university of groningen / faculty of science and engineering / mathematics and applied mathematics

# Galois groups and monic polynomials in $\mathbb{Z}[x]$ of degrees ≤ 6

Bachelor's Project Mathematics

June 2020

Student: J. Zhang

First supervisor: Prof. J. Top

Second assessor: Dr. F. Bianchi

**Abstract**

In this bachelor's project, I aim to describe, given a general monic polynomial with integer coefficients of degree $n \leq 6$, the Galois group of its splitting field over $\mathbb{Q}$. First of all, there are two situations to consider: the polynomial is irreducible or reducible. In the former case, we can use discriminant, resolvent and the subtle connection between irreducibility and transitive subgroups of $S_n$; in the latter case, we can factor the polynomial into irreducible factors of smaller degrees, explore the relation among their splitting fields and apply the results we already obtained.

# Contents

# 1 Introduction and preliminaries

Galois theory is a deep and rich branch of algebra named after the French mathematician Évariste Galois. In the beginning, it was introduced to solve the famous problem: does a general polynomial of degree at least 5 have an explicit formula for its roots? By works of Galois, the answer is no, because $S_n$ is not solvable for all $n \geq 5$. Later, Galois theory was also found helpful in both classical and contemporary mathematics, for example, trisecting an angle and differential equations. In this project, I will attempt to explore the relationship between polynomials and the Galois groups associated with them. This helps us in understanding the polynomial in many ways, for instance, given a polynomial, if we only know one of its roots but we also know how the Galois group acts on its roots, we might be able to guess the remaining roots without having to compute them.

The restriction that we are considering monic polynomials with integer coefficients might seem harsh here. But in fact, any polynomial $f(x) = a_n x^n + \ldots + a_1 x + a_0$ in $\mathbb{Q}[x]$ can be transformed into a monic one in $\mathbb{Z}[x]$, and these two polynomials will have the same splitting field. First note that we can multiply the least common multiple of the denominators of $a_n, \ldots, a_0$ so we have a polynomial in $\mathbb{Z}[x]$ that has the same zeros. Hence we may suppose $a_n, \ldots, a_0 \in \mathbb{Z}$. Next, note that the following polynomial:

$$g(x) = a_n^{n-1} f(\frac{x}{a_n}) = a_n^{n-1}(a_n \frac{x^n}{a_n^n} + a_{n-1} \frac{x^{n-1}}{a_n^{n-1}} + \ldots + \frac{a_1 x}{a_n} + a_0)$$

will be a monic polynomial in $\mathbb{Z}[x]$. Furthermore, let $\alpha_1, \ldots, \alpha_n$ be the zeros of $f(x)$, then $a_n\alpha_1, \ldots, a_n\alpha_n$ are the zeros of $g(x)$. Therefore they will have the same splitting field over $\mathbb{Q}$ and their Galois groups, which are the $\mathbb{Q}$-automorphisms of their splitting fields, will be the same.

## 1.1 Galois groups, transitive groups and permutations

First, we need some preliminaries before understanding what Galois groups are about. I assume the reader is familiar with basic concepts on fields, especially field extensions.

**Definition.** *A field extension $L \supseteq K$ is called normal if every irreducible polynomial $f(x) \in K[x]$ which has a zero in $L$, splits as a product of factors of degree one in $L[x]$.*

**Example 1.1.**

1. *Let $L = \mathbb{C}$ and $K = \mathbb{R}$, then $L \supseteq K$ is normal. Indeed, every $f(x) \in \mathbb{R}[x]$ has its zeros in $\mathbb{C}$.*
2. *Let $L = \mathbb{Q}(\sqrt[4]{2})$ and $K = \mathbb{Q}$, then $L \supseteq K$ is NOT normal, $x^4 - 2 = 0$ has a zero in $L$, but also has a zero $x = i\sqrt[4]{2}$ not in $L$.*

**Definition.** *An extension $L \supseteq K$ is called separable if every element of $L$ is algebraic and its minimal polynomial over $K$ is separable.*

**Theorem 1.1.** *Every algebraic extension of fields of characteristic* 0 *is separable.*

*Proof.* See, for example, page 112 of [1]. ☐

Since we are concerned with algebraic extensions over $\mathbb{Q}$, whose characteristic is 0, with this theorem we don't need to worry about separablility.

**Definition.** *A $K$-automorphism $L \supseteq K$ is an isomorphism $\sigma : L \to L$ such that*

$$\sigma(k) = k$$

*for all $k \in K$.*

**Definition.** *The Galois group* $\mathrm{Gal}(L/K)$ *is the group of all $K$-automorphism of the normal and separable extension $L \supseteq K$. We also denote by* $\mathrm{Gal}_f$ *the Galois group of the splitting field of a separable polynomial $f$ over a field.*

**Remark 1.2.** *Some instructive examples are included in section 2.3, which, hopefully, can provide a rough idea about Galois groups.*

**Theorem 1.3.** *Let $f(x) \in \mathbb{Z}[x]$, let $L$ be its splitting field over $\mathbb{Q}$ and consider $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Then if $a \in L$ is a zero of $f(x)$, so is $\sigma(a) \in L$.*

*Proof.* Let $f(x) = 0$, then:

$$\sigma(f(x)) = \sigma(a_n x^n + \ldots + a_1 x + a_0) = \sigma(a_n)(\sigma(x))^n + \ldots + \sigma(a_1)\sigma(x) + \sigma(a_0) = 0.$$

☐

**Theorem 1.4.** *The Galois group of the splitting field over $\mathbb{Q}$ of a polynomial in $\mathbb{Z}[x]$ of degree $n$ is isomorphic to a subgroup of $S_n$*

*Proof.* This is a direct consequence of previous theorem. ☐

**Definition.** *A subgroup $H \subseteq S_n$ is called transitive if for all $i, j \in \{1, 2, \ldots, n\}$ there exists $\sigma \in H$ such that $\sigma(i) = j$*

**Theorem 1.5.** *Let $L$ be the splitting field of a separable polynomial $f(x)$ in $\mathbb{Z}[x]$ of degree $n$, then* $\mathrm{Gal}(L/\mathbb{Q})$ *is isomorphic to a transitive subgroup of $S_n$ if and only if $f(x)$ is irreducible.*

*Proof.* Let $f(x) \in K[x]$ be irreducible and separable. By definition $f(x)$ has $n$ distinct zeros $a_1, a_2, \ldots, a_n \in L$. Therefore, for all $i, j \in \{1, 2, \ldots, n\}$ we can construct a $\mathbb{Q}$-automorphism sending $a_i$ to $a_j$, hence $\mathrm{Gal}_f$ is isomorphic to a transitive subgroup of $S_n$. Conversely, suppose $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to a transitive subgroup of $S_n$, let $h(x)$ be an irreducible factor of $f(x)$ and $a_1, a_2, \ldots, a_n \in L$ be the zeros of $f(x)$. Then there exists $a_i$ such that $h(a_i) = 0$, but we also have $h(a_j) = 0$ for all $j$ since $\mathrm{Gal}(L/\mathbb{Q})$ is transitive, which means (after possibly multiplying by a nonzero element of $K$) that $h = f$. ☐

**Theorem 1.6.** *Let $H$ be a transitive subgroup of $S_n$, then $n$ divides $|H|$.*

*Proof.* Let $X = \{1, \ldots, n\}$. Take $x \in X$, we have a subgroup of $H$, which is called the stabilizer, defined as $Stab(x) = \{h \in H : hx = x\}$.
The map

$$\varphi : H \to X, \qquad h \mapsto h(1)$$

is surjective as $H$ is transitive. Moreover, $H/Stab(1) \to X$ is clearly a bijection and hence $n = |X|$ is a divisor of $|H|$. □

**Theorem 1.7.** *Let $f(x) \in \mathbb{Z}[x]$ of degree $n$ be irreducible and separable and $L$ be its splitting field over $\mathbb{Q}$, then $n$ divides $|\mathrm{Gal}(L/\mathbb{Q})|$*

*Proof.* This is the direct consequence of previous two theorems. □

## 1.2 Discriminant, resultant and resolvent

In later sections, discriminants and resolvents will be used frequently to analyze our problem; in the meanwhile, discriminants would be difficult to compute by hand if we do not resort to resultants.

**Definition.** *The discriminant of a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, where $n > 1$, is defined as*

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

*where the $\alpha_i$ are the roots of $f$.*

**Remark 1.8.** *We generally do not consider discriminants for linear polynomials. In the rest of this text, mostly we will encounter monic polynomials, and in such cases $\Delta(f) = \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)^2$. Furthermore, note that $\Delta(f) = 0$ if and only if $f$ has multiple zeros. In this text we consider separable polynomials only, thus the discriminants are never zero. Moreover, $\Delta(f)$ is a symmetric polynomial in the $\alpha_i$'s and hence it can be expressed in terms of the elementary symmetric polynomials in the $\alpha_i$'s, which up to sign are the $a_j/a_n$.*

**Theorem 1.9.** *Let $f$ be a monic, separable and irreducible polynomial in $\mathbb{Q}[x]$ of degree $> 1$, then: $\sqrt{\Delta(f)} \in \mathbb{Q} \Leftrightarrow$ The Galois group of the splitting field of $f$ over $\mathbb{Q}$ consists of even permutations only.*

*Proof.* If $\sqrt{\Delta(f)} \in \mathbb{Q}$ then it is fixed by elements of the Galois group, but $\sqrt{\Delta(f)} = \prod_{1 \le i < j \le n}(x_i - x_j)$ can only be fixed by even permutations; the converse is obvious. □

The following tool will be very helpful to us in computing the discriminant of a polynomial, which can be found on pages 47-48 of `http://websites.math.leidenuniv.nl/algebra/ant.pdf`, lecture notes by P. Stevenhagen of the University of Leiden. However, Theorem 1.10 is not proved there.

**Definition.** *Let* $g(x) = b\prod_{i=1}^{r}(x-\beta_i)$ *and* $h(x) = c\prod_{i=1}^{s}(x-\gamma_i)$ *be polynomials with coefficients and roots in a field, then their resultant* $Res(f,g)$ *is defined as*

$$Res(g,h) = b^s c^r \prod_{i=1}^{r}\prod_{j=1}^{s}(\beta_i - \gamma_j).$$

**Theorem 1.10.** *Let* $g$*,* $h$ *be defined as in the previous definition, then we have:*

1. $Res(g,h) = (-1)^{rs}Res(h,g)$
2. $Res(g,h) = b^s \prod_{i=1}^{r} h(\beta_i)$
3. $Res(g,h) = b^{s-s_1}Res(g,h_1)$*, where* $h_1 \neq 0$ *satisfies* $h_1 \equiv h \bmod g$*, and* $s_1$ *is the degree of* $h_1$

*Proof.* 1. By definition, we have:

$$\begin{aligned} Res(g,h) &= b^s c^r \prod_{i=1}^{r}\prod_{j=1}^{s}(\beta_i - \gamma_j) \\ &= (-1)^{rs} c^r b^s \prod_{j=1}^{s}\prod_{i=1}^{r}(\gamma_j - \beta_i) \\ &= (-1)^{rs} Res(h,g) \end{aligned}$$

2. This is obvious by substituting the definition of $h$ into the definition of $Res(g,h)$.

3. $h_1(\beta_i) = h(\beta_i)$ as $h_1 \equiv h \bmod g$, hence $Res(g,h_1) = b^{s_1}\prod_{i=1}^{r} h_1(\beta_i)$ by property 2, and hence

$$\begin{aligned} b^{s-s_1}Res(g,h_1) &= b^{s-s_1}b^{s_1}\prod_{i=1}^{r} h_1(\beta_i) \\ &= b^s \prod_{i=1}^{r} h_1(\beta_i) \\ &= b^s \prod_{i=1}^{r} h(\beta_i) \\ &= Res(g,h) \end{aligned}$$

□

**Remark 1.11.** *In subsequent sections, we will need* $Res(f,f')$*, the importance of which is in the next theorem. Say* $f$ *is of degree 4, then* $Res(f,f')$ *involves the resultant of polynomials of degree 4 and 3, and the computation can be made easier by property 3, which allows us to replace* $f'$ *by the remainder of* $f$ *divided by* $f'$*. Repeat this process until the remainder is of low degree (usually 1 or*

*2), so we can spot its zeros (say, $\alpha_i$) very easily. Afterwards, we use property 1 to swap $f$ and that remainder, and finally we can use property 2 to get a simple formula linking $Res(f, f')$ and $\prod f(\alpha_i)$. For an explicit example using this theorem, refer to section 2.1 where the discriminant of a general, monic polynomial of degree 3 is calculated.*

**Theorem 1.12.** *Let $f \in F[x]$ be monic and of degree $n$ larger than 1, then:*

$$\Delta(f) = (-1)^{\frac{1}{2}n(n-1)} Res(f, f')$$

*Proof.* The proof of Theorem 1.12 requires new techniques, e.g. Sylvester's matrix, which are not very relevant to our problem here, thus I omit it. But the proof can be found on, for instance, pages 119-121 of [2]. □

Now we have a tool to determine whether $\text{Gal}_f$ consists of even permutations or not, using discriminants, which can be computed using resultants. But to obtain more information on $\text{Gal}_f$, we'll also need resolvents.

**Definition.** *Let $K$ be a field and $f(x) \in K[x]$ be separable and of degree $n$. The resolvent polynomial of $f(x)$ with respect to a subgroup $G \subseteq S_n$ and $F(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ such that $G = \{\sigma \in S_n : \sigma F = F\}$ is the stabilizer of $F$, is:*

$$r_{G,F}(f)(y) = \prod_{\sigma_i \in S_n/G} (y - (\sigma_i F))(x_1, \ldots, x_n), \quad x_i \mapsto a_i$$

*where $\sigma_i$ are coset representatives of $S_n/G$ and $a_i$ are roots of $f(x)$.*

**Theorem 1.13.** *The resolvent polynomial $r$ of $f(x) \in K[x]$ has its coefficients in $K$.*

*Proof.* Let $\tau \in \text{Gal}(L/K) \subseteq S_n$ where $L$ is the splitting field of $f$ over $K$, then:

$$\tau(r) = \prod_{\sigma \in S_n/G} (T - (\tau\sigma F))(a_1, \ldots, a_n) = \prod_{\sigma \in S_n/G} (T - (\sigma F))(a_1, \ldots, a_n) = r$$

Because if $\sigma_i$ are representatives of different coset then so are $\tau\sigma_i$. Thus, $r$ is fixed by all $K$-automorphisms and hence $r$ has its coefficients in $K$. □

**Theorem 1.14.** *Let the resolvent polynomial $r_{G_F,F}(f)$ of $f(x) \in K[x]$ be separable. Then $\text{Gal}(L/K)$, where $L$ is the splitting field of $f$ over $K$, is conjugate in $G$ to a subgroup of $G_F$, the stabilizer of $F$ in $G$, if and only if $r_{G,F}(f)$ has a root in $K$.*

*Proof.* ($\Rightarrow$) Let $\sigma \in G$ such that $\sigma^{-1}\text{Gal}(L/K)\sigma \subseteq G_F$ and let $\alpha_1, \ldots, \alpha_n$ be the zeros of $f(x)$. Then for $\tau \in \text{Gal}(L/K)$ one has $\sigma^{-1}\tau\sigma F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$. Hence

$$\tau\sigma F(\alpha_1, \ldots, \alpha_n) = \sigma F(\alpha_1, \ldots, \alpha_n)$$

and therefore $r$ has a root in $K$.

Before proving the other direction, we note a small consequence of $r$ being separable:
Let $\sigma_i$ be the representatives of $G/G_F$ and $\sigma_1 = e$. Then, for all $\sigma \in G$, we have $\sigma = \sigma_i \tau$ for some $i$, where $\tau \in G_F$. Then:

$$\sigma F(\alpha_1, \dots, \alpha_n) = \sigma_i \tau F(\alpha_1, \dots, \alpha_n) = \sigma_i F(\alpha_1, \dots, \alpha_n)$$

which is a zero of $r$. Since all zeros of $r$ are distinct, $\sigma_i F(\alpha_1, \dots, \alpha_n) = \sigma_1 F(\alpha_1, \dots, \alpha_n)$ if and only if $\sigma_i = \sigma_1 = e$. This means $\sigma F(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n)$ if and only if $\sigma = \sigma_1 \tau = \tau \in G_F$.

($\Leftarrow$) Assume $\sigma_i F(\alpha_1, \dots, \alpha_n) \in K$ for some $i$ and let $\tau \in G_F$. Then we have $\tau \sigma_i F(\alpha_1, \dots, \alpha_n) = \sigma_i F(\alpha_1, \dots, \alpha_n)$, which means $\sigma_i^{-1} \tau \sigma_i F(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n)$. Since $r$ is separable, by the discussion just before this proof, this occurs if and only if $\sigma_i^{-1} \tau \sigma_i \in G_F$, hence $\sigma^{-1} \mathrm{Gal}(L/K) \sigma \subseteq G_F$. □

**Remark 1.15.** *We can actually use Theorem 1.14 to prove Theorem 1.9. Consider* $F = \prod_{1 \le i < j \le n} (x_i - x_j) \in \mathbb{Q}[x_1, \dots, x_n]$ *and a monic, irreducible and separable polynomial of degree* $n$ *in* $\mathbb{Z}[x]$ *which has zeros* $\{a_1, \dots, a_n\}$. *Let* $\sigma \in S_n$, *then* $\sigma F = sgn(\sigma) F$, *hence the stabilizer is precisely* $A_n$. *Then our resolvent polynomial:*

$$\begin{aligned} r_{S_n, F}(f)(y) = & \prod_{\sigma_i \in S_n / A_n} (y - (\sigma_i F)), \quad x_i \mapsto a_i \\ = & (y - F)(y + F), \quad x_i \mapsto a_i \\ = & (y - \sqrt{\Delta})(y + \sqrt{\Delta}) \\ = & y^2 - \Delta \end{aligned}$$

*Note* $\Delta = \prod (a_i - a_j) \neq 0$ *because* $f$ *is separable, hence this resolvent is separable as well. Therefore* $y^2 - \Delta$ *has a solution in* $\mathbb{Q}$ *if and only if* $\mathrm{Gal}_f \subseteq A_n$ *(up to conjugacy, but since* $A_n$ *is a normal subgroup of* $S_n$, *no conjugation is needed). In fact, Theorem 1.9 does not hold for monic polynomials only. Let* $a_n$ *be the leading coefficient of* $f$ *and multiply* $F$ *by a constant* $a_n^{n-1}$, *the above discussion holds as well after referring to the definition of the discriminant of a general polynomial.*

Now I present a theorem which is sometimes much easier to use than using resolvents.

**Theorem 1.16** (Dedekind's Theorem)**.** *Let* $f(x)$ *be a separable and irreducible polynomial of degree* $n$ *in* $\mathbb{Z}[x]$, *and*

$$\varphi : \mathbb{Z}[x] \to \mathbb{F}_p[x], \quad \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \overline{a_i} x^i$$

*be the map of reduction modulo a prime number p. Assume $\varphi(f)$ is also separable and has the same degree as f, and $\varphi(f) = f_1^* \dots f_m^*$ where each $f_i^*$ is irreducible over $\mathbb{F}_p$, then $\mathrm{Gal}_f$, the Galois group of the splitting field of f over $\mathbb{Q}$, contains a permutation which is a product of cycles of lengths $deg(f_1^*), \dots deg(f_m^*)$.*

*Proof.* See, for example, Chapter VII section 2 of [3]. □

**Remark 1.17.** *In this paper we are only considering monic polynomials, thus the degree is always preserved under reduction. Note that in general, if G is a transitive subgroup of $S_n$ having a large index, it's impossible to conclude $\mathrm{Gal}_f \cong G$ using only Dedekind's Theorem, because that would be equivalent to proving that for all p, $f(x)$ factorizes into certain forms over $\mathbb{F}_p$. (See Example 4.5).*

## 1.3 Discussion on the reducibility of a polynomial

As noted in previous sections, it is crucial to know whether a given polynomial is reducible or not before we apply theorems, thus, in this section, we explore some common ways to do that.

