An exploration of Galois Theory

RQ: Are all algebraic numbers expressible using radicals?

Mathematics
Word count: 3996

Contents

Chapter 1

Introduction

1.1 motivation

I was recently drawn into group theory when I stumbled upon a video about the monster group on youtube from my favorite channel, 3Blue1Brown. Being a high school student, I had minimal knowledge of anything beyond calculus, which was the underlying reason why that video left such a sharp impression on me. The concept of algebraic structures gave me a whole new perspective on various things, where I even started treating numbers differently.Prompted by my curiosity, I dug deeper, and while self-learning materials on group theory on the internet, I saw an intriguing question in an online lecture video, which later became my RQ:

Are all algebraic numbers expressible using radicals?

This became the goal of this essay, which is not only to provide a solution that felt intuitive, but give an explanation based from the way I interpreted the question. Behind the solution to the question lies a intriguing fact, that there exists no general formula to polynomials of fifth degree and higher. In the following chapters, I will give what I believe the most natural way of approaching the solution of the problem.

1.2 aim and approach

The first part of the essay will give a clarification of what radicals and algebraic numbers are, in order to break the question into manageable pieces.

Then, we will start with exploring fields, an algebraic structure that is crucial to understanding the relationship between polynomials and radicals.

Next, we will move to investigating the relationship between a field and another algebraic structure known as groups.

Lastly, we will use the relationship between fields and groups to answer our RQ.

Chapter 2

Radicals and Algebraic numbers

First of all, let us start by understanding algebraic numbers and radicals. Formally, Algebraic numbers are defined as the following:

Definition 2.0.1. *The set of Algebraic numbers A is the set of numbers such that for a in A, there exist a a non-zero polynomial with rational coefficients f(x), such that f(a) = 0*

A easier way to understand this is to think of it as the set of all roots of all possible polynomials. Numbers like 2, $3 + \sqrt{2}$, $2 + i$, $\sqrt[3]{1 + \sqrt[5]{2}}$ all belongs to this set.

Radicals on the other hand is created by the inverse operation of exponentiation. We can think of it as "undoing" exponents. When a number is expressible using radicals, we mean that the number can be written down using the radical symbol $\sqrt[n]{}$ and arithmetic operations. From here onward, we will refer to the set of numbers that are expressible using radicals as R.

Recall that our RQ was:

Are all algebraic numbers expressible using radicals?

With the definition of algebraic numbers and radicals, we rephrase our RQ into the following equivalent question:

Are the roots of all polynomials expressible using the standard arithmetic operations and continuous root extraction?

To contextualize these sets of numbers, let us compare them to numbers we are familiar with, such as rational numbers and complex numbers. First of all, we know that the rational numbers $\mathbb{Q}$ is contained in the algebraic numbers and the radicals.

$$\begin{tikzcd}
A \arrow[dr, dash] & & R \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Fig. 1

Furthermore, it is easy to see that both algebraic numbers and radicals are subset of the complex numbers. This is because complex numbers is an extension to the real numbers, and there exists reals such as π and e that aren't roots of any rational polynomials. Theses are known as transcendental numbers, in the sense they they are "beyond" arithmetic. Hence, the relationship looks like the following:

$$\begin{tikzcd}
& \mathbb{C} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
A \arrow[dr, dash] & \mathbb{R} \arrow[d, dash] & R \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Fig. 2

We know both A and R are somewhere in between the rationals and the complex, but we do not know their relationship with each other. Because algebraic numbers and radicals can be complex, they contain numbers outside of $\mathbb{R}$. On the other hand, some reals, like π, are outside of A and R.

The diagram above demonstrates the first possibility, that A and R are sets with some intersection, but not subsets of one another. However, there are a few other possibilities:

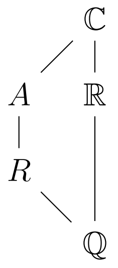


Fig. 3

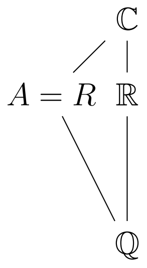


Fig. 4

Where in $Fig.3$, $R \subset A$ and in Figure 4, $R = A$. In the following chapters, we will try to figure out the exact relationship between A and R.

Chapter 3

Fields, field extension and symmetry

Before diving into the question, I would like to first bring up the concept of a field, because we will be discussing radicals and algebraic numbers as fields. Fields are complex algebraic structures that is satisfies a strict set of axioms:

Definition 3.0.1. *A field is a set S, together with functions* $+ : S + S \to S$ *and* $\times : S \times S \to S$*, called addition and multiplication, respectively, such that there are elements 0 and 1 in S with* $0 \neq 1$ *such that the following conditions [7] hold:*

- $(a + b) + c = a + (b + c)$ *for all* $a, b, c \in S$
- $a + b = b + a$ *for all* $a, b \in S$
- $(ab)c = a(bc)$ *for all* $a, b, c \in S$
- $ab = ba$ *for all* $a, b \in S$
- $a + 0 = 0 + a = a$ *for all* $a \in S$
- $a1 = 1a = a$ *for all* $a \in S$
- $a(b + c) = ab + ac$ *for all* $a, b, c \in S$
- $(a + b)c = ac + bc$ *for all* $a, b, c \in S$
- *for all* $a \in S$*, there exists a unique element* $-a \in S$ *such that* $a+(-a) = (-a)+a = 0$

- *for all $a \in S$ with $a \neq 0$, there exists a unique element $a^{-1} \in S$ such that $aa^{-1} = a^{-1}a = 1$*

At a glance, these may look trivial: the normal arithmetic, like adding and multiplying two numbers, satisfy all the criteria. This is because they originate from the way we deal with addition and multiplication, and extends the underlying pattern, the axioms, to operations beyond addition and multiplication and to sets beyond numbers.

For now, we don't need to worry about that, and can just treat fields as a set of numbers where normal addition and multiplication applies.

However, do note that any set of mathematical objects is a field if it has two mathematical operations acting on the elements of the set that satisfies the axioms. For example, all possible 2 by 2 matrices form a field, with matrix addition and multiplication as the operations.

The most crucial idea of treating sets of numbers like $\mathbb{Q}$ as a field is that a field has to be algebraically enclosed. This means that when applying addition and multiplication(and their inverses) on the elements, the result of the operations must also be an element of the field.

That is, when we have $s_1 \subset S$ and $s_2 \subset S$,

$$s_1 + s_2 \in S$$

$$s_1 \times s_2 \in S$$

For example, the set of integers do not form a field, because the numbers don't have multiplicative inverses, where for example,

$$3 \times x = 2 \implies x = \frac{2}{3} \implies x \notin \mathbb{Z}$$

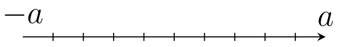
The motive of introducing fields is that, the notion of repeated utilization of arithmetic operation and root extraction is embedded in the concept of field extensions. To see why this is true, we now turn our attention to understanding what field extensions are.

