Torsion Subgroups of Rational Elliptic Curves over Nonic Galois Fields

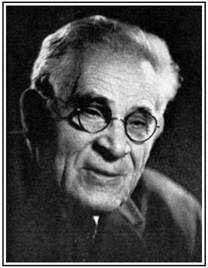
Caleb McWhorter
Syracuse University

Maine/Québec Number Theory Conference
October 5, 2019

Theorem (Mordell-Weil, 1922/1928)

Let K be a number field and A/K be an abelian variety. Then the group of K-rational points on A, denoted $A(K)$, is a finitely generated abelian group. In particular,

$$A(K) \cong \mathbb{Z}^{r_{A/K}} \oplus A(K)_{tors}$$



Louis J. Mordell

André Weil

Theorem (Levi-Ogg Conjecture; Mazur, 1977)

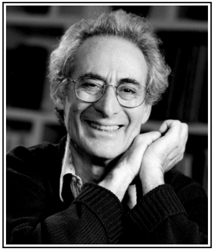
If $E/\mathbb{Q}$ is a rational elliptic curve, then the possible torsion subgroups $E(\mathbb{Q})_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 4 \end{cases}$$

Furthermore, each possibility occurs infinitely often.

Beppo Levi

Andrew Ogg



Barry Mazur

Theorem (Kenku, Momose, 1988; Kamienny, 1992)

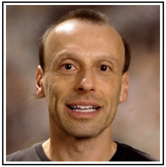
Let $K/\mathbb{Q}$ be a quadratic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 16, 18 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \end{cases}$$

Moreover, each possibility occurs infinitely often.

Monsur Kenku

Fumiyuki Momose



Sheldon Kamienny

Theorem (Jeon,Kim,Schweizer, 2004; Etropolski-Morrow-Zureick Brown; Derickx, 2016)

Let $K/\mathbb{Q}$ be a cubic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 16, 18, 20, 21 \\ \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 7 \end{cases}$$

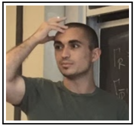
Each of these possibilities occurs infinitely many times except $\mathbb{Z}/21\mathbb{Z}$.

Jeon

Kim

Schweizer

Etropolski



Morrow

Z-B.

Derickx

Theorem (Jeon, Kim, Park, 2006)

Let $K/\mathbb{Q}$ be a quartic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 18, 20, 21, 22 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 9 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, 2, 3 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{cases}$$

Daeyeol Jeon

Chang Kim

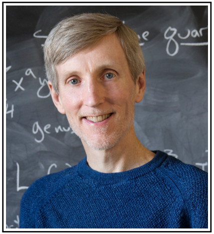
Eui-Sung Park

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbb{Q}$ be a quintic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 22, 24, 25 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 8 \end{cases}$$

Maarten Derickx



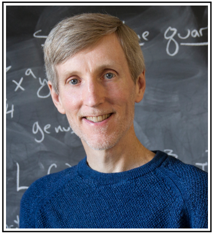
Drew Sutherland

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbb{Q}$ be a sextic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 30; n \neq 23, 25, 29 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 10 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, \ldots, 4 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} & \end{cases}$$

Maarten Derickx



Drew Sutherland

Theorem (Clark, Corn, Rice, Stankewicz; 2013)

Let K be a number field of degree $d = 1, 2, \ldots, 13$ and E/K be an elliptic curve with CM. Then all possible torsion subgroups are given, and an algorithm to compute the list.

Pete Clark

Patrick Corn

Alex Rice

James Stankewicz

Theorem (Bourdon, Pollack; 2018)

Let K be an odd degree number field and E/K be an elliptic curve with CM. Then the torsion subgroups $E(K)_{tors}$ are computable.

Abbey Bourdon

Paul Pollack

Theorem (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, Ogg, et al.)

If $E/\mathbb{Q}$ has an n-isogeny over $\mathbb{Q}$, then

$$n \in \{1, 2, \ldots, 19, 21, 25, 27, 37, 43, 67, 163\}.$$

If E does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.

