GALOIS REPRESENTATION ON ELLIPTIC CURVE

BY

HYECK KI MIN

AUGUST 8 2022

A THESIS SUBMITTED TO THE
FACULTY OF THE GRADUATE STUDIES OF
YORK UNIVERSITY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF ARTS
IN THE DEPARTMENT OF MATHEMATICS AND STATISTICS

Abstract

This thesis explores the orders of Galois representations about torsion subgroups of elliptic curves. We review the literature on elliptic curves and Serre's theorem. We describe a field formed by adjoining torsion subgroup of an elliptic curve. We show that the extension is finite and algebraic. Next, we construct a Galois group from the extension and use the relationship with a generalized linear group to find the possible values of the order of the Galois group. The order depends on the field where an elliptic curve is defined, the reducibility of $f(x)$, and structure of the torsion subgroup. This approach provides the same insight as Serre's theorem that provides an upper bound of the order of Galois representation of an extended field given by adjoining a subgroup of points of an elliptic curve.

Table of Contents

List of Figures

Chapter1

Introduction

An elliptic curve over a field F is a set of points (x, y) such that $y^2+sxy+ty = x^3+ux^2+vx+w$ with given coefficients s, t ,u, v, and $w \in F$. There are many applications of elliptic curves to answer mathematically interesting questions. Several examples of applications are presented in [7] and [14]. For example, given an area $n > 0$, elliptic curves can be used to find whether there is a right triangle whose area is n and its sides have rational lengths. For a given area $n > 0$, there are right triangles with rational length sides if and only if $y^2 = x^3 - n^2x$ has a rational point (x, y) with $y \neq 0$. To see this, we use a well-known one-to-one correspondence between the following two sets

$$C_n = \left\{(a, b, c) : a^2 + b^2 = c^2, \frac{ab}{2} = n\right\}$$
$$E_n = \left\{(x, y) : y^2 = x^3 - n^2x, y \neq 0\right\}$$

given by mutually inverse maps $f : C_n \to E_n$ and $g : E_n \to C_n$ defined as

$$f((a, b, c)) = \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right), g((x, y)) = \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right).$$

For instance, there is a right triangle of area 5 ($n = 5$) if and only if $y^2 = x^3 - 25x$ has a rational point. Since the curve passes through a point $P = (-4, 6)$, a rational point, one can find the corresponding right triangle of area 5 whose sides are $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$. Also, $y^2 = x^3 - 36x$

passes through (12,36). It corresponds to a right triangle of area 6 with sides 3,4, and 5.

Another application of elliptic curved is presented in [14]. We stack cannonballs in a square pyramid shape. Assuming that we have stacked up to x layers, we try to answer the question of whether they can be rearranged in a square form in two dimensions. This is equivalent to answer the question whether there are integers x and y such that $y^2 = \frac{x(x+1)(2x+1)}{6}$. We immediately see that $(1, 1)$ and $(0, 0)$ satisfy this equation. Can we find other integral points on this curve? To answer that, we consider a straight line that connects the two points $y = x$ and $y^2 = \frac{x(x+1)(2x+1)}{6}$. We find the intersection of the line $y = x$ and the elliptic curve $y^2 = \frac{x(x+1)(2x+1)}{6}$, which is $(x, y) = (\frac{1}{2}, \frac{1}{2})$. This is another point of $y^2 = \frac{x(x+1)(2x+1)}{6}$. Since $y^2 = \frac{x(x+1)(2x+1)}{6}$ is symmetric about x-axis, we can see that $(x, y) = (\frac{1}{2}, -\frac{1}{2})$ is also a point on $y^2 = \frac{x(x+1)(2x+1)}{6}$. After that, we find the linear line $y = 3x - 2$ that passes through $(\frac{1}{2}, -\frac{1}{2})$ and $(1, 1)$ and $y^2 = \frac{x(x+1)(2x+1)}{6}$ intersect at $(24, 70)$. This is another integer point on $y^2 = \frac{x(x+1)(2x+1)}{6}$.

Throughout this paper, we will focus on the case where points on an elliptic curve over a field F form a group. In particular, we do not consider curves $f(x, y) = 0$ such that the partial derivatives $f_x(P)$ and $f_y(P)$ are both zeros at a point P. The reason is that we have a cusp or a node at such a point and we cannot define the tangent line at the point. Hence, at such a point, it is impossible to clearly define a tangent line to the curve. We will see that this would prevent us to understand the algebraic structure of the points on the elliptic curve.

In the literature, a formal definition of elliptic curves includes the point at infinity, denoted by O, in addition to the points on them. This point is defined to be the identity of the group formed by the points on the given elliptic curve. Intuitively, the point at infinity is defined as the third point that the vertical line that connects a point P on an elliptic curve and another point symmetric with respect to the x-axis and the elliptic curve intersect. After introducing backgrounds about elliptic curves, we introduce torsion subgroups of an elliptic curve over arbitrary fields. The torsion subgroups help understanding of the group structure

of the set of points on an elliptic curve.

Next, based on [2] and [8], we consider extensions of a field where we add torsion subgroups of an elliptic curve. We demonstrate that this extension is algebraic and the Galois group formed by the extension can be represented by matrices. Using this representation, we find the possible values of the order of the Galois group if elliptic curves are defined over a field. We tried to limit the values that the order of a Galois extension can have. Based on [12], knowing possible values of the orders provide an intuition about how large the order of the Galois group will be.

Chapter2

Basic Theory about Elliptic Curves

2.1 Elliptic Curves

2.1.1 Definition about Elliptic Curves

This section begins with a definition of an elliptic curve over a field F.

Definition 1. *([7]) Given a field F and s, t ,u, v, and $w \in F$, elliptic curve over a field F is the set of the points (x, y) on the curve*

$$y^2 + sxy + ty = x^3 + ux^2 + vx + w \tag{2.1}$$

along with a point at infinity O. Denote it as $E(F)$.

An elliptic curve given by equation (2.1) is called the "generalized Weierstrass equation" of the curve. There is a simplified form of Generalized Weierstrass equations, which is determined by the characteristic of the field where the curve is defined.

Theorem 2.1.1. *([15] [10],[13]) The equation (2.1) in the Definition 1 can be transformed into the following forms, depending on the characteristics of the field F.*

1. *Let $char(F) = 2$. Then,*

$$y^2 + Ay = x^3 + Bx + C \text{ or} \tag{2.2}$$

$$y^2 + xy = x^3 + Ax^2 + B \tag{2.3}$$

where $A, B, C \in F$.

2. *Let* $char(F) = 3$. *Then,*

$$y^2 = x^3 + Ax^2 + B \tag{2.4}$$

where $A, B \in F$.

3. *Let* $char(F) > 3$ *or* $char(F) = 0$. *Then,*

$$y^2 = x^3 + Ax + B \tag{2.5}$$

where $A, B \in F$.

The proof uses a transformation of variables in equation (2.1). Here, the case where $char(F) > 3$ or $char(F) = 0$ (part 3 in Theorem 2.1.1) is proved.

Proof: Proof of (3). We start with the Generalized Weierstrass equation from (2.1).

$$y^2 + sxy + ty = x^3 + ux^2 + vx + w$$

Since char $(F) \neq 2$, through completing squares, we obtain

$$\begin{aligned}
&y^2 + (sx+t)\,y = x^3 + ux^2 + vx + w \\
&\rightarrow y^2 + (sx+t)\,y + \left(\tfrac{sx+t}{2}\right)^2 = x^3 + ux^2 + vx + w + \left(\tfrac{sx+t}{2}\right)^2 \\
&\rightarrow \left(y + \tfrac{sx+t}{2}\right)^2 = x^3 + (u + \tfrac{s^2}{4})x^2 + (v + \tfrac{ts}{2})x + w + \tfrac{t^2}{4}
\end{aligned}$$

Using the following substitutions, $\bar{y} = y + \frac{sx+t}{2}$, $\bar{a} = u + \frac{s^2}{4}$, $\bar{b} = v + \frac{ts}{2}$, and $\bar{c} = w + \frac{t^2}{4}$, we can rewrite above by

$$\bar{y}^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}$$

Let $\bar{x} = x + \frac{\bar{a}}{3}$, Then, it can be shown that $\bar{y}^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}$ is transformed to $\bar{y}^2 = \bar{x}^3 + A\bar{x} + B$ for some $A, B \in F$ where $A = \frac{\bar{a}^2}{3} + \bar{b}$ and $B = -\frac{\bar{a}^3}{27} + \bar{c} - \frac{\bar{a}\bar{b}}{3}$. We get the form of the equation as desired. ■

2.1.2 Addition of Points on an Elliptic Curve

In Chapter 1, we presented a method of finding different points on the same curve using existing points on an elliptic curve. Based on this approach, we define in this section the addition of two points on an elliptic curve. We follow [15].

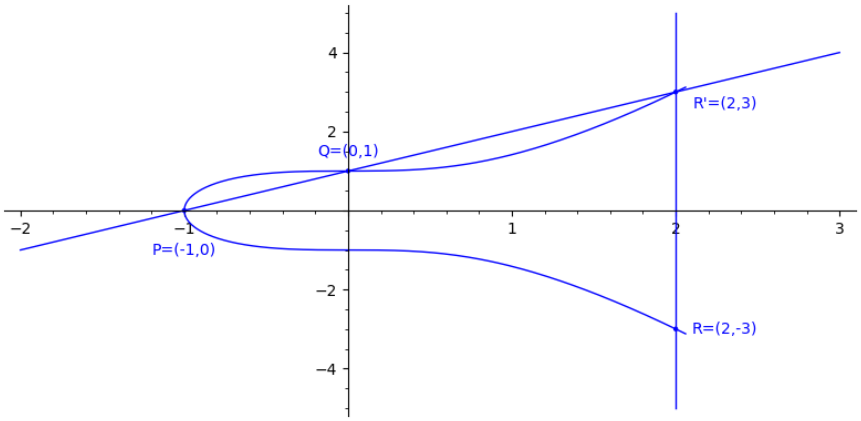
We start at two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ of an elliptic curve $E(F)$. Addition $+_E$ on $E(F)$ is loosely described geometrically as follows: consider a line L passing through P and Q. Then, we find another point on $E(F)$ that is on the line L. Let the point be $\bar{R}$. After finding a vertical line passing through $\bar{R}$, the intersection of that line and $E(F)$ is obtained. This gives us a point R and we define $R = P +_E Q$.

Before we give a formal definition of the addition, we provide an example of such an addition.

Example Let E be an elliptic curve over $\mathbb{R}$ and be given by $y^2 = x^3 + 1$. We know $(-1, 0)$ and $(2, 3)$ are on E. Then, the line connecting the two points is $y = x + 1$ and substituting it to $y^2 = x^3 + 1$ provides a new point $(0, 1)$ on the elliptic curve. Hence, $(-1, 0) +_E (2, 3) = (0, -1)$.

To study this in detail, let $char(F) > 3$ or $char(F) = 0$. Then, by Theorem 2.1.1, the elliptic curve is $y^2 = x^3 + Ax + B$ for some $A, B \in F$. Suppose we have two points on the curve $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ where $x_1 \neq x_2$. The line passing through $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ has a slope $\frac{y_2 - y_1}{x_2 - x_1}$ and hence L is $y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1$. Then, substituting y into $y^2 = x^3 + Ax + B$ will yield the other point on $E(F)$ where L intersects. The intersection is $(m^2 - x_1 - x_2, y_1 - m(2x_1 + x_2 - m^2))$. The reflection about x-axis will yield $R = (m^2 - x_1 - x_2, -y_1 + m(2x_1 + x_2 - m^2))$ and $R = P +_E Q$ that we desire (See Figure 2.1 below for an example of an elliptic curve that is drawn based on SageMath code from [9]).

Figure 2.1: Example of the addition of two points $P = (-1, 0)$ and $Q = (0, 1)$ $(R = P +_E Q)$ on an elliptic curve $y^2 = x^3 + 1$. The vertical line is $x = 2$ and the other line is $y = x + 1$.



Next, we consider the case where $x_1 = x_2$ and $y_1 \neq y_2$. That is, they are two distinct points P and Q with the same x-coordinate. In this case, the line that connects the two points is a vertical line. Hence, we define $P +_E Q$ as the point at infinity.