Here, we first define what a field extension is:

Definition 3.0.2. *$F \subset F(\alpha)$ is a field extension of F, where $F(\alpha)$the smallest field that contains both the base field F and the extension element α. It is the field of $F \cup \{\alpha\}$.*

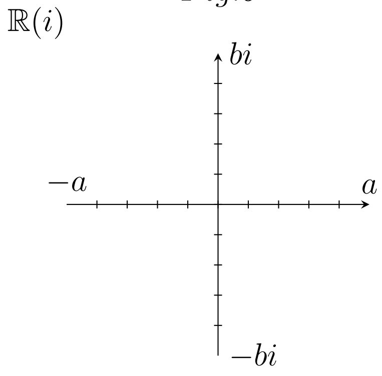
In other words, an extension field is a "larger" field that contains both the base field and extended element. Let's use the field of reals, $\mathbb{R}$, as an example. If we want to add additional elements to $\mathbb{R}$, such as $\sqrt{-1}$, we have make $\mathbb{R}$ larger by the means of a field extension. First, let us represent all elements of $\mathbb{R}$ using a number line:

$Fig.5$



Here, we simply cannot add i into the set of reals and call $\{\mathbb{R}\} + i$ the extension field. Remember that a field must be algebraically enclosed, meaning simply adding i itself will not suffice. The extension field $\mathbb{R}(i)$ needs to contain all of reals, which is $\mathbb{R}$, and all linear combinations of rational numbers and i. We can represent the field $\mathbb{R}(i)$ as the following

$Fig.6$



$$a \in \mathbb{R}$$
$$b \in \mathbb{R}$$

This is in fact the complex plane , which contains all elements of $\mathbb{R}(i)$. Another way of thinking about "the smallest field containing both the base field and the extended element" is to think of an algebraic expression that remains the same when under arithmetic operation with itself. $a + bi$ will always remain $a + bi$ when operated with itself. Therefore, all elements in the extended field $\mathbb{Q}(i)$ will take the form of $a + bi$.

Let's take a look at another example. For the field of $\mathbb{Q}(\sqrt[5]{5})$, by intuition, the smallest field containing $\mathbb{Q}$ and $\sqrt[5]{5}$ should contain all powers of $\sqrt[5]{5}$, where it exist the form of

$$a_1 + a_2\sqrt[5]{5} + a_3(\sqrt[5]{5})^2 + a_4(\sqrt[5]{5})^3 + a_5(\sqrt[5]{5})^4 \tag{3.1}$$

To show why this must be true, let's assume that $\mathbb{Q}(\sqrt[5]{5})$ is a field that only excludes $a_m\sqrt[5]{5}^m$, where $a_m\sqrt[5]{5}^m \notin \mathbb{Q}(\sqrt[5]{5})$, and m is an integer between 0 and 4. Then, we have

$$a_{m-k}\sqrt[5]{5}^{m-k} \cdot a_{m+k}\sqrt[5]{5}^{m+k} = a_m\sqrt[5]{5}^m$$

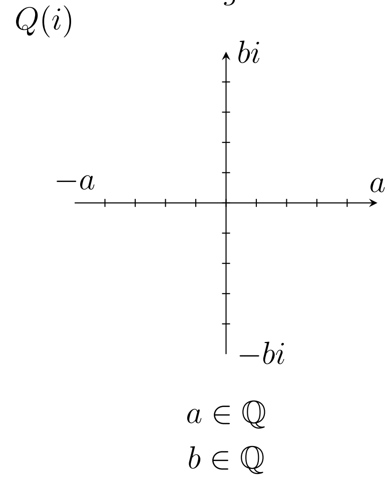
Where the products of two elements that are in $\mathbb{Q}(\sqrt[5]{5})$ are not in $\mathbb{Q}(\sqrt[5]{5})$. This means $\mathbb{Q}(\sqrt[5]{5})$ is not algebraically enclosed, and is thus not a field, hence a contradiction. Therefore, $\mathbb{Q}(\sqrt[5]{5})$ must have all powers of $\sqrt[5]{5}$.

In fact, this proves that in general, a radical field $\mathbb{Q}(\sqrt[p]{x})$ must contain all powers of $\sqrt[p]{x}$, where elements of $Q(\sqrt[p]{x})$ exist in the following:

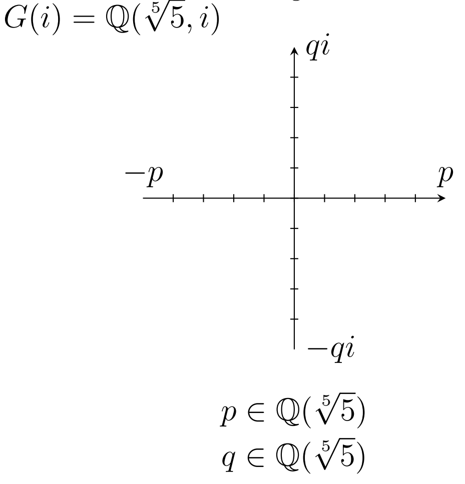
$$a_1\sqrt[p]{x} + a_2\sqrt[p]{x}^2 + \cdots + a_{p-1}\sqrt[p]{x}^{p-1} \tag{3.2}$$

Now, what would happen if we extend the field further? Let's think about the extension field $\mathbb{Q}(\sqrt[5]{5}, i)$. To simplify this, we call $\mathbb{Q}(\sqrt[5]{5})$ G, and think about the single extension G to $G(i)$, instead of two extensions at once. Let us compare $\mathbb{Q}(i)$ to $G(i)$:

$Fig.7$



$Fig.8$


$G(i) = \mathbb{Q}(\sqrt[5]{5}, i)$
qi
$-p$
p
$-qi$
$p \in \mathbb{Q}(\sqrt[5]{5})$
$q \in \mathbb{Q}(\sqrt[5]{5})$

Similar to before, all elements in $G(i)$ exist in the form of $p+qi$, where p and q are elements of G. However,remember G itself is an extension of $\mathbb{Q}$, where $G = \mathbb{Q}(\sqrt[5]{5})$. Since p and q are element in $\mathbb{Q}(\sqrt[5]{5})$, they also exist in the form described in (3.1). Furthermore, note that this is inherently different from the complex plane in $Fig.7$, where both axis has "gaps" of real numbers that can't be expressed as $p + qi$.

Then, elements of $\mathbb{Q}(\sqrt[5]{5}, i)$ should take the form of the following:

$$\begin{aligned} p + qi =& p_1 + p_2\sqrt[5]{5} + p_3(\sqrt[5]{5})^2 + p_4(\sqrt[5]{5})^3 + p_5(\sqrt[5]{5})^4 + \\ &(q_1 + q_2\sqrt[5]{5} + q_3(\sqrt[5]{5})^2 + q_4(\sqrt[5]{5})^3 + q_5(\sqrt[5]{5})^4)i \end{aligned} \tag{3.3}$$

From the example above, we can see that when we extend by more than one element, we get a linear combination of both elements with $\mathbb{Q}$, with every possible degree of root extraction from combinations of $\sqrt[5]{5}$ and i. This is where the idea of repeated arithmetic operation and root extraction come from. By creating a field extension, we are doing repeat arithmetic operation and root extraction, where we consider linear combinations of all possible powers of the root (3.2).

