

Colby



Colby College
Digital Commons @ Colby

Honors Theses


Student Research

2018

Parametric Polynomials for Small Galois Groups

Claire Huang

Follow this and additional works at: <https://digitalcommons.colby.edu/honorsthesis>

 Part of the [Algebra Commons](#), [Harmonic Analysis and Representation Commons](#), and the [Number Theory Commons](#)

Colby College theses are protected by copyright. They may be viewed or downloaded from this site for the purposes of research and scholarship. Reproduction or distribution for commercial purposes is prohibited without written permission of the author.

Recommended Citation

Huang, Claire, "Parametric Polynomials for Small Galois Groups" (2018). *Honors Theses*. Paper 902.

<https://digitalcommons.colby.edu/honorsthesis/902>

This Honors Thesis (Open Access) is brought to you for free and open access by the Student Research at Digital Commons @ Colby. It has been accepted for inclusion in Honors Theses by an authorized administrator of Digital Commons @ Colby.

Parametric Polynomials for Small Galois Groups

Claire Huang

May 22, 2018

Contents

1	Introduction	1
2	Preliminaries	2
3	Cubic Polynomials	5
4	Quartic Polynomials	18
5	Appendix	28

1 Introduction

This paper is the honor thesis for my senior year at Colby College. It is widely inspired by the book *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem* in reference [1].

Galois theory, named after French mathematician Evariste Galois in 19th-century, is an important part of abstract algebra. It brings together many different branches of mathematics by providing connections among fields, polynomials, and groups.

Specifically, Galois theory allows us to attach a finite field extension with a finite group. We call such a group the **Galois group** of the finite field extension. A typical way to attain a finite field extension to compute the splitting field of some polynomial. So we can always start with a polynomial and find the finite group associate to the field extension on its splitting field. This focus is well-understood, but the converse remains puzzling to people. The Inverse Galois Problem asks the mysterious question of whether for any finite group, there exists a finite field extension that is associate to it. Furthermore, is there a polynomial whose splitting field that can make such a field extension? This mystery is part of the motivation for my thesis. The other motivation is the desire to replace this existence problem with constructive problem. We will write out some families of polynomials whose splitting fields over the rational field have certain small groups as their Galois group.

The presentation of this thesis assumes familiarity with basic Galois theory, and number theory. In the preliminary section, we will recall some of the concepts involved and introduce the definition of **parametric polynomials**. Then in the next two sections, we will discuss the parametric polynomials for subgroups of S_3, S_4 .

Many people have helped me in writing this thesis. In particular, I am grateful to my adviser Professor Fernando Gouvêa, for his guidance and advice not only in mathematics but in writing during the year.

2 Preliminaries

A field extension E/F is a pair of fields such that F is a subfield of E . Its Galois group $\text{Gal}(E/F)$ is defined to be the group of automorphisms of E that fix F pointwise. If we have a polynomial $p(x)$ over the field F , then we can also have its splitting field L , which is the smallest field that contains F and all the roots of $p(x)$. L/F is a finite field extension, and the Galois group $\text{Gal}(L/F)$ can be identified with a permutation group of the roots of $p(x)$. Moreover, if $p(x)$ is irreducible, then $\text{Gal}(L/F)$ acts transitively on all the roots.

Now we see that with any polynomial $p(x)$ of degree n over a field F , we get a field extension L/F where L is the splitting field of $p(x)$ over F , and then we get a finite group $\text{Gal}(L/F)$ which is isomorphic to a subgroup of S_n . If $\text{Gal}(L/F)$ is isomorphic to a group $G < S_n$, we call L/F a **G -extension**. When n is large, it

is very hard to determine the exact subgroup that $\text{Gal}(E/F)$ is isomorphic to, but at least we know that we can always go from a polynomial to a finite group. So it is natural to raise the Inverse Galois Problem and question whether we can do the reverse and go from a finite group to a polynomial. In other words, Given a finite field F , is every finite group isomorphic to a Galois group of some field extension L/F , where L is the splitting field of a polynomial over F ?

The famous mathematician David Hilbert was the first one to study this question in depth. It still remains open today. Hilbert's Irreducibility theorem brings some constructive aspects of solving this problem for the rational field \mathbb{Q} , and it can be formulated as the following:

Theorem 2.1. (Hilbert's Irreducibility Theorem)

Let $\vec{t} = (t_1, \dots, t_r)$ and $\vec{x} = (x_1, \dots, x_s)$ be indeterminates. Also suppose $f_1(\vec{t}, \vec{x}), \dots, f_n(\vec{t}, \vec{x})$ are irreducible in the polynomial ring $\mathbb{Q}(\vec{t})[\vec{x}]$, whose splitting fields are denoted by $\langle f_1(\vec{t}, \vec{x}) \rangle, \langle f_2(\vec{t}, \vec{x}) \rangle, \dots, \langle f_n(\vec{t}, \vec{x}) \rangle$ respectively. For any $\vec{b} = (b_1, \dots, b_r) \in \mathbb{Q}^r$, the specialized polynomial $f_i(\vec{b}, \vec{x})$ is a polynomial in $\mathbb{Q}[\vec{x}]$ with splitting field $\langle f_i(\vec{b}, \vec{x}) \rangle$. The following is true:

(1) For all $\vec{b} \in \mathbb{Q}^r$, if the specialized polynomials $f_i(\vec{b}, \vec{x})$ all have nonzero discriminant, then every $\text{Gal}(\langle f_i(\vec{b}, \vec{x}) \rangle / \mathbb{Q})$ is isomorphic to a subgroup of $\text{Gal}(\langle f_i(\vec{t}, \vec{x}) \rangle / \mathbb{Q}(\vec{t}))$.

(2) There are infinitely many $\vec{b} \in \mathbb{Q}^r$ such that the specialized polynomials $f_1(\vec{b}, \vec{x}), \dots, f_n(\vec{b}, \vec{x})$ are irreducible in $\mathbb{Q}[\vec{x}]$, and for each i , $\text{Gal}(\langle f_i(\vec{b}, \vec{x}) \rangle / \mathbb{Q}) \cong \text{Gal}(\langle f_i(\vec{t}, \vec{x}) \rangle / \mathbb{Q}(\vec{t}))$.

People define a field satisfying the properties described in Hilbert's Irreducibility Theorem as a **hilbertian field**. So this irreducibility Theorem tells us that \mathbb{Q} is hilbertian.

Notice that the first part in the Irreducibility Theorem claims that for an irreducible polynomial $f(\vec{t}, \vec{x})$ in $\mathbb{Q}(\vec{t})[\vec{x}]$, there may be degenerate cases, where for some \vec{b} the Galois group of the specialized polynomial $f(\vec{b}, \vec{x})$ in $\mathbb{Q}[\vec{x}]$ is not isomorphic to $\text{Gal}(\langle f(\vec{t}, \vec{x}) \rangle / \mathbb{Q}(\vec{t}))$ but to a proper subgroup of it. For example $x^2 - t$ is irreducible over $\mathbb{Q}(t)$ and thus has Galois group C_2 , but $x^2 - 4$ splits over \mathbb{Q} . Note

that set of those $b \in \mathbb{Q}$ such that $x^2 - b$ has trivial Galois group is the set of squares in \mathbb{Q} . Hence, if we randomly pick a $b \in \mathbb{Q}$, $x^2 - b$ is more likely to be irreducible and have Galois group isomorphic to C_2 than to be reducible. In fact, this is true for any irreducible polynomial $f(\vec{t}, x)$ in $\mathbb{Q}(\vec{t})[x]$. To be precise, the \vec{b}' 's such that the specialized polynomial $f(\vec{b}', x)$ does not have the same Galois group over \mathbb{Q} as the Galois group of $f(\vec{t}, x)$ over $\mathbb{Q}(\vec{t})$ form a "thin set", and thin subsets of \mathbb{Q} has density zero. This paper will not dig deeper in this notion.

Although the original Inverse Galois Problem is really an existence problem, now with Theorem 2.1, we can ask a more explicit question: For any finite group G , can we have a polynomial $p(t, x)$ in $\mathbb{Q}(\vec{t})[x]$ that describes all polynomials in $\mathbb{Q}[x]$ whose splitting field over \mathbb{Q} has Galois group isomorphic to G ?

Such a polynomial $p(t, x)$ is called the **parametric polynomial** for G -extensions over \mathbb{Q} . Now let us see a formal definition.

Definition 2.2. (Parametric Polynomial)

Let G be a finite group, and $\vec{t} = (t_1, \dots, t_r)$, x be indeterminates. A monic polynomial $p(\vec{t}, x)$ in the polynomial ring $\mathbb{Q}(\vec{t})[x]$ is a parametric polynomial for G over \mathbb{Q} if it satisfies the following:

A1. The splitting field of $p(\vec{t}, x)$ over the field $\mathbb{Q}(\vec{t})$ is a G -extension.

A2. For any G -extension L over \mathbb{Q} , there exists some $\vec{b} \in \mathbb{Q}^r$ such that L is the splitting field of $p(\vec{b}, x)$ over \mathbb{Q} .

By Definition 2.2, if $p(\vec{t}, x)$ is a parametric polynomial for G -extensions, then every G -extension L/\mathbb{Q} can be identified with the splitting field of $p(\vec{b}, x)$ in $\mathbb{Q}[x]$, but according to Hilbert's Irreducibility Theorem, not every specialized polynomial $p(\vec{b}, x)$ has splitting field over \mathbb{Q} as a G -extension.

Having such a parametric polynomial $p(\vec{t}, x)$ for G -extensions of \mathbb{Q} , there are two known defects: one is that there are degenerate cases when the splitting field of some $p(\vec{b}, x)$ over \mathbb{Q} is not a G -extension, and the other is that there can be distinct elements that parametrize the same G -extension L/\mathbb{Q} . However, a parametric polynomial of G -extension is still significant because it not only helps us find one field over \mathbb{Q} that is a G -extension, but also describes all fields over \mathbb{Q} that are G -extensions.