The last case is when $P = Q$. For this, we consider the line L tangent to E at P. Through implicit differentiation, $\frac{dy}{dx}(x_1, y_1) = \frac{3x_1^2 + A}{2y_1}$. As long as $y_1 \neq 0$, the slope of the tangent line is well-defined. The line L will be $y = \frac{3x_1^2 + A}{2y_1}(x - x_1) + y_1$ and substituting y into $y^2 = x^3 + Ax + B$ results in finding $2P$, which is $(m^2 - 2x_1, m(3x_1 - m^2) - y_1)$ where $m = \frac{3x_1^2 + A}{2y_1}$. If $y_1 = 0$ and $3x_1^2 + A \neq 0$, then the tangent line at (x_1, y_1) is vertical and $2P$ is defined to be the point at infinity O.

An implicit assumption behind the operation $+_E$ is that an elliptic curve over a field F is smooth. That is, it is presumed that the curve does not have a cusp or a node at a point, which is called a singular point. To describe precisely, we define the singularity at a point and a non-singular curve.

Definition 2. *([7]) Suppose $E = \{(x, y) \in F^2 | f(x, y) = 0\}$ is a curve on F^2 and let $P \in E$. Then, P is called a singular point of E if and only if*

$$\frac{\partial f}{\partial x}(P) = 0 \text{ and } \frac{\partial f}{\partial y}(P) = 0 \tag{2.6}$$

If P is not a singular point, it is called a non-singular point. If none of the points of E are singular, then the curve is non-singular.

Remark If $\frac{\partial f}{\partial x}(P) = 0$ and $\frac{\partial f}{\partial y}(P) = 0$, then the curve $f(x, y)$ has a node or cusp at P.

Here, we study the meaning of an elliptic curve singular at a point. Suppose $f(x, y)$ in the Definition 1 is singular at a point P. Then, note that we cannot identify $2P$ since it is impossible to identify a tangent line to the point. Hence, the points on the curve with the singular points do not form a group in general. Hence, we will only consider an elliptic curve over a field that does not have a singular point hereafter.

Remark We assume an elliptic curve is defined over a field F whose characteristic is neither two nor three. The singularity of the elliptic curve is related to whether the right-hand side of an elliptic curve $y^2 = f(x)$ has a repeated root. Suppose the right-hand side of (2.5) has a repeated root. Then, we can express both of the equations as $y^2 = (x - \alpha)^2(x - \beta)$ or $y^2 = (x-\alpha)^3$. If $F(x, y) = y^2-(x-\alpha)^2(x-\beta)$, then $\frac{\partial F}{\partial x} = -(x-\alpha)(3x-\alpha-2\beta)$ and $\frac{\partial F}{\partial y} = 2y$ by the product rule of differentiation. Then, if we let $x = \alpha$ and $y = 0$, then $(\alpha, 0) \in E(F)$ and both of the partial derivatives vanishes at (x, y), which implies the curve is singular at the point. The similar argument applies for the case $y^2 = (x - \alpha)^3$. Conversely, we show if an elliptic curve $y^2 = x^3 + Ax + B$ is singular, then the right-hand side of $y^2 = x^3 + Ax + B$ has a repeated root. If $y^2 = x^3 + Ax + B$ is singular, then by differentiation of the curve

with respect to y and x respectively, we obtain $2y = 0$ and $3x^2 + A = 0$. Then $y = 0$. Also, if we let $f(x) = x^3 + Ax + B = 0$ and therefore $f'(x) = 3x^2 + A = 0$, then $f(x)$ has a repeated root. Note that we need to assume $char(F) \neq 2$ to make $2y = 0$ imply $y = 0$ and $char(F) \neq 3$ to ensure $f(x)$ has a repeated root. Hence, our assertion about the relationship between having a repeated root and singularity of an elliptic curve is proved.

2.1.3 Elliptic Curves over Fields of Characteristic 2 and 3

We need to give a different definition of the operation $+_E$ on elliptic curves defined over a field with characteristic 2 because the elliptic curves in such a field have different forms of equations from the ones when fields where those curves are defined have characteristics not equal to two. If a field F has characteristic two and is perfect, then by Theorem 2.1.1, the generalized Weierstrass equation can be written as as either in (2.2) or (2.3). Before defining $+_E$, it is necessary to examine the conditions under which Equations (2.2) and (2.3) are non-singular.

We consider equation (2.2). We find $y^2 + Ay + x^3 + Bx + C = 0$ is non-singular if and only if $A \neq 0$. This is because $F_x = 3x^2 + B = x^2 + B$ and $F_y = 2y + A = A$ do not both vanish if the non-singularity holds. Also, we consider elliptic curves of the form (2.3). We claim the elliptic curve is singular at $(0, 0)$. Let $G(x, y) = y^2 + xy + x^3 + Ax^2 + B$. $G_x = y + x^2$ and $G_y = x$ because $char(F) = 2$. Hence, $G_x = G_y = 0$ at $P = (0, 0)$. From this, we point out that by Definition 2 and the equation (2.3), if $B = 0$, then $P = (0, 0)$ is a singular point of the elliptic curve (2.3). If $B \neq 0$, we find the point $P = (0, 0)$ is not a singular point on the curve since it is not on the curve. Hence, we need the condition $B \neq 0$ to ensure the curve is not singular at $P = (0, 0)$.

We provide the doubling formula below.

Theorem 2.1.2. *([15]) Let P be a point on $E(F)$ where $char(F) = 2$ and F is a perfect field*

1) If an elliptic curve E is described by the equation $y^2 + Ay + x^3 + Bx + C = 0$ where $A \neq 0$,

then

$$2P = P +_E P = \left(\frac{x^4 + B^2}{A^2}, \left[\frac{x^2 + B}{A} \right] \left[\frac{x^4 + B^2}{A^2} - x \right] + A \right) \tag{2.7}$$

2) If an elliptic curve E is described by the equation $y^2 + xy + x^3 + Ax^2 + B = 0$ with $B \neq 0$, then

$$2P = P +_E P = \left(\frac{x^4 + B}{x^2}, \left[\frac{y + x^2}{x} \right] \left[\frac{x^4 + B}{x^2} - x \right] + \frac{x^4 + B}{x^2} \right) \tag{2.8}$$

For $x = 0$, $2P = O$.

Proof: We prove part 1). By implicit differentiation, we find $2yy' + Ay' + 3x^2 + B = 0$ Hence, $y' = \frac{x^2+B}{A}$. Then, the tangent line to (x_0, y_0) is $y = \frac{x^2+B}{A}(x - x_0) + y_0$. If we substitute $y = \frac{x^2+B}{A}(x - x_0) + y_0$ into $y^2 + Ay + x^3 + Bx + C = 0$, we find the x-coordinate of $2P$ is $(\frac{x_0^2+B}{A})^2$. Substituting $x = (\frac{x_0^2+B}{A})^2$ into $y^2 + Ay + x^3 + Bx + C = 0$ and finding the inverse of the y-coordinate of the resulting coordinate provide the y-coordinate of $2P$, which is given by $\left[\frac{x_0^2+B}{A} \right] \left[\frac{x_0^4+B^2}{A^2} - x_0 \right] + A$ ■

Remark The assumption that a field F must be perfect is needed to make $A \neq 0$ is a sufficient condition for the non-singularity of the elliptic curve in the part 1) in Theorem 2.1.2. More precisely, we know if $f(x, y) = y^2 + Ax + x^3 + Bx + C$, the elliptic curve is singular if $f_x(x, y) = x^2 + B = 0$ and $f_y(x, y) = A = 0$. If F is a perfect field, there exists $b \in F$ such that $b^2 + B = 0$. This implies the curve is singular if $A = 0$. Therefore, $A \neq 0$ becomes a sufficient condition for the non-singularity if F is a perfect field.

Also, for the distinct points, we define $P +_E Q$ if $P \in E(F)$ and $Q \in E(F)$.

Theorem 2.1.3. *([15]) Let $char(F) = 2$ and suppose an elliptic curve over F is given by $y^2 + xy = x^3 + Ax + B$. Then, for a given point $P = (x_1, y_1)$, $-P = (x_1, y_1 + x_1)$ and if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two distinct points such that $P \neq -Q$, then $P +_E Q = (m^2 + m + x_1 + x_2 + A, m(x_1 + x_3) + x_3 + y_1)$ where $m = \frac{y_1+y_2}{x_1+x_2}$ and $x_3 = m^2 + m + x_1 + x_2 + A$*

Proof: The inverse of a point $P = (x_1, y_1)$ is $-P = (x_1, x_1 + y_1)$. The reason is that a point (x, y) is on the curve if $y^2+x_1y = x_1^3+Ax_1^2+B = y_1^2+x_1y_1$ and hence $(y+y_1)(y+x_1+y_1) = 0$, which implies $y = y_1$ or $y = x_1 + y_1$. This means a vertical line $x = x_1$ intersects with the elliptic curve at (x_1, y_1) and $(x_1, x_1 + y_1)$. Hence, for the point P, $-P = (x_1, x_1 + y_1)$.

Suppose P and Q are distinct points such that $-P \neq Q$. The slope of a line that connects P and Q is $y = \frac{y_1+y_2}{x_1+x_2}(x - x_1) + y_1$. We substitute y into the elliptic curve and find $P+_EQ = (m^2+m+x_1+x_2, m(x_1+x_3)+x_3+y_1)$ where $m = \frac{y_1+y_2}{x_1+x_2}$ and $x_3 = m^2+m+x_1+x_2+A$ ■

Theorem 2.1.4. *([15]) Let $char(F) = 2$. Also, suppose an elliptic curve over F is given by $y^2 + Ay = x^3 + Bx + C$. Then, for a given point $P = (x_1, y_1)$, $-P = (x_1, A + y_1)$ and if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two distinct points such that $P \neq -Q$, then $P +_E Q = (m^2 + x_1 + x_2, A + m(x_1 + x_3) + y_1)$ where $m = \frac{y_1+y_2}{x_1+x_2}$ and $x_3 = m^2 + x_1 + x_2$.*

Proof: The proof is analogous to Theorem 2.1.3. ■

Remark In the case of $Q = -P$, then the line connecting the two points P and Q is a vertical line and $P +_E Q$ is the point at infinity O. If $P = Q$, then $2P$ is given in Theorem 2.1.2.

Next, we describe the operation $+_E$ on an elliptic curve over a field whose characteristic is 3. Based on [13], we can write an elliptic curve over such a field as $y^2 = x^3 + Ax^2 + B$. We provide conditions on A and B for non-singularity.

Theorem 2.1.5. *Let $y^2 = x^3+Ax^2+B$ is an elliptic curve over a field F with characteristic 3. Then, $y^2 = x^3 + Ax^2 + B$ is non-singular if $A \neq 0$ and $B \neq 0$.*

Proof: Let $F(x, y) = y^2 - x^3 - Ax^2 - B$. Then, $F_x = 3x^2 + 2Ax = 2Ax$ and $F_y = 2y$. Hence, if the elliptic curve is singular, then $A = 0$ and $y = 0$. If $x = 0$, then $B = 0$ if the elliptic curve is singular. This indicates the elliptic curve is non-singular if $A \neq 0$ and $B \neq 0$. ■

The addition of two points and doubling a point is defined as below:

Theorem 2.1.6. *([13]) Let $char(F) = 3$ and suppose an elliptic curve over F is given by $y^2 = x^3 + Ax^2 + B$. Then, for a given point $P = (x_1, y_1)$, $-P = (x_1, -y_1)$ and if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two distinct points such that $P \neq -Q$, then $P +_E Q = (m^2 - A - x_1 - x_2, m(x_1 - x_3) - y_1)$ where $m = \frac{y_2 - y_1}{x_2 - x_1}$ and $x_3 = m^2 - A - x_1 - x_2$. Also, $2P = (m^2 - A + x_1, m(x_1 - x_2) - y_1)$ where $m = \frac{Ax_1}{y_1}$ and $x_2 = m^2 - A + x_1$.*

Remark We assume $char(F) = 3$ and $y^2 = x^3 + Ax^2 + B$ be an elliptic curve over F. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two distinct points. If $x_1 = x_2$, then $P +_E Q$ will be the point at infinity. If $y_1 = 0$, $2P$ will be the point at infinity. For point $P = (x_1, y_1)$ on the curve, $-P = (x_1, -y_1)$ since the y-coordinate where vertical line $x = x_1$ meets the curve is characterized by $y^2 + 2x_1^3 + 2Ax_1^2 + 2B = 0$.

