Galois Group at Galois Point for Genus-One Curve

Mitsunori Kanazawa

Doctoral Program in
Information Science and Engineering
Graduate School of Science and Technology
Niigata University

Introduction

For an algebraic variety V defined over a field k, we denote by $k(V)$ the rational function field of V. For the study of transcendental extension of fields, it is important to study rational function fields. Let K/k be a transcendental extension of fields, and

$$n = tr.deg_k K$$

be the transcendence degree. Then, there exist

$$x_1, x_2, \cdots, x_n \in K$$

such that

$$K/k(x_1, \cdots, x_n)$$

is an algebraic extension of fields and

$$k(x_1, \cdots, x_n)/k$$

is a purely transcendental extension.
We define the degree of irrationality of K as follows

$$dr(K) = min\{[K : K_m] | K \supset K_m \supset k,\ K_m/k \text{ is purely transcendental extension } / \ k\}.$$

In a geometrical point of view,

$$K \supset k(x_1, \cdots, x_n) \supset k$$

means that there exists a hypersurface

$$S \subset \mathbb{P}_k{}^{n+1}$$

such that the function field of S is isomorphic to K, and $dr(K)$ is the minimal value of possible degree of defining equations of S.

THEOREM 1 (Namba). *Let C be a smooth plane curve of degree $d(\geq 2)$. Then the degree $[K : K_m]$ is $d-1$, which coincides with $dr(C)$, and the extension K/K_m is obtained by $\pi_P{}^* : k(\mathbb{P}^1) \hookrightarrow k(C)$, where π_P is the projection from C to a line l with a center $P \in C$.*

Now, let k be the ground field of our discussion, which we assume to be an algebraically closed field of characteristic zero. Let C be an irreducible projective plane curve of degree d (≥ 3) and $k(C)$ the function field. Let P be a point in the plane

$$\mathbb{P}^2 \setminus C$$

and consider the projection from P to $\mathbb{P}^1$,

$$\pi_P : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1.$$

Restricting π_P to C, we get a surjective morphism

$$\bar{\pi}_P : C \longrightarrow \mathbb{P}^1,$$

which induces a finite extension of fields

$$\bar{\pi}_P^* : k(\mathbb{P}^1) \hookrightarrow k(C).$$

If the extension is Galois, we call P an outer Galois point for C. (In case P is on the curve C, the P is called an inner Galois point. We do not consider this case in this paper.)
Let $G = G_P$ be the Galois group

$$\mathrm{Gal}(k(C)/\bar{\pi}_P^*(k(\mathbb{P}^1))).$$

We call G the Galois group at P. By definition each element of G induces a birational transformation of C over the projective line $\mathbb{P}^1$. If C is smooth, then the element is an automorphism of C. Moreover, if $d \geq 4$, then it can be extended to a projective transformation of $\mathbb{P}^2$ and G turns out to be a cyclic group ([**9**]).
However, in case C has a singular point, several new phenomena occur, for examples, the group is not necessarily cyclic, and the element of G cannot necessarily be extended to a birational transformation of $\mathbb{P}^2$ (cf. [**11**]). It seems interesting to determine Galois group when C has a singular point (cf. [**5**]).

Here is an additional remark on an automorphism group: It is well-known that an automorphism Group of $\mathbb{P}^1$ is one of the followings :

$$Z_m, D_m, A_4, S_4 \textit{ and } A_5$$

These groups are appeared as a Galois group at a Galois point for some rational plane curve([**12**]).
Therefore naturally the following problems arise:

(i) Finds every possible automorphisms of plane elliptic curves (as varieties).
(ii) Finds every possible Galois groups at a Galois point of genus-one curve.

We treat the cases (i) and (ii) in chapter one and two respectively. We will give the defining equations of the curve when Galois group is abelian, and some more defining equations for non abelian case.
Similar study for space elliptic curves and abelian surfaces have been done in [**10**].
Note that if the characteristic of the ground field k is positive, then many new phenomena occur and there exist lots of different results. For the recent development of positive characteristic case, see [**1**].
In this paper we assume $k = \mathbb{C}$; the field of complex numbers. By a *genus-one curve* we mean it is an irreducible plane curve whose smooth model has the genus one.

We have already the following results: Every Galois group of a Galois point is a cyclic group for a non singular plane curve. We are also interested in the case where there exist more than one Galois points. How many Galois points do there exit? Do there appear two Galois groups that are not isomorphic each other for one plane curve? How is the arrangement? On the number of Galois points , Professor Hisao Yoshihara showed that there exist at most four inner Galois points and at most three outer Galois points in a non singular plane curve. Moreover if a non singular plane curve has three outer Galois points then this curve is the Ferma't curve.
In chapter three, we examine a group generated four Galois groups of a non singular plane curve.

Acknowledgment

The author would like to express his heartfelt gratitude to Professor Hisao Yoshihara for his valuable advice, guidance and encouragement. Thanks are also due to persons who met in workshop on Galois point and related topics in kanagawa university hujimi kenshuujo, and to persons who met in the first international conference of graduate students with sisterhood universities in national changhua university of educations.

Contents

CHAPTER 1

Automorphism Groups

In this chapter, we decide all finite automorphism groups on an elliptic curve E as a variety. At first we see that an automorphism on E as a variety is represented by a function of degree one on the universal covering $\mathbb{C}$ of an elliptic curve E.
Hereafter we use the following notations and conventions, where n is a positive integer.

- E : an elliptic curve
- $\mathcal{L} = \mathbb{Z} + \mathbb{Z}\omega$: the lattice defining E, where $\Im\omega > 0$
- $A(E)$: the automorphism group of E as a variety
- $e_n := exp(2\pi\sqrt{-1}/n)$
- $Z_n := \mathbb{Z}/n\mathbb{Z}$
- D_n : the dihedral group of order $2n$
- $|G|$: the order of a finite group G
- $\langle\sigma_1, \cdots, \sigma_n\rangle$: the subgroup generated by $\sigma_1, \cdots, \sigma_n$

1. Representation of automorphism

We denote E as follows.

$$E = \mathbb{C}/\mathcal{L}$$
$$\mathcal{L} = \{m + nw \mid m, n \in \mathbb{Z},\ w \notin \mathbb{R}\}.$$

Let $\sigma \in A(E)$.
$\mathbb{C}$ is an universal covering of E, there exists a regular function $\tilde{\sigma}$ such that

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{\sigma}} & \mathbb{C} \\ {\scriptstyle\pi}\downarrow & & {\scriptstyle\pi}\downarrow \\ E & \xrightarrow{\sigma} & E \end{array}$$

$$\forall\lambda \in \mathcal{L}\ :\ \tilde{\sigma}(z+\lambda) - \tilde{\sigma}(z) \in \mathcal{L}.$$

$\tilde{\sigma}$ is continuous and $\mathcal{L}$ is discrete set so we have

$$\tilde{\sigma}(z+\lambda) - \tilde{\sigma}(z)$$

is constant. To differentiate , we have

$$\forall\lambda \in \mathcal{L}\ :\ \frac{d\tilde{\sigma}}{dz}(z+\lambda) = \frac{d\tilde{\sigma}}{dz}(z)$$

This is a regular function on a elliptic curve which is a compact Riemann surface, then this is a constant function. We can denote

$$\frac{d\tilde{\sigma}(z)}{dz} = c\ (c \in \mathbb{C})$$

and we have

$$\tilde{\sigma}(z) = cz + d.$$

Here we note that c is not zero because σ is an automorphism. For the commutativity of the above diagram, we have

$$\sigma(z) = cz + d.$$

By the coordinate exchange z to

$$z - \frac{d}{c},$$

we may assume

$$\sigma(z) = cz$$

and we have

$$c\mathcal{L} \subset \mathcal{L}.$$

This induce relations

(1)
$$\begin{gathered} c = m_1 + m_2\omega \\ c\omega = n_1 + n_2\omega \\ m_1, m_2, n_1, n_2 \in \mathbb{Z} \end{gathered}$$

σ has a finite order then

$$\exists n \in \mathbb{N} \ : \ c^n z - z \in \mathcal{L}.$$

So we have $c^n = 1$ and then $|c| = 1$.
If $m_2 = 0$ then c is an integer and $c = \pm 1$.
If $m_2 \neq 0$ then c is a imaginary number and

(2)
$$\omega = \frac{c - m_1}{m_2}.$$

So using (1) and (2) to eliminate ω, we have

$$c^2 - (m_1 + n_2)c - m_2 n_1 + m_1 n_2 = 0,$$

Because $|c| = 1$ and c has degree two on $\mathbb{Q}$,

$$c = \pm\sqrt{-1} \text{ or } \frac{\pm 1 \pm \sqrt{-3}}{2}.$$

Because of $\mathbb{Q}(c) = \mathbb{Q}(\omega)$ in the case that c is imaginary, we have

(i) In the case of $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-1})$.

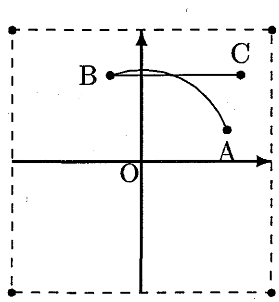
$$c = 1, -1, \sqrt{-1} \text{ or } -\sqrt{-1}.$$

(ii) In the case of $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$.

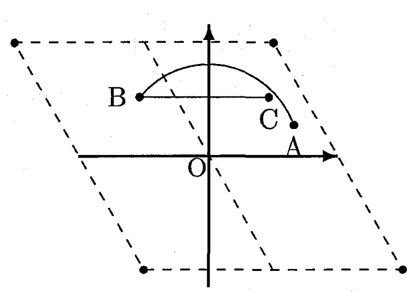
$$c = 1, -1, \frac{-1 + \sqrt{-3}}{2}, \frac{-1 - \sqrt{-3}}{2}, \frac{1 - \sqrt{-3}}{2}, \frac{1 + \sqrt{-3}}{2}.$$

(iii) Otherwise.

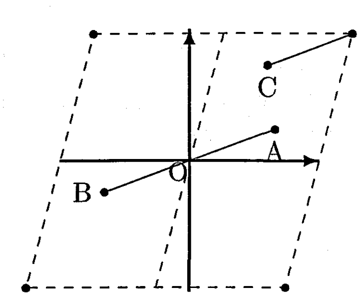
$$c = 1, -1.$$



The image of A is C by $\sigma(z) = \sqrt{-1}z$



The image of A is C by $\sigma(z) = e_3 z$



The image of A is C by $\sigma(z) = -z$

2. Finite Subgroup

Let G be a finite subgroup G $\subset A(E)$, and we define a homomorphism $\varphi : G \longrightarrow \mathbb{C}$ by $cx + d \rightarrow c$. We have $\mathrm{Im}(\varphi)$ is a cyclic group. Moreover $\mathrm{Im}(\varphi)$ is a subgroup of Z_4 or Z_6. We take c which is primitive element of $\mathrm{Im}(\varphi)$, and we take $\sigma \in G$ such that $\varphi(\sigma) = c$, and we put $\sigma(z) = cz + d$. By coordinate exchange

$$z \longrightarrow \frac{z-d}{c},$$

we may assume $G \ni cz$ so we have a split exact sequence as follows

$$1 \longrightarrow G_T \longrightarrow G \xrightarrow{\varphi} G_O \longrightarrow 1.$$

We have $G \cong G_T \rtimes G_O$. Here G_T is all translations in G and $G_O = \mathrm{Im}(\varphi)$.
If $G_T = 1$ then $G = G_O \cong 1$, Z_2, Z_3, Z_4 or Z_6.
We may assume $G_T \neq 1$.
G_T is a finite group with at most two generators , $G_T \cong Z_n$ or $Z_n \oplus Z_m$ $(m|n)$ where n,$m \in \mathbb{N}$.
If $G_O = 1$ then $G = G_T \cong Z_n$ or $Z_n \oplus Z_m$.
Now we may assume $G_O \neq 1$ furthermore.
Any element of G_T is written as $z+\tau$ $(\tau \in E)$, we identify it as τ. Because G_T is a finite group, we may assume $nG_T \subset \mathcal{L}$, so we may think $G_T \subset \frac{1}{n}\mathcal{L}$.
Moreover, we can denote

$$\tau = \frac{a+b\omega}{n}. \quad (a, b \in \mathbb{Z}).$$

We note that there exist a translator of order n, because Z_n has a generator.

LEMMA 1. *Taking $\sigma \in G_O$, $\tau \in G_T$ and we put $\sigma(z) = cz$ and $\tau(z) = z + d$, then we have*

$$\sigma\tau\sigma^{-1}(z) = \sigma\tau(c^{-1}z) = \sigma(c^{-1}z + d) = z + cd.$$

For all translations in G is in G_T, G_T is closed by inner automorphism of G_O. So we have $G_T \supset \langle \tau, \sigma\tau\sigma^{-1} \rangle$.