Now, we can determine whether or not a number is a radical, by checking if they are an element of a radical field. More precisely, a number k can be expressed as a radical if and only if it is an element of a radical field, where

$$k \in \mathbb{Q}(\sqrt[p_1]{\alpha_1}, \sqrt[p_2]{\alpha_2}, \cdots, \sqrt[p_n]{\alpha_n}) \implies k \in R \tag{3.4}$$

This is because any radical field extension is always a subset of all radicals, where $\mathbb{Q}(\sqrt[p_1]{\alpha_1}, \sqrt[p_2]{\alpha_2}, \cdots, \sqrt[p_n]{\alpha_n}) \subset R$. Here, we can apply this knowledge to roots of polynomials.

Let $P(x)$ be the general polynomial with distinct roots, where

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$$

We can factorize f(x) into linear factors, converting it in the form of

$$P(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$$

Then, P, the set of roots of $P(x)$ is the following, where

$$P = \{r_1, r_2, \cdots, r_n\}$$

Now, consider the smallest field that contains all roots of a polynomial. Formally, such a field is called the *splitting field* of a $P(x)$. It is named this way because $P(x)$ ”splits” and separates into linear factors. For the general polynomial, the splitting field is just the base field $\mathbb{Q}$ extending by each of the roots in P, which is

$$\mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n) \tag{3.5}$$

The splitting field is important because by definition, it is a field that contains all the roots to a polynomial. Here, we reach a central idea: **If** the splitting field of a polynomial $P(x)$ can be expressed as the following

$$\mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n) \subset \mathbb{Q}(\sqrt[p_1]{\alpha_1}, \sqrt[p_2]{\alpha_2}, \cdots, \sqrt[p_n]{\alpha_n}) \tag{3.6}$$

where $\mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n)$ can be constructed from a series of radical extensions, where each extension creates a splitting field for the previous one:

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \cdots \subset F_{m-1} \subset F_m = \mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n) \tag{3.7}$$

Then, the set of roots $\{r_1, r_2, \cdots, r_n\}$ are all expressible using repeat arithmetic operation and root extraction, where

$$(3.5) \implies \mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n) \subset R \tag{3.8}$$

From Chapter 2, we found our RQ to be equivalent to the following:

Are the roots of all polynomials expressible using repeat arithmetic operation and root extraction?

From what we just derived(the **If**... **Then**), we can write the RQ in terms of fields, and ask instead:

Does there exist finite numbers of field extensions, extending from the field of rationals to the splitting field for all polynomials?

Or, if we look from the perspective of the splitting field,

Does there exists a finite chain of subfield that connects the splitting field to the rationals for all polynomials?

Using the equivalent question above, we switch to a more useful perspective, where we examine the splitting field of the general polynomial and study it's subfields.

Chapter 4

Mapping fields to groups

4.1 Morphing a field

In this section, our aim is to simplify the structure of splitting fields, because looking at splitting fields themselves is still too abstract to derive anything meaningful. Here, we will introduce a simpler algebraic structure, called **groups**. When we introduced fields, we defined it as an algebraically enclosed set of objects that have two operations relating themselves following a set of axioms. A group is similarly an algebraically enclosed set S, but with only one operation $\circ$, that follows the following axioms:

Definition 4.0.1. *A group must satisfy the following criteria [10], where*

- $(a \circ b) \circ c = a \circ (b \circ c)$ *for all* $a, b, c \in S$
- *there exists a multiplicative identity* e*, such that* $a \circ e = e \circ a = a$ *for all* $a \in S$
- *for all* $a \in S$*, there exists a unique inverse* $-a \in S$ *such that* $a \circ (-a) = (-a) \circ a = 0$

The $\circ$ can be any mathematical operation. For example, when the set S is the integers $\mathbb{Z}$ and $\circ$ is the normal addition $+$, we form the group known as the additive group of integers. Just by the axioms, we see that a group is a lot less complicated than a field. Hence, our aim in this chapter is to describe the structure of fields, more specifically, the splitting fields, in terms of groups, as an attempt to further simply our RQ.

Now, we know that the structure of the splitting field is dependent on the nature of the extension element. In our previous examples, extending by a square root(i) gives us a two dimensional space, while a quintic($\sqrt[5]{2}$) root lead to a five dimensional space.

Let's think about the field $\mathbb{Q}(\sqrt[p]{\alpha_m})$, and imagine a set of functions F, where

$$F = \{f_1(x), f_2(x), \cdots, f_n(x)\} \tag{4.1}$$

is the set of all one-to-one functions that maps $\mathbb{Q}(\sqrt[p]{\alpha_m})$ onto itself, without mapping the elements of $\mathbb{Q}$. Specifically,

Definition 4.0.2. *f_i maps $\mathbb{Q}(\sqrt[p]{\alpha_m}) \leftrightarrow \mathbb{Q}(\sqrt[p]{\alpha_m})$, where*

$$f_i(x_1) = x_2 \ \ for \ \ x_1, x_2 \in \mathbb{Q}(\sqrt[p]{\alpha_m})$$

f_i fixes $\mathbb{Q}$(it doesn't map any element in $\mathbb{Q}$), where

$$f_i(x) = x \ for \ x \in \mathbb{Q}$$

$f_i(x)$ is a linear map, where

$$f_i(ab + cd) = f_i(a)f_i(b) + f_i(c)f_i(d) \ \ for \ a, b, c, d \ \ in \ \mathbb{Q}(\sqrt[p]{\alpha_m})$$

The motivation for such a definition is that, F encodes the information of the field in a simpler language. Breaking down the definitions, because f_i doesn't map elements in $\mathbb{Q}$, F only contains information about the extra properties the extension, $\sqrt[p]{\alpha_m}$, adds. Furthermore, the reason it must be linear is because it is mapping $\mathbb{Q}(\sqrt[p]{\alpha_m})$ to itself, so the structure of the field must be preserved.

In fact, the set F satisfies the criteria of a group. By definition, the set F contains **all** functions that satisfies (4.0.2), making it algebraically enclosed. Then, the group operation $\circ$ is function composition, where $f_i(x) \circ f_j(x) = f_i(f_j(x))$.

Formally, the f_i are called **field automorphisms**, and the group F is called the **automorphism group** of $\mathbb{Q}(\sqrt[p]{\alpha_m})$, and is written as $Aut(\mathbb{Q}(\sqrt[p]{\alpha_m})/\mathbb{Q})$ (the $/\mathbb{Q}$ means $\mathbb{Q}$ is not mapped by the group).