This paper will only discuss the parametric polynomials for transitive subgroups of S_3 and S_4 , whose parametric polynomials are cubic or quartic. Those results

are largely taken from reference [1].

3 Cubic Polynomials

Recall that the Galois group of an irreducible polynomial f of degree n is isomorphic to a subgroup of S_n and acts transitively on the roots of f .

For an irreducible cubic polynomial over \mathbb{Q} , its Galois group is isomorphic to either C_3 or S_3 ; on the other hand, if L/\mathbb{Q} is a C_3 -extension or a S_3 -extension, then L can only be the splitting field of an irreducible cubic polynomial. In this section, we will find some parametric polynomials for C_3 -extensions and S_3 -extensions over \mathbb{Q} .

A parametric polynomial for S_3 is easy. In fact, a parametric polynomial for any S_n is easy, because clearly the polynomial with $n + 1$ parameters $t_n x^n + t_{n-1} x^{n-1} + \cdots + t_1 x + t_0$ in $\mathbb{Q}(t_0, t_1, \dots, t_n)[x]$ is always parametric for any S_n -extensions. So in the case of S_n , the interesting question is to find parametric polynomials with fewer parameters. For example, the monic polynomial $x^n + t_{n-1} x^{n-1} + \cdots + t_1 x + t_0$ is a parametric for S_n -extensions with one fewer parameters than the previous polynomial, since every polynomial of degree n over \mathbb{Q} has the form $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, and we can scale all coefficients by $\frac{1}{a_n}$ and get a monic polynomials without changing the roots.

In this section, we will show that there are parametric polynomials for C_3 - and S_3 -extensions with only one parameter.

Lemma 3.1.

For any irreducible cubic polynomial $f(x)$ over \mathbb{Q} , there exists some $b \in \mathbb{Q}$ such that $x^3 + bx + b$ is irreducible over $\mathbb{Q}[x]$ and has the same splitting field as f .

Proof.

As an irreducible cubic polynomial in $\mathbb{Q}[x]$, $f(x)$ has the form $f(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$, where a_0, a_1, a_2, a_3 are in \mathbb{Q} . Since we can scale all coefficients by $\frac{1}{a_3}$ without changing roots, we can assume $a_3 = 1$, i.e. f is monic, without loss of generality.

Assume the three roots of $f(x)$ are $\gamma_1, \gamma_2, \gamma_3$.

Notice $a_2 = -(\gamma_1 + \gamma_2 + \gamma_3)$, which is equivalent to saying

$$-(\gamma_1 + \gamma_2 + \gamma_3) - a_2 = -\left(\left(\gamma_1 + \frac{1}{3}a_2\right) + \left(\gamma_2 + \frac{1}{3}a_2\right) + \left(\gamma_3 + \frac{1}{3}a_2\right)\right) = 0.$$

Substitute $x = y - \frac{1}{3}a_2$ into $f(x) = (x - \gamma_1)(x - \gamma_2)(x - \gamma_3)$. Without changing the splitting field, we get $f(y) = \left(y - \left(\gamma_1 + \frac{1}{3}a_2\right)\right)\left(y - \left(\gamma_2 + \frac{1}{3}a_2\right)\right)\left(y - \left(\gamma_3 + \frac{1}{3}a_2\right)\right) = y^3 + py + q \in \mathbb{Q}[x]$ with roots $\lambda_1, \lambda_2, \lambda_3$, where $\lambda_i = \gamma_i + \frac{1}{3}a_2$. Since $f(x)$ is irreducible, then $\lambda_i \neq 0$ for each i .

We claim that we can assume $p \neq 0$. Indeed, if $p = 0$, then $f(y) = y^3 + q$, and $\lambda_i^3 = -q$ for each i . If $q = 0$, then $f(y)$ splits over \mathbb{Q} , which is a contradiction. So $q \neq 0$. For each i , $\left(\lambda_i + \frac{1}{\lambda_i}\right)^3 = \lambda_i^3 + \frac{1}{\lambda_i^3} + 3\lambda_i + \frac{3}{\lambda_i} = -q - \frac{1}{q} + 3 \cdot \left(\lambda_i + \frac{1}{\lambda_i}\right)$, which implies $\left(\lambda_i + \frac{1}{\lambda_i}\right)^3 - 3\left(\lambda_i + \frac{1}{\lambda_i}\right) + \left(q + \frac{1}{q}\right) = 0$. In other words, $\lambda_i + \frac{1}{\lambda_i}$ for $i = 1, 2, 3$ are the three roots of the polynomial $g(x) = x^3 - 3x + \left(q + \frac{1}{q}\right)$. For each i ,

$\mathbb{Q} \subset \mathbb{Q}\left(\lambda_i + \frac{1}{\lambda_i}\right) \subset \mathbb{Q}(\lambda_i)$. Because there are no proper intermediate fields between the two, $\mathbb{Q}\left(\lambda_i + \frac{1}{\lambda_i}\right)$ is either \mathbb{Q} or $\mathbb{Q}(\lambda_i)$. If we can show $\mathbb{Q}(\lambda_i) = \mathbb{Q}\left(\lambda_i + \frac{1}{\lambda_i}\right)$, then we can conclude that f and g have the same splitting field. Suppose, for a contradiction, that $\lambda_i + \frac{1}{\lambda_i} = r \in \mathbb{Q}$ for some i . Then $\lambda_i^2 + 1 = r\lambda_i$ implies that λ_i is a root of the quadratic polynomial $x^2 - rx + 1$, which contradicts the fact that λ_i has degree 3. Hence, $f(x)$ and $g(x)$ over \mathbb{Q} have the same splitting field. From now on, we can work with g , which is in the form $g(x) = x^3 + px + q$ with $p \neq 0$.

So far, we have shown that for any irreducible cubic polynomial over \mathbb{Q} , there exists a polynomial in the form $y^3 + py + q$ in $\mathbb{Q}[x]$ such that $p \neq 0$, and with the same splitting field as the original one. Then we can substitute $y = \frac{q}{p}z$ into $f(y)$.

Again, without changing the splitting field, we get

$$f(z) = \frac{q^3}{p^3}z^3 + p \cdot \frac{q}{p}z + q = \frac{q^3}{p^3} \cdot \left(z^3 + \frac{p^3}{q^2}z + \frac{p^3}{q^2}\right).$$

Set $b = \frac{p^3}{q^2}$. Notice that $b \in \mathbb{Q}$ and $z^3 + bz + b$ in $\mathbb{Q}[x]$ has the same roots as

$f(z) = \frac{q^3}{p^3}(z^3 + bz + b)$, and hence it has the same splitting field as $f(z)$. Since we never change the splitting field to get $f(z)$, then $z^3 + tz + t$ also has the same splitting field as the original cubic irreducible polynomial $f(x)$. \square

Let us see an example of using this process described in Lemma 3.1 to find some $b \in \mathbb{Q}$ such that the polynomial $x^3 + bx + b$ has the same splitting field as $x^3 - 2$.

Since $x^3 - 2$ is in the form $x^3 + px + q$ with $p = 0$, we know it has the same splitting field as $g(x) = x^3 - 3x - (2 + \frac{1}{2}) = x^3 - 3x - \frac{5}{2}$. Substitute $x = \frac{5}{6}y$. We get $g(y) = \frac{125}{216}y^3 - \frac{5}{2}y - \frac{5}{2}$, which has the same splitting field as $x^3 - \frac{108}{25}x - \frac{108}{25}$. In particular, they both have the splitting field $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.

Clearly Lemma 3.1 shows that $p(t, x) = x^3 + tx + t$ in $\mathbb{Q}(t)[x]$ satisfies condition A2 for C_3 and S_3 . It cannot be a parametric polynomial for C_3 -extensions, because if it is, then a specialized polynomial $p(b, x)$ in \mathbb{Q} cannot have Galois group isomorphic to S_3 . However, our example $p(\frac{108}{25}) = x^3 - \frac{108}{25}x - \frac{108}{25}$ has the same splitting field as $x^3 - 2$ and thus has the same Galois group, which is isomorphic to S_3 .

Theorem 3.2.

$p_1(t, x) = x^3 + tx + t$ is a parametric polynomial for S_3 -extensions of \mathbb{Q} .

We can also prove the theorem by directly showing that the Galois group of $p_1(t, x)$ over the field $\mathbb{Q}(t)$ is isomorphic to S_3 . We can use the help of an important theorem from basic Galois theory stated as follows:

Theorem 3.3.

Let F be any field of characteristic 0. An irreducible polynomial of degree n over the field F has Galois group isomorphic a subgroup of the the alternating group A_n if and only if its discriminant is a square in F .

Now we finish the proof that $p_1(t, x) = x^3 + tx + t$ is a parametric polynomial for S_3 over \mathbb{Q} .

Proof of Theorem 3.2.

Let G be the Galois group of $p_1(t, x)$ over $\mathbb{Q}(t)$.

The discriminant $d_{p_1}(t)$ of $p_1(t, x)$ in $\mathbb{Q}(t)[x]$ is $d_{p_1}(t) = -4t^3 - 27t^2 = t^2(-4t - 27)$. Since $-4t - 27$ is not a square in $\mathbb{Q}(t)$, $d_{p_1}(t)$ is not a square in $\mathbb{Q}(t)$. Theorem 3.3 tells us that $G \cong S_3$.

Therefore, $p_1(t, x)$ satisfies A1 for S_3 , and is a parametric polynomial for S_3 . \square

As we see, if we randomly pick a $b \in \mathbb{Q}$, $p_1(b, x) = x^3 + bx + b$ is very likely to be irreducible and $-4b - 27$ is very likely not to be a square in \mathbb{Q} . Nevertheless, for some specific $b \in \mathbb{Q}$, $p_1(b, x)$ might not have Galois group isomorphic to S_3 or might not be irreducible. In the introduction, we refer to such b 's as “degenerate cases”. The following table displays some examples of $p_1(b, x)$, which may or may not display degenerate cases.