**Theorem 1.18** (Lemma of Gauss). *Let $f(x) \in \mathbb{Z}[x]$ be monic. If $g(x) \in \mathbb{Q}[x]$ is monic and divides $f(x)$, then $g(x) \in \mathbb{Z}[x]$ as well.*

*Proof.* This is a very famous result from algebra, thus I state it without proof. The proof can be found in many textbooks, for instance, chapter 11 section 3 of [4]. □

**Remark 1.19.** *Note that it means if $f(x) \in \mathbb{Z}[x]$ is monic and (non-trivially) reducible in $\mathbb{Q}[x]$, then its factors are monic (up to product with a unit) and have their coefficients in $\mathbb{Z}$ as well. Put another way, this means the reducibility of a monic polynomial with integer coefficients over $\mathbb{Q}$ is equivalent to its reducibility over $\mathbb{Z}$.*

**Theorem 1.20** (Eisenstein's criterion). *Let $f(X) = a_n x^n + a_{n-1}x^{x-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there exists a prime number p such that:*

- *p divides each $a_i$ for $0 \leq i < n$*
- *p does not divide $a_n$*
- *$p^2$ does not divide $a_0$*

*then $f(x)$ is irreducible over $\mathbb{Q}$.*

*Proof.* See, for instance, page 404 of [4]. □

**Remark 1.21.** *Note that the irreducible polynomials which satisfy the Eisenstein's criterion are only small portion of all irreducible polynomials. In a paper [5], it is shown that less than 1 percent of polynomials with at least 7 non-zero coefficients satisfy the Eisenstein's criterion; on the other hand, there are $p^n$*

*polynomials of degree $n$ in $\mathbb{F}_p[x]$, out of which $\frac{1}{n}\sum_{d|n}\mu(d)p^d$ polynomials are irreducible (see page 588 of [6]). For example, on $\mathbb{F}_5$ there are $5^7 = 78125$ polynomials of degree 5, and 11160 of them are irreducible, which accounts for a proportion much greater than 1 percent.*

**Theorem 1.22.** *Let $f$ be a polynomial over $\mathbb{Z}$. If $f$ splits into linear factors, then $\Delta(f)$, the discriminant of $f$, is a square in $\mathbb{Z}$.*

*Proof.* Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, then its discriminant is

$$\begin{aligned}\Delta(f) &= a_n^{2n-2} \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2 \\ &= \prod_{1\le i<j\le n} (a_n^{n-1}\alpha_i - a_n^{n-1}\alpha_j)^2\end{aligned}$$

where the $\alpha_i$ are the zeros of $f(x)$. Take an arbitrary $\alpha_i$. Construct a monic polynomial $g(x)$ in $\mathbb{Z}[x]$ such that after evaluation at $a_n^{n-1}\alpha_i$, every term has a common factor $a_n^{n^2-n-1}$:

$$\begin{aligned}g(x) =& x^n + a_{n-1}a_n x^{n-1} + \ldots + a_1 a_n^{n^2-2n} x a_0 a_n^{n^2-n-1} \\ g(a_n^{n-1}\alpha_i) =& a_n^{n^2-n-1} \cdot a_n\alpha_i^n + a_n^{n^2-n-1} \cdot a_{n-1}\alpha_i^{n-1} + \ldots \\ &+ a_n^{n^2-n-1} \cdot a_1\alpha_i + a_n^{n^2-n-1} \cdot a_0 \\ =& a_n^{n^2-n-1} f(\alpha_i) \\ =& 0.\end{aligned}$$

Thus $a_n^{n-1}\alpha_i$ are zeros of $g(x)$. But by Theorem 1.18, $a_n^{n-1}\alpha_i$ must be integers, hence $\Delta(f) = a_n^{2n-2}\prod_{1\le i<j\le n}(\alpha_i - \alpha_j)^2$ must be square in $\mathbb{Z}$. □

**Remark 1.23.** *The above theorem actually holds not just for $\mathbb{Z}$, but also for all domains; see [7] for more information. Notice the similarity and difference with Theorem 1.9, which proved a necessary and sufficient condition about when $\Delta(f)$ is a square in $\mathbb{Q}$, assuming $f(x)$ is irreducible in the first place; while in our current theorem, we assumed $f(x)$ splits into linear products then we arrive at a direct consequence of this: $\Delta(f)$ is a square in $\mathbb{Z}$.*

**Theorem 1.24.** *Let $f$ be a polynomial over $\mathbb{Z}$ of degree $n$. If $f$ is irreducible over $\mathbb{Z}$, then*

$$|\Delta(f)| \ge \frac{\pi^{\frac{n}{2}} n^n}{2^n n!}$$

*where $\Delta(f)$ is the discriminant of $f$.*

*Proof.* This is a direct consequence of a theorem called *Minkowski's bound* or *Minkowski's constant*. The proof can be found, for instance, chapter V section 4 of [8]. □

**Remark 1.25.** *By elementary logic ($A \Rightarrow B$ means not $A$ or $B$), this theorem also means that, either $f$ is not irreducible or $|\Delta(f)| \geq \frac{\pi^{\frac{n}{2}} n^n}{2^n n!}$, which is equivalent to say $|\Delta(f)| < \frac{\pi^{\frac{n}{2}} n^n}{2^n n!} \Rightarrow f$ is reducible. This could be helpful when discussing reducibility of polynomials. However, this theorem is not a good tool to detect reducible polynomials, because the discriminants tend to be much larger than the bound. A somewhat trivial example is when $n = 2$, the bound is $\pi/2 = 1.57...$, consider $f(x) = x^2+3x+2$ having discriminant $1 < 1.57$, so it must be reducible. In fact $f(x) = (x+1)(x+2)$.*

## 2 Polynomials of degrees of 1, 2 and 3

The case of degree 1 is trivial, as there is only one subgroup of $S_1$. The case of degree 2 is similar, there are only two subgroups of $S_2$. Let $f(x) = x^2 + a_1x + a_0$ be an arbitrary monic polynomial in $\mathbb{Z}[x]$. If its discriminant $\Delta(f) = a_1^2 - 4a_0$ is a square in $\mathbb{Q}$ then the zeros of $f(x)$, $-a_1 \pm \sqrt{a_1^2 - 4a_0}$, are in $\mathbb{Q}$ as well, hence $\mathrm{Gal}_f$ only consists of identity; otherwise its Galois group is isomorphic to $S_2$. Thus the remaining of this section will only concern polynomials of degree 3.

### 2.1 Irreducible polynomials

Let $f(x) = x^3 + a_2x^2 + a_1x + a_0$ be an arbitrary monic irreducible polynomial in $\mathbb{Z}[x]$ and $L$ be its splitting field over $\mathbb{Q}$. Thus $|\mathrm{Gal}(L/\mathbb{Q})|$ divides $|S_3| = 6$, and by Theorem 1.7, 3 divides $|\mathrm{Gal}(L/\mathbb{Q})|$, hence $|\mathrm{Gal}(L/\mathbb{Q})| = 3$ or 6. The only subgroup of $S_3$ of order 3 is $A_3$, which consists of even permutations only, and $S_3$ itself consists of both odd and even permutations, thus Theorem 1.9, which points out the connection between discriminant and even permutations, would be helpful here.
First, we need to calculate the discriminant of $f$, this can be done with the help of the resultant and Theorems 1.12 and 1.10:

$$\begin{aligned}
\Delta(f) =&(-1)^{\frac{1}{2}3\cdot 2} Res(f, f') = -Res(f, f') \qquad \text{by Thm 1.12} \\
=&(-1)(-1)^{3\cdot 2} Res(f', f) = -Res(f', f) \qquad \text{by Thm 1.10(1)} \\
=&-3^2 \cdot Res(3x^2 + 2a_2x + a_1, (\frac{2a_1}{3} - \frac{2a_2^2}{9})x + a_0 - \frac{a_1a_2}{9}) \qquad \text{by Thm 1.10(3)} \\
=&-9(-1)^{2\cdot 1} \cdot Res((\frac{2a_1}{3} - \frac{2a_2^2}{9})x + a_0 - \frac{a_1a_2}{9}, 3x^2 + 2a_2x + a_1) \quad \text{by Thm 1.10(1)} \\
=&-9 \cdot (\frac{2a_1}{3} - \frac{2a_2^2}{9})^2 \cdot (a_1 + 2a_2(\frac{a_1a_2}{9} - a_0)/(\frac{2a_1}{3} - \frac{2a_2^2}{9}) \\
&+ 3((\frac{a_1a_2}{9} - a_0)/(\frac{2a_1}{3} - \frac{2a_2^2}{9}))^2) \qquad \text{by Thm 1.10(2)} \\
=&-27a_0^2 - 4a_1^3 + 18a_0a_1a_2 + a_1^2a_2^2 - 4a_0a_2^3.
\end{aligned}$$

We can also transform $f(x)$ to a simpler polynomial in the form of $x^3 + px + q$, the discriminant of which is easier to compute, and it generally gives us more insight into its zeros. This will be presented below.

Write $f(x)$ in terms of its three roots, expand and compare with the original polynomial, we have:

$$\begin{aligned}
f(x) &= (x - x_1)(x - x_2)(x - x_3) \\
&= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3 \\
&= x^3 + a_2x^2 + a_1x + a_0
\end{aligned}$$

Note that if we substitute $x = y - \frac{a_2}{3}$ we have a 3rd-degree polynomial $h(y)$ in the form as $h(y) = y^3 + py + q$, and the roots of $h$ and $f$ differ by a fixed rational constant $\frac{a_2}{3}$, thus the Galois groups with respect to them are the same. Writing out the process explicitly:

$$\begin{aligned}
h(y) &= (y - \frac{a_2}{3})^3 + a_2(y - \frac{a_2}{3})^2 + a_1(y - \frac{a_2}{3}) + a_0 \\
&= y^3 - a_2y^2 + \frac{1}{3}a_2^2y - \frac{1}{27}a_2^3 + a_2y^2 - \frac{2}{3}a_2^2y + \frac{1}{9}a_2^3 + a_1y - \frac{1}{3}a_1a_2 + a_0 \\
&= y^3 + (-\frac{1}{3}a_2^2)y + (\frac{2}{27}a_2^3 - \frac{1}{3}a_1a_2 + a_0) \\
&= y^3 + py + q
\end{aligned}$$

Thus $p = -\frac{1}{3}a_2^2$ and $q = \frac{2}{27}a_2^3 - \frac{1}{3}a_1a_2 + a_0$.
Next, we would like to compute the discriminant of $h$. Let $x_1, x_2, x_3$ be its roots, expand $(x - x_1)(x - x_2)(x - x_3)$ and compare coefficients, we have:

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = p \\ x_1x_2x_3 = -q \end{cases}$$

which leads to:

$$\begin{aligned}
(x_1 - x_2)^2 &= (x_1 + x_2)^2 - 4x_1x_2 \\
&= x_3^2 + \frac{4q}{x_3}
\end{aligned}$$

and similar results for $(x_1 - x_3)^2$ and $(x_3 - x_2)^2$. Thus:

$$\begin{aligned}
\Delta =&(x_1 - x_2)^2(x_1 - x_3)^2(x_3 - x_2)^2 \\
=&\left(x_3^2 + \frac{4q}{x_3}\right)\left(x_1^2 + \frac{4q}{x_1}\right)\left(x_2^2 + \frac{4q}{x_2}\right) \\
=&\frac{(x_1x_2x_3)^3 + 16q^2\left(x_1^3 + x_2^3 + x_3^3\right) + 4q\left(x_1^3x_2^3 + x_2^3x_3^3 + x_3^3x_1^3\right) + 64q^3}{x_1x_2x_3} \\
=&\frac{63q^3 + 16q^2\left(x_1^3 + x_2^3 - (x_1 + x_2)^3\right) + 4q\left((px_1 + q)(px_2 + q) +\right)}{x_1x_2x_3} \\
&+ \frac{(px_1 + q)(px_3 + q) + (px_2 + q)(px_3 + q)}{x_1x_2x_3} \\
=& - 4p^3 - 27q^2
\end{aligned}$$

Thus, by Theorem 1.9, if $\sqrt{\Delta} \in \mathbb{Q}$, the Galois group with respect to this polynomial consists of even permutations only, and hence it must be isomorphic to $A_3$; if $\sqrt{\Delta} \notin \mathbb{Q}$, then the Galois group is isomorphic to $S_3$.

## 2.2 Reducible polynomials

Let $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ be reducible, then there are a few different cases to be considered:

- Case 1: $f(x) = (x - a)(x - b)(x - c)$ where $a, b, c \in \mathbb{Z}$

If this case happens, by Theorem 1.22, its discriminant is a square of an integer. In this case $\mathrm{Gal}_f$ is trivial as $f(x)$ has rational roots only.

- Case 2: $f(x) = (x^2 + ax + b)(x - c)$ where $(x^2 + ax + b)$ is irreducible over $\mathbb{Q}$ and $a, b, c \in \mathbb{Z}$

This case can be identified when $f(x)$ is reducible and contains only one integer root. In this case, $\mathrm{Gal}_f$ is the same as the Galois group of the splitting field over $\mathbb{Q}$ of $x^2 + ax + b$, which has been discussed in the beginning of this section.

## 2.3 Examples

**Example 2.1.** *Let $f(x) = x^2 - 3x + 2$, which does not have real zeors. Its zeros are:*

$$x = \frac{3 \pm \sqrt{17}i}{2}$$

*thus $\mathrm{Gal}_f \cong S_2$, and the action of its element is complex conjugation.*

**Example 2.2.** *Let $f(x) = x^3 - 2$, its discriminant is $-108$ which is not a square in $\mathbb{Q}$, thus $\mathrm{Gal}_f \cong S_3$.*
*The actions of elements in $\mathrm{Gal}_f$ can be seen intuitively by plotting its roots in the complex plane in figure 1:*

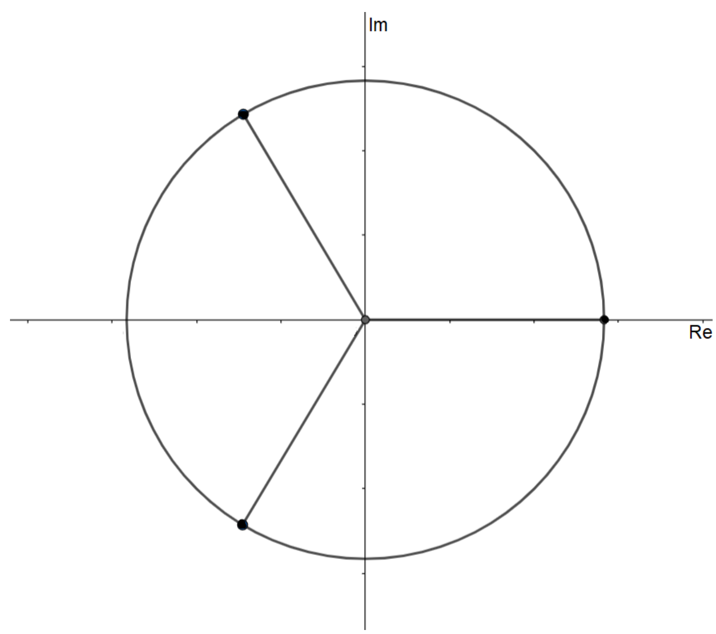


Figure 1: Roots of $x^3 - 2$ in complex plane

*Note $S_3 \cong \langle \sigma, \tau \rangle$ where $\sigma^3 = e$ and $\tau^2 = e$, thus here $\sigma$ corresponds to rotating the roots by 120 degrees and $\tau$ corresponds to flipping the roots about the x-axis.*

**Example 2.3.** *Let $f(x) = x^3 + x^2 - 2x - 1$, its discriminant is $49 = 7^2$, thus $\mathrm{Gal}_f \cong A_3 \cong \mathbb{Z}_3$.*
*The actions of elements in $\mathrm{Gal}_f$ can be seen by inspecting its three roots:*

$$x_1 = \varepsilon + \varepsilon^6$$
$$x_2 = \varepsilon^2 + \varepsilon^5$$
$$x_3 = \varepsilon^3 + \varepsilon^4$$

*where $\varepsilon$ is a primitive 7th root of unity (so $\varepsilon^7 = 1$ and $\varepsilon \neq 1$, in other words, $\varepsilon^6 + \varepsilon^5 + \varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0$). Note that*

$$\begin{aligned} x_1^2 &= (\varepsilon + \varepsilon^6)^2 \\ &= \varepsilon^2 + \varepsilon^{12} + 2 \cdot \varepsilon^{1+6} \\ &= \varepsilon^2 + \varepsilon^5 + 2 \\ &= x_2 + 2 \end{aligned}$$

*Similarly:*

$$x_2^2 = x_3 + 2, \quad x_3^2 = x_1 + 2,$$

*Hence the action of elements of $\mathrm{Gal}_f$ on the set of zeros is squaring and subtracting 2.*

# 3 Polynomials of degree of 4

## 3.1 Irreducible polynomials

Let $f(x)$ be an arbitrary monic irreducible polynomial in $\mathbb{Z}[x]$ and $L$ be its splitting field over $\mathbb{Q}$. Thus $|\mathrm{Gal}(L/\mathbb{Q})|$ divides $|S_4| = 24$, and by Theorem 1.7, 4 divides $|\mathrm{Gal}(L/\mathbb{Q})|$, hence $|\mathrm{Gal}(L/\mathbb{Q})| = 4, 8, 12, 24$. Thus, first of all, we make a classification of these transitive subgroups, and we only need them up to conjugacy within $S_4$, as we can always re-lable the zeros of $f(x)$.

- $V_4 = \{e, (12)(34), (13)(24), (14)(23)\} = \langle (14)(23), (12)(34)\rangle$, the Klein four-group which is normal in $S_4$.
- $D_4 = V_4 \cup \{(1243), (1342), (14), (23)\} = \langle (1234), (13)\rangle$, the dihedral group. In fact, there are three such subgroups in total, the other two are $V_4 \cup \{(1324), (1423), (12), (34)\}$ and $V_4 \cup \{(1234), (1432), (13), (24)\}$ and they are all conjugate in $S_4$.
- $Z_4 \cong \langle (1234)\rangle = \{e, (1234), (13)(24), (1432)\}$, the cyclic group of order 4. In fact there are 3 such subgroups, the remaining 2 are $\langle (1324)\rangle = \{e, (1324), (12)(34), (1423)\}$ and $\langle (1243)\rangle = \{e, (1243), (14)(23), (1342)\}$, and of course they are all conjugate in $S_4$.
- $A_4$.
- $S_4$.

There is another class of subgroups of order 4, the non-normal Klein four-group, which is $\langle (12), (34)\rangle = \{e, (12), (34), (12)(34)\}$ (or any of the 6 subgroups conjugate to this one in $S_4$). This group is clearly not transitive because, for example, no element in it maps 1 to 3. The above are the only classes of subgroups of order 4, 8, 12, 24 of $S_4$ and 5 of them are transitive.
It is not hard to describe the subgroup structure of these groups, which is summarized in Figure 2 in the next page, where $G_1 \to G_2$ means $G_1 \supset G_2$ (in general, after possibly conjugating $G_2$ inside $S_4$, but for the specific subgroups presented above no conjugation is needed).

Let $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ be monic and irreducible. The discriminant of $f(x)$ can be calculated, with the help of resultant, by using Theorem 1.12 and Theorem 1.10 to be:

$$\begin{aligned}\Delta =& 144a_0^2a_2a_3^2 + 18a_1^3a_2a_3 - 192a_0^2a_1a_3 - 6a_0a_1^2a_3^2 + 144a_0a_1^2a_2 - 4a_0a_2^3a_3^2\\ &+ a_1^2a_2^2a_3^2 + 256a_0^3 - 27a_1^4 + 18a_0a_1a_2a_3^3 - 4a_1^3a_3^3 - 128a_0^2a_2^2 + 16a_0a_2^4\\ &- 4a_1^2a_2^3 - 27a_0^2a_3^4 - 80a_0a_1a_2^2a_3.\end{aligned}$$

By the following command in Magma (freely available online at `http://magma.maths.usyd.edu.au/calc/`), we can find an $F \in \mathbb{Q}[x_1, \ldots, x_4]$ that has $D_4$ as stabilizer:

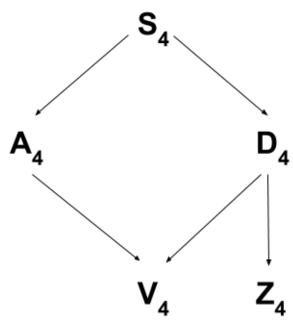


Figure 2: Structure of transitive subgroups of $S_4$

```
Q:=Rationals();
D4:=MatrixGroup<4,Q | [0,0,0,1, 1,0,0,0, 0,1,0,0, 0,0,1,0],
[0,0,1,0, 0,1,0,0, 1,0,0,0, 0,0,0,1]>;
InvariantsOfDegree(D4,2);
```

I chose $F = x_1x_3+x_2x_4$ here. The action of $S_4$ on $F = x_1x_3+x_2x_4$ clearly gives three different polynomials, namely $x_1x_3 + x_2x_4$, $x_1x_2 + x_3x_4$ and $x_1x_4 + x_2x_3$ (which is equivalent to say that the elements in $S_4/D_4$ are $e$, (23) and (34)). Hence the resolvent polynomial of $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ with respect to $F$ and $D_4$ equals:

$$r(y) = r_{D_4,F}(f)(y) = (y-(\alpha_1\alpha_3+\alpha_2\alpha_4))(y-(\alpha_1\alpha_2+\alpha_3\alpha_4))(y-(\alpha_1\alpha_4+\alpha_2\alpha_3))$$

where $\alpha_i$ are zeros of $f(x)$. Vieta's formula for $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = \prod_{i=1}^{4}(x - \alpha_i)$ gives:

$$\begin{aligned}
a_3 &= -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)\\
a_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_3\alpha_4\\
a_1 &= -(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4)\\
a_0 &= \alpha_1\alpha_2\alpha_3\alpha_4
\end{aligned}$$

Expand $r(y)$:

$$\begin{aligned}
r(y) =& y^3 - ((\alpha_1\alpha_2 + \alpha_3\alpha_4) + (\alpha_1\alpha_3 + \alpha_2\alpha_4) + (\alpha_1\alpha_4 + \alpha_2\alpha_3))y^2 \\
&+ ((\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_1\alpha_3 + \alpha_2\alpha_4) + (\alpha_1\alpha_3 + \alpha_2\alpha_4)(\alpha_1\alpha_4 + \alpha_2\alpha_3) \\
&+ (\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_1\alpha_4 + \alpha_2\alpha_3))y \\
&- ((\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_1\alpha_3 + \alpha_2\alpha_4)(\alpha_1\alpha_4 + \alpha_2\alpha_3)) \\
=& y^3 - (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_3\alpha_4)y^2 \\
&+ (\alpha_1^2\alpha_2\alpha_3 + \alpha_1\alpha_2^2\alpha_4 + \alpha_1\alpha_3^2\alpha_4 + \alpha_2\alpha_3\alpha_4^2 + \alpha_1^2\alpha_3\alpha_4 \\
&+ \alpha_1\alpha_2\alpha_3^2 + \alpha_1\alpha_2\alpha_4^2 + \alpha_2^2\alpha_3\alpha_4 + \alpha_1^2\alpha_2\alpha_4 + \alpha_1\alpha_2^2\alpha_3 + \alpha_1\alpha_3\alpha_4^2 \\
&+ \alpha_2\alpha_3^2\alpha_4)y - \alpha_1^3\alpha_2\alpha_3\alpha_4 - \alpha_1^2\alpha_2^2\alpha_3^2 - \alpha_1^2\alpha_2^2\alpha_4^2 \\
&- \alpha_1\alpha_2^3\alpha_3\alpha_4 - \alpha_1^2\alpha_3^2\alpha_4^2 - \alpha_1\alpha_2\alpha_3^3\alpha_4 - \alpha_1\alpha_2\alpha_3\alpha_4^3 - \alpha_2^2\alpha_3^2\alpha_4^2
\end{aligned}$$

Compare coefficients of the expansion with Vieta's formula, we have:

$$r(y) = y^3 - a_2y^2 + (a_1a_3 - 4a_0)y - a_1^2 - a_0a_3^2 + 4a_0a_2$$

To describe the Galois group $G = Gal_f$ of the splitting field $L$ over $\mathbb{Q}$ of $f(x)$, there are a few cases to be considered.