Written in equation form:

$$Aut(\mathbb{Q}(\sqrt[p]{\alpha_m})/\mathbb{Q}) = F = \{f_1(x), f_2(x), \cdots, f_n(x)\} \tag{4.2}$$

Through these definitions, we have successfully expressed the properties of the field $\mathbb{Q}(\sqrt[p]{\alpha_m})$ in terms of the group $Aut(\mathbb{Q}(\sqrt[p]{\alpha_m})/\mathbb{Q})$.

Notice how these functions are identical to matrices. For example, the set of all possible 2×2 matrices map $\mathbb{R}^2 \to \mathbb{R}^2$, fixes the origin $(0, 0)$, and is a linear map. This is identical to our definition in (4.0.2), where the f_i maps $\mathbb{Q}(\sqrt[p]{\alpha_m}) \to \mathbb{Q}(\sqrt[p]{\alpha_m})$, fixes $\mathbb{Q}$ in place, and are also linear. In fact, by treating $\mathbb{Q}(\sqrt[p]{\alpha_m})$ as a vector space, f_i are literal matrices.

To illustrate why this is useful, let us find the automorphism group of a specific splitting field. Let $P(x)$ be the following:

$$P(x) = x^3 - 2 \tag{4.3}$$

It is obvious to see that $\sqrt[3]{2}$ is a root, but we also needs to consider the complex roots. Let ω be the third root of unity, where $\omega = e^{(2\pi i)/3}$. Then,

$$\begin{aligned} p(\omega\sqrt[3]{2}) &= (\omega)^3(\sqrt[3]{2})^3 - 2 = 2 - 2 = 0 \\ p(\omega^2\sqrt[3]{2}) &= (\omega)^6(\sqrt[3]{2})^3 - 2 = 2 - 2 = 0 \end{aligned} \tag{4.4}$$

Hence, $P(x)$ can be factorized into the following:

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$$

From our expression, the smallest field is then

$$\mathbb{Q}(r_1, r_2, r_3) = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$$

Where elements of this field is can be seen as the following:

$$a_1 + a_2r_1 + a_3r_2 + a_4r_3 = a_1 + a_2\sqrt[3]{2} + a_3\omega\sqrt[3]{2} + a_4\omega^2\sqrt[3]{2} \tag{4.5}$$

This representation of the field directly follows the LHS of (3.5).

Furthermore, because we already solved $P(x)$, we know that the field is made of linear combinations of the radicals ω and $\sqrt[3]{2}$. Then, the splitting field can also be expressed as radical extensions of $\mathbb{Q}$, in the form of $\mathbb{Q}(\omega, \sqrt[3]{2})$, where all elements are as the following

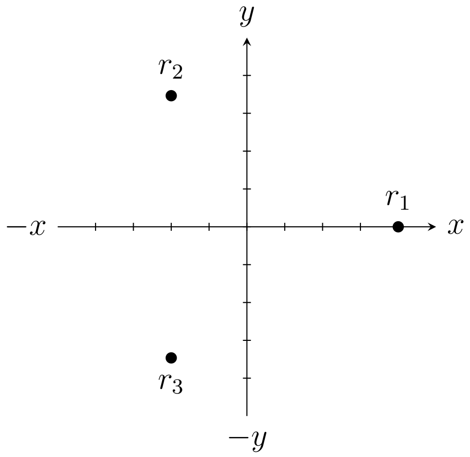
$$a_1 + a_2\sqrt[3]{2} + a_3(\sqrt[3]{2})^2 + a_4\omega + a_5\omega\sqrt[3]{2} + a_6\omega(\sqrt[3]{2})^2 \tag{4.6}$$

This representation of the field directly follows the RHS of (3.5). It is only when a splitting field is constructed from a series of radical extensions, can we represent the splitting field in this manner. For now, we will extensively explore (4.6).

Also, note that multiplies of ω^2 is nowhere to be seen in the expression. This is because $\omega^2 = -\omega - 1$, and is already included in the expression.

Following (4,6), We can visually express the field as the following

$Fig.9$



$$x = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$$
$$y = \omega(d + e\sqrt[3]{2} + f(\sqrt[3]{2})^2)$$

Where $r_1 = \sqrt[3]{2}$,$r_2 = \omega\sqrt[3]{2}$,$r_3 = \omega^2\sqrt[3]{2}$. Now, let us find the group F that corresponds to $P(x)$.

By the linearity of f_i in (4.0.2), all elements in $\mathbb{Q}(\omega, \sqrt[3]{2})$ will be mapped as the following:

$$\begin{aligned}&f_i(a_1 + a_2\sqrt[3]{2} + a_3(\sqrt[3]{2})^2 + a_4\omega + a_5\omega\sqrt[3]{2} + a_6\omega(\sqrt[3]{2})^2)\\ &= f_i(a_1) + f_i(a_2)f(\sqrt[3]{2}) + f_i(a_3)f_i(\sqrt[3]{2})^2 + f_i(a_4)f_i(\omega) + f_i(a_5)f_i(\omega\sqrt[3]{2}) + f_i(a_6)f_i(\omega\sqrt[3]{2}^2)\end{aligned} \tag{4.7}$$

Where we distribute f_i over each element. Furthermore, by the definition f_i in (4.0.2), f_i fixes $\mathbb{Q}$, so for the coefficients a_1 to a_6, we have $f_i(a_j) = a_j$. Hence,

$$\begin{aligned}&f_i(a_1) + f_i(a_2)f(\sqrt[3]{2}) + f_i(a_3)f_i(\sqrt[3]{2})^2 + f_i(a_4)f_i(\omega) + f_i(a_5)f_i(\omega\sqrt[3]{2}) + f_i(a_6)f_i(\omega\sqrt[3]{2}^2)\\ &= a_1 + a_2f_i(\sqrt[3]{2}) + a_3f_i(\sqrt[3]{2})^2 + a_4f_i(\omega) + a_5f_i(\omega)f_i(\sqrt[3]{2}) + a_6f_i(\omega)^2f_i(\sqrt[3]{2})^2\end{aligned} \tag{4.8}$$

Where we can see that only ω and $\sqrt[3]{2}$ are affected by the transformation. Therefore, we only need to pay attention to where ω and $\sqrt[3]{2}$ are mapped. In fact, there are only six possible $f_i(x)$ that satisfies (4.0.2), which are described in the following:

$$\begin{aligned}
&f_1 : f_1(\omega) = \omega, f_1(\sqrt[3]{2}) = \sqrt[3]{2}\\
&f_2 : f_2(\omega) = \omega, f_2(\sqrt[3]{2}) = \omega\sqrt[3]{2}\\
&f_3 : f_3(\omega) = \omega, f_3(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}\\
&f_4 : f_4(\omega) = \omega^2, f_4(\sqrt[3]{2}) = \sqrt[3]{2}\\
&f_5 : f_5(\omega) = \omega^2, f_5(\sqrt[3]{2}) = \omega\sqrt[3]{2}\\
&f_6 : f_6(\omega) = \omega^2, f_6(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}
\end{aligned} \tag{4.9}$$