2.1.4 Group Law

We defined the operation $+_E$ over any field. For this operation to be defined on an elliptic curve, the curve must be non-singular at every point. Otherwise, it is impossible to double a point at a singular point since a tangent line at such a point cannot be defined. Therefore, in all subsequent discussions, it is assumed that singular points of the elliptic curve that we consider do not exist.

The theorem below indicates that the set of points on $E(F)$ equipped with the operation $+_E$ is an Abelian group.

Theorem 2.1.7. *([15]) The set of the points on a non-singular elliptic curve E over the field F, denoted by $E(F)$ is an Abelian group under $+_E$. That is, for all P,Q, and R on E(F),*

1. *$P +_E Q \in E(F)$*
2. *(Associative) $(P +_E Q) +_E R = P +_E (Q +_E R)$.*
3. *There exists the identity element O on E such that $P +_E O = P$.*

4. There exists an inverse element of P, which is $-P$ such that the $P +_E (-P) = O$.

5. $P +_E Q = Q +_E P$.

We note the first four properties show $E(F)$ is a group under $+_E$. The last property indicates $E(F)$ is an Abelian group.

Proof: 1. This follows from the previous section.

2. We skip the proof for this part and refer to the reader to [15] or [11] for details.

3. If O is the point at infinity, the property follows from the definition.

4. Given that $char(F) \neq 2$, suppose $P = (x, y) \neq O$. Then, $-P = (x, -y)$ and $P +_E (-P) = O$. In the case of $P = O$, the same holds since $-P = O$. The analogous results holds when $char(F) = 2$. For details, refer to Theorem 2.1.3 and 2.1.4.

5. If $P = Q$, we are done. The statement holds if $P \neq Q$ since the algebraic expressions about doubling a point and addition of two points on an elliptic curve from the previous sections in this chapter do not change regardless of $P +_E Q$ or $Q +_E P$. ■

2.1.5 The map $\alpha_n : E(F) \to E(F)$

In this section, following [11] and [15], we study a map that sends a point P on an elliptic curve to another point on the same curve. In particular, the focus is on the map $\alpha_n : E[F] \to E[F]$ such that $P \to nP$ where $n \in \mathbb{Z}^+$ is fixed. $nP = P +_E P +_E \ldots +_E P$ denotes P is added n times. By Theorem 2.1.7, $nP \in E(F)$ if $P \in E(F)$.

Finding the smallest n such that nP is the point at infinity for any point P on $E(F)$ is an interesting task. This is because if such a (finite) n exists, we find a subgroup of $E(F)$ of order n created by P, which allows us to understand better the algebraic structure of $E(F)$.

Chapter3

Torsion Subgroups of Elliptic Curves

3.1 Torsion

To examine the algebraic structure of an elliptic curve defined over a field F, it is important to examine points on the curve with special properties. In particular, we focus on a subgroup of the group of the points on the curve, defined as n-torsion points.

Definition 3. *([7],[15]) Let $P \in E(\bar{F})$ where $\bar{F}$ is an algebraic closure of a field F. For $n \in Z$, P is a n-torsion point if $nP = O$. We denote the set of such points as $E[n]$.*

One thing to note among the properties of $E[n]$ is that $E[n]$ is a subgroup of $E(\bar{F})$.

Theorem 3.1.1. *([15]) $E[n]$ is a subgroup of $E(\bar{F})$.*

Proof: The proof is explicit since the operation $+_E$ is inherited to a subgroup of $E(\bar{F})$. Hence, the associativity of $+_E$, the existence of identity and inverse elements hold in $E[n]$. Also if P_1 and P_2 are in $E[n]$, then $n(P_1 +_E P_2)$ is the point at infinity since $n(P_1 +_E P_2) = nP_1 +_E nP_2 = O +_E O = O$ by Theorem 2.1.7. Hence, $E[n]$ is a subgroup of $E(\bar{F})$. ■

Remark Indeed, for a fixed $n \in \mathbb{N}$, the map $\alpha_n : P \to nP$ is a homomorphism and $ker(\alpha_n) = E[n]$.

Definition 4. *([11]) The smallest subgroup in $E(\bar{F})$ that contains all $E[n]$ for $n \geq 0$ is called torsion subgroup of $E(\bar{F})$ and is denoted by $E(\bar{F})_{tor}$. That is $E(\bar{F})_{tor} = \cup_{n\in\mathbb{N}} E[n]$.*

3.1.1 2-Torsion Points of an Elliptic Curve

We follow [15]. Suppose an elliptic curve is defined over a field F with $char(F) \neq 2$. 2-torsion points of an elliptic curve is a point $P \in E(\bar{F})$ such that $2P = O$. From the definition of the addition of the points on an elliptic curve in the previous chapter, the y-coordinate of a point P is zero if and only if P is a 2-torsion point. It is explicit from Theorem 2.1.2 that if the elliptic curve is defined over a field with $char(F) = 2$, then a point P is a 2-torsion point if its x-coordinate is zero given that the curve is of the form (2.3). If the curve is of the form (2.2), there are no 2-torsion points if the curve is non-singular.

Let $char(F) = 2$. Suppose a non-singular elliptic curve is of the form (2.2) in Theorem 2.1.1, which is $y^2 + Ay = x^3 + Bx + C$. where A, B and C are in F. We know $P \in E(F)$ is a 2-torsion point if and only if $2P = O$ or equivalently, $P = -P$. This implies $y = y + A$ therefore $A = 0$. However, in Theorem 2.1.2, A cannot be zero because of the non-singularity assumption. Hence, $E[2]$ is trivial in this case. Such an elliptic curve is called a "supersingular" elliptic curve. For details about a supersingular elliptic curve, refer to [14].

Also, suppose an elliptic curve is of the form (2.3) in Theorem 2.1.1, which is $y^2 + xy = x^3 + Ax^2 + B$ where $A, B \in F$ where F is a perfect field. We recall $B \neq 0$ is needed to non-singularity of the elliptic curve. Then, by the same argument above, $y = x + y$ so $x = 0$. Then, we obtain $y^2 = B$ and $y = \sqrt{B}$. Hence, $E[2] = \{O, (0, \sqrt{B})\}$ and $E[2] \cong Z_2$. This elliptic curve is sometimes called an "ordinary curve". The definition about an ordinary curve is found in [14].

Let F be a field with characteristic 3. Then, by Theorem 2.1.1, we get the reduced Weierstrass form of a non-singular elliptic curve $y^2 = x^3 + Ax^2 + B$. By the definition of 2-torsion points, the y-coordinate of every 2-torsion point is zero. Also, we find the discriminant of $x^3 + Ax^2 + B = 0$ is $2A^3B$ using SageMath code in [5]. We see $2A^3B \neq 0$ since $A \neq 0$ and $B \neq 0$ by Theorem 2.1.5. Since the degree of $x^3 + Ax^2 + B = 0$ is three, $E[2]$ consists of three distinct points on the x-axis together with the point at infinity. Therefore, $E[2] \cong Z_2 \oplus Z_2$

since every element has an order of 2, but the order of $E[2]$ is four.

Let $char(F) > 3$ or $char(F) = 0$. Then, by Theorem 2.1.1, Weierstrass equation can be written as $y^2 = x^3 + Ax + B$ where $A, B \in F$. The set of a 2-torsion points of this elliptic curve $E[2]$ is $\{O, (x_1, 0), (x_2, 0), (x_3, 0)\}$ where x_1, x_2, and x_3 is such that $y^2 = x^3 + Ax + B = (x - x_1)(x - x_2)(x - x_3)$. If the curve is non-singular, the discriminant of $x^3 + Ax + B$, which is equal to $-4A^3 - 27B^2$, is not zero, which implies $x^3 + Ax + B$ has three distinct roots. We can find $E[2] \cong Z_2 \oplus Z_2$ since every point of $E[2]$ has an order of at most 2 but the order of $E[2]$ is four.

3.1.2 n-Torsion points where $n > 2$

3.1.2.1 3-torsion points

Let $char(F) > 3$ or $char(F) = 0$ and $y^2 = x^3 + Ax + B$ is an elliptic curve over F. By the definition about n-torsion points, a point $P = (x, y) \in E(F)$ is a 3-torsion point if and only if $2P = -P$. From the definition of addition, $(m - 2x, m(3x - m^2) - y) = (x, -y)$ where $m = \frac{3x^2+A}{2y}$. We try to find an equation that x must satisfy to make P as a 3-torsion point.

From the expression for y-coordinates of $2P$ and $-P$, we obtain

$$\frac{3x^2+A}{2y}\{3x - \frac{(3x^2+A)^2}{4y^2}\} = 0$$

We expand the numerator of the second term in the curly bracket, and it follows

$$\frac{(3x^2+A)(3x^4+6Ax^2+12Bx-A^2)}{8y^3} = 0$$

Since $y \neq 0$, (otherwise, m is undefined and if $y = 0$, then Section 3.1.1 says the point is a 2-torsion point) and $3x^2 + A \neq 0$ (otherwise, then a x that satisfies $3x^2 + A = 0$ will be a repeated root of $x^3 + Ax + B = 0$ and this indicates the elliptic curve is singular), we find the x-coordinate of P must satisfy $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$.

Remark To determine $E[n]$, in general, we do not attempt to solve $nP = 0$. This is because O does not have a coordinate. Instead, we solve $(n-1)P = -P$ which is an equality between the points that we can solve.

Theorem 3.1.2. *[15] Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a field with characteristic 0 or greater than or equal to 5. Then, the x-coordinate of a point in $E[3]$ of the elliptic curve satisfies $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$. The equation has four distinct roots.*

Proof: By the characterization above, we can prove the the x-coordinate of a point in $E[3]$ must satisfy $3x^4+6Ax^2+12Bx-A^2 = 0$ from the definition about a 3-torsion subgroup above. Next, we prove $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$ has four distinct roots. By using Sagemath code based on [5], we find the discriminant of $3x^4 + 6Ax^2 + 12Bx - A^2$ is $(-6912)\,(4A^3 + 27B^2)^2$. We immediately find if $y^2 = x^3 + Ax + B$ is non-singular, which means $-4A^3 - 27B^2 \neq 0$, then the discriminant is non-zero. This implies $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$ has four distinct roots if $y^2 = x^3 + Ax + B$ is non-singular. ■

Therefore, there are a total of nine 3-torsion points including the point at infinity since $y^2 = x^3 + Ax + B$ is symmetric about the x-axis such that each non-zero x coordinate corresponds to two y-coordinates on the curve. Also, $E[3] \cong Z_3 \oplus Z_3$. The reason why $E[3] \cong Z_9$ does not hold is that every point in $E[3]$ has an order that is at most 3.

Next, we consider a field F with $char(F) = 2$. Suppose an elliptic curve is given by $E : y^2 + Ay + x^3 + Bx + C = 0$ over F. We know $P = (x, y) \in E(F)$ is a 3-torsion point if and only if $2P = -P$.

Theorem 3.1.3. *([15]) Let $E : y^2 + Ay + x^3 + Bx + C$ be a non-singular elliptic curve ($A \neq 0$) over a field F of characteristic 2. Then, the x-coordinate of a 3-torsion point satisfies $x^4 - A^2x + B = 0$ and it has four distinct roots.*

Proof: By definition of 3-torsion points and Theorem 2.1.2 , x-coordinate must satisfy $x^4 - A^2x + B = 0$. Specifically, from Theorem 2.1.2, we find $2P = -P$ implies $\frac{x^4+B^2}{A^2} = x$. This implies $x^4 - A^2x + B = 0$. Also, with SageMath code based on [5], we find the discriminant of $x^4 - A^2x + B$ is $-27A^8 + 256B^3 = A^8$ since $char(F) = 2$. Since $A \neq 0$ because of the non-singularity assumption, the discriminant is non-zero, which implies $x^4 - A^2x + B = 0$ has four distinct roots. ■

We claim $E[3] \cong Z_3 \oplus Z_3$. For each x that satisfies $x^4 - A^2x + B = 0$, we find the corresponding y-coordinates by finding zeros of $h(y) = y^2 + Ay + x^3 + Bx + C$. Since $h'(y) = 2y + A \equiv A$ in a field of characteristic 2 and $A \neq 0$ by the non-singularity assumption, $h'(y) \neq 0$ for all y. This implies $h(y)$ does not have a repeated root. Hence, we find for each x that satisfies $x^4 - A^2x + B = 0$, there are two distinct corresponding y-coordinates that make $y^2 + Ay + x^3 + Bx + C$ hold. Hence, there are 8 coordinates that belongs to $E[3]$. Hence, we find there are nine 3-torsion points if we additionally include O. Also, by the same argument for $char(F) = 0$ and $char(F) > 3$ cases, $E[3] \cong Z_3 \oplus Z_3$.