Table 1: Examples of specialized $p_1(t, x) = x^3 + tx + t$

b	$p_1(b, x)$	Irreducibility	Galois Group isomorphic to
-7	$x^3 - 7x - 7$	irreducible	C_3
0	x^3	reducible	$\{Id\}$
1	$x^3 + x + 1$	irreducible	S_3
3	$x^3 + 3x + 3$	irreducible	S_3

We call an irreducible polynomial whose splitting field is L over \mathbb{Q} is C_3 -extension a “**cyclic cubic**”. Then “a polynomial $p(t, x)$ in $\mathbb{Q}(t)[x]$ is a parametric cyclic cubic” means that $p(t, x)$ is a parametric polynomial for C_3 -extensions of \mathbb{Q} . In Lemma 3.1 we have showed that for every cyclic cubic $f(x)$ over \mathbb{Q} , there exists $b \in \mathbb{Q}$ such that $p_1(b, x) = x^3 + bx + b$ has the same splitting field as the given cyclic cubic $f(x)$. According to Theorem 3.3, for those $b \in \mathbb{Q}$ such that the specialized polynomial $p_1(b, x)$ is a cyclic cubic, the discriminant $d_{p_1}(b) = b^2(-4b - 27)$ of $p_1(b, x)$ is a square in \mathbb{Q} . This happens only if $-4b - 27$ is a square in \mathbb{Q} .

For any $a \in \mathbb{Q}$, we can solve for b in $-4b - 27 = a^2$ and get $b = -\frac{a^2 + 27}{4}$.

Hence, the polynomial $p_2(t, x) = x^3 - \frac{t^2 + 27}{4}x - \frac{t^2 + 27}{4}$ in $\mathbb{Q}(t)[x]$ has discrimi-

nant $d_{p_2}(t) = \left(\frac{t^2+27}{4}\right)^2 t^2$, which is a square in $\mathbb{Q}(t)$. Since $p_2(t, x)$ is irreducible over $\mathbb{Q}(t)$, the Galois group of $p_2(t, x)$ over \mathbb{Q} is isomorphic to C_3 . So we have shown:

Corollary 3.4.

$p_2(t, x) = x^3 - \frac{t^2+27}{4}x - \frac{t^2+27}{4}$ is a parametric cyclic cubic over \mathbb{Q} .

Here are some examples.

Table 2: Examples of specialized $p_2(t, x) = x^3 - \frac{t^2+27}{4}x - \frac{t^2+27}{4}$

b	$p_2(b, x)$	Irreducibility	Galois Group isomorphic to
0	$x^3 - \frac{27}{4}x - \frac{27}{4}$	$\frac{1}{4}(x-3)(2x+3)^2$	$\{Id\}$
1	$x^3 - 7x - 7$	irreducible	C_3
2	$x^3 - \frac{31}{4}x - \frac{31}{4}$	irreducible	C_3
3	$x^3 - 9x - 9$	irreducible	C_3

Note that we have derived a parametric polynomial for C_3 from a parametric polynomial for S_3 by looking at the discriminant. A more interesting parametric cyclic cubic $p_3(t, x) = x^3 - tx^2 + (t-3)x + 1$ can be derived by considering the action of C_3 on the roots. One advantage of this new parametric cyclic cubic is that the parameter will appear with degree one.

Consider the field $\mathbb{Q}(z)$, where (for now) z is an indeterminate. The map $\sigma : z \mapsto \frac{1}{1-z}$ generates a cyclic group of order three in $\text{Gal}(\mathbb{Q}(z)/\mathbb{Q})$:

$$\sigma^2 : z \mapsto \frac{1}{1 - \frac{1}{1-z}} = \frac{z-1}{z}, \text{ and } \sigma^3 : z \mapsto \frac{1}{1 - \frac{z-1}{z}} = z.$$

Consider the polynomial $f(z, x)$ in $\mathbb{Q}(z)[x]$:

$$\begin{aligned} f(z, x) &= (x - z) \left(x - \sigma(z) \right) \left(x - \sigma^2(z) \right) \\ &= (x - z) \left(x - \frac{1}{1-z} \right) \left(x - \frac{z-1}{z} \right) \end{aligned}$$

Clearly, if β is a complex number such that the specialized polynomial $f(\beta, x)$ is in $\mathbb{Q}[x]$, then the Galois group of $f(\beta, x)$ over \mathbb{Q} is isomorphic to C_3 and is generated by the map $\beta \mapsto \frac{1}{1-\beta}$.

Now we write out $f(z, x)$ as:

$$\begin{aligned} f(z, x) &= (x - z) \left(x - \frac{1}{1-z} \right) \left(x - \frac{z-1}{z} \right) \\ &= x^3 - \left(z + \frac{1}{1-z} + \frac{z-1}{z} \right) x^2 + \left(z \cdot \frac{1}{1-z} + \frac{1}{1-z} \cdot \frac{z-1}{z} + z \cdot \frac{z-1}{z} \right) x - \\ &\quad z \cdot \frac{1}{1-z} \cdot \frac{z-1}{z} \\ &= x^3 - \left(z + \frac{1}{1-z} + \frac{z-1}{z} \right) x^2 + \left(\frac{z}{1-z} - \frac{1}{z} + z - 1 \right) x + 1. \end{aligned}$$

Parameterize $t = z + \frac{1}{1-z} + \frac{z-1}{z}$. Then we get a polynomial in $\mathbb{Q}(t)[x]$:

$$\begin{aligned} f(t, x) &= x^3 - tx^2 + \left(\frac{z}{1-z} - \frac{1}{z} + t - \frac{1}{1-z} - \frac{z-1}{z} - 1 \right) x + 1 \\ &= x^3 - tx^2 + (t-3)x + 1. \end{aligned}$$

Theorem 3.5.

$p_3(t, x) = x^3 - tx^2 + (t-3)x + 1$ is a parametric cyclic cubic of \mathbb{Q} .

Proof.

Again, we need to show that $p_3(t, x)$ is a cyclic cubic over $\mathbb{Q}(t)$ and every C_3 -extension over \mathbb{Q} is the splitting field of the specialized polynomial $p(b, x)$ for some $b \in \mathbb{Q}$.

It is clear that $p_3(t, x) = x^3 - tx^2 + (t - 3)x + 1$ is irreducible in $\mathbb{Q}(t)[x]$. Hence, by Theorem 3.3, to show it is a cyclic cubic over $\mathbb{Q}(t)$, we only need to show the discriminant $d_{p_3}(t)$ is a square in $\mathbb{Q}(t)$. Indeed,

$$\begin{aligned} d(t) &= t^2(t-3)^2 - 4(t-3)^3 - 4t^3 - 27 - 18t(t-3) \\ &= t^2(t^2 - 6t + 9) - 4(t^3 - 27 + 27t - 9t^2) - 4t^3 - 27 - (18t^2 - 54t) \\ &= t^4 - 6t^3 + 27t^2 - 54t + 81 \\ &= (t^2 - 3t + 9)^2 \text{ is a square in } \mathbb{Q}(t). \end{aligned}$$

Hence, we have showed A1. We still need to show $p_3(t, x)$ has property A2.

Now let L/\mathbb{Q} be an arbitrary C_3 -extension, with Galois group $G = \langle \sigma \rangle \cong C_3$. We'll show there exists $b \in \mathbb{Q}$ such that the specialized polynomial $p_3(b, x)$ has splitting field L by showing L contains an element β such that $\sigma : \beta \mapsto \frac{1}{1-\beta}$.

By Normal Basis Theorem, there exists α in L such that $\{\alpha, \sigma(\alpha), \sigma^2(\alpha)\}$ is a basis of L over \mathbb{Q} .

Let $x, y \in L$ such that $x = \alpha - \sigma(\alpha), y = \sigma^2(\alpha) - \sigma(\alpha)$. We claim that x, y are linearly independent over \mathbb{Q} , and $\sigma(x) = -y, \sigma(y) = x - y$.

We can directly check that $\sigma(x) = \sigma(\alpha - \sigma(\alpha)) = \sigma(\alpha) - \sigma^2(\alpha) = -y$,

$$\begin{aligned} \text{and } \sigma(y) &= \sigma(\sigma^2(\alpha) - \sigma(\alpha)) \\ &= \alpha - \sigma^2(\alpha) \\ &= \alpha - \sigma(\alpha) - \sigma^2(\alpha) + \sigma(\alpha) \\ &= (\alpha - \sigma(\alpha)) - (\sigma^2(\alpha) - \sigma(\alpha)) \\ &= x - y. \end{aligned}$$

Observe that for any $a, b \in \mathbb{Q} : ax + by = a(\alpha - \sigma(\alpha)) + b(\sigma^2(\alpha) - \sigma(\alpha))$
 $= a\alpha - (a+b)\sigma(\alpha) + b\sigma^2(\alpha)$.

So $ax + by = 0$ only if $a, b = 0$. i.e. $x, y \in L$ are linearly independent over \mathbb{Q} .

In the Appendix, we will show how we found this pair of $x, y \in L$ using representation theory.

Since $x, y \neq 0$, we can let $\beta = \frac{x}{y}$, and $\beta \neq 0$. Also β is not in \mathbb{Q} , because x, y are linearly independent over \mathbb{Q} . Then $\sigma(\beta) = \frac{\sigma(x)}{\sigma(y)} = \frac{-y}{x-y} = \frac{\frac{-y}{y}}{\frac{x}{y} - \frac{y}{y}} = \frac{-1}{\beta - 1} = \frac{1}{1 - \beta}$.

Again, we let $b = \beta + \frac{1}{1 - \beta} + \frac{\beta - 1}{\beta}$. Notice b must be in \mathbb{Q} , because the Galois group $G = \langle \sigma \rangle$ fixes b . Thus, the specialized polynomial $p_3(b, x) = x^3 - bx^2 + (b - 3)x + 1 = (x - \beta)(x - \frac{1}{1 - \beta})(x - \frac{\beta - 1}{\beta})$ is a polynomial in $\mathbb{Q}[x]$, and has Galois group isomorphic to C_3 . Suppose it has splitting field M . We'll show $M = L$.

