University of Groningen
Faculty of Science and Engineering
Mathematics

Bachelor Project

# Torsion subgroups of elliptic curves over algebraic field extensions of $\mathbb{Q}$

*Manoy Trip*
*S2754738*
*m.t.trip@student.rug.nl*

1st supervisor
dr. M. Derickx

2nd supervisor
prof. dr. J. Top

July 2018

Abstract

In this thesis, an overview of research in the field of torsion subgroups of elliptic curves over algebraic field extensions of $\mathbb{Q}$ is provided. This field of research is currently very active. In 2018, a result was published by Daniels et al. showing that the torsion subgroup of an elliptic curve is finite, when the underlying field is a Galois extension of $\mathbb{Q}$ and contains only finitely many roots of unity. The proof of this result is discussed in this report. Furthermore, the compositum of all prime degree extensions is treated. For this field extension, a sufficient criterion is provided for which the prime torsion of an elliptic curve over this field is trivial.

# Contents

# 1 Introduction

The main topic of this thesis is the torsion subgroups of elliptic curves over algebraic field extensions of $\mathbb{Q}$. In the past years, many new results in this topic have been uncovered, and there is continued interest in this field of study.

Around the start of the 20th century, it was found that an elliptic curve over a number field forms a finitely generated abelian group. This group has a finite torsion group. A lot of research has since been dedicated to finding a classification of the torsion subgroups of such elliptic curves. The question was expanded to elliptic curves over infinite extensions of $\mathbb{Q}$, and results have been obtained for example for the composita of all degree 2 and all degree 3 extensions of $\mathbb{Q}$.

This report first of all aims to give a historical overview of what has been done in this area of research, while introducing all relevant concepts that are necessary to properly understand the results. Special attention is payed to one very recent result, published by Daniels, Lozano-Robledo, Najman and Sutherland [1]. We will look at a proof that was provided in this article and fill in details, aiming to make it more understandable for people who are less familiar with the field.

We will continue to provide a general approach that can be applied in the search for the torsion subgroup of an elliptic curve over a certain field. We will provide a few results that can be applied very generally, and may be helpful in classifying torsion subgroups in new cases.

Finally, we will show an application of this general approach. The field that we will consider is the compositum of all extensions of $\mathbb{Q}$ that have prime degree. We will give a sufficient criterion for the prime torsion of an elliptic curve over this field to be trivial.

# 2 Preliminaries

## 2.1 Field extensions

In this section, some basic definitions in the area of field theory will be summarized. These will first be stated, and then be made explicit by means of an example. A more elaborate treatment of this topic can be found in section 21 of [24].

We will start with the notion of a field extension, which we will need throughout this research. A **field extension** is a pair of two fields, of which the first is a subfield of the second. Important and well-known examples of field extensions are $\mathbb{Q} \subseteq \mathbb{R}$ and $\mathbb{Q} \subseteq \mathbb{C}$.

The smallest subfield of a field is called its **prime field**. This prime field can be characterized by a notion we call the **characteristic** of a field $K$. If the prime field is finite, it is isomorphic to a finite field of prime order $p$. In this case the field $K$ is said to have characteristic $p$, and we write $char(K) = p$. On the other hand, if the prime field is infinite, it can only be isomorphic to $\mathbb{Q}$. $K$ is then said to have characteristic zero, or $char(K) = 0$. In this last case, we can talk about the field extension $\mathbb{Q} \subseteq K$. In this research we will only consider fields with characteristic zero.

If we have a field extension $\mathbb{Q} \subseteq K$, we can consider $K$ as a vector space over $\mathbb{Q}$. This is used define the concept of the degree of a field extension.

**Definition 2.1** *The **degree** of a field extension $\mathbb{Q} \subseteq K$ is defined as the dimension of $K$ viewed as a $\mathbb{Q}$-vector space. The degree is denoted by $[K : \mathbb{Q}]$.*

We will only be interested in particular field extensions, which are called algebraic. To understand what is meant by this, we first need to define the notion of an algebraic element of a field extension $K \subseteq L$.

**Definition 2.2** *Let $K \subseteq L$ be a field extension. An element $\alpha \in L$ is called **algebraic over** $K$ if there exists a nonzero polynomial with coefficients in $K$, of which $\alpha$ is a zero.*
*The extension $K \subseteq L$ itself is called an **algebraic extension** if every element of $L$ is algebraic over $K$.*

If an extension $\mathbb{Q} \subseteq K$ is such that the degree $[K : \mathbb{Q}]$ is finite, the extension is automatically algebraic [8, p. 2-3]. In this case, the field $K$ is called a **number field**.

As an example, consider the field $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. $\mathbb{Q}$ is a subfield of this field, so we can consider the field extension $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$. It follows that $\mathbb{Q}[\sqrt{2}]$ has characteristic zero.
To determine the degree of this extension, we consider $\mathbb{Q}[\sqrt{2}]$ as a vector space over $\mathbb{Q}$. The pair $\{1, \sqrt{2}\}$ serves as a basis, so this vector space has dimension 2. We can conclude that the degree $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.
It can also be shown that the extension is algebraic. For example, the element $\sqrt{2}$ is a zero of the polynomial $X^2 - 2$, which has coefficients in $\mathbb{Q}$. Hence $\sqrt{2}$ is an algebraic element. In a similar way, for each element of the form $a + b\sqrt{2}$ it is possible to construct a polynomial with coefficients in $\mathbb{Q}$ of which it is a zero: the polynomial $x^2 - 2ax + a^2 - 2b^2 =$

$(x-(a+b\sqrt{2}))(x-(a-b\sqrt{2}))$ serves this purpose. The extension is therefore algebraic, and its degree is finite. It follows that $\mathbb{Q}[\sqrt{2}]$ is a number field.

Another useful notion is that of an algebraic closure. First of all, a field $K$ is called **algebraically closed** if all algebraic extensions of $K$ are trivial, i.e. if for any algebraic extension $K \subseteq L$ it follows that $K = L$. Intuitively this means that all elements that are algebraic over $K$ are already in $K$, and hence a nontrivial extension must contain elements that are not algebraic over $K$.

**Definition 2.3** *An **algebraic closure** of a field $K$ is an extension field $\overline{K}$ of $K$ such that*

- *$K \subseteq \overline{K}$ is algebraic,*
- *$\overline{K}$ is algebraically closed.*

For every field an algebraic closure exists, and it is unique up to isomorphism. This means that if we find two distinct fields satisfying the definition of an algebraic closure of $K$, these two fields are isomorphic.
$\overline{\mathbb{Q}}$ denotes an algebraic closure of $\mathbb{Q}$. In this text, we fix $\overline{\mathbb{Q}}$ to be the algebraic closure of $\mathbb{Q}$ that is contained in the field of complex numbers $\mathbb{C}$. All extensions of $\mathbb{Q}$ we will encounter in the sections to follow are considered as subfields of this algebraic closure. For such fields $K \subseteq \overline{\mathbb{Q}}$, we have $\overline{K} = \overline{\mathbb{Q}}$.

## 2.2 Elliptic curves

Now that we have introduced some general notions in field theory, we can use these to understand the main structure that is important in this research, namely that of an elliptic curve. The theory in this section is mainly based on [25].

Elliptic curves can be defined as the solution set of a degree three polynomial equation in the variables $x$ and $y$. The general form of this equation is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4$ and $a_6$ are constant elements in some field. This equation is called the **generalized Weierstrass equation**.

If the characteristic of the field is not equal to 2 or 3, an invertible coordinate transformation can be performed to obtain an equation of a simpler form. If we perform the substitutions $y \mapsto y - \frac{a_1x}{2} - a_3/2$ and $x \mapsto x - \frac{1}{3}(a_2 + \frac{a_1^2}{4})$, we obtain an equation of the following form:

$$y^2 = x^3 + Ax + B \tag{1}$$

where $x$ and $y$ are again variables, and $A$ and $B$ are constant elements in the field. We call this equation the **Weierstrass equation**. Because our research is concerned with fields of characteristic zero, we can focus on the form of equation (1).

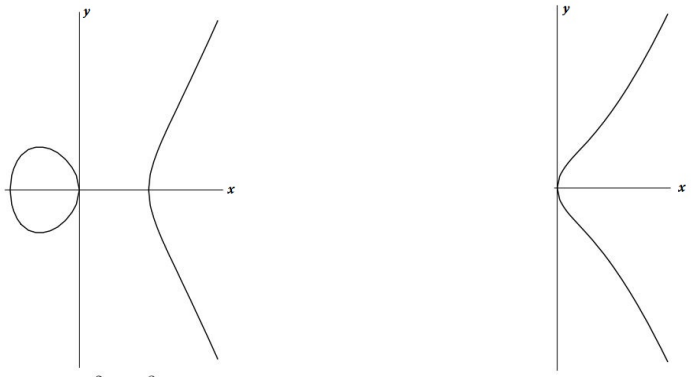
If $A$ and $B$ are elements of a field $K$, we say that the elliptic curve is **defined over** $K$. This is denoted as $E/K$. If $K \subseteq L$ is a field extension, we can look at the set of $L$-rational points $E(L)$ on the elliptic curve, which consists of all solutions of the Weierstrass equation with coordinates in the field $L$, together with one extra point $\infty$. The reason for adding this point will become clear later.

**Definition 2.4** *Let $E/K$ be an elliptic curve defined by the Weierstrass equation $y^2 = x^3 + Ax + B$. Let $K \subseteq L$ be a field extension. The set of* ***L-rational points of E****, denoted by $E(L)$, is defined as*

$$E(L) = \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

*The element $\infty$ is called the* ***point at infinity****.*

The addition of the point at infinity is necessary to introduce a group law on the set $E(L)$. This group law turns $E(L)$ into an abelian group in which $\infty$ serves as the identity element. The construction of the group law can be visualized easiest if we look at elliptic curves with coordinates in $\mathbb{R}$. In this setting we can plot a graph of the elliptic curves in the $(x, y)$-plane. Two representative examples are shown in figure 1.




(a) $y^2 = x^3 - x$ (b) $y^2 = x^3 + x$

Figure 1: Graphs of two elliptic curves over $\mathbb{R}$ [25, p. 10].

An elliptic curve over $\mathbb{R}$ has either three distinct real roots (figure 1a) or one real root (figure 1b). We want to exclude the case in which the curve has a multiple root, because in this case the curve has a singular point. In order to do this we introduce the concept of the discriminant of an elliptic curve. We define the **discriminant** as

$$\Delta = -16(4A^3 + 27B^2).$$

An elliptic curve is nonsingular if and only if its discriminant is nonzero [23, Prop III.1.4]. From now on we require all elliptic curves to be nonsingular.

We will first describe the group law on an elliptic curve $E(\mathbb{R})$ graphically (see figure 2), and then give the general formulas. First of all, consider two distinct points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ in $E(\mathbb{R}) \setminus \{\infty\}$. Draw a line $l$ through these two points. In the case that $P_1 = P_2$, we define $l$ to be the tangent line to the elliptic curve at $P_1$. If $l$ is not vertical, it will intersect the curve in a third point, which we call $P_3'$. This can also be a double intersection point if the line is tangent to the curve in $P_1$ or $P_2$. The reflection of $P_3'$ in the $x$-axis, $P_3$, is what we define to be the sum of $P_1$ and $P_2$. In the case that $l$ is a vertical line, we define $P_1 + P_2 = \infty$. We also define that $P + \infty = \infty + P = \infty$ for all points $P \in E(\mathbb{R})$.

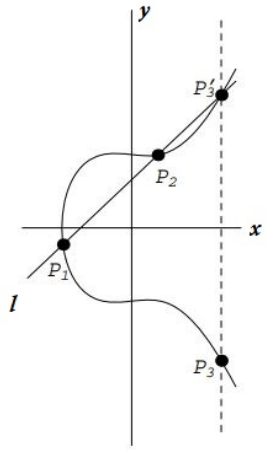



Figure 2: Addition of points $P_1$ and $P_2$ [25, p. 12].

The group law defined in this way turns $E(\mathbb{R})$ in an abelian group. The definition below makes the graphical construction more explicit, and generalizes to elliptic curves over general fields $K$.

**Definition 2.5** [25, Sec. 2.2] *Let $E$ be the elliptic curve defined by $y^2 = x^3 + Ax + B$, with $A, B \in K$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two elements in $E(K) \setminus \{\infty\}$.*
*We define the coordinates of the sum $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:*

1. *If $x_1 \neq x_2$, then*
$$x_3 = m^2 - x_1 - x_2 \text{ and } y_3 = m(x_1 - x_3) - y_1,$$
*where $m = \frac{y_2 - y_1}{x_2 - x_1}$ is the slope of the line through $P_1$ and $P_2$.*
2. *If $x_1 = x_2$ but $y_1 \neq y_2$, $P_1 + P_2 = \infty$.*
3. *If $P_1 = P_2$ and $y_1 \neq 0$, then*
$$x_3 = m^2 - 2x_1 \text{ and } y_3 = m(x_1 - x_3) - y_1,$$
*where $m = \frac{3x_1^2 + A}{2y_1}$ is the slope of the tangent line to $E$ at $P_1$.*
4. *If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.*
5. *for any $P \in E(K)$, $P + \infty = \infty + P = P$.*

Note that we can see using this definition that if $P_1$ and $P_2$ are in $E(K)$, then the coordinates of $P_3$ are also in $K$. Hence $E(K)$ is closed under the addition operation. Showing associativity becomes very technical because of the case distinction in the definition. The complete proof which shows how this addition operator turns $E(K)$ into an abelian group can be found in sections 2.2 and 2.4 of [25].

## 2.3 Maps between elliptic curves

It is possible to describe maps from one elliptic curve to another. These maps can be classified based on how much structure they preserve.

Let $E_1$ and $E_2$ be two elliptic curves (defined over a field $K$). A map $\alpha : E_1 \longrightarrow E_2$ is called a **morphism** when it is defined at every point of $E_1$, and its coordinate functions are given by rational functions with coefficients in $\overline{\mathbb{Q}}$. A morphism is a map that preserves the projective curve structure of elliptic curves. In this thesis, we will not go into the details of projective space and projective curves. An introduction to this topic can be found in [23].

A map $\alpha : E_1 \longrightarrow E_2$ is called an **isogeny** if it is a morphism, and furthermore the point at infinity is mapped to itself, i.e. $\alpha(\infty) = \infty$. It can be shown that an isogeny $\alpha : E_1(\overline{K}) \longrightarrow E_2(\overline{K})$ is a group homomorphism [25, Thm 12.10], and hence preserves the group structure of the elliptic curve. To define properties of isogenies, we introduce a standard form for the rational functions that define the isogeny.

**Lemma 2.6** [25, p. 50-51] *Let $E_1$, $E_2$ be elliptic curves defined over a field $K$. Let $\alpha : E_1 \longrightarrow E_2$ be an isogeny. Then $\alpha$ can be written in the form*

$$\alpha(x, y) = \left(\frac{p(x)}{q(x)}, \frac{u(x)}{v(x)}y\right)$$

*with $p(x), q(x), u(x), v(x) \in \overline{K}[x]$.*

If $q(x) = 0$ or $v(x) = 0$, we have $\alpha(x, y) = \infty$.

We say an isogeny on an elliptic curve $E/K$ is **rational** if the rational functions it is given by have coefficients in $K$. In this case we also say that the isogeny is **defined over** $K$.

We define the **degree** of an isogeny as follows:

$$deg(\alpha) = Max\{deg(p(x)), deg(q(x))\}.$$

Furthermore, we say $\alpha$ is **separable** if the derivative of $\frac{p(x)}{q(x)}$ is nonzero.

For separable isogenies, there is a relation between the degree and kernel of $\alpha$. Here we focus on nontrivial isogenies, i.e. isogenies that do not send every point to $\infty$ and are therefore nonconstant. These isogenies are automatically surjective [23, Thm II.2.3]. For fields of characteristic zero, every nonconstant isogeny is separable [25, p. 51], which is why separable isogenies are of particular interest for us.

**Proposition 2.7** [25, Prop 12.8] *Let $\alpha : E_1 \longrightarrow E_2$ be a nontrivial separable isogeny of an elliptic curve $E/K$. Then $deg(\alpha) = \#ker(\alpha)$, where $ker(\alpha) \subseteq E(\overline{K})$.*

In Section 5 we will make use of isogenies of a certain type. Their properties are defined below.

**Definition 2.8** *We call an isogeny $\alpha : E_1 \longrightarrow E_2$ **cyclic** if $ker(\alpha)$ is a cyclic subgroup of $E_1(\overline{K})$. An $n$-**isogeny** is a cyclic isogeny of degree $n$.*

The following result is useful in showing the existence of an isogeny in particular cases.

**Proposition 2.9** [23, Prop III.4.12, Remark III.4.13.2] *Let $E_1/K$ be an elliptic curve and let $\Phi$ be a finite subgroup of $E_1(\overline{K})$. Then there are a unique elliptic curve $E_2/\overline{K}$ and a separable isogeny $\alpha : E_1 \longrightarrow E_2$ satisfying $ker(\alpha) = \Phi$.*
*Furthermore, If $\Phi$ is invariant under the action of $Aut_K(\overline{K})$, Then we can find an elliptic curve $E_2$ and separable isogeny $\alpha$ that are both defined over $K$.*

We say that two nontrivial isogenies $\alpha : E_1 \longrightarrow E_2$ and $\phi : E_1 \longrightarrow E_3$ are equivalent if and only if they have the same kernel. Namely, nontrivial isogenies are surjective. When they have the same kernel, there exists an isogeny $\pi : E_2 \xrightarrow{\sim} E_3$, which has an inverse, such that $\phi = \pi \circ \alpha$ [23, Cor III.4.11]. Hence $\alpha$ and $\phi$ only differ by an isomorphism of elliptic curves.

## 2.4 Torsion points

We will now focus on a particular map, the multiplication-by-$n$ map on an additive abelian group $G$. For the rest of this report, we will denote by $\mathbb{N}$ the set of natural numbers starting at 1, i.e. $\mathbb{N} = \{1, 2, 3, \ldots\}$. For a number $n \in \mathbb{N}$, the map

$$[n] : G \longrightarrow G$$

is given by

$$[n](P) = P + \ldots + P$$

with $n$ terms in the right-hand side. We can extend this definition to all integers $\mathbb{Z}$, by for $n < 0$ defining $[n](P) = [-n](-P)$, and furthermore letting $[0](P) = 0$ for all $P \in G$ (where 0 denotes the identity element of G).
When applied to an elliptic curve, the addition on the right hand side is given by the addition operation of Definition 2.5. For an abelian group $G$, the multiplication-by-$n$ map is a group endomorphism.