When an elliptic curve is alternatively given by $y^2 + xy = x^3 + Ax^2 + B$, the similar argument shows the x-coordinate of a 3-torsion point P must satisfy $x^4 + x^3 + B = 0$ since any 3-torsion point P must satisfy $2P = -P$.

Theorem 3.1.4. *Let $E : y^2 + xy = x^3 + Ax^2 + B$ be a non-singular elliptic curve (or $B \neq 0$) over a field F of characteristic 2. Then, the x-coordinate of $E[3]$ must satisfy $x^4 + x^3 + B = 0$ and it has four distinct roots.*

Proof: We find from Theorem 2.1.2 that $2P = -P$ implies $\frac{x^4+B}{x^2} = x$. It follows $x^4 + x^3 + B = 0$. Through SageMath code based on [5], we find the determinant of $x^4 + x^3 + B$ is $(256B - 27)B^2 = B^2$ since $char(F) = 2$. $B \neq 0$ implies the discriminant is non-zero and $x^4 + x^3 + B = 0$ has four distinct roots. ■

Therefore, $E[3] \cong Z_3 \oplus Z_3$ as in the case where the elliptic curve is given by $E : y^2 + xy = x^3 + Ax^2 + B$. We claim this is because for each x that satisfies $x^4 + x^3 + B = 0$, there exist two distinct y-coordinates. We see this from the fact that if we take the first-order derivative of $g(y) = y^2 + xy + x^3 + Ax^2 + B$, we get $g'(y) = x$ and $x \neq 0$ ($x = 0$ implies the point P is a 2-torsion point) by the non-singularity assumption, $g'(y) \neq 0$ for all y. Hence, $g(y)$ does not have a repeated root and this proves our claim.

Before we go into the next section, we consider an elliptic curve defined over a field F of characteristic 3. By Theorem 2.1.1, the curve is of the form $y^2 = x^3 + Ax^2 + B$ where A and B are constants in the field F. From Theorem 2.1.6, $P = (x, y)$ is a 3-torsion point if

$m^2 - A + x = x$ where $m = \frac{Ax}{y}$. Hence,

$$Ax^3 + AB = 0 \tag{3.1}$$

Note that $A \neq 0$ is equivalent to the the non-singularity by Theorem 2.1.5. Hence, we can deduce the following theorem.

Theorem 3.1.5. *Let $E : y^2 = x^3 + Ax^2 + B$ be a non-singular elliptic curve over a field of characteristic 3 that is perfect. Then, $E[3] \cong Z_3$.*

Proof: We have to assume here that the field where E is defined is a perfect field. If $P = (x, y) \in E[3]$, then $2P = -P$ by definition. By Theorem 2.1.6, we find $m^2 - A + x = x$ where $m = \frac{Ax}{y}$. We can rewrite $m^2 - A + x = x$ to $Ax^3 + AB = 0$. Since $A \neq 0$ by non-singularity of the elliptic curve, we get $x^3 + B = 0$. Indeed, it has a single root with multiplicity 3 because the Frobenius map $\alpha : F \to F$ such that $\alpha \to \alpha^p$ where F is a field and p is a prime number is an isomorphism for perfect fields, hence surjective. That is, there exists $b \in F$ such that $x^3 + B = x^3 + b^3 = (x + b)^3$. This implies $x = -b$ is the single root. Hence, $E[3] \cong Z_3$ ■

In summary, the following theorem summarizes $E[2]$ and $E[3]$ of a non-singular elliptic curve over a field F that is perfect.

Theorem 3.1.6. *Let F be a field (or a perfect field when $char(F) = 2$ or 3) and $E(F)$ is a non-singular elliptic curve over the field F. Then,*

1. *Let $char(F) \neq 2$. Then, $E[2] \cong Z_2 \oplus Z_2$.*
2. *Let $char(F) = 2$. Then, $E[2] \cong Z_2$ or $\{O\}$.*
3. *Let $char(F) \neq 3$. Then, $E[3] \cong Z_3 \oplus Z_3$.*
4. *Let $char(F) = 3$. Then, $E[3] \cong Z_3$.*

3.1.2.2 4 and higher torsion points

A point $P \in E(F)$ where $E(F)$ is an elliptic curve over a field F is a 4-torsion point if and only if $4P = O$. $4P = O$ is equivalent to $2P = -2P$. This implies y coordinate of the point $2P$ must be zero (in a field of $char(F) \neq 2$.

Let $char(F) \neq 2, 3$ and $y^2 = x^3 + Ax + B$ where A,B are some constants in F. Let $P = (x, y) \in E(F)$. From the addition of the points on an elliptic curve as we have defined, the y coordinate of $2P$ is $m(3x - m^2) - y$ where $m = \frac{3x^2+A}{2y}$. Hence, we get

$2y - 2(\frac{3x^2+A}{2y})\{3x - (\frac{3x^2+A}{2y})^2\} = 0.$

Since $2y = 0$ when P is a 4-torsion point by definition $2P = -2P$, we obtain

$\frac{3x^2+A}{2y}\{3x - \frac{9x^4+6Ax^2+A^2}{4y^2}\} = 0$

Substituting $y^2 = x^3 + Ax + B$ results in

$\frac{\left(3x^2+A\right)\left\{12x\left(x^3+Ax+B\right)-9x^4-6Ax-1^2\right\}-8\left(x^3+Ax+3\right)^2}{8y^3} = 0$

Hence, y-coordinate of $2P$ is zero if and only if $x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4BAx - 8B^2 - A^3 = 0$.

Theorem 3.1.7. *$f(x) = x^6+5Ax^4+20Bx^3-5A^2x^2-4BAx-8B^2-A^3 = 0$ has six distinct roots. Hence, $E[4] \cong Z_4 \oplus Z_4$.*

Proof: By the computation through SageMath code based on [5], the discriminant $\Delta_{f(x)}$ of $f(x) = x^6+5Ax^4+20Bx^3-5A^2x^2-4BAx-8B^2-A^3 = 0$ is $(262144) \cdot (4A^3+27B^2)^5$. Since the elliptic curve $y^2 = x^3 + Ax + B$ is non-singular, $-4A^3 - 27B^2 \neq 0$. Hence, $\Delta_{f(x)}$ is not zero if $-4A^3 - 27B^2 \neq 0$, which proves $f(x)$ has six distinct roots. By the similar argument made in Section 3.1.1, $E[4] \cong Z_4 \oplus Z_4$. ■

Remark We find the equations that characterize x-coordinates of 2,3, and 4 torsion subgroups of elliptic curves over a field F. We can see that whether such equations have repeated roots is closely related to whether the elliptic curve is singular.

Example Let $E : y^2 = x^3 - 1$ over $\mathbb{R}$. Then, if $P \in E$ is a 4-torsion point, then by Theorem 3.1.7, $x^3 = 10 + 6\sqrt{3}$ or $x^3 = 10 - 6\sqrt{3}$. We can see that each of $x^3 = 10 + 6\sqrt{3}$ and

$x^3 = 10 - 6\sqrt{3}$ yields 6 4-torsion points and adding three 2-torsion points and the point at infinity O result in $E[4] \cong Z_4 \oplus Z_4$.

Here, we can infer a general outcome.

Theorem 3.1.8 ([11]). *Let F be a field such that $char(F) = 0$. Then, $E[n] \cong Z_n \oplus Z_n$.*

Here, following [15] and [8], we prove Theorem 3.1.8 for an elliptic curve defined over $\mathbb{Q}$. For this, we need the following definitions.

Definition 5. *([15]) Suppose z_1 and z_2 is linearly independent complex numbers over $\mathbb{R}$. Then, a set $L = \{a_1 z_1 + a_2 z_2 | a_1$ and $a_2 \in \mathbb{Z}\}$ is called a Lattice generated by z_1 and z_2.*

We use the notation $L = \langle z_1, z_2 \rangle$. The set L is a normal subgroup of $\mathbb{C}$ under the addition since it is a subgroup of an Abelian group, closed under the operation, and the inverse of an element exists in L.

Consider a quotient group $\mathbb{C}/L$. By definition, an element in the group is of the form $z + a_1 z_1 + a_2 z_2$ where $z \in \mathbb{C}$. We define an equivalent class in $\mathbb{C}$ with an entity called as a Fundamental Domain.

Definition 6. *([7]) Let L be a lattice generated by z_1 and z_2 ($L = \langle z_1, z_2 \rangle$). The region $D = \{\lambda z_1 + \mu z_2 | 0 \leq \lambda, \mu < 1\}$ is called as the Fundamental Domain of L.*

D is a parallelogram and each edge is equivalent to the opposite edge. An example of a Fundamental Domain is given below.

Here, we can use this equivalence relationship above $\mathbb{C}$ to define a meromorphic function called an elliptic function.

Definition 7. *([7]) An elliptic function (relative to a lattice $L \subset \mathbb{C}$) is a meromorphic function $f(z) : \mathbb{C} \to \mathbb{C}$ which satisfies $f(z + w) = f(z)$ for all $z \in \mathbb{C}$ and all $w \in L$. The set of all elliptic functions for L is denoted by $\mathbb{E}(L)$*

L is created with z_1 and z_2. Hence, f is a double periodic function. In other words, $f(z + z_1) = f(z) = f(z + z_2)$.

The most important example of an elliptic function is the Weierstrass $\wp$-function.

Definition 8 ([8]). *Let L be a lattice. The Weierstrass $\wp$-function relative to L is the function*

$$\wp(z, L) = \frac{1}{z^2} + \sum_{0 \neq w \in L} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

$\wp$ is a meromorphic function on $\mathbb{C} - L$. Also, it is known that it is a double-periodic function. This follows from the series expansion.

Theorem 3.1.9 ([8],[15]). *Suppose E be an elliptic curve over $\mathbb{Q}$. Define a map $\phi : \mathbb{C}/L \to E(\mathbb{C})$ such that*

$$\phi(u) = \begin{cases} (\wp(u, L), \wp'(u, L)) & \text{if } u \notin L \\ O & \text{if } u \in L \end{cases}$$

Then, there exists a lattice $L =< z_1, z_2 >$ such that ϕ is a group isomorphism.

Proof: Based on [15] and [14], we sketch a proof for showing ϕ is a group homomorphism such that $\phi(u + v) = \phi(u) +_E \phi(v)$ for all $u, v \in \mathbb{C}/L$ for some lattice L.

The proof starts from the theorem that Weierstrass $\wp(z)$ function satisfies $\wp'(z) = 4\wp(z)^3 + A\wp(z) + B$. By solving this differential equation, we can find L. From this, we know $\wp(z)$ function is described by an elliptic curve of the form $y^2 = 4x^3 + Ax + B$. For details, see [15]. Since the elliptic curves that we study is such that the coefficient of x^3 is one, we transform $y^2 = 4x^3 + Ax + B$ into an isomorphic curve $E_1 : y^2 = x^3 + A'x + B'$ using a map $(x, y) \to (x, \frac{y}{2})$. Then, it suffices to prove that there is an isomorphism (therefore homomorphism) between E_1 and $\mathbb{C}/L$ through a map $\phi^* : \mathbb{C}/L \to E_1$

To ease the notation, $u + L \in \mathbb{C}/L$ is denoted as u. We consider four cases, which are i) $u = v = 0$, ii) $u = 0$ and $v \neq 0$, iii) $u \neq 0$ and $v = 0$, and iv) $u \neq 0$ and $v \neq 0$. We find $\phi^*(u + v) = \phi^*(u) +_E \phi^*(v)$ holds for every case. For details, see [15].