Theorem (Chou,Daniels,González-Jimenez,Lozano-Robledo,Najman,Tornero,et al.)

Let $\mathcal{C}_n$ denote the cyclic subgroup of order n. Then

$$\Phi_{\mathbb{Q}}(2) = \{\mathcal{C}_n : n = 1, 2, \ldots, 10, 12, 15, 16\}$$
$$\cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : 1, 2, \ldots, 6\} \cup \{\mathcal{C}_3 \oplus \mathcal{C}_3, \mathcal{C}_3 \oplus \mathcal{C}_6, \mathcal{C}_4 \oplus \mathcal{C}_4\}$$
$$\Phi_{\mathbb{Q}}(3) = \{\mathcal{C}_n : n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21\}$$
$$\cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : n = 1, 2, 3, 4, 7\}$$
$$\Phi_{\mathbb{Q}}(4) = \{\mathcal{C}_n : n = 12, \ldots, 10, 12, 13, 15, 16, 20, 24\}$$
$$\cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : n = 1, 2, \ldots, 6, 8\} \cup \{\mathcal{C}_3 \oplus \mathcal{C}_{3n} : n = 1, 2\}$$
$$\cup \{\mathcal{C}_4 \oplus \mathcal{C}_{4n} : n = 1, 2\} \cup \{\mathcal{C}_5 \oplus \mathcal{C}_5\} \cup \{\mathcal{C}_6 \oplus \mathcal{C}_6\}$$
$$\Phi_{\mathbb{Q}}(5) = \{\mathcal{C}_n : n = 1, 2, \ldots, 12, 25\} \cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : n = 1, 2, 3, 4\}$$
$$\Phi_{\mathbb{Q}}(6) \supseteq \{\mathcal{C}_n : n = 1, 2, \ldots, 21, 30 : n \neq 11, 17, 19, 20\}$$
$$\cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : n = 1, 2, \ldots, 7, 9\}$$
$$\cup \{\mathcal{C}_3 \oplus \mathcal{C}_{3n} : n = 1, 2, 3, 4\} \cup \{\mathcal{C}_4 \oplus \mathcal{C}_4, \mathcal{C}_6 \oplus \mathcal{C}_6\}$$
$$\Phi_{\mathbb{Q}}(d^*) = \Phi_{\mathbb{Q}}(1)$$

Michael Chou

Harris Daniels

Enrique González-Jiménez

Álvaro Lozano-Robledo

Filip Najman

José Tornero

Theorem (M.)

Let $K/\mathbb{Q}$ be a nonic Galois field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13, 14, 16, 18, 19, 21, 27 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4, 7 \end{cases}$$

Theorem (M.)

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4, 7 \end{cases}$$

Theorem (M.)

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13^*, 18^*, 19, 21, 27 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4 \end{cases}$$

Outline of the Method

Theorem (Lozano-Robledo)

Let $S_{\mathbb{Q}}(d)$ be the set of primes such that there exists an elliptic curve $E/\mathbb{Q}$ with a point of order p defined in an extension $K/\mathbb{Q}$ of degree at most d. Then $S_{\mathbb{Q}}(9) = \{2, 3, 5, 7, 11, 13, 17, 19\}$.

Álvaro Lozano-Robledo

Remark

Lozano-Robledo computes $S_{\mathbb{Q}}(d)$ for $1 \leq d \leq 21$, and gives a conjecturally formula valid for all $1 \leq d \leq 42$, following from a positive answer to Serre's uniformity question.

Proposition (González-Jiménez, Najman)

1. $11 \in R_{\mathbb{Q}}(d)$ *if and only if* $5 \mid d$.
2. $13 \in R_{\mathbb{Q}}(d)$ *if and only if* $3 \mid d$ *or* $4 \mid d$.
3. $17 \in R_{\mathbb{Q}}(d)$ *if and only if* $8 \mid d$.