- Case 1: $r(y)$ is irreducible over $\mathbb{Q}$

Since $r(y)$ is of degree 3 and is irreducible, it does not have a zero in $\mathbb{Q}$ and moreover it is separable. Hence by Theorem 1.14, $\mathrm{Gal}_f$ cannot be a subgroup of $D_4$, so it is either $A_4$ or $S_4$, and this can be checked by whether $\sqrt{\Delta} \in \mathbb{Q}$ and apply Theorem 1.9.
Alternatively, we have that both $f(x)$ and $r(y)$ are irreducible over $\mathbb{Q}$, so they are minimal polynomials of $\alpha_1$ and $\alpha_1\alpha_2 + \alpha_3\alpha_4 \in L$ respectively. Thus, by the tower law, $[L : \mathbb{Q}]$ must be divisible by 3 and 4, the degrees of $f(x)$ and $r(y)$, and hence $|G| = |\mathrm{Gal}(L/\mathbb{Q})|$ must also be divisible by 3 and 4. From the list of transitive subgroups of $S_4$ we can see that only $A_4$ and $S_4$ satisfy this. Therefore, by Theorem 1.9, if $\sqrt{\Delta} \in \mathbb{Q}$ we have $G = A_4$, otherwise $G = S_4$.

- Case 2: $r(y)$ is reducible over $\mathbb{Q}$

Since $r(y)$ is of degree 3 and is reducible over $\mathbb{Q}$, it must has a zero $b \in \mathbb{Q}$, thus Theorem 1.14 applies here (provided $r(y)$ is separable), hence $\mathrm{Gal}_f$ must be one of $D_4$, $V_4$ or $Z_4$. Next, if $\sqrt{\Delta(f)} \in \mathbb{Q}$ by Theorem 1.9 we have $Gal_f \subseteq A_4$, and out of $V_4$, $Z_4$ and $D_4$ only $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ satisfies this, thus in this case $Gal_f = V_4$.

Now assume $\sqrt{\Delta(f)} \notin \mathbb{Q}$. Without loss of generality, let the zero $b = \alpha_1\alpha_2 + \alpha_3\alpha_4 \in \mathbb{Q}$ (as we can always re-label the $\alpha_i$ to make this happen), by using

Vieta's formula mentioned before, it can be shown that :

$$\begin{aligned}4b - a_3^2 - 4a_2 =& 4(\alpha_1\alpha_2 + \alpha_3\alpha_4) - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^2 \\ & - 4(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_3\alpha_4) \\ =& 4\alpha_1\alpha_2 + 4\alpha_3\alpha_4 - (2\alpha_1\alpha_2 + 2\alpha_1\alpha_3 + 2\alpha_1\alpha_4 + \alpha_1^2 + \alpha_2^2 \\ & + 2\alpha_2\alpha_3 + \alpha_3^2 + 2\alpha_2\alpha_4 + 2\alpha_3\alpha_4 + \alpha_4^2) - 4\alpha_1\alpha_2 \\ & - 4\alpha_1\alpha_3 - 4\alpha_2\alpha_3 - 4\alpha_1\alpha_4 - 4\alpha_2\alpha_4 - 4\alpha_3\alpha_4 \\ =& \alpha_1^2 + 2\alpha_1\alpha_2 - 2\alpha_1\alpha_3 - 2\alpha_1\alpha_4 + \alpha_2^2 + \alpha_3^2 \\ & - 2\alpha_2\alpha_3 + \alpha_4^2 + 2\alpha_3\alpha_4 - 2\alpha_2\alpha_4 \\ =& (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2\end{aligned}$$

Thus we have:

$$\sqrt{4b + a_3^2 - 4a_2} = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4$$

Consider $\sqrt{\Delta(f)(4b + a_3^2 - 4a_2)} = \sqrt{\Delta(f)}(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_1)$, if this expression lies in $\mathbb{Q}$ then elements of $G$ must fix it, and out of the two remaining choices $D_4$ and $Z_4$ only the latter one does so, because (1324) is a generator of $Z_4$ (up to conjugacy), and:

$$\begin{cases}(1324)\sqrt{\Delta(f)} = -\sqrt{\Delta(f)} \\ (1324)(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4) = \alpha_3 + \alpha_4 - \alpha_2 - \alpha_1 = -(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)\end{cases}$$

Therefore (1324) fixes $\sqrt{\Delta(f)}(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4) = \sqrt{\Delta(f)(4b + a_3^2 - 4a_2)}$. Hence if $\sqrt{\Delta(f)(4b + a_3^2 - 4a_2)} \in \mathbb{Q}$ then $Gal_f = Z_4$, otherwise $Gal_f = D_4$. The previous argument fails when $4b + a_3^2 - 4a_2 = 0$, in this case, we use a similar expression

$$b^2 - 4a_0 = (\alpha_1\alpha_2 + \alpha_3\alpha_4)^2 - 4\alpha_1\alpha_2\alpha_3\alpha_4 = (\alpha_1\alpha_2 - \alpha_3\alpha_4)^2$$

and proceed the same way, it's easy to see that if $\sqrt{\Delta(f)\,(b^2 - 4a_0)} \in \mathbb{Q}$ then $Gal_f = Z_4$, otherwise $Gal_f = D_4$.

**Remark 3.1.** *To differentiate whether $Gal_f$ is isomorphic to $D_4$ or $Z_4$, various other methods exist, e.g. Dedekind's Theorem 1.16 or another resolvent with respect to $Z_4$. The end of section 4.1 explores such possibilities, where we have to find a way to differentiate $D_5$ or $Z_5$.*

## 3.2 Reducible polynomials

There are several cases to be considered:

- Case 1: $f$ splits into linear factors in $\mathbb{Q}[x]$

If this case happens, by Theorem 1.22, its discriminant is a square of an integer. In this case the Galois group is simply the identity, as it only has rational roots.

- Case 2: $f$ has only one irreducible factor of degree 2 or 3

In this case, $f(x) = (x-a)(x-b)g(x)$ or $f(x) = (x-a)h(x)$ where $g(x)$ and $h(x)$ are irreducible over $\mathbb{Q}$ and are of degrees 2 and 3 respectively. Then clearly $\mathrm{Gal}_f \cong \mathrm{Gal}_g$ or $\mathrm{Gal}_f \cong \mathrm{Gal}_h$ and we can apply results we already have.

- Case 3: $f$ has two irreducible factors of degree 2

Write $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are irreducible over $\mathbb{Q}$ and are of degrees 2. Let $L_f$, $L_g$ and $L_h$ denote the splitting field of $f(x)$, $g(x)$ and $h(x)$ over $\mathbb{Q}$ respectively. If $h(x)$ splits in $L_g[x]$, then $L_f = L_g$ and hence $Gal_f = Gal_g = S_2$ . Otherwise, $L_f$ is the same field as $L_g \supset L_h \supset \mathbb{Q}$ where $\supset$ denotes field extensions of degree 2, and hence

$$Gal_f = Gal_g \times Gal_h = S_2 \times S_2 \cong V_4$$

The case in which $Gal_f \cong S_2$, i.e. $g(x)$ and $h(x)$ share a common splitting field, can be identified by the following theorem.

**Theorem 3.2.** *Let $f(x) = g(x)h(x)$, $L_g$ and $L_h$ defined as above. Then $h(x)$ splits in $L_g$ if and only if $\Delta(g)\Delta(h)$ is a square in $\mathbb{Q}$.*

*Proof.* Write $g(x) = x^2 + ax + b$, $h(x) = x^2 + cx + d \in \mathbb{Z}[x]$ for the irreducible factors (they have to be of this form by Lemma of Gauss 1.18). Then $L_g = \mathbb{Q}(\sqrt{a^2-4b})$ which has a basis $\{1, \sqrt{a^2-4b}\}$. If $h(x)$ splits in $L_g[x]$, then there must exist $q_1, q_2 \in \mathbb{Q}$ such that:

$$\begin{aligned} & \sqrt{c^2-4d} = q_1 + q_2\sqrt{a^2-4b} \\ \Rightarrow \quad & \sqrt{c^2-4d} - q_2\sqrt{a^2-4b} = q_1 \\ \Rightarrow \quad & c^2 - 4d + q_2^2(a^2-4b) - 2q_2\sqrt{c^2-4d}\sqrt{a^2-4b} = q_1^2 \end{aligned}$$

which holds if and only if $\sqrt{c^2-4d}\sqrt{a^2-4b} \in \mathbb{Q}$. □

## 3.3 Examples

We use the following command in Mathematica:

```
IrreduciblePolynomialQ[x^4+a3 x^3+a2 x^2+a1 x+a0]
d=256 a0^3-27 a1^4+144 a0 a1^2 a2-128 a0^2 a2^2-4 a1^2 a2^3
+16 a0 a2^4-192 a0^2 a1 a3+18 a1^3 a2 a3-80 a0 a1 a2^2 a3
-6 a0 a1^2 a3^2+144 a0^2 a2 a3^2+a1^2 a2^2 a3^2-4 a0 a2^3 a3^2
-4 a1^3 a3^3+18 a0 a1 a2 a3^3-27 a0^2 a3^4;
Sqrt[d]
theta:=y^3 -a2 y^2 +(a1 a3-4a0) y-a1^2 -a3^2 a0 +4 a2 a0
```

```
Factor[theta]

f=4 beta - a3^2 -4a2
Sqrt[d f]
```

This command except for the last two lines, given integer values $a_3, \ldots, a_0$, returns whether $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ is irreducible, $\sqrt{\Delta(f)}$, the resolvent polynomial and its factorization. If the resolvent has a unique zero in $\mathbb{Q}$, set this zero to be $\beta$ and run the last two lines.

**Example 3.1.** *Let $f(x) = x^4 + 2x^3 + 4x^2 + 6x + 8$ which is irreducible, then $\sqrt{\Delta(f)} = 4\sqrt{2685} \notin \mathbb{Q}$, and the resolvent polynomial $\theta(y) = 60 - 20y - 4y^2 + y^3$ which is irreducible over $\mathbb{Q}$, hence Case 1 in Section 3.1 applies and $\mathrm{Gal}_f \cong S_4$.*

**Example 3.2.** *Let $f(x) = x^4 + 8x + 12$ which is irreducible, then $\sqrt{\Delta(f)} = 576 \in \mathbb{Q}$, and the resolvent polynomial $\theta(y) = -64 - 48y + y^3$ which is irreducible over $\mathbb{Q}$. Hence Case 1 in Section 3.1 applies and $\mathrm{Gal}_f \cong A_4$*

**Example 3.3.** *Let $f(x) = x^4 + 4x^2 + 5$ which is irreducible, then $\sqrt{\Delta(f)} = 16\sqrt{5} \notin \mathbb{Q}$, and the resolvent polynomial $\theta(y) = (-4 + y)(-20 + y^2)$ which has a unique zero $y = 4$ in $\mathbb{Q}$ and is clearly separable. Set $\beta = 4$ and run the 2nd part of command, we have $4\beta + a_3^2 - 4a_2 = 0$ so we cannot use $\sqrt{\Delta(4\beta + a_3^2 - 4a_2)}$ here. But $\beta + a_3^2 - 4a_0 = -4 \neq 0$, and $\sqrt{\Delta(\beta + a_3^2 - 4a_0)} = 32\sqrt{5}i \notin \mathbb{Q}$, thus Case 2 in Section 3.1 applies and $\mathrm{Gal}_f \cong D_4$.*

**Example 3.4.** *Let $f(x) = x^4 + 1$ which is irreducible, then $\sqrt{\Delta(f)} = 16 \in \mathbb{Q}$, and the resolvent polynomial $\theta(y) = y(-2 + y)(2 + y)$ which splits into linear factors over $\mathbb{Q}$. Hence Case 2 in Section 3.1 applies and $\mathrm{Gal}_f \cong V_4$*

**Example 3.5.** *Let $f(x) = x^4 + 3x^3 + 9x^2 + 27x + 81$ which is irreducible, then $\sqrt{\Delta(f)} = 3645\sqrt{5} \notin \mathbb{Q}$, and the resolvent polynomial $\theta(y) = (-18 + y)(-81 + 9y + y^2)$ which has a unique zero $y = 18$ in $\mathbb{Q}$ and is clearly separable. Set $\beta = 18$ and run the 2nd part of command, we have $4\beta + a_3^2 - 4a_2 = 27 \neq 0$ and $\sqrt{\Delta(4\beta + a_3^2 - 4a_2)} = 10935\sqrt{15} \notin \mathbb{Q}$, thus Case 2 in Section 3.1 applies and $\mathrm{Gal}_f \cong Z_4$.*

# 4 Polynomials of degree of 5

## 4.1 Irreducible polynomials

Let $f(x)$ be an arbitrary monic and irreducible polynomial in $\mathbb{Z}[x]$ and $L$ be its splitting field over $\mathbb{Q}$. Thus $|\mathrm{Gal}(L/\mathbb{Q})|$ divides $|S_5| = 120$, and by Theorem 1.7 since $f(x)$ is irreducible in $\mathbb{Q}[x]$, moreover 5 divides $|\mathrm{Gal}(L/\mathbb{Q})|$. Hence $|\mathrm{Gal}(L/\mathbb{Q})|$ is one of $5, 10, 15, 20, 30, 40, 60, 120$. Thus, first of all, we would like to make a list of the transitive subgroups, of $S_5$ (again, up to conjugacy):

- $Z_5 \cong \langle(12345)\rangle = \{e, (12345), (13524), (14253), (15432)\}$, the cyclic group of order 5. Subgroups of 5 (a prime number) must be cyclic, thus $Z_5$ is the only kind of subgroup of order 5 up to conjugacy.
- $D_5 = \langle(12345), (14)(23)\rangle$, the dihedral group of order 10. Furthermore, a subgroup of order 10 must contain an element of order 2 and an element of order 5 by Cauchy's theorem, the latter can only be a 5-cycle and the former can only be either a transposition or the form of (ab)(cd). If it's a transposition we get a group of order larger than 10 (in fact, $S_5 = \{\langle(12345), (12)\rangle\}$); if it's (ab)(cd) we get $D_5$. Thus $D_5$ is the only kind of subgroup of order 10 up to conjugacy.
- $GA(1, 5) = \langle(12345), (1243)\rangle$, the general affine group of order 20. There are 6 such subgroups and all are conjugate in $S_5$. For more information on affine groups, see, for example, page 27 of [9].
- $A_5$.
- $S_5$.

The uniqueness of these transitive subgroups are proved by the following theorem.

**Theorem 4.1.** *Let $G$ be a transitive subgroup of $S_5$, then $G$ is conjugate to one of the above groups.*

*Proof.* 5 must divide the order of $G$, thus $G$ must contain a 5-cycle (abcde), furthermore $G$ contains $Z_5 \cong \langle(abcde)\rangle$ as a subgroup, which is also a Sylow-5 group. By Sylow's theorem, the number of Sylow-5 groups as subgroups in $G$ is equal to 1 mod 5, and it divides $\#G$. Thus either $G$ has exactly 1 or exactly 6 subgroups of order 5 (in the latter case all 5-cycles in $S_5$ are in $G$).

- Case 1: $G$ has exactly 6 subgroups of order 5.

Note that in this case, since all 5-cycles are contained, all 3-cycles in $S_5$ can also be obtained via:

$$(ijk) = (likjm)(jiklm), \quad i, j, k, l, m = 1, 2, 3, 4, 5$$

Hence $G$ contains $A_5$, so it is either $A_5$ or $S_5$. The fact that $A_n$ is generated by the 3-cyclesin $S_n$ is a well-known fact in group theory.

- Case 2: $G$ has exactly 1 subgroup of order 5.

Without loss of generality, let (12345) be the generator of this subgroup. Note that, for all $g \in G$:

$$g \langle (12345) \rangle g^{-1} = \langle (12345) \rangle$$

hence $G$ is a subgroup of the normaliser

$$N(\langle (12345) \rangle) = \left\{ \sigma \langle (12345) \rangle \sigma^{-1} = \langle (12345) \rangle , \sigma \in S_5 \right\}$$

On page 414, lemma 14.1.2 of [1], it is proved that $N = GA(1,5)$ (in fact, it's proved there that in $S_p$, $N(\langle (12\dots p) \rangle) = GA(1,p)$, where $p$ is a prime). Transitive subgroups of $GA(1,5)$ must be of order 5, 10 or 20, in the discussion in the beginning of this section, we saw that they can only be $Z_5$, $D_5$ and $GA(1,5)$ and hence $G$ must be conjugate to one of them.

□

$GA(1,5)$ is the group of maps $i \mapsto ci + d$ where $c, d \in \mathbb{F}_5$ and $c \neq 0$. It is generated by translation by 1 and multiplication by 2 which correspond to (12345) and (1243) respectively. Note that $GA(1,5) \cap A_5 = \langle (12345), (14)(23) \rangle = D_5$, because:

$$\begin{aligned} GA(1,5) \cap A_5 = & \{e, (12345), (13524), (14253), (15432)\} \\ & \cup \{(14)(23), (15)(24), (25)(34), (12)(35), (13)(45)\} \\ = & \left\{ e, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b \right\} \end{aligned}$$

where $a = (12345)$ and $b = (14)(23)$.

**Remark 4.2.** *This can also be proved using the sign homomorphism $GA(1,5) \to \{\pm 1\}$, of which the kernel is a subgroup of order 10 consisting of the even permutations in $GA(1,5)$. In our discussion in the beginning of this section, we saw that $D_5$ is the only subgroup (up to conjugacy) of $S_5$ of order 10.*

Hence, the connection between the 5 transitive subgroups can be described by Figure 3 in the next page, where $G_1 \to G_2$ means $G_1 \supseteq G_2$ (after possibly conjugating $G_2$):
Thus, one way to solve our problem could be: first use a resolvent polynomial whose stabilizer is $GA(1,5)$, then consider whether the discriminant is a square in $\mathbb{Q}$ or not, if it is, then the Galois group is a subset of $A_5$. In this text, we use $h = u^2$, where

$$u = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_1x_5 - x_1x_3 - x_3x_5 - x_2x_5 - x_2x_4 - x_1x_4$$

It is clear that $u^2$ is fixed by $GA(1,5) = \langle (12345), (1243) \rangle$, thus we have $Stab(u^2) \supseteq GA(1,5)$. On the other hand, elements of $Stab(u^2)$ must belong to one of the 5 transitive subgroups of $S_5$ mentioned earlier; many elements in $A_5$ and $S_5$, for example $(123) \in A_5 \subset S_5$, do not fix $u^2$ while the generators of $GA(1,5)$ do, thus $Stab(u^2) \subseteq GA(1,5)$ hence we have equality.