We show ϕ^* is onto. Let $(x, y) \in E_1$. Since $\wp(z) - x$ has double poles from the definition, there exists $z \in \mathbb{C}/L$ such that $\wp(z) = x$ because of Fundamental Theorem of Algebra. For

detailed argument, see [14]. Also, [15] finds $(\frac{\wp'(z)}{2})^2 = y^2$. Hence,$\frac{\wp'(z)}{2} = y$ or $-y$. If $\frac{\wp'(z)}{2} = y$, we are done. Now suppose $\frac{\wp'(z)}{2} = -y$. From definition 8, we find $\wp(z) = \wp(-z)$. Then, $\wp'(z) = -\wp'(-z)$. From this, if $-y = \frac{\wp'(z)}{2}$, then $y = -\frac{\wp'(z)}{2} = \frac{-\wp'(z)}{2} = \frac{\wp'(-z)}{2}$.

Also, $ker(\phi^*) = L$ by definition. Hence, ϕ^* is isomorphism. ■

Now, we can prove Theorem 3.1.8 using Theorem 3.1.9.

Proof of Theorem 3.1.8 We follow [8]. By Theorem 3.1.9, there exists a lattice $L = \langle z_1, z_2 \rangle$ such that $\mathbb{C}/L \cong E(\mathbb{C})$. Define a map $f : Z_n \oplus Z_n \to E[n]$ such that $f(a_1, a_2) = \phi^*(\frac{a_1 z_1 + a_2 z_2}{n})$ where ϕ^* is a map defined in the proof of the Theorem 3.1.9. We note all possible n-torsion points are in $E(\mathbb{C})$ since $E[n] \hookrightarrow E(\bar{\mathbb{Q}}) \hookrightarrow E(\mathbb{C})$.

The map f is injective since ϕ is an isomorphism. Also, f is also surjective since there is a pre-image in $Z_n \oplus Z_n$ of each $Q \in E[n]$. Hence, f is an isomorphism. Since $w = \frac{a_1 z_1 + a_2 z_2}{n}$ for some $a_1 \in Z_n$ and $a_2 \in Z_n$, w is associated with $(a_1, a_2) \in Z_n \oplus Z_n$. This implies $E[n] \cong Z_n \oplus Z_n$. ■

For the case where $char(F) \neq 0$, we get similar results.

Theorem 3.1.10 ([11]). *Let n be a positive integer. If $gcd(n, char(F)) = 1$, then $E[n] \cong Z_n \oplus Z_n$. In addition, if $char(F) = q$ where q is a prime, then $E[q^\lambda] \cong \{O\}$ or $E[q^\lambda] \cong Z/q^\lambda Z$ where $\lambda \in \mathbb{N}$.*

Proof of the Theorem 3.1.10 uses fundamental Theorem of finitely generated Abelian groups For details, see [14] and [15].

Chapter4

Galois Representation on Elliptic Curves

4.1 Galois Representation on Elliptic Curves

The main points presented in the previous sections are summarized as follows. We demonstrated that points on an elliptic curve E defined over a field F form an Abelian group under an operation $+_E$. In addition, we defined the torsion subgroup of an elliptic curve $E(\bar{F})$. We pointed out cases where n-torsion subgroup is isomorphic to a cyclic group or a direct sum of two cyclic groups.

As in [2], a mathematically interesting question is what extension field K will be formed when n-torsion points are adjoined to the field F. We present the case when we adjoin a n-torsion subgroup to the base field of the elliptic curve. Then the resulting extension field is finite and algebraic. Based on this, we analyze the possible orders of the Galois group $Gal(K/F)$ through its relationship to a generalized linear group. Also, assuming an elliptic curve is defined over $\mathbb{Q}$, we find the degrees of polynomials that characterize x-coordinates of n-torsion subgroups. This provides an alternative approach to finding the possible orders of Galois group $Gal(K/\mathbb{Q})$.

Knowing possible values of the orders provides a similar insight to Serre's Theorem that says the representations of $Gal(K/F)$ are subgroups of generalized linear group, therefore the order of $Gal(K/F)$ divides the order of $GL_2(Z_n)$.

4.1.1 Galois Theory and Backgrounds

Galois theory provides a tool for examining the algebraic structure of an elliptic curve. This is because when the coordinates of n-torsion points on the elliptic curve are adjoined to the field where the curve is defined, an algebraic extension field is formed. To see this, we introduce the definition of a Galois extension of a field F.

Definition 9. *A field extension K of a field F is Galois (extension) if and only if the degree of extension $[K : F] = |Aut(K/F)|$ where $Aut(K/F)$ is the set of automorphisms on K that fix F.*

From Definition 9, we find an extension K of a field F is Galois if $|Aut(K/F)|$ attains its maximum, which is $[K : F]$.

Example Let $K = \mathbb{Q}(\sqrt[3]{2})$ be a field extension of $\mathbb{Q}$. $[K : \mathbb{Q}] = 3$ since $\sqrt[3]{2}$ is a root of an irreducible polynomial $x^3 - 2 = 0$ in $\mathbb{Q}$ with degree 3. $Aut(K/\mathbb{Q})$ is trivial since any automorphism f in $Aut(K/\mathbb{Q})$ must map 1 to 1 and $\sqrt[3]{2}$ to $\sqrt[3]{2}$, $\xi\sqrt[3]{2}$ or $\xi^2\sqrt[3]{2}$ where $\xi = \frac{-1+i\sqrt{3}}{2}$. However, $\xi\sqrt[3]{2}$ and $\xi^2\sqrt[3]{2}$ are not in K. Hence, $|Aut(K/\mathbb{Q})| = 1 \neq [K : \mathbb{Q}] = 3$. Hence, K is not a Galois extension of $\mathbb{Q}$.

Example Let $K = \mathbb{Q}(\sqrt{2})$ is a Galois extension of $\mathbb{Q}$ since $Aut(K/\mathbb{Q}) = \{id, \sigma\}$ where id denotes the identity map and $\sigma : 1 \to 1$ *and* $\sqrt{2} \to -\sqrt{2}$. Also, $[K : \mathbb{Q}] = 2$ since $\sqrt{2}$ is a root of an irreducible polynomial $x^2 - 2$. Hence, $|Aut(K/\mathbb{Q})| = [K : \mathbb{Q}] = 2$.

We find an extension field K of a field F is a Galois extension if the number of automorphisms on K that fix F is equal to the degree of extension $[K : F]$.

Theorem 4.1.1. *([2]) Let E be an elliptic curve over a field F.*
Also, let $E[n] = \{O, (x_1, y_1), (x_2, y_2), \cdots, (x_k, y_k)\}$. Then, $F(E[n]) = F(x_1, y_1, x_2, y_2, \cdots, x_k, y_k)$ is an algebraic extension of F.

Proof: Based on [2], we know each of $x_1, \ldots, x_k$ is a solution to a polynomial over F. This implies $x_1, \ldots, x_k$ are algebraic. Also, each y_j is determined by x_j where $j \in \{1, \ldots, k\}$. This indicates $y_1, \ldots, y_k$ are also algebraic. Hence, $F(E[n])$ is algebraic. ■

Remark In the Lemma 4.1.14, we will find that the x-coordinates of $E[n]$ is a root of polynomial over a field F, which demonstrates the extension $F(E[n])$ is an algebraic extension.

Based on [2], we will show that the above mentioned $F(E[n])$ is a Galois extension of a field F.

Lemma 4.1.2 ([2]). *Let $K = F(E[n])$ and define $\sigma : K \to \bar{K}$ be a field homomorphism that fixes F such that for all $P = (x, y) \in E(K)$*

$$\sigma(P) = \begin{cases} (\sigma(x), \sigma(y)) \; if \; (x, y) \neq O, \\ O, \; otherwise \end{cases} \tag{4.1}$$

Then, σ preserves the order of a point $P \in E(K)$, $\sigma(P) \in E(K)$, and $\sigma(P +_E Q) = \sigma(P) +_E \sigma(Q)$ for $P, Q \in E(K)$

Proof: We first show that if $P = (x_1, y_1) \in E(\bar{F})$, then $\sigma(P) \in E(\bar{F})$. $P = (x_1, y_1) \in E(\bar{F})$ implies the point satisfies the equation of the elliptic curve. Applying σ to the equation yields the same curve. In particular, it results in the evaluation of the curve at $\sigma(P)$. Therefore, the assertion is proved.

We use the definition of σ in (4.1). Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ with $x_1 \neq x_2$ on $E(K)$. From section 2.1.2, $P +_E Q = (m^2 - x_1 - x_2, -y_1 + m(2x_1 + x_2 - m^2)$ where $m = \frac{y_2 - y_1}{x_2 - x_1}$. Then, x-coordinate of $\sigma(P +_E Q))$ is $\sigma(m^2 - x_1 - x_2) = \sigma(m^2) - \sigma(x_1) - \sigma(x_2) = \sigma(m)^2 - \sigma(x_1) - \sigma(x_2) = x(\sigma(P) +_E \sigma(Q))$ where $\sigma(m) = \frac{\sigma(y(Q)) - \sigma(y(P))}{\sigma(x(Q)) - \sigma(x(P))}$.

The y-coordinate of $P +_E Q$ can be expressed in terms of x-coordinates. Hence, $\sigma(P +_E Q) = \sigma(P) +_E \sigma(Q)$.

Let $P = (x_1, y_1)$ and $Q = (x_1, y_2)$. That is, suppose P and Q have the same x-coordinate with the different y coordinates. Then, by Section 2.1.2, $P +_E Q = O$ where O is the point at infinity. $\sigma(P +_E Q) = \sigma(O) = O$. The last equality holds by the definition of σ. Also,

$\sigma(P) +_E \sigma(Q)$ is $(m^2 - \sigma(x_1) - \sigma(x_1), -y_1 + m(2\sigma(x_1) + \sigma(x_2) - m^2)$ where $m = \frac{\sigma(y_2)-\sigma(y_1)}{\sigma(x_1)-\sigma(x_1)}$, which is undefined. That is, $\sigma(P) +_E \sigma(Q)$ is the point at infinity O.

Hence, $\sigma(P) +_E \sigma(Q) = O$. Therefore, $\sigma(P +_E Q) = \sigma(P) +_E \sigma(Q)$ holds if the two points P and Q share the same x-coordinate with different y-coordinates.

Let $P = Q$. Then, $\sigma(P +_E Q) = \sigma(2P) = (\sigma(m^2) - 2\sigma(x), \sigma(m)(3\sigma(x_1) - \sigma(m^2) - \sigma(y))$ where $m = \frac{3\sigma(x^2)+A}{2\sigma(y)}$. We can check $\sigma(P) +_E \sigma(P) = \sigma(2P)$. Hence, the operation is preserved under σ when we double a point P. If $P = O$ or $Q = O$, we can easily find the statement of the Lemma holds. ■

K contains F and $E[n] = \{O, (x_1, y_1), (x_2, y_2), \cdots, (x_k, y_k)\}$. Then, if $P \in E(K)$, then $\sigma(P)$ is also in $E[n]$ since $n\sigma(P) = \sigma(nP) = \sigma(O) = O$. Hence, $\sigma(P) \in K^2$. That is, $\sigma(x_j)$ *and* $\sigma(y_j) \in K$ for all $j \in \{1, 2, \cdots, k\}$. Since P is an arbitrary point in K^2, $\sigma(K^2) \subset K^2$. Also, $\sigma(F^2) = F^2$. Hence, we find K=$F(E[n])$ using $[K : F] = |\{\sigma : K \to \bar{K} | \sigma|_F = Id_F\}| = |Aut(K/F)|$ is a Galois extension of F by definition.

Corollary 4.1.3. *([8]) K=F(E[n]) is a Galois extension over F.*

Remark We find the Corollary 4.1.3 holds from the following observation. From Lemma 4.1.14 later in this chapter, there exists a polynomial whose roots are exactly the x-coordinates of the points in $E[n]$. We find the splitting field of such a polynomial is Galois and adjoining the y-coordinates is just a set of quadratic extensions which are always Galois if $char(F) \neq 2$.

Now, assume $F = \mathbb{Q}$. Then, by Theorem 3.1.8, the set of n-torsion points of an elliptic curve E on F $E[n]$ is isomoprhic to $Z_n \oplus Z_n$. Since $Z_n \oplus Z_n$ is generated by two elements in it, for example, by $(1, 0)$ and $(0, 1)$, we can conclude there are two generators of $E[n]$. If $E[n] =< P_1, P_2 >$, the representation of the Galois group K over F can be made using a matrix notation.