3. Case of $G_O = \langle -1 \rangle$

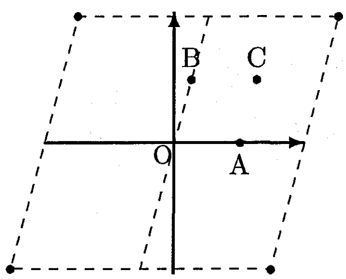
Let $\sigma(z) = -z$, $\tau(z) = z + \frac{a+b\omega}{n}$.

$$\begin{aligned} & \tau \text{ and } \sigma \text{ are commutative each other} \\ \Longleftrightarrow\ & \sigma\tau\sigma^{-1} = \tau \\ \Longleftrightarrow\ & \frac{-a-b\omega}{n} = \frac{a+b\omega}{n} \\ \Longleftrightarrow\ & \frac{2a+2b\omega}{n} \in \mathcal{L} \\ \Longleftrightarrow\ & 2a \equiv 2b \equiv 0 \mod n. \end{aligned}$$

The order of $\tau = n$, G.C.D.(a, b) and n are relatively prime. We have $n = 2$ and the order of τ=2.
A subgroup H of G_T has generators at most two, an abelian group in G including σ is one of the following :

$$\langle \sigma \rangle, \langle \sigma \rangle \times \langle \tau_1 \rangle, \langle \sigma \rangle \times \langle \tau_1 \rangle \times \langle \tau_2 \rangle.$$

Where $\tau_1 \neq \tau_2$, order of $\tau_1 = 2$, order of $\tau_2 = 2$.



Only three points A, B, C are translations of order two

Three translations exist and they correspond to

$$\frac{1}{2}, \frac{\omega}{2}, \frac{1+\omega}{2}.$$

For example

$$\langle -1\rangle,\ \langle -1\rangle \times \left\langle \frac{1}{2} \right\rangle,\ \langle -1\rangle \times \left\langle \frac{1}{2} \right\rangle \times \left\langle \frac{\omega}{2} \right\rangle.$$

So a finite abelian subgroup of $A(E)$ is one of the followings :

$$Z_2,\ {Z_2}^{\oplus 2},\ {Z_2}^{\oplus 3}.$$

If G is not abelian then

$$G \cong \langle\sigma\rangle \ltimes \langle\tau_1\rangle, \langle\sigma\rangle \ltimes \langle\tau_1, \tau_2\rangle$$
$$\text{where } \langle\tau_1\rangle \not\ni \tau_2.$$

The order of these groups are $2n$ and $2nm$ $(m \mid n)$. Relations between generators are

$$\sigma\tau_1\sigma^{-1} = {\tau_1}^{-1}, \sigma\tau_2\sigma^{-1} = {\tau_2}^{-1}, \tau_1\tau_2 = \tau_2\tau_1$$

$\langle\sigma\rangle \ltimes \langle\tau_1\rangle$ is a dihedral group.
$\langle\sigma\rangle \ltimes \langle\tau_1, \tau_2\rangle$ is similar to dihedral group, so we define as follows.

DEFINITION 1. BD_{mn} is called a bidihedral group which is generated by σ, τ and τ' with relations

$$\sigma^2 = 1,\quad \tau^{mn} = 1,\quad \tau'^{m} = 1,$$
$$\sigma\tau\sigma^{-1} = \tau^{-1},\quad \sigma\tau'\sigma^{-1} = \tau'^{-1},\quad \tau\tau' = \tau'\tau.$$

4. Case of G_T has one generator

We may assume $|G_O| > 2$. Let $n = |G_T|$ and we take a generator $\tau \in G_T$.From Lemma 1, we have $\langle\tau\rangle \supset \langle\sigma\tau\sigma^{-1}\rangle$ for any $\sigma \in G_O$. $\sigma\tau\sigma^{-1}$ has the same order to τ, then we have $\langle\tau\rangle = \langle\sigma\tau\sigma^{-1}\rangle$. Let σ be a generator of G_O and we put

$$\sigma(z) = cz \text{ and } \tau = \frac{a+b\omega}{n}.$$

We have

$$\sigma\tau\sigma^{-1} = \frac{ac+bc\omega}{n}.$$

Moreover we note that the G.C.D.(a, b) and n is relatively prime.

4.1. Case of $\omega = e_3$ and $c = e_3$. We have

$$\begin{aligned} & e_3 \cdot \frac{a + be_3}{n} = k \cdot \frac{a + be_3}{n} \\ \iff & \frac{ae_3 + b(e_3)^2}{n} = \frac{ka + kbe_3}{n} \\ \iff & \frac{ae_3 + b(-e_3 - 1)}{n} = \frac{ka + kbe_3}{n} \\ \iff & \frac{-b + (a - b)e_3}{n} = \frac{ka + kbe_3}{n} \\ \iff & ka \equiv -b \text{ and } kb \equiv a - b \mod n. \end{aligned}$$

We have

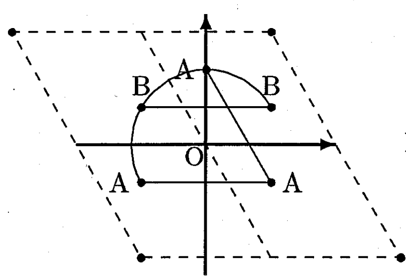
$$(k^2 + k + 1)a \equiv (k^2 + k + 1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2 + k + 1.$$

If σ and τ are commutative then $n \mid 1 + 1 + 1$ so we have $n = 3$.
In this case Abelian group appears as $Z_3 \oplus Z_3$. Generators of translations are

$$\frac{1 + 2\omega}{3}, \ \frac{2 + \omega}{3}.$$



Only two points A, B are translations which is invariant by inner automorphism of $\sigma(z) = e_3 z$. Namely only these translations are commutative with σ.

Indeed for $\sigma = e_3$ and $\tau = \frac{1+2e_3}{3}$, $\sigma\tau\sigma^{-1} = \tau$ holds.

4.2. Case of $\omega = e_3$ and $c = -e_3$. We have

$$\begin{aligned} & -e_3 \cdot \frac{a + be_3}{n} = k \cdot \frac{a + be_3}{n} \\ \iff & \frac{-ae_3 - b(e_3)^2}{n} = \frac{ka + kbe_3}{n} \\ \iff & \frac{-ae_3 - b(-e_3 - 1)}{n} = \frac{ka + kbe_3}{n} \\ \iff & \frac{b - (a - b)e_3}{n} = \frac{ka + kbe_3}{n} \\ \iff & ka \equiv b \text{ and } kb \equiv -a + b \mod n. \end{aligned}$$

We have

$$(k^2 - k + 1)a \equiv (k^2 - k + 1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2 - k + 1.$$

If σ and τ are commutative then $n \mid 1 - 1 + 1$, so we have $n = 1$.
In this case , No Abelian group appears.

4.3. Case of $\omega = e_3$ and $c = e_6 = -(e_3)^2$. We have

$$\begin{aligned} & -(e_3)^2 \cdot \frac{a+be_3}{n} = k \cdot \frac{a+be_3}{n} \\ \iff & \frac{-a(e_3)^2 - b(e_3)^3}{n} = \frac{ka+kbe_3}{n} \\ \iff & \frac{-b-a(-e_3-1)}{n} = \frac{ka+kbe_3}{n} \\ \iff & \frac{a-b+ae_3}{n} = \frac{ka+kbe_3}{n} \\ \iff & ka \equiv a-b \text{ and } kb \equiv a \mod n. \end{aligned}$$

We have

$$(k^2-k+1)a \equiv (k^2-k+1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2-k+1.$$

If σ and τ are commutative then $n \mid 1-1+1$, so we have $n=1$.
In this case , No Abelian group appears.

4.4. Case of $\omega = e_3$ and $c = -e_6 = (e_3)^2$. We have

$$\begin{aligned} & (e_3)^2 \cdot \frac{a+be_3}{n} = k \cdot \frac{a+be_3}{n} \\ \iff & \frac{a(e_3)^2 + b(e_3)^3}{n} = \frac{ka+kbe_3}{n} \\ \iff & \frac{a(-e_3-1)+b}{n} = \frac{ka+kbe_3}{n} \\ \iff & \frac{-a+b-ae_3}{n} = \frac{ka+kbe_3}{n} \\ \iff & ka \equiv -a+b \text{ and } kb \equiv -a \mod n. \end{aligned}$$

We have

$$(k^2+k+1)a \equiv (k^2+k+1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2+k+1.$$

If σ and τ are commutative then $n \mid 1+1+1$, so we have $n=3$.
In this case Abelian group appears as $Z_3 \oplus Z_3$.
Indeed for $\sigma = (e_3)^2$ and $\tau = \frac{1+2e_3}{3}$, $\sigma\tau\sigma^{-1} = \tau$ holds.

4.5. Case of $\omega = e_4$ and $c = e_4$. We have

$$\begin{aligned} & e_4 \cdot \frac{a+be_4}{n} = k \cdot \frac{a+be_4}{n} \\ \iff & \frac{-b+ae_4}{n} = \frac{ka+kbe_4}{n} \\ \iff & ka \equiv -b \text{ and } kb \equiv a \mod n. \end{aligned}$$

We have

$$(k^2+1)a \equiv (k^2+1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2+1.$$

If σ and τ are commutative then $n \mid 1+1$, so we have $n=2$.

In this case Abelian group appears as $Z_4 \oplus Z_2$.
Indeed for $\sigma = e_4$ and $\tau = \frac{1+e_4}{2}$, $\sigma\tau\sigma^{-1} = \tau$ holds.

4.6. Case of $\omega = e_4$ and $c = -e_4$. We have

$$\begin{aligned} & - e_4 \cdot \frac{a+be_4}{n} = k \cdot \frac{a+be_4}{n} \\ \Longleftrightarrow \quad & \frac{b-ae_4}{n} = k\frac{ka+kbe_4}{n} \\ \Longleftrightarrow \quad & ka \equiv b \text{ and } kb \equiv -a \mod n. \end{aligned}$$

We have

$$(k^2+1)a \equiv (k^2+1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2+1.$$

If σ and τ are commutative then $n \mid 1+1$, so we have $n = 2$.
In this case Abelian group appears as $Z_4 \oplus Z_2$.
Indeed for $\sigma = -e_4$ and $\tau = \frac{1+e_4}{2}$, $\sigma\tau\sigma^{-1} = \tau$ holds.

4.7. Case of $\omega = e_6$ and $c = e_3 = (e_6)^2$. We have

$$\begin{aligned} & (e_6)^2 \cdot \frac{a+be_6}{n} = k \cdot \frac{a+be_6}{n} \\ \Longleftrightarrow \quad & \frac{a(e_6)^2+b(e_6)^3}{n} = \frac{ka+kbe_6}{n} \\ \Longleftrightarrow \quad & \frac{-b+a(e_6-1)}{n} = \frac{ka+kbe_6}{n} \\ \Longleftrightarrow \quad & \frac{-a-b+ae_6}{n} = \frac{ka+kbe_6}{n} \\ \Longleftrightarrow \quad & ka \equiv -a-b \text{ and } kb \equiv a \mod n. \end{aligned}$$

We have

$$(k^2+k+1)a \equiv (k^2+k+1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2+k+1.$$

If σ and τ are commutative then $n \mid 1+1+1$, so we have $n = 3$.
In this case Abelian group appears as $Z_3 \oplus Z_3$.
Indeed for $\sigma = e_3$ and $\tau = \frac{1+e_6}{3}$, $\sigma\tau\sigma^{-1} = \tau$ holds.

4.8. Case of $\omega = e_6$ and $c = -e_3 = -(e_6)^2$. We have

$$\begin{aligned} & -(e_6)^2 \cdot \frac{a+be_6}{n} = k \cdot \frac{a+be_6}{n} \\ \Longleftrightarrow \quad & \frac{-a(e_6)^2-b(e_6)^3}{n} = \frac{ka+kbe_6}{n} \\ \Longleftrightarrow \quad & \frac{b-a(e_6-1)}{n} = \frac{ka+kbe_6}{n} \\ \Longleftrightarrow \quad & \frac{(a+b)-ae_6}{n} = \frac{ka+kbe_6}{n} \\ \Longleftrightarrow \quad & ka \equiv a+b \text{ and } kb \equiv -a \mod n. \end{aligned}$$

We have

$$(k^2-k+1)a \equiv (k^2-k+1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2-k+1.$$

If σ and τ are commutative then $n \mid 1-1+1$, so we have $n=1$. In this case , No Abelian group appears.

4.9. Case of $\omega = e_6$ and $c = e_6$. We have

$$\begin{aligned} e_6 \cdot \frac{a+be_6}{n} &= k \cdot \frac{a+be_6}{n} \\ \iff \frac{ae_6+b(e_6)^2}{n} &= \frac{ka+kbe_6}{n} \\ \iff \frac{ae_6+b(e_6-1)}{n} &= \frac{ka+kbe_6}{n} \\ \iff \frac{-b+(a+b)e_6}{n} &= \frac{ka+kbe_6}{n} \\ \iff ka \equiv -b \text{ and } kb &\equiv a+b \mod n. \end{aligned}$$

We have

$$(k^2-k+1)a \equiv (k^2-k+1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2-k+1.$$

If σ and τ are commutative then $n \mid 1-1+1$, so we have $n=1$. In this case , No Abelian group appears.

4.10. Case of $\omega = e_6$ and $c = -e_6$. We have

$$\begin{aligned} -e_6 \cdot \frac{a+be_6}{n} &= k \cdot \frac{a+be_6}{n} \\ \iff \frac{-ae_6-b(e_6)^2}{n} &= \frac{ka+kbe_6}{n} \\ \iff \frac{-ae_6-b(e_6-1)}{n} &= \frac{ka+kbe_6}{n} \\ \iff \frac{b-(a+b)e_6}{n} &= \frac{ka+kbe_6}{n} \\ \iff ka \equiv b \text{ and } kb &\equiv -a-b \mod n. \end{aligned}$$

We have

$$(k^2+k+1)a \equiv (k^2+k+1)b \equiv 0 \mod n,$$

so we have

$$n \mid k^2+k+1.$$

If σ and τ are commutative then $n \mid 1+1+1$, so we have $n=3$. In this case Abelian group appears as $Z_3 \oplus Z_3$. Indeed for $\sigma = -e_6$, $\tau = \frac{1+e_6}{3}$, $\sigma\tau\sigma^{-1} = \tau$ holds.