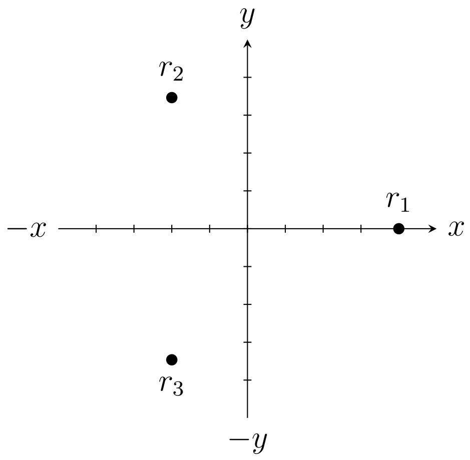
Notice how all $f_i(x)$ only include multiplying an element by ω. This is because ω is a complex number of magnitude 1, so multiplying by ω corresponds to a rotation around the origin, which is linear, reversible, and ignores elements in $\mathbb{Q}$. Whereas maps like $f(\omega) = \dfrac{\omega}{2}$ will end up mapping elements in $\mathbb{Q}$, where for example, $f(2) = f(\omega^3 2) = \omega^3\dfrac{2}{2^3} = \dfrac{1}{4}$. Hence,

$$Aut(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) = \{f_1, f_2, f_3, f_4, f_5, f_6\} \tag{4.10}$$

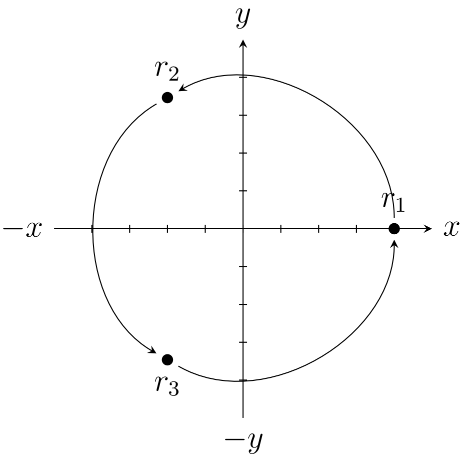
is the Automorphism group that corresponds to $\mathbb{Q}(\omega, \sqrt[3]{2})$.

Here, we can represent the effect of the group F on the field $\mathbb{Q}(\omega, \sqrt[3]{2})$ visually as the following, by focusing on where the three roots, r_1, r_2, and r_3 are mapped to:

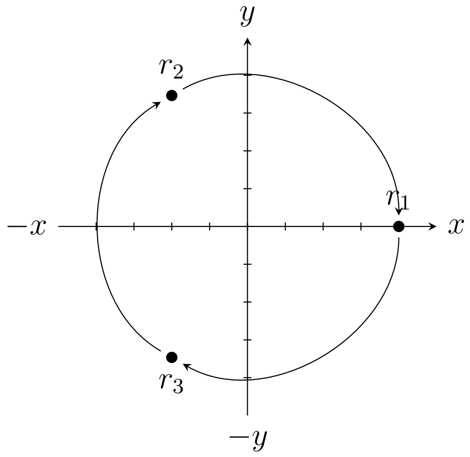
$f_1 : f_1(\omega) = \omega, f_1(\sqrt[3]{2}) = \sqrt[3]{2}$



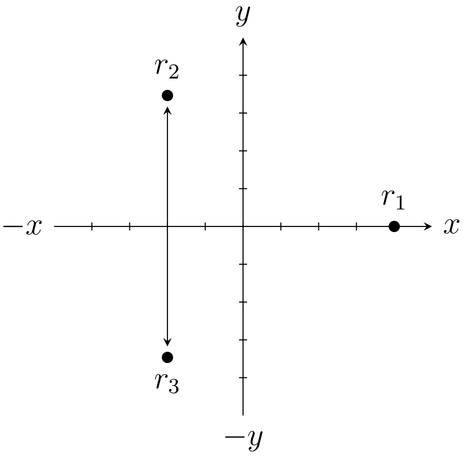
$f_2 : f_2(\omega) = \omega, f_1(\sqrt[3]{2}) = \omega\sqrt[3]{2}$



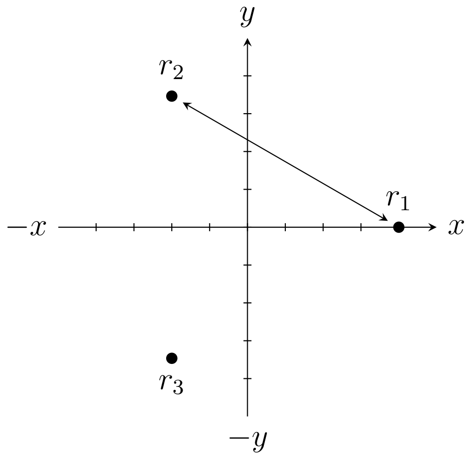
$f_3 : f_3(\omega) = \omega, f_1(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$



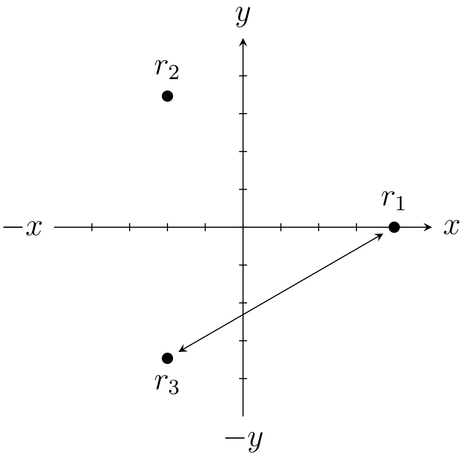
$f_4 : f_4(\omega) = \omega^2, f_1(\sqrt[3]{2}) = \sqrt[3]{2}$



$f_5 : f_5(\omega) = \omega^2, f_1(\sqrt[3]{2}) = \omega\sqrt[3]{2}$



$f_6 : f_6(\omega) = \omega^2, f_1(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$



$$x = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$$

$$y = \omega(d + e\sqrt[3]{2} + f(\sqrt[3]{2})^2)$$

$Fig.10$

Here, note that we resorted to presenting the field as a complex plane. However, even though the y axis is complex(a multiple of ω), this is inherently different from $\mathbb{C}$, since both x and y axis have "gaps" of real numbers that are not in $\mathbb{C}$.