Using the map $[n]$, we can define the **$n$-torsion subgroup** $G[n] \subseteq G$. This subgroup consists of all elements $P$ of order $n$, i.e. elements for which $[n]P$ is equal to the identity element. We can recognize these elements as elements of the kernel of $[n]$:

$$G[n] = \{P \in G \mid [n]P = 0\}.$$

Note that $G[n]$ has a group structure. Namely, if $P, Q \in G[n]$, then $[n]P = [n]Q = 0$. Because $[n]$ is a homomorphism of groups, we obtain $[n](P - Q) = [n]P - [n]Q = 0 - 0 = 0$. Hence $P - Q \in G[n]$, which implies that $G[n]$ is a subgroup of $G$.

We can also define the **full torsion subgroup** of $G$, consisting of all elements that have finite order. This set can be obtained as

$$G_{tors} = \bigcup_{n=1}^{\infty} G[n].$$

A third related concept that will be useful to us is the **$p$-primary component** of $G$. This is the subgroup of all elements of $G$ whose order is a power of $p$, where $p$ is a prime number. We will denote this subgroup as follows:

$$G[p^\infty] = \{P \in G \mid P \in G[p^i] \text{ for some } i \in \mathbb{N}\}.$$

The torsion subgroup and $p$-primary components are again subgroups of $G$.

Because we defined a group law on elliptic curves, we can apply all the concepts above in this setting. Let $E/K$ be an elliptic curve and $K \subseteq L$. In this case, the multiplication-by-$n$ map on $E(L)$ is an isogeny. Furthermore, if $E$ is defined over $K$, then $[n]$ is also defined over $K$ [23].

In the setting of elliptic curves we then obtain

$$E(L)[n] = \{P \in E(L) \mid [n]P = \infty\}.$$

Similarly,

$$E(L)_{tors} = \bigcup_{n=1}^{\infty} E(L)[n]. \tag{2}$$

An important result about $n$-torsion subgroups of elliptic curves is the following:

**Theorem 2.10** [25, Thm 3.2] *Let $\mathbb{Q} \subseteq K$ be an algebraic field extension, and let $E/K$ be an elliptic curve. Then for all $n \in \mathbb{N}$*

$$E(\overline{\mathbb{Q}})[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

The $\oplus$-sign indicates a direct sum. We will also use the notation $(\mathbb{Z}/n\mathbb{Z})^2 = \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Recall that because $\mathbb{Q} \subseteq K$ is an algebraic extension, $\overline{\mathbb{Q}}$ is the algebraic closure of $K$.

Theorem 2.10 gives a characterization of $n$-torsion subgroups for arbitrary elliptic curves over algebraic extensions of $\mathbb{Q}$. It states that these subgroups are always of the form of a direct sum of two finite abelian groups. This is a very powerful characterization.
An important consequence of Theorem 2.10 is that we can find a two-dimensional basis for $E(\overline{\mathbb{Q}})[n]$. Namely, $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2, which implies that there exist a basis of two elements for this module. We can thus also find a basis of two elements for $E(\overline{\mathbb{Q}})[n]$. The explicit isomorphism of Theorem 2.10 depends on the choice of this basis.

Theorem 2.10 will prove to be useful in finding a description of the full torsion group (as defined in (2)). A description of such a torsion group will not be fully general, but depends on which field and which specific Weierstrass equations are considered. In the next section, we will see an overview of existing literature concerning the full torsion groups of elliptic curves over specific fields.

# 3 Torsion subgroups of elliptic curves over extensions of $\mathbb{Q}$

## 3.1 Torsion subgroups of elliptic curves over number fields

We will start by focusing on elliptic curves over number fields. Recall that this means that the extensions of $\mathbb{Q}$ we consider are finite. We will first show that a torsion subgroup over such a number field is always of a particular form. It will then turn out that a very general result can be obtained about these torsion subgroups, which only depends on the degree of the field extension and not on the specific field or curve.

In 1922, it was shown by Mordell [20] that the abelian group $E(\mathbb{Q})$ of $\mathbb{Q}$-rational points on any elliptic curve $E/\mathbb{Q}$ is finitely generated. In 1929 Weil [26] proved that the same statement is true for the group of $K$-rational points $E(K)$, where $K$ is a number field and $E$ is defined over $K$. The following theorem therefore applies to these groups.

**Theorem 3.1 (Fundamental Theorem of Finitely Generated Abelian Groups)** *If $G$ is a finitely generated abelian group, it can be decomposed uniquely as follows:*

$$G \cong \mathbb{Z}^r \oplus (\mathbb{Z}/n_1\mathbb{Z}) \oplus (\mathbb{Z}/n_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_k\mathbb{Z})$$

*where $r \geq 0$, $n_i \geq 2$ for all $1 \leq i \leq k$ and $n_i \mid n_{i+1}$ for $1 \leq i \leq k-1$.*

From this theorem, it also follows that $G_{tors} \cong \bigoplus_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$ (the subgroup of all elements of finite order) is a finite group.

For elliptic curves over number fields $K$, we can even derive a stronger statement.

**Theorem 3.2** *Let $E/K$ be an elliptic curve, where $K$ is an algebraic field extension of $\mathbb{Q}$. If $E(K)_{tors}$ is finite, then*

$$E(K)_{tors} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nm\mathbb{Z}$$

*for some $n, m \in \mathbb{N}$.*

To prove this theorem, it is useful to start by introducing a few useful definitions and results.

**Definition 3.3** *The **exponent** of a group $G$, denoted by $exp(G)$, is defined as the least common multiple of the orders of all elements in the group, if this exists. Otherwise the exponent is taken to be infinity.*

If $exp(G) < \infty$, it follows from this definition that for each element $g \in G$, its order must divide the exponent of the group. Hence $[exp(G)]g = 0$ for all $g \in G$. The following result about the exponent of a finite group can be obtained.

**Proposition 3.4** *Let $G$ be a finite group of order $n$. Then $exp(G)$ is finite and it divides $n$.*

*Proof.* It follows from Lagrange's theorem that in a finite group, the order of each element divides the order of the group. Hence all elements have finite order. Their least common multiple is then also finite. Furthermore, if all numbers in a certain set divide $n$, then their least common multiple, which is in this case $exp(G)$, also divides $n$. ∎

The next two lemmas characterize the $m$-torsion subgroups for groups of the from $\bigoplus_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$ with $k, n_i \in \mathbb{N}$. These results will be useful in the proof of Theorem 3.2.

**Lemma 3.5** *Let $m, n \in \mathbb{N}$ be such that $m \mid n$. Then*

$$(\mathbb{Z}/n\mathbb{Z})[m] \cong \mathbb{Z}/m\mathbb{Z}.$$

*Proof.*

$$\begin{aligned}
\overline{a} \in (\mathbb{Z}/n\mathbb{Z})[m] &\iff \overline{ma} = \overline{0} \\
&\iff n \mid ma \\
&\iff \frac{n}{m} \mid a \\
&\iff a \in \frac{n}{m}\mathbb{Z} \\
&\iff \overline{a} \in \left(\frac{n}{m}\mathbb{Z}\right)/n\mathbb{Z}.
\end{aligned}$$

Hence $(\mathbb{Z}/n\mathbb{Z})[m] = (\frac{n}{m}\mathbb{Z})/n\mathbb{Z}$.

Note that $\mathbb{Z}/m\mathbb{Z} \cong (\frac{n}{m}\mathbb{Z})/n\mathbb{Z}$ by the explicit isomorphism

$$\begin{aligned}
\phi : \mathbb{Z}/m\mathbb{Z} &\longrightarrow \left(\frac{n}{m}\mathbb{Z}\right)/n\mathbb{Z} \\
a + m\mathbb{Z} &\longmapsto \left[\frac{n}{m}\right] a + n\mathbb{Z}.
\end{aligned}$$

It follows that $(\mathbb{Z}/n\mathbb{Z})[m] = (\frac{n}{m}\mathbb{Z})/n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$. ∎

**Lemma 3.6** *Let $G = \bigoplus_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$ with $k, n_i \in \mathbb{N}$. Let $m \in \mathbb{N}$. Then*

$$G[m] = \bigoplus_{i=1}^{k} (\mathbb{Z}/n_i\mathbb{Z})[m].$$

*Proof.*

$$\begin{aligned}
(a_1, \ldots, a_k) \in G[m] &\iff [m](a_1, \ldots, a_k) = (0, \ldots, 0) \\
&\iff ([m]a_1, \ldots, [m]a_k) = (0, \ldots, 0) \\
&\iff a_i \in (\mathbb{Z}/n_i\mathbb{Z})[m] \text{ for all } i \in \{1, \ldots, k\} \\
&\iff (a_1, \ldots, a_k) \in \bigoplus_{i=1}^{k} (\mathbb{Z}/n_i\mathbb{Z})[m].
\end{aligned}$$

∎

We can now use these results to formulate the proof of Theorem 3.2.

*Proof of Theorem 3.2.* We assume that $E(K)_{tors}$ is a finite group. By Proposition 3.4, the exponent of $E(K)_{tors}$ then is a finite number. Let us define $m = exp(E(K)_{tors})$. Then for each $P \in E(K)_{tors}$, we have $[m]P = \infty$. It follows that $E(K)_{tors} \subseteq E(K)[m]$.

Note that $K \subseteq \overline{\mathbb{Q}}$ implies that $E(K) \subseteq E(\overline{\mathbb{Q}})$, which in turn implies that $E(K)[m] \subseteq E(\overline{\mathbb{Q}})[m]$. From Theorem 2.10 we know that $E(\overline{\mathbb{Q}})[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. It follows that

$$E(K)_{tors} \subseteq E(\overline{\mathbb{Q}})[m] \cong (\mathbb{Z}/m\mathbb{Z})^2, \tag{3}$$

hence $E(K)_{tors}$ is isomorphic to a subgroup of $(\mathbb{Z}/m\mathbb{Z})^2$.

We also know as a result of Theorem 3.1 that $E(K)_{tors} \cong \bigoplus_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$ where $n_i \mid n_{i+1}$.

Let $p$ be a prime such that $p \mid n_1$. Then $p \mid n_i$ for all $i = 1, \ldots, k$. Lemma 3.5 implies that $(\mathbb{Z}/n_i\mathbb{Z})[p] \cong \mathbb{Z}/p\mathbb{Z}$. Using Lemma 3.6, we obtain

$$\begin{aligned} E(K)[p] = E(K)_{tors}[p] &\cong \left(\bigoplus_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}\right)[p] \\ &= \bigoplus_{i=1}^{k} (\mathbb{Z}/n_i\mathbb{Z})[p] \\ &= (\mathbb{Z}/p\mathbb{Z})^k. \end{aligned} \tag{4}$$

This also means that, unless $k = 0$ and $E(K)_{tors}$ is the trivial group, $E(K)_{tors}$ has an element of order $p$. In this case $p \mid m$. We can then, using Lemmas 3.6 and 3.5, conclude that

$$(\mathbb{Z}/m\mathbb{Z})^2[p] = ((\mathbb{Z}/m\mathbb{Z})[p])^2 \cong (\mathbb{Z}/p\mathbb{Z})^2. \tag{5}$$

From (3) it follows that $E(K)[p]$ is isomorphic to a subgroup of $(\mathbb{Z}/m\mathbb{Z})^2[p]$. Using (4) and (5), this translates into $(\mathbb{Z}/p\mathbb{Z})^k \subseteq (\mathbb{Z}/p\mathbb{Z})^2$. The only way in which this is possible is when $k \in \{0, 1, 2\}$.
We conclude $E(K)_{tors} \cong \bigoplus_{i=1}^{2} \mathbb{Z}/n_i\mathbb{Z}$ where $n_1 \mid n_2$, and $n_1, n_2 \in \mathbb{N}$. This can be written as

$$E(K)_{tors} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nm\mathbb{Z}$$

with $n, m \in \mathbb{N}$, as desired. ∎

The integers $n$ and $m$ in Theorem 3.2 depend both on the coefficients that define the Weierstrass equation of $E$, and on the field $K$ over which the elliptic curve is considered. Note that for number fields $K$ we know that $E(K)_{tors}$ is finite, and hence in this case we can apply Theorem 3.2. Attempts have been made to obtain more specific results for particular number fields. We will now give an overview of some of these results.

In 1977, Mazur found a description of all possible forms the torsion subgroups of elliptic curves over the rational numbers could take.

**Theorem 3.7 (Mazur)** [17] *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{with } 1 \leq m \leq 10 \text{ or } m = 12, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \text{with } 1 \leq m \leq 4. \end{cases}$$

Which particular group is attained depends on the coefficients of the Weierstrass equation of the elliptic curve. The theorem lists all possible group structures that can occur, and all of them actually do occur. This means that for every group mentioned in Theorem 3.7, there exists an elliptic curve $E/\mathbb{Q}$ such that $E(\mathbb{Q})_{tors}$ is isomorphic to this group.

From this theorem, we see in particular that there is only a very restricted number of possibilities for the torsion subgroup, considering the large amount of different Weierstrass equations

the theorem applies to. The maximum number of torsion elements for a group $E(\mathbb{Q})$ is equal to 16, the number of elements in the group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Hence we have a bound for this number of elements which does not depend on the elliptic curve $E$.

A result similar to Theorem 3.7 was determined for elliptic curves over number fields of degree 2, also called quadratic number fields. Kenku and Momose [11] started with this in 1988, and it was finished in 1992 by Kamienny [10].

**Theorem 3.8** [11, 10] *Let $K$ be a quadratic number field, and $E/K$ an elliptic curve defined over this field. Then*

$$E(K)_{tors} \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{with } 1 \leq m \leq 16 \text{ or } m = 18, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \text{with } 1 \leq m \leq 6, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} & \text{with } m = 1 \text{ or } 2, \text{ (only if } K = \mathbb{Q}(\sqrt{3})), \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \text{(only if } K = \mathbb{Q}(\sqrt{-1})). \end{cases}$$

Again the specific form depends on the field $K$ and the elliptic curve $E$. In this case, we again find that if we look at any quadratic number field $K$, we can find an upper bound for the number of elements in $E(K)_{tors}$ which is independent of $E$. In this case the number 24 is such a bound, the number of elements in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. This upper bound is even valid for all quadratic number fields.

It was conjectured that such an upper bound on the number of elements in the torsion group might exist also for fields extensions of a degree higher than 2. In 1996, Merel [19] indeed proved that there exists a uniform bound on the number of elements in $E(K)_{tors}$. This bound depends only on the degree of the extension $\mathbb{Q} \subseteq K$, and not on the particular number field $K$ or the coefficients of the elliptic curve $E$.

**Theorem 3.9 (Merel)** [19] *For all positive integers $n$, there exists a constant $B(n) \geq 0$ such that*

$$\#E(K)_{tors} \leq B(n)$$

*for all number fields $K$ that satisfy $[K : \mathbb{Q}] = n$, and for all elliptic curves $E/K$.*

Theorem 3.7 and 3.8 make this bound explicit for extensions of degree 1 and 2, respectively. Namely, the only degree 1 extension is $\mathbb{Q} \subseteq \mathbb{Q}$, and hence from Theorem 3.7 we saw that we can choose $B(1) = 16$. Similarly, from Theorem 3.8 it follows that we can choose $B(2) = 24$.

Naturally, attempts have been made to also find explicit descriptions of the torsion groups of elliptic curves over higher degree number fields. These attempts have however only been partially successful. From private conversations it was understood that for cubic fields (degree 3), a general description analogous to Theorem 3.8 has very recently been found. This has however not yet been published. For higher degree extensions, no general results have been obtained yet.

It is possible to obtain more specific results when we only consider the set of elliptic curves that are defined over $\mathbb{Q}$. In other words, we restrict the coefficients in the Weierstrass equation to rational numbers. In this case, a description of the torsion subgroups that appear over quadratic and cubic extensions has been found by Najman [21].

The discussion above describes torsion subgroups of elliptic curves over number fields, i.e. over finite algebraic extensions of the rational numbers. The word 'finite' is essential here. The next step is to look at elliptic curves with elements in infinite extensions $\mathbb{Q} \subseteq K$. This means that the field $K$ is an infinite-dimensional vector space over $\mathbb{Q}$. In this case, the group $E(K)$ is no longer automatically finitely generated. Theorem 3.1 can therefore no longer be applied to obtain a description of its torsion subgroup. In some specific cases we can however show in a different way that $E(K)$ still has a finite torsion subgroup.

## 3.2 Torsion subgroups of elliptic curves over infinite extensions of $\mathbb{Q}$

We will now look into elliptic curves over infinite algebraic extensions of $\mathbb{Q}$. We consider fields $K$ with $\mathbb{Q} \subseteq K \subseteq \overline{\mathbb{Q}}$, for which the degree of $\mathbb{Q} \subseteq K$ is infinite. The requirement that $K$ is contained in the algebraic closure of $\mathbb{Q}$ ensures that $K$ is an algebraic extension of $\mathbb{Q}$.
We will first look at fields of a specific form. To describe these, we need the notion of a compositum of fields. We will use a slightly restricted definition that requires the fields to be contained in a common field. This definition is sufficient for our purposes, because all fields we consider are subfields of $\overline{\mathbb{Q}}$.

**Definition 3.10** *Let $L$ be a field and $(K_i)_{i\in I}$ a collection of fields, all of characteristic zero, such that $K_i \subseteq L$ for all $i \in I$ (where $I$ is some indexing set). The* ***compositum*** *of the fields $(K_i)_{i\in I}$ is the field generated by the elements of each $K_i$. It can be written as $\mathbb{Q}(\cup_{i\in I} K_i)$. This is the smallest subfield of $L$ containing each of the fields $K_i$.*
*A field $\mathbb{Q}(V)$, where $V$ is some set, can be described as follows:*

$$\mathbb{Q}(V) = \{f(v_1, \ldots, v_n) \mid n \in \mathbb{N},\ f \in \mathbb{Q}[x_1, \ldots, x_n],\ v_1, \ldots, v_n \in V\}.$$

We will consider the compositum of all number fields of a certain degree $d$. We will look at the torsion subgroups of elliptic curves over such a compositum.