LEMMA 2. *$G \cong G_O \ltimes G_T$ is one of the followings :*

(i) $Z_3 \ltimes Z_n$ *, for some $k \in \mathbb{Z}$ such that* $n|k^2+k+1$
(ii) $Z_4 \ltimes Z_n$ *, for some $k \in \mathbb{Z}$ such that* $n|k^2+1$
(iii) $Z_6 \ltimes Z_n$ *, for some $k \in \mathbb{Z}$ such that* $n|k^2-k+1$

If G is abelian then G is one of the following :

$$Z_3 \oplus Z_3, Z_4 \oplus Z_2$$

5. Condition of n

Concerning the possibility of n of the Lemma2 we note the following,

PROPOSITION 3. *A rational integer n ($n > 1$) satisfies that $n \mid k^2 + 1$ for some rational integer k if and only if n equals to a product N of rational prime integers which is equivalent to 1 modulo 4 or n equals to $2N$.*

PROPOSITION 4. *A rational integer n ($n > 1$) satisfies that $n \mid k^2 + k + 1$ for some rational integer k if and only if n equals to a product N of rational prime integers which is equivalent to 1 modulo 3 or n equals to $3N$.*

5.1. Proof of Prop.3. At first we assume a rational integer n satisfies that $n \mid k^2+1$ for some rational integer k. $\mathbb{Z}[e_4] = \mathbb{Z}[\sqrt{-1}]$ is UFD because $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean Domain. We decompose n to primes in $\mathbb{Z}[\sqrt{-1}]$ as follows.

$$n = p_1 p_2 \cdots p_l \mid 1 + k^2 = (1 + k\sqrt{-1})(1 - k\sqrt{-1}).$$

Each p_j are a divisor of $1 + k\sqrt{-1}$ or $1 - k\sqrt{-1}$. If p_j is a divisor of $1 + k\sqrt{-1}$ then we can write $p_j(a + b\sqrt{-1}) = 1 + k\sqrt{-1}$. If p_j is a rational integer then $p_j a = 1$ holds, and it is contradicts that p_j is a prime number. So each prime divisors in the decomposition of n in $\mathbb{Z}$ are 2 or an odd prime number equivalent to 1 modulo 4. If p_j is a divisor of $1 - k\sqrt{-1}$ then same discussion holds. If two prime divisor 2 are included in n then we have one of followings :

$$\begin{aligned}
(1 + \sqrt{-1})^2 = 2\sqrt{-1} &\mid 1 + k\sqrt{-1}, \\
(1 + \sqrt{-1})(1 - \sqrt{-1}) = 2 &\mid 1 + k\sqrt{-1}, \\
(1 + \sqrt{-1})^2 = 2\sqrt{-1} &\mid 1 - k\sqrt{-1}, \\
(1 + \sqrt{-1})(1 - \sqrt{-1}) = 2 &\mid 1 - k\sqrt{-1}.
\end{aligned}$$

This contradicts that both $1 + k\sqrt{-1}$ and $1 - k\sqrt{-1}$ hasn't divisor 2. So there is at most one prime divisor 2 in n.
Secondly we see the reverse holds by using three lemmas below.

LEMMA 5. *Let p be an odd prime number which is equivalent to 1 modulo 4. For any positive integer n, there exist integers a and b such that*

$$p^{2^n} = a^2 + b^2, \quad ab \neq 0, \quad a \neq b, \quad a > 0, \quad b > 0, \quad (a, b) = 1.$$

LEMMA 6. *For integers a, b, c, d such that*

$$(a, b) = 1, \quad (c, d) = 1, \quad (a^2 + b^2, c^2 + d^2) = 1,$$

we can write

$$(a^2 + b^2)(c^2 + d^2) = A^2 + B^2$$

for some rational integer A and B that are relatively prime.

LEMMA 7. *If two positive integer a and b are relatively prime each other then $a^2 + b^2$ is a divisor of $1 + A^2$ for some rational integer A.*

Let $n = p_0 {p_1}^{f_1} {p_2}^{f_2} \cdots {p_n}^{f_n}$ be a decomposition of rational integer n in $\mathbb{Z}$, where p_0 equals to 1 or 2 and each p_i $(i > 0)$ are different odd prime numbers each other which is equivalent to 1 module 4 and each f_i are non negative integers. By multiplying suitable rational integer we assume f_i is power of 2 and let this number as N. Because $n \mid N$, it is sufficient to show that there exists rational integer A such that $N \mid 1 + A^2$. From lemma5 , we can write $p^f = a^2 + b^2$ $(a, b) = 1$ for each odd prime divisors in n.
From lemma6 , we can write $n \mid A^2 + B^2$ where $(A, B) = 1$. Even if n is even then we also can write $n \mid A^2 + B^2$ where $(A, B) = 1$.
From lemma7 , there exists a rational integer A such that N is a divisor of $1 + A^2$.

5.2. Proofs of Lemmas.

5.2.1. *Proof of Lemma5.* p is a rational prime number and $p \equiv 1 \mod 4$, we can write $p = a^2 + b^2$. Here

$$ab \neq 0, \quad a \neq b, \quad a > 0, \quad b > 0, \quad (a, b) = 1$$

because p is a odd prime number. If we assume

$$p^{2^n} = a^2 + b^2, \quad ab \neq 0, \quad a \neq b, \quad a > 0, \quad b > 0, \quad (a, b) = 1$$

then we have

$$p^{2^{n+1}} = (a^2 + b^2)(a^2 + b^2) = (a^2 - b^2)^2 + (2ab)^2.$$

Moreover

$$(a^2 - b^2)ab \neq 0, \quad a^2 - b^2 \neq 2ab$$

because a and b have different parity,

$$(a^2 - b^2, 2ab) = 1.$$

And then by mathematical induction we have done.

5.2.2. *Proof of Lemma6.* Generally we have

$$(a^2 + b^2)(c^2 + d^2) = (ad - bc)^2 + (ac + bd)^2.$$

Putting $\alpha = ad - bc$ and $\beta = ac + bd$. We have the followings.

$$\begin{aligned} \alpha c - \beta d &= -b(c^2 + d^2), \\ \alpha d + \beta c &= a(c^2 + d^2), \\ \alpha a + \beta b &= d(a^2 + b^2), \\ \alpha b - \beta a &= -c(a^2 + b^2). \end{aligned}$$

Then the common divisor of α and β is 1 because

$$(a, b) = 1, \quad (c, d) = 1, \quad (a^2 + b^2, c^2 + d^2) = 1.$$

5.2.3. *Proof of Lemma7.* For $(a, b) = 1$, there exist a pair of rational integer (x, y) such that $ax + by = 1$. Because

$$(a + bi)(x - yi) = (ax + by) + (-ay + bx)i,$$

we have

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2 = 1 + (ay - bx)^2.$$

5.3. Proofs of Prop.4. At first we assume n satisfies $n \mid 1+k+k^2$ for some integer k. We note that $1+k+k^2$ is odd and n is odd. $\mathbb{Z}[\sqrt{-3}]$ is UFD because $\mathbb{Z}[\sqrt{-3}]$ is a Euclidean Domain. We decompose n to primes as follows.

$$\begin{aligned} n = p_1 p_2 \cdots p_l \mid 1+k+k^2 &= (1-ke_3)(1-k(e_3)^2) \\ &= \frac{2+k-k\sqrt{-3}}{2} \cdot \frac{2+k+k\sqrt{-3}}{2} \Bigg| \ (2+k-k\sqrt{-3})(2+k+k\sqrt{-3}). \end{aligned}$$

Each p_j are a divisor of $2+k-k\sqrt{-3}$ or $2+k+k\sqrt{-3}$. We may assume p_j is a divisor of $2+k-k\sqrt{-3}$, we can write $p_j(a+b\sqrt{-3}) = 2+k-k\sqrt{-3}$ for some rational integers a, b. If p_j is a rational integer then $p_j a = 2+k$ and $p_j b = -k$ so we have $p_j(a+b) = 2$, but it is contradiction that p_j is odd prime.
So each prime divisors in the decomposition of n in $\mathbb{Z}$ are 3 or an odd prime number which is equivalent to 1 modulo 3.
Because the decomposition of the rational number 3 is $-\sqrt{-3} \cdot \sqrt{-3}$ in $\mathbb{Z}[\sqrt{-3}]$, if two prime divisor 3 are included in n then we have one of followings :

$$\begin{aligned} 3 &\mid 2+k-k\sqrt{-3}, \\ 3 &\mid 2+k+k\sqrt{-3} \end{aligned}$$

This is contradiction and there is at most one divisor 3 in decomposition of n.
Secondly we see the reverse holds by using three lemmas below.

LEMMA 8. *Let p be a odd prime number which is equivalent to 1 modulo 3, there exists rational integers a and b such that*

$$p^{2^n} = a^2 + 3b^2, \quad ab \neq 0, \quad a \neq b, \quad a > 0, \quad b > 0, \quad (a,b) = 1.$$

LEMMA 9. *For integers a, b, c, d such that*

$$(a,b) = 1, \quad (c,d) = 1, \quad (a^2+3b^2, c^2+3d^2) = 1$$

there exists relatively prime rational integers A and B such that

$$(a^2+3b^2)(c^2+3d^2) = A^2 + 3B^2.$$

LEMMA 10. *Odd number a^2+3b^2 ($(a,b)=1$) is a divisor of $1+A+A^2$ for some rational integer A.*

Let $n = p_0 {p_1}^{f_1} {p_2}^{f_2} \cdots {p_n}^{f_n}$ be a decomposition of rational integer n in $\mathbb{Z}$, where p_0 equals to 1 or 3 and each p_i ($i > 0$) are different odd prime numbers each other which is equivalent to 1 module 3, each f_i are non negative integers. By multiplying suitable rational integer we assume f_i is power of 2 and let this number as N. Because $n \mid N$, it is sufficient to show that there exists rational integer A such that $N \mid 1+A+A^2$. From Lemma8 , we can write $p^f = a^2+3b^2$ $(a,b)=1$ for each odd prime divisors p.
From Lemma9 , we can write products of these numbers as A^2+3B^2 ($(A,B)=1$). If $3 \mid n$ then $3(A^2+3B^2) = (3B)^2 + 3A^2$, $(3B, A) = 1$. It is because 3 doesn't divide A^2+3B^2 then 3 doesn't divide A and $(A,B)=1$.
From Lemma10 , there exists a rational integer A such that N is a divisor of $1+A+A^2$.

5.4. Proofs of Lemmas.

5.4.1. *Proof of Lemma8.* p is a prime number and $p \equiv 1 \mod 3$, we can write $p = a^2 + 3b^2$. $ab \neq 0$, $a \neq b$, $a > 0$, $b > 0$, $(a, b) = 1$ because p is a odd prime number. If we assume

$$p^{2^n} = a^2 + 3b^2, \quad ab \neq 0, \quad a \neq b, \quad a > 0, \quad b > 0, \quad (a, b) = 1$$

then we have

$$p^{2^{n+1}} = (a^2 + 3b^2)(a^2 + 3b^2) = (a^2 - 3b^2)^2 + 3(2ab)^2.$$

Moreover

$$\begin{aligned}(a^2 - 3b^2)ab &\neq 0,\\ a^2 - 3b^2 &\neq 2ab,\\ (a^2 - 3b^2, 2ab) &= 1.\end{aligned}$$

And then by mathematical induction we have done.