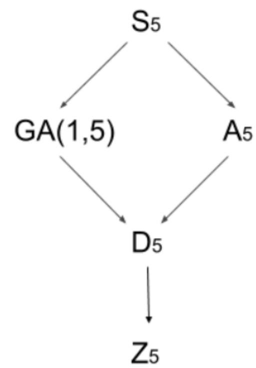


Figure 3: Structure of transitive subgroups of $S_5$

There are 6 coset representatives in $S_5/GA(1,5)$: (1), (123), (234), (345), (145) and (125), hence the resolvent polynomial $\theta(y)$ of $f(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, with respect to $h(x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}[x_1, x_2, x_3, x_4, x_5]$ and $GA_{1,5} \subset S_5$ is:

$$\begin{aligned}\theta_{GA(1,5),h}(y) &= \prod_{\tau \in S_5/GA(1,5)} (y - \tau h)(x_1, x_2, x_3, x_4, x_5), \quad x_i \mapsto \alpha_i \\ &= \prod_{i=1}^{6} (y - \tau_i h)(x_1, x_2, x_3, x_4, x_5), \quad x_i \mapsto \alpha_i \\ &= \prod_{i=1}^{6} (y - \tau_i h)(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)\end{aligned}$$

where $\tau_i$ are the six coset representatives and $\alpha_i$ are the roots of $f(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. For sake of simplicity we'll write $\theta(y)$ instead of $\theta_{GA(1,5),h}(y)$ from now on.
Note that if we define a new polynomial

$$\Gamma(y) = \prod_{i=1}^{6} (y - \tau_i u)$$

then $\theta(y)$ can be calculated with the help of $\Gamma(y)$:

$$\begin{aligned}
\theta(y^2) =& \prod_{i=1}^{6}(y^2 - \tau_i h) \\
=& \tau_i \prod_{i=1}^{6}(y^2 - h) \qquad \text{(as } \tau_i \in S_5 \text{ do not act on the indeterminate } y\text{)} \\
=& \tau_i \prod_{i=1}^{6}(y^2 - u^2) \\
=& \tau_i \prod_{i=1}^{6}(y - u)(y + u) \\
=& (-1)^6 \prod_{i=1}^{6}(y - \tau_i u)(-y - \tau_i u) \\
=& \Gamma(y)\Gamma(-y)
\end{aligned}$$

followed by replacing $y^2$ by $y$. The product ending up having even powers of $y$ only is a guaranteed result, as polynomials in $R[x]$ in the form $g(x)g(-x)$ must be invariant under the change of sign of $x$, where $R$ is commutative.

**Remark 4.3.** *In this section, as in the previous one, we will need some results that are too complicated to work out by hand, (for example, determining whether the resolvent has a root in* $\mathbb{Q}$ *and the explicit formula of the discriminant of a general quintic), and I would like to leave them to computer programs (e.g. Mathematica) where appropriate.*

In *Mathematica*, define the 6 $u$ as:

```
u1 := x1 x2 + x2 x3 + x3 x4 + x4 x5 + x1 x5 - x1 x3 - x3 x5 - x2 x5 -
  x2 x4 - x1 x4
u2 := u1 /. {x1 -> x2, x2 -> x3, x3 -> x1}
u3 := u1 /. {x2 -> x3, x3 -> x4, x4 -> x2}
u4 := u1 /. {x3 -> x4, x4 -> x5, x5 -> x3}
u5 := u1 /. {x1 -> x4, x4 -> x5, x5 -> x1}
u6 := u1 /. {x1 -> x2, x2 -> x5, x5 -> x1}
```

Then run the following:

```
Eliminate[{Gamma==(y - u1)(y - u2)(y - u3)(y - u4)(y - u5)(y - u6),
  e1 == x1 + x2 + x3 + x4 + x5,
  e2 == x1 x2 + x1 x3 + x1 x4 + x1 x5 + x2 x3 + x2 x4 + x2 x5 +
    x3 x4 + x3 x5 + x4 x5,
  e3 == x1 x2 x3 + x1 x2 x4 + x1 x2 x5 + x1 x3 x4 + x1 x3 x5 +
    x1 x4 x5 + x2 x3 x4 + x2 x3 x5 + x2 x4 x5 + x3 x4 x5,
  e4 == x1 x2 x3 x4 + x1 x2 x3 x5 + x1 x2 x4 x5 + x1 x3 x4 x5 +
    x2 x3 x4 x5,
  e5 == x1 x2 x3 x4 x5}, {x1, x2, x3, x4, x5}]
```

By the result and the expression for $\sqrt{\Delta}$, we have:

$$\Gamma(y) = y^6 + B_2 y^4 + B_4 y^2 + B_6 - 2^5\sqrt{\Delta}y$$

where $\Delta$ is the discriminant of $f(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$,

$$\begin{aligned}
B_2 =& 8\sigma_1\sigma_3 - 3\sigma_2^2 - 20\sigma_4 \\
B_4 =& 3\sigma_2^4 - 16\sigma_1\sigma_2^2\sigma_3 + 16\sigma_1^2\sigma_3^2 + 16\sigma_2\sigma_3^2 + 16\sigma_1^2\sigma_2\sigma_4 - 8\sigma_2^2\sigma_4 \\
& - 112\sigma_1\sigma_3\sigma_4 + 240\sigma_4^2 - 64\sigma_1^3\sigma_5 + 240\sigma_1\sigma_2\sigma_5 - 400\sigma_3\sigma_5 \\
B_6 =& 8\sigma_1\sigma_2^4\sigma_3 - \sigma_2^6 - 16\sigma_1^2\sigma_2^2\sigma_3^2 - 16\sigma_2^3\sigma_3^2 + 64\sigma_1\sigma_2\sigma_3^3 - 64\sigma_3^4 \\
& - 16\sigma_1^2\sigma_2^3\sigma_4 + 28\sigma_2^4\sigma_4 + 64\sigma_1^3\sigma_2\sigma_3\sigma_4 - 112\sigma_1\sigma_2^2\sigma_3\sigma_4 \\
& - 128\sigma_1^2\sigma_3^2\sigma_4 + 224\sigma_2\sigma_3^2\sigma_4 - 64\sigma_1^4\sigma_4^2 + 224\sigma_1^2\sigma_2\sigma_4^2 \\
& - 176\sigma_2^2\sigma_4^2 - 64\sigma_1\sigma_3\sigma_4^2 + 320\sigma_4^3 + 48\sigma_1\sigma_2^3\sigma_5 - 192\sigma_1^2\sigma_2\sigma_3\sigma_5 \\
& - 80\sigma_2^2\sigma_3\sigma_5 + 640\sigma_1\sigma_3^2\sigma_5 + 384\sigma_1^3\sigma_4\sigma_5 - 640\sigma_1\sigma_2\sigma_4\sigma_5 \\
& - 1600\sigma_3\sigma_4\sigma_5 - 1600\sigma_1^2\sigma_5^2 + 4000\sigma_2\sigma_5^2
\end{aligned}$$

and $\sigma_i$ are elementary symmetric polynomials. Now

$$\begin{aligned}
\theta\left(y^2\right) &= \Gamma(y)\Gamma(-y) \\
&= \left(y^6 + B_2y^4 + B_4y^2 + B_6\right)^2 - 2^{10}\Delta \cdot y^2
\end{aligned}$$

and replace $y^2$ by $y$, we have

$$\theta(y) = \left(y^3 + B_2y^2 + B_4y + B_6\right)^2 - 2^{10}\Delta \cdot y$$

After evaluation $x_i \mapsto \alpha_i$, we also have $\sigma_i \mapsto a_i \in \mathbb{Z}$ and hence the resolvent $\theta(y) \in \mathbb{Z}[y]$ indeed, which can also be inferred from Theorem 1.13.
We could use Theorems 1.10 and 1.12 to compute $\Delta$ explicitly, but it's too much of work to do polynomial division manually, so we can use tools like *Mathematica* or *Maple* to do it. In *Mathematica*, run

```
Discriminant[x^5 + a4 x^4 + a3 x^3 + a2 x^2 + a1 x + a0, x]
```

we have:

$$
\begin{aligned}
\Delta =&256a_4^5a_0^3 - 192a_4^4a_3a_1a_0^2 - 128a_4^4a_2^2a_0^2 + 144a_4^4a_2a_1^2a_0 - 27a_4^4a_1^4 + 144a_4^3a_3^2a_2a_0^2 \\
&- 6a_4^3a_3^2a_1^2a_0 - 80a_4^3a_3a_2^2a_1a_0 + 18a_4^3a_3a_2a_1^3 - 1600a_4^3a_3a_0^3 + 16a_4^3a_2^4a_0 - 4a_4^3a_2^3a_1^2 \\
&+ 160a_4^3a_2a_1a_0^2 - 36a_4^3a_1^3a_0 - 27a_4^2a_3^4a_0^2 + 18a_4^2a_3^3a_2a_1a_0 - 4a_4^2a_3^3a_1^3 - 4a_4^2a_3^2a_2^3a_0 \\
&+ a_4^2a_3^2a_2^2a_1^2 + 1020a_4^2a_3^2a_1a_0^2 + 560a_4^2a_3a_2^2a_0^2 - 746a_4^2a_3a_2a_1^2a_0 + 144a_4^2a_3a_1^4 \\
&+ 24a_4^2a_2^3a_1a_0 - 6a_4^2a_2^2a_1^3 + 2000a_4^2a_2a_0^3 - 50a_4^2a_1^2a_0^2 - 630a_4a_3^3a_2a_0^2 + 24a_4a_3^3a_1^2a_0 \\
&+ 356a_4a_3^2a_2^2a_1a_0 - 80a_4a_3^2a_2a_1^3 + 2250a_4a_3^2a_0^3 - 72a_4a_3a_2^4a_0 + 18a_4a_3a_2^3a_1^2 \\
&- 2050a_4a_3a_2a_1a_0^2 + 160a_4a_3a_1^3a_0 - 900a_4a_2^3a_0^2 + 1020a_4a_2^2a_1^2a_0 - 192a_4a_2a_1^4 \\
&- 2500a_4a_1a_0^3 + 108a_3^5a_0^2 - 72a_3^4a_2a_1a_0 + 16a_3^4a_1^3 + 16a_3^3a_2^3a_0 - 4a_3^3a_2^2a_1^2 \\
&- 900a_3^3a_1a_0^2 + 825a_3^2a_2^2a_0^2 + 560a_3^2a_2a_1^2a_0 - 128a_3^2a_1^4 - 27a_2^4a_1^2 + 2250a_2^2a_1a_0^2 \\
&- 630a_3a_2^3a_1a_0 + 144a_3a_2^2a_1^3 - 3750a_3a_2a_0^3 + 2000a_3a_1^2a_0^2 + 108a_2^5a_0 \\
&- 1600a_2a_1^3a_0 + 256a_1^5 + 3125a_0^4
\end{aligned}
$$

Summing up what we have right now:

1. $f(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ is irreducible;
2. $\mathrm{Gal}_f \subseteq S_5$ is conjugate to one of the following: $Z_5$, $D_5$, $GA(1,5)$, $A_5$ or $S_5$,;
3. If $\sqrt{\Delta} \in \mathbb{Q}$, then $\mathrm{Gal}_f \subseteq A_5$ by Theorem 1.9;
4. If $\theta(y)$, the resolvent we found, is separable and has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f$ is conjugate to a subgroup of $GA(1,5)$ by Theorem 1.14;
5. If 3 holds but not 4, then $\mathrm{Gal}_f = A_5$;
6. If 4 holds but not 3, then $\mathrm{Gal}_f = GA(1,5)$;
7. If both 3 and 4 do not hold, then $\mathrm{Gal}_f = S_5$.
8. If 3 and 4 hold simultaneously, $\mathrm{Gal}_f = Z_5$ or $\mathrm{Gal}_f = D_5$ as seen from Figure 3;

**Remark 4.4.** *In situation 4, checking whether $\theta(y)$ has a root in $\mathbb{Q}$ or not can be explored a bit further. Note that $\theta(y)$ must be monic and have its coefficients in $\mathbb{Z}$, thus by Lemma of Gauss 1.18, if it has a zero in $\mathbb{Q}$ that zero must be in $\mathbb{Z}$; further more, that zero must divide the constant term of $\theta(y)$, so in our case it divides $B_6^2$ hence it must divide $B_6$. Therefore we can try substituting factors of $B_6$ into $\theta(y)$ and see if we get zero. Likewise, reducing the polynomial in $\mathbb{F}_p$ might help too.*

Thus, only situation 8 needs to be explored further. One way to do this is through the next small theorem:

**Theorem 4.5.** *Let $f(x)$ be a monic and irreducible polynomial in $\mathbb{Z}[x]$, then $\mathrm{Gal}_f$ is conjugate to $Z_5 \cong \langle(12345)\rangle$ if and only if $f(x)$ splits into linear products in $\mathbb{Q}(\alpha)[x]$, where $\alpha$ is a root of $f(x)$.*

*Proof.* If $f(x)$ splits completely in $\mathbb{Q}(\alpha)$, $[L : Q] = 5$ where $L$ is the splitting field of $f(x)$ over $\mathbb{Q}$, but $|\mathrm{Gal}_f| = [L : Q] = 5$, $\mathrm{Gal}_f \subseteq S_5$ and $\mathrm{Gal}_f$ must be transitive, thus, up to conjugacy, $\mathrm{Gal}_f = \mathbb{Z}_5$ by the discussion in the beginning of this section.
Similarly, if $\mathrm{Gal}_f = \mathbb{Z}_5$, then $[L : Q] = |\mathrm{Gal}_f| = 5$, hence the result follows. □

**Remark 4.6.** *However, note that this theorem could be difficult to apply without the help of a computing program. Suppose $f(x)$ has zeros $\alpha_i$ and $f(x)$ splits into linear factors in $\mathbb{Q}(\alpha_1)[x]$, then the above theorem tells us that the Galois extension is of degree 5, hence for the remain zeros $\alpha_2, \alpha_3, \alpha_4, \alpha_5$ there exists a 4-by-5 matrix in $\mathbb{Q}$ such that:*

$$\begin{bmatrix} a_1 & b_1 & c_1 & d_1 & e_1 \\ a_2 & b_2 & c_2 & d_2 & e_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 \\ a_4 & b_4 & c_4 & d_4 & e_4 \end{bmatrix} \begin{bmatrix} 1 \\ \alpha_1 \\ \alpha_1^2 \\ \alpha_1^3 \\ \alpha_1^4 \end{bmatrix} = \begin{bmatrix} \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \end{bmatrix}$$

*Furthermore, by expanding $\prod(x - \alpha_i) = f(x) = \sum s_i x^i \in \mathbb{Z}[x]$ and comparing coefficients, for each of the coefficients in front of the terms $x^4, x^3, x^2, x^1, 1$ we obtain similar equations. But again, in general it would be difficult to solve them. A quick way using this theorem with Mathematica is presented in Example 4.5.*

Another way to differentiate situation 8 could be using Dedekind's Theorem 1.16, which in this case implies $\mathrm{Gal}_f$ contains 5-cycles if and only if for every prime number $p$ such that the reduction modulo $p$ of $f$ is separable, it is either irreducible or splits into linear factors over $\mathbb{F}_p$. On the other hand, if situation 8 happens and for some $p$, the reduction modulo $p$ of $f$ contains two irreducible quadratic polynomials in $\mathbb{F}_p[x]$, then $\mathrm{Gal}_f$ must be isomorphic to $D_5$, which contains a generator of the form (ab)(cd).

However, note that the above method using Dedekind's Theorem works well in situation 8 only in case $\mathrm{Gal}_f = D_5$; see the remark below Dedekind's Theorem 1.16. Yet another, more systematic way to differentiate situation 8 could be using a new resolvent polynomial with respect to $\mathbb{Z}_5$ instead of $GA(1, 5)$. First, we need to find a polynomial in $\mathbb{Z}[x_1, \ldots, x_5]$ that has $\mathbb{Z}_5$ as its stabilizer, then check whether the resolvent has a root in $\mathbb{Q}$ and apply Theorem 1.14. This can also be done using *Magma*.

Note that subgroups of $S_n$ can be represented by a matrix group. E.g. (12345) corresponds to the following 5-by-5 matrix because:

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} x_2 & x_3 & x_4 & x_5 & x_1 \end{pmatrix}$$

Thus the five transitive subgroups of $S_5$ can be represented as follows in Magma:

```
Q:=Rationals();
Z5:=MatrixGroup<5,Q | [0,0,0,0,1, 1,0,0,0,0, 0,1,0,0,0, 0,0,1,0,0,
0,0,0,1,0]>;
D5:=MatrixGroup<5,Q | [0,0,0,1,0, 0,0,1,0,0, 0,1,0,0,0, 1,0,0,0,0,
0,0,0,0,1],[0,0,0,0,1, 1,0,0,0,0, 0,1,0,0,0,
0,0,1,0,0, 0,0,0,1,0]>;
GA15:=MatrixGroup<5,Q | [0,0,1,0,0, 1,0,0,0,0, 0,0,0,1,0, 0,1,0,0,0,
0,0,0,0,1], [0,0,0,0,1, 1,0,0,0,0, 0,1,0,0,0,
0,0,1,0,0, 0,0,0,1,0]>;
A5:=MatrixGroup<5,Q | [0,0,1,0,0, 1,0,0,0,0, 0,1,0,0,0, 0,0,0,1,0,
0,0,0,0,1],[0,0,0,0,1, 1,0,0,0,0, 0,1,0,0,0,
0,0,1,0,0, 0,0,0,1,0]>;
S5:=MatrixGroup<5,Q | [0,0,0,0,1, 1,0,0,0,0, 0,1,0,0,0, 0,0,1,0,0,
0,0,0,1,0],[0,1,0,0,0, 1,0,0,0,0, 0,0,1,0,0,
0,0,0,1,0, 0,0,0,0,1]>;
```

We want to find an $F \in \mathbb{Q}[x_1, \ldots, x_5]$ such that $F$ is fixed by $Z_5$ but not by any element in any larger group. It helps to use the following command to find the number of basis of the invariant space of degree $d = 1, 2, 3, 4$ in the polynomial ring $\mathbb{Q}[x_1, \ldots, x_5]$:

```
[#InvariantsOfDegree(Z5,d) : d in [1..4]];
[#InvariantsOfDegree(D5,d) : d in [1..4]];
[#InvariantsOfDegree(GA15,d) : d in [1..4]];
[#InvariantsOfDegree(A5,d) : d in [1..4]];
[#InvariantsOfDegree(S5,d) : d in [1..4]];
```

The result says when $d = 1$ the invariant space of five groups have dimension 1; when $d = 2$, the invariant space of $Z_5$ or $D_5$ has dimension 3 and for the remaining groups the dimension is 2; when $d = 3$, the invariant space of $Z_5$ has dimension 7, that of $D_5$ has dimension 5 and for the remaining groups the dimension is 3. Thus there must exist an $F$ of degree 3 such that $F$ is fixed by $Z_5$ but not by any larger group. Run the following and compare the result, we can find a choice for our $F$:

```
InvariantsOfDegree(Z5,3);
InvariantsOfDegree(D5,3);
```

```
InvariantsOfDegree(GA15,3);
InvariantsOfDegree(A5,3);
InvariantsOfDegree(S5,3);
```

One option is $F = x_1^2x_2 + x_1x_5^2 + x_2^2x_3 + x_3^2x_4 + x_4^2x_5 - x_1x_2x_3 - x_1x_2x_5 - x_1x_4x_5 - x_2x_3x_4 - x_3x_4x_5$, which is a difference between two elements that appear in `InvariantsOfDegree(Z5,3);` for invariant space for $Z_5$. To find the coefficients of our resolvent $r_{S_5,u}(y) = \prod_{\tau \in S_5/Z_5}(y - \tau(u))$, use the following command:

```
U:=InvariantsOfDegree(Z5,3); u:=U[2]-U[6];
P<x1,x2,x3,x4,x5>:=PolynomialRing(Q,5);
orb:=(P!u)^Sym(5); #orb;
R<e1, e2, e3, e4, e5> := PolynomialRing(Q, 5);
a,b:=IsSymmetric(-&+orb, R); b;
```

The last line gives us the coefficient of $y^{23}$, the other coefficients can be found similarly using Vieta's formula. For example, the constant term is the product of all terms in *orb* so it can be calculated by :

```
&*orb
```

The coefficient in front of $y^{22}$ can be given as:

```
c:=&+[orb];
X:=[0: j in [1..24]];
i:=1;
while i le 24 do
X[i]=&+[orb[i]: i in [1..i]];
i=i+1;
end while;
d:=&+[orb[k]*(c-X[k]): k in [1..24]];
```

## 4.2 Reducible polynomials

Let $f(x)$ be a monic reducible polynomial of degree 5 in $\mathbb{Z}[x]$. As always, let's discuss this case by case.

- Case 1: $f(x)$ contains a linear factor.

Examples of this case could be $f(x) = (x-a)(x^4 + bx^3 + cx^2 + dx + e)$, $f(x) = (x-a)(x-b)(x-c)(x^2 + dx + e)$, $f(x) = (x-a)(x^2 + bx + c)(x^2 + dx + e)$ etc., where $a, b, c, d, e \in \mathbb{Z}$. Since linear factors in $\mathbb{Z}$ always split in $\mathbb{Q}$, in this case we can always refer to results we already have and there is nothing new to say.

- Case 2: $f(x)$ has two irreducible factors, one of which is of degree 2 and the other is of degree 3.

