric polynomial for A_n, with n unknown.

7 Conclusion

We started this thesis with the explanation of the inverse Galois problem, which was the reason to study Noether's problem and the existence of generic polynomials. We proved the following implications

$$\text{Noether's Problem} \implies \text{Generic Polynomial} \implies \text{Galois Extension}$$

for solutions of the different problems. The proof of the first implication, proposition 4, also contained a construction for a generic polynomial.

In the third section generating invariant polynomials were found for the cyclic, dihedral and alternating groups. They were used in the next section, were we solved Noether's problem for several small groups. In the following sections, we looked at the existence of generic polynomials in detail for cyclic groups and in a short way for dihedral groups, p-groups and Frobenius groups. The results of these sections are as follows.

In section 4 we showed that Noether's problem is solvable for all subgroups of S_n $n \leq 4$ and also for Q_8. In section 4.7, we reduced Noether's problem for Q_{16} to a smaller problem, but unfortunately without solving it. A generic polynomial exists over $\mathbb{Q}$ for C_n and D_n if n is odd and does not exists over $\mathbb{Q}$ if $8|n$, as proved in section 5. A generic polynomial over a field with characteristic p exists for all p-groups and over $\mathbb{Q}$ for QC_8, QD_8, D_8 and H_{p^3}. It also exists over $\mathbb{Q}$ for the Frobenius groups F_{pl} if $8 \nmid l$. Furthermore, some other groups are noted for which Noether's problem is solvable, with one of them being A_5.

Even though we managed to obtain several results, Noether's problem remains unsolved for the majority of the groups, which means there is still a lot to discover in this branch of mathematics. We hope the reader is wondered by the beauty of these simple-looking problems and enriched with the results of this thesis.

8 Appendix

The following codes were used throughout this thesis. The code that gave the minimal polynomial of l_4 in section 4.2 is the following.

In[2]:= **SymmetricReduction[(a - (x z + y t)) (a - (x y + z t)) (a - (x t + y z)), {x, y, z, t}, {s1, s2, s3, s4}]**
Out[2]=$\{a^3 - a^2 s2 + as1s3 - s3^2 - 4as4 - s1^2 s4 + 4s2s4, 0\}$

In section 4.3 the following code was used in order to determine $(l_4' - l_4'')^2$ in terms of s_1, s_2, s_3, s_4 and l_4. First observe that we must end with the expression

$$(l_4' - l_4'')^2 = A_0 + A_1 l_4 + A_2 l_4^2,$$

with $A_i \in M$, as the left hand side is of degree 2. Letting S_4 act on this equation gives

$$(l_4'' - l_4)^2 = A_0 + A_1 l_4' + A_2 l_4'^2 \text{ and } ((l_4 - l_4'))^2 = A_0 + A_1 l_4'' + A_2 l_4''^2.$$

Hence,

$$\begin{pmatrix} A_0 \\ A_1 \\ A_2 \end{pmatrix} = \begin{pmatrix} 1 & l_4 & l_4^2 \\ 1 & l_4' & l_4'^2 \\ 1 & l_4'' & l_4''^2 \end{pmatrix}^{-1} \begin{pmatrix} (l_4' - l_4'')^2 \\ (l_4'' - l_4)^2 \\ (l_4 - l_4')^2 \end{pmatrix}.$$

The following Mathematica code gives an expression for A_i:

In[3]:=$\mathbf{m} = \{\{\mathbf{1}, \mathbf{xz} + \mathbf{yt}, (\mathbf{xz} + \mathbf{yt})^{\mathbf{2}}\}, \{\mathbf{1}, \mathbf{xy} + \mathbf{zt}, (\mathbf{xy} + \mathbf{zt})^{\mathbf{2}}\}, \{\mathbf{1}, \mathbf{xt} + \mathbf{yz}, (\mathbf{xt} + \mathbf{yz})^{\mathbf{2}}\}\}$
Out[3]= $\{\{1, ty + xz, (ty + xz)^2\}, \{1, xy + tz, (xy + tz)^2\}, \{1, tx + yz, (tx + yz)^2\}\}$

In[5]:=$\mathbf{n} = \{\{(\mathbf{xy} + \mathbf{zt} - \mathbf{xt} - \mathbf{zy})^{\mathbf{2}}\}, \{(\mathbf{xt} + \mathbf{zy} - \mathbf{xz} - \mathbf{yt})^{\mathbf{2}}\}, \{(\mathbf{xz} + \mathbf{yt} - \mathbf{xy} - \mathbf{zt})^{\mathbf{2}}\}\}$
Out[5]= $\{\{(-tx + xy + tz - yz)^2\}, \{(tx - ty - xz + yz)^2\}, \{(ty - xy - tz + xz)^2\}\}$

