Abelian Divison Fields Over Real Quadratic Fields

Alex Abrams Tesfa Asmara David W. Bonds, Jr. Aniyah Stephen

August 1, 2023

Our Project

- We want to look at extension fields that arise from elliptic curves and points on those curves of specified order.
- When are the Galois groups corresponding to these fields abelian?

Outline

Outline

1. Definitions
2. Goal
3. Narrowing Our Search
4. Results

Extension Field

Definition

Given fields K and F, we say K is an **extension field** of F if $F \subseteq K$. We denote this as K/F.

- When you add something to a field, you have to add additional elements to make sure you still have a field.

Examples

$$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$$
$$\mathbb{Q}(\sqrt[3]{19}) = \{a + b\sqrt[3]{19} + c(\sqrt[3]{19})^2 \mid a, b, c \in \mathbb{Q}\}$$
$$\mathbb{Q}(i, \sqrt{2}) = \{a + b\sqrt{2} + ci + di\sqrt{2} \mid a, b, c, d \in \mathbb{Q}\}$$

For an extension K/F, we call the field F the **base field**.

Why Extension Fields

Question

The polynomial $x^2 - 5$ does not factor in $\mathbb{Q}$. What is the smallest field where it can?

Why Extension Fields

Question

The polynomial $x^2 - 5$ does not factor in $\mathbb{Q}$. What is the smallest field where it can?

Answer

$\mathbb{Q}(\sqrt{5})$

Why Extension Fields

Question

The polynomial $x^2 - 5$ does not factor in $\mathbb{Q}$. What is the smallest field where it can?

Answer

$\mathbb{Q}(\sqrt{5})$

If K/F is a field extension, then K is a vector space over F and the **degree of K over F** is the dimension.

Elliptic Curves

Introduction

An elliptic curve, E, over $\mathbb{Q}$ can be defined by an equation of the form $y^2 = x^3 + Ax + B$, where A,B $\in \mathbb{Q}$ and $\Delta_E = -16(4A^3 + 27B^2) \neq 0$.

Elliptic Curves

Introduction

An elliptic curve, E, over $\mathbb{Q}$ can be defined by an equation of the form $y^2 = x^3 + Ax + B$, where A,B $\in \mathbb{Q}$ and $\Delta_E = -16(4A^3 + 27B^2) \neq 0$.

The discriminant, Δ_E, of an elliptic curve E defined over $\mathbb{Q}$, is a nonzero integer (when $\Delta_E \neq 0$, the equation $x^3 + Ax + B$ has distinct roots over the complex numbers). We require $\Delta_E \neq 0$ because it is necessary for the elliptic curve to have a group structure.

Elliptic Curves

Introduction

An elliptic curve, E, over $\mathbb{Q}$ can be defined by an equation of the form $y^2 = x^3 + Ax + B$, where A,B $\in \mathbb{Q}$ and $\Delta_E = -16(4A^3 + 27B^2) \neq 0$.

The discriminant, Δ_E, of an elliptic curve E defined over $\mathbb{Q}$, is a nonzero integer (when $\Delta_E \neq 0$, the equation $x^3 + Ax + B$ has distinct roots over the complex numbers). We require $\Delta_E \neq 0$ because it is necessary for the elliptic curve to have a group structure.

Elliptic Curves have been used in Cryptography and to prove

- Fermat's Last Theorem
- Gauss's Class#1 Conjecture

Group Law on Elliptic Curves

Definition

We denote $E(\mathbb{Q})$ as the set of points (x, y) such that x and y are rational numbers that satisfy $y^2 = x^3 + Ax + B$ along with a point at infinity, denoted O_E.

Group Law on Elliptic Curves

Definition

We denote $E(\mathbb{Q})$ as the set of points (x, y) such that x and y are rational numbers that satisfy $y^2 = x^3 + Ax + B$ along with a point at infinity, denoted O_E.

Proposition

1. There exists a binary operation $\oplus$ such that $(E(\mathbb{Q}), \oplus)$ is an abelian group with identity O_E.
2. Points P, Q, R on $E(\mathbb{Q})$ lie on a line if and only if $P \oplus Q \oplus R = O_E$.

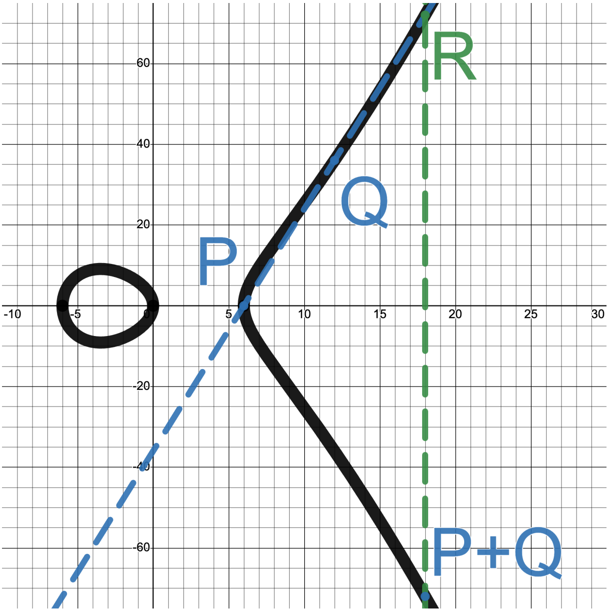


Figure: The Chord-and-Tangent Construction on $E : y^2 = x^3 - 36x$

Torsion Points

Definition

A point $P \in E(\mathbb{Q})$ has **order** n if n is the smallest positive integer such that

$$[n]P = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n \text{ times}} = O_E$$

.

If such n exists, P is said to have finite order, otherwise it has infinite order.

Torsion Points

Definition

A point $P \in E(\mathbb{Q})$ has **order** n if n is the smallest positive integer such that

$$[n]P = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n \text{ times}} = O_E$$

.

