

Bounds on Torsion Groups From Geometric Isogeny Classes

Tyler Genao

Department of Mathematics
University of Georgia

(50-minute version)

arXiv: 2210.10177, 2112.11566.

- Given a number field F , an **elliptic curve defined over F** is an algebraic curve E/F defined by

$$y^2 = x^3 + Ax + B$$

for some $A, B \in F$ where $4A^3 - 27B^2 \neq 0$.

- Unless otherwise stated, all elliptic curves in this talk are defined over number fields!
- Unlike other algebraic curves, elliptic curves (genus = 1) are endowed with a **geometric group law**.

For an elliptic curve E/F , we will use $E(F)$ to denote the group of F -rational points on E .

- $P := (x, y) \in E$ is **F -rational** if $x, y \in F$.

Theorem (Mordell-Weil).

Let F be a number field. Then for all elliptic curves E/F , the group $E(F)$ is finitely generated.

- The **torsion subgroup** of E is the subgroup of points with finite order.

Corollary.

With notation as above, the torsion subgroup $E(F)[\text{tors}]$ is finite.

Fixing the degree:

Elliptic curves over number fields satisfy a “strong uniform boundedness” in their torsion subgroups.

Theorem (Merel, 1996).

For each $d \in \mathbb{Z}^+$, there exists a constant $B := B(d) \in \mathbb{Z}^+$ so that for all elliptic curves E/F where $[F : \mathbb{Q}] = d$ one has

$$\#E(F)[\text{tors}] \leq B := B(d).$$

- “Fix the number field degree, and get a uniform bound.”
- Examples: for E/F , one has:
 - $[F : \mathbb{Q}] = 1 \Rightarrow \#E(F)[\text{tors}] \leq 16$;
 - $[F : \mathbb{Q}] = 2 \Rightarrow \#E(F)[\text{tors}] \leq 24$;
 - $[F : \mathbb{Q}] = 3 \Rightarrow \#E(F)[\text{tors}] \leq 28$.

Fixing the elliptic curve:

Not fixing the number field degree, but instead fixing E/F and studying $E(L)[\text{tors}]$ where L varies:

- For each $M \in \mathbb{Z}^+$ there exists torsion points $R \in E$ with $[F(R) : F] > M$.

Do we have any control over $\#E(L)[\text{tors}]$ when varying L ?

Torsion under isogenies

Let's make this question harder!

- For the rest of this talk, fix an algebraic closure $\overline{\mathbb{Q}}$.
- Recall that an *isogeny* between two elliptic curves E_1, E_2 is a morphism $\phi : E_1 \rightarrow E_2$ which fixes basepoints.
 - ϕ is also a group homomorphism.
- The “ $\overline{\mathbb{Q}}$ -isogeny class of E ” is the collection of elliptic curves E' which are $\overline{\mathbb{Q}}$ -isogenous to E .
- As an adjective, *geometric* means $\overline{\mathbb{Q}}$ -rational.

- Any $\overline{\mathbb{Q}}$ -isogeny class of elliptic curves has j -invariants of arbitrarily large degree over \mathbb{Q} .
 - Non-CM elliptic curves: use Serre's open image theorem.
 - CM elliptic curves: use that class numbers of imaginary quadratic order tend to infinity as their discriminants $\Delta \rightarrow -\infty$.

Do we have any control over $\#E(L)[\text{tors}]$ when varying L and E in a fixed $\overline{\mathbb{Q}}$ -isogeny class?

Theorem 1 (G., 2022).

Polynomial bounds: Fix a $\overline{\mathbb{Q}}$ -isogeny class \mathcal{E} . Then for each $\epsilon > 0$ there exists a constant $C_\epsilon := C_\epsilon(\mathcal{E})$ such that for all elliptic curves $E_{/F} \in \mathcal{E}$ one has

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{2+\epsilon}.$$

Theorem 2 (G., 2022).