Since $\beta = \frac{x}{y} \in L$, we know $M = \mathbb{Q}(\beta) \leq L$. By the Tower Law, $[L : M][M : \mathbb{Q}] = [L : \mathbb{Q}] = 3$. Since 3 is a prime number, either $[L : M] = 1$ or $[M : \mathbb{Q}] = 1$. $[M : \mathbb{Q}] \neq 1$ because $\beta \notin \mathbb{Q}$. Thus, $[L : M]$ has to equal 1 and $L = M$.

In other words, for this particular $b \in \mathbb{Q}$, the specialized polynomial $p_3(b, x) = x^3 - bx^2 + (b - 3)x + 1$ in $\mathbb{Q}[x]$ has the splitting field L , and we have finished our proof of showing $p_3(t, x) = x^3 - tx^2 + (t - 3)x + 1$ is a parametric polynomial for C_3 -extensions of \mathbb{Q} . \square

Table 3: Examples of specialized $p_2(t, x) = x^3 - \frac{t^2+27}{4}x - \frac{t^2+27}{4}$

b	$p_2(b, x)$	Irreducibility	Galois Group isomorphic to
-1	$x^3 + x^2 - 4x + 1$	irreducible	C_3
0	$x^3 - 3x + 1$	irreducible	C_3
1	$x^3 - x^2 - 2x + 1$	irreducible	C_3
2	$x^3 - 2x^2 - x + 1$	irreducible	C_3
3	$x^3 - 3x^2 + 1$	irreducible	C_3

Remark 3.6.

In fact, if b is an integer, then $p_3(b, x) = x^3 - bx^2 + (b - 3)x + 1$ is always a cyclic cubic over \mathbb{Q} .

Here is the argument: if for some $b \in \mathbb{Z}$ the specialized polynomial $p_3(b, x) = x^3 - bx^2 + (b-3)x + 1$ is reducible, then it has a rational root. By the Rational Roots Theorem, its rational root can only be ± 1 . In other words, $p_3(b, 1) = 0$ or $p_3(b, -1) = 0$. Since $p_3(b, 1) = 1 - b + (b-3) + 1 = -1$ is never 0, the only case $p_3(b, x)$ is reducible for integer b is when $p_3(b, -1) = -1 - b - (b-3) + 1 = -2b + 3 = 0$. However, this implies $b = \frac{3}{2} \notin \mathbb{Z}$. Therefore, if b is an integer, $p_3(b, x)$ is a cyclic cubic.

We can think about some cases when $b \in \mathbb{Q}$ and $p_3(b, x)$ is reducible. We know one example of $b = \frac{3}{2}$. Since we have showed that $p_3\left(\frac{3}{2}, -1\right) = 0$, $p_3\left(\frac{3}{2}, x\right) = x^3 - \frac{3}{2}x^2 + \left(\frac{3}{2} - 3\right)x + 1$ has to be reducible. Indeed, in this case, $p_3\left(\frac{3}{2}, x\right)$ can be factored as $(x+1)\left(x - \frac{1}{2}\right)(x-2)$.

More generally, if the specialized polynomial $p_3(b, x)$ in $\mathbb{Q}[x]$ is reducible for some $b \in \mathbb{Q}$, then it has a rational root r .

$$\begin{aligned} p_3(b, r) = 0 &\iff r^3 - br^2 + (b-3)r + 1 = 0 \\ &\iff (-r^2 + r) \cdot b = -1 + 3r - r^3. \end{aligned}$$

Since $p_3(b, 0) = 0 - b \cdot 0 + (b-3) \cdot 0 + 1 = 1$ and $p_3(b, 1) = -1$, the rational root r cannot be 0 or 1, which implies $-r^2 + r$ is never 0. So

$$p_3(b, r) = 0 \iff b = \frac{r^3 - 3r + 1}{r^2 - r}.$$

Hence, for any non-zero rational number r , the specialized polynomial $p_3(b, x)$ in $\mathbb{Q}[x]$ is reducible for $b = \frac{r^3 - 3r + 1}{r^2 - r}$. We can make the following remark:

Remark 3.7.

There are infinitely many rational number b 's such that $p_3(b, x) = x^3 - tx^2 + (t-3)x + 1$ is reducible over \mathbb{Q} .

The table below demonstrates some examples of some specialized $p_3(t, x)$ that are reducible in $\mathbb{Q}[x]$.

Table 4: Examples of specialized $p_3(t, x) = x^3 - tx^2 + (t - 3)t + 1$ that are reducible

r	b	$p_3(b, x)$	Factorization
$\frac{1}{2}$	$\frac{3}{2}$	$x^3 - \frac{3}{2}x^2 - \frac{3}{2}x + 1$	$(x + 1)(x - \frac{1}{2})(x - 2)$
$\frac{2}{3}$	$\frac{19}{6}$	$x^3 - \frac{19}{6}x^2 - \frac{1}{6}x + 1$	$\frac{1}{6}(3x - 2)(2x + 1)(x - 3)$
$\frac{1}{3}$	$-\frac{1}{6}$	$x^3 + \frac{1}{6}x^2 - \frac{19}{6}x + 1$	$\frac{1}{6}(3x - 1)(2x - 3)(x + 2)$
-3	$-\frac{17}{12}$	$x^3 + \frac{53}{12}x^2 - \frac{19}{12}x + 1$	$\frac{1}{12}(4x - 1)(3x - 4)(x + 3)$

Now we have an interesting parametric cyclic cubic over \mathbb{Q} $p_3(t, x) = x^3 - tx^2 + (t - 3)x + 1$. It is natural to ask whether there can be two different $b_1, b_2 \in \mathbb{Q}$ such that the specialized polynomial $p_3(b_1, x)$ and $p_3(b_2, x)$ parametrize the same C_3 -extension of \mathbb{Q} .

The answer is yes.

Theorem 3.8.

For all $b \in \mathbb{Q}$ such that $p_3(b, x)$ is a cyclic cubic, $p_3(b, x)$ and $p_3(3 - b, x)$ have the same splitting field over \mathbb{Q} .

Proof.

Suppose $b \in \mathbb{Q}$ and $p_3(b, x)$ is a cyclic cubic with splitting field L . We will show $p_3(3 - b, x) = x^3 - (3 - b)x^2 - bx + 1$ has the same splitting field as $p_3(b, x)$.

In the proof of Theorem 3.5, we have showed that there is an irrational $\beta \in L$ such that $b = \beta + \frac{1}{1 - \beta} + \frac{\beta - 1}{\beta}$ and $p_3(b, x) = (x - \beta)\left(x - \frac{1}{1 - \beta}\right)\left(x - \frac{\beta - 1}{\beta}\right)$. Then $3 - b = 3 - \left(\beta + \frac{1}{1 - \beta} + \frac{\beta - 1}{\beta}\right) = (1 - \beta) + \left(1 - \frac{1}{1 - \beta}\right) + \frac{1}{\beta}$.

Write $u = 1 - \beta$, $v = 1 - \frac{1}{1 - \beta} = \frac{\beta}{\beta - 1}$, $w = \frac{1}{\beta}$. Notice β is not rational, so u, v, w cannot be rational. Since $\mathbb{Q}(u, v, w) \leq \mathbb{Q} = L$ and $\mathbb{Q}(u, v, w) \neq \mathbb{Q}$, it must be true that $\mathbb{Q}(u, v, w) = L$.

We claim that $(x-u)(x-v)(x-w) = x^3 - (u+v+w)x^2 + (uv+uw+vw)x - uvw$ is a polynomial in $\mathbb{Q}[x]$. In other words, we will show $u+v+w, uv+uw+vw, uvw \in \mathbb{Q}$ through straight forward computation.

By assumption, $u+v+w = 3-b \in \mathbb{Q}$. Now consider

$$uv = (1-\beta) \left(1 - \frac{1}{1-\beta}\right) = (1-\beta) - 1 = -\beta,$$

$$uw = (1-\beta) \cdot \frac{1}{\beta} = \frac{1}{\beta} - 1 = \frac{1-\beta}{\beta},$$

$$vw = \left(1 - \frac{1}{1-\beta}\right) \cdot \frac{1}{\beta} = \frac{-\beta}{1-\beta} \cdot \frac{1}{\beta} = \frac{-1}{1-\beta}.$$

As we can see, $uv+uw+vw = -\beta + \frac{1-\beta}{\beta} + \frac{-1}{1-\beta} = -b \in \mathbb{Q}$.

And $uvw = (uv)w = -\beta \cdot \frac{1}{\beta} = -1$

Hence, $(x-u)(x-v)(x-w) = x^3 - (3-b)x - b + 1$ is a polynomial in $\mathbb{Q}[x]$. Moreover, $(x-u)(x-v)(x-w) = p_3(3-b, x)$, and has splitting field $\mathbb{Q}(u, v, w) = L$.

Therefore, we have shown that for all $b \in \mathbb{Q}$ such that the specialized polynomial $p_3(b, x)$ is a cyclic cubic over \mathbb{Q} , $p_3(3-b, x)$ in $\mathbb{Q}[x]$ has the same splitting field as $p_3(b, x)$. \square

Let z be an indeterminate, and $t = z + \frac{1}{1-z} + \frac{z-1}{z}$. We know that the parametric cyclic cubic $p_3(t, x) = (x-z) \left(x - \frac{1}{1-z}\right) \left(x - \frac{z-1}{z}\right)$. Theorem 3.8 implies that $p_4(t, x) = p_3(t-3, x)$ in $\mathbb{Q}(t)[x]$ is also a parametric cyclic cubic of \mathbb{Q} , and $p_4(t, x) = \left(x - (1-z)\right) \left(x - \frac{z}{z-1}\right) \left(x - \frac{1}{z}\right)$. It is natural to think about the relationship between $p_3\left(t, \frac{1}{x}\right)$ and $p_4(t, x)$ in the field $\mathbb{Q}(t, x)$.

$$\begin{aligned} p_3\left(t, \frac{1}{x}\right) &= \frac{1}{x^3} - \frac{t}{x^2} + \frac{t-3}{x} + 1, \text{ and} \\ p_4(t, x) &= x^3 - (3-t)x^2 - tx + 1 \\ &= x^3 \cdot p_3\left(t, \frac{1}{x}\right). \end{aligned}$$

For the specialized polynomials $p_3(b, x)$ and $p_4(b, x) = p_3(3 - b, x)$, who have the same splitting field, the only case $b = 3 - b$ is when $b = \frac{3}{2}$, but we have shown that $p_3\left(\frac{3}{2}, x\right)$ is reducible. So we can claim that for any C_3 -extension L/\mathbb{Q} , there are at least two distinct b 's such that L is the splitting field of the specialized polynomial $p_3(b, x) = x^3 - bx^2 + (b - 3)x + 1$. And there can be more than two. For example, $p_3(0, x)$, $p_3(-3, x)$, $p_3(6, x)$, and $p_3(3, x)$ all parametrize the same C_3 -extension.