If such n exists, P is said to have finite order, otherwise it has infinite order.

Definition

A point $P \in E(\mathbb{Q})$ is called a **torsion point** if it has finite order.

Demonstration of the Group Law on Torsion Points

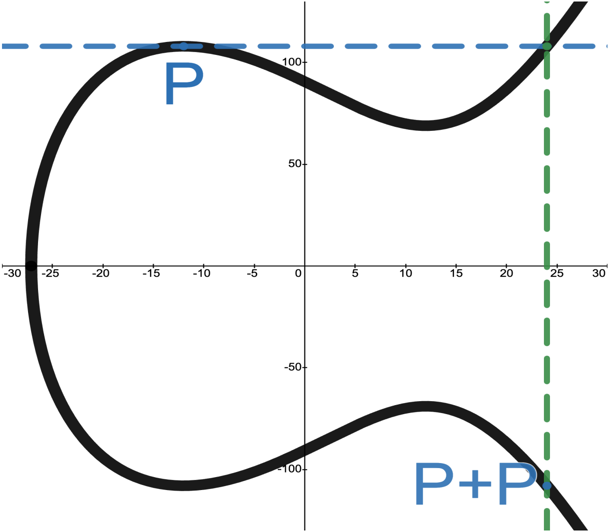


Figure: Computation of P+P on $E : y^2 = x^3 - 432 * x + 8208$

Demonstration of the Group Law on Torsion Points

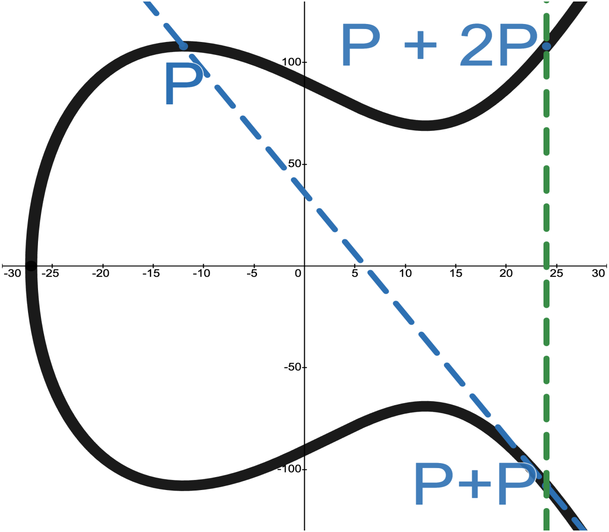


Figure: Computation of P+2P on $E : y^2 = x^3 - 432 * x + 8208$

Demonstration of the Group Law on Torsion Points

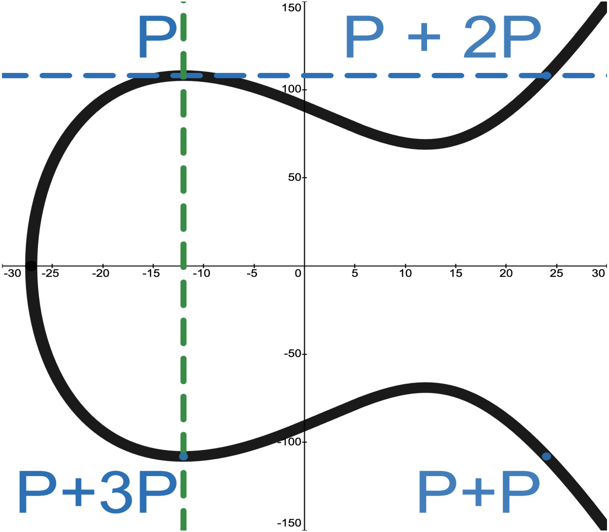


Figure: Computation of P+3P on $E : y^2 = x^3 - 432 * x + 8208$

Demonstration of the Group Law on Torsion Points

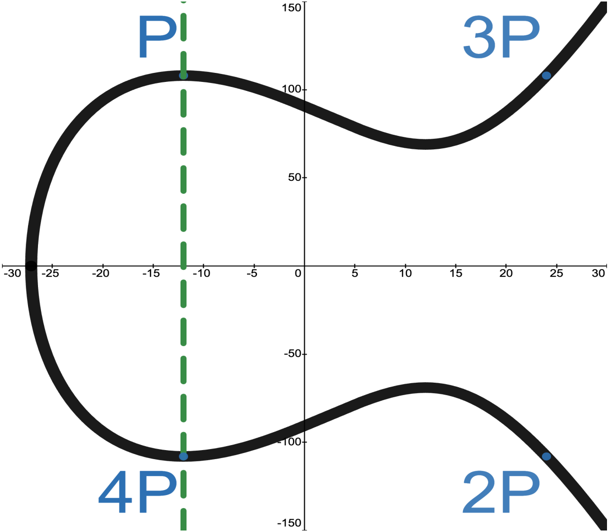


Figure: All of the 5-torsion points and O_E on $E : y^2 = x^3 - 432 * x + 8208$

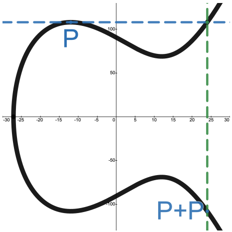


Figure: Computation of P+P

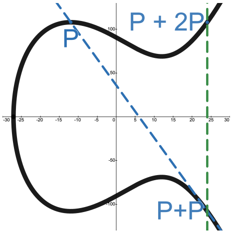


Figure: Computation of P+2P

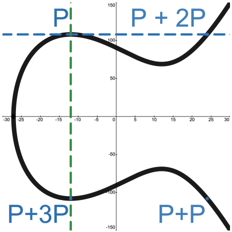


Figure: Computation of P+3P

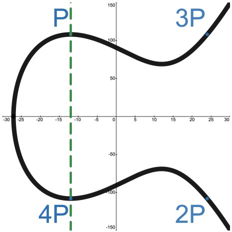


Figure: All 5-torsion points and O_E

Torsion Points

Definition

The set of rational torsion points for an elliptic curve E denoted $E(\mathbb{Q})_{\text{tors}}$.