Typical boundedness: Fix a number field F_0 . Then for each $\epsilon > 0$ there exists a constant $B_\epsilon := B_\epsilon(F_0)$ such that for all elliptic curves $E_{/F}$ $\overline{\mathbb{Q}}$ -isogenous to some elliptic curve E' with $j(E') \in F_0$, one has

$$\#E(F)[\text{tors}] \leq B_\epsilon$$

when $[F : \mathbb{Q}]$ does not lie in a certain subset of \mathbb{Z}^+ of upper density $\leq \epsilon$.

Polynomial Bounds on Torsion From Fixed Isogeny Classes

Recall:

Theorem (Merel, 1996).

For each $d \in \mathbb{Z}^+$, there exists a constant $B := B(d) \in \mathbb{Z}^+$ so that for all elliptic curves E/F where $[F : \mathbb{Q}] = d$ one has

$$\#E(F)[\text{tors}] \leq B := B(d).$$

- (Parent, 1999) If $p^n \mid \#E(F)[\text{tors}]$ then

$$p^n \leq 129(5^d - 1)(3d)^6$$

where $d := [F : \mathbb{Q}]$.

Folklore Conjecture (Clark, Cook and Stankewicz, 2013).

There exists a constant $\alpha > 0$ such that for all elliptic curves E/F , one has

$$\#E(F)[\text{tors}] \leq [F : \mathbb{Q}]^\alpha.$$

In support of this conjecture: for an elliptic curve E/F and $d := [F : \mathbb{Q}] > 1$,

- ① (Hindry and Silverman, 1999) if $j(E)$ is integral then

$$\#E(F)[\text{tors}] \leq 1977408 \cdot d \log d;$$

- ② (Clark and Pollack, 2015) if E has CM then

$$\#E(F)[\text{tors}] \leq C \cdot d \log \log d$$

for some effectively computable constant $C \in \mathbb{Z}^+$.

- For a finite abelian group G , we let $\exp G$ denote the *exponent* of G .
- ③ (Clark and Pollack, 2018) For each $\epsilon > 0$ there exists $C_\epsilon > 0$ such that for all elliptic curves E/F *base-changed from \mathbb{Q}* one has

$$\exp E(F)[\text{tors}] \leq C_\epsilon \cdot d^{3/2+\epsilon}$$

and

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot d^{5/2+\epsilon}$$

where $d := [F : \mathbb{Q}]$.

More generally:

- ④ (Clark and Pollack, 2018) Fix a number field F_0 . Assume that **A. GRH is true**, and that **B. F_0 contains no Hilbert class fields of imaginary quadratic fields**. Then for each $\epsilon > 0$ there exists $C_\epsilon > 0$ such that for all elliptic curves $E_{/F}$ with F_0 -rational j -invariant, one has both

$$\exp E(F)[\text{tors}] \leq C_\epsilon \cdot d^{3/2+\epsilon}$$

and

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot d^{5/2+\epsilon}$$

where $d := [F : \mathbb{Q}]$.

- **A.** and **B.** are the **LV Hypotheses**.

To add to these results:

Theorem 1 (G., 2022).

Fix a number field F_0 and an elliptic curve E_{0/F_0} . Then for each $\epsilon > 0$ there exists $C_\epsilon := C_\epsilon(E_0, F_0) > 0$ such that for all elliptic curves E/F geometrically isogenous to E_{0/F_0} one has both

$$\exp E(F)[\text{tors}] \leq C_\epsilon \cdot d^{1+\epsilon}$$

and

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot d^{2+\epsilon}$$

where $d := [F : \mathbb{Q}]$.

Proof sketch

- ① For each $\epsilon > 0$,

$$\exp E(F)[\text{tors}] \leq d^B \Rightarrow \#E(F)[\text{tors}] \leq C_\epsilon \cdot d^{B+1+\epsilon}$$

for some $C_\epsilon > 0$.

- ② Assume E is non-CM. We then take for a certain $M \in \mathbb{Z}^+$

$$\exp E(F)[\text{tors}] = \exp E(F)[M^\infty] \cdot \exp E(F)[M'].$$

Here, $E(F)[M^\infty]$ is the “ M -primary torsion” and $E(F)[M']$ is the torsion supported away from M .