Let $f(x) = g(x)h(x) = (x^2 + ax + b)(x^3 + cx^2 + dx + e)$, where $a, b, c, d, e \in \mathbb{Z}$, $g(x)$ and $h(x)$ are irreducible over $\mathbb{Q}$. Let $L_f$, $L_g$ and $L_h$ denote the splitting field of $f(x)$, $g(x)$ and $h(x)$ over $\mathbb{Q}$ respectively.
First of all, note that:

$$\begin{cases} [L_g : \mathbb{Q}] = 2 \\ [L_h : \mathbb{Q}] = 3 \quad \text{or} \quad 6, \end{cases}$$

Thus if $g(x)$ splits in $L_h$, we must have $L_f = L_h$, $[L_h : \mathbb{Q}] = 6$ and $[L_h : L_g] = 3$, hence $G_f = G_h = S_3$.
Let $x_1$ and $x_2$ be roots of $g(x)$, $x_3$, $x_4$ and $x_5$ be roots of $h(x)$. Note that $[L_g : \mathbb{Q}] = 2$, thus $x_1, x_2 \in L_h$ if and only if they are swapped by elements of order 2 and fixed otherwise, but elements of order 2 in $S_3$ are precisely 3 transpostisions which are odd, and odd permutations reverse the sign of $(x_3 - x_4)(x_3 - x_5)(x_4 - x_5)$ and even ones fix it. Therefore, all elements of $S_3$ fix $(x_1 - x_2)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5) = \sqrt{\Delta(g)}\sqrt{\Delta(h)}$, This is equivalent to saying

$$\sqrt{\Delta(g)}\sqrt{\Delta(h)} \in \mathbb{Q}$$

Now suppose $g(x)$ and $h(x)$ do not share the same splitting field. Thus $L_f = L_g \supset L_h \supset \mathbb{Q}$ where $\supset$ denotes field extension, and $G_f = G_g \times G_h$ must be a nontrivial subgroup of $S_2 \times S_3 \cong D_6$, the dihedral group of order 12, thus either $G_f = D_6$, or $S_2 \times A_3 \cong Z_6$ which is isomorphic to the cyclic group of order 6. Finally, note that the latter happens if and only if $\Delta(h)$, the discriminant of $h(x)$, is a square in $\mathbb{Q}$ by Theorem 1.9.

## 4.3 Examples

First of all, use the following code in Mathematica for our discriminant and resolvent polynomial:

```
IrreduciblePolynomialQ[x^5+a4 x^4+a3 x^3+a2 x^2+a1 x+a0]
B2=8 a4 a2-3 a3^2-20 a1 ;
```

```
B4=3 a3^4-16 a4 a3^2 a2+16 a4^2 a2^2+16 a3 a2^2+16 a4^2 a3 a1-8 a3^2
a1 -112 a4 a2 a1+240 a1^2-64 a4^3 a0+240 a4 a3 a0-400 a2 a0 ;
B6=8 a4 a3^4 a2-a3^6-16 a4^2 a3^2 a2^2-16 a3^3 a2^2+64 a4 a3 a2^3
-64 a2^4 -16 a4^2 a3^3 a1+28 a3^4 a1+64 a4^3 a3 a2 a1-112 a4 a3^2 a2 a1
-128 a4^2 a2^2 a1+224 a3 a2^2 a1-64 a4^4 a1^2+224 a4^2 a3 a1^2
-176 a3^2 a1^2-64 a4 a2 a1^2 +320 a1^3+48 a4 a3^3 a0-192 a4^2 a3 a2 a0
-80 a3^2 a2 a0+640 a4 a2^2 a0 +384 a4^3 a1 a0-640 a4 a3 a1 a0
-1600 a2 a1 a0 -1600 a4^2 a0^2+4000 a3 a0^2 ;
d=Discriminant[x^5+a4 x^4+a3 x^3+a2 x^2+a1 x+a0,x];
Sqrt[d]
theta=(y^3+B2 y^2 +B4 y +B6)^2 - 2^10 d y
Factor[theta]
PolynomialGCD[theta, D[theta,y]]
```

Given integer values $a_4, \ldots, a_0$, Mathematica will display the following: whether $f = x^5 + a4x^4 + a3x^3 + a2x^2 + a1x + a0$ is irreducible, $\sqrt{\Delta}$, the resolvent polynomial and its factorization over $\mathbb{Z}$, and whether it is separable (only value 1 means separable, because of the well-known fact that a non-constant polynomial $f$ is separable if and only if gcd(f,f')=1). Our resolvent polynomial will be monic and with integer coefficients, so by Lemma of Gauss if it has a root in $\mathbb{Q}$, that root will also be in $\mathbb{Z}$, thus factorization over $\mathbb{Z}$ suffices here.

**Example 4.1.** *Let $f(x) = x^5 - 6x + 3$. We have $\sqrt{\Delta} = 9i\sqrt{21451} \notin \mathbb{Q}$, and the resolvent polynomial is $1779231744y + (-69120 + 8640y + 120y^2 + y^3)^2$ which is irreducible over $\mathbb{Z}$. Furthermore, it is separable. Therefore $\mathrm{Gal}_f$ cannot be a subgroup of $GA(1,5)$ (by Theorem 1.14) or $A_5$ (by Theorem 1.9), thus $\mathrm{Gal}_f \cong S_5$.*

**Example 4.2.** *Let $f(x) = x^5 + 10x^2 + 24$. We have $\sqrt{\Delta} = 36000 \in \mathbb{Q}$, and the resolvent polynomial is $-1327104000000y + (-640000 - 96000y + y^3)^2$, which is irreducible over $\mathbb{Z}$. Furthermore, it is separable. Therefore $\mathrm{Gal}_f$ cannot be a subgroup of $GA(1,5)$ (by Theorem 1.14), nor can it be $S_5$ (by Theorem 1.9), thus $\mathrm{Gal}_f \cong A_5$.*

**Example 4.3.** *Let $f(x) = x^5 - 2$. We have $\sqrt{\Delta} = 100\sqrt{5} \notin \mathbb{Q}$, which means $\mathrm{Gal}_f$ is either $S_5$ or $GA(1,5)$ by Theorem 1.9. Furthermore, the resolvent polynomial is $-51200000y + y^6$, which clearly has a root $y = 0$ in $\mathbb{Q}$. In addition, it is separable. Thus $\mathrm{Gal}_f \cong GA(1,5)$ by Theorem 1.14.*

**Example 4.4.** *Let $f(x) = x^5 - 5x + 12$. We have $\sqrt{\Delta} = 8000 \in \mathbb{Q}$, and the resolvent polynomial is $(-100 + y)(-16000000 + 660000000y + 6320000y^2 + 52000y^3 + 300y^4 + y^5)$, so it clearly has a root in $\mathbb{Q}$. Furthermore, it is separable. Thus $\mathrm{Gal}_f \cong D_5$ or $\mathrm{Gal}_f \cong Z_5$ by Theorems 1.9 and 1.14. In $\mathbb{F}_3[x]$ $f = (x+2)(x^2+x+2)(x^2+2x+2)$, hence by Dedekind's Theorem 1.16 $\mathrm{Gal}_f$ contains a product of two 2-cycle, thus $\mathrm{Gal}_f \cong D_5$. (Factorization of a polynomial $f$ over $\mathbb{F}_p$ can be done in many convenient ways, for example, the command 'Factor[f, Modulus −> p]' in Mathematica.)*

**Example 4.5.** *Let* $f(x) = x^5+x^4-4x^3-3x^2+3x+1$. *We have* $\sqrt{\Delta} = 121 \in \mathbb{Q}$, *and the resolvent polynomial is* $-14992384y + (3872y - 132y^2 + y^3)^2$, *which clearly has a root* $y = 0$ *in* $\mathbb{Q}$. *Furthermore, it is separable. Thus* $\mathrm{Gal}_f \cong D_5$ *or* $\mathrm{Gal}_f \cong Z_5$ *by Theorems 1.9 and 1.14. First, I tried factoring* $f(x)$ *over* $\mathbb{F}_p$ *for* $p = 2, 3, 5, \ldots, 67$, *it turns out* $f(x)$ *either is irreducible or splits into linear factors, so there is a good chance that* $\mathrm{Gal}_f \cong Z_5$. *To validate this, Dedekind's Theorem alone will not work, becasue then we have to prove that for all p,* $f(x)$ *either is irreducible or splits into linear factors over* $\mathbb{F}_p$. *Instead, we can apply Theorem 4.5 by running the following in Mathematica:*

```
Factor[theta, Extension -> Root[1+3*#1-3*#1^2-4*#1^3+#1^4+#1^5&,1]]
```

*The result says* $\theta$ *splits into linear factors over* $\mathbb{Q}(\alpha_1)$, *where* $\alpha_1$ *is a root of* $f$. *Thus indeed* $\mathrm{Gal}_f \cong Z_5$.

# 5 Polynomials of degree of 6

## 5.1 Irreducible polynomials

As seen from previous sections, the idea of determining Galois group with respect to an irreducible monic polynomial of degree $n$ in $\mathbb{Z}[x]$ can be quite straightforward : first we classify all the transitive subgroups of $S_n$, then we use resolvents and discriminants. Both parts are significantly more difficult in case of degree 6 than lower degrees: there are 1455 subgroups of $S_6$ while there are only 156 of $S_5$ [10], and the degrees of resolvent polynomials would be very high. Since the latter part is essentially rational root-finding, it does not provide us much insight into Galois theory and it can be handled by computer algorithms relatively easily, in this section I would like to focus on the first part only.
First of all, we describe the element structure of $S_6$:

| Representative | Number of elements | Order | Odd or even |
|---|---|---|---|
| identity | 1 | 1 | Even |
| (12) | 15 | 2 | Odd |
| (123) | 40 | 3 | Even |
| (1234) | 90 | 4 | Odd |
| (12345) | 144 | 5 | Even |
| (123456) | 120 | 6 | Odd |
| (12)(34) | 45 | 2 | Even |
| (123)(45) | 120 | 6 | Odd |
| (123)(456) | 40 | 3 | Even |
| (12)(34)(56) | 15 | 2 | Odd |
| (1234)(56) | 90 | 4 | Even |

Consider a single cycle of length $n$. Firstly, there are $\binom{6}{n}$ ways to choose them; secondly, for each combination of these $n$ numbers we have $n!$ ways to permute them; lastly, $n$ single cycles $(a_1 a_2 \dots a_n)$, ..., $(a_i a_1 \dots a_{n-1})$ represent the same element, thus we divide the number by $n$. For a product of 2 cycles of lengths $n$ and $m$, repeat the above firstly choose $n$ elements in 6 then choose $m$ elements in $6-n$ and multiply the result together. In case $n = m$, divide the number by 2 because (ab)(cd)=(cd)(ab); in case $n \neq m$, this is unnecessary because (abc)(de)≠(dea)(bc). A similar result holds for a product of 3 cycles of length 2. Thus the second column is calculated to be $\frac{6!}{(6-n)!n}$ for a single cycle of length $n$, $\frac{6!}{(6-n)!n}\frac{(6-n)!}{(6-n-m)!m}$ for a product of two disjoint cycles of lengths $n, m$ when $n \neq m$, $\frac{6!}{(6-n)!n}\frac{(6-n)!}{(6-n-m)!m}\frac{1}{2}$ when $n = m$, and $\frac{6!}{(6-2)!2}\frac{4!}{(4-2)!2}\frac{2!}{(2-2)!2}\frac{1}{3}$ for a product of three cycles of lenght 2.

By theorems 1.5 and 1.7, we are looking for transitive subgroups of $S_6$ of order 6, 12, 18, 24, 30, 36, 48, 60, 72, 90, 120, 144, 180, 240, 360 and 720. The classification of these transitive subgroups are available in many places online (e.g.

the command *TransitiveGroups(6)* in Magma lists every transitive subgroup of $S_6$), thus in some difficult cases I'll prove (non-)existence only; in simpler cases I'll prove both (non-)existence and uniqueness

- Order of 6

Any group of order 6 must be isomorphic to either the cyclic group $Z_6 \cong \langle (123456) \rangle$ or $S_3$. In fact they can both act transitively. Transitivity of $Z_6$ is obvious. In the case of $S_3$, note that the group

$$\langle (145)(263), (12)(34)(56) \rangle$$

$= \{e, (145)(263), (154)(236), (12)(34)(56), (16)(24)(35), (13)(25)(46)\}$ is clearly transitive and is isomorphic to $S_3$.

**Remark 5.1.** *Another way to gain more insight into the transitivity of $S_3$ in $S_6$ is, instead of numbers, we consider letters, and $S_3 = \langle (xyz), (xy) \rangle$ clearly acts transitively on this set of six elements $\left\{x^2y, x^2z, xy^2, y^2z, xz^2, yz^2\right\}$.*

- Order of 12

If $G$ is a transitive subgroup of order 12, $G$ cannot be cyclic because no element in $S_6$ has order 12. Out of the non-cyclic groups of order 12, $D_6$ or $A_4$ are transitive. $D_6 \cong \langle \sigma, \tau \rangle$ constructed from $Z_6 \cong \langle \sigma \rangle$ and a transposition $\tau \in S_6$ such that $\tau\sigma\tau = \sigma^{-1}$ is clearly transitive. In addition, note that the following group

$$\begin{aligned}\langle (145)(263), (12)(34) \rangle = &\{e, (145)(263), (154)(236), (12)(34), (1635)(24)\} \\ &\cup \{(13)(2546), (13)(2645), (1536)(24), (164)(235)\} \\ &\cup \{(146)(253), (145)(263), (154)(236)\}\end{aligned}$$

is clearly transitive and is isomorphic to $A_4 \cong \langle (123), (12)(34) \rangle$, since we can construct a bijection between the conjugacy classes (123) and (123)(456) by the element structure table.

- Order of 18

$S_3 \times Z_3$ constructed from $S_3$ discussed earlier is transitive. Note that all the elements of order 3 in $S_3$ belong to the conjugacy class (123)(456), thus we can choose $\sigma \in S_6$ of order 3 belonging to the class (123) such that $\sigma \notin S_3$ and $\sigma\tau = \tau\sigma$ for all $\tau \in S_3$ to construct $S_3 \times Z_3$.

- Order of 24

The obvious ones are $A_4 \times Z_2$ and $S_4$, they are transitive as $A_4$ is transitive. The construction of the former is explored in the following remark; for the latter, note that by adding a generator (14)(25)(36) into $A_4 \cong \langle (135)(246), (14)(25) \rangle$ we obtain $\langle (135)(246), (36) \rangle \cong S_4$

**Remark 5.2.** *From the element structure table of $S_6$ we can see that elements of order 2 can be odd or even, thus this gives us two classes of subgroups isomorphic to $A_4 \times Z_2$, one is $A_4 \times Z_2 \cong \langle(135)(246),(14)(25),(15)(24)\rangle$ , which consist of even permutations only; the other is $A_4 \times Z_2 \cong \langle(135)(246),(14)(25),(15)(24)(36)\rangle$, which consists of 12 even permutations and 12 odd ones. Such problem does not occur when coupling a group with $Z_3$, because all elements of order 3 in $S_6$ are even. In addition, this is also not a problem for $S_4 \times Z_2$, because $S_4$ already has half of its elements even and the other half odd, so no matter the generator of $Z_2$ is even or odd, $S_4 \times Z_2$ must be half odd half even as well.*

- Order of 30

No subgroup of 30 exists in $S_6$. Otherwise, by Sylow's theorem, there must be a Sylow-3 subgroup of order 3 and a Sylow-5 subgroup of order 5. They are of prime orders so they are cyclic and their intersection is trivial, hence they must generate a cyclic group of order 15, which is impossible in $S_6$.

**Remark 5.3.** *Similar reasoning can also be used to explain why no subgroup of order 15 or 30 exist in $S_5$.*

- Order of 36

$S_3 \times S_3$ and $(Z_3 \times Z_3) \rtimes Z_4$, where the latter is a semi-direct product, are transitive subgroups of $S_6$.

- Order of 48

$Z_2 \times S_4$ is a transitive subgroup.

- Order of 60

$A_5$ is a transitive subgroup, see the case of *Order of 120* for details.

- Order of 72

$S_3 \wr Z_2$ is a transitive subgroup, where $\wr$ denotes a wreath product. Let $G \subseteq S_n$ and $H$ be groups, then the wreath product of $H$ and $G$ is defined as the semi-direct product:

$$H \wr G = H^n \rtimes G$$

where $G$ acts on $H$ via as a subgroup of $S_n$. So in our case:

$$S_3 \wr Z_2 = S_3^2 \rtimes Z_2$$

- Order of 90

There does not exist subgroup of order $90 = 2 \cdot 3^2 \cdot 5$ in $S_6$. Suppose there exists, let $G$ be such a group.

Suppose $G$ contains even permutations only, then by similar argument in the case *Order of 240* below, we have $A_6$ is isomorphic to a subgroup of $S_4$, which is impossible;
Thus $G$ must contain precisely 45 even elements and $H = G \cap A_6$ is a subgroup of $A_6$ of order 45. But by Sylow's theorem (where $n_p$ denotes the number of Sylow p-subgroups), $n_5 = 1 \bmod 5$ and $n_5$ divides 9 so $n_5 = 1$ and similarly $n_3 = 1$, but these two Sylow subgroups together generate a cyclic group of order 15, which is impossible in $S_6$.

- Order of 120

In Theorem 4.1, we used the fact that $S_5$ contains exactly 6 Sylow-5 subgroups which are cyclic groups of order 5. Furthermore, these subgroups are conjugate to each other by Sylow's theorem. Let $S = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ be the set of these subgroups and note that $\forall i, j \in \{1, 2, 3, 4, 5, 6\}$, $\exists \sigma \in S_5$ such that $\sigma P_i \sigma^{-1} = P_j$ because $P_i$ are conjugate. This shows that $S_5$ acts transitively on $S$. Now define $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ to be the set of roots of our polynomial. Clearly $X \cong S$ thus $S_5$ acts transitively on $X$ as well. In fact, in Theorem 4.1 we noted that if a subgroup of $S_5$ contains exactly 6 Sylow-5 subgroups, then it is either $A_5$ or $S_5$, thus the above also holds for $A_5$, hence $A_5$ is also a transitive subgroup of $S_6$.
There are no other subgroups of order 120, because the number of these subgroups is $\frac{720}{120} = 6$ and there are already 6 subgroups isomorphic to $S_5$ .

- Order of 144

No subgroup of this order exists in $S_6$. Suppose there is, let $G$ be such a group, note that 144 does not divide $360 = |A_6|$ hence $G$ cannot consist of even permutations only, thus it contains precisely 72 even elements and $G \cap A_6$ is a subgroup of $A_6$ of index $\frac{360}{72} = 5$, which is a prime, by the second part of Remark 5.4 we know this is impossible,

- Order of 180

There does not exist subgroups of order 180 in $S_6$. If it exists, name it $G$. $G$ cannot be a subgroup of $A_6$ because having index 2 means $G$ is a normal subgroup of $A_6$, which is impossible. Hence $G$ must contain precisely 90 odd permutations and 90 even permutations. By similar argument in the case *Order of 240* below, we have $A_6$ is isomorphic to a subgroup of $S_4$, a contradiction.

- Order of 240

There does not exist a subgroup $G$ of $S_6$ of order 240. If $G$ exists, $G$ can not have even permutations only as 240 does not divide $360 = |A_6|$, thus $G$ contains 120 even permutations and 120 odd ones. Hence $G \cap A_{6=N}$ is a subgroup of index 3 of $A_6$. Let $A_6$ act on $N$ by conjugation given by the map:

$$\varphi(\sigma)(N) : N \mapsto \sigma N \sigma^{-1}$$

where $\sigma \in A_6$. Since $A_6$ is simple, every non-trivial element in it maps $N$ to a different coset, thus we actually have a map from $A_6$ to $S_3$. This map is in fact a homomorphism, because:

$$\varphi(\sigma\tau)(N) = \sigma\tau N\tau^{-1}\sigma^{-1} = \varphi(\sigma)\varphi(\tau)(N)$$

furthermore it's injective as the kernel contains identity only, so we must have $A_6$ is isomorphic to a subgroup of $S_3$, which is impossible.

**Remark 5.4.** *The above can also be used to prove that no subgroup of order 40 exists in $S_5$, using the fact that $A_5$ is simple. (In fact $A_n$ is simple for all $n \geq 5$).*
*Furthermore, this can be proved in a different way, using the fact that if $H$ is a subgroup of $G$ of index $n$ where $n$ is the smallest prime dividing the order of $G$, then $H$ must be normal. (See, e.g. page 36 of [3]). And since $A_6$ is simple, every subgroup of $A_6$ must have a non-prime index.*

- Orders of 720 and 360

$S_6$ and $A_6$ are the only ones.

