# Abelian Division Fields Over Real Quadratic Fields

Alex Abrams (Loyola Marymount University), Tesfa Asmara (Pomona College),
David W. Bonds, Jr. (California State University Los Angeles), Aniyah Stephen (Hartwick College)
Pomona Research in Mathematics Experience (PRiME)

## Abstract

An $n$ division field of an elliptic curve is an extension field containing all points of n torsion. It is of interest to find when these fields are abelian. Previously, Enrique González-Jiménez and Álvaro Lozano-Robledo showed what $n$ it is possible to have abelian division fields for elliptic curves defined over $\mathbb{Q}$.
In this project we investigate when abelian division fields of non-CM elliptic curves arise after a base change from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{5})$.

## Elliptic Curves

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 Group Law on an Elliptic Curve

There exists a binary operation $\oplus$ such that $(E(\mathbb{C}), \oplus)$ forms a group with $O_E$ as the identity. This operation is known as the **group law** on the elliptic curve. Its construction is known as the **chord-and-tangent method.**

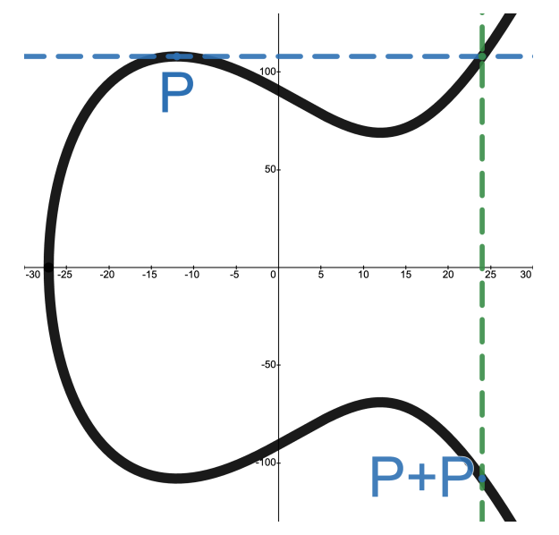

Figure 1:Computation of P+P

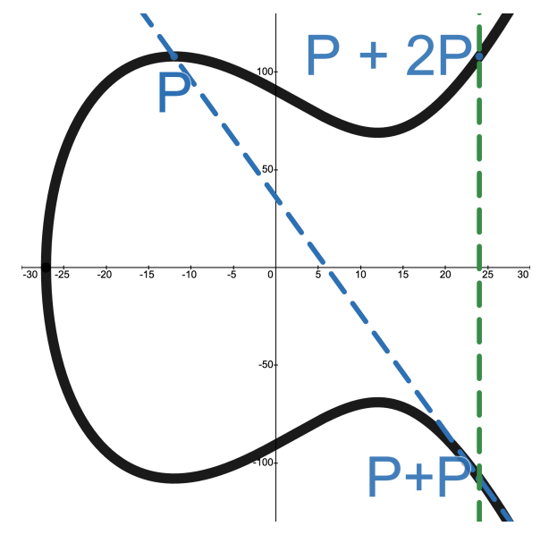

Figure 2:Computation of P+2P

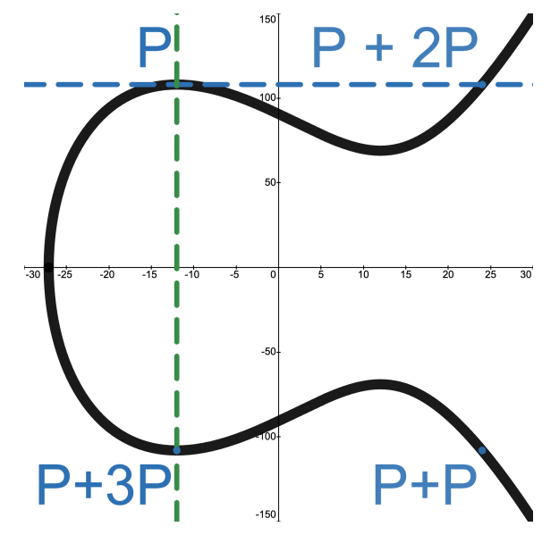

Figure 3:Computation of P+3P

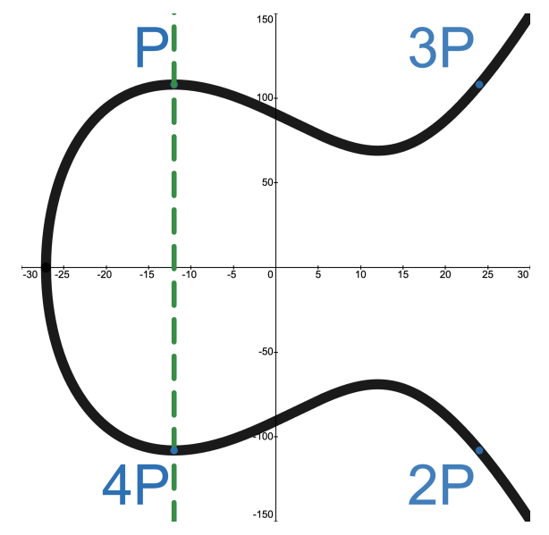

Figure 4:All 5-torsion points and $O_E$

A point $P \in E(\mathbb{Q})$ has **order** $n$ if $n$ is the smallest positive integer such that $nP = P \oplus P \oplus \cdots \oplus P = O_E$. If no such $n$ exists, $P$ has **infinite order**.
A point $P \in E(\mathbb{Q})$ is called a **torsion point** if it has finite order.

## Division Fields

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. This means $K(E[n])/K$ has a Galois group which fixes $K$.
A division field is **abelian** if its corresponding Galois group is abelian.

## Abelian Division Fields Over $\mathbb{Q}$

- Enrique González-Jiménez and Álvaro Lozano-Robledo previously determined all of the integers $n$ for which there is some elliptic curve $E/\mathbb{Q}$ such that $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian.
- They proved when $\mathbb{Q}(E[n])$ is as small as possible, that is, when $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, and this is only possible when $n =$ 2,3,4,or 5.