**Definition 3.11** *For all $d \in \mathbb{N}$ , $\mathbb{Q}(d^\infty)$ denotes the compositum of all field extensions of degree $d$:*

$$\mathbb{Q}(d^\infty) := \mathbb{Q}(\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] = d\}).$$

We will focus our attention again on elliptic curves that are defined over $\mathbb{Q}$. In this case, for all $d \geq 2$ the group $E(\mathbb{Q}(d^\infty))$ is not finitely generated [3, 6]. This means we can not use Theorem 3.1 to obtain information about its torsion group. However, the torsion groups have been studied for $d \in \{1, 2, 3\}$.

For $d = 1$, $\mathbb{Q}(d^\infty)$ is simply equal to $\mathbb{Q}$. Hence we arrive at the torsion subgroup structure already described in Theorem 3.7.
The case $d = 2$ has been described by Laska, Lorenz [16] and Fujita [4, 5]. In this case the compositum can be characterized as $\mathbb{Q}(2^\infty) = \mathbb{Q}(\{\sqrt{m} \mid m \in \mathbb{Z}\})$. The group $E(\mathbb{Q}(2^\infty))$ is not finitely generated, but the torsion subgroup $E(\mathbb{Q}(2^\infty))_{tors}$ was found to be finite. The classification of all possible structures of the torsion subgroup can be found in Theorem 2 of [5].
This year, in 2018, Daniels, Lozano-Robledo, Najman and Sutherland [1] published an article in which they described the torsion subgroup for the elliptic curves over $\mathbb{Q}(3^\infty)$, the compositum of all cubic fields. Their result is the following.

**Theorem 3.12** [1, Thm 1.8] *Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup $E(\mathbb{Q}(3^\infty))_{tors}$ is finite, and isomorphic to a group of one of the following forms:*

$$E(\mathbb{Q}(3^\infty))_{tors} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \text{with } m = 1, 2, 4, 5, 7, 8, 13, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z} & \text{with } m = 1, 2, 4, 7, \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6m\mathbb{Z} & \text{with } m = 1, 2, 3, 5, 7, \text{ or} \\ \mathbb{Z}/2m\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \text{with } m = 4, 6, 7, 9. \end{cases}$$

We again see that there is a finite number of possibilities for the torsion subgroup.

A more general result that was presented in the same article [1], deals with elliptic curves over fields that are Galois extensions of $\mathbb{Q}$. The definition of a Galois extension will be presented in the next section. In the following theorem, the concept of **roots of unity** in a field $K$ is mentioned. An element $x \in K$ is called a root of unity if there exists some positive integer $n$ for which $x^n = 1$.

**Theorem 3.13** [1, Thm 4.1] *Let $E/\mathbb{Q}$ be an elliptic curve, and let $K$ be a (possibly infinite) Galois extension of $\mathbb{Q}$. Assume $K$ contains only finitely many roots of unity. Then $E(K)_{tors}$ is finite.*
*Furthermore, there exists a uniform bound $B$, depending only on $K$, such that for every elliptic curve $E/\mathbb{Q}$*

$$\#E(K)_{tors} \leq B.$$

This theorem says that if we impose certain properties on a field, then similar to the situations before, the torsion group of an elliptic curve over this field is finite. We can find a bound for the number of elements in this group, which does not depend on the elliptic curve $E/\mathbb{Q}$.

In the next section, we will introduce some new concepts that will help us to formulate a proof of Theorem 3.13. The main objective there is to fill in details in the proof provided by Daniels et al. [1] to make it more self-contained and accessible. This proof will be formulated in Section 5.

# 4 Galois Theory

## 4.1 Introduction to Galois theory

In the proof of Theorem 3.13 and the sections to follow, we will make use of a very powerful theory called Galois theory. We will give a brief introduction of general Galois theory, which is applicable to infinite field extensions. For finite extensions, many details are less complicated, but since we will also be dealing with infinite extensions this is not sufficient. Only the relevant and useful results are treated here. A more elaborate treatment can be found in lecture notes by Stevenhagen [24], on which this section is based.

First of all, let $K \subseteq L$ be an algebraic field extension. Then for every element $\alpha \in L$, there exists a polynomial $f_K^\alpha \in K[x]$ which is the monic polynomial of minimal degree in $K[x]$ such that $\alpha$ is a zero of $f_K^\alpha$. A **monic** polynomial is a polynomial for which the coefficient of the highest power of $x$ is equal to 1. This unique polynomial $f_K^\alpha$ is called the **minimal polynomial** of $\alpha$ over $K$. We can use this concept to define two important notions.

**Definition 4.1** *Let $K \subseteq L$ be a field extension. An element $\alpha \in L$ is called **separable** over $K$ if its minimal polynomial over $K$, $f_K^\alpha$, has no multiple roots. A field extension $K \subseteq L$ is called **separable** if all $\alpha \in L$ are separable over $K$.*

**Definition 4.2** [24, Def 23.12] *A field extension is called **normal** if for each $\alpha \in L$, its minimal polynomial over $K$ splits into linear factors in $L[x]$.*

We use these notions to formulate a definition of a Galois extension.

**Definition 4.3** *A field extension $K \subseteq L$ is called **Galois** if it is algebraic, separable and normal.*
*The **Galois group** of $K \subseteq L$ is defined as $Gal(L/K) := Aut_K(L)$ (The group of field automorphisms of $L$ that act as identity on $K$).*

The following theorem states the well-known Galois correspondence. It makes use of the notion of closed subgroups. In order not to get stuck on the details, we refer to Section 28 of [24] for the construction of the used topology.

**Theorem 4.4 (Galois Correspondence)** [24, Thm 28.8] *Let $K \subseteq L$ be a Galois extension with Galois group $G$. Let $\mathcal{M}$ be the set of all subfields $F$ such that $K \subseteq F \subseteq L$, and let $\mathcal{H}$ be the set of all closed subgroups of $G$. There exists an inclusion reversing bijection:*

$$\begin{aligned} \psi : \mathcal{M} &\longrightarrow \mathcal{H} \\ F &\longmapsto Aut_F(L). \end{aligned}$$

*The inverse is given by $\psi^{-1}(G) = L^G$, where $L^G$ is the subfield of $L$ consisting of elements that are fixed by $G$.*

*Let $F \in \mathcal{M}$. Then $F \subseteq L$ is Galois with Galois group $H = \psi(F) = Aut_F(L)$. For each $\sigma \in G$, the field $\sigma(F) \in \mathcal{M}$ corresponds to the group $\sigma H \sigma^{-1}$ under $\psi$. The extension $K \subseteq F$ is normal if and only if $H$ is a normal subgroup of $G$. In this case $K \subseteq F$ is Galois and $Gal(F/K) \cong G/H$.*

It follows from this theorem that if we look at an extension $\mathbb{Q} \subseteq K \subseteq \overline{\mathbb{Q}}$, we have that $\mathbb{Q} \subseteq K$ is Galois if and only if $Gal(\overline{\mathbb{Q}}/K) \lhd Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, where $\lhd$ indicates a normal subgroup. If this is not the case, the following concept can be useful.

**Definition 4.5** *Let $K \subseteq L$ be an algebraic field extension. The **normal closure** of this extension is the smallest field $M$ containing $L$ for which $K \subseteq M$ is a normal extension.*

For all algebraic extensions, such a normal closure exists and is unique up to isomorphism.

## 4.2 Galois Representation

In this section, we will show how Galois theory can be useful in the context of elliptic curves and their torsion subgroups. We start with the following useful result.

**Proposition 4.6** [24, Thm 23.8] *Let $K$ be a field of characteristic zero. Then every algebraic extension of $K$ is separable.*

Consider the extension $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$. It follows directly from the definition of an algebraic closure that this extension is algebraic. Proposition 4.6 implies that it is also separable. $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ is also automatically normal. To see this, note that all zeros of every polynomial over $\mathbb{Q}$ are by definition algebraic over $\mathbb{Q}$. It follows that all these zeros are in the algebraic closure $\overline{\mathbb{Q}}$, hence every polynomial splits into linear factors in $\overline{\mathbb{Q}}[x]$. We conclude that $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ is Galois, by Definition 4.3. We can speak of its Galois group $G_{\mathbb{Q}} := Gal(\overline{\mathbb{Q}}/\mathbb{Q}) = Aut_{\mathbb{Q}}(\overline{\mathbb{Q}})$.

Let us now look at the group $E(\overline{\mathbb{Q}})$ for some elliptic curve $E/\mathbb{Q}$. The Galois group $G_{\mathbb{Q}}$ can act on the elements of $E(\overline{\mathbb{Q}})$ coordinate-wise in the following way: for $P = (x, y) \in E(\overline{\mathbb{Q}})$ and $\sigma \in G_{\mathbb{Q}}$, we let $\sigma(P) = (\sigma(x), \sigma(y))$. Note that since $E$ is defined over $\mathbb{Q}$, $\sigma(P)$ is again a point on the elliptic curve:

$$\begin{aligned} y^2 &= x^3 + Ax + B \\ \sigma(y^2) &= \sigma(x^3 + Ax + B) \\ \sigma(y)^2 &= \sigma(x)^3 + A\sigma(x) + B. \end{aligned}$$

The last step follows from the fact that $\sigma$ is a homomorphism that acts as identity on $\mathbb{Q}$, and $A, B \in \mathbb{Q}$. We define $\sigma(\infty) = \infty$.

It can be observed that $G_{\mathbb{Q}}$ also acts on the group $E(\overline{\mathbb{Q}})[n]$. Namely, if $P = (x, y) \in E(\overline{\mathbb{Q}})[n]$, then $[n]P = \infty$. Recall from Section 2.4 that the isogeny $[n]$ is defined over $\mathbb{Q}$, so any $\sigma \in G_{\mathbb{Q}}$ acts as identity on the coefficients of $[n]$. We thus have $[n](\sigma(P)) = \sigma([n]P) = \sigma(\infty) = \infty$. This implies that $\sigma(P) \in E(\overline{\mathbb{Q}})[n]$.
We can furthermore show that $\sigma$ acts as an automorphism on $E(\overline{\mathbb{Q}})[n]$, because $\sigma$ is an automorphism on $\overline{\mathbb{Q}}$. Namely, if $\sigma(x_1, y_1) = \sigma(x_2, y_2)$, then $(\sigma(x_1), \sigma(y_1)) = (\sigma(x_2), \sigma(y_2))$. Because $\sigma$ is injective this implies $x_1 = x_2$ and $y_1 = y_2$, so $\sigma$ acts injectively. Because $E(\overline{\mathbb{Q}})[n]$ is a finite group (Theorem 2.10), this implies that the action is automorphic.

The action of $G_{\mathbb{Q}}$ on $E(\overline{\mathbb{Q}})[n]$ therefore induces a so-called Galois representation

$$\rho_{E,n} : G_{\mathbb{Q}} \longrightarrow Aut(E(\overline{\mathbb{Q}})[n]). \tag{6}$$

We consider $Aut(E(\overline{\mathbb{Q}})[n])$ as a group, In which case the map $\rho_{E,n}$ is a homomorphism of groups.
The automorphism group of $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ is equal to the general linear group $GL_2(\mathbb{Z}/n\mathbb{Z})$, which consists of all $2 \times 2$ matrices with coordinates in $\mathbb{Z}/n\mathbb{Z}$ that are invertible. Such a matrix is invertible if and only if its determinant is a unit in $\mathbb{Z}/n\mathbb{Z}$. From Theorem 2.10 we can deduce that $Aut(E(\overline{\mathbb{Q}})[n]) \cong GL_2(\mathbb{Z}/n\mathbb{Z})$. The explicit isomorphism depends on the choice of basis for $E(\overline{\mathbb{Q}})[n]$ that defines the isomorphism in Theorem 2.10. We will denote by

$$\psi_{E,n} : Aut(E(\overline{\mathbb{Q}})[n]) \longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z})$$

such an explicit isomorphism.

We can define the field $\mathbb{Q}(E[n])$, obtained by adjoining the $x$- and $y$-coordinates of points in $E(\overline{\mathbb{Q}})[n]$ to the field $\mathbb{Q}$. This is a subfield of the extension $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$.
Note that $\sigma \in G_{\mathbb{Q}}$ is in the kernel of $\rho_{E,n}$ if and only if it fixes all coordinates of points in $E(\overline{\mathbb{Q}})[n]$, in other words, if and only if it fixes $\mathbb{Q}(E[n])$. Hence $\mathbb{Q}(E[n]) = \overline{\mathbb{Q}}^{ker(\rho_{E,n})}$. The Galois correspondence then imples that

$$Gal(\overline{\mathbb{Q}}/\mathbb{Q}(E[n])) = Aut_{\mathbb{Q}(E[n])}(\overline{\mathbb{Q}}) = ker(\rho_{E,n}).$$

$Gal(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$ is thus the kernel of a group homomorphism, and therefore a normal subgroup of $G_{\mathbb{Q}}$. It follows, again from the Galois correspondence, that the extension $\mathbb{Q} \subseteq \mathbb{Q}(E[n])$ is Galois with Galois group $G_{\mathbb{Q}}/ker(\rho_{E,n})$.
By the first isomorphism theorem, this Galois group is also isomorphic to the image of $\rho_{E,n}$. It is thus a subgroup of $Aut(E(\overline{\mathbb{Q}})[n])$. Now using the isomorphism $\psi_{E,n}$, we obtain that $Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ is isomorphic to a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$.

# 5 Proof of a uniform bound for torsion subgroups

In this section, we will elaborate on the proof of Theorem 3.13 given by Daniels, Lozano-Robledo, Najman and Sutherland in their article [1]. We will walk through their implicit intermediate steps and in this way provide a more self-contained explanation of their work, which is understandable for people who are less familiar with this field of research.

In this entire section, we will work under the assumptions of the theorem. So $E$ is an elliptic curve with coefficients in $\mathbb{Q}$, and $K$ is a Galois extension of $\mathbb{Q}$ containing finitely many roots of unity.

The finiteness of $E(K)_{tors}$ will be shown in three separate steps. We will start by showing that $E(K)_{tors}$ is isomorphic to a direct sum of its $p$-primary components. This shifts the problem to showing that this direct sum is finite. Secondly, we will show that the $p$-primary component of $E(K)_{tors}$ is nontrivial for only finitely many primes $p$. Thirdly, for these primes, we will show that the $p$-primary component is finite. These three results together then imply that $E(K)_{tors}$ is a finite group. The uniform bound on the number of elements of $E(K)_{tors}$ will follow directly from the proof.

## 5.1 Direct sum of $p$-primary components

We will prove the following proposition in the general setting of abelian groups.

**Proposition 5.1** *Let $G$ be an abelian group. Then the torsion subgroup $G_{tors}$ is isomorphic to the direct sum of the $p$-primary components of $G$.*

*Proof.* Let $g \in G_{tors}$. Then $g$ has some finite order $m$, for which $[m]g = 0$. Consider its prime factorization $m = \prod_{i=1}^{k} p_i^{e_i}$.
Let $m_i = m/p_i^{e_i}$. We have that $gcd\{m_1, \ldots, m_k\} = 1$. This implies that there exist $l_1, \ldots, l_k \in \mathbb{Z}$ for which $\sum_{i=1}^{k} l_i m_i = 1$ (this is a generalization of Bézout's identity).
Let $g_i = [m_i]g$. We obtain

$$g = \left[\sum_{i=1}^{k} l_i m_i\right] g = \sum_{i=1}^{k} [l_i] g_i$$

Note that $[p_i^{e_i}]\ g_i = [p_i^{e_i}]\ [m_i]g = [m]g = 0$. Because $m$ is the order of $g$, this implies that $p_i^{e_i}$ is the order of $g_i$. It follows that $g_i \in G[p_i^\infty]$, and so is $[l_i]g_i$ (because $G[p_i^\infty]$ is a group). Hence $g$ can be written as a sum of elements of the $p$-primary components of $G$. Because this reasoning is true for any $g \in G_{tors}$, we can conclude that $G_{tors}$ is the sum of the $p$-primary components of $G$.

Furthermore notice that whenever $p_1 \neq p_2$ for two prime numbers, we have that $G[p_1^\infty] \cap G[p_2^\infty] = \{0\}$. This implies that the sum of $p$-primary components of $G$ is actually a direct sum, which concludes the proof. ∎

Because $E(K)$ is an abelian group, Proposition 5.1 tells us that we can write

$$E(K)_{tors} \cong \bigoplus_{p\ prime} E(K)[p^\infty]. \tag{7}$$

In order to show that $E(K)_{tors}$ is finite, we can focus on showing that the above direct product is finite. This is how we will proceed.

## 5.2 The $p$-primary component is nontrivial for only finitely many $p$

To show that there are only finitely many $p$-primary components of $E(K)_{tors}$ that are nontrivial, we need a few intermediate results first. We will first try to say something about the $p$-torsion subgroups $E(K)[p]$. Recall from Theorem 2.10 that $E(\overline{\mathbb{Q}})[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$. Because $E(K)[p]$ is a subgroup of $E(\overline{\mathbb{Q}})[p]$, it must be isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^2$. For a prime number $p$, $(\mathbb{Z}/p\mathbb{Z})^2$ only has 3 distinct isomorphism classes of subgroups. The order of a subgroup of $(\mathbb{Z}/p\mathbb{Z})^2$ must divide $p^2$. First of all, if a subgroup has exactly $p^2$ elements, we obtain the full group $(\mathbb{Z}/p\mathbb{Z})^2$. Secondly, we have the trivial subgroup $\{(0,0)\}$, which has only one element. The final possibility is a subgroup of order $p$. If we look at $(\mathbb{Z}/p\mathbb{Z})^2$ as a $\mathbb{Z}/p\mathbb{Z}$-vector space, the subgroups of order $p$ are exactly the one-dimensional subspaces of $(\mathbb{Z}/p\mathbb{Z})^2$. these are the cyclic groups generated by elements of the form $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^2 \setminus \{(0,0)\}$, which are isomorphic to $\mathbb{Z}/p\mathbb{Z}$. To summarize, the three isomorphism classes of subgroups of $(\mathbb{Z}/p\mathbb{Z})^2$ are the following:

- $(\mathbb{Z}/p\mathbb{Z})^2$,
- $\mathbb{Z}/p\mathbb{Z}$,
- $\{0\}$.

