Abelian Divison Fields Over Real Quadratic Fields

Alex Abrams Tesfa Asmara David Bonds Aniyah Stephen

Japheth Varlack Lori D. Watson

PRiME 2023

1 Background

Enrique González-Jiménez and Álvaro Lozano-Robledo wrote a paper in 2017 and were able to 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 [8]. In their paper they proved for all curves $E/\mathbb{Q}$ such that $\mathbb{Q}(E[n])$ 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 $\mathbb{Q}(E[n])$ is contained in a cyclotomic extension of $\mathbb{Q}$ or, equivalently, when $\mathbb{Q}(E[n])/\mathbb{Q}$ is an abelian extension and this only happens when n = 2,3,4,5,6, or 8 and they also classified the possible Galois groups that occur for each value of n. They also used the Weil pairing thm to see when $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$ are equal and to be more specific to $\mathbb{Q}$.

2 Defintions

Definition 2.1. An abelian extension is a Galois extension whose Galois group is abelian.

Definition 2.2. Galois extension: Let L/F be a Galois extension if $|Aut(L/F)| = [L : F]$. And if L/F is Galois we call $Aut(L/F) := Gal(L/F)$ a Galois Group.

Definition 2.3. Isogeny: A morphism of algebraic groups (also known as group varieties) that is surjective and has a finite kernel.

Definition 2.4. $GL_2(F_p)$: The general linear group over F_p is the group of 2 x 2 invertible matrices with $x_i \in F_p$ with det(M) $\neq 0$.

Definition 2.5. Kronecker - Weber Theorem: Every finite abelian extension of the rational number field $\mathbb{Q}$ is contained within some cyclotomic field.

Definition 2.6. Division Field for an Elliptic Curve: The m-th division field is the field generated over K by the coordinates of the m-torsion points of an elliptic curve E; we denote it as $K(E[m])/K$.

3 Our Goal

For our project, we wanted to extend the work of Enrique and Álvaro to determine when division fields over non-CM elliptic curves are abelian over real quadratic fields. Specifically, we want to determine when $K(E[n])/K$ is abelian when K is the real quadratic field $\mathbb{Q}(\sqrt{5})$.

Over the period of this program, we set out with this goal in hopes of generalizing results from this to other real quadratic fields. We started by looking at curves that could be defined over $\mathbb{Q}(\sqrt{5})$ but not over $\mathbb{Q}$. We later specified to only looking at division fields of elliptic curves defined over $\mathbb{Q}$ which could be defined over $\mathbb{Q}(\sqrt{5})$ as well. This was a better specification as we

could work more closely off Enrique and Álvaro's work, which tells us about division fields over $\mathbb{Q}$.

Our process involved looking at large example sets of elliptic curves. First curves defined over $\mathbb{Q}(\sqrt{5})$, and then some defined over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$. We managed to gather tens of thousands of examples thanks to LMFDB, a database of curves and other related objects. In the next section, we will discuss specifically what we wanted to look for when gathering some of these datasets.

In these example sets, we wanted to look at curves which have non-abelian division fields over $\mathbb{Q}$ but are abelian over $\mathbb{Q}(\sqrt{5})$. This proved to be difficult as we wanted to do work in the SageMath algebra system, but Sage provides no way to calculate Galois groups over $\mathbb{Q}(\sqrt{5})$. The system always assumes you want the Galois group over $\mathbb{Q}$. We attempted to get around this by creating our own code to calculate the Galois group over $\mathbb{Q}(\sqrt{5})$, but it constantly ran too slow of did not compute what we wanted it to. In addition, calculating Galois groups over $\mathbb{Q}$ to check if division fields are non-abelian is slow computationally. This meant we could only really check n division fields for small prime n, such as 2,3, and 5.

Eventually we switch to the Magma algebra software, which could check the conditions we wanted much faster. We were able together a few examples of various prime division fields and form our conjectures from that work.

4 Narrowing The Search

We started by showing some propositions that would help us to narrow down what curves would have the properties we want. As a consequence of the Néron-Ogg-Shafarevich Criterion, we have the following:

Proposition 4.1. *Let $5 \nmid n$ and $5 \nmid \Delta_E$. If Gal$(\mathbb{Q}(E[n])/\mathbb{Q})$ is non-abelian, then Gal$(\mathbb{Q}(\sqrt{5})(E[n])/\mathbb{Q}(\sqrt{5}))$ is non-abelian as well.*

Proof. Assume 5 is a prime of good reduction. Let $K = \mathbb{Q}(\sqrt{5})$, $F = \mathbb{Q}(E[n])$, $L = \mathbb{Q}(\sqrt{5})(E[n])$; we can say K and F are linearly disjoint since $5 \nmid n$ and $5 \nmid \Delta_E$. Let $G = \mathrm{Gal}(F/\mathbb{Q})$ and let $H = \mathrm{Gal}(L/K)$. If $\sigma \in H$, the restriction of σ_F of σ to F is in G, giving us an isomorphism from H to G proving $H \cong G$. □

When $5 \nmid \Delta_E$, this means that 5 is a **prime of good reduction**. If this is not the case, it is a **prime of bad reduction**. This proposition tells us that if we want curves whose division fields are non-abelian over $\mathbb{Q}$ but abelian over $\mathbb{Q}(\sqrt{5})$, then we need them to have 5 as a prime of bad reduction. This narrows down which curves could be examples of what we want.