Theorem (Mordell-Weil, 1928)

The group of rational points on an elliptic curve denoted $E(\mathbb{Q})$ is a finitely generated abelian group.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$$

Mazur's Theorem

Theorem (Mazur, 1977-1978)

Let E be an elliptic curve over $\mathbb{Q}$. If $P \in E(\mathbb{Q})_{\text{tors}}$ is a point of prime order p, then $p < 11$.

- This tells us there are no non-trivial rational prime p-torsion points when $p \geq 11$.
- There are also no non-trivial rational n-torsion points when n is a multiple of a prime $p \geq 11$.

Division Fields

Definition

Let E be an elliptic curve. Let K be a field. The **n-th division field of E/K** denoted $K(E[n])/K$ is an extension field of K with all the points of n torsion.

Division Fields

Definition

Let E be an elliptic curve. Let K be a field. The **n-th division field of E/K** denoted $K(E[n])/K$ is an extension field of K with all the points of n torsion.

- All division fields are Galois extensions.
- In these extensions, the automorphism group is called the **Galois group** and is denoted by $\mathrm{Gal}(K(E[n])/K)$.

Division Fields

Definition

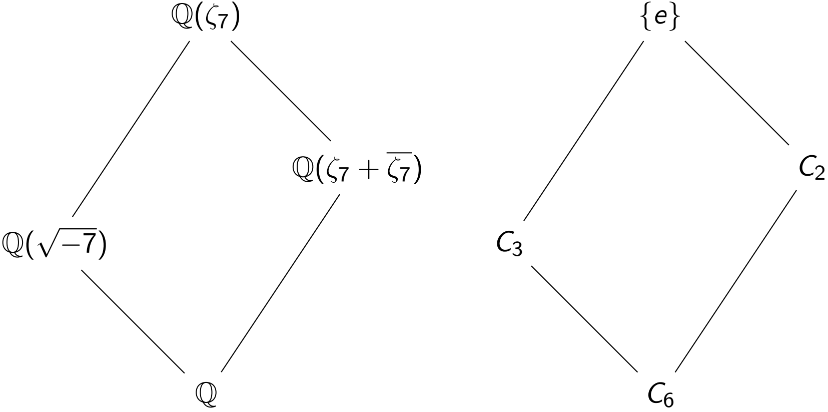
Let E be an elliptic curve. Let K be a field. The **n-th division field of E/K** denoted $K(E[n])/K$ is an extension field of K with all the points of n torsion.

- All division fields are Galois extensions.
- In these extensions, the automorphism group is called the **Galois group** and is denoted by $\mathrm{Gal}(K(E[n])/K)$.

Definition

A division field is **abelian** if its corresponding Galois group is abelian.

By the Fundamental Theorem of Galois Theory, there is a correspondence between the subfield structure of Galois extensions and the structure of the subgroups of the Galois group.



Cyclotomic Fields

Definition

We say that ζ_n is a primitive nth root of unity when $\zeta_n^n = 1$ and $\zeta_n^k \neq 1$ for $1 \leq k < n$.

Cyclotomic Fields

Definition

We say that ζ_n is a primitive nth root of unity when $\zeta_n^n = 1$ and $\zeta_n^k \neq 1$ for $1 \leq k < n$.

ζ_4 example: $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$

Cyclotomic Fields

Definition

We say that ζ_n is a primitive nth root of unity when $\zeta_n^n = 1$ and $\zeta_n^k \neq 1$ for $1 \leq k < n$.

ζ_4 example: $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$

Definition

The nth cyclotomic field is the extension $\mathbb{Q}(\zeta_n)$.

Weil Pairing

Theorem: Weil-Pairing (Weil, 1940)

Let K be a field, ζ_n be a primitive nth root of unity where $n \in \mathbb{Z}^+$, and E be an elliptic curve over K. Then, $K(\zeta_n) \subseteq K(E[n])$.

Weil Pairing

Theorem: Weil-Pairing (Weil, 1940)

Let K be a field, ζ_n be a primitive nth root of unity where $n \in \mathbb{Z}^+$, and E be an elliptic curve over K. Then, $K(\zeta_n) \subseteq K(E[n])$.

By the Weil-Pairing, for each $n \geq 3$, we know that there is a quadratic extension field F such that $F \subseteq \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\mathrm{E}[n])$.

Weil Pairing

Theorem: Weil-Pairing (Weil, 1940)

Let K be a field, ζ_n be a primitive nth root of unity where $n \in \mathbb{Z}^+$, and E be an elliptic curve over K. Then, $K(\zeta_n) \subseteq K(E[n])$.

By the Weil-Pairing, for each $n \geq 3$, we know that there is a quadratic extension field F such that $F \subseteq \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\mathrm{E}[n])$.

We have $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(\mathrm{E}[3])$

Similarly, we have $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(\mathrm{E}[5])$

as well as, $\mathbb{Q}(\sqrt{-7}) \subseteq \mathbb{Q}(\zeta_7) \subseteq \mathbb{Q}(\mathrm{E}[7])$

Kronecker-Weber

Kronecker-Weber Theorem(Kronecker, 1853; Weber, 1886; Hilbert, 1895)

For a field L, if $L/\mathbb{Q}$ is an abelian extension, then $L \subseteq \mathbb{Q}(\zeta_n)$ where $n \in \mathbb{Z}$.

Previous Work on Division Fields

Theorem (González-Jiménez and Lozano-Robledo, 2017)

In "Elliptic Curves with Abelian Division Fields", Enrique González-Jiménez and Álvaro Lozano-Robledo showed for which curves the n-th division field is as small as possible, meaning that $\mathbb{Q}(\zeta_n) = \mathbb{Q}(E[n])$, which is only possible when $n = 2, 3, 4$, or 5.