By looking at $Fig.10$, we can further see the connection between f_i and matrices. By comparing the field $\mathbb{Q}(\omega, \sqrt[3]{2})$ to the Cartesian plane $\mathbb{R}^2$, the action of f_1 on $\mathbb{Q}(\omega, \sqrt[3]{2})$ is the same as the action of the identity matrix I on $\mathbb{R}^2$. In fact, we can represent all the functions as matrices: f_2 and f_3 can be represented as rotational matrices, while f_4, f_5, f_6 can be represented as reflection matrices:

For example, if we just look at f_2 in $Fig.10$, it is a form of rotation of $2\pi/3$ about the origin. This is identical to the matrix $\begin{bmatrix} \cos(\frac{2\pi}{3}) & -\sin(\frac{2\pi}{3}) \\ \sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{bmatrix}$ that rotates $\mathbb{R}^2$ by $2\pi/3$ about the origin. if we look at f_4, it reflects $\mathbb{Q}(\omega, \sqrt[3]{2})$ about the x axis. A corresponding matrix in $\mathbb{R}^2$ would be $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. We can further represent all f_i in (4.8) as the following:

$Aut(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$

$= \{f_1, f_2, f_3, f_4, f_5, f_6\}$

$$\leftrightarrow \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \cos(\frac{2\pi}{3}) & -\sin(\frac{2\pi}{3}) \\ \sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{bmatrix}, \quad \begin{bmatrix} \cos(\frac{2\pi}{3}) & \sin(\frac{2\pi}{3}) \\ -\sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{bmatrix}, \right.$$
$$\left. \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} \cos(\frac{2\pi}{3}) & -\sin(\frac{2\pi}{3}) \\ \sin(\frac{2\pi}{3}) & -\cos(\frac{2\pi}{3}) \end{bmatrix}, \quad \begin{bmatrix} \cos(\frac{2\pi}{3}) & \sin(\frac{2\pi}{3}) \\ -\sin(\frac{2\pi}{3}) & -\cos(\frac{2\pi}{3}) \end{bmatrix} \right\}$$

$$= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \right\} \tag{4.11}$$

This is a good way to visualize what f_i does on the roots, but it doesn't fully represent its effect on the entire field, because these matrices are still describing the effect on $\mathbb{R}^2$.

Hence, from (4.6), we directly express all elements in $\mathbb{Q}(\omega, \sqrt[3]{2})$ as 6 dimensional vectors, where we can write

$$a_1 + a_2\sqrt[3]{2} + a_3(\sqrt[3]{2})^2 + a_4\omega + a_5\omega\sqrt[3]{2} + a_6\omega(\sqrt[3]{2})^2 = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix} \tag{4.12}$$

where the basis B is the following:

$$B = \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \omega\sqrt[3]{2}, \omega(\sqrt[3]{2})^2\} \tag{4.13}$$

This enables us to see $\mathbb{Q}(\omega, \sqrt[3]{2})$ as a vector space on it's own, and the f_i as 6×6 matrices.

$$Aut(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$$

$$= \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

$$\leftrightarrow \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega \end{bmatrix}, \right.$$
$$\left. \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega^2 \end{bmatrix} \right\} \tag{4.14}$$

Allowing us to contextualize the abstract automorphism groups, where we use matrices to represent the transformations.

However, Recall that $\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(r_1, r_2, r_3)$, where we could represent the splitting field directly in terms of the roots. We can express the field with a vector space of basis B:

$$B = \{1, \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2(\sqrt[3]{2})\} = \{1, r_1, r_2, r_3\} \tag{4.15}$$

Under this basis, the elements in $\mathbb{Q}(\omega, \sqrt[3]{2})$ is the following

$$a_1 + a_2\sqrt[3]{2} + a_3\omega\sqrt[3]{2} + a_4\omega^2(\sqrt[3]{2}) = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} \tag{4.16}$$

Where the LHS of the expression follows from (4.5).This expression is useful because it is generalizable to polynomial with roots ranging from r_1 to r_n, whether they are radicals or not. In this basis, the automorphisms appears differently:

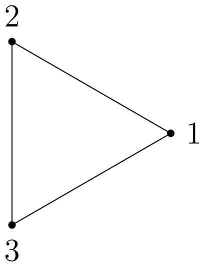
$Aut(\mathbb{Q}(r_1, r_2, r_3)/\mathbb{Q})$

$= \{f_1, f_2, f_3, f_4, f_5, f_6\}$

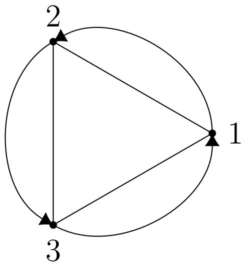
$$\leftrightarrow \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \right\} \tag{4.17}$$

Where they become permutation matrices that rearranging the roots in the same way as $Fig.8$. To see why they are permutations, if we connect the roots from $Fig.10$ to form triangle, and number the vertices, we have the following, where

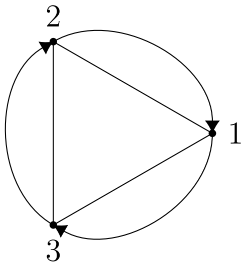
(123) $\Leftrightarrow$



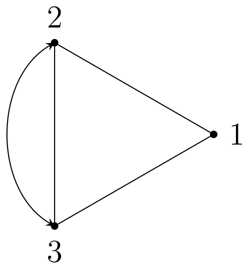
(231) $\Leftrightarrow$



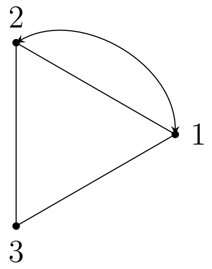
(312) $\Leftrightarrow$



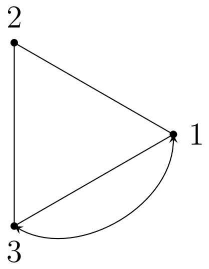
(132) $\Leftrightarrow$



(132) $\Leftrightarrow$



(213) $\Leftrightarrow$



Where the action of (4.17) is equivalent to the group of permutating of 3 numbers.

To summarize, we found two distinct matrix representations of the automorphism group.

We also notice something interesting: by definition, the splitting field only take the form of a series of radical extensions if the roots are expressible using radicals (see (3.6)).

Then, the diagonal matrices we obtain from $Aut(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$, is related to the fact that $Aut(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ is constructed from radical extensions. $Aut(\mathbb{Q}(r_1, r_2, r_3)/\mathbb{Q})$ on the other hand gives permutation matrices.

4.2 Mapping subfields

However, our previous conclusion was not exactly rigorous. Recall that we previously obtained an equivalent RQ, which was:

Does there exists a finite chain of subfield that connects the splitting field to the rationals for all polynomials?