- M depends on E_0/F_0 (it is the *adelic level of E_0/F_0*).

- ③ We will bound $\exp E(F)[M^\infty]$ and $\exp E(F)[M']$ independently!

Uniformly bounded support

Theorem 3 (G., 2022; variant of Clark and Pollack, 2018).

For integers $d_0, M > 0$, there exists a constant $C := C(d_0, M) > 0$ such that for any non-CM elliptic curve E/F geometrically isogenous to an elliptic curve whose j -invariant j_0 has degree $[\mathbb{Q}(j_0) : \mathbb{Q}] = d_0$, one has

$$\exp E(F)[M^\infty] \leq C \cdot \sqrt{d}$$

where $d := [F : \mathbb{Q}]$.

N -adic representations under isogeny

- To bound $\exp E(F)[M']$, we will exploit a relation between N -adic representations of E and E_0 .
- Given an elliptic curve E/F , for each integer $N \in \mathbb{Z}^+$ the absolute Galois group $G_F := \text{Gal}(\overline{\mathbb{Q}}/F)$ acts on the N -adic Tate module

$$T_N(E) := \varprojlim_{k \geq 1} E[N^k],$$

giving rise to the N -adic representation

$$\rho_{E, N^\infty} : G_F \rightarrow \text{GL}_2(\mathbb{Z}_N).$$

Theorem 4 (G., 2022, à la Greenberg, 2012).

Let E/F and E'/F be F -rationally isogenous non-CM elliptic curves. Then for all integers $N \in \mathbb{Z}^+$ one has

- 1 $[\mathrm{GL}_2(\mathbb{Z}_N) : \rho_{E, N^\infty}(G_F)] = [\mathrm{GL}_2(\mathbb{Z}_N) : \rho_{E', N^\infty}(G_F)];$
- 2 $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \rho_{E, N}(G_F)] \mid [\mathrm{GL}_2(\mathbb{Z}_N) : \rho_{E', N^\infty}(G_F)].$

- Can use this to show that for each $\epsilon > 0$, one has

$$\exp E(F)[M'] \leq c_\epsilon(d_0) \cdot d^{1/2+\epsilon}$$

for some constant $c_\epsilon(d_0) > 0$.

- Combine this with $\exp E(F)[M^\infty] \leq C \cdot \sqrt{d}$.

- Conclusion: we have polynomial bounds on each geometric isogeny class of elliptic curves over number fields.
- Next, we'll describe uniformity results on torsion from all " F_0 -rational" geometric isogeny classes.

Typically Bounding Torsion From \mathcal{I}_{F_0}

- Definition: a subset $S \subseteq \mathbb{Z}^+$ has *upper density*

$$\bar{\delta}(S) := \limsup_{x \rightarrow \infty} \frac{\#(S \cap [1, x])}{x}.$$

- Say that a family \mathcal{F} of elliptic curves is **typically bounded in torsion** if for all $\epsilon > 0$ there exists $B := B(\epsilon) > 0$ so that the set

$$\{d \in \mathbb{Z}^+ : \max_{\substack{E/F \in \mathcal{F}: \\ [F:\mathbb{Q}] = d}} \#E(F)[\text{tors}] \geq B\} \subseteq \mathbb{Z}^+$$

has upper density $\leq \epsilon$.

- So for any $\epsilon > 0$, there is a bound on torsion subgroups which works over **any** degree, as long as one ignores a subset of degrees of arbitrarily small upper density.

- ① $\mathcal{E}_{\text{CM}} := \{\text{CM elliptic curves}\} \Rightarrow \mathcal{E}_{\text{CM}}$ is typically bounded in torsion (Bourdon, Clark and Pollack, 2017).
- ② $\mathcal{E} := \{\text{all elliptic curves}\} \Rightarrow \mathcal{E}$ is *not* typically bounded in torsion (Clark, Milosevic and Pollack, 2018).