What we will do is make a rough classification of the cases in which $E(K)[p]$ is in each of these three isomorphism classes.

One of the useful concepts we will need in order to do this is a map called the Weil pairing. To define this map, let $n$ be a positive integer. We will make use of the group of $n$th roots of unity in $\overline{\mathbb{Q}}$, defined as follows:

$$\mu_n = \{x \in \overline{\mathbb{Q}} \mid x^n = 1\}.$$

This is a cyclic group of order $n$. The Weil pairing is a map

$$e_n : E(\overline{\mathbb{Q}})[n] \times E(\overline{\mathbb{Q}})[n] \longrightarrow \mu_n$$

for some elliptic curve $E$, that satisfies a set of properties. The following theorem ensures the existence of such a mapping.

**Theorem 5.2 (Weil pairing)** [25, Thm 3.9] *Let $K$ be a field of characteristic zero, let $E/K$ an elliptic curve and let $n \in \mathbb{N}$. Then there exists a* ***Weil pairing***

$$e_n : E(\overline{\mathbb{Q}})[n] \times E(\overline{\mathbb{Q}})[n] \longrightarrow \mu_n$$

*satisfying:*

1. *$e_n$ is bilinear in each variable:*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$
$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

   *for all $S, S_1, S_2, T, T_1, T_2 \in E(\overline{\mathbb{Q}})[n]$.*

2. *If* $e_n(S,T) = 1$ *for all* $T \in E(\overline{\mathbb{Q}})[n]$*, then* $S = \infty$*. Similarly, if* $e_n(S,T) = 1$ *for all* $S \in E(\overline{\mathbb{Q}})[n]$*, then* $T = \infty$*.*

3. $e_n(T,T) = 1$ *for all* $T \in E(\overline{\mathbb{Q}})[n]$*.*

4. $e_n(S,T) = e_n(T,S)^{-1}$ *for all* $S, T \in E(\overline{\mathbb{Q}})[n]$*.*

5. $e_n(\sigma(S), \sigma(T)) = \sigma(e_n(S,T))$ *for all* $\sigma \in Aut(\overline{\mathbb{Q}})$ *that are the identity map on the coefficients of* $E$*.*

6. $e_n(\alpha(S), \alpha(T)) = e_n(S,T)^{deg(\alpha)}$ *for all separable endomorphisms* $\alpha$ *of* $E$*.*

We introduced the Weil pairing because it has some results that will become useful in proving Theorem 3.13. These results rely on the fact that there exists a basis of two elements of $E(\overline{\mathbb{Q}})[n]$ (Section 2.4).

**Corollary 5.3** [25, Cor 3.10] *Let* $\{T_1, T_2\}$ *be a basis of* $E(\overline{\mathbb{Q}})[n]$*. Then* $e_n(T_1, T_2)$ *is a primitive* $n$*th root of unity, meaning it is a generator of* $\mu_n$*.*

**Corollary 5.4** [25, Cor 3.11] *If* $E(\overline{\mathbb{Q}})[n] \subseteq E(K)$*, then* $\mu_n \subseteq K$*.*

*Proof.* Let $\sigma \in Aut_K(\overline{\mathbb{Q}})$. Let $\{T_1, T_2\}$ be a basis of $E(\mathbb{Q})[n]$. By assumption, $E(\overline{\mathbb{Q}})[n] \subseteq E(K)$, so $T_1$ and $T_2$ have coordinates in $K$. Hence $\sigma(T_1) = T_1$ and $\sigma(T_2) = T_2$. It follows from property 5 in Theorem 5.2 that

$$e_n(T_1, T_2) = e_n(\sigma(T_1), \sigma(T_2)) = \sigma(e_n(T_1, T_2)),$$

and hence $e_n(T_1, T_2)$ is fixed by all $\sigma \in Aut_K(\overline{\mathbb{Q}})$. We conclude $e_n(T_1, T_2) \in \overline{\mathbb{Q}}^{Aut_K(\overline{\mathbb{Q}})}$. By the Galois correspondence, $K = \psi^{-1}(\psi(K)) = \psi^{-1}(Aut_K(\overline{\mathbb{Q}})) = \overline{\mathbb{Q}}^{Aut_K(\overline{\mathbb{Q}})}$. It follows that $e_n(T_1, T_2) \in K$. By Corollary 5.3, we know that $e_n(T_1, T_2)$ is a primitive $n$th root of unity, and hence it generates $\mu_n$. We conclude $\mu_n \subseteq K$. ∎

For the rest of this section we will again restrict to an elliptic curve $E/\mathbb{Q}$ and a field $K$ that is a Galois extension of $\mathbb{Q}$ containing only finitely many roots of unity. We have the following lemma.

**Lemma 5.5** [1, Lemma 4.3] *Let* $E/\mathbb{Q}$ *and let* $K$ *be as in Theorem 3.13. Then* $E(\overline{\mathbb{Q}})[n] \subseteq E(K)$ *for only finitely many* $n \in \mathbb{N}$*.*

*Proof.* Assume $E(\overline{\mathbb{Q}})[n] \subseteq E(K)$ for an infinite number of $n \in \mathbb{N}$. Then by Corollary 5.4, for all these $n$, $\mu_n \subseteq K$. Since $\mu_n$ is cyclic for all $n \in \mathbb{N}$, each $\mu_n$ contains an element of exactly order $n$. Therefore there is at least one unique root of unity for each number $n$. It follows that $K$ contains an infinite number of roots of unity, which contradicts the initial assumption. We conclude that $E(\overline{\mathbb{Q}})[n] \subseteq E(K)$ for only finitely many $n$. ∎

It follows from Lemma 5.5 that $E(K)[p] = E(\overline{\mathbb{Q}})[p]$ for only finitely many prime numbers $p$. Hence there are only finitely many primes $p$ for which $E(K)[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$.

Next we would like to characterize when $E(K)[p]$ can be isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and for this we will rely on a result about $n$-isogenies. The next result gives a restriction on the rational $n$-isogenies that can occur for elliptic curves defined over $\mathbb{Q}$. It is based on results by Mazur [18] and Kenku [12, 14, 13, 15].

**Theorem 5.6** [1, Thm 4.4] *Let $E/\mathbb{Q}$ be an elliptic curve with a rational $n$-isogeny. Then either $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$.*

We will use this theorem to find a restriction on when $E(K)[p]$ can be isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

**Lemma 5.7** [1, Lemma 4.5] *Let $E/\mathbb{Q}$, and let $K$ be as in Theorem 3.13. If $E(K)[p] \cong \mathbb{Z}/p\mathbb{Z}$, then $p \leq 163$.*

*Proof.* We will prove this lemma by first showing that there exists a rational $p$-isogeny of $E$, and then applying Theorem 5.6.

First of all, $E(K)[p]$ is a subgroup of $E(\overline{\mathbb{Q}})$, so by Proposition 2.9 there is a separable isogeny $\alpha$ of $E$ with $ker(\alpha) = E(K)[p]$. By assumption, $E(K)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Therefore $ker(\alpha)$ is a cyclic group of order $p$. Because $\alpha$ is separable, Proposition 2.7 implies that $deg(\alpha) = p$. Hence $\alpha$ is a $p$-isogeny.

In Section 4.2, we showed that the group $E(\overline{\mathbb{Q}})[p]$ is stable under the action of $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, meaning that the action permutes the elements in $E(\overline{\mathbb{Q}})[p]$. Because $\mathbb{Q} \subseteq K$ is Galois, a completely analogous argument shows that $E(K)[p]$ is stable under the action of $Gal(K/\mathbb{Q})$. Hence $E(K)[p] = ker(\alpha)$ is Galois-stable. Proposition 2.9 implies that we can choose $\alpha$ such that it is defined over $\mathbb{Q}$, and hence rational. By Theorem 5.6, we obtain that $p \leq 163$. ∎

We will use Lemma 5.5 and 5.7 to finalize the second part of our proof of Theorem 3.13.

**Lemma 5.8** *Let $E/\mathbb{Q}$, let $K$ be as in Theorem 3.13. Then $E(K)[p^\infty]$ is nontrivial for only finitely many primes $p$.*

*Proof.* By assumption $K$ contains only a finite number of roots of unity, so we can define the number $m$ to be the maximum of the orders of roots of unity in $K$. Furthermore define $n = max\{m, 163\}$.
Let $p \geq n$ be prime. Since $p \geq m$, $K$ does not contain a root of unity of order $p$. Hence $\mu_p \nsubseteq K$. From the contrapositive of Corollary 5.4, it follows that $E(\overline{\mathbb{Q}})[p] \nsubseteq E(K)$. Hence $E(K)[p] \neq E(\overline{\mathbb{Q}})[p]$, and $E(K)[p] \ncong (\mathbb{Z}/p\mathbb{Z})^2$. Recall that this means that either $E(K)[p] \cong \mathbb{Z}/p\mathbb{Z}$ or $E(K)[p]$ is trivial. Now from Lemma 5.7, it follows that if $E(K)[p] \cong \mathbb{Z}/p\mathbb{Z}$, $p$ must be less than or equal to 163. Because this is not the case, $E(K)[p]$ is trivial.

We will now show that this implies that also the $p$-primary component of $E(K)$ is trivial. For assume there is some $P \in E(K)[p^\infty]$ such that $P \neq \infty$. Then $[p^e]P = \infty$ for some $e \in \mathbb{N}$, where $p^e$ is the order of $P$. It follows that $[p]([p^{e-1}]P) = \infty$, so $[p^{e-1}]P \in E(K)[p]$. Now either $[p^{e-1}]P \neq \infty$, which contradicts the fact that $E(K)[p]$ is trivial, or $[p^{e-1}]P = \infty$, which contradicts the fact that $p^e$ is the order of $P$. Hence such a $P$ can not exist and we conclude that $E(K)[p^\infty]$ is trivial.

The $p$-primary component of $E(K)_{tors}$ is therefore trivial for all $p > n$. ∎

## 5.3 Finiteness of $p$-primary components

The last part in proving Theorem 3.13 will be showing that all $p$-primary components that are nontrivial have a finite number of elements. We will again make use of Theorem 5.6.

**Lemma 5.9** [1, Lemma 4.6] *Let $E/\mathbb{Q}$, let $K$ be as in Theorem 3.13. Let $p$ be prime, and let $k$ be the largest integer for which $E(\overline{\mathbb{Q}})[p^k] \subseteq E(K)$. If $E(K)_{tors}$ contains a subgroup isomorphic to $\mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^j\mathbb{Z}$ with $j \geq k$, then $E$ admits a rational $p^{j-k}$-isogeny. Moreover,*

$$j-k \leq \begin{cases} 4 & \text{if } p=2, \\ 3 & \text{if } p=3, \\ 2 & \text{if } p=5, \\ 1 & \text{if } p \in \{7,11,13,17,19,43,67,163\}, \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* Because $E(K)_{tors}$ contains a subgroup isomorphic to $\mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^j\mathbb{Z}$, we can choose $Q \in E(K)$ a point of order $p^j$. Recall from Section 2.4 that we can find a $\mathbb{Z}/p^j\mathbb{Z}$-basis for $E(\overline{\mathbb{Q}})[p^j]$. Let $\{P, Q\}$ be such a basis.
Let $\sigma \in G_{\mathbb{Q}}$. By the action of the Galois representation (Section 4.2), $\sigma(Q) \in E(\overline{\mathbb{Q}})[p^j]$. We can thus write $\sigma(Q) = [a]P + [b]Q$ for some $a, b \in \mathbb{N}$. Rearranging gives $[a]P = \sigma(Q) - [b]Q$. Recall that $\mathbb{Q} \subseteq K$ is Galois, which implies from the Galois correspondence that $\sigma(K) = K$ and hence $\sigma(Q) \in E(K)$. It follows that $[a]P \in E(K)$.

Let $t$ be the power of $p$ in the prime factorization of $a$. Then $[a]P \in E(K)[p^{j-t}]$. Note that $[p^t]Q \in E(K)[p^{j-t}]$ as well. Because $P$ and $Q$ are linearly independent, so are $[a]P$ and $[p^t]Q$, and hence $\{[a]P, [p^t]Q\}$ is a basis for $E(\overline{\mathbb{Q}})[p^{j-t}]$. Both basis elements are in $E(K)$, so we conclude that $E(\overline{\mathbb{Q}})[p^{j-t}] \subseteq E(K)$. It follows from the definition of $k$ that $j - t \leq k$.
We obtain $j - k \leq t$, and hence $p^{j-k}$ is a divisor of $a$. We can write $a = p^{j-k}c$ for some $c \in \mathbb{N}$.

We can show that $E$ admits a rational $p^{j-k}$ isogeny by constructing a subgroup of $E(\overline{\mathbb{Q}})$ that is cyclic of with degree $p^{j-k}$, and furthermore Galois-stable.
Consider the subgroup $\langle [p^k]Q \rangle$. By Proposition 2.9, there exists a separable isogeny $\alpha$ of $E$ with $ker(\alpha) = \langle [p^k]Q \rangle$. First of all note that $\langle [p^k]Q \rangle$ is cyclic by definition. Secondly, because $Q$ has order $p^j$, we know that $[p^k]Q$ has order $p^{j-k}$, so $\langle [p^k]Q \rangle$ has $p^{j-k}$ elements. Proposition 2.7 then implies that $deg(\alpha) = p^{j-k}$. This shows that $\alpha$ is a $p^{j-k}$-isogeny.
To show Galois-stability, let $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Then

$$\begin{aligned} \sigma([p^k]Q) &= [p^k]\sigma(Q) && (\text{$[p^k]$ is defined over } \mathbb{Q}) \\ &= [p^k]([a]P + [b]Q) \\ &= [p^k]([p^{j-k}c]P + [b]Q) \\ &= [p^j c]P + [bp^k]Q \\ &= [b][p^k]Q \in \langle [p^k]Q \rangle && (P \in E(\overline{\mathbb{Q}})[p^j]) \end{aligned}$$

So $\langle [p^k]Q \rangle$ is indeed Galois-stable. This implies by Proposition 2.9 that we can choose $\alpha$ as a rational $p^{j-k}$-isogeny.

Theorem 5.6 now restricts the possible values of $p^{j-k}$. The restrictions on $j-k$ follow directly from the possibilities listed in this theorem. ∎

Lemma 5.9 will be useful in showing the last ingredient to our proof of Theorem 3.13, showing that all $p$-primary components of $E(K)_{tors}$ are finite.

**Lemma 5.10** *Let $E/\mathbb{Q}$, and let $K$ be as in Theorem 3.13. Let $m$ be the maximum order of a root of unity in $K$, and let $n = max\{m, 163\}$. Then for all primes $p \leq n$, $E(K)[p^\infty]$ is finite.*

*Proof.* Let $p \leq n$ be prime. First of all, note that

$$E(K)[p] \subseteq E(K)[p^2] \subseteq \cdots \subseteq E(K)[p^i] \subseteq \cdots \subseteq E(K)[p^\infty].$$

Furthermore each $E(K)[p^i]$ is finite (Theorem 2.10). We want to show that $E(K)[p^\infty] \subseteq E(K)[p^i]$ for some $i \in \mathbb{N}$.

Let $k$ be the largest integer for which $E(\overline{\mathbb{Q}})[p^k] \subseteq E(K)$ (which exists by Lemma 5.5). For this $k$, we have $E(K)[p^k] \cong (\mathbb{Z}/p^k\mathbb{Z})^2$. Let us assume that there is some $j > k$, such that

$$E(K)[p^{j-1}] \neq E(K)[p^j] \tag{8}$$

(if this is not the case, $E(K)[p^\infty] \subseteq E(K)[p^k]$ and we are done). For this $j$, we have

$$(\mathbb{Z}/p^k\mathbb{Z})^2 \subsetneq E(K)[p^j] \subsetneq (\mathbb{Z}/p^j\mathbb{Z})^2. \tag{9}$$

The first set inclusion follows from (8) and the second one follows because $E[p^j] \nsubseteq E(K)$ by definition of $k$. The $\subseteq$ symbol in (9) is taken in a broad sense, in this case meaning "is isomorphic to a subset of". We will use this convention more often without explicitly mentioning it.

It follows from (9) that $E(K)[p^j]$ will be of the form $\mathbb{Z}/p^i\mathbb{Z} \oplus \mathbb{Z}/p^l\mathbb{Z}$ for some $k \leq i \leq j$ and $k \leq l \leq j$. Note that this means $E(K)[p^j] \subseteq E(K)[p^{max\{i,l\}}]$. It follows from (8) that either $i$ or $l$ must be equal to $j$. Because the other number is greater than or equal to $k$, we obtain

$$\mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^j\mathbb{Z} \subseteq E(K)[p^j].$$

This means the conditions for Lemma 5.9 are met, and this lemma says that $j - k \leq 4$. So for all $j > k + 4$ we have $E(K)[p^{j-1}] = E(K)[p^j]$ and hence $E(K)[p^\infty] \subseteq E(K)[p^{k+4}]$. This shows that the $E(K)[p^\infty]$ is finite. ∎

Taking together (7), Lemma 5.8 and Lemma 5.10, we can derive that $E(K)_{tors}$ is isomorphic to a finite direct sum of finite groups. We conclude that $E(K)_{tors}$ is finite.

Note that the number of elements in $E(K)_{tors}$ is equal to the product of the number of elements in each $p$-primary component $E(K)[p^\infty]$. The number of nontrivial p-primary components is bounded by $n$ (as defined in the proof of Lemma 5.8). Note that the value of $n$ only depends on the chosen field $K$. From the proof of Lemma 5.10, it follows that for each prime $p \leq n$, we have $E(K)[p^\infty] \subseteq E(K)[p^{k+4}]$. We also have $\#E(K)[p^{k+4}] \leq \#E(\overline{\mathbb{Q}})[p^{k+4}] = \#(\mathbb{Z}/p^{k+4}\mathbb{Z})^2 = p^{2(k+4)}$. The number of elements in $E(K)[p^\infty]$ is therefore bounded by $p^{2k+8}$. The maximum value of this $k$ over primes $p \leq n$, is bounded by the value of $m$ (the maximum of the orders of roots of unity in $K$) through Proposition 5.4. The number $m$ in turn only depends on the field $K$. It follows that a uniform bound on the order of $E(K)_{tors}$ can be given, depending only on the field $K$. This bound actually only depends on the maximum of the orders of roots of unity in $K$. This concludes the proof of Theorem 3.13.