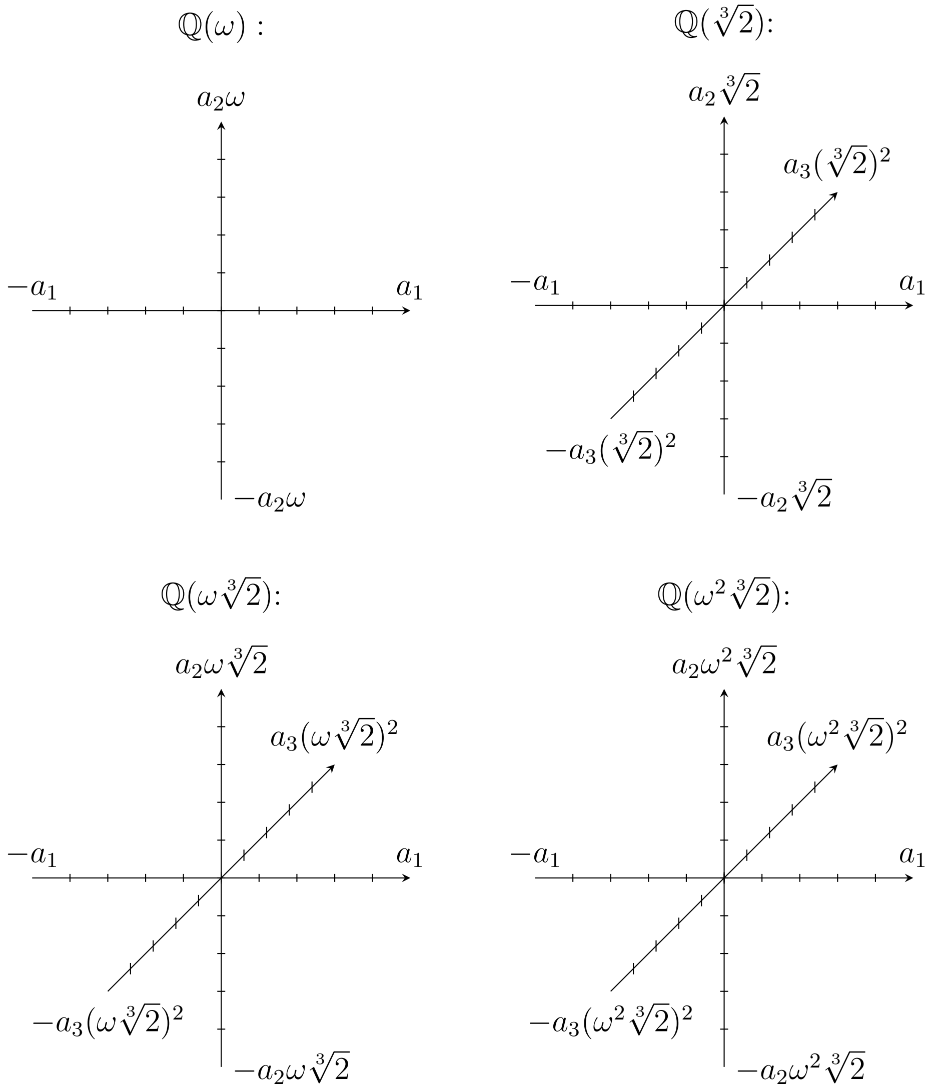
Where we needed a "chain of subfields" as described in (3.7), extending from $\mathbb{Q}$ to the splitting field of the general polynomial:

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \cdots \subset F_{m-1} \subset F_m = \mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n)$$

Therefore, our next step is to show that the subfields of $\mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n)$, has a one-to-one correspondence to the subgroups of $Aut(\mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n)/\mathbb{Q})$.

Let's look at the subfields of our example before moving to the general case. In our example, there are four subfields in $\mathbb{Q}(\omega, \sqrt[3]{2})$(not including $\mathbb{Q}(\omega, \sqrt[3]{2})$ itself and the identity):

$$\begin{aligned}
&\mathbb{Q}(\omega) = \{x|x = a_1 + a_2\omega, a_1, a_2 \in \mathbb{Q}\}\\
&\mathbb{Q}(\sqrt[3]{2}) = \{x|x = a_1 + a_2\sqrt[3]{2} + a_3(\sqrt[3]{2})^2, a_1, a_2, a_3 \in \mathbb{Q}\}\\
&\mathbb{Q}(\omega\sqrt[3]{2}) = \{x|x = a_1 + a_2\omega\sqrt[3]{2} + a_3(\omega\sqrt[3]{2})^2, a_1, a_2, a_3 \in \mathbb{Q}\}\\
&\mathbb{Q}(\omega^2\sqrt[3]{2}) = \{x|x = a_1 + a_2\omega^2\sqrt[3]{2} + a_3(\omega^2\sqrt[3]{2})^2, a_1, a_2, a_3 \in \mathbb{Q}\}
\end{aligned} \tag{4.18}$$



$\mathbb{Q}(\omega)$:

$\mathbb{Q}(\sqrt[3]{2})$:

$\mathbb{Q}(\omega\sqrt[3]{2})$:

$\mathbb{Q}(\omega^2\sqrt[3]{2})$:

$Fig.11$

What we need to do now is to find a subset of matrices in $Aut(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ in (4.13), that somehow relates to fields in (4.14).

An interesting observation can be made on the location of 1s on the diagonal of matrices in (4.13): Each 1 indicate which specific sub-section of $\mathbb{Q}(\omega, \sqrt[3]{2})$ is not mapped. For example, from (4.14),

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega \end{bmatrix}$$

has 1s in the diagonal of the first three rows. The first three rows corresponds to a_1,$a_2\sqrt[3]{2}$ and $a_3(\sqrt[3]{2})^2$, (Refer back to (4.12)), and the 1 in those position indicate that elements of $\mathbb{Q}(\sqrt[3]{2})$ are fixed by the matrix.

This directly relates a specific subset of $Aut(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ to a specific subset of $\mathbb{Q}(\omega, \sqrt[3]{2})$, which is what our aim is in the first place: mapping subfields to subgroups.

The below are the corresponding subfields and subgroups:

$$
\begin{gathered}
\left\{ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega \end{bmatrix} \right\} \leftrightarrow \mathbb{Q}(\omega) \\
\left\{ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega \end{bmatrix} \right\} \leftrightarrow \mathbb{Q}(\sqrt[3]{2}) \\
\left\{ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega^2 \end{bmatrix} \right\} \leftrightarrow \mathbb{Q}(\omega\sqrt[3]{2}) \\
\left\{ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \right\} \leftrightarrow \mathbb{Q}(\omega^2\sqrt[3]{2})
\end{gathered}
\tag{4.19}
$$

Where each group of matrices on the left, fixes the fields on the right.

This one-to-one correspondence, or a **bijection**, between the subfields and subgroups, also applies to any splitting field F_m, where the bulk of the proof can be found at [5].