- They were also able to classify all curves such that $\mathbb{Q}(E[n])/\mathbb{Q}$ is an abelian extension and this only happens when $n =$ 2,3,4,5,6, or 8.
- They classified the possible Galois groups that occur for each value of $n$.
- They also used the Weil pairing theorem to see when $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$.

## Motivating Questions

For what values of n can the n-th division field become abelian over the real quadratic field $\mathbb{Q}(\sqrt{5})$ if it wasn't abelian over $\mathbb{Q}$?

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

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

## Method

- We want to start with choosing a prime $p$.
- We consider all the possible $p$-division fields for non-CM elliptic curves.
- 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.

## Narrowing the Possibilities

**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 $\mathbb{Q}$. The examples of abelian division fields over $\mathbb{Q}$ they have also stay abelian over $\mathbb{Q}(\sqrt{5})$.

**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.

This means that if we want division field to go from non-abelian over $\mathbb{Q}$ to abelian over $\mathbb{Q}(\sqrt{5})$, we want to look at curves where $5 \mid n$ or $5 \mid \Delta_E$.

**Proposition**: 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.

This proposition tells us that if we can say something about prime division fields being non-abelian, then we can say that multiples of those primes produce non-abelian division fields.

Let

$$p^* = \begin{cases} p & \text{if } p \equiv 1 \pmod 4 \\ -p & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

where $p \neq 5$.
With this, the $p$ division field has subfields as follows:

$$\begin{tikzcd}
 & \mathbb{Q}(E[p]) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{p^*}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{5}) \arrow[d, dash] & \mathbb{Q}(\sqrt{5p^*}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

A result by Serre [3] tells us the possibile subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ can be isomorphic to. This result only holds for **non-CM elliptic curves**.
In the above case, we have 3 degree 2 extensions over $\mathbb{Q}$. This means the corresponding Galois group of the $p$ division field has 3 index 2 subgroups.
When we are in these cases, we only need to consider subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ which have 3 index 2 subgroups.