5.4.2. *Proof of Lemma9.* Generally we have

$$(a^2 + 3b^2)(c^2 + 3d^2) = 3(ad + bc)^2 + (ac - 3bd)^2.$$

Putting $\alpha = ad + bc$ and $\beta = ac - 3bd$. We have the followings.

$$\begin{aligned}\alpha c - \beta d &= b(c^2 + 3d^2),\\ \alpha d + \beta c &= a(c^2 + 3d^2),\\ \alpha a - \beta b &= d(a^2 + 3b^2),\\ \alpha b + \beta a &= c(a^2 + 3b^2).\end{aligned}$$

Then the common divisor of α and β is 1 because

$$\begin{aligned}(a, b) &= 1,\\ (c, d) &= 1,\\ (a^2 + 3b^2, c^2 + 3d^2) &= 1.\end{aligned}$$

5.4.3. *Proof of Lemma10.*

$$a^2 + 3b^2 = (a - \sqrt{-3}b)(a + \sqrt{-3}b) = (a - b - 2be_3)(a + b + 2be_3),$$

this is odd and $(a, b) = 1$, so we have

$$\begin{aligned}(a - b, 2b) &= 1,\\ (a + b, 2b) &= 1.\end{aligned}$$

Because $(a + b, 2b) = 1$, there exists a pair of rational integers (x, y) such that

$$(a + b)x + 2by = 1.$$

We can write

$$\begin{aligned}(a + b + 2be_3)(x - ye_3) &= (a + b)x - (a + b)ye_3 + 2bxe_3 - 2by(e_3)^2\\ &= (a + b)x - (a + b)ye_3 + 2bxe_3 + 2by(1 + e_3)\\ &= (ax + bx + 2by) + (-ay + by + 2bx)e_3\\ &= 1 - Ae_3,\\ &\text{where } A = -ay + by + 2bx \in \mathbb{Z}.\end{aligned}$$

So we have

$$\begin{aligned} a^2+3b^2 &= (a+b+2be_3)(a+b+2b(e_3)^2) \\ &= (a+b+2be_3)\overline{(a+b+2be_3)} \mid (1-Ae_3)(1-A(e_3)^2) \\ &\qquad\qquad\qquad\qquad = 1-Ae_3-A(e_3)^2+A^2(e_3)^2 \\ &\qquad\qquad\qquad\qquad = 1+A+A^2. \end{aligned}$$

6. Case of G_T has two generators

G_T is a finite group with two generators, we can write $G_T = Z_n \oplus Z_m$ $(m|n)$. For any element $\tau \in G_T$, $n\tau = 0$ thus we may assume $\tau \in \frac{1}{n}\mathcal{L}$. We put a generator of Z_n to $\tau = \frac{a+b\omega}{n}$ and we may assume $(a,b) = 1$. Because (a,b) and n are relatively prime then there exist integer x, y such that $x(a,b)+yn = 1$, so it is sufficient to substitute a, b by xa, $xb \mod n$. We note that $\omega = e_3$ (respectively e_4, e_6) if $\mathcal{L} = (1,e_3)$ (respectively $(1,e_4)$, $(1,e_6)$)

Because $\sigma\tau\sigma^{-1}$ has order n , $\langle\tau,\sigma\tau\sigma^{-1}\rangle \neq \frac{1}{n}\mathcal{L}$ holds if and only if $\langle\tau\rangle \cap \langle\sigma\tau\sigma^{-1}\rangle \neq 1$ holds. We assume $\frac{1}{n}\mathcal{L}/\langle\tau\rangle \ni \overline{\sigma\tau\sigma^{-1}}$. Let k be the order of this element, we can write $\sigma\tau^k\sigma^{-1} = \tau^l$ and k is a minimal number in these numbers. Moreover $\overline{\sigma\tau\sigma^{-1}}^n = \overline{\sigma\tau^n\sigma^{-1}} = \overline{1}$, we have $k \mid n$.

Here let $l = \alpha k + \beta \, (0 \leqq \beta < k)$. Because of $\{\sigma\tau^k\sigma^{-1}\}^{\frac{n}{k}} = \{\tau^{\alpha k+\beta}\}^{\frac{n}{k}}$, we have $1 = \tau^{\beta\cdot\frac{n}{k}}$, and we have $\beta = 0$.

Thus for τ such as $\langle\tau,\sigma\tau\sigma^{-1}\rangle \neq \frac{1}{n}\mathcal{L}$, there exist minimal k and λ uniquely such as $\sigma\tau^k\sigma^{-1} = \tau^{k\lambda}$.

We put $\mathbb{Z}-$module as follows using minimal k and λ such as $\sigma\tau^k\sigma^{-1} = (\tau^k)^\lambda$ for an element τ of order n.

$$\begin{aligned} L\left(\lambda,\frac{n}{k}\right) &:= \left\{\frac{a+b\omega}{n} \,\middle|\, \lambda a+b \equiv 0 \mod \frac{n}{k}\right\} \\ L_2\left(\lambda,\frac{n}{k}\right) &:= \left\{\frac{a+b\omega}{n} \,\middle|\, \lambda a+a+b \equiv 0 \mod \frac{n}{k}\right\} \\ L_3\left(\lambda,\frac{n}{k}\right) &:= \left\{\frac{a+b\omega}{n} \,\middle|\, \lambda a-a+b \equiv 0 \mod \frac{n}{k}\right\} \end{aligned}$$

σ	ω	kind	condition
e_4	e_4	L	$\lambda^2+1\equiv 0$
e_3	e_3	L	$\lambda^2+\lambda+1\equiv 0$
e_3	e_6	L_2	$\lambda^2+\lambda+1\equiv 0$
e_6	e_3	L_3	$\lambda^2-\lambda+1\equiv 0$
e_6	e_6	L	$\lambda^2-\lambda+1\equiv 0$

We show that these sets include the generator τ and are closed by the action of G_O.

6.1. Case of $\sigma = e_4$.

From $\omega = e_4$ and $\sigma\tau^k\sigma^{-1} = (\tau^k)^\lambda$, we have

$$\frac{kae_4 + kb(e_4)^2}{n} = \frac{k\lambda a + k\lambda b e_4}{n},$$
$$-b \equiv \lambda a \text{ and } a \equiv \lambda b \mod \frac{n}{k}.$$
$$(\lambda^2+1)a \equiv (\lambda^2+1)b \equiv 0 \mod \frac{n}{k}.$$

Because $(a,b)=1$,

$$\lambda^2 + 1 \equiv 0 \mod \frac{n}{k}.$$

Because $-b \equiv \lambda a \mod \frac{n}{k}$, $\tau = \frac{a+be_4}{n} \in L(\lambda, \frac{n}{k})$.
For $\tau' = \frac{a'+b'e_4}{n} \in L(\lambda, \frac{n}{k})$, $\lambda a' + b' \equiv 0 \mod \frac{n}{k}$.

$$\sigma\tau'\sigma^{-1} = \frac{-b' + a'e_4}{n},$$
$$\lambda(-b') + a' \equiv \lambda^2 a' + a' \equiv (\lambda^2+1)a' \equiv 0 \mod \frac{n}{k}.$$

Thus $L(\lambda, \frac{n}{k})$ is closed with action of σ.

6.2. Case of $\sigma = e_3$ and $\omega = e_3$. From $\sigma\tau^k\sigma^{-1} = (\tau^k)^\lambda$, we have

$$\frac{e_3(ka + kbe_3)}{n} = \frac{k\lambda a + k\lambda b e_3}{n},$$
$$\frac{kae_3 + kb(-e_3 - 1)}{n} = \frac{k\lambda a + k\lambda b e_3}{n}.$$
$$-b \equiv \lambda a \text{ and } a - b \equiv \lambda b \mod \frac{n}{k}.$$
$$(\lambda^2+\lambda+1)a \equiv (\lambda^2+\lambda+1)b \equiv 0 \mod \frac{n}{k}.$$

Because $(a,b)=1$,

$$\lambda^2 + \lambda + 1 \equiv 0 \mod \frac{n}{k}.$$

Because $-b \equiv \lambda a \mod \frac{n}{k}$, $\tau = \frac{a+be_3}{n} \in L(\lambda, \frac{n}{k})$.
For $\tau' = \frac{a'+b'e_3}{n} \in L(\lambda, \frac{n}{k})$, $\lambda a' + b' \equiv 0 \mod \frac{n}{k}$.

$$\sigma\tau'\sigma^{-1} = \frac{-b' + (a'-b')e_3}{n},$$
$$\lambda(-b') + (a'-b') \equiv \lambda^2 a' + a' + \lambda a' \equiv (\lambda^2+\lambda+1)a' \equiv 0 \mod \frac{n}{k}.$$

Thus $L(\lambda, \frac{n}{k})$ is closed with action of σ.

6.3. Case of $\sigma = e_3$ and $\omega = e_6$. From $\sigma\tau^k\sigma^{-1} = (\tau^k)^\lambda$, we have

$$
\begin{aligned}
&\frac{(e_6)^2(ka+kbe_6)}{n} = \frac{k\lambda a + k\lambda b e_6}{n},\\
&\frac{ka(e_6-1)-kb}{n} = \frac{k\lambda a + k\lambda b e_6}{n}.\\
&-a-b \equiv \lambda a \text{ and } a \equiv \lambda b \mod \frac{n}{k}.\\
&(\lambda^2+\lambda+1)a \equiv (\lambda^2+\lambda+1)b \equiv 0 \mod \frac{n}{k}.
\end{aligned}
$$

Because $(a,b)=1$,

$$\lambda^2+\lambda+1 \equiv 0 \mod \frac{n}{k}.$$

Because $-a-b \equiv \lambda a \mod \frac{n}{k}$, $\tau = \frac{a+be_6}{n} \in L_2(\lambda, \frac{n}{k})$.
For $\tau' = \frac{a'+b'e_6}{n} \in L_2(\lambda, \frac{n}{k})$, $\lambda a' + a' + b' \equiv 0 \mod \frac{n}{k}$.

$$
\begin{aligned}
\sigma\tau'\sigma^{-1} &= \frac{-a'-b'+a'e_6}{n},\\
\lambda(-a'-b')+(-a'-b')+a' &\equiv -\lambda a' - \lambda b' - b'\\
&\equiv a'+b'-\lambda b' - b'\\
&\equiv a'-\lambda b'\\
&\equiv (-\lambda^2-\lambda)a' - \lambda b'\\
&\equiv (\lambda)(-\lambda a' - a' - b') \equiv 0 \mod \frac{n}{k}.
\end{aligned}
$$

Thus $L_2(\lambda, \frac{n}{k})$ is closed with action of σ.

6.4. Case of $\sigma = e_6$ and $\omega = e_3$. From $\sigma\tau^k\sigma^{-1} = (\tau^k)^\lambda$, we have

$$
\begin{aligned}
&\frac{-(e_3)^2(ka+kbe_3)}{n} = \frac{k\lambda a + k\lambda b e_3}{n},\\
&\frac{ka(e_3+1)-kb}{n} = \frac{k\lambda a + k\lambda b e_3}{n}.\\
&a-b \equiv \lambda a \text{ and } a \equiv \lambda b \mod \frac{n}{k}.\\
&(\lambda^2-\lambda+1)a \equiv (\lambda^2-\lambda+1)b \equiv 0 \mod \frac{n}{k}.
\end{aligned}
$$

Because $(a,b)=1$,

$$\lambda^2-\lambda+1 \equiv 0 \mod \frac{n}{k}.$$

Because $a-b \equiv \lambda a \mod \frac{n}{k}$, $\tau = \frac{a+be_3}{n} \in L_3(\lambda, \frac{n}{k})$.

For $\tau' = \frac{a'+b'e_3}{n} \in L_3(\lambda, \frac{n}{k})$, $\lambda a' - a' + b' \equiv 0 \mod \frac{n}{k}$.

$$\begin{aligned}\sigma\tau'\sigma^{-1} &= \frac{a'e_3 + b'(e_3)^2}{n} \\ &= \frac{a'e_3 + b'(-e_3 - 1)}{n} \\ &= \frac{-b' + (a' - b')e_3}{n}, \\ \lambda(-b') + b' + a' - b' &\equiv -\lambda b' + a' \\ &\equiv \lambda^2 a' - \lambda a' + a' \\ &\equiv (\lambda^2 - \lambda + 1)a' \equiv 0 \mod \frac{n}{k}.\end{aligned}$$

Thus $L_3(\lambda, \frac{n}{k})$ is closed with action of σ.

6.5. Case of $\sigma = e_6$ and $\omega = e_6$. From $\sigma\tau^k\sigma^{-1} = (\tau^k)^\lambda$, we have

$$\begin{aligned}&\frac{e_6(ka + kbe_6)}{n} = \frac{k\lambda a + k\lambda b e_6}{n}, \\ &\frac{kae_6 + kb(e_6 - 1)}{n} = \frac{k\lambda a + k\lambda b e_6}{n}. \\ &-b \equiv \lambda a \text{ and } a + b \equiv \lambda b \mod \frac{n}{k}. \\ &(\lambda^2 - \lambda + 1)a \equiv (\lambda^2 - \lambda + 1)b \equiv 0 \mod \frac{n}{k}.\end{aligned}$$

Because $(a, b) = 1$,

$$\lambda^2 - \lambda + 1 \equiv 0 \mod \frac{n}{k}.$$

Because $-b \equiv \lambda a \mod \frac{n}{k}$, $\tau = \frac{a+be_6}{n} \in L(\lambda, \frac{n}{k})$.
For $\tau' \in L(\lambda, \frac{n}{k})$, $\tau' = \frac{a'+b'e_6}{n}$, $\lambda a' + b' \equiv 0 \mod \frac{n}{k}$.

$$\begin{aligned}\sigma\tau'\sigma^{-1} &= \frac{-b' + (a' + b')e_6}{n}, \\ \lambda(-b') + (a' + b') &\equiv \lambda^2 a' + a' - \lambda a' \\ &\equiv (\lambda^2 - \lambda + 1)a' \equiv 0 \mod \frac{n}{k}.\end{aligned}$$

Thus $L(\lambda, \frac{n}{k})$ is closed with action of σ.

6.6. Number of elements. Let $\rho = \sigma\tau\sigma^{-1}$, $\langle\tau, \rho\rangle$ has elements as $\tau^i\rho^j$ $(i, j = 0, 1, \cdots, n-1)$, where $\rho^k = \tau^{k\lambda}$. Different elements are case of $i = 0, \cdots, n-1$, $j = 0, 1, \cdots, k-1$, so number of elements is nk.
Elements in $L(\lambda, \frac{n}{k})$ is written as $\frac{a+b\omega}{n}$ where $(a, b) = (a, -\lambda a + \frac{n}{k}l)$ so number of elements $^{\#}L(\lambda, \frac{n}{k}) = nk$.
Elements in $L_2(\lambda, \frac{n}{k})$ is written as $\frac{a+b\omega}{n}$ where $(a, b) = (a, -(\lambda+1)a + \frac{n}{k}l)$ so number of elements $^{\#}L_2(\lambda, \frac{n}{k}) = nk$.
Elements in $L_3(\lambda, \frac{n}{k})$ is written as $\frac{a+b\omega}{n}$ where $(a, b) = (a, -(\lambda-1)a + \frac{n}{k}l)$. so number of elements $^{\#}L_3(\lambda, \frac{n}{k}) = nk$.
Number of elements are coincide and then we have $\langle\tau, \sigma\tau\sigma^{-1}\rangle = L(\lambda, \frac{n}{k})$.