# 6 General Approach

The main problem we have been talking about until now is finding the torsion subgroup for elliptic curves with points in several extensions of $\mathbb{Q}$. In Section 3, we provided an overview of some results of this type that are known today. In this section, a general approach to problems of this nature will be described, which could be helpful to tackle similar problems in the future.

## 6.1 Characterizing the torsion subgroup using the Galois representation

We will consider an algebraic field extension $\mathbb{Q} \subseteq K$ and an elliptic curve $E/K$ for which we know that the torsion subgroup $E(K)_{tors}$ is finite. As an example, we know from Section 3.1 that $K$ can be any number field. Similarly, by Theorem 3.13 we can choose $K$ to be a Galois extension of $\mathbb{Q}$ containing finitely many roots of unity.

Under the assumption that $E(K)_{tors}$ is finite, we already saw in the proof of Theorem 3.2 that if $M = exp(E(K)_{tors})$, we have $E(K)_{tors} \subseteq E(K)[M]$. From the definition of the torsion subgroup, we also have $E(K)[M] \subseteq E(K)_{tors}$. We can conclude $E(K)_{tors} = E(K)[M]$. The problem of describing the torsion subgroup of an elliptic curve has now reduced to describing the $M$-torsion subgroup for some natural number $M$.

In this section, we will make use of the Galois representation to obtain a description of the torsion subgroup $E(K)_{tors}$. Recall the map $\rho_{E,n}$ from (6), whose image lies in $Aut(E(\overline{\mathbb{Q}})[n])$. For practicality, we also define a map

$$\rho'_{E,n} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}). \tag{10}$$

This map is equal to $\rho_{E,n}$ composed with the isomorphism $\psi_{E,n}$, and can also be referred to as a Galois representation.

Let us consider $G_K := Gal(\overline{\mathbb{Q}}/K)$, which is a subgroup of $G_{\mathbb{Q}}$. It follows from the Galois correspondence that $K = \overline{\mathbb{Q}}^{G_K}$. Using this equality, we can give another description of the $M$-torsion subgroup of $E(K)$. Namely, $E(K)[M]$ consists of the points in $E(\overline{\mathbb{Q}})[M]$ that have coordinates in $K$, so coordinates that are fixed by $G_K$. This means that $E(K)[M]$ is the subgroup of elements that are fixed by $\rho_{E,M}(G_K)$. We can write this as

$$E(K)[M] = \left(E(\overline{\mathbb{Q}})[M]\right)^{\rho_{E,M}(G_K)}. \tag{11}$$

Using Theorem 2.10 and the fact that $E(K)_{tors} = E(K)[M]$ we obtain

$$E(K)_{tors} \cong \left((\mathbb{Z}/M\mathbb{Z})^2\right)^{\rho'_{E,M}(G_K)}. \tag{12}$$

$E(K)_{tors}$ is therefore isomorphic to a subgroup of $(\mathbb{Z}/M\mathbb{Z})^2$, as we already saw in the proof of Theorem 3.2. The relation in (12) gives a description of this subgroup using the Galois representation.

## 6.2 Characterizing the n-torsion subgroup

For algebraic field extensions $\mathbb{Q} \subseteq K$, we would now like to find some strategies for characterizing $E(K)[n]$ as a subgroup of $(\mathbb{Z}/n\mathbb{Z})^2$ for arbitrary $n$. This information can be used to describe $E(K)_{tors}$.

First of all, we give a condition under which $E(K)[n]$ is equal to the full torsion group.

**Proposition 6.1** *Let $K$ be an algebraic extension of $\mathbb{Q}$, and let $E/K$ be an elliptic curve. Let $n \in \mathbb{N}$. Then*

$$E(K)[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 \iff \rho'_{E,n}(G_K) = \{\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\}.$$

*Proof.* Recall that $E(K)[n] \subseteq E(\overline{\mathbb{Q}})[n]$ and $E(\overline{\mathbb{Q}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. It follows that

$$\begin{aligned}
E(K)[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 &\iff E(\overline{\mathbb{Q}})[n] = E(K)[n] \\
&\iff E(\overline{\mathbb{Q}})[n] = (E(\overline{\mathbb{Q}})[n])^{\rho_{E,n}(G_K)} && \text{(by (11))} \\
&\iff \text{ for all } \sigma \in \rho_{E,n}(G_K), \text{ we have } \sigma = id_{E(\overline{\mathbb{Q}})[n]} \\
&\iff \rho_{E,n}(G_K) = \{id_{E(\overline{\mathbb{Q}})[n]}\} \\
&\iff \rho'_{E,n}(G_K) = \{\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\}.
\end{aligned}$$

∎

Next, we can give a characterization of the cases for which $E(K)[n]$ contains an element of order $n$. In other words, $E(K)[n]$ will have at least $n$ elements. In the following, we will write elements of $(\mathbb{Z}/n\mathbb{Z})^2$ as column vectors, such that we can apply matrices of $GL_2(\mathbb{Z}/n\mathbb{Z}) = Aut((\mathbb{Z}/n\mathbb{Z})^2)$ by multiplication from the right.

The following characterization will rely on the concept of a stabilizer subgroup.

**Definition 6.2** *Let $G$ be a group that acts on a set $X$. Then for $x \in X$, the **stabilizer of** $x$ **by** $G$ is defined as $Stab(x) = \{g \in G \mid g(x) = x\}$.*

First of all, we will choose the element $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) \in (\mathbb{Z}/n\mathbb{Z})^2$ as a particular element of order $n$. We will show that the stabilizer of $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ by $GL_2(\mathbb{Z}/n\mathbb{Z})$ is equal to the following subgroup:

$$B_n := \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Z}/n\mathbb{Z} \right\} \cap GL_2(\mathbb{Z}/n\mathbb{Z}). \tag{13}$$

To see this, let $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ be any matrix in $GL_2(\mathbb{Z}/n\mathbb{Z})$. Then $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ is in the stabilizer of $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ if and only if we have

$$\begin{aligned}
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
\begin{pmatrix} a \\ c \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}.
\end{aligned}$$

Hence we must have $a = 1$ and $c = 0$. By definition, this is equivalent to stating $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in B_n$.

We can give the following classification about elements of order $n$:

**Proposition 6.3** *Let $K$ be an algebraic field extension of $\mathbb{Q}$. Let $E/K$ be an elliptic curve, and let $n \in \mathbb{N}$. Then $E(K)[n]$ contains an element of order $n \iff \rho'_{E,n}(G_K)$ is contained in a conjugate subgroup of $B_n$.*

To show this, we will need two intermediate results, that require the concept of a transitive group action.

**Definition 6.4** *A permutation group $G$ on $\{1, \dots n\}$ is called **transitive** if for all $x, y \in \{1, \dots n\}$ there is a $\sigma \in G$ such that $\sigma(x) = y$.*

**Lemma 6.5** *The group $GL_2(\mathbb{Z}/n\mathbb{Z})$ acts transitively on the elements of order $n$ in $(\mathbb{Z}/n\mathbb{Z})^2$.*

*Proof.* First of all, note that the elements of $GL_2(\mathbb{Z}/n\mathbb{Z})$ are homomorphisms of $(\mathbb{Z}/n\mathbb{Z})^2$, and hence they send elements of order $n$ to elements of order $n$.
Let $\binom{a}{b} \in (\mathbb{Z}/n\mathbb{Z})^2$ be arbitrary. Let us denote by $[a, b] = \{xa + yb \mid x, y \in \mathbb{Z}/n\mathbb{Z}\}$ the ideal of $\mathbb{Z}/n\mathbb{Z}$ generated by $a, b \in \mathbb{Z}/n\mathbb{Z}$. (we deviate from standard notation of ideals to avoid possible confusion with elements in $(\mathbb{Z}/n\mathbb{Z})^2$). We know that all ideals of $\mathbb{Z}$ are of the form $m\mathbb{Z}$ for some $m \in \mathbb{N}$. The third isomorphism theorem for rings implies that all ideals of $\mathbb{Z}/n\mathbb{Z}$ are then of the form $m\mathbb{Z}/n\mathbb{Z}$, for some $m \in \mathbb{N}$ such that $m \mid n$. Therefore we can write $[a, b] = [m]$ for some $m \mid n$. Let us denote by $d$ the order of $\binom{a}{b}$. First note that

$$[da, db] = [d][a, b] = [d][m] = [dm]$$

as ideals of $\mathbb{Z}/n\mathbb{Z}$. We then have:

$$\begin{aligned} d\binom{a}{b} = \binom{0}{0} &\iff da \equiv db \equiv 0 \bmod n \\ &\iff [da, db] = [0] \\ &\iff [dm] = [0] \\ &\iff dm \equiv 0 \bmod n. \end{aligned}$$

The order of $\binom{a}{b}$ in $(\mathbb{Z}/n\mathbb{Z})^2$ is therefore equal to the order of $m$ in $\mathbb{Z}/n\mathbb{Z}$. This is the smallest number $d$ such that $dm \mid n$. Because $m \mid n$, we obtain $d = \frac{n}{m}$.
Now if $\binom{a}{b}$ is an element of order $n$, this implies that we have $m = 1$ and hence $[a, b] = [1]$. By definition of an ideal, there exist $x, y \in \mathbb{Z}/n\mathbb{Z}$ such that $xa + yb \equiv 1 \bmod n$.

The matrix $M_{ab} = \left(\begin{smallmatrix} a & -y \\ b & x \end{smallmatrix}\right)$ is an element of $GL_2(\mathbb{Z}/n\mathbb{Z})$, because its determinant is $ax + by \equiv 1 \in \mathbb{Z}/n\mathbb{Z}^\times$ and hence it is invertible. This matrix maps the element $\binom{1}{0}$ to $\binom{a}{b}$. Hence we know that for any two elements $\binom{a}{b}, \binom{c}{d} \in (\mathbb{Z}/n\mathbb{Z})^2$ of order $n$, we have $\binom{c}{d} = M_{cd}M_{ab}^{-1}\binom{a}{b}$. This implies that $GL_2(\mathbb{Z}/n\mathbb{Z})$ acts transitively on the elements of order $n$. ∎

We will proceed by showing that the stabilizer subgroups of elements of order $n$ are exactly the conjugate subgroups of $B_n$.

**Proposition 6.6** *Let $P, Q \in (\mathbb{Z}/n\mathbb{Z})^2$ be two elements of order $n$. Then their stabilizers are conjugate subgroups.*
*Conversely, if $G$ is the stabilizer of some element of order $n$, then all conjugate subgroups of $G$ are stabilizers of some element of order $n$ in $(\mathbb{Z}/n\mathbb{Z})^2$.*

*Proof.* Let $P, Q \in (\mathbb{Z}/n\mathbb{Z})^2$ be two elements of order $n$. Because $GL_2(\mathbb{Z}/n\mathbb{Z})$ acts transitively on the elements of order $n$ (Lemma 6.5), there exists a matrix $M \in GL_2(\mathbb{Z}/n\mathbb{Z})$ such that $Q = MP$. We have

$$\begin{aligned} \sigma \in Stab(P) &\iff \sigma P = P \\ &\iff \sigma M^{-1} Q = P \\ &\iff M\sigma M^{-1} Q = Q \\ &\iff M\sigma M^{-1} \in Stab(Q). \end{aligned}$$

It follows that $Stab(Q) = MStab(P)M^{-1}$.

For the converse statement, let $Stab(P)$ be the stabilizer of some element $P \in (\mathbb{Z}/n\mathbb{Z})^2$ of order $n$. Let $M \in GL_2(\mathbb{Z}/n\mathbb{Z})$ be arbitrary. Recall that $MP$ is again an element of order $n$. We look at its stabilizer:

$$\begin{aligned} \sigma \in Stab(MP) &\iff \sigma MP = MP \\ &\iff M^{-1}\sigma MP = P \\ &\iff M^{-1}\sigma M \in Stab(P) \\ &\iff \sigma \in MStab(P)M^{-1} \end{aligned}$$

We obtain that a conjugate subgroup $MStab(P)M^{-1}$ is the stabilizer of the element $MP \in (\mathbb{Z}/n\mathbb{Z})^2$. ∎

We can use this result to formulate the proof of Proposition 6.3.

*Proof of Proposition 6.3.* First of all, recall from (11) and (12) that

$$E(K)[n] = \left(E(\overline{\mathbb{Q}})[n]\right)^{\rho_{E,n}(G_K)} \cong \left((\mathbb{Z}/n\mathbb{Z})^2\right)^{\rho'_{E,n}(G_K)}. \tag{14}$$

($\Rightarrow$) It follows from (14) that $E(K)[n]$ contains an element of order $n \iff \left((\mathbb{Z}/n\mathbb{Z})^2\right)^{\rho'_{E,n}(G_K)}$ contains an element of order $n$. Let us call this element $P$. $\rho'_{E,n}(G_K)$ fixes this element, meaning $\rho'_{E,n}(G_K) \subseteq Stab(P)$. Proposition 6.6 implies that $Stab(P)$ is conjugate to $B_n$, because $B_n$ stabilizes an element of order $n$.

($\Leftarrow$) Now assume $\rho'_{E,n}(G_K) \subseteq MB_nM^{-1}$ for some conjugate subgroup of $B_n$, where $M \in GL_2(\mathbb{Z}/n\mathbb{Z})$. Then by Proposition 6.6 we know that $MB_nM^{-1}$ is the stabilizer of some element $P \in (\mathbb{Z}/n\mathbb{Z})^2$ of order $n$. hence $P$ is fixed by the automorphisms of $\rho'_{E,n}(G_K)$, and it follows that $P \in \left((\mathbb{Z}/n\mathbb{Z})^2\right)^{\rho'_{E,n}(G_K)}$. Using (14) we conclude that $E(K)[n]$ also contains an element of order $n$.

∎

The results in Propositions 6.1 and 6.3 show how the Galois representation can be used to obtain information about the $n$-torsion subgroup $E(K)[n]$.

## 6.3 Application to prime torsion subgroups

A particular case that we can consider is that of $n$ being a prime number, which we instead will denote by $p$. As mentioned in Section 5.2, $(\mathbb{Z}/p\mathbb{Z})^2$ only has 3 distinct isomorphism classes of subgroups: the full group, the trivial group and subgroups isomorphic to $\mathbb{Z}/p\mathbb{Z}$. In the following proposition, we classify under what conditions $E(K)[p]$ is in each of the three possible isomorphism classes of subgroups.

**Theorem 6.7** *Let $K$ be an algebraic field extension of $\mathbb{Q}$. Let $E/K$ be an elliptic curve, and let $p$ be a prime number. Then*

$$E(K)[p] \cong \begin{cases} (\mathbb{Z}/p\mathbb{Z})^2 & \iff \rho'_{E,p}(G_K) = \{\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\} \\ \mathbb{Z}/p\mathbb{Z} & \iff \rho'_{E,p}(G_K) \text{ is contained in a conjugate subgroup of } B_p, \\ & \quad \text{but } \rho'_{E,p}(G_K) \neq \{\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\} \\ \{0\} & \iff \rho'_{E,p}(G_K) \text{ is not contained in any conjugate subgroup of } B_p. \end{cases}$$

*Proof.*

1. The first equivalence follows directly from Proposition 6.1.
2. For $E(K)[p]$ to be isomorphic to $\mathbb{Z}/p\mathbb{Z}$, we know it must contain an element of order $p$. From Proposition 6.3, we know that this is the case if and only if $\rho'_{E,p}(G_K)$ is contained in a conjugate subgroup of $B_p$. Now there are only two possibilities for which $E(K)[p]$ contains an element of order $p$: either $E(K)[p] \cong (\mathbb{Z}/p\mathbb{Z})$ or $E(K)[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$. We can exclude the second possibility, according to item 1 of this proposition, by requiring $\rho'_{E,p}(G_K) \neq \{\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\}$. This shows the second equivalence.
3. Note that $\{0\}$ is the only isomorphism class of subgroups of $(\mathbb{Z}/p\mathbb{Z})^2$ that does not contain an element of order $p$. We can therefore conclude that

   $$E(K)[p] \cong \{0\} \iff E(K)[p] \text{ does not contain an element of order } p.$$

   Proposition 6.3 then implies the required equivalence.

∎

If we are looking at elliptic curves over a specific field extension of $\mathbb{Q}$, and we know something about the Galois representation corresponding to this curve, the above results can be used in finding a classification of the corresponding torsion subgroup. We can illustrate this with a relatively simple example, namely the case $p = 2$.

Let us look at the 2-torsion subgroup of an elliptic curve. In this case, the group $GL_2(\mathbb{Z}/2\mathbb{Z})$ is isomorphic to $S_3$, the symmetric group on three elements. Furthermore, note that $B_2 = \{\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)\} \cong \mathbb{Z}/2\mathbb{Z}$. Let us consider a field $K$ and some elliptic curve $E/K$. Then the image of $G_K$ under the Galois representation is isomorphic to a subgroup of $S_3$. $S_3$ has four isomorphism classes of subgroups, and each possibility will be considered below.

1. If $\rho'_{E,p}(G_K) \cong S_3$, it is equal to the full group $GL_2(\mathbb{Z}/2\mathbb{Z})$. We then know that it is not contained in any conjugate subgroup of $B_2$, because these are all isormorphic to $\mathbb{Z}/2\mathbb{Z}$. Hence from Theorem 6.7 we conclude that $E(K)[2] = \{\infty\}$, so $E(K)$ contains no elements of order 2.

2. If $\rho'_{E,p}(G_K) \cong A_3$, we can use the same reasoning to conclude that $E(K)[2] = \{\infty\}$.

3. If $\rho'_{E,p}(G_K) \cong \mathbb{Z}/2\mathbb{Z}$, it is equal to a conjugate subgroup of $B_2$. Hence Theorem 6.7 implies that $E(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$, and there is exactly one element of order 2 in $E(K)$.