Now, remember from (3.6) that we need a series of ”radical” extensions, where each extension creates a splitting field for the previous field. This brings restrictions to the subgroups, where the subgroups of G has to satisfy certain criteria. For any intermediate field F_k, where $\mathbb{Q} \subset F_k \subset F_m$, we have

$$Aut(F_m/F_k)\sigma = \sigma Aut(F_m/F_k) \text{ for } \sigma \in Aut(F_m/\mathbb{Q})$$

[9]

A subgroup that satisfies this is called a **normal** subgroup. One way to interpret why this is true, is by the idea that the automorphisms can only be expressed as diagonal matrices if the splitting field is constructed from radical extensions, and all diagonal matrices are commutative.

Here, we map every subfield to their respective normal subgroups:

$$\begin{tikzcd}
Q \arrow[dd, leftrightarrow] & \subset & F_1 \arrow[dd, leftrightarrow] & \subset & F_2 \arrow[dd, leftrightarrow] & \subset & F_3 \arrow[dd, leftrightarrow] & & F_{m-1} \arrow[dd, leftrightarrow] & \subset & F_m \arrow[dd, leftrightarrow] \\
 & & & & & & & \cdots & & & \\
Aut(F_m/\mathbb{Q}) & \rhd & Aut(F_m/F_1) & \rhd & Aut(F_m/F_2) & \rhd & Aut(F_m/F_3) & & Aut(F_m/F_{m-1}) & \rhd & \{e\}
\end{tikzcd}$$

$$e = Aut(F_m/F_m) \lhd Aut(F_m/F_{m-1}) \lhd \cdots \lhd Aut(F_{m-1}/F_1) \lhd Aut(F_m/\mathbb{Q}) = G$$

($\lhd$ is the notation for normal subgroups, where the tip of the triangle is the subgroup of the base of the triangle.)

Notice that the order is flipped when mapped. $\mathbb{Q}$, the smallest field, is mapped to $Aut(F_m/\mathbb{Q})$, the largest group, because we map a field to the group that fixes the field, like our example in (4.19).

Instead of examining a chain of subfields, we switch our attention to a chain of corresponding normal subgroups. This concept of mapping a field to a group is in fact the crux of this essay, because being able to translate information regarding fields into groups allows us to answer our question in terms of a simpler algebraic structure.

Recall that we had an equivalent form of our RQ, which was:

Does there exists a finite chain of subfield that connects the splitting field to the rationals for all polynomials?

Because of the equivalence of automorphism groups and fields, we also have an equivalent question:

Does there exists a finite chain of normal subgroups that connects the automorphism group of a splitting field, to the trivial group $\{e\}$ for all polynomials?

Chapter 5

Insolvability of the quintic and conclusion

Now, by our logic established in previous chapters, for the general polynomial $P(x)$, where

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = (x - r_1)(x - r_2)\cdots(x - r_n)$$

There exists a chain of normal subgroups from $Aut(\mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n))$ to $\{e\}$

$\Leftrightarrow$ The splitting field of all polynomials can be expressed as a tower of radical extensions

$\Leftrightarrow$ The root to all polynomials, the algebraic numbers, are expressible using radicals.

Which means the relationship is that in $Fig.4$ is true. If the first statement is false, the the algebraic numbers are not expressible using radicals, meaning $Fig.3$ is true.

If we go back to $P(x)$, the splitting field $\mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n)$ can be represented by a vector space, where

$$a_1 + a_2 r_1 + \cdots + a_{n+1} r_n = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \cdots \\ a_{n+1} \end{bmatrix} \tag{5.1}$$

Then, each automorphism is an $(n+1) \times (n+1)$ permutation matrix, in the form of the following:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \\ \vdots & & \ddots & \\ 0 & & & \ddots \end{bmatrix} \tag{5.2}$$

Where the 1 in the top left corner indicates the fixing of $\mathbb{Q}$. Because only the $n \times n$ subsection of the matrix contains permutations, The group of automorphisms is equivalent to S_n,the permutation group of n subjects, where:

$$Aut(\mathbb{Q}(r_1, r_2, \cdots, r_{n-1}, r_n)) \simeq S_n$$

Where $\simeq$ means they are equivalent in terms of structure. Now, examining the subgroups of S_n, which is the set of permutations of n objects, the set of even permutations form a group. This is because the combination of even permutations leads to even permutations only, just like how the addition of even numbers leads to only even numbers. We call the group of even permutations A_n.

Here, something special happens when $n = 5$, where A_5 is not a normal subgroup [8]. This implies, for general quintic polynomials with distinct roots, they are not solvable using radicals. Hence, we can conclude that $R \subset A$.

This answers our RQ, where we showcased that algebraic numbers are not all expressible using radicals.

This has some significant implications, one of them being, we cannot have general root formulas for polynomials of degree 5 and higher. That is, there is no equivalent quadratic formula for higher degree polynomials (5 and more). Furthermore, this idea of mapping field to groups is actually a very central part of abstract algebra, and is often used to study abstract field extensions, since it is very good at encoding information of a field.

Bibliography

[1] Rosen, Michael I. “Niels Hendrik Abel and Equations of the Fifth Degree.” The American Mathematical Monthly, vol. 102, no. 6, 1995, pp. 495–505. JSTOR, www.jstor.org/stable/2974763. Accessed 4 Mar. 2021.

[2] Ayoub, Raymond G. “Paolo Ruffini’s Contributions to the Quintic.” Archive for History of Exact Sciences, vol. 23, no. 3, 1980, pp. 253–277. JSTOR, www.jstor.org/stable/41133596. Accessed 4 Mar. 2021.

[3] Stillwell, John. “Galois Theory for Beginners.” The American Mathematical Monthly, vol. 101, no. 1, 1994, pp. 22–27. JSTOR, www.jstor.org/stable/2325119. Accessed 4 Mar. 2021.

[4] Jiang, Yunye, ”Galois Theory and the Quintic Equation” (2018). Honors Theses. 1602. https://digitalworks.union.edu/theses/1602

[5] Dickinson, Mark. ”GALOIS THEORY: THE PROOFS, THE WHOLE PROOFS, AND NOTHING BUT THE PROOFS”. Pitt.Edu, http://www.pitt.edu/ gmc/algebra/galoistheory.pdf?scrlybrkr=e51d1b3f. Accessed 14 Dec 2020.

[6] Apostol, T. M. ”The Field Axioms.” §I 3.2 in Calculus, 2nd ed., Vol. 1: One-Variable Calculus, with an Introduction to Linear Algebra. Waltham, MA: Blaisdell, pp. 17-19, 1967.

[7] Weisstein, Eric W. ”Field Axioms.” From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/FieldAxioms.html

[8] Shrestha, Abhinav. “The Classification of Simple Finite Groups.” Math.uchicago.edu, The University of Chicago, www.math.uchicago.edu/ may/VIGRE/VIGRE2010/REUPapers/Shrestha.pdf.

[9] marlu (https://math.stackexchange.com/users/26204/marlu), Galois correspondence between normal groups and normal extensions, URL (version: 2013-01-25): https://math.stackexchange.com/q/286906

[10] Rowland, Todd and Weisstein, Eric W. ”Group.” From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/Group.html