6.7. Generators of $L(\lambda, \frac{n}{m})$.

$$L\left(\lambda, \frac{n}{m}\right) = \left\{\frac{a+b\omega}{n} \,\middle|\, \lambda a + b \equiv 0 \mod \frac{n}{m}\right\} \ni \frac{1-\lambda\omega}{n}$$

So we have

$$L\left(\lambda, \frac{n}{m}\right) \ni \frac{\frac{n}{m}\omega}{n} = \frac{\omega}{m}$$

And we have

$$L\left(\lambda, \frac{n}{m}\right) = \left\langle \frac{1-\lambda\omega}{n}, \frac{\omega}{m} \right\rangle$$

Also we have

$$L_2\left(\lambda, \frac{n}{m}\right) = \left\langle \frac{1-(\lambda+1)\omega}{n}, \frac{\omega}{m} \right\rangle$$

$$L_3\left(\lambda, \frac{n}{m}\right) = \left\langle \frac{1-(\lambda-1)\omega}{n}, \frac{\omega}{m} \right\rangle$$

6.8. Subgroup including $L_*(\lambda, \frac{n}{m})$ and Main Theorem.

$$L\left(\lambda, \frac{n}{m}\right) = \left\langle \frac{1-\lambda\omega}{n}, \frac{\omega}{m} \right\rangle$$

$$L_2\left(\lambda, \frac{n}{m}\right) = \left\langle \frac{1-(\lambda+1)\omega}{n}, \frac{\omega}{m} \right\rangle$$

$$L_3\left(\lambda, \frac{n}{m}\right) = \left\langle \frac{1-(\lambda-1)\omega}{n}, \frac{\omega}{m} \right\rangle$$

We have obtained above results not in case that G_T has one generator or $G = \frac{1}{n}\mathcal{L}$. But in case that G_T has one generator , we may think $m = 1$ because $\langle \sigma\tau\sigma^{-1} \rangle = \langle \tau \rangle$. Moreover in case that $G = \frac{1}{n}\mathcal{L}$, we may think $m = n$.
Subgroup of $\frac{1}{n}\mathcal{L}$ including these is obtained as $\langle \frac{1-\lambda\omega}{n}, \frac{\omega}{mk} \rangle$. The order of this subgroup is $n \times mk = \frac{n}{mk}(mk)^2$. where $\frac{n}{mk}$ is a divisor of $\frac{n}{m}$ and $\frac{n}{m}$ is a divisor of n and moreover $\frac{n}{m}$ is a factor of $1 + A^2$ (respectively $1 + A + A^2$) for some rational integer A if $\omega = e_4$ (respectively e_3 or e_6).
Conversely for minimal m such as $\frac{n}{m}|\mu$, there exists τ such that there exists subgroup of $Z_n \oplus Z_m$ including $\langle \tau, \sigma\tau\sigma^{-1} \rangle$.

THEOREM 2. *A finite automorphism group G as a plane elliptic curve is written as $Z_l \ltimes (Z_n \oplus Z_m)$ $(m \mid n)$ where $l = 1, 2, 3, 4, 6$.*
In case of $l = 1$, $G \cong Z_n$ or $G \cong Z_n \oplus Z_m$ (n,m is natural number and $m \mid n$.)
In case of $l = 2$, $G \cong Z_2 \ltimes Z_n \cong D_n$ or $G \cong Z_2 \ltimes (Z_n \oplus Z_m) \cong BD_{nm}$.
In case of $l = 3, 6$, $G \cong Z_l \ltimes (Z_n \oplus Z_m)$ where $\frac{n}{m} = p_0p_1p_2 \cdots p_k$. ($p_0 = 1$ or 3 and $p_i(i > 0)$ is an odd prime number equivalent to 1 modulo 3)
In case of $l = 4$, $G \cong Z_l \ltimes (Z_n \oplus Z_m)$ where $\frac{n}{m} = p_0p_1p_2 \cdots p_k$. ($p_0 = 1$ or 2 and $p_i(i > 0)$ is an odd prime number equivalent to 1 modulo 4)

DEFINITION 2. A finite non-Abelian group in Theorem2 which is neither dihedral nor bidihedral group called exceptional elliptic group. If it has one (resp. two) generators then we denote $E(l, n)$ (resp. $E(l, n, m)$).

CHAPTER 2

Examples

A finite subgroup G of an automorphism group $A(E)$ of an elliptic curve E as varieties can be a Galois group at a Galois point for a genus-one curve C if and only if $|G| \geqq 3$ and G has an element σ which is not translation. Thus the main theorem is stated as follows :

THEOREM 3. *A finite group G can be the Galois group at a Galois point for a subgroup of $A(E)$ for some elliptic curve E if and only if G is isomorphic to one of the following :*

(i) *abelian case :*
$Z_2{}^{\oplus 2},\ Z_2{}^{\oplus 3},\ Z_3,\ Z_3{}^{\oplus 2},\ Z_4,\ Z_2 \oplus Z_4,\ Z_6.$

(ii) *non-abelian case :*
  (a) D_n *or* BD_{mn}.
  (b) $E(l,n)$, $E(l,n,m)$.

In this chapter, we give examples of defining equations and actions for all abelian cases and for some non-abelian cases.
The following Remark is useful to find the examples.

REMARK 11. Let G be the group in Theorem3 and suppose the invariant subfield $\mathbb{C}(x,y)^G = \mathbb{C}(t)$. Then taking an affine coordinate t, we have a morphism $p : E \longrightarrow E/G \cong \mathbb{P}^1$. Let D be the polar divisor of t on E. Next, find an element $s \in \mathbb{C}(x,y)$ satisfying that $div(s) + D \geq 0$ and $\mathbb{C}(x,y) = \mathbb{C}(s,t)$. Then, the curve C defined by s and t has the Galois point at ∞ with the Galois group G.

The proof of this remark is follows :
Let $\mathcal{L}(D) = \{\ \varphi \in \mathbb{C}(x,y) \mid div(\varphi) + D \geqq 0\ \}$. Then the elements of $\mathcal{L}(D)$ defines the embedding of E into $\mathbb{P}^n$, where $n+1 = \dim \mathcal{L}(D)$ if $\deg D \geqq 3$. (Indeed, by Riemann-Roch theorem we have $\dim \mathcal{L}(D) = \deg D$.) By definition $t,\ s,\ 1$ belong to $\mathcal{L}(D)$ and $\langle t, s, 1\rangle$ generates a sublinear system of $\mathcal{L}(D)$. Furthermore, the morphism $f : E \longrightarrow P^2$ defined by $f(x) = (t(x) : s(x) : 1),\ x \in E$ is a birational morphism and the image coincides with the curve C defined by the relation of $t,\ s$. Therefore C has a Galois point at $(0:1:0)$, where $(T : S : U)$ are homogeneous coordinates on $\mathbb{P}^2$ and $t = T/U,\ s = S/U$.

1. Procedure to make defining equation

We make defining equations and actions as follows :
For given group G ,

(i) Take a suitable elliptic curve E and automorphism on group E.
(ii) Take a suitable translations on E.
(iii) Find an invariant t by G in $\mathbb{C}(E) = \mathbb{C}(x,y)$.
(iv) Find $s \in \mathbb{C}(E)$ such that $(s) + (t)_\infty \geq 0$.
(v) Check $\mathbb{C}(s,t) = \mathbb{C}(x,y)$.
(vi) Find the irreducible equation of s and t.
(vii) Check that above equation is monic polynomial of s and has degree $|G|$ which is order of G.

2. rotation

In this chapter, we use i (resp. ω) instead of e_4 (resp. e_3).
Generally , for any lattice $\mathcal{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, we have Weierstrass $\wp$-function

$$\wp(z) = \frac{1}{z^2} + \sum_{\zeta \in \mathcal{L}\setminus\{0\}} \left\{ \frac{1}{(z-\zeta)^2} - \frac{1}{\zeta^2} \right\},$$
$$\wp'(z) = -2 \sum_{\zeta \in \mathcal{L}} \frac{1}{(z-\zeta)^3}.$$

we put

$$u_1 = \wp\left(\frac{\omega_1}{2}\right),$$
$$u_2 = \wp\left(\frac{\omega_2}{2}\right),$$
$$u_3 = \wp\left(\frac{\omega_1}{2} + \frac{\omega_2}{2}\right).$$

We have analytic isomorphism Φ as follows :

$$\Phi \ : \ \mathbb{C}/\mathcal{L} \longrightarrow \Phi(\mathbb{C}/\mathcal{L}) \subset \mathbb{P}^2(\mathbb{C})$$
$$\Phi(z) = \begin{cases} (\wp(z) : \wp'(z) : 1) \ (\text{if } z \neq 0) \\ (0 : 1 : 0) \ (\text{if } z = 0) \end{cases}$$

image(Φ) is defined by $y^2 = 4(x-u_1)(x-u_2)(x-u_3)$

Z_2 acts any plane elliptic curve, but Z_3, Z_4, Z_6 acts special ones below.
We will use the Weierstrass's canonical form

$$\mathbb{C}/(1,\omega) : y^2 = x^3 + 1$$

and

$$\mathbb{C}/(1,i) : y^2 = x^3 + x.$$

As a relation between coordinate x, y and z, we have $x = \wp(z)$, $y = \wp'(z)$.

2.1. action of order 2. Action of Z_2 is $\sigma(z) = -z$, we have $\sigma(x) = \wp(-z) = x$, $\sigma(y) = \wp(-z) = -y$.

2.2. action on $y^2 = x^3 + x$ of order 4. Action of Z_4 is $\sigma(z) = iz$, we have $\sigma(x) = \wp(iz) = -x$, $\sigma(y) = \wp(iz) = iy$.

2.3. action on $y^2 = x^3 + 1$ of order 3. Action of Z_3 is $\sigma(z) = \omega z$, we have $\sigma(x) = \wp(\omega z) = \omega x$, $\sigma(y) = \wp(\omega z) = y$.

2.4. action on $y^2 = x^3 + 1$ of order 6. Action of Z_2 is $\sigma(z) = -\omega z$, we have $\sigma(x) = \wp(-z) = \omega x$, $\sigma(y) = \wp(-\omega z) = -y$.

3. Translations

It is too difficult to examine translations using Weierstrass $\wp$ function.
The elliptic curve E which is defined by $y^2 = x^3 + x$ or $y^2 = x^3 + 1$ have a group structure.
We can use this arithmetic to examine translations.
In a geometric point of view, for two points $\mathrm{P}(a, b)$ and $\mathrm{Q}(c, d)$ on a elliptic curve E, the line l through points P and Q intersects E with a point $\mathrm{R}(e, -f)$, and then we have addition of points on E as

$$(a, b) + (c, d) = (e, f).$$

Calculating this addition by formula manipulation software MAXIMA.
In case of $y^2 = x^3 + x$, we have

$$e = \frac{(a+c)(ac+1) - 2bd}{(a-c)^2},$$
$$f = \frac{(3a^2c + c + a^3 + 3a)d - (c^3 + 3ac^2 + 3c + a)b}{(a-c)^3}.$$

In case of $y^2 = x^3 + 1$, we have

$$e = \frac{-2bd + ac^2 + a^2c + 2}{(a-c)^2},$$
$$f = \frac{(3a^2c + a^3 + 4)d - bc^3 - 3abc^2 - 4b}{(a-c)^3}.$$

In a geometric point of view, the tangent line at $\mathrm{P}(a, b)$ on a elliptic curve E intersects a point $\mathrm{Q}(e, -f)$ with E, then we have

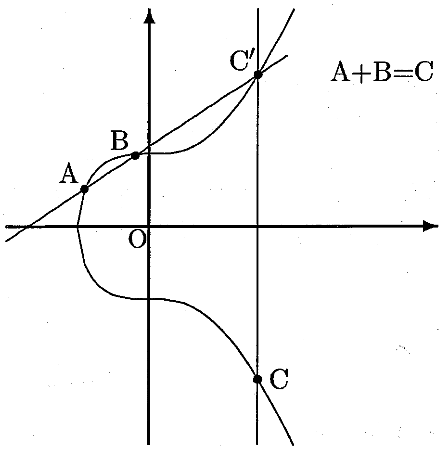
$$2(a, b) = (e, f).$$

In case of $y^2 = x^3 + x$, we have

$$2(a, b) = \left(\frac{(a^2-1)^2}{4b^2}, \frac{a^6 + 5a^4 - 5a^2 - 1}{8b^3} \right)$$

In case of $y^2 = x^3 + 1$, we have

$$2(a, b) = \left(\frac{a(b^2-9)^2}{4b^2}, \frac{b^4 + 18b^2 - 27}{8b^3} \right)$$



3.1. Case of order 2 on $y^2 = x^3 + x$. There is a well known fact that the point of order 2 is obtained by $y = 0$. We have

$$(0,0), \quad (i,0), \quad (-i,0).$$

So we have three translations as follows.