Definition 10. *([8]) A representation of a group G on a vector space V over a field F is a group homomorphism from G to the general linear group on V, denoted* $\mathrm{GL}(V)$:

$$\rho : G \to \mathrm{GL}_d(V)$$

for some $d \geq 0$.

The definition below is that when F is a rational field, an arbitrary automorphism $\sigma \in Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ is represented in terms of P_1 and P_2 with $d = 2$ in Definition 10.

Definition 11 ([8])**.** *Let E be a rational elliptic curve and fix P_1 and P_2 as the generators of $E[n]$. Then for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$, the constants $\alpha_\sigma, \beta_\sigma, \gamma_\sigma, \delta_\sigma$ are determined by*

$$\sigma(P_1) = \alpha_\sigma P_1 + \gamma_\sigma P_2$$
$$\sigma(P_2) = \beta_\sigma P_1 + \delta_\sigma P_2$$

$\rho_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to \mathrm{GL}_2(Z_n)$ is represented as $\rho_n(\sigma) = \begin{bmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{bmatrix}$. Here, $Z_n \oplus Z_n$ is not a vector space but a Z_n-module since $Z_n \oplus Z_n$ is not a vector space. The map ρ_n *is the Galois representation of* $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

Theorem 4.1.4. *([8]) Let E be a non-singular rational elliptic curve and take $n \geq 2$. Fix P_1 and P_2 as generators for $E[n]$. Then the* map ρ_n *from Definition 11 is an injective homomorphism.*

Proof: We need to show $\rho_n(\tau\sigma) = \rho_n(\tau)\rho_n(\sigma)$. Let $\rho_n(\tau) = \begin{bmatrix} a_\tau & b_\tau \\ c_\tau & d_\tau \end{bmatrix}$ and $\rho_n(\sigma) = \begin{bmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{bmatrix}$.

Then, $\rho_n(\tau)\rho_n(\sigma) = \begin{bmatrix} a_\tau a_\sigma + b_\tau c_\sigma & a_\tau b_\sigma + b_\tau d_\sigma \\ c_\tau a_\sigma + d_\tau c_\sigma & c_\tau b_\sigma + d_\tau d_\sigma \end{bmatrix}$. On the other hand,

$\tau\sigma(P_1) = \tau(\sigma(P_1)) = \tau(a_\sigma P_1 + b_\sigma P_2) = a_\sigma \tau(P_1) + b_\sigma \tau(P_2) = a_\sigma(a_\tau P_1 + b_\tau P_2) + b_\sigma(c_\tau P_1 + d_\tau P_2) = (a_\sigma a_\tau + b_\sigma c_\tau)P_1 + (a_\sigma b_\tau + b_\sigma d_\tau)P_2$.

The same argument holds for $(\tau\sigma)(P_2) = (c_\tau a_\sigma + d_\tau c_\sigma)P_1 + (c_\tau b_\sigma + d_\tau d_\sigma)P_2$.

Hence, $\rho_n(\tau\sigma) = \rho_n(\tau)\rho_n(\sigma)$.

Now, we show ρ_n is a one-to-one map. Let $\sigma \in ker(\rho_n)$ and $E[n]$ be generated by the two points P_1 and P_2. Then, $\sigma(P_1) = P_1$ and $\sigma(P_2) = P_2$, which implies $\sigma(P) = P$ for all $P \in E[n]$. By the definition $\sigma(P) = (x(P), y(P))$, σ fixes the coordinates of a point in

$\mathbb{Q}(E[n])$ including the generators. Hence, σ must be the identity map and ρ_n is a one-to-one map. ■

Remark The condition about non-singularity in Theorem 4.1.4 is essential for defining $E[n]$.

This theorem shows that there is a one-to-one homomorphism between the Galois group $Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ and $GL_2(Z_n)$. Since ρ_n is a homomorphic map, the image of ρ_n is a subgroup of $GL_2(Z_n)$. A natural task here is to figure out the size of the image $\rho_n(\mathbb{Q}(E[n])/\mathbb{Q})$. Serre's Theorem provides an upper bound of the number of (left) cosets of $im(\rho_n)$ in $GL_2(Z_n)$.

Theorem 4.1.5 (Serre's Theorem,[2])**.** *Let E be an elliptic curve of the form $E(\mathbb{Q}) : y^2 = x^3 + Ax + B$, with coefficients in $\mathbb{Q}$. Then,*
$\exists N \geq 1$ depending on E, such that for all $n \geq 1$ with the property $\gcd(n, N) = 1$,

$$\rho_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \longrightarrow GL_2(Z/nZ)$$

is an isomorphism.

Serre's Theorem gives a condition where the size of $Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ and $GL_2(Z_n)$ is the same. We find an upper bound of $|Gal(\mathbb{Q}(E[n])/\mathbb{Q})|$ is $|GL_2(Z/nZ)|$.

4.1.2 Examples

Examples are given to demonstrate what has been described above.

Example 1 Let $E : y^2 = x^3 - 1$ over $F = \mathbb{Q}$. Then, $E[2] = \{(x, 0) \in E | x^3 - 1 = 0\} \cup \{O\} = \{O, (1, 0), (\frac{-1+\sqrt{3}i}{2}, 0), (\frac{-1-\sqrt{3}i}{2}, 0))\}$. Hence, $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-3})$. From these, we find the group of automorphisms that fix $\mathbb{Q}$ is $Gal(\mathbb{Q}(E[2])/\mathbb{Q} = \{id, \sigma\}$ where id is the identity map and σ is the complex conjugation. Note $P_1 = (1, 0)$ and $P_2 = (\xi, 0)$ where $\xi = \frac{-1+\sqrt{3}i}{2}$ are generators of $E[2]$. Then,

$$id(P_1) = P_1 \quad \sigma(P_1) = P_1 \tag{4.2}$$

$$id(P_2) = P_2 \quad \sigma(P_2) = P_3 = (\frac{-1-\sqrt{3}i}{2}, 0) = P_1 + P_2 \tag{4.3}$$

Remark This gives an example where $\sigma(P +_E Q) = \sigma(P) +_E \sigma(Q)$ for $P, Q \in E(K)$ holds in Lemma 4.1.2. Here, $P_1 +_E P_2 = (\frac{-1-i\sqrt{3}}{2}, 0)$. Then, $id(P_1 +_E P_2) = (id(\frac{-1-i\sqrt{3}}{2}), id(0)) = (\frac{-1-i\sqrt{3}}{2}, 0) = id(P_1) + id(P_2) = (id(\frac{-1+i\sqrt{3}}{2}, id(0)) +_E (id(1), id(0))$. Also, $\sigma(P_1 +_E P_2) = (\sigma(\frac{-1-i\sqrt{3}}{2}), \sigma(0)) = (\frac{-1+i\sqrt{3}}{2}, 0) = \sigma(P_1) + \sigma(P_2) = (\sigma(\frac{-1+i\sqrt{3}}{2}, \sigma(0)) +_E (\sigma(1), \sigma(0))$.

The isomorphism σ in the Galois group in the above remark can be represented by a 2 by 2 matrix. In fact, $\rho_2(\sigma)$ is given by

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

Hence, the image of ρ_2 in Theorem 4.1.5 has order 2 that divides $|GL_2(Z/2Z)| = 6$.

Example 2 [8] Let $E : y^2 = x^3 - p$ over $\mathbb{Q}$ where p is a prime number. $E[2] = O, (\beta, 0), (\beta\xi, 0), (\beta\xi^2, 0)$ where $\beta = p^{\frac{1}{3}}$ and ξ is the third root of unity. We find $\mathbb{Q}(\beta, \xi)$ is a splitting field of $x^3 - p$. We find there are six homomorphisms in $Gal(\mathbb{Q}(\beta, \xi)/\mathbb{Q}) = \{id, \sigma, \tau, \sigma^2\tau, \sigma^2, \sigma\tau\}$. We define

$$\sigma(\beta) = \xi\beta \quad \tau(\beta) = \beta \tag{4.4}$$

$$\sigma(\xi) = \xi \quad \tau(\xi) = \xi^2 \tag{4.5}$$

Also, $P_1 = (\beta, 0)$ and $P_2 = (\beta\xi, 0)$ can be regarded as two generators of $E[2]$. From these information, we find

$$\rho_2(\sigma) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \rho_2(\tau) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \rho_2(\sigma^2\tau) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \rho_2(\sigma\tau) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\rho_2(\sigma^2) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \rho_2(id) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Hence, we find the order of $Gal(\mathbb{Q}(E[2])/\mathbb{Q}$ is 6 that divides $GL_2(Z/2Z) = 6$.

However, representation in example 1 is not surjective. However, for $E : y^2 = x^3 - p$ where p is a prime, then, Galois representation ρ_2 is surjective.

Therefore, we can see that the map presented in Theorem 4.1.5 is not always surjective. Hence, we find the possible orders of a Galois representation by finding divisors of $|GL_2(Z_n)|$.

4.1.3 $Y^2 = X^3 + AX + B$ with Rational Coefficients

In this section, the above tasks are performed for the elliptic curve defined in the rational field whose characteristic is zero. First, we study 2-torsion points. Recall that a point P on an elliptic curve over $\mathbb{Q}$ is a 2-torsion point if and only if $P = -P$, which implies the y-coordinate of such a point is zero.

Theorem 4.1.6. *Let $y^2 = x^3 + Ax + B$ be a non-singular elliptic curve over $\mathbb{Q}$. Assume $f(x) = x^3 + Ax + B$ is irreducible over $\mathbb{Q}[x]$. Then, $|Gal(\mathbb{Q}(E[2]/\mathbb{Q})| = 3$ or 6.*

Proof: Assume $f(x)$ is irreducible over $\mathbb{Q}$. Depending on the value of the discriminant of $f(x)$, we know that $f(x)$ can have 3 real roots (not rational) or 1 real root (not rational) and 2 complex conjugate roots. If $\Delta = -4A^3 - 27B^2 > 0$, there are three non-rational distinct real roots. Suppose α is a root of $f(x)$. Then,$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ since $deg(f(x)) = 3$. Suppose now that $\Delta < 0$ and β satisfies $\beta^3 + A\beta + B = 0$. Then, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$. Since two roots of this equation are complex conjugates, $Gal(\mathbb{Q}(E[2])/\mathbb{Q})$ has an element of order 2. Therefore, 6 divides the order of $Gal(\mathbb{Q}(E[2])/\mathbb{Q})$ by Lagrange's theorem. Also, it is explicit to see $|Gal(\mathbb{Q}(E[2])/\mathbb{Q})| \leq 6$. Hence, we find $|Gal(\mathbb{Q}(E[2])/\mathbb{Q})| = 6$. Therefore, by the definition about a Galois extension, $|Gal(\mathbb{Q}(E[2]/\mathbb{Q})| = 3$ or 6. ■

Remark We do not need to consider the case where $\Delta = 0$ since the curve is non-singular.

Example Let $E : y^2 = x^3 - 2$ over $\mathbb{Q}$. By Eisenstein's criteria, $x^3 - 2$ is not reducible over $\mathbb{Q}$. However, $\mathbb{Q}(2^{\frac{1}{3}}, i)$ is an algebraic extension of $\mathbb{Q}$ such that it has all of the roots of $x^3 - 2$. $[\mathbb{Q}(2^{\frac{1}{3}}, i) : \mathbb{Q}] = 6$ and $|Gal(\mathbb{Q}(E[2]/\mathbb{Q})| = 6$ since $\mathbb{Q}(E[2])/\mathbb{Q}$ is a Galois extension.