Magma can list all 16 transitive and proper subgroups of $S_6$. Summarizing the transitive subgroups up to conjugacy:

| ID in Magma | Name | Order | Generators |
|---|---|---|---|
| 1 | $Z_6$ | 6 | (123456) |
| 2 | $S_3$ | 6 | (135)(246), (14)(23)(56) |
| 3 | $D_6$ | 12 | (123456), (14)(23)(56) |
| 4 | $A_4$ | 12 | (135)(246), (14)(25) |
| 5 | $Z_3 \times S_3$ | 18 | (246), (14)(25)(36) |
| 6 | $S_4$ | 24 | (135)(246), (36) |
| 7 | $Z_2 \times A_4$ | 24 | (135)(246), (14)(25), (15)(24) |
| 8 | $Z_2 \times A_4$ | 24 | (135)(246), (14)(25), (15)(24)(36) |
| 9 | $S_3^2$ | 36 | (246), (15)(24), (14)(25)(36) |
| 10 | $Z_3^2 \rtimes Z_4$ | 36 | (246), (15)(24), (1452)(36) |
| 11 | $Z_2 \times S_4$ | 48 | (135)(246), (15)(24), (36) |
| 12 | $A_5$ | 60 | (12346), (14)(56) |
| 13 | $S_3 \wr Z_2$ | 72 | (24), (246), (14)(25)(36) |
| 14 | $S_5$ | 120 | (12346), (12)(34)(56) |
| 15 | $A_6$ | 360 | (123), (12)(3456) |
| 16 | $S_6$ | 720 | (123456), (12) |

We can also use Magma to check the subgroup structure of these groups. We are interested in classifying subgroups up to conjugacy, i.e. check whether $\tau G\tau^{-1} \subset H$ for all $\tau \in S_6$, thus the following command does so:

```
All:=TransitiveGroups(6); n:=#All;
T:=[All[i] : i in [1..n]];
cT1:={@ Conjugate(T[j],t) : t in Sym(6)@};
{i : i in [1..n] | #T[j] in {#(G meet T[i]) : G in cT1 }};
```

Given a transitive subgroup T[j], the result gives up to conjugacy which T[k] contains T[j]. Perform this process for all transitive subgroups, we find that, up to conjugacy:

| Group | Is a (proper) subgroup of |
|---|---|
| $Z_6$ | $D_6$, $Z_3 \times S_3$, $S_4$, $S_3^2$, $Z_2 \times S_4$, $S_3 \wr Z_2$, $S_5$, $S_6$ |
| $S_3$ | $D_6$, $Z_3 \times S_3$, $Z_2 \times A_4$, $S_3^2$, $Z_2 \times S_4$, $S_3 \wr Z_2$, $S_5$, $S_6$ |
| $D_6$ | $S_3^2$, $Z_2 \times S_4$, $S_3 \wr Z_2$, $S_5$, $S_6$ |
| $A_4$ | $S_4$, $Z_2 \times A_4$, $Z_2 \times A_4$, $Z_2 \times S_4$, $A_5$, $S_5$, $A_6$, $S_6$ |
| $Z_3 \times S_3$ | $S_3^2$, $S_3 \wr Z_2$, $S_6$ |
| $S_4$ | $Z_2 \times S_4$, $S_6$ |
| $Z_2 \times A_4$ | $Z_2 \times S_4$, $A_6$, $S_6$ |
| $Z_2 \times A_4$ | $Z_2 \times S_4$, $S_5$, $S_6$ |
| $S_3^2$ | $S_3 \wr Z_2$, $S_6$ |
| $Z_3^2 \rtimes Z_4$ | $S_3 \wr Z_2$, $A_6$, $S_6$ |
| $Z_2 \times S_4$ | $S_6$ |
| $A_5$ | $S_5$, $A_6$, $S_6$ |
| $S_3 \wr Z_2$ | $S_6$ |
| $S_5$ | $S_6$ |
| $A_6$ | $S_6$ |

where the blue $Z_2 \times A_4 \cong \langle (135)(246), (14)(25), (15)(24) \rangle$ and the black $Z_2 \times A_4 \cong \langle (135)(246), (14)(25), (15)(24)(36) \rangle$.

This can also be summarised in the following Figure 4, where $A \to B$ indicates $A \supset B$, and name in blue means the group consists of even permutations only. Figure 4 looks still messy, so we'd better consider the blue ones and black ones separately based on Theorem 1.9.

Let $f(x)$ be a monic, irreducible polynomial of degree 6 with integer coefficients. First of all, we would like to consider whether $\Delta(f)$ is a square in $\mathbb{Z}$
**Case 1: $\Delta(f)$ is a square in $\mathbb{Q}$.** By Theorem 1.9, $\mathrm{Gal}_f$ must consist of even permutations only, thus we can only consider Figure 5.

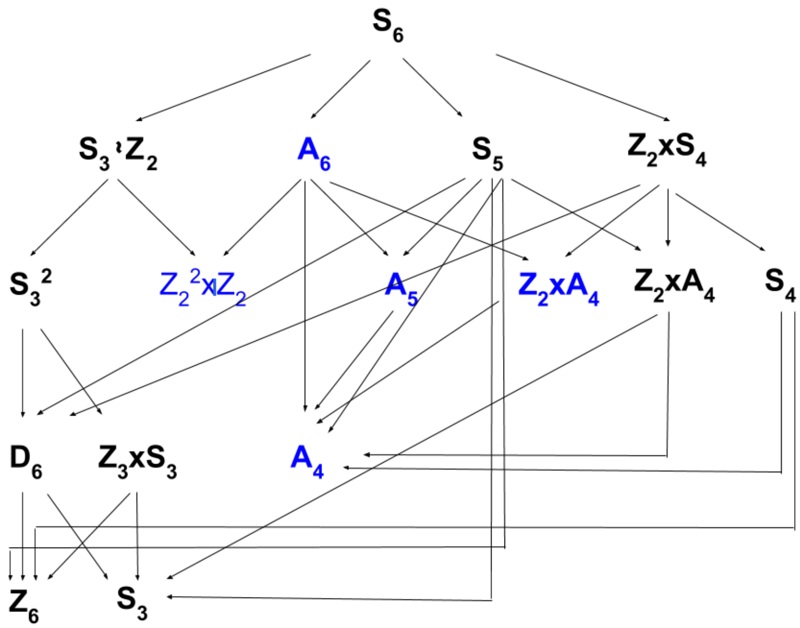


Figure 4: Structure of transitive subgroups of $S_6$

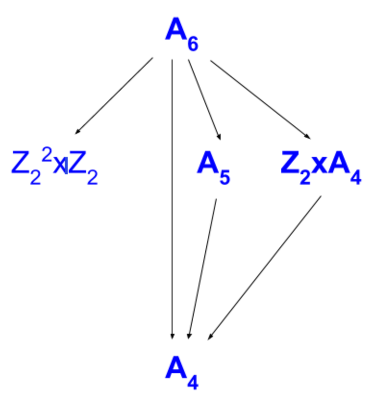


Figure 5: Structure of transitive subgroups of $S_6$ consisting even permutations only

For simplicity's sake, let $r_G$ denote $r_{G,F}(f)$, the resolvent polynomial of $f(x)$ with respect to a transitive subgroup $G$ of $S_6$, where $G$ is the stabilizer of a polynomial $F \in \mathbb{Q}[x_1, .., x_6]$. The corresponding polynomials $F$ will be determined later. And assume all the resolvents are separable. (If not, we can always try a different $F$). A straightforward strategy is constructing 4 resolvent polynomials $r_{Z_3^2 \rtimes Z_4}$, $r_{Z_2 \times A_4}$ and $r_{A_5}$, and consider whether they have a zero in $\mathbb{Q}$. By Theorem 1.14 Only one of the following situations can happen:

1. None of $r_{Z_3^2 \rtimes Z_4}$, $r_{Z_2 \times A_4}$ and $r_{A_5}$ has a zero in $\mathbb{Q} \Leftrightarrow \mathrm{Gal}_f \cong A_4$;
2. Only $r_{Z_3^2 \rtimes Z_4}$ has a zero in $\mathbb{Q} \Leftrightarrow \mathrm{Gal}_f \cong Z_3^2 \rtimes Z_4$;
3. Only $r_{Z_2 \times A_4}$ has a zero in $\mathbb{Q} \Leftrightarrow \mathrm{Gal}_f \cong Z_2 \times A_4$;
4. Only $r_{A_5}$ has a zero in $\mathbb{Q} \Leftrightarrow \mathrm{Gal}_f \cong A_5$;
5. Both $r_{Z_2 \times A_4}$ and $r_{A_5}$ have a zero in $\mathbb{Q} \Leftrightarrow \mathrm{Gal}_f \cong A_4$.

We can use Dedekind's Theorem 1.16 to make this strategy faster. By the element structure table of $S_6$, we know that the only kinds of even permutations are: e, (12)(34), (123), (123)(456), (12345), (1234)(56). These must occur in $A_6$, but not necessarily in other groups in Figure 5. To find out what kind of cycles are contained in the other 4 groups, we can use the command *Classes(G)* in Magma, where $G$ denote a group.

- $A_4$ only contains cycles of the form: e, (123)(456) and (12)(34);
- $Z_2 \times A_4 \cong \langle (135)(246), (14)(25), (15)(24) \rangle$ contains what $A_4$ has, and (1234)(56);
- $Z_2^2 \rtimes Z_4$ contains cycles of the form: e, (12)(34), (123), (123)(456) and (1234)(56); (So, compared to $A_6$, it does not contain the class (12345)).
- $A_5$ contains cycles of the form: e, (12)(34), (123), (123)(456) and (12345); (So, compared to $A_6$, it does not contain the class (1234)(56)).

Thus, by the above discussion and Dedekind's Theorem 1.16, the following observation would be very helpful:

**Corollary 5.1.** *Let $f(x)$ be a monic, irreducible polynomial of degree 6 with integer coefficients and $\sqrt{\Delta(f)} \in \mathbb{Z}$. Then:*

1. *if $f(x)$ factorises into an irreducible quadratic and an irreducible quartic over some $\mathbb{F}_p$, then $\mathrm{Gal}_f$ must be one of $A_6$, $Z_2 \times A_4$ or $Z_2^2 \rtimes Z_4$;*
2. *if $f(x)$ factorises into a linear factor and an irreducible quintic over some $\mathbb{F}_p$, then $\mathrm{Gal}_f$ must be $A_6$ or $A_5$;*
3. *if $f(x)$ factorises into three linear factor and an irreducible cubic over some $\mathbb{F}_p$, then $\mathrm{Gal}_f$ must be one of $A_6$, $A_5$ or $Z_2^2 \rtimes Z_4$;*
4. *if two of 1, 2 and 3 hold simultaneously, $\mathrm{Gal}_f$ must be $A_6$.*

**Case 2: $\Delta(f)$ is not a square in $\mathbb{Q}$.** For simplicity's sake, let $r_G$ denote $r_{G,F}(f)$, the resolvent polynomial of $f(x)$ with respect to a transitive subgroup $G$ of $S_6$, where $G$ is the stabilizer of a polynomial $F \in \mathbb{Q}[x_1, .., x_6]$. The corresponding polynomials $F$ will be determined later. And assume all the resolvents are separable. (If not, we can always try a different $F$). With the help of Theorem 1.14 and Figure 6, we can proceed in the following steps:

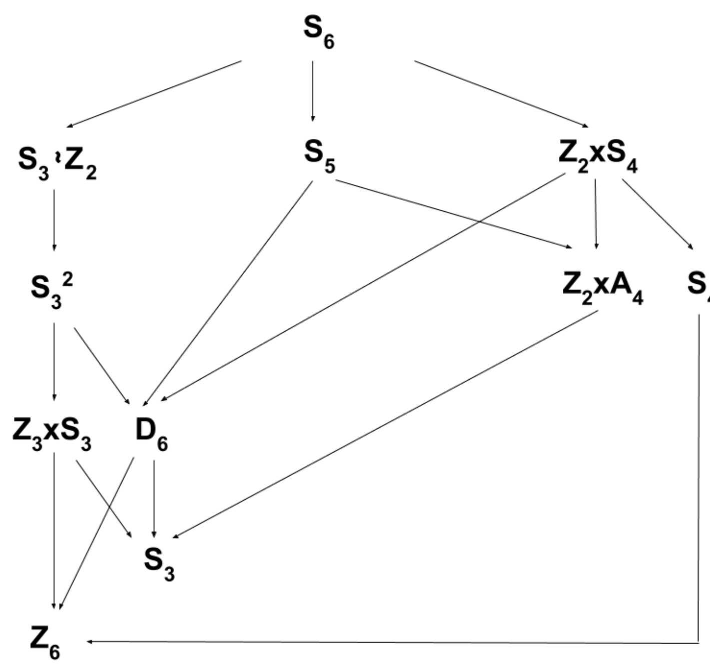


Figure 6: Structure of transitive subgroups of $S_6$ consisting both odd and even permutations

- **Step 1**: check whether $r_{S_3 \wr Z_2}$, $r_{S_5}$ and $r_{S_4 \times Z_2}$ has a root in $\mathbb{Q}$.

By Theorem 1.14, only one of these five situations can occur:

(i) If none of the above three resolvents has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = S_6$;

(ii) If only $r_{S_5}$ has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = S_5$;

(iii) If both $r_{S_3 \wr Z_2}$ and $r_{S_4 \times Z_2}$ or both $r_{S_3 \wr Z_2}$ and $r_{S_5}$ have a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f$ is one of $Z_6$, $S_3$ or $D_6$, we proceed to Step 2;

(iv) If both $r_{S_5}$ and $r_{S_4 \times Z_2}$ have a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f$ is one of $Z_6$, $S_3$, $D_6$ or $Z_2 \times A_4$, we'll have to proceed to both Step 2 and 4;

(v) If only $r_{S_3 \wr Z_2}$ has a zero in $\mathbb{Q}$, then proceed to Step 3;

(vi) If only $r_{S_4 \times Z_2}$ has a zero in $\mathbb{Q}$, then proceed to Step 4.

- **Step 2**: check whether $r_{Z_6}$ and $r_{S_3}$ has a root in $\mathbb{Q}$.

(i) If neither of these 2 resolvents has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = D_6$;

(ii) If $r_{Z_6}$ has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = Z_6$;

(iii) If $r_{S_3}$ has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = S_3$.

- **Step 3**: check whether $r_{S_3^2}$ and $r_{Z_3 \times S_3}$ has a root in $\mathbb{Q}$.

(i) If neither of these 2 resolvents has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = S_3 \wr Z_2$;

(ii) If $r_{S_3^2}$ but not $r_{Z_3 \times S_3}$ has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = S_3^2$;

(iii) If both resolvents have a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = Z_3 \times S_3$.

**Remark 5.5.** *Note that in this step we don't need to consider $Z_6$, $S_3$ or $D_6$, because if* $\mathrm{Gal}_f$ *is one of these three groups, we would have situation (iii) in Step 1. Similar result applies for Step 4.*

- **Step 4**: check whether $r_{S_4}$ and $r_{Z_2 \times A_4}$ has a root in $\mathbb{Q}$.

(i) If neither of these 2 resolvents has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = S_4 \times Z_2$;

(ii) If $r_{S_4}$ has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = S_4$;

(iii) If $r_{Z_2 \times A_4}$ has a zero in $\mathbb{Q}$, then $\mathrm{Gal}_f = Z_2 \times A_4$.

And of course, sometimes we can also use Dedekind's Theorem 1.16 to make this process faster. Again, with the help of Magma, we can find out that:

- $S_3 \wr Z_2$ contains all conjugacy classes except for (12345) and (1234);
- $S_5$ contains all conjugacy classes except for (12), (123), (1234)(56) and (123)(45);
- $S_4 \times Z_2$ contains all conjugacy classes except for (123), (123)(45) and (12345);

- $S_3^2$ contains all conjugacy classes except for (12), (123)(45), (1234), (12345) and (1234)(56);
- $S_4$ contains all conjugacy classes except for (123), (123)(45), (1234), (12345) and (1234)(56);
- $Z_2 \times A_4 \cong \langle (135)(246), (14)(25), (15)(24)(36) \rangle$ contains all conjugacy classes except for (12), (123), (123)(45), (12345), (1234)(56) and (123456);
- $Z_3 \times S_3$ only contains the classes e, (12)(34)(56), (123), (123)(456) and (123456);
- $Z_6$, $S_3$ and $D_6$ only contains the classes e, (12)(34), (12)(34)(56), (123)(456) and (123456).

Thus, by the above discussion and Dedekind's Theorem 1.16, we can make the following useful information:

**Corollary 5.2.** *Let $f(x)$ be a monic, irreducible polynomial of degree 6 with integer coefficient and $\sqrt{\Delta(f)} \notin \mathbb{Z}$. Then:*

1. *if $f(x)$ factorises into four linear factors and an irreducible quadratic over some $\mathbb{F}_p$, then $\mathrm{Gal}_f$ must be one of $S_6$, $S_3 \wr Z_2$, $S_4 \times Z_2$ or $S_4$;*
2. *if $f(x)$ factorises into three linear factors and an irreducible cubic over some $\mathbb{F}_p$, then $\mathrm{Gal}_f$ must be one of $S_6$, $S_3 \wr Z_2$, $S_3^2$ or $Z_3 \times S_3$;*
3. *if $f(x)$ factorises into one linear factor and an irreducible quintic over some $\mathbb{F}_p$, then $\mathrm{Gal}_f$ must be $S_6$ or $S_5$;*
4. *if $f(x)$ factorises into an irreducible quadratic and an irreducible quartic over some $\mathbb{F}_p$, then $\mathrm{Gal}_f$ must be one of $S_6$, $S_3 \wr Z_2$ or $S_4 \times Z_2$;*
5. *if $f(x)$ factorises into one linear factor, an irreducible quadratic and an irreducible cubic over some $\mathbb{F}_p$, then $\mathrm{Gal}_f$ must be $S_6$ or $S_3 \wr Z_2$.*

Summarizing, we need 3 (when $\sqrt{\Delta(f)} \in \mathbb{Z}$) + 9 (when $\sqrt{\Delta(f)} \notin \mathbb{Z}$) = 12 resolvent polynomials if Dedekind's Theorem 1.16 doesn't help. Define these groups in Magma:

```
Q:=Rationals();
Z6:=MatrixGroup<6,Q | [0,0,0,0,0,1, 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]>;
S3:=MatrixGroup<6,Q | [0,0,0,0,1,0, 0,0,0,0,0,1, 1,0,0,0,0,0,
0,1,0,0,0,0, 0,0,1,0,0,0, 0,0,0,1,0,0],[0,0,0,1,0,0, 0,0,1,0,0,0,
0,1,0,0,0,0, 1,0,0,0,0,0,0,0,0,0,0,1, 0,0,0,0,1,0]>;
Z3S3:=MatrixGroup<6,Q | [1,0,0,0,0,0, 0,0,0,0,0,1, 0,0,1,0,0,0,
0,1,0,0,0,0, 0,0,0,0,1,0, 0,0,0,1,0,0],[0,0,0,1,0,0, 0,0,0,0,1,0,
0,0,0,0,0,1,1,0,0,0,0,0, 0,1,0,0,0,0, 0,0,1,0,0,0]>;
S4:=MatrixGroup<6,Q | [0,0,0,0,1,0, 0,0,0,0,0,1, 1,0,0,0,0,0,
```

```
0,1,0,0,0,0, 0,0,1,0,0,0, 0,0,0,1,0,0],[1,0,0,0,0,0, 0,1,0,0,0,0,
0,0,0,0,0,1, 0,0,0,1,0,0, 0,0,0,0,1,0, 0,0,1,0,0,0]>;
Z2A4EVEN:=MatrixGroup<6,Q | [0,0,0,0,1,0, 0,0,0,0,0,1, 1,0,0,0,0,0,
0,1,0,0,0,0, 0,0,1,0,0,0, 0,0,0,1,0,0], [0,0,0,1,0,0, 0,0,0,0,1,0,
0,0,1,0,0,0, 1,0,0,0,0,0, 0,1,0,0,0,0, 0,0,0,0,0,1], [0,0,0,0,1,0,
0,0,0,1,0,0, 0,0,1,0,0,0, 0,1,0,0,0,0, 1,0,0,0,0,0, 0,0,0,0,0,1]>;
Z2A4ODD:=MatrixGroup<6,Q | [0,0,0,0,1,0, 0,0,0,0,0,1, 1,0,0,0,0,0,
0,1,0,0,0,0, 0,0,1,0,0,0, 0,0,0,1,0,0],[0,0,0,1,0,0, 0,0,0,0,1,0,
0,0,1,0,0,0, 1,0,0,0,0,0, 0,1,0,0,0,0, 0,0,0,0,0,1], [0,0,0,0,1,0,
0,0,0,1,0,0, 0,0,0,0,0,1, 0,1,0,0,0,0, 1,0,0,0,0,0, 0,0,1,0,0,0]>;
S3S3:=MatrixGroup<6,Q | [1,0,0,0,0,0, 0,0,0,0,0,1, 0,0,1,0,0,0,
0,1,0,0,0,0, 0,0,0,0,1,0, 0,0,0,1,0,0],[0,0,0,0,1,0, 0,0,0,1,0,0,
0,0,1,0,0,0, 0,1,0,0,0,0, 1,0,0,0,0,0, 0,0,0,0,0,1], [0,0,0,1,0,0,
0,0,0,0,1,0, 0,0,0,0,0,1, 1,0,0,0,0,0, 0,1,0,0,0,0, 0,0,1,0,0,0]>;
Z3Z3Z4:=MatrixGroup<6,Q | [1,0,0,0,0,0, 0,0,0,0,0,1, 0,0,1,0,0,0,
0,1,0,0,0,0, 0,0,0,0,1,0, 0,0,0,1,0,0],[0,0,0,0,1,0, 0,0,0,1,0,0,
0,0,1,0,0,0, 0,1,0,0,0,0, 1,0,0,0,0,0, 0,0,0,0,0,1], [0,1,0,0,0,0,
0,0,0,0,1,0, 0,0,0,0,0,1, 1,0,0,0,0,0, 0,0,0,1,0,0, 0,0,1,0,0,0]>;
Z2S4:=MatrixGroup<6,Q | [0,0,0,0,1,0, 0,0,0,0,0,1, 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, 0,0,0,1,0,0,
0,0,1,0,0,0, 0,1,0,0,0,0, 1,0,0,0,0,0, 0,0,0,0,0,1], [1,0,0,0,0,0,
0,1,0,0,0,0, 0,0,0,0,0,1, 0,0,0,1,0,0, 0,0,0,0,1,0, 0,0,1,0,0,0]>;
A5:=MatrixGroup<6,Q | [0,0,0,0,0,1, 1,0,0,0,0,0, 0,1,0,0,0,0,
0,0,1,0,0,0, 0,0,0,0,1,0, 0,0,0,1,0,0],[0,0,0,1,0,0, 0,1,0,0,0,0,
0,0,1,0,0,0, 1,0,0,0,0,0, 0,0,0,0,0,1, 0,0,0,0,1,0]>;
S3wrZ2:=MatrixGroup<6,Q | [1,0,0,0,0,0, 0,0,0,1,0,0, 0,0,1,0,0,0,
0,1,0,0,0,0, 0,0,0,0,1,0, 0,0,0,0,0,1], [1,0,0,0,0,0, 0,0,0,0,0,1,
0,0,1,0,0,0, 0,1,0,0,0,0, 0,0,0,0,1,0, 0,0,0,1,0,0], [0,0,0,1,0,0,
0,0,0,0,1,0, 0,0,0,0,0,1, 1,0,0,0,0,0, 0,1,0,0,0,0, 0,0,1,0,0,0]>;
S5:=MatrixGroup<6,Q | [0,0,0,0,0,1, 1,0,0,0,0,0, 0,1,0,0,0,0,
0,0,1,0,0,0, 0,0,0,0,1,0, 0,0,0,1,0,0],[0,1,0,0,0,0, 1,0,0,0,0,0,
0,0,0,1,0,0, 0,0,1,0,0,0, 0,0,0,0,0,1, 0,0,0,0,1,0]>;
```

and run the command

```
[#InvariantsOfDegree(G,d) : d in [1..12]];
```

for all of those groups $G$, the result is:

```
[ 1, 4, 10, 22, 42, 80, 132, 217, 335, 504, 728, 1038 ]
[ 1, 5, 10, 24, 42, 83, 132, 222, 335, 511, 728, 1047 ]
[ 1, 3, 6, 12, 20, 37, 56, 90, 133, 197, 276, 391 ]
[ 1, 3, 7, 13, 23, 41, 63, 98, 146, 210, 294, 408 ]
[ 1, 3, 6, 11, 18, 32, 48, 75, 111, 160, 224, 313 ]
[ 1, 3, 5, 10, 15, 29, 41, 68, 98, 147, 202, 291 ]
[ 1, 3, 5, 10, 15, 27, 38, 60, 84, 123, 166, 233 ]
[ 1, 3, 5, 10, 15, 26, 38, 59, 84, 121, 166, 230 ]
```

```
[ 1, 3, 5, 10, 15, 27, 38, 60, 84, 122, 164, 229 ]
[ 1, 2, 4, 6, 10, 17, 24, 36, 53, 74, 102, 141 ]
[ 1, 3, 5, 10, 15, 26, 37, 57, 79, 113, 151, 207 ]
[ 1, 2, 3, 5, 7, 12, 15, 23, 31, 44, 57, 80 ]
```