$$\begin{aligned}
(x,y) + (0,0) &= \left(\frac{1}{x}, -\frac{y}{x^2}\right) = (\tau_1(x), \tau_1(y)),\\
(x,y) + (i,0) &= \left(\frac{i(x+i)}{x-i}, \frac{2y}{(x-i)^2}\right) = (\tau_2(x), \tau_2(y)),\\
(x,y) + (-i,0) &= \left(-\frac{i(x-i)}{x+i}, \frac{2y}{(x+i)^2}\right) = (\tau_3(x), \tau_3(y)).\\
x + \tau_2(x) &= \frac{x^2-1}{x-i} \in \mathbb{C}(x,y)^{\langle\tau_2\rangle},\\
x + \tau_3(x) &= \frac{x^2-1}{x+i} \in \mathbb{C}(x,y)^{\langle\tau_3\rangle}.
\end{aligned}$$

3.2. Case of order 2 on $y^2 = x^3 + 1$. The point of order 2 is obtained by $y = 0$. We have

$$(-1,0), \quad (-\omega,0), \quad (-\omega^2,0),$$

and three translations as follows.

$$\begin{aligned}
(x,y) + (-1,0) &= \left(-\frac{x-2}{x+1}, \frac{3y}{(x+1)^2}\right) = (\tau_1(x), \tau_1(y)),\\
(x,y) + (-\omega,0) &= \left(\frac{\omega(x^2-\omega x-2\omega^2)}{(x+\omega)^2}, \frac{(\omega-2)(3x-\omega)y}{(x+\omega)^3}\right) = (\tau_2(x), \tau_2(y)),\\
(x,y) + (-\omega^2,0) &= \left(\frac{-\omega^2(x^2-\omega^2 x-2\omega)}{(x+\omega^2)^2}, -\frac{\omega(3x-\omega^2)y}{(x+\omega^2)^3}\right) = (\tau_3(x), \tau_3(y)).
\end{aligned}$$

3.3. Case of order 3. On $y^2 = x^3 + 1$,

$$4(0,1) = 2(0,1) + 2(0,1) = 2(0,-1) = (0,1).$$

So we have $3(0,1) = O$ and the order of a point (0,1) is 3.
We have a translation τ of order 3,

$$\begin{aligned}(x,y) + (0,1) &= \left(\frac{2-2y}{x^2}, \frac{x^3+4-4y}{x^3}\right)\\ &= \left(\frac{2-2y}{x^2}, \frac{y-3}{y+1}\right)\\ &= (\tau(x), \tau(y))\end{aligned}$$

$$x + \tau(x) + \tau^2(x) = \frac{y+3}{x^2}$$

And we have

$$\tau^2(x) = \frac{2x}{y-1}, \quad \tau^3(x) = x, \quad \tau^2(y) = \frac{-y-3}{y-1}, \quad \tau^3(y) = y.$$

3.4. Case of order 4. On $y^2 = x^3 + x$, $2(\pm 1, \pm\sqrt{2}) = (0,0)$. Because (0,0) is a point of order 2, $(\pm 1, \pm\sqrt{2})$ are points of order 4.
We have a translation of order 4,

$$(x,y) + (1,\sqrt{2}) = \left(\frac{(x+1)^2 - 2\sqrt{2}y}{(x-1)^2}, \frac{\sqrt{2}(x+1)\tau(x)}{x-1}\right) = (\tau(x), \tau(y)).$$

$$\begin{aligned}\tau^2(x) &= \frac{1}{x}, \quad \tau^3(x) = \frac{1}{\tau(x)}, \quad \tau^4(x) = x.\\ \tau^2(y) &= -\frac{y}{x^2}, \quad \tau^3(y) = -\frac{\sqrt{2}(x+1)}{(x-1)\tau(x)}, \quad \tau^4(y) = y.\end{aligned}$$

Moreover it is useful to note below.

$$\begin{aligned}x + \tau(x) + \tau^2(x) + \tau^3(x) &= \frac{x^4 + 6x^2 + 1}{x(x-1)^2} \in \mathbb{C}(x,y)^{\langle\tau\rangle}\\ \tau\left(\frac{y}{x}\right) &= \frac{\sqrt{2}(x+1)}{x-1} \cdot \frac{\tau(x)}{\tau(x)} = \frac{\sqrt{2}(x+1)}{x-1}.\\ -\frac{y}{x} = \tau^2\left(\frac{y}{x}\right) &= \tau\left(\frac{\sqrt{2}(x+1)}{x-1}\right).\end{aligned}$$

So we have a following.

$$\tau\left(\frac{\sqrt{2}(x+1)}{x-1}\right) = -\frac{y}{x}.$$

3.5. Rational point of finite order. For non singular cubic

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c,$$

we put

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Then we have the following generally :
If P=(x, y) is a rational point of finite order then x and y are both integers , moreover $y = 0$ (i.e. P has order two.) or $y \mid D$.
We say in our case :
If E is $y^2 = x^3 + x$ then (0,0) is a point of order two.
If E is $y^2 = x^3 + 1$ then $(-1, 0)$ is a point of order two, (0,1) and (2,3) of order three , (2,3) of order six.

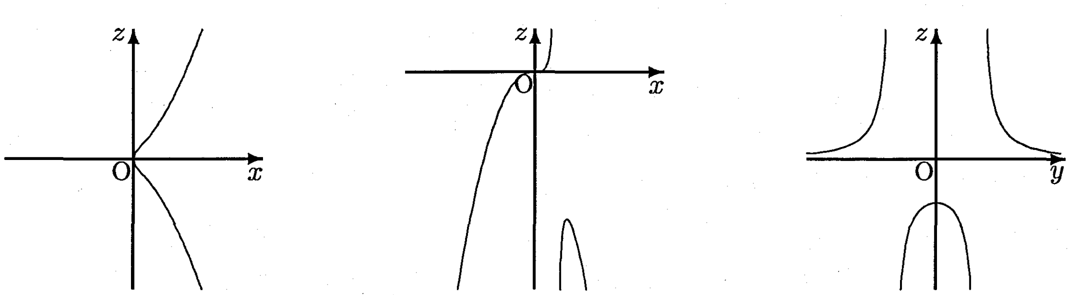
4. Divisors

In case $y^2 = x^3 + x$, we have

$$(x - \lambda) = -2(0:1:0) + (\lambda : \sqrt{\lambda^3 + \lambda} : 1) + (\lambda : -\sqrt{\lambda^3 + \lambda} : 1)$$
$$(y - \lambda) = -3(0:1:0) + (\zeta_1 : \lambda : 1) + (\zeta_2 : \lambda : 1) + (\zeta_3 : \lambda : 1)$$
$$\text{where } \zeta_1, \zeta_2, \zeta_3 \text{ are the roots of } x^3 + x = \lambda^2.$$

In case $y^2 = x^3 + 1$, we have

$$(x - \lambda) = -2(0:1:0) + (\lambda : \sqrt{\lambda^3 + 1} : 1) + (\lambda : -\sqrt{\lambda^3 + 1} : 1)$$
$$(y - \lambda) = -3(0:1:0) + (\zeta_1 : \lambda : 1) + (\zeta_2 : \lambda : 1) + (\zeta_3 : \lambda : 1)$$
$$\text{where } \zeta_1, \zeta_2, \zeta_3 \text{ are the roots of } x^3 = \lambda^2 - 1.$$



5. Abelian Case

5.1. Case of Z_3. Take an elliptic curve and action on it :

$$E : y^2 = x^3 + 1.$$
$$\sigma(x) = \omega x, \ \sigma(y) = y.$$

Let

$$t = y \in \mathbb{C}(x, y)^G.$$

We have

$$(t)_\infty = 3(0:1:0),$$

so we have

$$(x) + (t)_\infty = (0:1:0) + (0:1:1) + (0:-1:1) \geq 0.$$

Moreover , clearly

$$\mathbb{C}(x,t) = \mathbb{C}(y,x)$$
$$x^3 = t^2 + 1.$$

Finally $x^3 = t^2 + 1$ is a monic irreducible polynomial of x of degree 3.

5.2. Case of Z_4. Take an elliptic curve and action on it :

(3)
$$E : y^2 = x^3 + x$$
$$\sigma(x) = -x, \quad \sigma(y) = iy.$$

Let

(4)
$$t = x^2 \in \mathbb{C}(x,y)^G.$$

We have

$$(t)_\infty = 4(0:1:0),$$

so we have

$$(y) + (t)_\infty = (0:1:0) + (0:0:1) + (i:0:1) + (-i:0:1) \geq 0.$$

Moreover for (3) and (4) , we have

$$x = \frac{y^2}{t+1} \in \mathbb{C}(y,t)$$

so we have

$$\mathbb{C}(y,t) = \mathbb{C}(y,x).$$

To eliminate x from (3) and (4), we have

$$y^4 = t(t+1)^2.$$

This is a monic irreducible polynomial of y of degree 4.

5.3. Case of Z_6. Take an elliptic curve and action on it :

(5)
$$E : y^2 = x^3 + 1.$$
$$\sigma(x) = \omega x, \quad \sigma(y) = -y.$$

Let

(6)
$$t = x^3 \in \mathbb{C}(x,y)^G$$

and

(7)
$$s = xy.$$

Note that

$$\forall i \in \{1, \cdots, 5\} \ : \ \sigma^i(s) \neq s.$$

We have

$$(t)_\infty = 6(0:1:0),$$

so

$$(s) + (t)_\infty = (0:1:0) + (0:1:1) + (0:-1:1)$$
$$+ (-1:0:1) + (-\omega:0:1) + (-\omega^2:0:1) \geq 0.$$

$$\frac{s^2 x}{t} = \frac{s^2}{x^2} = y^2 = t + 1 \in \mathbb{C}(s,t).$$

So we have

$$x \in \mathbb{C}(s,t), \quad y = \frac{s}{x} \in \mathbb{C}(s,t).$$

Thus we have

$$\mathbb{C}(s,t) = \mathbb{C}(x,y).$$

To eliminate x, y from (5) , (6) and (7) , we have

$$s^6 = x^6y^6 = t^2(t+1)^3.$$

This is a monic irreducible polynomial of s of degree 6.

5.4. Case of $Z_2{}^{\oplus 2}$. Take an elliptic curve and actions on it :

$$E : y^2 = x^3 + x \tag{8}$$

$$\sigma(x) = x,\ \sigma(y) = -y,\ \tau(x) = \frac{i(x+i)}{x-i},\ \tau(y) = \frac{2y}{(x-i)^2}.$$

$$x + \tau(x) = \frac{x^2-1}{x-i}.$$

Take an invariant and a generator :

$$t = \frac{x^2-1}{x-i} \in \mathbb{C}(x,y)^G \tag{9}$$

$$s = \frac{y-i}{x-i}. \tag{10}$$

We have

$$(t)_\infty = 2(0:1:0) + 2(i:0:1),$$
$$(s) = -(0:1:0) - 2(i:0:1) + (\zeta_1 : i : 1) + (\zeta_2 : i : 1) + (\zeta_3 : i : 1),$$
where $\zeta_1, \zeta_2, \zeta_3$ are the roots of $x^3 + x + 1 = 0$.

So

$$(s) + (t)_\infty \geq (0:1:0) \geq 0.$$

Next , we check generators. From (9) we have

$$x^2 = tx - it + 1. \tag{11}$$

Using (8),(10),(11), we have

$$\begin{aligned}
y^2 &= x^3 + x \\
&= (x^2)x + x \\
&= (tx - it + 1)x + x \\
&= tx^2 - itx + 2x \\
&= t(tx - it + 1) - itx + 2x \\
&= (t^2 - it + 2)x - it^2 + t, \\
y^2 &= (s(x-i) + i)^2 \\
&= s^2(x^2 - 2ix - 1) + 2is(x-i) - 1 \\
&= s^2(tx - it + 1) - s^2(2ix + 1) + 2is(x-i) - 1 \\
&= (s^2t - 2is^2 + 2is)x - is^2t + 2s - 1.
\end{aligned}$$

Combine these equation, we have

$$(t^2 - it + 2 - s^2t + 2is^2 - 2is)x = it^2 - t - is^2t + 2s - 1.$$

Thus $x \in \mathbb{C}(s,t)$ and $y \in \mathbb{C}(s,t)$.
Calculating resultant of (8), (9) and (10), we can eliminate x and y , we have

$$\begin{aligned}(12)\quad 4s^4 - 4(it+2)s^3 - (t^2 + 4(2+i)t - 8(1-i))s^2 \\ + 2(2it^2 + (2-i)t - 2(1-2i))s \\ + (t^3 + 4t^2 - 3it^2 + 4t + 8it - 3) = 0.\end{aligned}$$

This is a monic irreducible polynomial of s of degree 4.