4. Finally, if $\rho'_{E,p}(G_K) \cong \{0\}$, then we immediately obtain from Theorem 6.7 that $E(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

# 7 Application to the compositum of prime degree extensions

We would now like to apply the theory introduced in the previous section to prove a result about a particular field extension of $\mathbb{Q}$. The field we will be looking at is the compositum of all prime degree extensions of $\mathbb{Q}$:

$$K := \mathbb{Q}(\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] \text{ is prime}\}).$$

This is an algebraic field extension of $\mathbb{Q}$. The result we will prove about this field will be stated in Section 7.5. It relies on a set of assumptions that will not be proven in this report. To formulate the statement and these assumptions, first some extra concepts need introduction.

## 7.1 Serre's uniformity problem

The first conjecture that we will assume to be satisfied is proposed by Serre, and concerns the Galois representation for prime power torsion groups.

The statement mentions the concept of complex multiplication, which we will briefly explain. Recall that the multiplication-by-$n$ map is an endomorphism of an elliptic curve $E$ for all $n \in \mathbb{Z}$. If there exist additional endomorphisms of $E$ besides these multiplication-by-$n$ maps, the curve is said to have **complex multiplication**.

**Conjecture 7.1 (Serre's Uniformity Problem)** [22] *Let $p > 37$ be prime. Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then the Galois representation $\rho'_{E,p^i}$ is surjective for all powers $i \in \mathbb{N}$:*

$$\rho'_{E,p^i}(G_{\mathbb{Q}}) = GL_2(\mathbb{Z}/p^i\mathbb{Z}).$$

There are only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over $\mathbb{Q}$ with complex multiplication [23, p. 427]. Therefore this conjecture only excludes a relatively small amount of possibilities, which makes the result very powerful.

The conjecture has neither been verified nor disproved at this moment, but a lot of partial results have already been found and there is continued interested in the problem [7].

## 7.2 Composition series

To formulate the second assumption of our theorem, we will first need another concept. Let us consider a finite group $G$. We can define a composition series of $G$, which is a way to break up $G$ into a series of subgroups.

**Definition 7.2** *A group $G \neq \{0\}$ is called **simple** if $\{0\}$ and $G$ are the only normal subgroups of $G$.*

**Definition 7.3** *Let $G$ be a finite group. Consider a sequence of subgroups*

$$\{0\} = N_k \lhd N_{k-1} \lhd \cdots \lhd N_1 \lhd N_0 = G$$

*This sequence $(N_i)_{i=0}^k$ is called a **composition series of $G$** if for all $i = 0, \ldots, k-1$:*

1. *$N_{i+1}$ a normal subgroup of $N_i$,*

2. *$N_{i+1}/N_i$ is a simple group.*

*We call the groups $N_{i+1}/N_i$ the **composition factors** of $G$. The number $k$ is called the **composition length** of the composition series.*

For all finite groups, a composition series exists. A composition series is the longest chain of mutually normal subgroups that can be constructed for a group $G$. Namely, because $N_{i+1}/N_i$ is simple, there is no subgroup $H$ such that $\{0\} \cong N_i/N_i \lhd H/N_i \lhd N_{i+1}/N_i$. The third isomorphism theorem implies that it is impossible to find a group $H$ for which $N_{i+1} \lhd H \lhd N_i$. A composition series is characteristic for a group in the sense of the following theorem, due to Jordan and Hölder.

**Theorem 7.4 (Jordan-Hölder Theorem)** *Let $G$ be a group. Then any two composition series of $G$ have the same composition length, and the same collection of factor groups (up to isomorphism and ordering).*

A useful way to start constructing a composition series of $G$ is looking for any normal subgroup $N$ of $G$. This breaks up the problem into two smaller problems. The first problem is finding the composition series of the smaller group $N$:

$$\{0\} \lhd H_{l-1} \lhd \cdots \lhd H_1 \lhd N.$$

Secondly, find a composition series of $G/N$:

$$\{0\} \cong N/N \lhd N_{k-1}/N \lhd \cdots \lhd N_1/N \lhd G/N.$$

By the third isomorphism theorem for groups, $N_{i+1}/N \lhd N_i/N$ implies that $N_{i+1} \lhd N_i$. The same theorem implies that if $(N_{i+1}/N)/(N_i/N)$ is simple then also $N_{i+1}/N_i$ is simple, because these groups are isomorphic. We can take all information together and conclude that

$$\{0\} \lhd H_{l-1} \lhd \cdots \lhd H_1 \lhd N \lhd N_{k-1} \lhd \cdots \lhd N_1 \lhd G$$

is a composition series for $G$. The composition factors of $G$ are the composition factors of $N$ together with those of $G/N$.

## 7.3 Composition series of $GL_2(\mathbb{Z}/p\mathbb{Z})$

We are interested in finding the composition series of $GL_2(\mathbb{Z}/p\mathbb{Z})$ for a prime $p$, which will be useful later on. A good start is by considering the subgroup $SL_2(\mathbb{Z}/p\mathbb{Z})$, consisting of all matrices with determinant 1. This is a normal subgroup of $GL_2(\mathbb{Z}/p\mathbb{Z})$, because it is the kernel of the map

$$det : GL_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

that assigns to each matrix its determinant. Because the determinant map is surjective, it also follows that $GL_2(\mathbb{Z}/p\mathbb{Z})/SL_2(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

We now have $SL_2(\mathbb{Z}/p\mathbb{Z}) \lhd GL_2(\mathbb{Z}/p\mathbb{Z})$. The next step in finding the composition series, is finding the composition series of $SL_2(\mathbb{Z}/p\mathbb{Z})$. We would like to repeat the process and find a normal subgroup. A starting point is to find the center of $SL_2(\mathbb{Z}/p\mathbb{Z})$. The **center** of a

group $G$ is defined as the group $Z(G) := \{h \in G \mid \forall g \in G, hg = gh\}$. This is by construction always a normal subgroup of $G$. The center of $SL_2(\mathbb{Z}/p\mathbb{Z})$ [9, Thm 14.3] is:

$$Z(SL_2(\mathbb{Z}/p\mathbb{Z})) = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\}.$$

We define the projective special linear group $PSL_2(\mathbb{Z}/p\mathbb{Z}) := SL_2(\mathbb{Z}/p\mathbb{Z})/Z(SL_2(\mathbb{Z}/p\mathbb{Z}))$. For all primes $p > 3$, this group is simple [2]. Because $Z(SL_2(\mathbb{Z}/p\mathbb{Z})) \cong \mathbb{Z}/2\mathbb{Z}$ is simple as well (the group of two elements has only two subgroups), for $p \geq 3$ the composition series of $SL_2(\mathbb{Z}/p\mathbb{Z})$ is completely determined as $\{id\} \lhd Z(SL_2(\mathbb{Z}/p\mathbb{Z})) \lhd SL_2(\mathbb{Z}/p\mathbb{Z})$. The composition factors are $\mathbb{Z}/2\mathbb{Z}$ and $PSL_2(\mathbb{Z}/p\mathbb{Z})$.

For $p = 2$, we have $PSL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$, which is the symmetric group on 3 elements. The subgroup $A_3$ is the alternating group on 3 elements. This is a normal subgroup of $S_3$, and because it has three elements, $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ is simple. The factor group $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ is also simple. We thus obtain the composition series $\{0\} \lhd A_3 \lhd S_3$ with composition factors $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.
For $p = 3$ we have $PSL_2(\mathbb{Z}/3\mathbb{Z}) \cong A_4$, the alternating group on 4 elements. To find the composition series of this group, first of all consider the normal subgroup

$$V_4 = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

The factor group $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ is simple. Now consider the subgroup $\{(), (1,2)(3,4)\} \subseteq V_4$. This is a normal subgroup because $V_4$ is abelian. Both remaining factor groups are simple, because $\{(), (1,2)(3,4)\} \cong V_4/\{(), (1,2)(3,4)\} \cong \mathbb{Z}/2\mathbb{Z}$. We have obtained the composition series $\{0\} \lhd \{(), (1,2)(3,4)\} \lhd V_4 \lhd A_4$, with corresponding composition factors $\mathbb{Z}/3\mathbb{Z}$ and two copies of $\mathbb{Z}/2\mathbb{Z}$.

We summarize the analysis above in the following result.

**Theorem 7.5** *Let $p$ be prime. Then the composition factors of $SL_2(\mathbb{Z}/p\mathbb{Z})$ are the following groups (up to isomorphism).*
*For $p = 2$:*

- $\mathbb{Z}/2\mathbb{Z}$ *(two times),*
- $\mathbb{Z}/3\mathbb{Z}$*.*

*For $p = 3$:*

- $\mathbb{Z}/2\mathbb{Z}$ *(three times),*
- $\mathbb{Z}/3\mathbb{Z}$*.*

*For $p > 3$:*

- $\mathbb{Z}/2\mathbb{Z}$*,*
- $PSL_2(\mathbb{Z}/p\mathbb{Z})$*.*

Now the second part of the composition series of $GL_2(\mathbb{Z}/p\mathbb{Z})$ is derived from the composition series of the factor group $GL_2(\mathbb{Z}/p\mathbb{Z})/SL_2(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$. To find this, we will describe how to find the composition series of a cyclic group $\mathbb{Z}/n\mathbb{Z}$ in general.

**Proposition 7.6** *Let $n \in \mathbb{N}$. Then $\mathbb{Z}/n\mathbb{Z}$ is simple $\iff$ $n$ is prime.*

*Proof.*

($\Rightarrow$) Assume $n$ is not prime. Then there exist $k, l \in \mathbb{N}$ such that $n = kl$, where both $k$ and $l$ are not equal to $n$. We can construct the map $\phi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ given by $\phi(m) = lm$. Then $ker(\phi) = k\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/l\mathbb{Z}$ is a proper nontrivial subgroup of $\mathbb{Z}/n\mathbb{Z}$, which is normal because it is the kernel of a homomorphism. Hence $\mathbb{Z}/n\mathbb{Z}$ is not simple.

($\Leftarrow$) Let $n$ be prime. Suppose $G \subseteq \mathbb{Z}/n\mathbb{Z}$ is a normal subgroup. By Lagrange's Theorem, $\#G$ divides $\#\mathbb{Z}/n\mathbb{Z} = n$. But $n$ is prime, so either $\#G = 1$ or $\#G = n$. It follows that $\mathbb{Z}/n\mathbb{Z}$ is simple.

∎

**Proposition 7.7** *Let $n \in \mathbb{N}$, and let $n = p_1 \cdots p_k$ be the prime factorization of $n$. A composition series of $\mathbb{Z}/n\mathbb{Z}$ can be given as follows:*

$$\{0\} \lhd (p_1 \cdots p_{k-1})\mathbb{Z}/n\mathbb{Z} \lhd \cdots \lhd (p_1 p_2)\mathbb{Z}/n\mathbb{Z} \lhd p_1\mathbb{Z}/n\mathbb{Z} \lhd \mathbb{Z}/n\mathbb{Z}.$$

*It has composition factors $\mathbb{Z}/p_i\mathbb{Z}$ with $i = 1, \ldots, k$.*

*Proof.* First of all, because $\mathbb{Z}/n\mathbb{Z}$ and its subgroups are abelian, the sequence

$$\{0\} \subset (p_1 \cdots p_{k-1})\mathbb{Z}/n\mathbb{Z} \subset \cdots \subset p_1\mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}.$$

is a sequence of normal subgroups. Now let us look at $(p_1 \cdots p_i)\mathbb{Z}/n\mathbb{Z} \lhd (p_1 \cdots p_{i-1})\mathbb{Z}/n\mathbb{Z}$ for $i = 1, \ldots k$. The corresponding factor group is

$$\left((p_1 \cdots p_{i-1})\mathbb{Z}/n\mathbb{Z}\right) / \left((p_1 \cdots p_i)\mathbb{Z}/n\mathbb{Z}\right) \cong (p_1 \cdots p_{i-1})\mathbb{Z}/(p_1 \cdots p_i)\mathbb{Z},$$

where the isomorphism follows from the third isomorphism theorem. Note that we can construct an isomorphism

$$\begin{aligned} \phi : (p_1 \cdots p_{i-1})\mathbb{Z}/(p_1 \cdots p_i)\mathbb{Z} &\longrightarrow \mathbb{Z}/p_i\mathbb{Z} \\ a + (p_1 \cdots p_i)\mathbb{Z} &\longmapsto \frac{a}{(p_1 \cdots p_{i-1})} + p_i\mathbb{Z} \end{aligned}$$

It follows that $(p_1 \cdots p_{i-1})\mathbb{Z}/(p_1 \cdots p_i)\mathbb{Z} \cong \mathbb{Z}/p_i\mathbb{Z}$, which is a simple group by Proposition 7.6. We conclude that the composition series is of the desired form with composition factors $\mathbb{Z}/p_i\mathbb{Z}$ for $i = 1, \ldots, k$. ∎

Proposition 7.7 tells us how to construct a composition series of $\mathbb{Z}/(p-1)\mathbb{Z}$, which completes the composition series for $GL_2(\mathbb{Z}/p\mathbb{Z})$. We can now combine Theorem 7.5 and Proposition 7.7 to list all composition factors of $GL_2(\mathbb{Z}/p\mathbb{Z})$.

**Theorem 7.8** *Let $p > 3$ be prime. Let $p - 1 = q_1 \cdots q_k$ be the prime factorization of $p - 1$. Then the composition factors of $GL_2(\mathbb{Z}/p\mathbb{Z})$ are the following groups (up to isomorphism):*

- $\mathbb{Z}/2\mathbb{Z}$,
- $PSL_2(\mathbb{Z}/p\mathbb{Z})$,
- $\mathbb{Z}/q_i\mathbb{Z}$ *for* $i = 1, \ldots, k$.

## 7.4 Question on transitive subgroups

Besides Serre's uniformity problem, our theorem about the compositum of prime degree extensions will rely on another assumption. We ask ourselves the following question:

***Question: Let*** $p > 5$ ***be prime. Can*** $PSL_2(\mathbb{Z}/p\mathbb{Z})$ ***be a composition factor of a transitive subgroup of*** $S_q$ ***for a prime*** $q$***?***

This question is not answered in this article. However, we can show an interesting result about the compositum of all prime degree extensions of $\mathbb{Q}$, in the case that the answer to this question is negative. Note that we assume $p > 5$, because for $p = 5$ we can actually find a value of $q$ for which the answer to this question is yes. Namely, $PSL_2(\mathbb{Z}/5\mathbb{Z}) \cong A_5$, which is a composition factor of $S_5$, so we can pick $q = 5$ in this case. As we mentioned in Section 7.3, for $p \geq 5$, the group $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is simple.

In our theorem in the next section, we will thus assume the following:

**Assumption 7.9** *Let $p > 5$ be prime. Then $PSL_2(\mathbb{Z}/p\mathbb{Z})$ cannot be a composition factor of a transitive subgroup of $S_q$ for any prime $q$.*

## 7.5 Elliptic curves over the compositum of all prime degree extensions

Now that we have properly introduced all necessary preliminaries, we can state the main result that we are going to prove in this section.

**Theorem 7.10** *Let $K := \mathbb{Q}(\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}]$ is prime$\})$. Let $p > 37$ be a prime, and let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Assume that Conjecture 7.1 (Serre's uniformity problem) and Assumption 7.9 are true. Then*

$$E(K)[p] \cong \{0\}.$$

The proof of this theorem is separated into a few intermediate results and will be given over the course of section 7.5.

### 7.5.1 Shifting the problem to finding composition series

In order to prove this theorem, we will first state a useful intermediate result. This will change our problem into a problem of finding composition series.

**Lemma 7.11** *If $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is a composition factor of $\rho'_{E,p}(G_K)$, then $E(K)[p] \cong \{0\}$.*

We will make use of the following notion for the proof of Lemma 7.11.

**Definition 7.12** *A group $G$ is called **solvable** if all composition factors of $G$ are abelian.*

**Proposition 7.13** *Let $G$ be a finite abelian group. Then $G$ is solvable.*

*Proof.* Consider the composition series of $G$. All subgroups in this composition series are subgroups of $G$ and hence abelian. The composition factors are quotient groups of these abelian groups, which are also abelian. Hence $G$ is solvable. ∎

Recall the definition of $B_n$ from (13). We have the following lemma:

**Lemma 7.14** *All conjugate subgroups of $B_n$ are solvable.*

*Proof.* Note that any conjugate subgroup of $B_n$ is isomorphic to $B_n$. Hence if $B_n$ is solvable, all conjugate subgroups are solvable as well.

Define the group $C_n := \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \mid a \in (\mathbb{Z}/n\mathbb{Z})^\times\}$. Consider the group homomorphism

$$\phi : B_n \longrightarrow C_n$$

given by $\phi(\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right)) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right)$. We have $ker(\phi) = \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbb{Z}/n\mathbb{Z}\}$. Note that $\phi$ is surjective. It follows that $ker(\phi) \lhd B_n$, and $C_n \cong B_n/ker(\phi)$. So the composition factors of $B_n$ are the compositon factors of $ker(\phi)$ together with those of $C_n$.

First we will focus on $ker(\phi)$. Note that $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a+b \\ 0 & 1 \end{smallmatrix}\right)$ for all $a, b \in \mathbb{Z}/n\mathbb{Z}$. $Ker(\phi) \cong \mathbb{Z}/n\mathbb{Z}$ is thus an abelian group, and from Proposition 7.13 it is solvable.
Now consider the group $C_n$. Because $\left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & ab \end{smallmatrix}\right)$ for all $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$, we can conclude that $C_n \cong \mathbb{Z}/n\mathbb{Z}^\times$ is abelian. again, Proposition 7.13 implies that $C_n$ is solvable.

We hence know that the composition factors of both $ker(\phi)$ and $C_n$ are all abelian groups. The composition factors of $B_n$ are thus all abelian, and we conclude that $B_n$ is solvable. ∎

**Lemma 7.15** *Let $G$ be a solvable group, and let $H$ be a (not necessarily normal) subgroup of $G$. Then $H$ is solvable.*

*Proof.* Let $G$ be a solvable group. Consider a composition series of $G$:

$$\{0\} = N_k \lhd N_{k-1} \lhd \cdots \lhd N_1 \lhd N_0 = G.$$

Define $M_i = N_i \cap H$ for all $i = 0, \ldots, k$. We can now consider the sequence

$$\{0\} = M_k \subseteq \cdots \subseteq M_1 \subseteq M_0 = H.$$

Because $N_{i+1} \lhd N_i$, we know there exists a group homomorphism $\phi_i : N_i \longrightarrow N_i/N_{i+1}$ such that $ker(\phi_i) = N_{i+1}$. Then if we restrict $\phi_i$ to the subgroup $M_i$, we obtain $ker(\phi_i|_{M_i}) = ker(\phi_i) \cap M_i = N_{i+1} \cap N_i \cap H = M_{i+1}$. It follows that $M_{i+1} \trianglelefteq M_i$ for all $i = 0, \ldots k-1$.