Enrique González-Jiménez

Filip Najman

Lemma

Let $K/\mathbb{Q}$ be an odd degree number field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain full p-torsion for all odd primes.

Lemma

Let $K/\mathbb{Q}$ be an odd degree number field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain full p-torsion for all odd primes.

Proof. If $E(K)$ contains full n-torsion, then $\mathbb{Q}(\zeta_n) \subseteq K$.

Lemma

Let $K/\mathbb{Q}$ be an odd degree number field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain full p-torsion for all odd primes.

Proof. If $E(K)$ contains full n-torsion, then $\mathbb{Q}(\zeta_n) \subseteq K$. But

$$[K\colon \mathbb{Q}] = [K\colon \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n)\colon \mathbb{Q}] = [K\colon \mathbb{Q}(\zeta_n)]\phi(n),$$

and $\phi(n)$ is even for $n > 2$. □

Lemma

Let $K/\mathbb{Q}$ be a Galois extension, and let $E/\mathbb{Q}$ be a rational elliptic curve. If $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$, then E has a rational n-isogeny.

Lemma

Let $K/\mathbb{Q}$ be a Galois extension, and let $E/\mathbb{Q}$ be a rational elliptic curve. If $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$, then E has a rational n-isogeny.

Proof. Let $\{P, Q\}$ be a basis for $E[n]$. Without loss of generality, assume that $P \in E(K)$ and $Q \notin E(K)$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Because $K/\mathbb{Q}$ is Galois and $P \in E(K)$, $P^\sigma \in E(K)[n] = \langle P \rangle$. But then $E(K)[n] = \langle P \rangle$ is Galois stable, which implies that E has an n-isogeny over $\mathbb{Q}$. □

Theorem (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, Ogg, et al.)

If $E/\mathbb{Q}$ has an n-isogeny over $\mathbb{Q}$, then

$$n \in \{1, 2, \ldots, 19, 21, 25, 27, 37, 43, 67, 163\}.$$

If E does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.

Theorem (Rouse,Zureick-Brown, 2015)

Let $E/\mathbb{Q}$ be a rational elliptic curve without CM. Then the index of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ divides 64 or 96, and all such indices occur. Furthermore, the image of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the inverse image in $\mathrm{GL}_2(\mathbb{Z}_2)$ of the image of $\rho_{E,32}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$.

Jeremy Rouse

David Zureick-Brown

Remark

They also enumerate all 1,208 possibilities and find their rational points.

Theorem (González-Jiménez, Lozano-Robledo)

Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \subseteq E[2^N]$ be a subgroup isomorphic to $\mathbb{Z}/2^s/Z \oplus \mathbb{Z}/2^N\mathbb{Z}$. Then $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by 2 if $s = N = 2$, and otherwise by $2^{2N+2s-8}$ if $N \geq 3$, unless $s \geq 4$ and $j(E)$ is one of the two values:

$$-\frac{3 \cdot 18249920^3}{17^{16}} \quad \text{or} \quad -\frac{7 \cdot 1723187806080^3}{79^{16}}$$

in which case $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $3 \cdot 2^{2N+2s-9}$. Moreover, this is best possible in that there are one-parameter families $E_{s,N}(t)$ of elliptic curves over $\mathbb{Q}$ such that for each $s, N \geq 0$ and each $t \in \mathbb{Q}$, and subgroups $T_{s,N} \in E_{s,N}(t)(\overline{\mathbb{Q}})$ isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$ such that $[\mathbb{Q}(T_{s,N}) : \mathbb{Q}]$ is equal to the bound given above.

Theorem (Knapp)

Let E/K be an elliptic curve over a field of characteristic not equal to 2 or 3. Suppose E is given by

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

where $\alpha, \beta, \gamma \in K$. For $P = (x_0, y_0) \in E(K)$, there exists a point Q with $Q \in E(K)$ with $2Q = P$ if and only if $x_0 - \alpha$, $x_0 - \beta$, $x_0 - \gamma$ are squares in K.