In[14]:= **Simplify[Inverse[m].n]**
Out[14]= $\{\{x^2(y - z)^2 + y^2 z^2 - 2xyz(y + z) + t^2(x^2 + (y - z)^2 - 2x(y + z)) - 2t(x^2(y + z) + yz(y + z) + x(y^2 - 3yz + z^2))\}, \{2(yz + x(y + z) + t(x + y + z))\}, \{-3\}\}$

We see $A_2 = -3$. The following code reduces the expressions of A_0 and A_1 in terms of s_1, s_2, s_3, s_4:

In[12]:= $\mathbf{SymmetricReduction}[\mathbf{x^2(y - z)^2 + y^2z^2 - 2xyz(y + z) + t^2(x^2 + (y - z)^2 - 2x(y + z) - 2t(x^2(y + z) + yz(y + z) + x(y^2 - 3yz + z^2)), \{x, y, z, t\}, \{s1, s2, s3, s4\}}]$
Out[12]= $\{s2^2 - 4s1s3 + 16s4, 0\}$

In[13]:= $\mathbf{SymmetricReduction}[\mathbf{2(yz + x(y + z) + t(x + y + z)), \{x, y, z, t\}, \{s1, s2, s3, s4\}}]$
Out[13]= $\{2s2, 0\}$

The following code gives the relation in section 4.4:

In[15]:= $\mathbf{SymmetricReduction}[\mathbf{(x - y + z - t)^2, \{x, y, z, t\}, \{s1, s2, s3, s4\}}]$
Out[15]= $\{s1^2 - 4s2, 4ty + 4xz\}$

The code for the polynomial $P(z)$ in section 5.1.1. is the following:

In[4]:=$\mathbf{ExpToTrig[Simplify[Expand[(z - (c1c2^3c3^2c4^4 + c1^2c2c3^4c4^3 + c1^3c2^4c3c4^2 + c1^4c2^2c3^3c4))(z - (c1c2^3c3^2c4^4Exp[2IPi/5] + c1^2c2c3^4c4^3Exp[2IPi/5]^2 + c1^3c2^4c3c4^2Exp[2IPi/5]^3 + c1^4c2^2c3^3c4Exp[2IPi/5]^4))(z - (c1c2^3c3^2c4^4Exp[2IPi/5]^2 + c1^2c2c3^4c4^3Exp[2IPi/5]^4 + c1^3c2^4c3c4^2Exp[2IPi/5] + c1^4c2^2c3^3c4Exp[2IPi/5]^3))(z - (c1c2^3c3^2c4^4Exp[2IPi/5]^3 + c1^2c2c3^4c4^3Exp[2IPi/5] + c1^3c2^4c3c4^2Exp[2IPi/5]^4 + c1^4c2^2c3^3c4Exp[2IPi/5]^2))(z - (c1c2^3c3^2c4^4Exp[2IPi/5]^4 + c1^2c2c3^4c4^3Exp[2IPi/5]^3 + c1^3c2^4c3c4^2Exp[2IPi/5]^2 + c1^4c2^2c3^3c4Exp[2IPi/5]))]]]}$

Out[4]= $-c1^{20}c2^{10}c3^{15}c4^5 - c1^{15}c2^{20}c3^5c4^{10} - c1^{10}c2^5c3^{20}c4^{15} - c1^5c2^{15}c3^{10}c4^{20} - 5c1^{15}c2^{10}c3^{10}c4^5z - 5c1^{10}c2^{15}c3^5c4^{10}z + 5c1^{10}c2^{10}c3^{10}c4^{10}z - 5c1^{10}c2^5c3^{15}c4^{10}z - 5c1^5c2^{10}c3^{10}c4^{15}z - 5c1^{10}c2^{10}c3^5c4^5z^2 - 5c1^{10}c2^5c3^{10}c4^5z^2 - 5c1^5c2^{10}c3^5c4^{10}z^2 - 5c1^5c2^5c3^{10}c4^{10}z^2 - 10c1^5c2^5c3^5c4^5z^3 + z^5$

The code for the polynomial $g(X;\mathbf{T})$ in example 1 is as follows:

In[66]:= $\mathbf{w = Exp[2PiI/3]}$
Out[66]= $e^{\frac{2\pi i}{3}}$

In[68]:= $\mathbf{Simplify[Product[(x - w^jA - w^{2j}B), \{j, 0, 2\}]]}$
Out[68]= $-A^3 - B^3 - 3ABx + x^3$

References

[Bor+12] A. Borel et al. *Emmy Noether in Bryn Mawr: Proceedings of a Symposium Sponsored by the Association for Women in Mathematics in Honor of Emmy Noether's 100th Birthday*. Springer New York, 2012. ISBN: 9781461255475.