Now let us look at the factor groups of this series of normal subgroups. These are of the form $M_i/M_{i+1}$ for $i = 0, \ldots k-1$. First of all, note that

$$M_i/M_{i+1} \cong Im(\phi_i|_{M_i}) \subseteq Im(\phi_i) \cong N_i/N_{i+1}.$$

Because $G$ is solvable, $N_i/N_{i+1}$ is abelian and it follows that since $M_i/M_{i+1}$ is isomorphic to a subgroup of $N_i/N_{i+1}$, it is also abelian. If $M_i/M_{i+1}$ is not simple, there are two possibilities.

Either $M_i/M_{i+1} = \{0\}$, in which case $M_i = M_{i+1}$ and we take one of these groups out of the sequence. If this is not the case, we can find the composition series of $M_i/M_{i+1}$. By Proposition 7.13, the corresponding composition factors are abelian. The composition factors of $H$ are obtained by taking together all composition factors of each $M_i/M_{i+1} \not\equiv \{0\}$. Because these are all abelian, we conclude that $H$ is solvable. ∎

We now have all ingredients to prove Lemma 7.11.

*Proof of Lemma 7.11.* We assume that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is a composition factor of $\rho'_{E,p}(G_K)$. As an explicit example can show, the group $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is not abelian. Namely, $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}2&1\\1&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&1\\1&2\end{smallmatrix}\right)$, while $\left(\begin{smallmatrix}2&1\\1&1\end{smallmatrix}\right) \neq \left(\begin{smallmatrix}1&1\\1&2\end{smallmatrix}\right)$ modulo $Z(SL_2(\mathbb{Z}/p\mathbb{Z}))$. By definition, $\rho'_{E,p}(G_K)$ is therefore not solvable.
Lemma 7.14 says that all conjugate subgroups of $B_n$ are solvable, and according to Lemma 7.15, their subgroups are also solvable. It follows that $\rho'_{E,p}(G_K)$ cannot be a subgroup of any conjugate subgroup of $B_n$. Using the third equivalence in Theorem 6.7, we can conclude that $E(K)[p] \cong \{0\}$. ∎

We now have a different problem to solve, namely showing that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ must be a composition factor of $\rho'_{E,p}(G_K)$.

### 7.5.2 $K$ is a Galois extension of $\mathbb{Q}$

We would like to show that $\mathbb{Q} \subseteq K$ is a Galois extension. When we know this, we can use all results that follow from the Galois correspondence.

Recall that we defined $K$ as follows: $K := \mathbb{Q}(\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] \text{ is prime}\})$. We will first try to find a different description of $K$. We will break up the field in the following way:

**Proposition 7.16** *The field $K$ is equal to the compositum of all fields of the form $\mathbb{Q}(q^\infty)$ for a prime $q$.*

*Proof.* This is relatively straightforward from the definitions of these fields. We know from Definition 3.11 that

$$\mathbb{Q}(q^\infty) := \mathbb{Q}(\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] = q\}).$$

By Definition 3.10, we can write the compositum of all fields $\mathbb{Q}(q^\infty)$ as follows:

$$\begin{aligned}\mathbb{Q}\left(\bigcup_{q \text{ prime}} \mathbb{Q}(q^\infty)\right) &= \mathbb{Q}\left(\bigcup_{q \text{ prime}} \{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] = q\}\right) \\ &= \mathbb{Q}\left(\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] \text{ is prime}\}\right) = K.\end{aligned}$$

We conclude therefore that $K$ is equal to this compositum. ∎

Now we focus on the fields $\mathbb{Q}(q^\infty)$. We want to find a different description of such a field. In order to do this we need the notion of a splitting field of a polynomial. The **splitting field** of a polynomial $f \in L[x]$ over a field $L$ is the smallest field extension of $L$ in which $f$ splits into linear factors. This splitting field exists and is unique (up to isomorphism) for all monic

polynomials $f$. If $\alpha_1, \dots \alpha_k$ are the roots of $f$ in an algebraic closure of $L$, the splitting field, denoted by $\Omega_L^f$, is equal to $L(\alpha_1, \dots, \alpha_k)$.

**Proposition 7.17** *We have the following equality of fields:*

$$\mathbb{Q}(q^\infty) = \mathbb{Q}(\{\Omega_{\mathbb{Q}}^f \mid f \in \mathbb{Q}[x], f \text{ irreducible and } deg(f) = q\}).$$

*Proof.*

($\subseteq$) Let us start from the field $\mathbb{Q}(q^\infty) := \mathbb{Q}(\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] = q\})$. Let $\alpha$ be one of the generators of $\mathbb{Q}(q^\infty)$, for which $[\mathbb{Q}(\alpha) : \mathbb{Q}] = q$. It follows that the minimal polynomial $f_{\mathbb{Q}}^\alpha$ has degree $q$, and it is by definition irreducible.

By definition of a splitting field, we know that $\alpha \in \Omega_{\mathbb{Q}}^{f_{\mathbb{Q}}^\alpha}$, and hence it is in the compositum on the right-hand side. Because $\alpha$ is arbitrary, all generators of $\mathbb{Q}(q^\infty)$ are in this compositum, and we conclude $\mathbb{Q}(q^\infty) \subseteq \mathbb{Q}(\{\Omega_{\mathbb{Q}}^f \mid f \in \mathbb{Q}[x], f \text{ irreducible and } deg(f) = q\})$.

($\supseteq$) Now let us consider some irreducible polynomial $f \in \mathbb{Q}[x]$ with $deg(f) = q$. Let $\alpha_1, \dots, \alpha_q$ be the zeros of $f$. Then $\Omega_{\mathbb{Q}}^f = \mathbb{Q}(\alpha_1, \dots, \alpha_q)$. Now because $f$ is irreducible, we have that $f$ is the minimal polynomial of each $\alpha_i$ over $\mathbb{Q}$. Hence $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = q$ for each $i = 1, \dots, q$. It follows that $\alpha_i \in \mathbb{Q}(q^\infty)$. Hence also $\Omega_{\mathbb{Q}}^f \subseteq \mathbb{Q}(q^\infty)$, and because the compositum on the right-hand side is generated by these splitting fields, we conclude $\mathbb{Q}(q^\infty) \supseteq \mathbb{Q}(\{\Omega_{\mathbb{Q}}^f \mid f \in \mathbb{Q}[x], f \text{ irreducible and } deg(f) = q\})$. This concludes the proof.

∎

Note that the field $\mathbb{Q}(\{\Omega_{\mathbb{Q}}^f \mid f \in \mathbb{Q}[x], f \text{ irreducible and } deg(f) = q\})$ is a compositum of all fields of the form $\Omega_{\mathbb{Q}}^f$ for some irreducible polynomial in $\mathbb{Q}[x]$ of degree $q$. This set of polynomials is countable, because the polynomials have coefficients in the countable set $\mathbb{Q}$. Therefore $\mathbb{Q}(q^\infty)$ is equal to a compositum over a countable number of splitting fields. $K$ is the compositum of all fields $\mathbb{Q}(q^\infty)$, and there are also a countable number of primes. Hence we can conclude that $K$ is a compositum of a countable number of splitting fields.

Any splitting field $\Omega_{\mathbb{Q}}^f$ over $\mathbb{Q}$ is a normal extension of $\mathbb{Q}$ [24, Thm 23.14]. We can use the following result to show that $K$ must also be normal.

**Theorem 7.18** *Let $(K_n)_{n \in N}$ be a countable collection of normal, algebraic extensions of $\mathbb{Q}$. Then the compositum $\mathbb{Q}(\cup_{n \in \mathbb{N}} K_n)$ is also a normal extension of $\mathbb{Q}$.*

*Proof.* Let us denote the compositum of the collection $(K_n)_{n \in N}$ by $L$. Let $\tilde{L}$ be the normal closure of $L$. Then we can look at the Galois extension $\mathbb{Q} \subseteq \tilde{L}$. For any subfield $F$ of $\tilde{L}$, define $\tilde{G}_F := Gal(\tilde{L}/F)$. From the Galois correspondence, we know that a subfield $F \subseteq \tilde{L}$ is a normal extension of $\mathbb{Q}$ if and only if $\tilde{G}_F \lhd \tilde{G}_{\mathbb{Q}}$. We therefore know that $\tilde{G}_{K_n} \lhd \tilde{G}_{\mathbb{Q}}$ for all $n \in \mathbb{N}$.

We will show that $\tilde{G}_L = \bigcap_{n=1}^\infty \tilde{G}_{K_n}$. First of all, $\tilde{G}_L$ consists of all automorphisms of $\tilde{L}$ fixing $L$. Because $K_n \subseteq L$ for all $n \in \mathbb{N}$, these automorphisms also fix the fields $K_n$. Hence we conclude $\tilde{G}_L \subseteq \bigcap_{n=1}^\infty \tilde{G}_{K_n}$.
On the other hand, if $\sigma \in \bigcap_{n=1}^\infty \tilde{G}_{K_n}$, it fixes all fields $K_n$, so it fixes $\cup_{n \in \mathbb{N}} K_n$. $L$ is the compositum of these fields, which can be written as $\mathbb{Q}(\cup_{n \in \mathbb{N}} K_n)$ and is generated by this union.

We conclude $\sigma$ also fixes $L$. Hence $\sigma \in \tilde{G}_L$. We conclude $\tilde{G}_L = \bigcap_{n=1}^{\infty} \tilde{G}_{K_n}$.

The intersection of an arbitrary number of normal subgroups is again a normal subgroup, so we obtain $\tilde{G}_L \lhd \tilde{G}_{\mathbb{Q}}$. We conclude $\mathbb{Q} \subseteq L$ is a normal extension. ∎

We noted before that the field $K$ is a countable compositum of splitting fields. These splitting fields are all normal, algebraic extensions of $\mathbb{Q}$. Therefore Theorem 7.18 implies that $\mathbb{Q} \subseteq K$ is also normal. We know already that $K$ is algebraic, and by Proposition 4.6 that it is separable. We conclude that $\mathbb{Q} \subseteq K$ is a Galois extension.

### 7.5.3 The use of Serre's uniformity problem

Note that because $\mathbb{Q} \subseteq K$ is a Galois extension, we have $G_K \lhd G_{\mathbb{Q}}$. We will now use Serre's conjecture, which states that the Galois representation $\rho'_{E,p}$ is surjective. A surjective homomorphism preserves normal subgroups, hence we also have $\rho'_{E,p}(G_K) \lhd \rho'_{E,p}(G_{\mathbb{Q}}) = GL_2(\mathbb{Z}/p\mathbb{Z})$.

Recall from Section 7.2 that the collection of composition factors of $GL_2(\mathbb{Z}/p\mathbb{Z})$ then consists of the composition factors of $\rho'_{E,p}(G_K)$ together with those of $GL_2(\mathbb{Z}/p\mathbb{Z})/\rho'_{E,p}(G_K)$. In Theorem 7.8 we saw that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is a composition factor of $GL_2(\mathbb{Z}/p\mathbb{Z})$. Hence if we show $PSL_2(\mathbb{Z}/p\mathbb{Z})$ can not be a factor of $GL_2(\mathbb{Z}/p\mathbb{Z})/\rho'_{E,p}(G_K)$, this implies that it must be a factor of $\rho'_{E,p}(G_K)$. To do this, we will first try to find a description for the group $GL_2(\mathbb{Z}/p\mathbb{Z})/\rho'_{E,p}(G_K)$ that is easier to handle, such that is becomes easier to find the corresponding composition factors.

Let us define $I_{\mathbb{Q}} := ker(\rho_{E,p})$. In Section 4.2 we saw that $\mathbb{Q}(E[p]) = \overline{\mathbb{Q}}^{ker(\rho_{E,p})}$. We introduce the notation

$$L := \mathbb{Q}(E[p]) = \overline{\mathbb{Q}}^{I_{\mathbb{Q}}}.$$

We also saw that $Gal(\overline{\mathbb{Q}}/L) = I_{\mathbb{Q}}$ from the Galois correspondence. Furthermore, $\mathbb{Q} \subseteq L$ is Galois.

Define the following restriction map:

$$\begin{aligned} \rho : G_{\mathbb{Q}} &\longrightarrow Gal(L/\mathbb{Q}) \\ \sigma &\longmapsto \sigma|_L, \end{aligned}$$

and let

$$L' := L^{\rho(G_K)}.$$

Note that $L'$ contains exactly the elements of $L$ that are fixed by $\rho(G_K)$, in other words, the elements in $K$. Hence $L' = L \cap K$. Because $\mathbb{Q} \subseteq L$ is Galois, the Galois correspondence tells us that $L' \subseteq L$ is also Galois with Galois group $Gal(L/L') = \rho(G_K)$.

**Claim 7.19** $\rho(G_K) \cong \rho_{E,p}(G_K)$.

*Proof.* Consider the Galois representation $\rho_{E,p} : G_{\mathbb{Q}} \longrightarrow Aut(E(\overline{\mathbb{Q}})[p])$. We have $ker(\rho_{E,p}) = I_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/L)$. Similarly, it can be seen that $ker(\rho) = Gal(\overline{\mathbb{Q}}/L)$. We conclude that $ker(\rho) = ker(\rho_{E,p})$.

Let us now restrict the two maps to $G_K$. We define $\rho^K := \rho|_{G_K}$ and $\rho^K_{E,p} := \rho_{E,p}|_{G_K}$. Note that $ker(\rho^K) = ker(\rho) \cap G_K = ker(\rho_{E,p}) \cap G_K = ker(\rho^K_{E,p})$. The first isomorphism theorem then gives

$$\rho(G_K) \cong G_K/ker(\rho^K) = G_K/ker(\rho^K_{E,p}) \cong \rho_{E,p}(G_K).$$

∎

We conclude that $Gal(L/L') \cong \rho_{E,p}(G_K) \cong \rho'_{E,p}(G_K)$.

Recall from the Galois correspondence that

$$Gal(L/\mathbb{Q}) \cong Gal(\overline{\mathbb{Q}}/\mathbb{Q})/Gal(\overline{\mathbb{Q}}/L) = G_\mathbb{Q}/I_\mathbb{Q} \cong \rho_{E,p}(G_\mathbb{Q}) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$$

These last steps follows from applying the first isomorphism theorem to the map $\rho_{E,p}$ and from Serre's conjecture.

Recall that $\rho'_{E,p}(G_K) \lhd GL_2(\mathbb{Z}/p\mathbb{Z})$, and hence $Gal(L/L') \lhd Gal(L/\mathbb{Q})$. It follows that $\mathbb{Q} \subseteq L'$ is Galois. We obtain

$$Gal(L'/\mathbb{Q}) \cong Gal(L/\mathbb{Q})/Gal(L/L') = GL_2(\mathbb{Z}/p\mathbb{Z})/\rho'_{E,p}(G_K).$$

We recognize this last quotient as the group we were interested in. Our goal is now to show that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is not a composition factor of $Gal(L'/\mathbb{Q})$.

### 7.5.4 $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is not a composition factor of $Gal(L'/\mathbb{Q})$

By Theorem 2.10 we know that $E(\overline{\mathbb{Q}})[p]$ is a finite group (of algebraic elements), and hence $L = \mathbb{Q}(E[p])$ is a finite algebraic extension of $\mathbb{Q}$. $L'$, which is contained in $L$, is thus also a finite algebraic extension of $\mathbb{Q}$.

**Theorem 7.20 (Theorem of the primitive element)** [24, Thm 23.9] *Let $K \subseteq L$ be a finite separable extension. Then there exists an element $x \in L$ with $L = K(x)$.*

Proposition 4.6 and Theorem 7.20 together imply that there is some $\beta \in L'$ such that $L' = \mathbb{Q}(\beta)$.

Recall that $L' = L \cap K$, and hence $L' \subseteq K$. Therefore $\beta \in K$. Let $(K_i)_{i\in I}$ be the collection of prime degree extensions of $\mathbb{Q}$, such that $K$ is the compositum of all fields $(K_i)_{i\in I}$. Recall from Definition 3.10 that $\beta \in K$ must be of the form $\beta = f(v_1, \ldots, v_n)$ with $n \in \mathbb{N}$, $v_1, \ldots, v_n \in \bigcup_{i\in I} K_i$ and $f \in \mathbb{Q}[x_1, \ldots, x_n]$. If $v_i \in K_{e_i}$, then $\beta \in K_{e_1} \bullet \ldots \bullet K_{e_n}$, the finite compositum of the fields $K_{e_1}, \ldots, K_{e_n}$. Hence $L' = \mathbb{Q}(\beta) \subseteq K_{e_1} \bullet \ldots \bullet K_{e_n}$. Now let $\tilde{K}_{e_i}$ be the normal closure of $K_{e_i}$. Then by definition, $\mathbb{Q} \subseteq \tilde{K}_{e_i}$ is Galois.

**Claim 7.21** *$Gal(\tilde{K}_{e_i}/\mathbb{Q})$ is a transitive subgroup of $S_{q_i}$, where $q_i$ is the degree of $\mathbb{Q} \subseteq K_{e_i}$.*

*Proof.* We know that $\mathbb{Q} \subseteq K_{e_i}$ is a prime extension. Therefore $[K_{e_i} : \mathbb{Q}] = q_i$ for some prime $q_i$. Because $\mathbb{Q} \subseteq K_{e_i}$ is separable (by Proposition 4.6), we can apply Theorem 7.20 to conclude that there exists $\gamma \in K_{e_i}$ such that $K_{e_i} = \mathbb{Q}(\gamma)$. Note that $deg(f^\gamma_\mathbb{Q}) = q_i$.