Theorem 4.1.7. *Let $y^2 = x^3 + Ax + B = f(x)$ be an elliptic curve over $\mathbb{Q}$. Assume $f(x) = x^3 + Ax + B$ is reducible over $\mathbb{Q}[x]$. Then, $|Gal(\mathbb{Q}(E[2]/\mathbb{Q})| = 1$ or 2.*

Proof: If $f(x)$ is reducible over $\mathbb{Q}[x]$, then one of the possibilities is having one rational root and two complex conjugate roots. Then, a splitting field will be $E = Q(\sqrt{-d})$ with $d > 0$. Then, by the similar argument as in Theorem 4.1.6, $|Gal(\mathbb{Q}(E[2]/\mathbb{Q})| = 2$. If the roots of $f(x)$ are all rational numbers, then we find $|Gal(\mathbb{Q}(E[2]/\mathbb{Q})| = 1$. Furthermore, if $f(x)$ has one rational root q and two real roots in $\mathbb{R} - \mathbb{Q}$, then $[Q(\alpha) : Q] = 2$ where $\alpha = \sqrt{d}$ with $d > 0$ is a non-rational root of $f(x)$. This is because $f(x) = (x - q)g(x)$ with $g(\alpha) = 0$ and $deg(g(x)) = 2$. Hence, $|Gal(\mathbb{Q}(E[2]/\mathbb{Q})| = 2$ in this case. ■

Here, the discussion is naturally extended to the Galois group formed by n-torsion points where $n > 2$. These points are often difficult to calculate through group law[8]. It is necessary to consider the order of $GL_2(V)$, which is the maximal range of ρ map in definition 10.

Theorem 4.1.8. *Let q be a prime. $|Gal(\mathbb{Q}(E[q])/\mathbb{Q})|$ divides $|GL_2(Z_q)| = (q^2 - 1)(q^2 - q)$.*

Proof: By Theorem 4.1.4, we know a map $\rho_n \colon Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \to GL_2(Z_n)$ is an injective homomorphism (or an embedding) and we have seen the examples where the map is not surjective in general. Hence, $im(\rho_n)$ is a subgroup of $GL_2(Z_n)$ and $|im(\rho_n)|$ divides $|GL_2(Z_n)|$. Hence, the Theorem follows. ■

Example In example 1 in section 4.1.2, I_2 and

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

represent the group of automorphisms on $\mathbb{Q}(E[2])/\mathbb{Q}$ that fixes $\mathbb{Q}$. Since $|GL_2(Z_2)| = 6$ and $|im(\rho_2)| = 2$ divides 6.

We can extend Theorem 4.1.6 and 4.1.7 to $|Gal(\mathbb{Q}(E[n])/\mathbb{Q})|$ where $n \in Z^+$ which is not a necessarily prime number.

Lemma 4.1.9. *Let $n = mq$ where $gcd(m, q) = 1$. Then, $GL_2(Z_n) \cong GL_2(Z_m) \oplus GL_2(Z_q)$.*

Proof: Let $n = mq$ where $gcd(m, q) = 1$. Then, $Z_n \cong Z_m \oplus Z_q$ by the basic group theory. This implies $Z_n \oplus Z_n \cong (Z_m \oplus Z_q) \oplus (Z_m \oplus Z_q) \cong (Z_m \oplus Z_m) \oplus (Z_q \oplus Z_q)$. The first congruence relationship holds due to $gcd(m, q) = 1$. Therefore, $GL(2, Z_n) = Aut(Z_m \oplus Z_m) \oplus Aut(Z_q \oplus Z_q) = GL(2, Z_m) \oplus GL(2, Z_q)$. ■

Once we know what is the cardinality of any $GL(2, Z_{p^k})$ for prime p's, then the cardinality of $GL(2, n)$ is the product of the $|GL(2, Z_{p^k})|$ where k is the maximum power of the prime p in n.

Lemma 4.1.10. *[17] $|GL(2, Z_{p^k})| = (p^2 - 1)(p^2 - p) * p^{4k-4}$ where $k \in Z^+$ and p is a prime.*

Proof: We follow [17]. Z_{p^k} where $k > 1$ is a local ring and by definition it has the unique maximal ideal of the form (m). Hence, $Z_{p^k}/(m)$ is a field and it is equal to Z_p. Consider a canonical map $\phi : GL_2(Z_{p^k}) \to GL_2(Z_p)$. We find $ker(\phi) = I_2 + A$ where $A \in M_2(m)$ and ϕ is surjective since the map $\psi : Z_{p^k} \to Z_p$ is surjective. Hence, $|GL_2(Z_{p^k})| = |GL_2(Z_p)||M_2(m)|$. The first term of this multiplication is $(p^2-p)(p^2-1)$ by Theorem 4.1.8. Also, $|M_2(m)| = p^{4k-4}$ since $m = Z_{p^{k-1}}$ and each entry in $M_2(m)$ can take a value in $\{0, 1, \cdots, p^{k-1}\}$. ■

By the Lemmas 4.1.9 and 4.1.10, we can prove the following theorem.

Theorem 4.1.11. *Let $n > 2$ be an integer and suppose $n = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ where p_is are distinct primes. Then, $|Gal(\mathbb{Q}(E[n])/\mathbb{Q})|$ divides $\prod_{i=1}^{n}(p_i^2 - 1)(p_i^2 - p_i) * p_i^{4k_i-4}$.*

Proof: Note that $Z_n = \oplus_{i=1}^{n} Z_{p_i^{k_i}}$ Hence, $GL(2, Z_n) = Aut(\oplus_{i=1}^{n}(Z_{p_i^{k_i}} \oplus Z_{p_i^{k_i}}) \cong \oplus_{i=1}^{n} Aut(Z_{p_i^{k_i}} \oplus Z_{p_i^{k_i}}) \cong \sum_{i=1}^{n} GL(2, Z_{p_i^{k_i}})$. By Lemma 4.1.10, $|Gal(\mathbb{Q}(E[n])/\mathbb{Q})|$ divides $\prod_{i=1}^{n}(p_i^2 - 1)(p_i^2 - p_i) * p_i^{4k_i-4}$ ■

Remark Since $gcd(p_i^{k_i}, p_j^{k_j}) = 1$ if p_i and p_j is distinct primes, we can apply Lemma 4.1.9 in the proof of Theorem 4.1.11.

4.1.4 $Y^2 = X^3 + AX + B$ with Coefficients over a Finite Field

The elliptic curve group on a finite field F_q has several important differences from the elliptic curve group defined on the continuous field. An elliptic curve on F_q consists of a finite number of elements, which is a desirable property for cryptography applications.

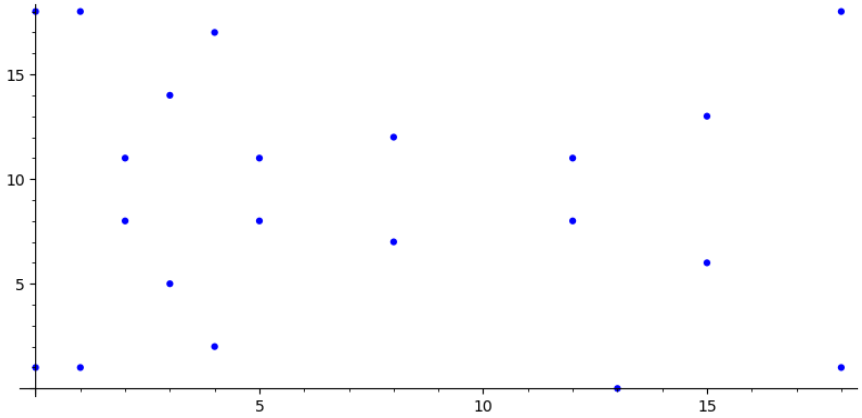
Example Let $E(F_4) : y^2 = x^3 + 1$ where $F_4 = \{0, 1, \omega, \omega^2\}$ and ω satisfies $\omega^2 + \omega + 1 = 0$.

- If $x = 0$, then $y = 1$. We get $(0, 1)$.
- If $x = 1$, then $y^2 = 1 + 1 = 0$ since $char(F_4) = 2$. We get $(1, 0)$.
- If $x = \omega$, then $y^2 = \omega^3 + 1 = \omega^2\omega + 1 = -\omega^2 - \omega + 1 = 1 + 1 = 0$. We get $(\omega, 0)$.
- If $x = \omega^2$, then $y^2 = \omega^6 + 1 = (\omega^3)^2 + 1 = 0$ since $w^3 = 1$. We get $(\omega^2, 0)$

Hence, we get 5 points including the point at infinity O.

Example Let $E(F_{19}) : y^2 = x^3 - x + 1$. Then, O,(0,1),(0,18),(1,1),(1,18),(2,8),(2,11), (3,5),(3,14),(4,2) (4,17) (5,8) (5,11) (8,7) (8,12) (12,8) (12,11) (13,0) (15,6) (15,13) (18,1) and (18,18) are the 22 points of $E(F_{19})$. These points are illustrated as below based on SageMath codes in [9] and [4].

Figure 4.1: $E(F_{19}) : y^2 = x^3 - x + 1$



The question to be studied here is under which conditions the points of an elliptic curve over a field form a group.

If an elliptic curve over F_q is non-singular, then the group law in Section 2.1.4 is applied to perform the operation $+_E$. One can refer to Chapter 2 for the definitions of the $+_E$ in a field of the characteristic of zero, 2, 3, and greater than 3.

It is possible to better understand the algebraic structure of $E[n]$ through its Galois group.

Lemma 4.1.12. *Let $q = p^k$ where $p \geq 5$ is a prime and $y^2 = x^3 + Ax + B$ be a non-singular elliptic curve over F_q. Then,*

$$|Gal(F_q(E[2])/F_q)| = 1, 2, 3 \, or \, 6 \tag{4.6}$$

Proof: By definition $E[2] = \{(x, 0)|y^2 = x^3 + Ax + B\}$. Because of non-singularity of $y^2 = x^3 + Ax + B$, we find there are three distinct roots to $f(x) = x^3 + Ax + B = 0$. Suppose $x^3 + Ax + B$ is irreducible over F_q and r_1 is a root of the equation $x^3 + Ax + B$=0. Then, $[F_q(r_1) : F_q] = 3$. If r_2 is another root, then it is a root of a degree at most 2 polynomial. Since r_1 is a root of $x^3+Ax+B = 0$, we can find $f(x) = (x-r_1)h(x)$ over $F_q(r_1)$. If $h(x)$ is irreducible over $F_q(r_1)$, then $[F_q(r_1, r_2) : F_q] = 6$ since $deg(h(x)) = 2$ implies $[F_q(r_1, r_2) : F_q(r_1)] = 2$. Otherwise, $[F_q(r_1, r_2) : F_q] = 3$ since $[F_q(r_1, r_2) : F_q(r_1)] = 1$. Hence, $|Gal(F_q(E[2])/F_q)| = 3$ or 6.

If $x^3 + Ax + B$ is reducible over F_q, then at least one of the roots of the equation is in F_q. We denote it as s_1. Then, $[F_q(s_1) : F_q] = 1$. If s_2 is another root, then $[F_q(s_1, s_2) : F_q(s_1)]$ is 1 or 2 since s_2 is a root of a degree 2 polynomial. Using the same argument above, we find $[F_q(E[2]) : F_q] = 1$ *or* 2. Since $F_q(E[2])$ is a finite normal extension of F_q, we find $|Gal(F_q(E[2])/F_q)| = 1, 2, 3$ *or* 6. ■

Example We study an example about Lemma 4.1.12 when F_2 is the field where an elliptic curve is defined. By Theorem 2.1.1, there are six possible characterizations about x-coordinates of 2-torsion subgroups of an elliptic curve over characteristic 2.

$$0 = x^3 \tag{4.7}$$

$$0 = x^3 + 1 \tag{4.8}$$

$$0 = x^3 + x \tag{4.9}$$

$$0 = x^3 + x + 1 \tag{4.10}$$

$$0 = x^3 + x^2 \tag{4.11}$$

$$0 = x^3 + x^2 + 1 \tag{4.12}$$

We focus on non-singular curves, which are (4.8),(4.9),(4.10), and (4.12). For $E[2]$ on (4.10) and (4.12), there are no roots in F_2. However, a direct calculation through SageMath code based on [16] finds that $Gal(F_2(E[2])/F_2) = 6$. We can see this from a direct computation with SageMath code based on [1] because a splitting field of (4.10) and (4.12) is $F_2(i, r)$ where $r = k^{\frac{1}{3}}$ where k is not a cubic number. For (4.8) and (4.9), they have one root in F_2 and the other two roots are in $\bar{F_2} - F_2$. Hence, $Gal(F_2(E[2])/F_2) = 2$.

For higher torsion subgroups of elliptic curves over F_q, there is an analogous result as Theorem 4.1.11.