For groups $S_3^2$ and $Z_3^2 \rtimes Z_4$, the dimensions of their invariant spaces are represented by lines 7 and 8, which are very close to each other, hence it is especially difficult to find their corresponding $F$ and I took $d = 20$ for them. For the remaining cases I took $d = 6$. For each group, I take a difference of two bases in its invariant space. To ensure that the stabilizer of the chosen polynomial $F$ is really $G$, I first define $G$ as a matrix group and then run the command

```
orb:=F^Sym(6);#orb;
```

The result returns a number, and will be $|G|$ if $Stab(F) = G$. As an example, take $G = Z_6$ and run the following:

```
Q:=Rationals();
G:=MatrixGroup<6,Q | [0,0,0,0,0,1, 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]>;
inv:=InvariantsOfDegree(G,6);
n:=#inv;
F:=inv[n-7]-inv[n-5];
orb:=F^Sym(6);
#orb;
```

The result is 120, exactly the index of $Z_6$. If the result is undesirable, we can change the numbers $n - 7$ and $n - 5$ slightly and try again. The result can be summarized below, where for each group $G$, an $F$ such that $Stab(F) = G$ is presented:

- $Z_6$

$x_1^2x_2x_4^2x_6 - x_1^2x_2x_4x_5x_6 + x_1^2x_3x_4^2x_5 + x_1x_2^2x_3x_5^2 - x_1x_2^2x_3x_5x_6 - x_1x_2x_3^2x_4x_6 - x_1x_2x_3x_4^2x_5 + x_1x_3^2x_5x_6^2 - x_1x_3x_4x_5x_6^2 + x_2^2x_4x_5^2x_6 + x_2x_3^2x_4x_6^2 - x_2x_3x_4x_5^2x_6$

- $S_3$

$x_1^2x_2x_5x_6^2 - x_1^2x_3^2x_5x_6 - x_1^2x_3x_4x_5^2 + x_1x_2^2x_3^2x_4 - x_1x_2x_3^2x_5^2 - x_1x_2x_4^2x_6^2 - x_2^2x_3x_4x_6^2 - x_2^2x_4^2x_5x_6 + x_3x_4^2x_5^2x_6$

- $Z_3 \times S_3$

$-x_1^2x_2x_3x_4x_6 + x_1^2x_2x_4x_5x_6 - x_1x_2^2x_3x_4x_5 + x_1x_2^2x_3x_5x_6 + x_1x_2x_3^2x_4x_6 + x_1x_2x_3x_4^2x_5 - x_1x_2x_3x_5x_6^2 - x_1x_2x_4x_5^2x_6 - x_1x_3x_4^2x_5x_6 + x_1x_3x_4x_5x_6^2 - x_2x_3^2x_4x_5x_6 + x_2x_3x_4x_5^2x_6$

- $S_4$

$-x_1^2x_2x_3x_5x_6+x_1^2x_2x_4^2x_5-x_1x_2^2x_3x_4x_6-x_1x_2x_3^2x_4x_5-x_1x_2x_4x_5x_6^2+x_1x_3^2x_4x_6^2-x_1x_3x_4x_5^2x_6+x_2^2x_3x_5^2x_6-x_2x_3x_4^2x_5x_6$

- $Z_2 \times A_4$ (subgroup of $A_6$)

$-x_1^2x_2^2x_6^2+x_1^2x_2x_3x_5x_6-x_1^2x_3^2x_5^2+x_1x_2^2x_3x_4x_6+x_1x_2x_3^2x_4x_5+x_1x_2x_4x_5x_6^2+x_1x_3x_4x_5^2x_6-x_2^2x_3^2x_4^2+x_2x_3x_4^2x_5x_6-x_4^2x_5^2x_6^2$

- $Z_2 \times A_4$ (not a subgroup of $A_6$)

$x-x_1^3x_4^3+x_1^2x_2^2x_3x_4+x_1^2x_2^2x_5x_6+x_1^2x_2x_3^2x_6+x_1^2x_2x_3x_5^2+x_1^2x_2x_4x_6^2+x_1^2x_3^2x_4x_5+x_1^2x_3x_5x_6^2+x_1^2x_4x_5^2x_6+x_1x_2^2x_3^2x_5+x_1x_2^2x_3x_6^2+x_1x_2^2x_4^2x_6+x_1x_2x_3^2x_4^2+x_1x_2x_5^2x_6^2+x_1x_3^2x_5^2x_6+x_1x_3x_4^2x_5^2+x_1x_4^2x_5x_6^2-x_2^3x_5^3+x_2^2x_3^2x_4x_6+x_2^2x_3x_4^2x_5+x_2^2x_4x_5x_6^2+x_2x_3^2x_4x_5^2+x_2x_3x_4^2x_6^2+x_2x_4^2x_5^2x_6-x_3^3x_6^3+x_3^2x_4^2x_5x_6+x_3x_4x_5^2x_6^2$

- $S_3 \times S_3$

$x_1^7x_2^6x_3x_4^5x_6+x_1^7x_2^6x_4x_5x_6^5+x_1^7x_2^5x_3x_4x_6^6+x_1^7x_2^5x_4^6x_5x_6+x_1^7x_2x_3x_4^6x_6^5+x_1^7x_2x_4^5x_5x_6^6+x_1^6x_2^7x_3^5x_4x_5+x_1^6x_2^7x_3x_5^5x_6-x_1^6x_2^2x_3^6x_4^2x_5^3x_6-x_1^6x_2^2x_3^6x_4x_5^3x_6^2-x_1^6x_2^2x_3^3x_4^2x_5^6x_6-x_1^6x_2^2x_3^3x_4x_5^6x_6^2-x_1^6x_2x_3^6x_4^2x_5^3x_6^2+x_1^6x_2x_3^5x_5x_6^7-x_1^6x_2x_3^3x_4^2x_5^6x_6^2+x_1^6x_2x_3x_4^7x_5^5+x_1^6x_3^5x_4^7x_5x_6+x_1^6x_3x_4x_5^5x_6^7+x_1^5x_2^7x_3^6x_5x_6+x_1^5x_2^7x_3x_4x_5^6+x_1^5x_2x_3^6x_4^7x_5+x_1^5x_2x_3x_5^6x_6^7+x_1^5x_3^6x_4x_5x_6^7+x_1^5x_3x_4^7x_5^6x_6-x_1^3x_2^2x_3^6x_4^2x_5^6x_6-x_1^3x_2^2x_3^6x_4x_5^6x_6^2-x_1^3x_2x_3^6x_4^2x_5^6x_6^2-x_1^2x_2^6x_3^2x_4^6x_5x_6^3-x_1^2x_2^6x_3^2x_4^3x_5x_6^6-x_1^2x_2^6x_3x_4^6x_5^2x_6^3-x_1^2x_2^6x_3x_4^3x_5^2x_6^6-x_1^2x_2^3x_3^2x_4^6x_5x_6^6-x_1^2x_2^3x_3x_4^6x_5^2x_6^6+x_1x_2^7x_3^6x_4x_5^5+x_1x_2^7x_3^5x_5^6x_6+x_1x_2^6x_3^7x_4x_6^5-x_1x_2^6x_3^2x_4^6x_5^2x_6^3-x_1x_2^6x_3^2x_4^3x_5^2x_6^6+x_1x_2^6x_4^5x_5^7x_6+x_1x_2^5x_3^7x_4^6x_6+x_1x_2^5x_4x_5^7x_6^6-x_1x_2^3x_3^2x_4^6x_5^2x_6^6+x_1x_2x_3^7x_4^5x_6^6+x_1x_2x_3^6x_5^5x_6^7+x_1x_2x_3^5x_4^7x_5^6+x_1x_2x_4^6x_5^7x_6^5+x_1x_3^6x_4^7x_5^5x_6+x_1x_3^5x_4x_5^6x_6^7+x_2^6x_3^7x_4^5x_5x_6+x_2^6x_3x_4x_5^7x_6^5+x_2^5x_3^7x_4x_5x_6^6+x_2^5x_3x_4^6x_5^7x_6+x_2x_3^7x_4^6x_5x_6^5+x_2x_3x_4^5x_5^7x_6^6$

- $Z_3^2 \rtimes Z_4$

$-x_1^6x_2^5x_3^3x_4x_5^2x_6^3-x_1^6x_2^5x_3^2x_4^3x_5^3x_6+x_1^6x_2^3x_3^4x_4^3x_5x_6^3-x_1^6x_2^3x_3^3x_4^5x_5^2x_6-x_1^6x_2^3x_3^2x_4x_5^3x_6^5+x_1^6x_2^3x_3x_4^3x_5^4x_6^3-x_1^6x_2x_3^3x_4^3x_5^2x_6^5-x_1^6x_2x_3^2x_4^5x_5^3x_6^3-x_1^5x_2^6x_3^3x_4^3x_5x_6^2-x_1^5x_2^6x_3x_4^2x_5^3x_6^3-x_1^5x_2^3x_3^3x_4^2x_5x_6^6-x_1^5x_2^3x_3x_4^6x_5^3x_6^2-x_1^5x_2^2x_3^3x_4^6x_5x_6^3-x_1^5x_2^2x_3x_4^3x_5^3x_6^6+x_1^4x_2^3x_3^6x_4^3x_5x_6^3+x_1^4x_2^3x_3x_4^3x_5^6x_6^3-x_1^3x_2^6x_3^5x_4^2x_5x_6^3+x_1^3x_2^6x_3^3x_4^4x_5^3x_6+x_1^3x_2^6x_3^3x_4x_5^3x_6^4-x_1^3x_2^6x_3x_4^3x_5^5x_6^2-x_1^3x_2^5x_3^6x_4^3x_5^2x_6-x_1^3x_2^5x_3^2x_4x_5^6x_6^3+x_1^3x_2^4x_3^3x_4^6x_5^3x_6+x_1^3x_2^4x_3^3x_4x_5^3x_6^6-x_1^3x_2^3x_3^6x_4x_5^2x_6^5-x_1^3x_2^3x_3^5x_4^6x_5x_6^2-x_1^3x_2^3x_3^2x_4^5x_5^6x_6-x_1^3x_2^3x_3x_4^2x_5^5x_6^6-x_1^3x_2^2x_3^5x_4^3x_5x_6^6-x_1^3x_2^2x_3x_4^6x_5^5x_6^3-x_1^3x_2x_3^6x_4^5x_5^2x_6^3+x_1^3x_2x_3^3x_4^6x_5^3x_6^4+x_1^3x_2x_3^3x_4^4x_5^3x_6^6-x_1^3x_2x_3^2x_4^3x_5^6x_6^5-x_1^2x_2^5x_3^6x_4x_5^3x_6^3-x_1^2x_2^5x_3^3x_4^3x_5^6x_6-x_1^2x_2^3x_3^6x_4^5x_5^3x_6-x_1^2x_2^3x_3^3x_4x_5^6x_6^5-x_1^2x_2x_3^6x_4^3x_5^3x_6^5-x_1^2x_2x_3^3x_4^5x_5^6x_6^3-x_1x_2^6x_3^5x_4^3x_5^3x_6^2-x_1x_2^6x_3^3x_4^2x_5^5x_6^3+x_1x_2^3x_3^6x_4^3x_5^4x_6^3-x_1x_2^3x_3^5x_4^2x_5^3x_6^6+x_1x_2^3x_3^4x_4^3x_5^6x_6^3-x_1x_2^3x_3^3x_4^6x_5^5x_6^2-x_1x_2^2x_3^5x_4^6x_5^3x_6^3-x_1x_2^2x_3^3x_4^3x_5^5x_6^6$

- $Z_2 \times S_4$

$-x_1^4x_2x_5-x_1^4x_3x_6+x_1^3x_2x_3x_4+x_1^3x_2x_4x_6+x_1^3x_3x_4x_5+x_1^3x_4x_5x_6-x_1x_2^4x_4+x_1x_2^3x_3x_5+x_1x_2^3x_5x_6+x_1x_2x_3^3x_6+x_1x_2x_3x_4^3+x_1x_2x_3x_5^3+x_1x_2x_3x_6^3+x_1x_2x_4^3x_6+x_1x_2x_5^3x_6-x_1x_3^4x_4+x_1x_3^3x_5x_6+x_1x_3x_4^3x_5+x_1x_3x_5x_6^3+x_1x_4^3x_5x_6-x_1x_4x_5^4-x_1x_4x_6^4-x_2^4x_3x_6+x_2^3x_3x_4x_5+x_2^3x_4x_5x_6-x_2x_3^4x_5+x_2x_3^3x_4x_6+x_2x_3x_4x_5^3+x_2x_3x_4x_6^3-x_2x_4^4x_5+x_2x_4x_5^3x_6-x_2x_5x_6^4+x_3^3x_4x_5x_6-x_3x_4^4x_6+x_3x_4x_5x_6^3-x_3x_5^4x_6$

- $A_5$

$$x_1^4x_2^2 + x_1^4x_3^2 + x_1^4x_4^2 + x_1^4x_5^2 + x_1^4x_6^2 + x_1^2x_2^4 - x_1^2x_2^2x_4x_5 - x_1^2x_2x_3x_4^2 - x_1^2x_2x_5^2x_6 + x_1^2x_3^4 - x_1^2x_3^2x_4x_6 - x_1^2x_3x_5x_6^2 + x_1^2x_4^4 + x_1^2x_5^4 + x_1^2x_6^4 - x_1x_2^2x_3x_5^2 - x_1x_2^2x_4^2x_6 - x_1x_2x_3^2x_6^2 - x_1x_3^2x_4^2x_5 - x_1x_4x_5^2x_6^2 + x_2^4x_3^2 + x_2^4x_4^2 + x_2^4x_5^2 + x_2^4x_6^2 + x_2^2x_3^4 - x_2^2x_3^2x_5x_6 - x_2^2x_3x_4x_6^2 + x_2^2x_4^4 + x_2^2x_5^4 + x_2^2x_6^4 - x_2x_3^2x_4x_5^2 - x_2x_4^2x_5x_6^2 + x_3^4x_4^2 + x_3^4x_5^2 + x_3^4x_6^2 + x_3^2x_4^4 + x_3^2x_5^4 + x_3^2x_6^4 - x_3x_4^2x_5^2x_6 + x_4^4x_5^2 + x_4^4x_6^2 + x_4^2x_5^4 + x_4^2x_6^4 + x_5^4x_6^2 + x_5^2x_6^4$$

- $S_3 \wr Z_2$

$$x_1^2x_2x_3^2x_5 - x_1^2x_2x_3x_4x_6 + x_1^2x_2x_3x_5^2 - x_1^2x_2x_4x_5x_6 + x_1^2x_3^2x_4x_5 + x_1^2x_3^2x_5x_6 + x_1^2x_3x_4x_5^2 + x_1^2x_3x_5^2x_6 - x_1x_2^2x_3x_4x_5 - x_1x_2^2x_3x_5x_6 + x_1x_2^2x_4^2x_6 + x_1x_2^2x_4x_6^2 - x_1x_2x_3^2x_4x_6 + x_1x_2x_3^2x_5^2 - x_1x_2x_3x_4^2x_5 - x_1x_2x_3x_5x_6^2 + x_1x_2x_4^2x_6^2 - x_1x_2x_4x_5^2x_6 + x_1x_3^2x_4x_5^2 + x_1x_3^2x_5^2x_6 - x_1x_3x_4^2x_5x_6 - x_1x_3x_4x_5x_6^2 + x_2^2x_3x_4^2x_6 + x_2^2x_3x_4x_6^2 + x_2^2x_4^2x_5x_6 + x_2^2x_4x_5x_6^2 - x_2x_3^2x_4x_5x_6 + x_2x_3x_4^2x_6^2 - x_2x_3x_4x_5^2x_6 + x_2x_4^2x_5x_6^2$$

- $S_5$

$$-x_1^2x_2^2x_3x_4 - x_1^2x_2^2x_3x_5 + x_1^2x_2^2x_3x_6 + x_1^2x_2^2x_4x_5 - x_1^2x_2^2x_4x_6 - x_1^2x_2^2x_5x_6 - x_1^2x_2x_3^2x_4 + x_1^2x_2x_3^2x_5 - x_1^2x_2x_3^2x_6 + x_1^2x_2x_3x_4^2 - x_1^2x_2x_3x_5^2 - x_1^2x_2x_3x_6^2 - x_1^2x_2x_4^2x_5 - x_1^2x_2x_4^2x_6 - x_1^2x_2x_4x_5^2 + x_1^2x_2x_4x_6^2 + x_1^2x_2x_5^2x_6 - x_1^2x_2x_5x_6^2 - x_1^2x_3^2x_4x_5 + x_1^2x_3^2x_4x_6 - x_1^2x_3^2x_5x_6 - x_1^2x_3x_4^2x_5 - x_1^2x_3x_4^2x_6 + x_1^2x_3x_4x_5^2 - x_1^2x_3x_4x_6^2 - x_1^2x_3x_5^2x_6 + x_1^2x_3x_5x_6^2 + x_1^2x_4^2x_5x_6 - x_1^2x_4x_5^2x_6 - x_1^2x_4x_5x_6^2 + x_1x_2^2x_3^2x_4 - x_1x_2^2x_3^2x_5 - x_1x_2^2x_3^2x_6 - x_1x_2^2x_3x_4^2 + x_1x_2^2x_3x_5^2 - x_1x_2^2x_3x_6^2 - x_1x_2^2x_4^2x_5 + x_1x_2^2x_4^2x_6 - x_1x_2^2x_4x_5^2 - x_1x_2^2x_4x_6^2 - x_1x_2^2x_5^2x_6 + x_1x_2^2x_5x_6^2 - x_1x_2x_3^2x_4^2 - x_1x_2x_3^2x_5^2 + x_1x_2x_3^2x_6^2 + x_1x_2x_4^2x_5^2 - x_1x_2x_4^2x_6^2 - x_1x_2x_5^2x_6^2 + x_1x_3^2x_4^2x_5 - x_1x_3^2x_4^2x_6 - x_1x_3^2x_4x_5^2 - x_1x_3^2x_4x_6^2 + x_1x_3^2x_5^2x_6 - x_1x_3^2x_5x_6^2 - x_1x_3x_4^2x_5^2 + x_1x_3x_4^2x_6^2 - x_1x_3x_5^2x_6^2 - x_1x_4^2x_5^2x_6 - x_1x_4^2x_5x_6^2 + x_1x_4x_5^2x_6^2 - x_2^2x_3^2x_4x_5 - x_2^2x_3^2x_4x_6 + x_2^2x_3^2x_5x_6 + x_2^2x_3x_4^2x_5 - x_2^2x_3x_4^2x_6 - x_2^2x_3x_4x_5^2 + x_2^2x_3x_4x_6^2 - x_2^2x_3x_5^2x_6 - x_2^2x_3x_5x_6^2 - x_2^2x_4^2x_5x_6 + x_2^2x_4x_5^2x_6 - x_2^2x_4x_5x_6^2 - x_2x_3^2x_4^2x_5 + x_2x_3^2x_4^2x_6 + x_2x_3^2x_4x_5^2 - x_2x_3^2x_4x_6^2 - x_2x_3^2x_5^2x_6 - x_2x_3^2x_5x_6^2 - x_2x_3x_4^2x_5^2 - x_2x_3x_4^2x_6^2 + x_2x_3x_5^2x_6^2 - x_2x_4^2x_5^2x_6 + x_2x_4^2x_5x_6^2 - x_2x_4x_5^2x_6^2 - x_3^2x_4^2x_5x_6 - x_3^2x_4x_5^2x_6 + x_3^2x_4x_5x_6^2 + x_3x_4^2x_5^2x_6 - x_3x_4^2x_5x_6^2 - x_3x_4x_5^2x_6^2$$

## 5.2 Reducible polynomials

- Case 1: the polynomial contains a linear factor.