Because $\mathbb{Q} \subseteq \mathbb{Q}(\gamma)$ is separable, we know that $f_{\mathbb{Q}}^{\gamma}$ has $q_i$ distinct roots. Let us denote the set of roots by $\{\gamma_1, \ldots, \gamma_{q_i}\}$, where $\gamma_1 = \gamma$. Now we claim that $\tilde{K}_{e_i} = \mathbb{Q}(\gamma_1, \ldots, \gamma_{q_i})$, the splitting field of $f_{\mathbb{Q}}^{\gamma}$ over $\mathbb{Q}$.
To see this, first of all, note that $\tilde{K}_{e_i}$ is the normal closure of $\mathbb{Q} \subseteq \mathbb{Q}(\gamma)$, and hence a normal extension of $\mathbb{Q}$. Because $\gamma \in \tilde{K}_{e_i}$, all roots $\{\gamma_1, \ldots, \gamma_{q_i}\}$ of the polynomial $f_{\mathbb{Q}}^{\gamma}$ are elements of $\tilde{K}_{e_i}$. It follows that $\mathbb{Q}(\gamma_1, \ldots, \gamma_{q_i}) \subseteq \tilde{K}_{e_i}$. However, we know that $\mathbb{Q}(\gamma_1, \ldots, \gamma_{q_i})$ is the splitting field of $f_{\mathbb{Q}}^{\gamma}$ over $\mathbb{Q}$. Recall that any splitting field over $\mathbb{Q}$ is a normal extension of $\mathbb{Q}$. Hence $\mathbb{Q}(\gamma_1, \ldots, \gamma_{q_i})$ is a normal extension of $\mathbb{Q}(\gamma)$, whereas $\tilde{K}_{e_i}$ is by definition the smallest normal extension of $\mathbb{Q}(\gamma)$. It follows that $\tilde{K}_{e_i} \subseteq \mathbb{Q}(\gamma_1, \ldots, \gamma_{q_i})$, and hence these fields must be equal.

Because $\tilde{K}_{e_i} = \mathbb{Q}(\gamma_1, \ldots, \gamma_{q_i})$, it follows that all automorphisms in $Gal(\tilde{K}_{e_i}/\mathbb{Q})$ are completely determined by their action on the roots $\{\gamma_1, \ldots, \gamma_{q_i}\}$. Furthermore, these automorphisms must permute the roots of $f_{\mathbb{Q}}^{\gamma}$. Namely, if $\gamma_j$ is such a root, then $f_{\mathbb{Q}}^{\gamma}(\gamma_j) = 0$. Now for $\sigma \in Gal(\tilde{K}_{e_i}/\mathbb{Q})$, we have $\sigma(f_{\mathbb{Q}}^{\gamma}(\gamma_j)) = f_{\mathbb{Q}}^{\gamma}(\sigma(\gamma_j)) = \sigma(0) = 0$, because $\sigma$ acts as identity on the coefficients of $f_{\mathbb{Q}}^{\gamma}$. Hence $\sigma(\gamma_j)$ is also a zero of $f_{\mathbb{Q}}^{\gamma}$. We now know that $\sigma \in Gal(\tilde{K}_{e_i}/\mathbb{Q})$ can completely be characterized by the permutation it performs on the zeros of $f_{\mathbb{Q}}^{\gamma}$, which is an element of the symmetric group $S_{q_i}$. We can thus consider the map $\chi : Gal(\tilde{K}_{e_i}/\mathbb{Q}) \longrightarrow S_{q_i}$ sending each automorphism to the corresponding permutation on the zeros of $f_{\mathbb{Q}}^{\gamma}$. Because each $\sigma$ is completely determined by this permutation of the zeros, $\chi$ is injective and hence we can view $Gal(\tilde{K}_{e_i})$ as a subgroup of $S_{q_i}$.

We still need to show that $Gal(\tilde{K}_{e_i})$ is transitive. Note that for each root $\gamma_j$ we have the isomorphism

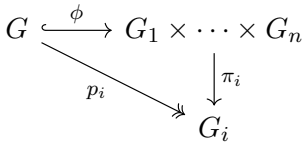
$$\begin{aligned} \phi_j : \ \mathbb{Q}[x]/(f_{\mathbb{Q}}^{\gamma}) &\longrightarrow \mathbb{Q}(\gamma_j) \\ g(x) + (f_{\mathbb{Q}}^{\gamma}) &\longmapsto g(\gamma_j). \end{aligned}$$

Hence for each combination of zeros we can construct an isomorphism $\phi_{jk} = \phi_k \circ \phi_j^{-1} : \mathbb{Q}(\gamma_j) \longrightarrow \mathbb{Q}(\gamma_k)$ sending $\gamma_j$ to $\gamma_k$. By Lemma 21.17 from [24], it follows that there exists an automorphism of $\tilde{K}_{e_i}$ extending $\phi_{jk}$. So for all $\gamma_j, \gamma_k$, there exists a $\sigma \in Gal(\tilde{K}_{e_i}/\mathbb{Q})$ such that $\sigma(\gamma_j) = \gamma_k$. By definition, this means $Gal(\tilde{K}_{e_i}/\mathbb{Q})$ acts transitively on $\{\gamma_1, \ldots, \gamma_{q_i}\}$. ∎

Recall that we work under Assumption 7.9. Therefore, since $Gal(\tilde{K}_{e_i}/\mathbb{Q})$ is a transitive subgroup of $S_{q_i}$, where $q_i$ is prime, we conclude that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is not a composition factor of $Gal(\tilde{K}_{e_i}/\mathbb{Q})$. This holds for all $i \in \{1, \ldots, n\}$.

Our final step is to use this fact in showing that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is not a composition factor of $Gal(L'/\mathbb{Q})$. In order to do this, the following lemma is useful.

**Lemma 7.22** *Let $G, G_1, \ldots, G_n$ be finite groups. Let $\phi$ is some injective map from $G$ to $G_1 \times \cdots \times G_n$, and let $\pi_i$ be the projection of $G_1 \times \cdots \times G_n$ on the $i$th coordinate. Assume the map $p_i$ satisfying the following commutative diagram is a surjective map for each $i = 1, \ldots, n$:*



*Then the collection of composition factors of $G$ is equal to the union of the composition factors of the groups $G_1, \ldots, G_n$ (with possibly different multiplicities).*

*Proof.* The proof of this theorem will be given by induction on $n$. In the following, we will use the notation $\pi_i$ for all maps that project on the $i$th coordinate, trusting that the corresponding domain will be clear from context.

*Base step*
Let us first consider the case where $n = 2$. Let $N_i = ker(p_i)$ for $i = 1, 2$. Then $N_1 = \{g \in G \mid \phi(g) = (1, h) \text{ for some } h \in G_2\}$. We have $N_1 \lhd G$ because it is the kernel of a homomorphism, and $G/N_1 \cong G_1$. Hence the composition factors of $G$ are the composition factors of $N_1$ together with the composition factors of $G_1$.

As mentioned before, a surjective map preserves normal subgroups. Hence $p_2(N_1) \lhd p_2(G) = G_2$. The fact that $\phi$ is injective implies that $N_1 \cong \phi(N_1)$. By construction, $\phi(N_1) \subseteq \{(1, h) \mid h \in G_2\})$ and hence $\phi(N_1) \cong (\pi_2 \circ \phi)(N_1) = p_2(N_1)$. It follows that $p_2(N_1) \cong N_1$. Hence the composition factor of $N_1$ are isomorphic to the composition factors of $p_2(N_1)$, and the collection of these factors is contained in the collection of composition factors of $G_2$.

In a completely analogous way, we can show that the composition factors of $G$ are the composition factors of $N_2$ together with the composition factors of $G_2$, and that the collection of factors of $N_2$ is contained in the collection of factors of $G_1$. Taking all this information together we arrive at the conclusion that the collection of composition factors of $G$ must be equal to the union of the composition factors of $G_1$ and $G_2$ (where the multiplicities might differ, because some factors may appear in both the composition series of $G_1$ and $G_2$).

*Induction Step*
Now assume that the statement of the lemma is satisfied whenever $n < m$. We will now consider the case where $n = m$.

$$\begin{array}{ccc} G & \xhookrightarrow{\phi} & G_1 \times \cdots \times G_m \\ & \searrow^{p_i} & \downarrow{\scriptstyle \pi_i} \\ & & G_i \end{array}$$

Consider the following definition of the map $r_i$ by means of a commutative diagram.

$$\begin{array}{ccc} G & \xhookrightarrow{\phi} & G_1 \times \cdots \times G_m \\ & \searrow^{r_i} & \downarrow{\scriptstyle projection} \\ & & G_1 \times \cdots \times \hat{G}_i \times \cdots G_m \end{array}$$

$\hat{G}_i$ indicates the absence of the $G_i$ in the product. By the first isomorphism theorem, $G/ker(r_i) \cong r_i(G)$. Hence we can define an injective map

$$\phi_i : G/ker(r_i) \longrightarrow G_1 \times \cdots \times \hat{G}_i \times \cdots G_n$$

given by this isomorphism, sending $\overline{g}$ to $r_i(g)$. Let us furthermore define the natural map $\mu_i : G \longrightarrow G/ker(r_i)$ given by $\mu_i(g) = \overline{g}$. Then we can compose these maps with the

projection on the $j$th coordinate ($i \neq j$) as follows: $\pi_j \circ \phi_i \circ \mu_i = \pi_j \circ r_i = \pi_j \circ \phi$, which is surjective by our initial assumption. So $\pi_j \circ \phi_i$ is also surjective and we arrive at the following diagram:

$$\begin{array}{ccc} G/ker(r_i) & \xhookrightarrow{\phi_i} & G_1 \times \cdots \times \hat{G_i} \times \cdots G_m \\ & \searrow & \downarrow \pi_j \\ & & G_j \end{array}$$

Now we have a diagram of the form presented in the lemma, with a product of $m-1 < m$ groups. Hence by our induction hypothesis, The collection of composition factors of $G/ker(r_i)$ is equal to the union over $j \in \{1, \ldots, m\} \setminus \{i\}$ of the collection of composition factors of each $G_j$ (with possibly different multiplicities).

Note that the natural map $\tau : G \longrightarrow G/ker(r_1) \times G/ker(r_2)$ is injective. Namely, $g$ is in the kernel $\tau$ if and only if $g \in ker(r_1)$ and $g \in ker(r_2)$. Note that $g \in ker(r_1)$ if and only if all coordinates of $\phi(g)$, except possibly the first one, are zero. Similarly, $g \in ker(r_2)$ if and only if all coordinates of $\phi(g)$, except possibly the second one, are zero. To be in both these kernels, we thuse need $\phi(g) = 0$ and hence $g = 0$ because $\phi$ is injective. It follows that $ker(\tau) = \{0\}$ and hence $\tau$ is injective.

Projection on either of the two coordinates gives the natural map to the factor group of that coordinate, which is surjective. Hence we obtain the following diagram for $i = 1, 2$:

$$\begin{array}{ccc} G & \xhookrightarrow{\tau} & G/ker(r_1) \times G/ker(r_2) \\ & \searrow & \downarrow \pi_i \\ & & G/ker(r_i) \end{array}$$

This diagram satisfies the assumptions of the lemma, and hence from the induction hypothesis we know that the composition factors of $G$ are the composition factors of $G/ker(r_1)$ together with the composition factors of $G/ker(r_2)$. Together with our earlier result this implies the desired conclusion for $n = m$.

The base step and induction step together prove the lemma for all $n \in \mathbb{N}$. ∎

Define $\tilde{K} = \tilde{K}_{e_1} \bullet \ldots \bullet \tilde{K}_{e_n}$, and write $G_i = Gal(\tilde{K}_{e_i}/\mathbb{Q})$ and $G = Gal(\tilde{K}/\mathbb{Q})$. The groups $G_i$ are finite by Claim 7.21, and by definition of $\tilde{K}$ it follows that $G$ is also finite. These groups satisfy the following commutative diagram for $i = 1, \ldots, n$:

$$\begin{array}{ccc} G & \longhookrightarrow & G_1 \times \cdots \times G_n \\ & \searrow^{g_i} & \downarrow \pi_i \\ & & G_i \end{array}$$

where $g_i$ corresponds to restriction to $\tilde{K}_{e_i}$. We can apply Lemma 7.22, to conclude that the composition factors of $G$ are the union of the composition factors of each $Gal(\tilde{K}_{e_i}/\mathbb{Q})$.

We concluded before that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is not a composition factor of each $Gal(\tilde{K}_{e_i}/\mathbb{Q})$. It follows that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is not a composition factor of $Gal(\tilde{K}/\mathbb{Q})$.

Recall that $L' \subseteq K_{e_1} \bullet \ldots \bullet K_{e_n} \subseteq \tilde{K}$. Consider the surjective homomorphism $\phi : Gal(\tilde{K}/\mathbb{Q}) \longrightarrow Gal(L'/\mathbb{Q})$ defined by restriction of maps. We have $ker(\phi) \lhd Gal(\tilde{K}/\mathbb{Q})$, and hence the composition factors of $Gal(\tilde{K}/\mathbb{Q})$ are the factors of $ker(\phi)$ together with the factors of $Gal(\tilde{K}/\mathbb{Q})/ker(\phi) \cong Gal(L'/\mathbb{Q})$. We conclude that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ can not be a factor of $Gal(L'/\mathbb{Q})$.

We will now pull all the information together to arrive at the desired conclusion. Recall that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is a composition factor of $GL_2(\mathbb{Z}/p\mathbb{Z})$. We showed that this implies that it is either a composition factor of $\rho'_{E,p}(G_K)$, or of $GL_2(\mathbb{Z}/p\mathbb{Z})/\rho'_{E,p}(G_K) \cong Gal(L'/\mathbb{Q})$. We have now shown that this last statement is not the case. The conclusion is that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ must be a composition factor of $\rho'_{E,p}(G_K)$. Now we can apply Lemma 7.11 to find that $E(K)[p] \cong \{0\}$, which concludes our proof of Theorem 7.10.

# 8 Conclusion

In this report, we saw an overview of the most important results that were found in the research area of torsion subgroups of elliptic curves over algebraic field extensions of $\mathbb{Q}$. A classification exists of all torsion subgroups that appear for elliptic curves over degree one and two extensions of $\mathbb{Q}$. Merel even showed the existence of a uniform bound on the size of the torsion subgroups, which only depends on the degree of the field extension of $\mathbb{Q}$. However, for degrees larger than three, an explicit classification of these subgroups has not yet been reported.

If we restrict to elliptic curves defined over $\mathbb{Q}$, results can be obtained about elliptic curves over infinite extensions of $\mathbb{Q}$. We payed closer attention to the recently published classification of the torsion group of elliptic curves over $\mathbb{Q}(3^\infty)$. We reproduced in more detail the proof of Daniels, Lozano-Robledo, Najman and Sutherland, in which it is shown that if we look at a Galois extension of $\mathbb{Q}$ that contains only finitely many roots of unity, the torsion subgroup of an elliptic curve over this extension is finite.

Finally we provided some general results that can be used to classify torsion subgroups. We applied these general results to the compositum of all prime degree extensions of $\mathbb{Q}$, denoted by $K$. Under two assumptions, we showed for all primes $p > 37$ and for all elliptic curves defined over $\mathbb{Q}$ without complex multiplication, that the $p$-torsion subgroup of the elliptic curve over $K$ is trivial. These assumptions are Serre's uniformity problem and a statement about transitive subgroups of the symmetric groups $S_q$.

# References


[1] H. Daniels, A. Lozano-Robledo, F. Najman, and A. Sutherland. Torsion subgroups of rational elliptic curves over the compositum of all cubic fields. *Mathematics of Computation*, 87(309):425–458, 2018.

[2] L. E. Dickson. Theory of linear groups in an arbitrary field. *Transactions of the American Mathematical Society*, 2(4):363–394, 1901.

[3] G. Frey and M. Jarden. Approximation theory and the rank of abelian varieties over large algebraic fields. *Proceedings of the London Mathematical Society*, 3(1):112–128, 1974.

[4] Y. Fujita. Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$. *Acta Arithmetica*, 115:29–45, 2004.

[5] Y. Fujita. Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$. *Journal of Number Theory*, 114(1):124–134, 2005.

[6] I. Gal and R. Grizzard. On the compositum of all degree d extensions of a number field. *J. Théor. Nombres Bordeaux*, 26(3):655–673, 2014.

[7] E. González-Jiménez and Á. Lozano-Robledo. Elliptic curves with abelian division fields. *Mathematische Zeitschrift*, 283(3-4):835–859, 2016.

[8] M. Hazewinkel, N. Gubareni, and V.V. Kirichenko. Algebras, rings and modules. vol. 1. *Kluwer Academic Publishers, Dordrecht*, 21:22, 2004.

[9] K. Igusa. *The Special Linear Group $SL(n, F)$*. Brandeis University, 2002. Lecture notes. `http://people.brandeis.edu/~igusa/Math101b/SL.pdf`.

[10] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Inventiones mathematicae*, 109(1):221–229, 1992.

[11] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 109:125–149, 1988.

[12] M.A. Kenku. The modular curve x 0 (39) and rational isogeny. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 85, pages 21–23. Cambridge University Press, 1979.

[13] M.A. Kenku. The modular curve x0 (169) and rational isogeny. *Journal of the London Mathematical Society*, 2(2):239–244, 1980.

[14] M.A. Kenku. The modular curves x 0 (65) and x 0 (91) and rational isogeny. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 87, pages 15–20. Cambridge University Press, 1980.

[15] M.A. Kenku. On the modular curves x0 (125), x1 (25), x1 (49). *Journal of the London Mathematical Society*, 2(3):415–427, 1981.

[16] M. Laska and M. Lorenz. *Rational Points on Elliptic Curves Over $\mathbb{Q}$ in Elementary Abelian 2-extensions of $\mathbb{Q}$*. Universität Bonn. SFB 40. Theoretische Mathematik/Max-Planck-Institut für Mathematik, 1984.

[17] B. Mazur. Modular curves and the Eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[18] B. Mazur and D. Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978.

[19] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, 124(1-3):437–449, 1996.

[20] L. J. Mordell. On the rational resolutions of the indeterminate equations of the third and fourth degree. In *Proc. Cambridge Phil. Soc.*, volume 21, pages 179–192, 1922.

[21] F. Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. *arXiv preprint arXiv:1211.2188*, 2012.

[22] J. P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259–331, 1971.

[23] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[24] P. Stevenhagen. *Algebra III*. Universiteit Leiden, 2012. Lecture notes (Dutch). `websites.math.leidenuniv.nl/algebra/algebra3.pdf`.

[25] L. C. Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2003.

[26] A. Weil. L'arithmétique sur les courbes algébriques. *Acta mathematica*, 52(1):281–315, 1929.