P1: Given integers $\ell, n_0 \in \mathbb{Z}^+$ with ℓ prime, there exists $n := n(\mathcal{F}, \ell, n_0) \in \mathbb{Z}^+$ such that for all $E/F \in \mathcal{F}$, if $E(F)[\ell^n] \setminus E(F)[\ell^{n-1}] \neq \emptyset$ then

$$\ell^{n_0} \mid [F : \mathbb{Q}].$$

P2: There exists $c := c(\mathcal{F}) \in \mathbb{Z}^+$ such that for all primes $\ell \in \mathbb{Z}^+$ and all $E/F \in \mathcal{F}$, if $E(F)[\ell] \setminus \{O\} \neq \emptyset$ then

$$\ell - 1 \mid c[F : \mathbb{Q}].$$

Theorem (Theorem 3.2, Clark, Milosevic and Pollack, 2018).

*If \mathcal{F} satisfies **P1** and **P2**, then \mathcal{F} is typically bounded in torsion.*

- Recall the family

$$\mathcal{I}_{F_0} := \{E/F : E \text{ is } \overline{\mathbb{Q}}\text{-isogenous to some } E'_{/F_0}\}.$$

- “Elliptic curves $\overline{\mathbb{Q}}$ -isogenous to at least one F_0 -rational elliptic curve.”

Theorem 2 (G., 2022).

For any number field F_0 , the family \mathcal{I}_{F_0} is typically bounded in torsion.

P1: strong uniform bounds on levels of ℓ -adic representations

Using a uniform bound on ℓ -adic levels of non-CM elliptic curves over a fixed degree (proven by Arai (2008)) and later strengthened by Clark and Pollack (2018)), we have shown the following.

Theorem 5 (G., 2022).

For all $d_0 \in \mathbb{Z}^+$ and prime ℓ , there exists $A := A(d_0, \ell) \in \mathbb{Z}^+$ such that for all non-CM E/F with $[F : \mathbb{Q}] = d_0$, one has for all $n \geq A$ and all cyclic subgroups $C \subseteq E$ of order ℓ^n that

$$\ell^{n-A} \mid [F(C) : F].$$

Theorem 5 (G., 2022).

For all $d_0 \in \mathbb{Z}^+$ and prime ℓ , there exists $A := A(d_0, \ell) \in \mathbb{Z}^+$ such that for all non-CM E/F with $[F : \mathbb{Q}] = d_0$, one has for all $n \geq A$ and all cyclic subgroups $C \subseteq E$ of order ℓ^n that

$$\ell^{n-A} \mid [F(C) : F].$$

This is enough to prove **P1** for \mathcal{I}_{F_0} .

P1: Given integers $\ell, n_0 \in \mathbb{Z}^+$ with ℓ prime, there exists $n := n(\mathcal{I}_{F_0}, \ell, n_0) \in \mathbb{Z}^+$ such that for all $E/F \in \mathcal{I}_{F_0}$, if $E(F)[\ell^n]^* \neq \emptyset$ then

$$\ell^{n_0} \mid [F : \mathbb{Q}].$$

P2: isogeny characters

P2: There exists $c := c(\mathcal{F}) \in \mathbb{Z}^+$ such that for all primes $\ell \in \mathbb{Z}^+$ and all $E/F \in \mathcal{F}$, if $E(F)[\ell]^* \neq \emptyset$ then

$$\ell - 1 \mid c[F : \mathbb{Q}].$$

We prove that \mathcal{I}_{F_0} satisfies **P2** using **isogeny characters**.

- Given E/F and prime ℓ , a cyclic subgroup $C \subseteq E[\ell]$ is called **F -rational** if it is G_F -stable.
- The resulting 1-D representation is the **isogeny character** of C ,

$$r: G_F \rightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times.$$

Back to the **LV** hypotheses:

Theorem (Larson and Vaintrob, 2014).