Anthony Knapp

Lemma (Najman)

Let p, q be distinct odd primes, F_2/F_1 a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$ and E/F_1 an elliptic curve with no p-torsion over F_1. Then if q does not divide $p-1$ and $\mathbb{Q}(\zeta_p) \not\subset F_2$, then $E(F_2)[p] = 0$.

Lemma (Najman)

Let p be an odd prime number, q a prime not dividing p, F_2/F_1 a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$, E/F_1 an elliptic curve, and suppose $E(F_1) \supset \mathbb{Z}/p\mathbb{Z}$, $E(F_1) \not\supset \mathbb{Z}/p^2\mathbb{Z}$, and $\zeta_p \notin F_2$. Then $E(F_2) \not\supset \mathbb{Z}/p^2\mathbb{Z}$.

Lemma

Let $K/\mathbb{Q}$ be a nonic Galois field, and let $E/\mathbb{Q}$ be a rational elliptic curve. If $P \in E(K)$ is a point of order n and $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$, then $\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Lemma

Let $K/\mathbb{Q}$ be a nonic Galois field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Let $P \in E(K)$ be a point of order p.

1. *If $p = 2, 3, 5$, then P is rational or defined over a cubic field.*
2. *If $p = 7, 13$, then P is defined over a cubic field.*

Nonic Bicyclic Galois Fields

Theorem (Daniels, Lozano-Robledo, Najman, Sutherland, 2017)

Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q}(3^\infty))_{tors}$ is finite and is isomorphic to one of the following:

$$\begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 4, 5, 7, 8, 13 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}4n\mathbb{Z}, & n = 1, 2, 4, 7 \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6n\mathbb{Z}, & n = 1, 2, 3, 5, 7 \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 4, 6, 7, 9 \end{cases}$$

Pete Clark

Patrick Corn

Alex Rice

James Stankewicz

Theorem (Najman)

Let $K/\mathbb{Q}$ be a cubic number field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then

$$E(F)_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 10, 12, 13, 14, 18, 21 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 4, 7 \end{cases}$$

Moreover, the elliptic curve 162B1 over $\mathbb{Q}(\zeta_9)^+$ is the unique rational elliptic curve over a cubic number field with torsion subgroup $\mathbb{Z}/21\mathbb{Z}$.

Filip Najman

Nonic Cyclic Galois Fields

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.
- $F \subseteq K \subseteq \mathbb{Q}(\zeta_N)$ for some $N = 7^s m$.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.
- $F \subseteq K \subseteq \mathbb{Q}(\zeta_N)$ for some $N = 7^s m$.
- $|(\mathbb{Z}/7^s\mathbb{Z})^\times| = 7^{s-1}(7-1) = 6 \cdot 7^{s-1} = 2 \cdot 3 \cdot 7^{s-1}$

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.
- $F \subseteq K \subseteq \mathbb{Q}(\zeta_N)$ for some $N = 7^s m$.
- $|(\mathbb{Z}/7^s\mathbb{Z})^\times| = 7^{s-1}(7-1) = 6 \cdot 7^{s-1} = 2 \cdot 3 \cdot 7^{s-1}$
- CRT produces $u \in \mathbb{N}$ with $\zeta_N \mapsto \zeta_N^u$ automorphism of K of order 3

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.
- $F \subseteq K \subseteq \mathbb{Q}(\zeta_N)$ for some $N = 7^s m$.
- $|(\mathbb{Z}/7^s\mathbb{Z})^\times| = 7^{s-1}(7-1) = 6 \cdot 7^{s-1} = 2 \cdot 3 \cdot 7^{s-1}$
- CRT produces $u \in \mathbb{N}$ with $\zeta_N \mapsto \zeta_N^u$ automorphism of K of order 3
- $\zeta_N \mapsto \zeta_N^u$ non-trivial in F, K, contradiction

□

Questions?