The equation (12) seems too difficult rather than other equations. If we use actions

$$\sigma(x) = x, \quad \sigma(y) = -y, \quad \tau(x) = \frac{1}{x}, \quad \tau(y) = -\frac{y}{x^2}$$

and an invariant

$$t = x + \frac{1}{x} = \frac{x^2+1}{x} = \frac{y^2}{x^2}, \tag{13}$$

we have

$$(y) + (t)_\infty \not\geq 0.$$

But we have

$$\begin{aligned} y^2 &= x \cdot \frac{y^2}{t} + x = x\left(\frac{y^2}{t} + 1\right). \\ x &= \frac{ty^2}{y^2+t} \in \mathbb{C}(y,t). \\ \tau(y) &= -\frac{t}{y}, \end{aligned}$$

Calculating resultant of (8) and (13), we can eliminate x , we have

$$y^4 + (2t - t^3)y^2 + t^2 = 0.$$

5.5. Case of $Z_4 \oplus Z_2$. Take an elliptic curve and actions on it :

$$E : y^2 = x^3 + x \tag{14}$$

$$\sigma(x) = -x, \ \sigma(y) = iy, \ \tau(x) = \frac{1}{x}, \ \tau(y) = -\frac{y}{x^2}.$$

Moreover we take an invariant

$$t = \frac{y^4}{x^4} \in \mathbb{C}(x,y)^{\langle \sigma, \tau \rangle}. \tag{15}$$

We have

$$\begin{aligned} (t)_\infty &= 4(0:1:0) + 4(0:0:1), \\ (y) &= -3(0:1:0) + (0:0:1) + (i:0:1) + (-1:0:1). \end{aligned}$$

So we have

$$(y) + (t)_\infty \geq 0.$$

Secondly from (14) and (15) we have

$$x^3 = y^2 - x, \tag{16}$$

$$tx^4 = y^4. \tag{17}$$

Using (17) and (16) we have

$$tx(y^2 - x) = y^4$$

so

$$tx^2 = ty^2x - y^4. \tag{18}$$

Using (16) and (18), we have

$$t(y^2 - x) = x(ty^2x - y^4).$$

To repeat this way, we have finally

$$(ty^4 - y^4 + t)x = ty^2 + y^6$$

so we have

$$\mathbb{C}(y, t) = \mathbb{C}(y, x).$$

Finally we eliminate x from (14), (17) by calculating resultant, we have

$$y^8 - (t^3 - 4t^2 + 2t)y^4 + t^2 = 0.$$

This is a monic irreducible polynomial of y of degree 8.
Actions on t and y is as follows.

$$\sigma(t) = t, \tau(t) = t,$$
$$\sigma(y) = iy, \tau(y) = \frac{t^2 - (t^3 - 4t^2 + 3t)y^4}{(t-2)y^7}, \tau^2(y) = y$$

5.6. Case of $Z_2{}^{\oplus 3}$. Take an elliptic curve and actions on it :

$$E : y^2 = x^3 + x \tag{19}$$

$$\sigma(x) = x, \sigma(y) = -y,$$
$$\tau(x) = \frac{1}{x}, \tau(y) = -\frac{y}{x^2},$$
$$\rho(x) = \frac{i(x+i)}{x-i}, \rho(y) = \frac{2y}{(x-i)^2}.$$

$$\begin{aligned} x + \tau(x) + \rho(x) + \tau\rho(x) &= x + \frac{1}{x} + \frac{i(x+i)}{x-i} + \frac{i(1/x+i)}{(1/x-i)} \\ &= \frac{(x^2-1)^2}{y^2}. \end{aligned}$$

We take an invariant

$$t = \frac{(x^2-1)^2}{y^2} \in \mathbb{C}(x, y)^{\langle \sigma, \tau, \rho \rangle}. \tag{20}$$

We have

$$(t)_\infty = 2(0:1:0) + 2(0:0:1) + 2(i:0:1) + 2(-i:0:1)$$

and

$$(y) = -3(0:1:0) + (0:0:1) + (i:0:1) + (-i:0:1),$$

so we have

$$(1/y) + (t)_\infty = 5(0:1:0) + (0:0:1) + (i:0:1) + (-i:0:1) \geq 0.$$

Put

$$s = \frac{1}{y}. \tag{21}$$

Secondly using

$$s^2(x^3 + x) = 1$$

and

$$s^2(x^2 - 1)^2 = t,$$

we have

$$s^2x^3 + s^2x = 1$$

and

$$s^2x^4 - 2s^2x^2 + s^2 = t.$$

Using these pair of equations we can descend degree of x by substituting each other as follows.

$$\left(x^4 = \frac{2s^2x^2 - s^2 + t}{s^2}, x^3 = \frac{-s^2x + 1}{s^2}\right)$$
$$\left(x^3 = \frac{-s^2x + 1}{s^2}, x^2 = \frac{x + s^2 - t}{3s^2}\right)$$
$$\left(x^2 = \frac{x + s^2 - t}{3s^2}, x^2 = (t - 4s^2)x + 3\right)$$

At last we have

$$(3s^2(t - 4s^2) - 1)x = -8s^2 - t.$$

So $x \in \mathbb{C}(s,t)$ and then $\mathbb{C}(x,y) = \mathbb{C}(s,t)$.
Finally we eliminates x, y from (19), (20), (21) by calculating resultant, we have

$$16s^8 - 24ts^6 + (-8 + 9t^2)s^4 - (t^3 + 10t)s^2 + 1 = 0.$$

This is a monic polynomial of s of degree 8.

5.7. Case of ${Z_3}^{\oplus 2}$. Take an elliptic curve and actions on it :

$$E : y^2 = x^3 + 1 \tag{22}$$

$$\sigma(x) = \omega x, \quad \sigma(y) = y,$$
$$\tau(x) = \frac{2 - 2y}{x^2}, \quad \tau(y) = \frac{y - 3}{y + 1}.$$

$$y + \tau(y) + \tau^2(y) = y + \frac{y - 3}{y + 1} + \frac{\frac{y-3}{y+1} - 3}{\frac{y-3}{y+1} + 1}$$
$$= \frac{y(y^2 - 9)}{y^2 - 1}.$$

And take an invariant

$$t = \frac{y(y^2 - 9)}{y^2 - 1} \in \mathbb{C}(x,y)^{\langle \sigma, \tau \rangle} \tag{23}$$

We have

$$(t)_\infty = 3(0:1:0) + 3(0:1:1) + 3(0:-1:1),$$
$$(x) = -2(0:1:0) + (0:1:1) + (0:-1:1).$$

So

$$(s) + (t)_\infty \geq 0.$$

From (23) we have

$$y^3 = ty^2 + 9y - t.$$

Using (22) , we have

$$\begin{aligned} y \cdot y^2 &= t(y^2) + 9y - t \\ (x^3+1)y &= t(x^3+1) + 9y - t \\ (x^3-8)y &= tx^3 \end{aligned}$$

Thus

$$y \in \mathbb{C}(x,t).$$

In fact it is easy to see

$$y = \frac{t(y^2-1)}{y^2-9} = \frac{tx^3}{x^3-8} \in \mathbb{C}(x,t)$$

Finally calculating resultant of (22) and (23), we can eliminate y and have

$$x^9 - t^2x^6 - 15x^6 + 48x^3 + 64 = 0.$$

This equation is also obtained by

$$(x^3+1) = y^2 = \left(\frac{tx^3}{x^3-8}\right)^2.$$

This equation is a monic irreducible polynomial of x of degree 9.

6. Non Abelian Case

6.1. Case of D_3. We choose an elliptic curve and action on it

$$E : y^2 = x^3 + 1 \tag{24}$$

$$\sigma(x) = x, \sigma(y) = -y.$$

Moreover, we have a translation of order three as follows.

$$\tau(x) = \frac{2-2y}{x^2}, \tau(y) = \frac{y-3}{y+1}, \tau^2(x) = \frac{2x}{y-1}, \tau^3(x) = x.$$

$$x + \tau(x) + \tau^2(x) = x + \frac{2-2y}{x^2} + \frac{2x}{y-1} = \frac{y^2+3}{x^2}$$

Taking an invariant

$$t = \frac{y^2+3}{x^2} \in \mathbb{C}(x,y)^{\langle\sigma,\tau\rangle}. \tag{25}$$

Secondly we calculate divisors.

$$(t)_\infty = 2(0:1:0) + 2(0:1:1) + 2(0:-1:1),$$
$$(x) = -2(0:1:0) + (0:1:1) + (0:-1:1),$$
$$(y) = -3(0:1:0) + (-1:0:1) + (-\omega:0:1) + (-\omega^2:0:1).$$

So we have

$$\left(\frac{y}{x}\right) + (t)_\infty > 0.$$

Putting

$$s = \frac{y}{x}. \tag{26}$$

Eliminate y from (24), (25) and (26), we have

$$s^2x^2 = x^3 + 1 \tag{27}$$

$$tx^2 = s^2x^2 + 3. \tag{28}$$

Using

$$x^2 = \frac{3}{t - s^2},$$

we have

$$x = \frac{4s^2 - t}{3} \in \mathbb{C}(s,t), \quad y = sx \in \mathbb{C}(s,t).$$

Finally , by calculating resultant of (27) and (28), we have

$$16s^6 - 24s^4t + 9s^2t^2 - t^3 + 27 = 0.$$

By dividing 16, this equation will be a monic irreducible polynomial of x of degree 6.

Using

$$s = y$$

instead of (26),

$$(y) + (t)_\infty \ngeq 0.$$

Action on y is the following.

$$\sigma(y) = -y,$$
$$\tau(y) = \frac{y-3}{y+1}, \ \tau^2(y) = \frac{-y-3}{y-1}, \ \tau^3(y) = y.$$

From

$$x^3 = y^2 - 1$$

and

$$x^3 = tx^2 - 4,$$

we have the relation

$$x = \frac{t(y^2-1)}{y^2+3} \in \mathbb{C}(y,t).$$

We can eliminates x from (24) and (25), we have an equation

$$y^6 + (9 - t^3)y^4 + (2t^3 + 27)y^2 - t^3 + 27 = 0,$$

and its degree of y is $6 = |D_3|$.

6.2. Case of D_4. We choose an elliptic curve and action on it :

$$E : y^2 = x^3 + x \tag{29}$$

$$\sigma(x) = x, \sigma(y) = -y.$$

Moreover we choose a translation τ of order 4 by a point $(1,\sqrt{2})$ of order 4.

$$\tau(x) = \frac{(x+1)^2 - 2\sqrt{2}y}{(x-1)^2}, \tau(y) = \frac{\sqrt{2}(x+1)^3 - 4(x+1)y}{(x-1)^3}$$

$$\begin{aligned} x + \tau(x) + \tau^2(x) + \tau^3(x) &= x + \frac{(x+1)^2 - 2\sqrt{2}y}{(x-1)^2} + \frac{1}{x} + \frac{(x-1)^2}{(x+1)^2 - 2\sqrt{2}y} \\ &= \frac{x^4 + 6x^2 + 1}{x(x-1)^2} \end{aligned}$$

Taking an invariant

$$t = \frac{x^4 + 6x^2 + 1}{x(x-1)^2} \in \mathbb{C}(x, y)^{\langle \sigma, \tau \rangle}. \tag{30}$$

Which is invariant for τ because of the way to make , and invariant for σ too. Secondly we calculate divisors.

$$\begin{aligned} (t)_\infty &= 2(0:1:0) + 2(0:0:1) + 2(1:\sqrt{2}:1) + 2(1:-\sqrt{2}:1), \\ (x-1) &= -2(0:1:0) + (1:\sqrt{2}:1) + (1:-\sqrt{2}:1), \\ (y-1) &= -3(0:1:0) + (\zeta_1:1:1) + (\zeta_2:1:1) + (\zeta_3:1:1), \end{aligned}$$

where $\zeta_1, \zeta_2, \zeta_3$ are the roots of $x^3 + x = 1$.

We put

$$s = \frac{y-1}{x-1}, \tag{31}$$

then

$$(s) \geq -(0:1:0) - (1:\sqrt{2}:1) - (1:-\sqrt{2}:1)$$

and we have

$$(s) + (t)_\infty \geq 0.$$

Finally, we eliminate x and y from (29), (30), (31)

$$\begin{aligned} s^2t^3 - 2st^3 + t^3 - 49s^4t^2 + 210s^3t^2 - 329s^2t^2 + 222st^2 - 55t^2 \\ + 112s^6t - 464s^5t + 648s^4t - 64s^3t - 730s^2t + 674st - 186t \\ - 64s^8 + 256s^7 - 320s^6 - 192s^5 + 800s^4 - 512s^3 - 344s^2 + 504s - 153 = 0 \end{aligned}$$

If we use

$$s = \frac{y}{x} \tag{32}$$

instead of (31)

$$(s) + (t)_\infty \geq 0$$

holds but we don't get correct result.
From (32) and (29) we have

$$s^2x^2 = x^3 + x$$

and then

$$x^2 = s^2x - 1.$$

Applying this equation to

$$t = \frac{(x^2+1)^2 + 4x^2}{x(x^2-2x+1)}$$

then we have

$$\begin{aligned} t &= \frac{x^3+6x^2+1}{x^3-2x^2+x} \\ &= \frac{s^2x^3 - x^2 + 6x^2 + 1}{x^2(s^2-2)} \\ &= \frac{s^2(s^2x^2 - x) + 5x^2 + 1}{(s^2-2)x^2} \\ &= \frac{(s^4+5)(s^2x-1) - (s^2x-1)}{s^2(s^2-2)x - s^2 + 2} \\ &= \frac{(s^4+5-1)(s^2x-1)}{(s^2x-1)(s^2-2)} \\ &= \frac{s^4+5-1}{s^2-2} \end{aligned}$$

Degree of

$$s^2t - 2t - s^4 = 4$$

is four then s and t doesn't generate x or y.
On actions , we have

$$\begin{aligned} \tau(y) &= \frac{\sqrt{2}(x+1)\tau(x)}{x-1}, \\ \tau^2\left(\frac{y}{x}\right) &= -\frac{y}{x}, \\ \sigma\left(\frac{y}{x}\right) &= -\frac{y}{x} \end{aligned}$$

So σ and τ are not separated , and we can't use (32).
Moreover eliminating x form

$$tx^2 - s^2x^2 - 3 = 0, \quad s^2x^2 - x^3 - 1 = 0,$$

we have

$$t^3 - 9s^2t^2 + 24s^4t - 16s^6 - 27 = 0.$$

Degree 6 of this equation on s does not coincide with $8 = |G|$, and this show that (32) doesn't succeed.