Previous Work on Division Fields

Theorem (González-Jiménez and Lozano-Robledo, 2017)

They also determined for which n a field $\mathbb{Q}(E[n])$ is contained in some cyclotomic extension of $\mathbb{Q}$ or, equivalently, when $\mathbb{Q}(E[n])/\mathbb{Q}$ is an abelian extension. This only happens when $n = 2, 3, 4, 5, 6$, or 8.

$\mathrm{GL}_2(\mathbb{F}_p)$

Let $\mathbb{F}_p$ be the field with p elements, where p is prime. The group $\mathrm{GL}_2(\mathbb{F}_p)$ is

$$\mathrm{GL}_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \not\equiv 0 \pmod{p} \right\}.$$

$\mathrm{GL}_2(\mathbb{F}_p)$

Definition

Let $E[p]$ denote the set of p-torsion points of the elliptic curve E. This means that $E[p] = \{R \in E(\mathbb{Q}) \mid [p]R = O_E\}$.

$\mathrm{GL}_2(\mathbb{F}_p)$

Definition

Let $E[p]$ denote the set of p-torsion points of the elliptic curve E. This means that $E[p] = \{R \in E(\mathbb{Q}) \mid [p]R = O_E\}$.

The set $E[p]$ of p-torsion points is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. As a result, the set of automorphisms of $E[p]$ is isomorphic to $GL_2(\mathbb{F}_p)$.

$\mathrm{GL}_2(\mathbb{F}_p)$

Definition

Let $E[p]$ denote the set of p-torsion points of the elliptic curve E. This means that $E[p] = \{R \in E(\mathbb{Q}) \mid [p]R = O_E\}$.

The set $E[p]$ of p-torsion points is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. As a result, the set of automorphisms of $E[p]$ is isomorphic to $GL_2(\mathbb{F}_p)$.

Since each field automorphism of the field $\mathbb{Q}(E[p])$ will also be an automorphism of $E[p]$, $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ is isomorphic to a subgroup of $GL_2(\mathbb{F}_p)$.

Serre's Result

Theorem (Serre, 1972)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Let $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong G \subseteq GL_2(\mathbb{F}_p)$, and supppose $G \ncong GL_2(\mathbb{F}_p)$. Then, there is an $\mathbb{F}_p$-basis of $E[p]$ such that one of the following possibilities holds:

(1) G is contained in the normalizer of a split Cartan subgroup of $GL_2(\mathbb{F}_p)$, or

(2) G is contained in the normalizer of a non-split Cartan subgroup of $GL_2(\mathbb{F}_p)$, or

(3) The projective image of G in $PGL_2(\mathbb{F}_p)$ is isomorphic to A_4, S_4, or A_5, where S_n is the symmetric group and A_n is the alternating group, or

(4) G is contained in a Borel subroup of $GL_2(\mathbb{F}_p)$.

Why Serre's Result?

Key Points

- We find that Serre's result is important for our method to find specific Galois groups.

Why Serre's Result?

Key Points

- We find that Serre's result is important for our method to find specific Galois groups.
- We are only looking at elliptic curves defined over $\mathbb{Q}$ to see when $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ can become abelian over $\mathbb{Q}(\sqrt{5})$.

Why Serre's Result?

Key Points

- We find that Serre's result is important for our method to find specific Galois groups.
- We are only looking at elliptic curves defined over $\mathbb{Q}$ to see when $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ can become abelian over $\mathbb{Q}(\sqrt{5})$.
- Since the Galois groups in question are necessarily contained in certain subgroups of $GL_2(\mathbb{F}_p)$, we can narrow down our search to find what subgroups are even possible to become abelian over $\mathbb{Q}(\sqrt{5})$.

Non-CM Elliptic Curves

- **CM elliptic curves** are a special kind of elliptic curve.
- Serre's result applies to certain curves called **non-CM elliptic curves**.
- Most elliptic curves are non-CM elliptic curves.
- CM elliptic curves are known to have smaller division fields.
- We know what these curves are since there are 13 j-invariants that correspond to CM elliptic curves.

Definition

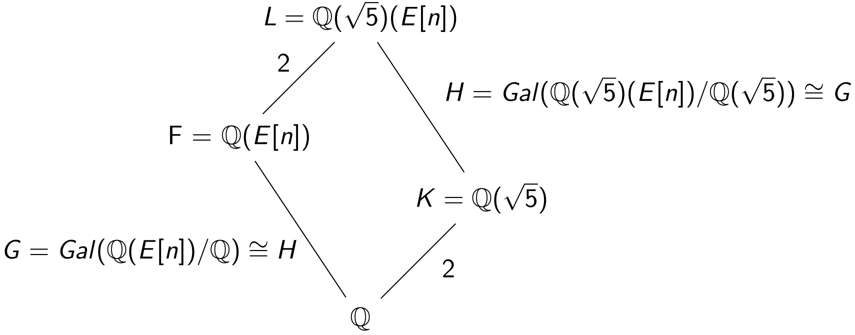
Given an elliptic curve defined by $y^2 = x^3 + Ax + B$, the **j-invariant** can be defined as

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

Outline

Our Question

- When are division fields of non-CM elliptic curves abelian over real quadratic fields?
- Specifically, when is $\mathbb{Q}(\sqrt{5})(E[n])/\mathbb{Q}(\sqrt{5})$ abelian?



General Method

- We want to start with choosing a prime p.
- We consider all the possible Galois groups of p division fields over an arbitrary non-CM elliptic curve.
- We determine whether or not $\mathbb{Q}(\sqrt{5})$ can be contained in these division fields.
- If that division field is not abelian over $\mathbb{Q}$, then we want to see if it is abelian over $\mathbb{Q}(\sqrt{5})$.
- We compute Galois groups and their subgroups to determine more about the fields and their subfields.