Recall that when we proved $p_3(t, x) = x^3 + tx + t$ is a parametric polynomial for S_3 -extensions of \mathbb{Q} , we showed that for every cubic polynomial $f(x)$, there exists $b \in \mathbb{Q}$ such that $p_3(b, x) = x^3 + bx + b$ by computing this $b \in \mathbb{Q}$ directly. However, as indicated in the proof of Theorem 3.5, we can do the similar thing for the parametric cyclic cubic $p_3(t, x) = x^3 - tx^2 + (t - 3)x + 1$ as long as we have an algorithm that can compute the normal basis $\{\alpha, \sigma(\alpha), \sigma^2(\alpha)\}$ of a given C_3 -extension over L/\mathbb{Q} .

For some simpler cases, we can try to do this without computing the normal basis.

Suppose $f(x)$ is a cyclic cubic with integer coefficients. Since $f(x)$ in $\mathbb{Z}[x]$ has Galois group isomorphic to C_3 , then its discriminant d_f is a square in \mathbb{Z} . So the simplest case is when $d_f = p^2$, where p is a prime number. Suppose $f(x)$ has splitting field L with field discriminant d_L . Since d_f is always a square multiple of the field discriminant d_L , and d_L cannot be 1 (see reference [6]), then it has to be true that $d_f = d_L = p^2$. We know from the proof of Theorem 3.5 that if for some $b \in \mathbb{Q}$, the specialized polynomial $p_3(b, x)$ in $\mathbb{Q}[x]$ has splitting field L , then its discriminant $d_{p_3}(b) = (b^2 - 3b + 9)^2$. We can try to solve the equation $(b^2 - 3b + 9)^2 = p^2$ for b to see whether it has rational solutions. If $b^2 - 3b + 9 = -p$, then there is no real solution, because $9 - 4 \cdot (9 + p) < 0$. We only need to consider when $b^2 - 3b + 9 = p$, which is when $b = \frac{1}{2}(3 \pm \sqrt{4p - 27})$. Notice $\frac{1}{2}(3 + \sqrt{4p - 27}) + \frac{1}{2}(3 - \sqrt{4p - 27}) = 3$. So by Theorem 3.8, these two b 's parametrize the same splitting field. We can work with only one of them.

As we can see, if $4p - 27$ is a square, then we can try and see whether $p(b, x)$ with $b = \frac{1}{2}(3 + \sqrt{4p - 27})$ has the same splitting field L as $f(x)$. Since we need $p > \frac{27}{4}$ to have $4p - 27$ be a square, we can try this method for odd primes greater than 5. Note that for a prime number p , $4p - 27$ is a square in \mathbb{Z} implies some

congruence conditions:

$$\begin{aligned}
4p - 27 = k^2 &\implies k^2 \equiv -27 \pmod{p} \\
&\implies -3 \text{ is a square modulo } p \\
&\implies p \equiv 1 \pmod{3}.
\end{aligned}$$

Also, if $4p - 27$ is a square, it must be an odd square, and $b = \frac{1}{2}(3 + \sqrt{4p - 27})$ must be an integer. This implies that our method only helps us find integer parameters.

Table 5: Examples of cyclic cubics with b 's found by this method

$f(x)$	$d_f = p^2$	$4p - 27$	b	$p_3(b, x)$
$x^3 - x^2 - 2x + 1$	7^2	1	2	$x^3 - 2x^2 - x + 1$
$x^3 - x^2 - 4x - 1$	13^2	$25 = 5^2$	4	$x^3 - 4x^2 + x + 1$
$x^3 - x^2 - 6x + 7$	19^2	$49 = 7^2$	5	$x^3 - 5x^2 + 2x + 1$
$x^3 - x^2 - 12x - 11$	37^2	$121 = 11^2$	7	$x^3 - 7x^2 + 4x + 1$
$x^3 - x^2 - 26x - 41$	79^2	$289 = 17^2$	10	$x^3 - 10x^2 + 7x + 1$

Because there can be non-isomorphic number fields that are C_3 extensions with same field discriminant, we cannot generalize the following method as an algorithm of finding a specialized polynomial $p_3(b, x)$ for some C_3 -extension with field discriminant p^2 , but we can always try and find out whether the method works.

Since not every prime number p has the property that $4p - 27$ is a square, this method does not find an integer b when $d_L = p^2$ for such p . For example, $x^3 - x^2 - 10x + 8$ has discriminant 31^2 , and $4 \cdot 31 - 27 = 97$. For such a field extension, no integer value of b works. In fact, taking $t = \frac{1}{2}, p\left(\frac{1}{2}, x\right)$ has the same splitting field as $x^3 - x^2 - 10x + 8$, and the discriminant of $p\left(\frac{1}{2}, x\right)$ is $d_{p_3}\left(\frac{1}{2}\right) = \left(\frac{31}{4}\right)^2$, which is a square multiple of 31^2 over \mathbb{Q} . However, we know of no algorithm to find $t = \frac{1}{2}$ from the given polynomial. Indeed, we constructed this example by taking $t = \frac{1}{2}$ and then find an integer polynomial with the same splitting field.

4 Quartic Polynomials

Again, recall that for an irreducible polynomial $f(x)$ of degree n , the Galois group is isomorphic to a subgroup of S_n and acts transitively on the roots of $f(x)$. So for an irreducible quartic polynomial $f(x)$, its Galois group is isomorphic to a transitive subgroup of S_4 . Unlike the cubic case, where S_3 only has 2 transitive subgroups, S_4 has 5 transitive subgroups: C_4, D_4, V_4, A_4, S_4 . Before we start finding parametric polynomials for those subgroups, we first think about when given an irreducible quartic polynomial, how we decide which subgroup of S_4 its Galois group is isomorphic to.

Let $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ be a monic irreducible quartic polynomial over \mathbb{Q} with splitting field M and Galois group G . We know that G must be isomorphic to one of C_4, D_4, V_4, A_4, S_4 . Since we have learned a lot about cubic polynomials, we can make a related cubic polynomial to help us find out which one of the 5 subgroups G is isomorphic to. We call this helping cubic polynomial **the cubic resolvent** for $f(x)$, and it is defined as the following:

Definition 4.1. (Cubic Resolvent)

Let $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ be the roots of $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. The cubic resolvent for $f(x)$ is the cubic polynomial $g(y)$, where

$$\begin{aligned} g(y) &= \left(y - (\gamma_1\gamma_2 + \gamma_3\gamma_4)\right) \left(y - (\gamma_1\gamma_3 + \gamma_2\gamma_4)\right) \left(y - (\gamma_1\gamma_4 + \gamma_2\gamma_3)\right) \\ &= y^3 - a_2y^2 + (a_1a_3 - 4a_0)y - (a_0a_3^2 - 4a_0a_2 + a_1^2). \end{aligned}$$

Notice that $g(y)$ is always a polynomial in $\mathbb{Q}[x]$, and that its splitting field is contained in the splitting field of $f(x)$. Here are some examples.

Table 6: Examples of cubic resolvents

Polynomial $f(x)$	Cubic Resolvent $g(y)$	Irreducibility of $g(y)$	Gal
$x^4 - x^3 - x^2 + x + 1$	$y^3 + y^2 - 5y - 6$	$g(y) = (y + 2)(y^2 - y - 3)$	D_4
$x^4 - x^3 + x^2 - x + 1$	$y^3 - y^2 - 3y + 2$	$g(y) = (y - 2)(y^2 + y - 1)$	C_4
$x^4 - x^2 + 1$	$y^3 + y^2 - 4y - 4$	$g(y) = (y + 1)(y - 2)(y + 2)$	V_4
$x^4 - 2x^3 + 2x^2 + 2$	$y^3 - 2y^2 - 8y + 8$	irreducible	A_4
$x^4 - x + 1$	$y^3 - 4y - 1$	irreducible	S_4

As we can see from the table, $g(y)$ can be reducible. It turns out that we can use $g(y)$ to get information about f .

For our irreducible quartic polynomial $f(x)$, the cubic resolvent $g(y)$ has discriminant

$$\begin{aligned}\Delta(g) &= \left((\gamma_1\gamma_2 + \gamma_3\gamma_4) - (\gamma_1\gamma_3 + \gamma_2\gamma_4) \right)^2 \left((\gamma_1\gamma_2 + \gamma_3\gamma_4) - (\gamma_1\gamma_4 + \gamma_2\gamma_3) \right)^2 \\ &\quad \left((\gamma_1\gamma_3 + \gamma_2\gamma_4) - (\gamma_1\gamma_4 + \gamma_2\gamma_3) \right)^2 \\ &= \left((\gamma_1 - \gamma_4)(\gamma_2 - \gamma_3) \right)^2 \left((\gamma_1 - \gamma_3)(\gamma_2 - \gamma_4) \right)^2 \left((\gamma_1 - \gamma_2)(\gamma_3 - \gamma_4) \right)^2 \\ &= (\gamma_1 - \gamma_4)^2 (\gamma_2 - \gamma_3)^2 (\gamma_1 - \gamma_3)^2 (\gamma_2 - \gamma_4)^2 (\gamma_1 - \gamma_2)^2 (\gamma_3 - \gamma_4)^2 \\ &= \Delta(f).\end{aligned}$$

From Theorem 3.3, we know that the discriminant of an irreducible polynomial tells us whether the polynomial has Galois group isomorphic to a subgroup of the alternating group. Since $f(x)$ has the same discriminant as its cubic resolvent $g(y)$, we can work with $g(y)$ since we have learned a lot about cubic polynomials and their splitting fields.