## 2 Division Fields

- The 2 division field of an elliptic curve is the field containing the roots of $x^3 + Ax + B$.
- The polynomial $x^3 + Ax + B$ can split in different ways producing different corresponding Galois groups:
  1. All of it's roots could be in $\mathbb{Q}$ and $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \{e\}$.
  2. If it has 1 rational root and 2 irrational roots, $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong C_2$.
  3. If the roots are irrational and $\Delta_E$ is a perfect square, then $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong C_3$.
  4. If the roots are irrational and $\Delta_E$ is not a perfect square, then $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$.
- All of those are abelian except for the $S_3$ case. For this, we have found a result:

### Theorem

If $Gal(\mathbb{Q}(E[2])/\mathbb{Q})$ is isomorphic to $S_3$, then $Gal(\mathbb{Q}(E[2])/\mathbb{Q}(\sqrt{5}))$ is abelian if and only if $\Delta_E = 5d$, where $d$ is a perfect square.

## 3 Division Fields

- The 3 division field of an elliptic curve is the smallest field containing the 3-torsion points of the elliptic curve.
- $Gal(\mathbb{Q}(E[3])/\mathbb{Q})$ is isomorphic to the following subgroups of $GL_2(\mathbb{F}_3)$: $C_2, D_4, D_6, SD_{16}$, and $S_3$.

### Theorem

If $Gal(\mathbb{Q}(E[3])/\mathbb{Q})$ is isomorphic to $D_6$, $S_3$, or $SD_{16}$, then $Gal(\mathbb{Q}(E[3])/\mathbb{Q}(\sqrt{5}))$ remains nonabelian.

## 5 Division Field

- The 5 division field of an elliptic curve is the smallest field containing the 5-torsion points of the elliptic curve.
- $Gal(\mathbb{Q}(E[5])/\mathbb{Q})$ is isomorphic to one of the following: $C_2 \times C_4, C_4^2, OD_{16}, C_4 \wr C_2, C_2 \times F_5, C_{24} : C_2, C_4 \times F_5, C_4, F_5$, or $GL_2(\mathbb{F}_5)$.

### Theorem

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

$$\begin{tikzcd}
\mathbb{Q}(E[5]) \arrow[d, dash] \arrow[dd, dash, bend left=60, "G"] \\
\mathbb{Q}(\zeta_5) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{5}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

## 7 Division Field

- 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: $C_6^2$, $C_6 \times S_3$, $C_2 \times F_7$, $C_6 \times D_7$, $C_6 \wr C_2$, $C_6 \times F_7$, and $C_3 \times \mathrm{SD}_{32}$.
- Since $C_6^2$ is abelian already, we know it will stay abelian after a base change to $\mathbb{Q}(\sqrt{5})$. We have already excluded the others either by some theoretical argument or by computing determinants.
- So far, $C_6 \times S_3$, $C_6 \wr C_2$, and $C_3 \times \mathrm{SD}_{32}$ are the potential index 2 subgroups that could become abelian after a base change to $\mathbb{Q}(\sqrt{5})$.

## Future Work

- 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.

## References

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

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

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

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

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

## Acknowledgements

- Dr. Edray Herber Goins (Pomona College)
- Dr. Alex Barrios (University of St. Thomas)
- Dr. Lori D. Watson (Trinity College)
- Dr. Jeremy Rouse (Wake Forest University)
- Japheth Varlack (Wake Forest University)
- Dr. Álvaro Lozano-Robledo (University of Connecticut)
- Department of Mathematics, Pomona College
- National Science Foundation (DMS-2113782)

- Research at PRiME was supported by the National Science Foundation award DMS-2113782.
- Any opinions, findings, and conclusions or recommendations expressed in this article are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.