Outline

Abelian Division Fields Over $\mathbb{Q}$

Proposition

If $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian then $\mathbb{Q}(\sqrt{5}, E[n])/\mathbb{Q}(\sqrt{5})$ is abelian.

Abelian Division Fields Over $\mathbb{Q}$

Proposition

If $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian then $\mathbb{Q}(\sqrt{5}, E[n])/\mathbb{Q}(\sqrt{5})$ is abelian.

- González-Jiménez and Lozano-Robledo tells us when division fields are abelian over $\mathbb{Q}$.
- This gives us infinite examples of abelian division fields over $\mathbb{Q}(\sqrt{5})$.

Abelian Division Fields Over $\mathbb{Q}$

Proposition

If $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian then $\mathbb{Q}(\sqrt{5}, E[n])/\mathbb{Q}(\sqrt{5})$ is abelian.

- González-Jiménez and Lozano-Robledo tells us when division fields are abelian over $\mathbb{Q}$.
- This gives us infinite examples of abelian division fields over $\mathbb{Q}(\sqrt{5})$.
- We are interested when this is not the case.

Good Reduction

Proposition

Let $5 \nmid n$ and $5 \nmid \Delta_E$. If $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is non-abelian, then $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})(E[n])/\mathbb{Q}(\sqrt{5}))$ is non-abelian as well.

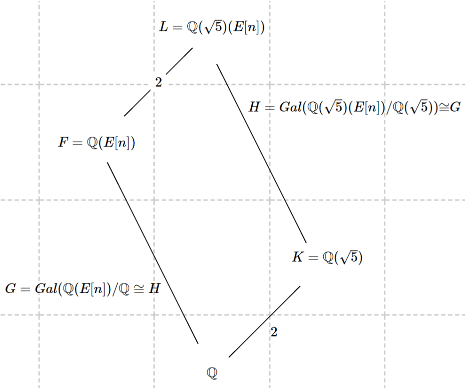
Good Reduction

Proposition

Let $5 \nmid n$ and $5 \nmid \Delta_E$. If $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is non-abelian, then $\text{Gal}(\mathbb{Q}(\sqrt{5})(E[n])/\mathbb{Q}(\sqrt{5}))$ is non-abelian as well.

In this case we are assuming that 5 is a prime of good reduction. When 5 is a prime of good reduction and $5 \nmid n$ we know a non-abelian n-division field will remain non-abelian over $\mathbb{Q}(\sqrt{5})$.

Good Reduction



Under these conditions $Gal(L/\mathbb{Q}(\sqrt{5})$ is isomorphic to Gal$(F/\mathbb{Q})$

Bad Reduction

Motivating Question

When can non-abelian over $\mathbb{Q}$ become abelian over $\mathbb{Q}(\sqrt{5})$?

Bad Reduction

Motivating Question

When can non-abelian over $\mathbb{Q}$ become abelian over $\mathbb{Q}(\sqrt{5})$?

Motivating Results

- The conditions for having a prime, in our case 5, be of bad reduction is that $5 \mid \Delta_E$.
- In order to have this occur $\sqrt{5}$ must be contained in $\mathbb{Q}(E[n])$ and this can only happen when $5 \mid n$ or $5 \mid \Delta E$. If $5 \mid n$, then by the Weil-Pairing, $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(E[n])$

Prime Division Fields

We have proven this result

Proposition

Let L, C, F be fields such that $F \subseteq C \subseteq L$. Let L/F be Galois, and let C/F be Galois. Then if $\mathrm{Gal}(C/F)$ is not abelian, $\mathrm{Gal}(L/F)$ is not abelian.

Which gives us a useful corollary

Corollary

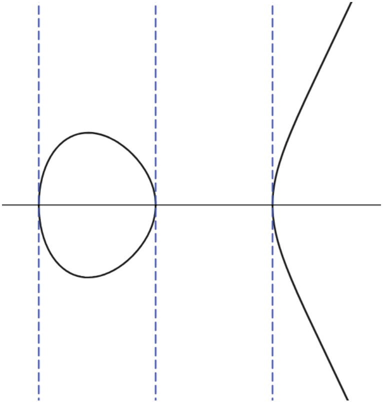
If $K(E[n])/K$ is not abelian, then $K(E[dn])/K$ is not abelian for $d \in \mathbb{Z}^+$. And if $K(E[dn])/K$ is abelian, then $K(E[n])/K$ is abelian.

$$\begin{array}{c} K(E[dn]) \\ | \\ K(E[n]) \\ | \\ K \end{array}$$

Outline

2 Division Fields

- Let E be the elliptic curve defined by $y^2 = x^3 + Ax + B$.
- The 2 division field of an elliptic curve is the field containing the roots of $x^3 + Ax + B$.



2 Division Fields

- The polynomial $x^3 + Ax + B$ can split in different ways producing different corresponding Galois groups for the 2 division field:

2 Division Fields

- The polynomial $x^3 + Ax + B$ can split in different ways producing different corresponding Galois groups for the 2 division field:
  1. All of it's roots could be in $\mathbb{Q}$ and thus it's division field is $\mathbb{Q}$. The corresponding Galois group is $\{e\}$.

2 Division Fields

- The polynomial $x^3 + Ax + B$ can split in different ways producing different corresponding Galois groups for the 2 division field:
  1. All of it's roots could be in $\mathbb{Q}$ and thus it's division field is $\mathbb{Q}$. The corresponding Galois group is $\{e\}$.
  2. If it has 1 rational root and 2 irrational roots, then the corresponding Galois group is C_2.

2 Division Fields

- The polynomial $x^3 + Ax + B$ can split in different ways producing different corresponding Galois groups for the 2 division field:
  1. All of it's roots could be in $\mathbb{Q}$ and thus it's division field is $\mathbb{Q}$. The corresponding Galois group is $\{e\}$.
  2. If it has 1 rational root and 2 irrational roots, then the corresponding Galois group is C_2.
  3. If all the roots are irrational and Δ_E is a perfect square, then the corresponding Galois group is C_3.