[Coh12] H. Cohen. *Advanced Topics in Computational Number Theory*. Graduate Texts in Mathematics. Springer New York, 2012. ISBN: 9781441984890.

[Den95] R. Dentzer. "Polynomials with Cyclic Galois Group". In: *Communications in Algebra* 23.4 (1995), pp. 1593–1603.

[Fur25] Ph. Furtwängler. "Über Minimalbasen für Körper rationaler Funktionen". In: *S.B.Akad. Wiss. Wien* 134 (1925), pp. 69–80.

[Gas59] W. Gaschütz. "Fixkörper von p-Automorphismengruppen rein-transzendenter Körpererweiteriungen von p-Charakteristik". In: *Math. Zeitschr.* 71 (1959), pp. 466–468.

[Grö34] W. Gröbner. "Minimalbasis der Quaternionengruppe". In: *Monatshefte f. Math. und Physik* 41 (1934), pp. 78–84.

[HHR08] K. Hashimoto, A. Hoshi, and Y. Rikuna. "Noether's Problem and Q-Generic Polynomials for the Normalizer of the 8-Cycle in S8 and its Subgroups". In: *Mathematics of Computation* 77.262 (Apr. 2008), pp. 1153–1183.

[Hus] S. Hussein. *Valuation theory*. University of Houston. URL: `https://www.math.uh.edu/~saud/Number%20Theory/Valuation%20Theory.pdf`.

[JLY02] C.U. Jensen, A. Ledet, and N. Yui. *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*. Mathematical Sciences Research Institute Publications. Cambridge University Press, 2002. ISBN: 9780521819985.

[Keu15] F. Keune. *Galoistheorie*. Epsilon Uitgaven, Amsterdam, 2015. ISBN: 978-90-5041-150-9.

[Kob77] N. Koblitz. *p-adic Numbers, p-adic Analysis and Zeta Functions*. Springer-Verlag New York, 1977. ISBN: 978-1-4612-7014-0.

[Led00] A. Ledet. "Generic Extensions and Generic Polynomials". In: *J. Symbolic Computation* 30 (2000), pp. 867–872.

[Mae89] T. Maeda. "Noether's problem for A5". In: *Journal of Algebra* 125 (1989), pp. 418–430.

[Mer02] F. Mertens. "Ein Beweis des Galoisschen Fundamentalsatzes". In: *Wiener Sitz. Ber.* 111 (1902).

[Mer16] F. Mertens. "Gleichungen achten Grades mit Quaternionengruppe". In: *Wiener Sitz. Ber.* 125 (1916).

[Nak00] S. Nakano. "On generic cyclic polynomials of odd prime degree". In: *Proc. Japan Acad.* 76.10 (2000), pp. 159–162.

[Roe18] E. Roebroek. "Computation of Galois groups and corresponding polynomials". In: *Bachelor Thesis at Utrecht University* (2018).

[Sal82] D.J. Saltman. "Generic Galois extensions and problems in field theory". In: *Adv. Math.* 43 (1982), pp. 250–283.

[Sch92] L. Schneps. "On Cyclic Field Extensions of Degree 8". In: *Mathematica Scandinavica* 71 (1992), pp. 24–30.

[Smi91] G. W. Smith. “Generic Cyclic Polynomials of odd degree”. In: *Comm. Alg.* 19.12 (1991), pp. 3367–3391.

[Ste17] P. Stevenhagen. *Number Rings*. Universiteit Leiden, 2017. URL: `http://websites.math.leidenuniv.nl/algebra/ant.pdf`.

[Sut17] A. Sutherland. *Lecture Notes on Number Theory I*. Massachusetts Institute of Technology, 2017. URL: `https://math.mit.edu/classes/18.785/2017fa/LectureNotes11.pdf`.

[Swa69] R. G. Swan. “Invariant rational functions and a problem of Steenrod”. In: *Invent. Math.* 7 (1969), pp. 148–158.

[Wan48] S. Wang. “A Counter-Example to Grunwald’s Theorem”. In: *Annals of Mathematics, Second Series* 49.4 (1948), pp. 1008–1009.

[Zho15] J. Zhou. “Rationality for Subgroups of S6”. In: *Communications in Algebra* 43 (June 2015), pp. 2724–2738.