Again, let $f(x)$ be an irreducible quartic polynomial over \mathbb{Q} with splitting field M and Galois group G . Let $g(y)$ in \mathbb{Q} be the cubic resolvent for $f(x)$, L be the splitting field of $g(y)$ over \mathbb{Q} , and let $m = [L : \mathbb{Q}] = |\text{Gal}(L/\mathbb{Q})|$. Notice $\text{Gal}(L/\mathbb{Q})$ has to be isomorphic to a subgroup of S_3 . So $m = 1, 2, 3$, or 6 . In particular, $m = 3$ or 6 if $g(y)$ is irreducible; $m = 2$ if $g(y)$ has a unique rational root; $m = 1$ if $g(y)$ splits over \mathbb{Q} .

Since M is a Galois G -extension, then $[M : \mathbb{Q}] = |\text{Gal}(M/\mathbb{Q})| = |G|$. Clearly, L is a subfield of M . So by Tower Law, $[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}]$. This gives us that m divides $|G|$.

We claim that with one exception, the number m tells us which subgroup of S_4 G is isomorphic to.

Proposition 4.2.

$$G \cong \begin{cases} S_4 & \text{if } m = 6, \\ A_4 & \text{if } m = 3, \\ D_4 \text{ or } C_4 & \text{if } m = 2, \\ V_4 & \text{if } m = 1. \end{cases}$$

Proof.

First we apply Theorem 3.3 here. by looking at the discriminant $\Delta(f)$ of the given quartic polynomial f , we get:

(1). If the discriminant $\Delta(f)$ of f is a square in \mathbb{Q} , then its Galois group G is isomorphic to a subgroup of A_4 . i.e. $G \cong V_4$ or A_4 .

(2). If the discriminant $\Delta(f)$ of f is not a square in \mathbb{Q} , then its Galois group G is not isomorphic to a subgroup of A_4 . i.e. $G \cong C_4, D_4$ or S_4 .

Case 1: $m = 6$.

Then $\text{Gal}(L/\mathbb{Q}) \cong S_3$, and $g(y)$ is irreducible. So the discriminant $\Delta(g) = \Delta(f)$ is not a square in \mathbb{Q} . By (2), G is isomorphic to C_4, D_4 or S_4 . Since we have shown that m divides $|G|$, and among those subgroups only $|S_4| = 24$ is divisible by $m = 6$, then G has to be isomorphic to S_4 .

Case 2: $m = 3$.

Then $\text{Gal}(L/\mathbb{Q}) \cong C_3$, and $g(y)$ is irreducible again. The discriminant $\Delta(g) = \Delta(f)$ has to be a square in \mathbb{Q} . By (1), G is isomorphic to V_4 or A_4 . Since only $|A_4| = 12$ is divisible by $m = 3$, then G has to be isomorphic to A_4 .

Case 3: $m = 2$.

Then $g(y)$ is reducible, and among the three roots $\gamma_1\gamma_2 + \gamma_3\gamma_4$, $\gamma_1\gamma_3 + \gamma_2\gamma_4$, $\gamma_1\gamma_4 + \gamma_2\gamma_3$ of $g(y)$, there is one rational root and two irrational roots. Without loss of generality, assume $\gamma_1\gamma_2 + \gamma_3\gamma_4 \in \mathbb{Q}$, and $\gamma_1\gamma_3 + \gamma_2\gamma_4$, $\gamma_1\gamma_4 + \gamma_2\gamma_3$ are not in \mathbb{Q} . Then $\gamma_1\gamma_3 + \gamma_2\gamma_4$, $\gamma_1\gamma_4 + \gamma_2\gamma_3$ must be complex conjugates. Hence, there exists $\varphi \in G$ such that

$$\varphi(\gamma_1\gamma_2 + \gamma_3\gamma_4) = \gamma_1\gamma_2 + \gamma_3\gamma_4,$$

$$\varphi(\gamma_1\gamma_3 + \gamma_2\gamma_4) = \gamma_1\gamma_4 + \gamma_2\gamma_3,$$

$$\varphi(\gamma_1\gamma_4 + \gamma_2\gamma_3) = \gamma_1\gamma_3 + \gamma_2\gamma_4.$$

Since φ has to permute the four roots $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ of $f(x)$, and φ cannot fix any of the γ_i , it has to be the power of the automorphism of the splitting field M of $f(x)$

identified with

$$\begin{array}{l} \gamma_1 \mapsto \gamma_3 \quad , \quad \gamma_3 \mapsto \gamma_2 \\ \gamma_2 \mapsto \gamma_4 \quad , \quad \gamma_4 \mapsto \gamma_1. \end{array}$$

Clearly, ϕ is a 4-cycle. So G must contain a 4-cycle, and thus $G \cong C_4$ or D_4 .

Case 4: $m = 1$.

Then all three roots of $g(y)$ are rational. So G consists of permutations of the four roots $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ of $f(x)$ that fix $\gamma_1\gamma_2 + \gamma_3\gamma_4$, $\gamma_1\gamma_3 + \gamma_2\gamma_4$, $\gamma_1\gamma_4 + \gamma_2\gamma_3$. Since the elements of G cannot fix any γ_i , they must be the permutations that swapping the two pairs of roots $\gamma_1, \gamma_2, \gamma_3, \gamma_4$. Each of such swapping has order 2. So $G \cong V_4$. \square

Since when $\text{Gal}(L/\mathbb{Q}) \cong C_3$ or S_3 are exactly the cases that g is irreducible. We can also translate Proposition 4.2 into this:

Suppose $f(x)$ is a monic irreducible quartic polynomial with cubic resolvent $g(y)$ and Galois group G ,

- (1) If $g(y)$ is irreducible, and $\Delta(g) = \Delta(f)$ is a square in \mathbb{Q} , then $G \cong A_4$;
- (2) If $g(y)$ is irreducible, and $\Delta(g) = \Delta(f)$ is not a square in \mathbb{Q} , then $G \cong S_4$;
- (3) If $g(y)$ is reducible, and $\Delta(g) = \Delta(f)$ is a square in \mathbb{Q} , then $G \cong V_4$;
- (4) If $g(y)$ is reducible, and $\Delta(g) = \Delta(f)$ is not a square in \mathbb{Q} , then $G \cong C_4$ or D_4 .

Let us work out the 5 examples displayed in Table 6 with their discriminants. The discriminants of $x^4 - x^3 - x^2 + x + 1$, $x^4 - x^3 + x^2 - x + 1$, $x^4 - x + 1$ are not squares in \mathbb{Q} . Among them, $x^4 - x^3 - x^2 + x + 1$ and $x^4 - x^3 + x^2 - x + 1$ have reducible cubic resolvents, so their Galois groups are isomorphic to D_4 or C_4 . It remains to separate the two cases of C_4 and D_4 . $x^4 - x + 1$ has irreducible cubic resolvents, so its Galois group is isomorphic to S_4 . The discriminants of $x^4 - x^2 + 1$ and $x^4 - 2x^3 + 2x^2 + 2$ are squares in \mathbb{Q} . The cubic resolvent of $x^4 - x^2 + 1$ splits in \mathbb{Q} , so its Galois group is isomorphic to V_4 ; the cubic resolvent of $x^4 - 2x^3 + 2x^2 + 2$ is irreducible, so its Galois group is isomorphic to A_4 .

Table 7: Examples of cubic resolvents

$f(x)$	$g(y)$	Factorization of $g(y)$	$\Delta(g) = \Delta(f)$	Gal
$x^4 - x^3 - x^2 + x + 1$	$y^3 + y^2 - 5y - 6$	$(y+2)(y^2 - y - 3)$	117	D_4
$x^4 - x^3 + x^2 - x + 1$	$y^3 - y^2 - 3y + 2$	$(y-2)(y^2 + y - 1)$	125	C_4
$x^4 - x^2 + 1$	$y^3 + y^2 - 4y - 4$	$(y+1)(y-2)(y+2)$	$144 = 12^2$	V_4
$x^4 - 2x^3 + 2x^2 + 2$	$y^3 - 2y^2 - 8y + 8$	irreducible	$3136 = 56^2$	A_4
$x^4 - x + 1$	$y^3 - 4y - 1$	irreducible	229	S_4

From Proposition 4.2 and its proof, we know that when $m = 2$, or equivalently, g is reducible and $\Delta(g) = \Delta(f)$ is not a square in \mathbb{Q} , g can be factored as $g(y) = (y-r)(y^2 + sy + t)$ with $r, s, t \in \mathbb{Q}$ and $y^2 + sy + t$ irreducible over \mathbb{Q} , but we cannot distinguish whether the Galois group of f is isomorphic to C_4 or D_4 . Therefore, to decide the Galois group in the $m = 2$ case, we need an additional criterion.

Proposition 4.3. Suppose $m = 2$, and $g(y) = (y-r)(y^2 + sy + t)$ with $r, s, t \in \mathbb{Q}$ and $y^2 + sy + t$ irreducible over \mathbb{Q} . Then G is isomorphic to C_4 if and only if $x^2 - rx + a_0$ and $x^2 + a_3x + (a_2 - r)$ both have roots in L , the splitting field of g .

Proof.

Since $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ are the roots of $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, then

$$\begin{aligned} a_0 &= \gamma_1 \gamma_2 \gamma_3 \gamma_4, \\ a_2 &= \gamma_1 \gamma_2 + \gamma_1 \gamma_3 + \gamma_1 \gamma_4 + \gamma_2 \gamma_3 + \gamma_2 \gamma_4 + \gamma_3 \gamma_4 \\ a_3 &= \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 \end{aligned}$$

One direction is easy: If $G \cong C_4$, then L is the unique subfield of M with degree 2. So the roots of these two quadratic polynomials must belong to L .