Let F_0 be a number field. Then for all $\ell \gg_{F_0} 0$, if E/F_0 is an elliptic curve with an F_0 -rational ℓ -isogeny, then for its isogeny character $r: G_{F_0} \rightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times$ we have one of the following:

- 1 There exists a CM elliptic curve E' defined over F_0 such that its CM field $K := \text{End}(E') \otimes \mathbb{Q}$ is with $K \subseteq F_0$; and E' has an F_0 -rational ℓ -isogeny, whose isogeny character $s: G_{F_0} \rightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times$ satisfies

$$r^{12} = s^{12}.$$

- 2 GRH fails for $F_0(\sqrt{-\ell})$, and

$$r^{12} = \chi_\ell^6$$

where χ_ℓ is the mod- ℓ cyclotomic character.

- Thus, if F_0 has no rationally defined CM and GRH is true, then there are no F_0 -rational isogenies of large prime degree.

- This has previously been applied towards proving a subfamily of \mathcal{I}_{F_0} is typically bounded in torsion, conditionally.
- Define the subfamily

$$\mathcal{E}_{F_0} := \{E/F : j(E) \in F_0\}.$$

Theorem (Clark, Milosevic and Pollack, 2018).

Let F_0 be a number field. Assuming the **LV hypotheses** for F_0 , the family \mathcal{E}_{F_0} is typically bounded in torsion.

- To prove **P2** for \mathcal{E}_{F_0} , they use a classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Theorem (Serre-Dickson Classification).

Let $\ell \geq 5$ be a prime. Then for a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$:

1. If $\ell \mid \#G$, then up to conjugacy one of the following holds:
 - a. G contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.
 - b. G is contained in $B(\ell)$.
2. If $\ell \nmid \#G$, then up to conjugacy one of the following holds:
 - a. G is contained in $N_s(\ell)$ or $N_{ns}(\ell)$.
 - b. The image \overline{G} of G in $\mathrm{PGL}_2(\ell)$ is isomorphic to one of the groups A_4 , S_4 or A_5 .

- $B(\ell) :=$ Borel subgroup (upper triangular).
- $N_s(\ell)$ (resp. $N_{ns}(\ell)$) := normalizer of split (resp. non-split) Cartan subgroup.
- $\mathrm{PGL}_2(\ell) := \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/(\mathbb{Z}/\ell\mathbb{Z})^\times$.

Theorem (Serre-Dickson Classification).

Let $\ell \geq 5$ be a prime. Then for a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$:

1. If $\ell \mid \#G$, then up to conjugacy one of the following holds:
 - a. G contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. **doable.**
 - b. G is contained in $B(\ell)$. **doable?**
2. If $\ell \nmid \#G$, then up to conjugacy one of the following holds:
 - a. G is contained in $N_s(\ell)$ or $N_{ns}(\ell)$. **doable.**
 - b. The image \overline{G} of G in $\mathrm{PGL}_2(\ell)$ is isomorphic to one of the groups A_4 , S_4 or A_5 . **doable.**

- $B(\ell) :=$ Borel subgroup (upper triangular).
- $N_s(\ell)$ (resp. $N_{ns}(\ell)$) := normalizer of split (resp. non-split) Cartan subgroup.
- $\mathrm{PGL}_2(\ell) := \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/(\mathbb{Z}/\ell\mathbb{Z})^\times$.

Theorem (Serre-Dickson Classification).

Let $\ell \geq 5$ be a prime. Then for a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$:

1. If $\ell \mid \#G$, then up to conjugacy one of the following holds:
 - a. G contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. **doable.**
 - b. G is contained in $B(\ell)$. **exclude via LV hypotheses!**
2. If $\ell \nmid \#G$, then up to conjugacy one of the following holds:
 - a. G is contained in $N_s(\ell)$ or $N_{ns}(\ell)$. **doable.**
 - b. The image \overline{G} of G in $\mathrm{PGL}_2(\ell)$ is isomorphic to one of the groups A_4 , S_4 or A_5 . **doable.**

- $B(\ell) :=$ Borel subgroup (upper triangular).
- $N_s(\ell)$ (resp. $N_{ns}(\ell)$) := normalizer of split (resp. non-split) Cartan subgroup.
- $\mathrm{PGL}_2(\ell) := \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/(\mathbb{Z}/\ell\mathbb{Z})^\times$.