Another proposition we have is

Proposition 4.2. *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 Gal(C/F) is not abelian, Gal(L/F) is not abelian.*

Proof. Let $G = \mathrm{Gal}(L/F)$. We know $\mathrm{Gal}(K/F) \cong G/N$ for some $N \trianglelefteq G$ (In fact, we know $N \cong \mathrm{Gal}(L/K)$). Since G/N is not abelian, we have that for some $g, h \in G, gN \cdot hN \neq hN \cdot gN$. By the definition of the group law of quotients, this means $(gh)N \neq (hg)N$. $gh \in G = hg \in G \Rightarrow (gh)N = (hg)N$. By the contrapositive, $(gh)N \neq (hg)N \Rightarrow gh \neq hg$, so G is not abelian. □

This has a useful corollary for us to use

Corollary 4.3. *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 tells us we want to look at n division fields where n is prime. If we can show that for some prime n, that the n division field is non abelian over $\mathbb{Q}(\sqrt{5})$, then we can say that the division field for all multiples of n is also non-abelian over $\mathbb{Q}(\sqrt{5})$.

Additionally, the contrapositive statement means that if we can say something about a composite n, such as 4, being abelian, we can then say that the d division fields, where d is a factor of n, is abelian as well.

5 Main Results

In this section, we list the main results from our research.

5.1 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 $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \{e\}$.
2. If it has 1 rational root and 2 irrational roots, $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong C_2$.
3. If the roots are irrational and Δ_E is a perfect square, then $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong C_3$.
4. If the roots are irrational and Δ_E is not a perfect square, then $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$.

All of those are abelian except for the S_3 case. For this, we have found a result:

Theorem 5.1. *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.*

5.2 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 5.2. *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.*

5.3 5 Division Fields

The 5 division field of an elliptic curve is the smallest field containing the 5-torsion points of the elliptic curve. By a result of Serre, $Gal(\mathbb{Q}(E[5])/\mathbb{Q})$ 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 5.3. *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.*

6 "Future Work"- its not supposed to be named that but I'll change that after more is written

1. $\mathbb{Q}(E[4])/\mathbb{Q}$
   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 $\text{Gal}(C/F)$ is not abelian, $\text{Gal}(L/F)$ is not abelian.
   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.

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

$\mathbb{Q}(E[4])/\mathbb{Q}(\sqrt{5}) : 80.a1(G_pD_4 \to C_2^2)$

2. $\mathbb{Q}(E[7])/\mathbb{Q}$
   If the 7 division field is defined over $\mathbb{Q}(\sqrt{5})$, then it has 3 quadratic subfields: $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-35})$. This means $\mathrm{Gal}(\mathbb{Q}(E[7])/\mathbb{Q})$ has 3 index two 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:

   C_6^2, $C_6 \times S_3$, $C_2 \times F_7$, $C_6 \times D_7$, $C_6 \wr C_2$, $C_6 \times F_7$, $C_3 \times \mathrm{SD}_{32}$.

   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 $C_3 \times \mathrm{SD}_{32}$.

3. $\mathbb{Q}(E[10])/\mathbb{Q}$
   $\mathbb{Q}(E[10])/\mathbb{Q}(\sqrt{5}) : y^2 = x^3 - x(G_pC_2^2 : C_4 \to C_2^3)$

4. $\mathbb{Q}(E[d^2])/\mathbb{Q}$

5. Plans for $\mathbb{Q}(E[p])/\mathbb{Q}$

7 Acknowledgements

We would like to thank the following:

Professor Edray Herber Goins
Professor Alex Barrios
Mark Curiel
Olivia Del Guercio
Fabian Ramirez
Cameron Thomas
Professor Jeremy Rouse
Pomona College
National Science Foundation (DMS-2113782)

References

[1] Houria Baaziz. Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points. *Mathematics of Computation*, 79:2371–2386, 10 2010.

[2] Alexander J. Barrios. Minimal models of rational elliptic curves with non-trivial torsion. *Research in Number Theory*, 8(1), nov 2021.

[3] Keith Conrad. The galois correspondence at work
. `https://kconrad.math.uconn.edu/blurbs/galoistheory/galoiscorrthms.pdf`.

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

[5] Harris B. Daniels and Álvaro Lozano-Robledo. Coincidences of division fields. 2021.

[6] Harris B. Daniels, Álvaro Lozano-Robledo, and Jackson S. Morrow. Towards a classification of entanglements of galois representations attached to elliptic curves. 2023.

[7] Enrique González–Jiménez and Filip Najman. Growth of torsion groups of elliptic curves upon base change. *Mathematics of Computation*, 89(323):1457–1485, oct 2019.

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

[9] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer, 3rd edition, 2002.

[10] Álvaro Lozano-Robledo. *Elliptic Curves, Modular Forms, and Their L-functions*. Student Mathematical Library. American Mathematical Society, 2011.

[11] Álvaro Lozano-Robledo. Division fields of elliptic curves with minimal ramification. *Rev. Mat. Iberoam*, 31:1311–1332, 2015.

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

[13] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2nd edition, 2019.

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

[15] David Zywina. Elliptic curves with maximal galois action on their torsion points. *Bulletin of the London Mathematical Society*, 42(5):811–826, jul 2010.

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