Now we need to show the converse. Suppose the two quadratic polynomials $x^2 - rx + a_0$ and $x^2 + a_3x + (a_2 - r)$ both have roots in L .

Recall that $g(y) = (y - (\gamma_1 \gamma_2 + \gamma_3 \gamma_4))(y - (\gamma_1 \gamma_3 + \gamma_2 \gamma_4))(y - (\gamma_1 \gamma_4 + \gamma_2 \gamma_3))$.

Without loss of generality, assume $\gamma_1 \gamma_2 + \gamma_3 \gamma_4 = r \in \mathbb{Q}$, so that $\gamma_1 \gamma_3 + \gamma_2 \gamma_4$ and $\gamma_1 \gamma_4 + \gamma_2 \gamma_3$ are the two irrational roots of $y^2 + sy + t$.

Then $x^2 - rx + a_0 = x^2 - (\gamma_1 \gamma_2 + \gamma_3 \gamma_4)x + \gamma_1 \gamma_2 \gamma_3 \gamma_4 = (x - \gamma_1 \gamma_2)(x - \gamma_3 \gamma_4)$, and

$$x^2 + a_3x + (a_2 - r) = x^2 + (\gamma_1 + \gamma_2 + \gamma_3 + \gamma_4)x + (\gamma_1\gamma_3 + \gamma_1\gamma_4 + \gamma_2\gamma_3 + \gamma_2\gamma_4) = \left(x - (\gamma_1 + \gamma_2) \right) \left(x - (\gamma_3 + \gamma_4) \right).$$

By our assumption, $\gamma_1\gamma_2, \gamma_3\gamma_4, \gamma_1 + \gamma_2, \gamma_3 + \gamma_4 \in L$.

Since $\gamma_1 + \gamma_2 \in L, \gamma_1\gamma_2 \in L$, then $(\gamma_1 - \gamma_2)^2 = (\gamma_1 + \gamma_2)^2 - 4\gamma_1\gamma_2 \in L$, which implies $[L(\gamma_1 - \gamma_2) : L] \leq 2$.

Notice $\gamma_1 = \frac{(\gamma_1 + \gamma_2) + (\gamma_1 - \gamma_2)}{2} \in L(\gamma_1 - \gamma_2)$, and $\gamma_2 = \frac{(\gamma_1 + \gamma_2) - (\gamma_1 - \gamma_2)}{2} \in L(\gamma_1 - \gamma_2)$. So $L(\gamma_1, \gamma_2) = L(\gamma_1 - \gamma_2)$.

Also, since $\gamma_1\gamma_3 + \gamma_2\gamma_4, \gamma_1\gamma_4 + \gamma_2\gamma_3$ are two roots of g , then they are in L , and $(\gamma_1\gamma_3 + \gamma_2\gamma_4) - (\gamma_1\gamma_4 + \gamma_2\gamma_3) = (\gamma_1 - \gamma_2)(\gamma_3 - \gamma_4) \in L$. So $\gamma_3 - \gamma_4 \in L(\gamma_1, \gamma_2)$.

The fact both $\gamma_3 + \gamma_4$ and $\gamma_3 - \gamma_4$ are in $L(\gamma_1, \gamma_2)$ gives us that $\gamma_3, \gamma_4 \in L(\gamma_1, \gamma_2)$. Hence, M , the splitting field of our quartic polynomial $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, is equal to $L(\gamma_1, \gamma_2, \gamma_3, \gamma_4) = L(\gamma_1, \gamma_2) = L(\gamma_1 - \gamma_2)$.

So we see, $[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}] = [L(\gamma_1 - \gamma_2) : L] \cdot m \leq 2 \cdot 2 = 4$. Therefore, G has to be isomorphic to C_4 . \square

From Proposition 4.3, we can derive a new proposition as follows:

Proposition 4.4. Suppose $f(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ is irreducible over \mathbb{Q} , and has Galois group G .

- (1) If b is a square in \mathbb{Q} , then $G \cong V_4$.
- (2) If b is not a square in \mathbb{Q} , but $b(a^2 - 4b)$ is a square in \mathbb{Q} , then $G \cong C_4$.
- (3) If neither b or $b(a^2 - 4b)$ is a square in \mathbb{Q} , then $G \cong D_4$.

Proof.

By definition, $g(y) = y^3 - ay^2 - 4by + 4ab = (y - a)(y^2 - 4b)$. Since it is reducible, by Lemma 4.2, $G \cong V_4, C_4$ or D_4 .

If b is a square in \mathbb{Q} , then $g(y) = (y - a)(y - 2\sqrt{b})(y + 2\sqrt{b})$ splits in \mathbb{Q} . This shows $G \cong V_4$.

Suppose b is not a square in \mathbb{Q} . Then the splitting field of g has degree 2 over \mathbb{Q} , and the splitting field L of g is equal to $\mathbb{Q}(\sqrt{b})$. According to Lemma 4.3, we need to consider the polynomials $x^2 - ax + b$ and x^2 . It is trivial that x^2 has roots

in L . We only need to check whether the roots of $x^2 - ax + b$ are in L . Note that $\frac{a + \sqrt{a^2 - 4b}}{2}$ and $\frac{a - \sqrt{a^2 - 4b}}{2}$ are in L if and only if $\sqrt{a^2 - 4b} \in L = \mathbb{Q}(\sqrt{b})$. If $b(a^2 - 4b)$ is a square in \mathbb{Q} , then $\sqrt{b(a^2 - 4b)} \in \mathbb{Q}$ implies $\sqrt{a^2 - 4b} \in \mathbb{Q}(\sqrt{b}) = L$. So in this case, roots of $x^2 - ax + b$ splits in L , and $G \cong C_4$. Hence, the only case left when $b(a^2 - 4b)$ is not a square in \mathbb{Q} , and G has to isomorphic to D_4 . \square

Table 8: Examples of irreducible $x^4 + ax^2 + b$

$f(x) = x^4 + ax^2 + b$	b	$b(a^2 - 4b)$	Gal
$x^4 + 1$	$1 = 1^2$	doesn't matter	V_4
$x^4 - 3x^2 + 4$	$4 = 2^2$	doesn't matter	V_4
$x^4 + 5x + 5$	5	$25 = 5^2$	C_4
$x^4 - 20x^2 + 50$	50	$10000 = 100^2$	C_4
$x^4 - 2x^2 + 2$	2	-8	D_4
$x^4 + 5x^2 + 7$	7	-21	D_4

Lemma 4.5.

Suppose L/\mathbb{Q} is a G -extension, where $G \cong V_4, C_4$, or D_4 . Then L is the splitting field of a biquadratic polynomial. i.e. there exists some $a, b \in \mathbb{Q}$ such that $x^4 + ax^2 + b$ has splitting field L .

Proof.

Notice all C_4, V_4, D_4 are solvable, because $\mathbb{1} \triangleright C_2 \triangleright C_4$, $\mathbb{1} \triangleright C_2 \triangleright V_4$, $\mathbb{1} \triangleright V_4 \triangleright D_4$. Also since $|C_4 : C_2| = |V_4 : C_2| = |D_4 : V_4| = 2$, when L/\mathbb{Q} is a C_4 - or V_4 - or D_4 -extension, there exists intermediate field K such that $[K : \mathbb{Q}] = 2$. In other words, K/\mathbb{Q} is a quadratic extension over \mathbb{Q} . We can assume $K = \mathbb{Q}(\sqrt{\alpha})$ with $\alpha \in \mathbb{Q}$. If L/\mathbb{Q} is a C_4 - or V_4 -extension, then $[L : K] = |C_2| = 2$ and L/K is a quadratic extension. We let $L = K(\sqrt{\beta})$ for $\beta \in K = \mathbb{Q}(\sqrt{\alpha})$. Then $\sqrt{\beta} = \sqrt{a + b\sqrt{\alpha}}$, which is a root of the biquadratic polynomial $x^4 - 2ax^2 + a^2 - b^2\alpha$. If L/\mathbb{Q} is a D_4 -extension, then $\text{Gal}(L/K) \cong V_4$, and so there exists $\beta \in K$ but not a square in K such that $\sqrt{\beta} \in L$. By the same argument, the minimal polynomial of $\sqrt{\beta}$ is a quartic polynomial and has splitting field L . \square

Combining Proposition 4.4 and Lemma 4.5, we conclude that a G -extension of \mathbb{Q} can be parametrized by a biquadratic polynomial $x^4 + ux^2 + v$ in $\mathbb{Q}(u, v)[x]$ if and only if $G \cong C_4, D_4$ or V_4 . If $f(x)$ in $\mathbb{Q}[x]$ with splitting field L has Galois group S_4 or A_4 over \mathbb{Q} , then the degree 4 extension obtained by adjoining a root of $f(x)$ does not contain a quartic subfield.

Theorem 4.6.

$p_5(s, t, x) = (x^2 - s)(x^2 - t)$ is a parametric polynomial for V_4 -extensions of \mathbb{Q} .

Proof.

This should be easy to see. First notice $p_5(s, t, x)$ clearly has Galois group V_4 over $\mathbb{Q}(s, t)[x]$, because every element of the Galois group has to have order 2. Now let L/\mathbb{Q} be a V_4 -extension. Then L/\mathbb{Q} has three distinct quadratic intermediate fields E_1, E_2, E_3 . Since E_1, E_2 are quadratic over \mathbb{Q} , we can assume $E_1 = \mathbb{Q}(\sqrt{a})$, and $E_2 = \mathbb{Q}(\sqrt{b})$, where a, b are not squares in \mathbb{Q} . So ab must not be a square in \mathbb{Q} , and $E_3 = \mathbb{Q}\sqrt{ab}$. Therefore, the polynomial $(x - a^2)(x - b^2)$ has splitting field L . \square

Notice $p_5(s, t, x) = (x^2 - s)(x^2 - t)$ in $\mathbb{Q}(s, t)[x]$ is a biquadratic polynomial, but it is not irreducible. The following is an irreducible biquadratic parametric polynomial for V_4 :

Theorem 4.7.