As discussed in previous sections, this case is completely the same to one of the situations we've already considered.

- Case 2: the polynomial factors into 3 irreducible polynomials of degree 2.

Let $f(x) = g(x)h(x)j(x)$ where $g(x), h(x), j(x)$ are irreducible quadratics, and let $L_f$ denote the splitting field of a polynomial $f$ over $\mathbb{Q}$. As $g, h, j$ are irreducible quadratics, we know $L_g, L_h, L_j$ are generated by attaching one of the zeros to $\mathbb{Q}$, or, equivalently, by attaching $\sqrt{\Delta}$ to $\mathbb{Q}$. Thus, two of $L_g, L_h, L_j$, say $L_g$ and $L_h$, are actually the same extension, if and only if $\sqrt{\Delta(g)} = q\sqrt{\Delta(h)}$ for some $q \in \mathbb{Q}$, which is equivalent to say $\sqrt{\Delta(g)}\sqrt{\Delta(h)} \in \mathbb{Q}$. Now suppose $L_g$ and $L_h$ define different extension, we want to consider whether the remaining $L_j$ is a subfield of $L = L_g \cup L_h = \mathbb{Q}(\sqrt{\Delta(g)}, \sqrt{\Delta(h)})$. By previous discussion, if $\sqrt{\Delta(g)} = q\sqrt{\Delta(j)}$ or $\sqrt{\Delta(h)} = q\sqrt{\Delta(j)}$ then $L_j$ is certainly a subfield of $L$, so let's also assume this does not hold. Note that a basis for $L$ is $\left\{1, \sqrt{\Delta(g)}, \sqrt{\Delta(h)}, \sqrt{\Delta(g)}\sqrt{\Delta(h)}\right\}$, so if $L_j$ is a subfield of $L$, then there must exist $a, b, c, d \in \mathbb{Q}$ such that

$$a + b\sqrt{\Delta(g)} + c\sqrt{\Delta(h)} + d\sqrt{\Delta(g)}\sqrt{\Delta(h)} = \sqrt{\Delta(j)}$$

By the assumption that $\sqrt{\Delta(j)}$ is not a rational multiple of $\sqrt{\Delta(g)}$ or $\sqrt{\Delta(h)}$, we have that $b = c = 0$, and by similar method in case 3 in Section 3.2, we have that $L_j$ is a subfield of $L$ if and only if $\sqrt{\Delta(g)}\sqrt{\Delta(h)}\sqrt{\Delta(j)} \in \mathbb{Q}$.
Summarizing:

1. If the product of every pair of $\sqrt{\Delta(g)}, \sqrt{\Delta(h)}, \sqrt{\Delta(j)}$ is in $\mathbb{Q}$, then $G_f \cong S_2$
2. If $\sqrt{\Delta(g)\Delta(h)\Delta(j)} \in \mathbb{Q}$ or precisely one pair of $\sqrt{\Delta(g)}, \sqrt{\Delta(h)}, \sqrt{\Delta(j)}$ has its product in $\mathbb{Q}$, then $G_f \cong S_2 \times S_2$
3. Otherwise, $G_f \cong S_2 \times S_2 \times S_2$

- Case 3: the polynomial factors into 2 irreducible polynomials, one is of degree 2, the other is of degree 4.

Let $f(x) = g(x)h(x)$, where $g(x), h(x)$ are monic, irreducible polynomials of degrees 2 and 4 respectively. Then the question is whether the zeros of $g(x)$ are contained in the splitting field of $h(x)$. Suppose it does, let $L_g$ and $L_h$ be the splitting field over $\mathbb{Q}$ of $g$ and $h$ respectively, we have:

$$2 = |\mathrm{Gal}_g| = [L_g : \mathbb{Q}] = \frac{|L_h : \mathbb{Q}|}{|L_h : L_g|} = \frac{|\mathrm{Gal}_h|}{|\mathrm{Gal}_h(L_h/L_g)|}$$

note that $h$ must not have a zero in $L_g$. Suppose it does, then 0 cannot be its zero so it has two or four zeros in $L_g$ because it is of even degree, Having four zeros in $L_g$ means $|\mathrm{Gal}_h| = 2$, impossible; having two zeros in $L_g$ means $\mathrm{Gal}_h$ is $V_4 \cong Z_2 \times Z_2$, so it factors into two quadratic polynomials over $\mathbb{Q}$, contradiction to the assumption that it is irreducible. Thus $\mathrm{Gal}_h(L_h/L_g)$ must be a transitive subgroup of $S_4$, and this means $\mathrm{Gal}_h$, being a transitive group itself, contains a transitive subgroup having index 2. From previous discussions on transitive subgroups of $S_4$, we see that only $S_4$ (having $A_4$ as subgroup of index 2) and $D_4$ (having $Z_4$ or $V_4$ as subgroup of index 2) satisfy this. Thus, if $\mathrm{Gal}_h$ is not $S_4$ or $D_4$, then the zeros of $g(x)$ cannot be contained in the splitting field of $h(x)$ and thus $\mathrm{Gal}_f = \mathrm{Gal}_h \times Z_2$, i.e. one of $A_4 \times Z_2$, $V_4 \times Z_2$ and $Z_4 \times Z_2$.
Now suppose $\mathrm{Gal}_h$ is either $S_4$ or $D_4$, note that in both cases $\Delta(h)$ is not a quare in $\mathbb{Q}$. We would like to know when zeros of $g(x)$ are contained in the splitting field of $h(x)$. If this happens, then $\mathrm{Gal}_f = Gal_h = S_4$ or $D_4$, which have orders 24 and 8. We know a zero of $h(x)$ must generate a subfield of degree 4, thus, the quadratic subfield must be generated by both $\sqrt{\Delta(h)}$ and a zero of $g(x)$, equivalently $\sqrt{\Delta(g)}$, thus we must have $\sqrt{\Delta(g)} = q\sqrt{\Delta(h)}$ for some $q \in \mathbb{Q}$, which is equivalent to say $\sqrt{\Delta(g)}\sqrt{\Delta(h)} \in \mathbb{Q}$.
Summarizing case 3:

(i) If $\mathrm{Gal}_h = S_4$ or $D_4$ and $\sqrt{\Delta(g)}\sqrt{\Delta(h)} \in \mathbb{Q}$, then $\mathrm{Gal}_f = Gal_h$;

(ii) If $\mathrm{Gal}_h = S_4$ or $D_4$ and $\sqrt{\Delta(g)}\sqrt{\Delta(h)} \notin \mathbb{Q}$, then $\mathrm{Gal}_f = Gal_h \times Z_2$;

(iii) If $\mathrm{Gal}_h$ is neither $S_4$ or $D_4$, then $\mathrm{Gal}_f = Gal_h \times Z_2$.

- Case 4: the polynomial factors into 2 irreducible polynomials of degree 3.

Let $f(x) = g(x)h(x)$, where $g(x), h(x)$ are monic, irreducible, cubic polynomials. Note that if $g, h$ define the same extension, i.e. $L_g = L_h$, then the problem reduces to the case of irreducible polynomial of degree 3, which has been discussed. Thus we only consider $L_g \neq L_h$. By previous discussions in Section 2.1, we know both $L_g$ and $L_h$ satisfy $L = \mathbb{Q}(\alpha, \sqrt{\Delta})$ where $\alpha$ is a zero, and $[L : \mathbb{Q}] = 3$ if $\sqrt{\Delta} \in \mathbb{Q}$ or 6 otherwise. Thus if both $\sqrt{\Delta(g)}$ and $\sqrt{\Delta(h)}$ are not in $\mathbb{Q}$, then $L_g$ and $L_h$ have a common subfield of degree 2 if and only if $\sqrt{\Delta(g)} = q\sqrt{\Delta(h)}$ for some $q \in \mathbb{Q}$, which is equivalent to say $\sqrt{\Delta(g)}\sqrt{\Delta(h)} \in \mathbb{Q}$. Next, note that $L_g$ and $L_h$ have a common subfield of degree 3 if and only if there exists an isomorphism

$$\varphi : \mathbb{Q}[x]/(g) \to \mathbb{Q}[x]/(h), \quad x \mapsto ax^2 + bx + c$$

for some $a, b, c \in \mathbb{C}$. Equivalently, $g(x)$ must be sent to 0, i.e. $g(ax^2+bx+c) = 0 \mod h$. Let $g(x) = x^3 + a_2x^2 + a_1x + a_0$ and $h(x) = x^3 + b_2x^2 + b_1x + b_0$ (the fact that they are monic follows from $f$ is monic and Lemma of Gauss). Then:

$$\begin{aligned}g(ax^2+bx+c) =& a^3x^6+3a^2bx^5+(3ab^2+3a^2c+a^2a_2)x^4+(b^3+6abc+2aba_2)x^3\\ & (3ac^2+b^2a_2+3b^2c+2aca_2+aa_1)x^2\\ & (3bc^2+2bca_2+ba_1)x+ca_1+a_0+c^3+c^2a_2\end{aligned}$$

On the other hand, let $q(x)=q_3x^3+q_2x^2+q_1x+q_0\in\mathbb{Q}[x]$ be arbitrary. Then:

$$\begin{aligned}h(x)q(x) =& (x^3+b_2x^2+b_1x+b_0)(q_3x^3+q_2x^2+q_1x+q_0)\\ =& q_3x^6+(q_2+b_2q_3)x^5+(b_1q_3+q_1+b_2q_2)x^4+(b_0q_3+b_2q_1+q_0+b_1q_2)x^3\\ & +(b_0q_2+b_2q_0+b_1q_1)x^2+(b_1q_0+b_0q_1)x+b_0q_0\end{aligned}$$

Thus if there exists $q_3, q_2, q_1q_0\in\mathbb{Q}$ making the above two expressions equal, then $L_g$ and $L_h$ have a common subfield of degree 3.
Summarizing case 4:

(i) If $L_g, L_h$ don't have a common cubic subfield and both $\sqrt{\Delta(g)}, \sqrt{\Delta(h)}\in\mathbb{Q}$ (so their product is also in $\mathbb{Q}$) then $\mathrm{Gal}_f\cong A_3\times A_3$;

(ii) If $L_g, L_h$ don't have a common cubic subfield and precisely one of $\sqrt{\Delta(g)}$, $\sqrt{\Delta(h)}$ lies in $\mathbb{Q}$ (so their product is not in $\mathbb{Q}$), then $\mathrm{Gal}_f\cong S_3\times A_3$ ;

(iii) If $L_g, L_h$ don't have a common cubic subfield, neither of $\sqrt{\Delta(g)}, \sqrt{\Delta(h)}$ lies in $\mathbb{Q}$ and their product is not in $\mathbb{Q}$, then $\mathrm{Gal}_f\cong S_3\times S_3$;

(iv) If $L_g, L_h$ don't have a common cubic subfield and neither of $\sqrt{\Delta(g)}, \sqrt{\Delta(h)}$ lies in $\mathbb{Q}$, but their product is in $\mathbb{Q}$, then again $\mathrm{Gal}_f\cong S_3\times A_3$;

(v) If $L_g, L_h$ have a common cubic subfield, then $\mathrm{Gal}_f$ is one of $S_3\times Z_2$, $A_3\times Z_2$ and $S_3$, depending whether they have and share a common quadratic subfield or not.

## 5.3 Examples

Since in this section, the resolvents are generally of much higher degrees and have much more coefficients than in previous cases, I would like to determine the Galois group of a polynomial by a different way using Magma, without having to compute the coefficients of the resolvent explicitly. But essentially we are still using the facts we obtained about resolvents.

**Example 5.1.** *Let's construct a monic, irreducible polynomial $f(x)$ of degree 6 in $\mathbb{Z}[x]$ that has $\mathbb{Z}_6$ as $\mathrm{Gal}_f$. By Theorem 1.14, this happens if and only if we can construct a separable of degree $\frac{|S_6|}{|S_3|}=120$. The idea is the following:*

- ***Step 1**. Take a polynomial $F\in\mathbb{Q}[x_1,..,x_6]$ such that $Stab(F)=Z_6$*

*I take $h(x_1,..,x_6)$ to be:*

```
inv:=InvariantsOfDegree(Z6,5);
h:=inv[41]-inv[40];
```

- ***Step 2***. *Take a polynomial $f(x)$ whose Galois group to be determined.*

*Based on Example 2.3, I'm guessing that the minimal polynomial of $\varepsilon + \frac{1}{\varepsilon}$ could have its Galois group isomorphic to $\mathbb{Z}_6$, where $\varepsilon$ is the $2 \cdot 6 + 1 = 13$-th root of unity. The minimal polynomial can be determined to be $f(x) = x^6 + x^5 - 5x^4 - 4x^3 + 6x^2 + 3x - 1$. (Many ways to do that, I used WolframAlpha by simply typing in $-(-1)^{(1/13)} + 1/(-(-1)^{(1/13)})$ and the result displays its minimal polynomial, among other things). Its discriminant is $371293 = 13^5$, thus $\mathrm{Gal}_f$ cannot be a subgroup of $A_6$ so it could be $Z_6$, hence at least we didn't make a mistake from the beginning.*

- ***Step 3***. *Obtain the splitting field $K$ of $f$ in the form of $K = \mathbb{Q}(a)$, and the 6 different zeros of $f(x)$*

*Here we already have it: $a = \varepsilon + \frac{1}{\varepsilon}$, and the other roots are obtained by repeatedly squaring and subtracting 2 (again, compare Example 2.3). But for other functions we might still need to do this again.*

- ***Step 4***. *Obtain different $\sigma_i h(x_1, .., x_6)$, where $\sigma_i$ are representatives $S_6/Z_6$;*

*Since the index of $Z_6$ is 120, we should obtain 120 different $\sigma_i h$ here.*

- ***Step 5***. *Evaluate those $\sigma_i h(x_1, .., x_6)$ at the zeros of $f(x)$.*

*If the number of different outcome equals 120, then the resolvent is separable; moreover, if in these outcomes we can found a rational number, then by Theorem 1.14 $\mathrm{Gal}_f \cong Z_6$.*
*Summarizing, we can achieve this by the following command in Magma:*

```
Q:=Rationals();P<x>:=PolynomialRing(Q);
f:=x^6+x^5-5*x^4-4*x^3+6*x^2+3*x-1;
Z6:=MatrixGroup<6,Q | [0,0,0,0,0,1, 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]>;
inv:=InvariantsOfDegree(Z6,5);
h:=inv[41]-inv[40];
orb:=h^Sym(6);
#orb;
K<a>:=SplittingField(f);
rt:=Roots(f, K);
PK<x1,x2,x3,x4,x5,x6>:=PolynomialRing(K,6);
zeroes:=[ rt[i][1] : i in [1..6]];
#{Evaluate(PK!G,zeroes) : G in orb};
{Evaluate(PK!G,zeroes) : G in orb}
```

*The result contains 2 numbers and a list. The first number is the number of different $\sigma_i h(x_1, .., x_6)$, if it is less than the index of the transitive subgroup $G$ we are considering, then $Stab(h) \neq G$ so we need to try a different $h$. The second number is the number of different $\sigma_i h(x_1, .., x_6), x_i \mapsto a_i$, i.e. the zeros of the resolvent. If this number is not equal to the index, then we also need to try a different $h(x_1, .., x_6)$. Assume both numbers are equal to the index, in the list, see if there is a rational number in it, if there is then $\mathrm{Gal}_f$ is conjugate to a subgroup of $G$ by Theorem 1.14; if not, either try a different $h(x_1, .., x_6)$ or $\mathrm{Gal}_f$ is not conjugate to a subgroup of $G$.*
*In our case, both numbers are 120 and there is a number 13 in the list, thus $\mathrm{Gal}_f \cong Z_6$.*

**Example 5.2.** *Let $f(x) = x^6 + 2x^5 + 3x^4 + 5x^3 + 8x^2 + 13x + 21$, $\Delta(f) = -60209295851 = -41 \cdot 113 \cdot 12995747$ which is not a square in $\mathbb{Q}$, thus $\mathrm{Gal}_f$ cannot be a subgroup of $A_6$. Furthermore, we have:*

$$\begin{aligned} f(x) =& x(x^5 + 2x^4 + 2x^2 + 2x + 1) \quad mod \quad 3 \\ =& (x + 7)\left(x^2 + x + 6\right)\left(x^3 + 11x^2 + 4x + 9\right) \quad mod \quad 17 \end{aligned}$$

*By Corollary 5.2 (3) and (5), $\mathrm{Gal}_f \cong S_6$.*

**Example 5.3.** *Let $f(x) = x^6 + 2x^5 + 3x^4 + 5x^3 + 8x^2 + 13x + 21$, $\Delta(f) = -13424896 = -(3664)^2$ which is not a square in $\mathbb{Q}$. Hence $\mathrm{Gal}_f$ is not a subgroup of $A_6$. Using similar method in Example 5.1 by changing the 2nd to 5th lines to this:*

```
f:=x^6 + x^5 - 3*x^4 - 2*x^3 - 3*x^2 + x + 1;
Z2S4:=MatrixGroup<6,Q | [0,0,0,0,1,0, 0,0,0,0,0,1, 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, 0,0,0,1,0,0,
0,0,1,0,0,0, 0,1,0,0,0,0,1,0,0,0,0,0, 0,0,0,0,0,1],[1,0,0,0,0,0,
0,1,0,0,0,0, 0,0,0,0,0,1,0,0,0,1,0,0, 0,0,0,0,1,0, 0,0,1,0,0,0]>;
inv:=InvariantsOfDegree(Z2S4,5);
h:=inv[13]-inv[14];
```

*Both numbers in the result are 15, which is equal to the index of $Z_2 \times S_4$, thus $\mathrm{Gal}_f$ is conjugate to a transitive subgroup of $Z_2 \times S_4$. Furthermore, $f(x) = (x^2 + 24x + 1)(x^4 + 6x^3 + 26x^2 + 6x + 1)$ mod 29, thus by Corollary 5.2, $\mathrm{Gal}_f \cong Z_2 \times S_4$*

**Example 5.4.** *Let $f(x) = x^6 - 24x^4 + 21x^2 + 9x + 1$, $\Delta(f) = 13775482161 = 3^{12} \cdot 7^2 \cdot 23^2$, thus $\mathrm{Gal}_f$ is a subgroup of $A_6$. Moreover:*

$$\begin{aligned} f(x) =& (x + 1)(x^5 + x^4 + x^3 + x^2 + 1) \quad mod \quad 2 \\ =& (x + 5)^3(x^3 + 6x^2 + 6) \quad mod \quad 7 \end{aligned}$$

*Thus, $\mathrm{Gal}_f \cong A_6$ by Corollary 5.1 (4).*

# References

[1] David Cox. *Galois Theory.* Wiley, 2012.

[2] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer, 1996.

[3] Serge Lang. *Algebra, revised third edition.* Springer, 2000.

[4] Michael Artin. *Algebra, second edition.* Prentice-HaIl, Inc., 1991.

[5] Arturas Dubickas. Polynomials irreducible by eisenstein's criterion. *Applicable Algebra in Engineering, Communication and Computing*, 2003.

[6] David S. Dummit and Richard M. Foote. *Algebraic algebra, third edition.* Wiley, 2004.

[7] M. Fried and S. Friedland. A discriminant criteria for reducibility of a polynomial. *Israel Journal of Mathematics*, 54(25-32), 1986.

[8] Serge Lang. *Algebraic number theory, second edition.* Springer, 1994.

[9] S. P. Novikov B. A. Dubrovin, A. T. Fomenko. *Modern Geometry, Methods and Applications, Part I.* Springer, 1984.

[10] Derek F. Holt. Enumerating subgroups of the symmetric group. *Contemporary Mathematics*, 2009.