Theorem 4.1.13. *Let $n > 2$ be an integer and suppose $n = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ where p_is are distinct primes. Then, $|Gal(F_q(E[n])/F_q)|$ divides $\prod_{i=1}^{n}(p_i^2 - 1)(p_i^2 - p_i) * p_i^{4k_i - 4}$.*

So far, for a given elliptic curve over a field F, we studied the possible values of the order of a Galois representation presented in Serre's Theorem. We investigated the possible values of $|Gal(F(E[n])/F|$ in Definition 10 by paying attention to the fact that the order $|Gal(F(E[n])/F|$ must divide $|GL_2(Z_n)|$. In this section, focusing on the fact that we can express the x-coordinates of the n-torsion subgroup of an elliptic curve over a field through a polynomial, we find out the possible values $|Gal(F(E[n])/F|$. We deal with this aspect in the next section.

4.1.5 Alternative Methods

Lemma 4.1.14. *([15]) Let $E(\mathbb{Q}) : y^2 = x^3 + Ax + B$ be a non-singular elliptic curve over $\mathbb{Q}$. Then, for $n > 2$, there exists a polynomial $f_n(x)$ such that $E[n] = \{(x, y) | f_n(x) = 0$ and $y = \pm\sqrt{x^3 + Ax + B}$ and $n(x, y) = O\} \cup \{O\}$ has degree less than or equal to $\frac{n^2-1}{2}$ if n is an odd number and less than or equal $\frac{n^2}{2} + 1$ if n is an even number.*

Proof: We follow [14] to prove this theorem. By definition about a n-torsion point, a point $P \in E[n]$ if and only if $nP = O$. Also, we find an endomorphism $\alpha_n : E(\bar{\mathbb{Q}}) \to E(\bar{\mathbb{Q}})$ defined by $P \to nP$ is given by $\alpha_n(x, y) = n(x, y) = (\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)})$ where $\phi_n \in Z[x, y^2, A, B]$. Also, $\psi_n \in Z[x, y^2, A, B]$ if n is an odd number and $\psi_n \in 2yZ[x, y^2, A, B]$ if n is an even number, and $\omega_n \in Z[x, y^2, A, B]$. [15] presents the detailed derivations of the endomorphism. [14] finds this endomorphism is separable and hence the size of $ker(\alpha_n)$ is equal to the degree of α_n where the degree of α_n is defined by $max\{deg(\phi_n), deg(\psi_n^2)\}$. We find $ker(\alpha_n) = E[n]$ and if $(x, y) \in ker(\alpha_n)$, then $\psi_n^2(x) = 0$ by the definition about a n-torsion point. We claim $\psi_n^2(x) = 0$ must have $n^2 - 1$ distinct roots. This is because $deg(\alpha_n) = max\{deg(\phi_n), deg(\psi_n^2)\} = n^2 = |ker(\alpha_n)|$ due to the fact that α_n is separable and $deg(\psi_n^2) = n^2 - 1$ based on [14]. Here, the point at infinity $O \in ker(\alpha_n)$ is obviously not a root of $\psi_n^2(x)$ because it does not have a coordinate.

We now consider the degree of $f_n(x)$ in the statement of this Lemma. Suppose n is an even number. Then, $E[n]$ includes the subgroup $E[2]$ which is of the from $(x, 0)$ together with the identity O that does not have a coordinate. Also, the elliptic curve $E(\mathbb{Q})$ is symmetric about x-axis. Hence, $deg(f_n(x)) = \frac{n^2-4}{2} + 3 = \frac{n^2}{2} + 1$. If n is an odd number, then there are no points in $E[n]$ whose y-coordinate is zero, $deg(f_n(x)) = \frac{n^2-1}{2}$ using the similar argument above. ■

The next theorem is an immediate result of Lemma 4.1.14.

Theorem 4.1.15. *Suppose $E(\mathbb{Q}) : y^2 = x^3 + Ax + B$ be a non-singular elliptic curve over $\mathbb{Q}$ with characteristic 0. Then, for $n > 2$, $|Gal(\mathbb{Q}(E[n])/\mathbb{Q})|$ divides $2^k(\frac{n^2-1}{2})!$ if n is an odd*

number for some $k \geq 0$ *and* $2^k(\frac{n^2}{2}+1)!$ *if* n *is an even number for some* $k \geq 0$.

Remark We need the factor 2^k for some $k \geq 0$ in the numbers that is divisible by $|Gal(\mathbb{Q}(E[n])/\mathbb{Q})|$ in the Theorem 4.1.15. This is because we need to find the y-coordinate once we find x-coordinate of a n-torsion point and square root of each $x^3 + Ax + B$ may be in a different extension.

From Theorem 4.1.5, we know $im(\rho)$ is a subgroup of $GL_2(Z_n)$ and hence, $|im(\rho)|$ divides $|GL_2(Z_n)|$. This led to the calculation of possible values that $|Gal(F(E[n]))]/F|$ can take. However, when n is a large number, it is difficult to pinpoint the exact value of $|Gal(F(E[n]))]/F|$.

Rather, for various elliptic curves over $\mathbb{Q}$, we consider a measure such that the overall surjectivity of the Galois expressions ρ_n can be expected and compared across elliptic curves. It requires the following proposition.

Proposition 4.1.16. *([3]) There is a map* $r(E) : G \to GL_2(\hat{Z})$ *where* E *is an elliptic curve over* $\mathbb{Q}$, $G = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ *and* $\hat{Z}$ *is the profinite completion of integer.*

Proof: We know $\mathbb{Q}(E[n]) \subset \bar{\mathbb{Q}}$ and $Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ acts on the generators of $E[n]$, say P_1 and P_2. This can be extended to the absolute Galois group $G = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. It is clear that $Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \subset G$. Conversely, let $g \in G$. Then, if $g \in Gal(\mathbb{Q}(E[n])/\mathbb{Q})$, then g permutes the generators P_1 and P_2. If $g \in Gal(\mathbb{Q}(E[m])/\mathbb{Q}$ with $gcd(n, m) = 1$, then g acts on $\mathbb{Q}(E[n])$ as an identity map.

To define $r(E)$ from this observation, we also need to see how the representations patch together. We observe that if $n = p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}$ where p_is are distinct primes and $k_i \geq 1$ for all $i \in \{k_1, \ldots, k_n\}$, $E[n]$ is the product of $E[p_i^{k_i}]$ and $GL_2(Z_n)$ is also the product of $GL_2(Z_{p_i}^{k_i})$. Hence, it suffices to consider a map from $E[p_i^{k_i}]$ into $GL_2(Z_{p_i})$ where Z_{p_i} is the ring of p_i-adic integers to patch the p_i-power torsions together.

Since $E[p_i^{k_i}]$ is a subset of $E[p_i^{k_i+1}]$, the image in $GL_2(Z_{p_i^{k_i}})$ of the action of Galois on $E[p_i^{k_i}]$ can be connected to the image in $GL_2(Z_{p_i^{k_i+1}})$ based on the action on $E[p_i^{k_i+1}]$. Hence,

maps from G to $GL_2(Z_{p_i^{k_i}})$ are patched as $k_i \to \infty$. Hence, $r(E)$ in the theorem is defined across p_i for $i \in \{k_1, \ldots, k_n\}$. ■

We consider an index $[GL_2(\hat{Z}) : im(r(E))]$ where $im(r(E))$ is the image of $r(E)$. We find from the definition of an index that as $[GL_2(\hat{Z}) : im(r(E))]$ increases (decreases), then more of ρ_n's are not surjective (surjective, respectively). There is a special type of elliptic curves called a "Serre's Curve".

Definition 12 ([3]). *An elliptic curve $E(F)$ is called a Serre's curve if* $[\mathrm{GL}_2(\hat{Z}) : im(r(E))] = 2$.

Jones points out in [6] that almost every elliptic curve is Serre's curve.

Remark $[\mathrm{GL}_2(\hat{Z}) : im(r(E))]$ indicates the expectation that we have a surjective map $r(E)$. In particular, if $[\mathrm{GL}_2(\hat{Z}) : im(r(E))] = 2$, we find the chance that we will have a surjective map ρ_n for a randomly chosen $n \in \{1, 2, \ldots\}$ is greater compared to the case where $[\mathrm{GL}_2(\hat{Z}) : im(r(E))] > 2$.

Chapter5

Conclusion

We focused on the algebraic structure of an elliptic curve defined on a field throughout this paper. The significance of this study is an attempt to find possible values of the order of the Galois representations based on the fact that the Galois representation of $n-$torsion subgroup is injective into a generalized linear group.

However, this approach has limitations in its application to higher torsion subgroups. This is because the size of the generalized linear group in Serre's theorem grows as n increases and the degree of the polynomial that characterizes the x-coordinate of n torsion subgroup explodes. Therefore, it is necessary to pay attention to the surjectivity across $n \in \mathbb{N}$ of the Galois representation. When an elliptic curve is a Serre's Curve, relatively more surjectivity is established than other types of elliptic curves.

Subsequent studies will focus on finding other methods for measuring the surjectiveness of Galois representation $r(E)$. The index $[\mathrm{GL}_2(\hat{Z}) : im(r(E))]$ itself is not a measure of the surjectiveness of a given Galois representation. Rather, the larger the index is, the smaller expectation that we will have a surjective representation. The next research task will be to think of an alternative index that overcomes this limitation and to find variables that determine the expectation for the surjectivity.

Bibliography

[1] *Basic Algebra and Calculus*. URL: https://doc.sagemath.org/html/en/tutorial/tour_algebra.html (visited on 05/10/2022).

[2] AJ Bull. *Galois Representations and Elliptic Curves*. Dec. 14, 2018. URL: http://www.math.utah.edu/~moss/AJ_Bull_Galois_Representations_and_Elliptic_Curves.pdf (visited on 10/01/2021).

[3] Harris B Daniels. "An infinite family of Serre curves". *Journal of Number Theory* 155 (2015), pp. 226–247.

[4] *Elliptic curves over a general field*. URL: https://doc.sagemath.org/html/en/reference/arithmetic_curves/sage/schemes/elliptic_curves/ell_field.html (visited on 05/22/2022).

[5] *How to use sage to solve the discriminant of polynomial*. Mar. 30, 2021. URL: https://dev.to/maxwizard01/how-to-use-sage-to-solve-the-determinant-of-polynomia-13no (visited on 11/01/2021).

[6] Nathan Jones. "Almost all elliptic curves are Serre curves". *Transactions of the American Mathematical Society* 362.3 (2010), pp. 1547–1570.

[7] Alvaro Lozano-Robledo. *Elliptic curves, modular forms, and their L-functions*. American Mathematical Society Providence, RI, 2011. 186 pp.

[8] Tarika Mane. *Galois Actions on Torsions of Elliptic Curves*. Aug. 25, 2020. URL: http://math.uchicago.edu/~may/REU2020/REUPapers/Mane.pdf (visited on 09/01/2021).

[9] *Sage Math Tutorial - Plotting*. URL: http://sage.brandoncurtis.com/plotting.html (visited on 05/21/2022).

[10] Andrew Shallue and Christiaan E van de Woestijne. "Construction of rational points on elliptic curves over finite fields". *International Algorithmic Number Theory Symposium*. Springer. 2006, pp. 510–524.

[11] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009. 400 pp.

[12] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*. Vol. 9. Springer, 1992. 281 pp.

[13] Nigel P Smart and Edward John Westwood. "Point multiplication on ordinary elliptic curves over fields of characteristic three". *Applicable Algebra in Engineering, Communication and Computing* 13.6 (2003), pp. 485–497.

[14] Lawrence C Washington. *Elliptic curves: Number theory and Cryptography*. CRC press, 2008. 524 pp.

[15] Samuel L. Wenberg. "Elliptic curves and their cryptographic applications". Eastern Washington University, 2013. 139 pp. URL: http://dc.ewu.edu/theses/160?utm_source=dc.ewu.edu%2Ftheses%2F160&utm_medium=PDF&utm_campaign=PDFCoverPages.

[16] William Stein and David Loeffler. *Galois Groups of Number Fields*. URL: https://doc.sagemath.org/html/en/reference/number_fields/sage/rings/number_field/galois_group.html (visited on 05/10/2022).

[17] Qiaochu Yuan. *Order of GL(2,Z_4)*. URL: https://math.stackexchange.com/questions/3357934/order-of-gl2-mathbbz-4 (visited on 10/06/2021).