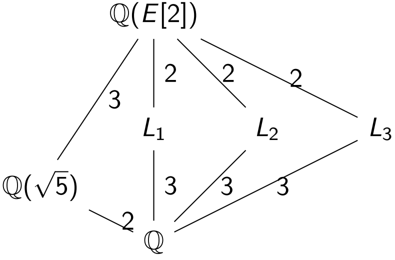
2 Division Fields

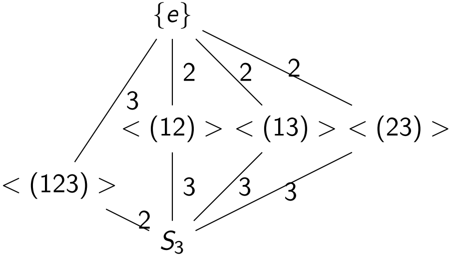
- The polynomial $x^3 + Ax + B$ can split in different ways producing different corresponding Galois groups for the 2 division field:
  1. All of it's roots could be in $\mathbb{Q}$ and thus it's division field is $\mathbb{Q}$. The corresponding Galois group is $\{e\}$.
  2. If it has 1 rational root and 2 irrational roots, then the corresponding Galois group is C_2.
  3. If all the roots are irrational and Δ_E is a perfect square, then the corresponding Galois group is C_3.
  4. If all the roots are irrational and Δ_E is not a perfect square, then the corresponding Galois group S_3.

2 Division Fields Becoming Abelian

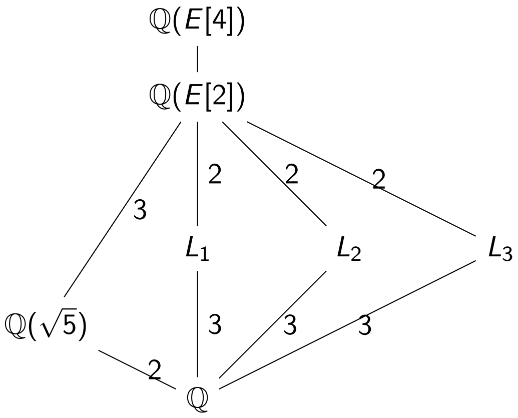
Theorem

If the 2 division field is an S_3 extension over $\mathbb{Q}$, then the 2 division field is abelian over $\mathbb{Q}(\sqrt{5})$ iff $\Delta_E = 5d$, where d is a perfect square.





4 Division Fields Becoming Abelian



Sub groups of $Gal(\mathbb{Q}(E[3])/\mathbb{Q})$

Theorem (Zywina, 2015)

$Gal(\mathbb{Q}(E[3])/\mathbb{Q})$ is isomorphic to one of the following subgroups of $GL_2(\mathbb{F}_3)$: $C_2, D_4, D_6, SD_{16}, S_3$, and $GL_2(\mathbb{F}_3)$.

Sub groups of $Gal(\mathbb{Q}(E[3])/\mathbb{Q})$

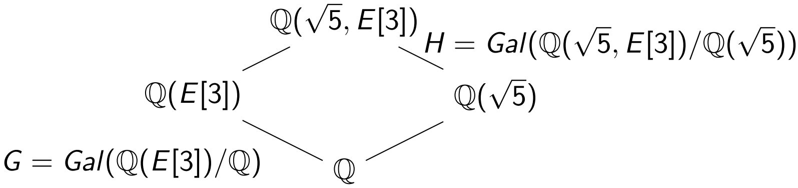
Theorem (Zywina, 2015)

$Gal(\mathbb{Q}(E[3])/\mathbb{Q})$ is isomorphic to one of the following subgroups of $GL_2(\mathbb{F}_3)$: $C_2, D_4, D_6, SD_{16}, S_3$, and $GL_2(\mathbb{F}_3)$.

Conjecture

If $Gal(\mathbb{Q}(E[3])/\mathbb{Q})$ is not abelian, then $Gal(\mathbb{Q}(E[3])/\mathbb{Q}(\sqrt{5}))$ is not abelian.

When $\mathbb{Q}(E[3])$ and $\mathbb{Q}(\sqrt{5})$ are Linearly Disjoint

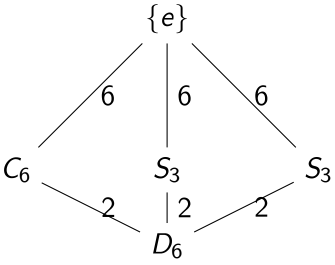


If $\mathbb{Q}(E[3])$ and $\mathbb{Q}(\sqrt{5})$ are linearly disjoint (i.e. $\mathbb{Q}(E[3]) \cap \mathbb{Q}(\sqrt{5}) = \mathbb{Q}$), then $H \cong G$. However, being not disjoint with $\mathbb{Q}(\sqrt{5})$, then it already contains $\mathbb{Q}(\sqrt{5})$ when you base change.

$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong D_6$

Proposition

The three subgroups of order six inside of D_6 are S_3, S_3, and C_6, which is the only abelian subgroup.

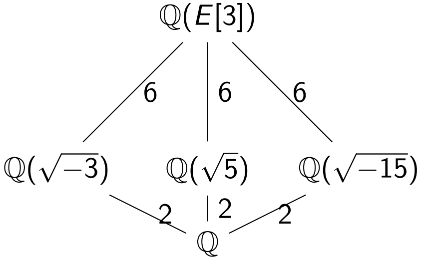


$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong D_6$

Theorem

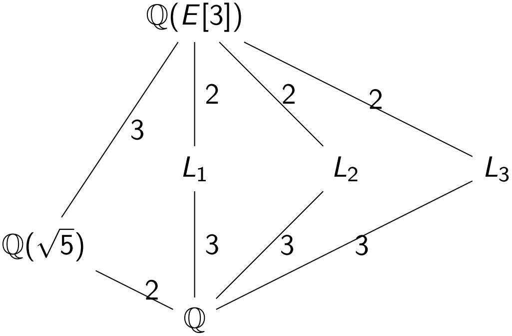
If $Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong D_6$, then $Gal(\mathbb{Q}(E[3])/\mathbb{Q}(\sqrt{5}))$ is also nonabelian.