We've shown that assuming the **LV hypotheses** is unnecessary:

Theorem 6 (G., 2022).

For any number field F_0 , the family \mathcal{E}_{F_0} is typically bounded in torsion.

Corollary 7 (G., 2022).

*The family \mathcal{I}_{F_0} satisfies **P2**, and thus is typically bounded in torsion.*

Continuing Work

Recall

$$\mathcal{I}_{F_0} := \{E/F : E \text{ is } \overline{\mathbb{Q}}\text{-isogenous to some } E' \text{ with } j(E') \in F_0\}.$$

Theorem 0 (G., 2022).

\mathcal{I}_{F_0} is typically bounded in torsion.

- The study of \mathcal{I}_{F_0} is originally motivated by a study of \mathbb{Q} -curves.

- Given an elliptic curve E/F , for each automorphism $\sigma \in G_{F_0}$ one produces a new elliptic curve $E^\sigma/\sigma(F)$ by applying σ to the equation for E .
- Let us define the family of F_0 -**curves**

$$\mathcal{Q}_{F_0} := \{E/F : \forall \sigma \in G_{F_0}, E \text{ is } \overline{\mathbb{Q}}\text{-isogenous to } E^\sigma/\sigma(F)\}.$$

- “Geometrically isogenous to Galois conjugates”.
- When $F_0 = \mathbb{Q}$, this is the well-studied family of \mathbb{Q} -curves.

$$\mathcal{E}_{F_0} \subseteq \mathcal{I}_{F_0} \subseteq \mathcal{Q}_{F_0}$$

- If F/\mathbb{Q} has odd degree, then $E_{/F}$ is a \mathbb{Q} -curve iff it is isogenous to a \mathbb{Q} -rational j -invariant (Cremona and Najman, 2021).

Conjecture.

The family $\mathcal{Q}_{\mathbb{Q}}$ is typically bounded in torsion.

- Follows from a boundedness conjecture on rational points on Atkin-Lehner quotients $X^*(N)$.
- Can try to show this for *central* \mathbb{Q} -curves, whose torsion subgroups are better understood; see e.g. (Sairaiji and Yamauchi, 2008).

Polynomial Bounds

Theorem -1 (G., 2022).

For each $\epsilon > 0$ and **fixed** geometric isogeny class \mathcal{E} , there exists a constant $C_\epsilon := C_\epsilon(\mathcal{E})$ for which there are polynomial bounds of the form $C_\epsilon \cdot d^{1+\epsilon}$ on the exponent of torsion subgroups from \mathcal{E} .

- Can we produce **uniform** polynomial bounds on “ F_0 -rational” geometric isogeny classes?

Project A

Conjecture.

For each number field F_0 , there exists polynomial bounds on \mathcal{I}_{F_0} : for each $\epsilon > 0$ there are $B := B(F_0) > 0$ and $C_\epsilon := C_\epsilon(F_0) > 0$ such that for all $E/F \in \mathcal{I}_{F_0}$ one has

$$\exp E(F)[\text{tors}] \leq C_\epsilon \cdot d^{B+\epsilon}$$

and

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot d^{B+1+\epsilon}.$$

- For $E/F \in \mathcal{I}_{\mathbb{Q}}$ with $[F : \mathbb{Q}]$ odd, one has

$$\#E(F)[\text{tors}] \leq 720720\sqrt{35} \cdot [F : \mathbb{Q}]^{1/2}$$

(consequence of Bourdon and Najman, 2022).

Project B

Conjecture.

*Fix a number field F_0 and an **abelian variety** A_0/F_0 . Then there exists polynomial bounds on the geometric isogeny class of A_0/F_0 .*

- Would need analogous results on N -adic indices of isogenous abelian varieties, as well as an open image theorem for $\rho_{A_0, N}: G_{F_0} \rightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$.
 - The latter exists for PPAV's A_0/F_0 with $\mathrm{End}(A_0) = \mathbb{Z}$ and $\dim(A_0) \in \{2, 6\} \cup \{\text{odd } n \in \mathbb{Z}^+\}$ (Serre, 1986).

Thank you!