$p_6(u, v, x) = x^4 + ux^2 + v^2$ is a parametric polynomial for V_4 -extension of \mathbb{Q} .

Proof.

Since u^2 is a square in $\mathbb{Q}(u, v)$, then according to Proposition 4.4, the splitting field of $p(u, v, x)$ over $\mathbb{Q}(u, v)$ is a V_4 -extension. Since we showed that every V_4 -extension is the splitting field of a biquadratic polynomial, and that biquadratic polynomial must have the constant term a square in \mathbb{Q} , we can conclude that $p_6(u, v, x)$ is a parametric polynomial for V_4 -extensions of \mathbb{Q} . \square

Similarly, using Proposition 4.4 and Lemma 4.5, we can write the parametric polynomials for C_4 - and D_4 -extensions of \mathbb{Q} :

Theorem 4.8.

$p_7(u, v, x) = x^4 + ux^2 + \frac{u^2}{v^2 + 4}$ is a parametric polynomial for C_4 over \mathbb{Q} .

$p_8(u, v, x) = x^4 + ux^2 + v$ is a parametric polynomial for D_4 over \mathbb{Q} .

For any irreducible quartic polynomial $f(x)$, we can go through the same process as in Lemma 3.1 and find $(a, b) \in \mathbb{Q}^2$ such that $x^4 + ax^2 + bx + b$ has the same splitting field as $f(x)$. And we can prove $p(s, t, x) = x^4 + sx^2 + tx + t$ in $\mathbb{Q}(s, t)[x]$ is a parametric polynomial for S_4 -extensions of \mathbb{Q} by showing the discriminant $d(s, t) = 256t^3 - 128s^2t^2 + 144st^3 - 17t^4 + 16s^4t - 4s^3t^2$ is not a square in $\mathbb{Q}(s, t)$.

Theorem 4.9.

$p_9(s, t, x) = x^4 + sx^2 + tx + t$ in $\mathbb{Q}(s, t)[x]$ is a parametric polynomial for S_4 -extensions of \mathbb{Q} .

The only subgroup of S_4 left is A_4 , which is the most sophisticated case. The following is a parametric polynomial for A_4 -extensions of \mathbb{Q} from reference [1], but we will not include a proof.

Theorem 4.10.

$p_{10}(\alpha, \beta, x) = x^4 - \frac{6A}{B}x^2 - 8x + \frac{9A^2 - 12(\alpha^3 - \beta^3 + 27)B}{B^2}$ in $\mathbb{Q}(\alpha, \beta)[x]$, where

$$A = \alpha^3 - \beta^3 - 9\beta^2 - 27\beta - 54,$$

$$B = \alpha^3 - 3\alpha\beta^3 - 9\alpha\beta + 9\beta^2 - 27\alpha + 27\beta + 27,$$

is a parametric polynomial for A_4 -extensions of \mathbb{Q} .

According to reference [1], all groups of degree ≤ 15 has been proved to be the Galois group of field extensions over \mathbb{Q} . Also, reference [1] gives specific results of **generic polynomials** for degree 3, 4, 5, 7 and 11 over a field K with characteristic $\neq 2$. For a parametric polynomial $p(\vec{t}, x)$ in $K(\vec{t}, x)$ to be generic for some G -extension, it requires the following additional condition besides the conditions A1, A2 in Definition 2.2

A3. $p(\vec{t}, x)$ is parametric for G -extensions over any field containing K .

In fact, all the parametric polynomials we discussed in this paper are also generic. Although much more complicated, the method used to construct the generic polynomials of degree 5, 7, 11 is similar to what we did for quartic polynomials. It uses resolvent polynomials over \mathbb{Q} to reduce the case to smaller degree. The constructive aspects of the Inverse Galois Problem have made some progress, and the work still needs to be continued.

5 Appendix

When L/\mathbb{Q} is a C_3 -extension with Galois group $G = \langle \sigma \rangle \cong C_3$, why can we always find linearly independent $x, y \in L$ such that $\sigma(x) = -y$ and $\sigma(y) = x - y$?

Consider the representation $G \rightarrow GL_2(\mathbb{Q})$ where

$$\sigma \mapsto \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \text{ and } \sigma^2 \mapsto \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Let $V = \mathbb{Q} \times \mathbb{Q}$, then

$$\text{for all } \begin{pmatrix} a \\ b \end{pmatrix} \in V = \mathbb{Q} \times \mathbb{Q}: \sigma \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -b \\ a-b \end{pmatrix}, \text{ and } \sigma^2 \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -a+b \\ a \end{pmatrix}.$$

We want to show there exist two linearly independent elements x, y in L such that $\sigma(x) = -y$, and $\sigma(y) = x - y$.

We start by looking at the dual space V^* of V , which is the set of all linear and continuous maps from $V = \mathbb{Q} \times \mathbb{Q}$ to \mathbb{Q} . It is a $\mathbb{Q}[G]$ -module by the action $\sigma(\varphi) : \mathbf{v} \mapsto \varphi(\sigma^{-1}\mathbf{v})$. We'll show it is a cyclic $\mathbb{Q}[G]$ -module.

Clearly, V^* is generated by the two projection functions $\varepsilon_1, \varepsilon_2$, where

$$\varepsilon_1 : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto a, \text{ and } \varepsilon_2 : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto b.$$

So to show V^* is a cyclic $\mathbb{Q}[G]$ -module, it is sufficient to show that ε_2 can be written as a linear combination of $\varepsilon_1, \sigma(\varepsilon_1), \sigma^2(\varepsilon_1)$.

For all $\mathbf{v} = \begin{pmatrix} a \\ b \end{pmatrix} \in V$:

$$(\sigma(\varepsilon_1))(\mathbf{v}) = \varepsilon_1 \left(\sigma^{-1} \begin{pmatrix} a \\ b \end{pmatrix} \right) = \varepsilon_1 \left(\begin{pmatrix} -a+b \\ a \end{pmatrix} \right) = -a+b = -\varepsilon_1(\mathbf{v}) + \varepsilon_2(\mathbf{v}).$$

Hence, $\sigma(\varepsilon_1) = -\varepsilon_1 + \varepsilon_2$, which implies that V^* is cyclic generated by ε_1 over $\mathbb{Q}[G]$.

By Normal Basis Theorem, there exists α in L such that $\{\alpha, \sigma(\alpha), \sigma^2(\alpha)\}$ spans L .

Now we claim the map

$$\rho : \mathbf{v} \mapsto \sum_{g \in G = \langle \sigma \rangle} \varepsilon_1(g^{-1} \mathbf{v}) g(\alpha) \text{ is an injective homomorphism from } V \text{ to } L.$$

For all $\mathbf{v} = \begin{pmatrix} a \\ b \end{pmatrix} \in V$:

$$\begin{aligned} \rho \left(\begin{pmatrix} a \\ b \end{pmatrix} \right) &= \varepsilon_1 \left(\text{Id} \begin{pmatrix} a \\ b \end{pmatrix} \right) \text{Id}(\alpha) + \varepsilon_1 \left(\sigma^{-1} \begin{pmatrix} a \\ b \end{pmatrix} \right) \sigma(\alpha) + \varepsilon_1 \left(\sigma \begin{pmatrix} a \\ b \end{pmatrix} \right) \sigma^2(\alpha) \\ &= \varepsilon_1 \left(\begin{pmatrix} a \\ b \end{pmatrix} \right) \text{Id}(\alpha) + \varepsilon_1 \left(\begin{pmatrix} -a+b \\ a \end{pmatrix} \right) \sigma(\alpha) + \varepsilon_1 \left(\begin{pmatrix} -b \\ a-b \end{pmatrix} \right) \sigma^2(\alpha) \\ &= a \cdot \alpha + (-a+b) \cdot \sigma(\alpha) - b \cdot \sigma^2(\alpha). \end{aligned}$$

Clearly, ρ is a homomorphism. And it has trivial kernel, because for each $\begin{pmatrix} a \\ b \end{pmatrix} \in \text{Ker}(\rho)$, it must be true that $a = 0, -a + b = 0, -b = 0$.

Hence, ρ is an injective homomorphism from V to L .

$$\text{Now let } x = \rho \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) = \alpha - \sigma(\alpha), y = \rho \left(\begin{pmatrix} 0 \\ -1 \end{pmatrix} \right) = -\sigma(\alpha) + \sigma^2(\alpha)$$

Since $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \end{pmatrix}$ are linearly independent over \mathbb{Q} , then x, y are also linearly independent over \mathbb{Q} .

Also,

$$\begin{aligned}\sigma(x) &= \sigma(\alpha - \sigma(\alpha)) \\ &= \sigma(\alpha) - \sigma^2(\alpha) \\ &= -y, \\ \sigma(y) &= \sigma(-\sigma(\alpha) + \sigma^2(\alpha)) \\ &= -\sigma^2(\alpha) + \alpha \\ &= -\sigma^2(\alpha) + \sigma(\alpha) + \alpha - \sigma(\alpha) \\ &= -(-\sigma(\alpha) + \sigma^2(\alpha)) + (\alpha - \sigma(\alpha)) \\ &= -y + x.\end{aligned}$$

References

- [1] Christian U. Jensen, Arne Ledet, Noriko Yui, *GGeneric Polynomials: Constructive Aspects of the Inverse Galois Problem*. Cambridge University Press, 2002.
- [2] Helmut Volklein, *Groups as Galois Groups*, Cambridge University Press, 1996.
- [3] Emil Artin, *Galois Theory*, University of Notre Dame Press, 1944.
- [4] <https://math.stackexchange.com/questions/922006/normal-basis-theorem-proof>
- [5] Daniel Shanks, *The Simplest Cubic Fields*, Mathematics of Computation, Volume 28, 1974
- [6] Henri Cohen, *A Course in Computational Algebraic Number Theory*. Springer, 2000.
- [7] Ian Stewart, *Galois Theory*. Chapman & Hall/CRC, 2004