When we look at the subgroup of D_6, we consider the corresponding matrices in $GL_2(\mathbb{F}_3)$. The determinants of the matrices that correspond to C_6 are always $1 \mod 3$ and, hence, correspond to the extension $\mathbb{Q}(\sqrt{-3})$.



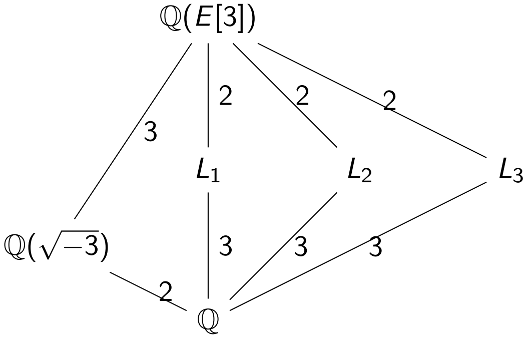
$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong S_3$

Consider that in order for $Gal(\mathbb{Q}(E[3])/\mathbb{Q}(\sqrt{5}))$ to be abelian, then $\mathbb{Q}(E[3])$ must contain $\mathbb{Q}(\sqrt{5})$ as depicted in the following diagram:



$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong S_3$

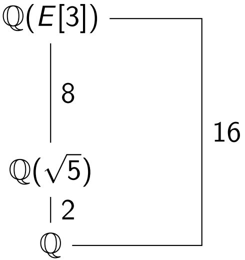
However, we know that this can never be the case because $\mathbb{Q}(\sqrt{-3})$ is the unique quadratic field in $\mathbb{Q}(E[3])$ since $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(E[3])$ and $\mathbb{Q}(\sqrt{-3})$ is degree 2 over $\mathbb{Q}$.



$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong SD_{16}$

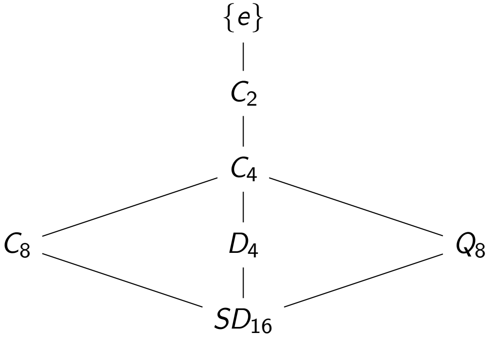
Proposition

Since $\mathbb{Q}(\sqrt{5})$ is a degree two extension, the corresponding field must have relative Galois group $Gal(\mathbb{Q}(E[3])/\mathbb{Q}(\sqrt{5}))$ that has order $16/2 = 8$. This is because SD_{16}, which is not abelian over $\mathbb{Q}$, has order 16.



$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong SD_{16}$

Up to isomorphism, there are only two subgroups of order eight in SD_{16}, namely Q_8 and C_8. C_8 is abelian and the nonsplit Cartan subgroup of $GL_2(\mathbb{F}_3)$. That nonsplit Cartan subgroup is the relative Galois group of an imaginary quadratic extension inside of $\mathbb{Q}(E[3])$.



$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong SD_{16}$

Since C_8 corresponds to an imaginary field which is not over $\mathbb{Q}(\sqrt{-3})$ nor $\mathbb{Q}(\sqrt{5})$, then we know that the relative Galois group $Gal(\mathbb{Q}(E[3])/\mathbb{Q}(\sqrt{5}))$ is not isomorphic to C_8.

Theorem

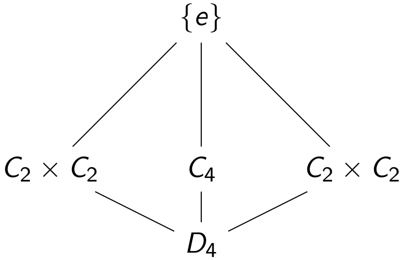
If $Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong SD_{16}$, then $Gal(\mathbb{Q}(E[3])/\mathbb{Q}(\sqrt{5}))$ is not abelian.

$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong D_4$

Now to introduce the problem child of the 3rd division field's Galois group, D_4.

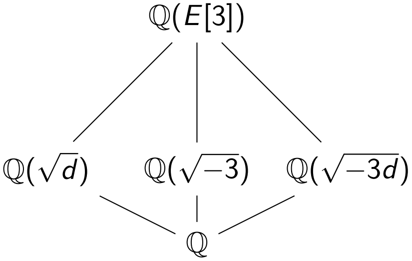
$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong D_4$

Now to introduce the problem child of the 3rd division field's Galois group, D_4.



In the diagram we see that D_4 has these three subgroups of index 2 and we want to rule out that $\mathbb{Q}(\sqrt{5})$ could ever be one of the corresponding quadratic fields.

$Gal(\mathbb{Q}(E[3])/\mathbb{Q}) \cong D_4$



BOOO 5! GO HOME

- If 5 does appear then this field diagram would go from non-abelian D_4 to some abelian order 4 group, and every order 4 group is abelian.
- We've worked over 1000's of curves where 5 was of bad reduction and we found no examples, concluding that 5 will never happen.

$Gal(\mathbb{Q}(E[5])/\mathbb{Q})$

A paper of Zywina's classify all possible subgroups of $GL_2(\mathbb{F}_5)$ that appear as the galois group of a 5 division field for some elliptic curve, $E/\mathbb{Q}$.