6.3. Case of $BD_{2\times4}$. We choose an elliptic curve and action on it :

$$E : y^2 = x^3 + x \tag{33}$$

$$\sigma(x) = x, \sigma(y) = -y.$$

We choose a translation τ of order 2 by a point $(i,0)$ and ρ of order 4 by a point $(1,\sqrt{2})$.

$$\tau(x) = \frac{i(x+i)}{x-i}, \tau(y) = \frac{2y}{(x-i)^2},$$

$$\rho(x) = \frac{(x+1)^2 - 2\sqrt{2}y}{(x-1)^2}, \rho(y) = \frac{\sqrt{2}(x+1)}{x-1} \cdot \rho(x)$$

$$\begin{aligned}
&x + \rho(x) + \rho^2(x) + \rho^3(x) + \tau(x) + \tau\rho(x) + \tau\rho^2(x) + \tau\rho^3(x) \\
&= \frac{x^4+6x^2+1}{x(x-1)^2} + \tau\left(\frac{x^4+6x^2+1}{x(x-1)^2}\right) \\
&= \frac{(x^4+6x^2+1)^2}{x(x-1)^2(x+1)^2(x^2+1)}.
\end{aligned}$$

Taking an invariant

$$t = \frac{(x^4+6x^2+1)^2}{x(x-1)^2(x+1)^2(x^2+1)} \in \mathbb{C}(x,y)^{\langle\sigma,\tau\rangle}. \tag{34}$$

Secondly we calculate divisors.

$$\begin{aligned}
(t)_\infty &= 2(0:0:1) + 2(1:\sqrt{2}:1) + 2(1:-\sqrt{2}:1) \\
&\quad + 2(-1:\sqrt{-2}:1) + 2(-1:-\sqrt{-2}:1) + 2(i:0:1) + 2(-i:0:1), \\
(x) &= -2(0:1:0) + 2(0:0:1), \\
(y) &= -3(0:1:0) + (0:0:1) + (i:0:1) + (-i:0:1), \\
(x-1) &= -2(0:1:0) + (1:\sqrt{2}:1) + (1:-\sqrt{2}:1), \\
(y-1) &= -3(0:1:0) + (\zeta_1:1:1) + (\zeta_2:1:1) + (\zeta_3:1:1), \\
(x+1) &= -2(0:1:0) + (-1:\sqrt{-2}:1) + (1:-\sqrt{-2}:1), \\
(y+1) &= -3(0:1:0) + (\zeta_1:-1:1) + (\zeta_2:-1:1) + (\zeta_3:-1:1), \\
(x+i) &= -2(0:1:0) + 2(-i:0:1), \\
(y+i) &= -3(0:1:0) + (\zeta_4:-i:1) + (\zeta_5:-i:1) + (\zeta_6:-i:1), \\
&\quad \text{where } \zeta_1, \zeta_2, \zeta_3 \text{ are the roots of } x^3 + x = 1, \\
&\quad \text{where } \zeta_4, \zeta_5, \zeta_5 \text{ are the roots of } x^3 + x = -1.
\end{aligned}$$

Because

$$\sigma\left(\frac{y}{x}\right) = -\frac{y}{x} = \rho^2\left(\frac{y}{x}\right)$$

$$\frac{y}{x},\quad t$$

doesn't generate x or y.
We put

$$s = \frac{x-1}{y}, \tag{35}$$

then

$$(s) = (0:1:0) - (1:\sqrt{2}:1) - (1:-\sqrt{2}:1) + (0:0:1) + (i:0:1) + (-i:0:1).$$

And we have

$$(s) + (t)_\infty \geq 0.$$

Secondly, we must show s and t generates x and y.
From (33), (34), (35), we have relations

$$s^2(x^3+x) = (x-1)^2, (x^4+6x^2+1)^2 = tx(x-1)^2(x+1)^2(x^2+1).$$

Using these relations to descent the degree of x, we have

$$\begin{aligned}
((8s^{10} &+ 32s^8 + 38s^6 + 10s^4)t^2 \\
&+ (2s^{12} + 32s^{10} + 82s^8 + 210s^6 + 6s^4 - 42s^2)t \\
&+ 30s^{14} + 188s^{12} + 206s^{10} - 352s^8 + 192s^6 + 80s^4 - 88s^2 + 32)x \\
+ (-s^{10} &- 8s^8 - 15s^6 - 8s^4)t^2 \\
&+ (s^{12} - 8s^8 - 78s^6 - 49s^4 + 32s^2)t \\
&- 30s^12 - 136s^10 + 58s^8 + 112s^6 - 184s^4 + 96s^2 - 24 = 0
\end{aligned}$$

So we have

$$x \in \mathbb{C}(s,t) \text{ and } y = \frac{x-1}{s} \in \mathbb{C}(s,t).$$

Finally, we make a defining equation.
To Eliminate x and y from (33), (34), (35), we have the defining equation as follows.

$$\begin{aligned}
&- 4s^{16} + (4t-32)s^{14} + (-t^2+20t-128)s^{12} \\
&+ (t^3-2t^2+8t-192)s^{10} + (4t^3-13t^2-160t-32)s^8 + (4t^3-12t^2-80t+384)s^6 \\
&\qquad + (-36t^2-176t-512)s^4 + (96t+256)s^2 - 64 = 0.
\end{aligned}$$

This have a degree $16 = |BD_{2\times4}|$.

7. More examples

We perhaps make $BD_{2\times3}$ to use a rational point of order three, and D_6 , $BD_{2\times6}$ to use a rational point of order six.
By the same way as to make $Z_4 \oplus Z_2$, we can't make non Abelian group $E(4,n)$ to use a translation of order two. We might make exceptional elliptic group $Z_4 \ltimes Z_5$ as smallest one in this way.
This way to make Galois groups is not work to make examples generally.

CHAPTER 3

Galois point

We start from the following.

THEOREM 4 (Yoshihara). *If non singular projective plane curve C of degree four has two Galois points then the defining equation of C is*

$$y + x^4 + y^4 = 0$$

by suitable projective transformation. And C has four Galois points on the line $x = 0$.

We call the curve as C_4 in this theorem.

THEOREM 5 (Yoshihara). *We denote number of Galois points by $\delta(C)$ where C is a non singular projective plane curve of degree four. Then $\delta(C) = 0, 1, 4$ (resp. $\delta(C) = 0, 1$) if $d = 4$ (resp. $d > 4$).*

We treat a curve

$$C_4 \ : \ YZ^3 + X^4 + Y^4 = 0$$

and a surface

$$S_8 \ : \ XY^3 + ZW^3 + X^4 + Z^4 = 0.$$
$$(\partial_X, \partial_Y, \partial_Z) = (4X^3, Z^3 + 4Y^3, 3YZ^2).$$

So C is non singular projective plane curve of degree four.
Galois group at Galois point P induces a transformation between points in the intersection of a line through P and the curve C. So if the line l through P is a tangent line then l is a bitangent line or intersection is 2-flex.

$$\mathrm{Hess}(YZ^3 + X^4 + Y^4) = \begin{vmatrix} \partial_{XX} & \partial_{XY} & \partial_{XZ} \\ \partial_{YX} & \partial_{YY} & \partial_{YZ} \\ \partial_{ZX} & \partial_{ZY} & \partial_{ZZ} \end{vmatrix}$$
$$= \begin{vmatrix} 12X^2 & 0 & 0 \\ 0 & 12Y^2 & 3Z^2 \\ 0 & 3Z^2 & 6YZ \end{vmatrix} = 2^2 \times 3^3(8Y^3 - Z^3)X^2Z$$

Because a tangent line at a 2-flex point intersects with Hessian of multiplicity two, 2-flex point is on the line $X = 0$ and we have

$$(0 : 0 : 1), \quad (0 : {e_6}^1 : 1), \quad (0 : {e_6}^3 : 1), \quad (0 : {e_6}^5 : 1)$$

Translating a point

$$(0 : {e_6}^3 : 1) = (0 : -1 : 1)$$

to origin , we have defining equation

$$(y - 1) + x^4 + (y - 1)^4 = x^4 + y^4 - 4y^3 + 6y^2 - 3y = 0.$$

Let $y = tx$ and dividing by x, we have

$$(1 + t^4)x^3 - 4t^3x^2 + 6t^2x - 3t = 0$$

Calculating resultant , we have a discriminant D of this equation as follows :

$$D = \frac{3t^2(9+t^4)^2}{(1+t^4)^4}$$

Because D is complete square , $(0:-1:1)$ is a Galois point. By action of Galois group Z_3 at a Galois point $(0:0:1)$, a point $(0:-1:1)$ mapped to a point $(0:-{e_3}^n:1)$, so we have three Galois points

$$(0:-{e_3}^2:1),\quad (0:-1:1),\quad (0:-e_3:1).$$

These four points are all of Galois points and we rewrite to use e_6 as follows :

$$(0:0:1),\quad (0:e_6:1),\quad (0:{e_6}^3:1),\quad (0:{e_6}^5:1).$$

Next, we want to automorphism group at a Galois point P. For this purpose, we determine an element $\sigma \in (3,\mathbb{C})$ such that :

(i) $\sigma(P) = P$.
(ii) $\sigma(l) = l$ where l is any line through P.
(iii) σ fixes the curve C_4.

It is too difficult to calculate by hand so we calculate by MATHEMATICA.
Put σ_1 (resp. σ_2, σ_3, σ_4) be a generator of a Galois group at a point $P_1(0:0:1)$ (resp. $P_2(0:e_:1)$, $P_3(0:{e_6}^3:1)$, $P_4(0:{e_6}^5:1)$).

$$\sigma_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & {e_6}^2 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2e_6-1 & -e_6-1 \\ 0 & 4e_6-2 & e_6+1 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2e_6-1 & -e_6+2 \\ 0 & -2e_6+4 & e_6+1 \end{pmatrix} \qquad \sigma_4 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2e_6-1 & -e_6-1 \\ 0 & -2e_6-2 & e_6+1 \end{pmatrix}$$

Any Galois group at a Galois point is cyclic , but each Galois group acts on 4 Galois points, so all groups are represented in S_4 simultaneously.
Let $G(V)$ denote the group generated by automorphisms at Galois points on $V = C_4$ or S_8. Since $G(V)$ has an injective representation in $PGL(n,k)$ ($n = 3$ or 4), *we use the same notation of an element of $G(V)$ as the projective transformation induced by it.*

THEOREM 6. *There exist exact sequences of groups*

$$1 \longrightarrow \langle \mathrm{diag}[1,-1,-1] \rangle \longrightarrow G(C_4) \longrightarrow A_4 \longrightarrow 1$$
$$1 \longrightarrow \langle \mathrm{diag}[\sqrt{-1},1,1] \rangle \longrightarrow \mathrm{Aut}(C_4) \longrightarrow A_4 \longrightarrow 1.$$

For the surface $S_8 : XY^3 + ZW^3 + X^4 + Z^4 = 0$, we have the following.

THEOREM 7. *There exist exact sequences of groups*

$$1 \longrightarrow \langle I_2 \oplus (-I_2) \rangle \longrightarrow G(S_8) \longrightarrow G(l_1) \times G(l_2) \longrightarrow 1$$
$$1 \longrightarrow \langle (I_2 \oplus (-I_2), I_2 \oplus (-I_2)) \rangle \longrightarrow \widetilde{G_1} \times \widetilde{G_2} \longrightarrow G(S_8) \longrightarrow 1,$$

Especially the order of $G(S_8)$ is $2^5 3^2$.

For details please see ([8]).

Bibliography

[1] S.Fukasawa, Galois points for a plane curve in arbitrary characteristic, *Geom. Dedicata.* **139** (2009), 211-218.

[2] Joseph H. Silverman, The arithmetic of Elliptic Curves, *Graduate Studies in Math.* **106** (1985), Springer-Verlag.

[3] Joseph H.Silverman and Jhon Tate, Rational Points on Elliptic Curves, (1992),Springer-Verlag, New York.

[4] J.S.Chahal, Topics in Number Theory, (1988),Plenum Press,New York.

[5] K.Miura, Galois points on singular plane quartic curves, *J. Algebra.* **287** (2005), 283-294.

[6] K.Miura and H.Yoshihara, Field theory for function fields of plane curves, *J. Algebra.* **226** (2000), 283-294.

[7] M.Kanazawa and H.Yoshihara, Galois Group at Galois Point for Genus-One Curve, *Int J. Algebra.* **5** (2011), 1161–1174.

[8] M. Kanazawa, T. Takahashi and H. Yoshihara, The group generated by automorphisms belonging to Galois points of the quartic surface, *Nihonkai Mathematical Journal.* vol.12 (2001) 89 – 99.

[9] H.Yoshihara, Function field theory of plane curves by dual curves, *J. Algebra.* **239** (2001), 340-355.

[10] H.Yoshihara, Galois embedding of algebraic variety and its application to abelian surface. *Rend. Sem. Mat. Univ. Padova.* **117** (2007), 69-85.

[11] H.Yoshihara, Rational curve with Galois point and extendable Galois automorphism, *J. Algebra.* **321** (2009), 1463-1472.

[12] H.Yoshihara, A relation between Galois automorphism and curve singularity, *JP J. Algebra, Number theory and applications.* **2** (2011), 213-223.