$Gal(\mathbb{Q}(E[5])/\mathbb{Q})$

- $C_2 \times C_4$
- C_4^2
- OD_{16}
- $C_4 \wr C_2$
- $C_2 \times F_5$
- $C_{24} : C_2$
- $C_4 \times F_5$
- $C_4.S_4$
- C_4
- F_5

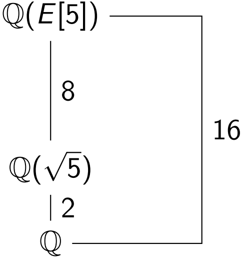
$Gal(\mathbb{Q}(E[5])/\mathbb{Q})$

- $C_2 \times C_4$
- C_4^2
- OD_{16}
- $C_4 \wr C_2$
- $C_2 \times F_5$
- $C_{24} : C_2$
- $C_4 \times F_5$
- $C_4.S_4$
- C_4
- F_5

$Gal(\mathbb{Q}(E[5])/\mathbb{Q}) \cong OD_{16}$

Proposition

Since $\mathbb{Q}(\sqrt{5})$ is a degree two extension, the corresponding field must have relative Galois group $Gal(\mathbb{Q}(E[5])/\mathbb{Q}(\sqrt{5}))$ that has order $\frac{16}{2} = 8$. This is because OD_{16}, which is not abelian over $\mathbb{Q}$, has order 16.



$Gal(\mathbb{Q}(E[5])/\mathbb{Q}) \cong OD_{16}$

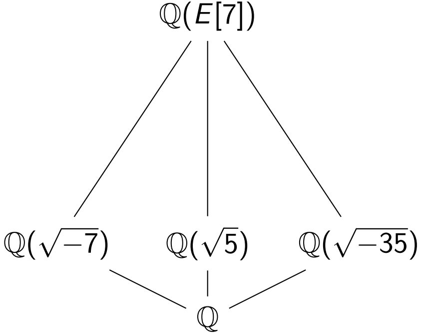
Up to isomorphism, there are only two subgroups of order 8 in OD_{16}, namely $C_4 \times C_2$ and C_8 both of which are abelian.

Theorem

If $Gal(\mathbb{Q}(E[5])/\mathbb{Q}) \cong OD_{16}$, then $Gal(\mathbb{Q}(E[5])/\mathbb{Q}(\sqrt{5}))$ is abelian.

$Gal(\mathbb{Q}(E[7])/\mathbb{Q})$

If $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(E[7])/\mathbb{Q}$, then $\mathbb{Q}(E[7])$ has 3 quadratic subfields: $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-35})$. This means Gal($\mathbb{Q}(E[7])/\mathbb{Q}$) has 3 index 2 subgroups. Since the Galois group is a subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$, we only need to look at subgroups of $\mathrm{GL}_2(\mathbb{F}_7)$ which have at least 3 index 2 subgroups.



$Gal(\mathbb{Q}(E[7])/\mathbb{Q})$

Group	Order
C_6^2	36
$C_6 \times S_3$	36
$C_2 \times F_7$	84
$C_6 \times D_7$	84
$C_6 \wr C_2$	72
$C_6 \times F_7$	252
$C_3 \times \mathrm{SD}_{32}$	96

Table: Possible Subgroups of $\mathrm{GL}_2(\mathbb{F}_7)$ up to isomorphism

These groups are subgroups of $\mathrm{GL}_2(\mathbb{F}_7)$ that can appear as Galois groups of 7-division fields over $\mathbb{Q}$ that have at least 3 subgroups of index 2.

$Gal(\mathbb{Q}(E[7])/\mathbb{Q})$

Group	Order
C_6^2	36
$C_6 \times S_3$	36
$C_2 \times F_7$	84
$C_6 \times D_7$	84
$C_6 \wr C_2$	72
$C_6 \times F_7$	252
$C_3 \times \mathrm{SD}_{32}$	96

Table: Possible Subgroups of $\mathrm{GL}_2(\mathbb{F}_7)$ up to isomorphism

These groups are subgroups of $\mathrm{GL}_2(\mathbb{F}_7)$ that can appear as Galois groups of 7-division fields over $\mathbb{Q}$ that have at least 3 subgroups of index 2.

So far, the potential groups with index 2 subgroups that could become abelian after a base change to $\mathbb{Q}(\sqrt{5})$ are: $C_6 \times S_3$, $C_6 \wr C_2$, and $C_3 \times \mathrm{SD}_{32}$.

Future Works

- We plan to finish our work in 3 and 7 division fields. We also plan to follow up on some promising results in 4 and 10 division fields.
- We would like to determine which other primes p and composites n can give us abelian extensions over $\mathbb{Q}(\sqrt{5})$.
- We would like to look at division fields of elliptic curves that are defined over $\mathbb{Q}(\sqrt{5})$ and not over $\mathbb{Q}$.
- We would also like to extend this work to CM elliptic curves as well.

Acknowledgements

Professor Edray Herber Goins
Professor Alex Barrios
Professor Lori D. Watson
Mark Curiel
Olivia Del Guercio
Fabian Ramirez
Cameron Thomas
Japheth Varlack 
Professor Jeremy Rouse
Elise Farr
Pomona College
National Science Foundation (DMS-2113782)

References

Harris B. Daniels and Enrique González-Jiménez.
Serre's constant of elliptic curves over the rationals.
Experimental Mathematics, 31(2):518–536, dec 2019.

Enrique González-Jiménez and Álvaro Lozano-Robledo.
Elliptic curves with abelian division fields.
Mathematische Zeitschrift, 283(3-4):835–859, feb 2016.

Jean-Pierre Serre.
Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.
Invent. Math., 15:259–331, 12 1971.

Andrew V. Sutherland.
Computing images of galois representations attached to elliptic curves.
Cambridge University Press, Forum of Mathematics, Sigma, 4, 2016.

David Zywina.
On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$, 2015.