TORSION ON ELLIPTIC CURVES IN ISOGENY CLASSES

YASUTSUGU FUJITA AND TETSUO NAKAMURA

Abstract. Let $E$ be an elliptic curve over a number field $K$ and $C$ its $K$-isogeny class. We are interested in determining the orders and the types of torsion groups $E(K)_{\text{tors}}$ in $C$. For a prime $l$, we give the range of possible types of $l$-primary parts $E(K)_{(l)}$ of $E(K)_{\text{tors}}$ when $E$ runs over $C$. One of our results immediately gives a simple proof of a theorem of Katz on the order $\sup_{E \in C}|E(K)_{(l)}|$ of maximal $l$-primary torsion in $C$.

1. Introduction

Let $E$ be an elliptic curve over a number field $K$. The group $E(K)$ of $K$-rational points on $E$ is finitely generated; in particular, the torsion subgroup $E(K)_{\text{tors}}$ is finite. Let $C$ be the $K$-isogeny class of an elliptic curve over $K$. Since there exist at most finitely many $K$-isomorphism classes of elliptic curves over $K$ in $C$ (cf. [3, Corollary 6.2, p. 264]), the types of torsion groups $E(K)_{\text{tors}}$ ($E \in C$) are finite. We are interested in determining the orders and the types of torsion groups $E(K)_{\text{tors}}$ in $C$. For this purpose, we study those properties of the $l$-primary parts $E(K)_{(l)}$ of $E(K)_{\text{tors}}$ in $C$ for each prime number $l$.

Fix a prime number $l$. Let $G_K$ denote the Galois group $\text{Gal}(\overline{K}/K)$. For $E \in C$, denote by $T_l(E)$ the $l$-adic Tate module of $E$ and by

$$\rho : G_K \to \text{Aut}(T_l(E))$$

the corresponding $l$-adic representation. As seen in [1, Introduction], $|E(K)_{(l)}|$ divides $\det(I - \rho(\sigma))$ for all $\sigma \in G_K$. This also holds for any $E' \in C$ and for the same $\rho$ as above. Katz showed that the converse is also true in some sense.

Theorem 1.1 (cf. [1, Problem I (ter) and Theorem 1]). Let $N \geq 0$ be an integer. If $\det(I - \rho(\sigma)) \equiv 0 \pmod{l^N}$ for all $\sigma \in G_K$, then there exists an elliptic curve $E$ in $C$ such that $|E(K)_{(l)}| \equiv 0 \pmod{l^N}$.

Note that using this result Katz described the order $\sup_{E \in C}|E(K)_{\text{tors}}|$ of maximal torsion in $C$ in terms of the reductions $E_\varphi$ of $E$ modulo $\varphi$ for almost all primes $\varphi$ (see [1, Introduction and Theorem 2 (bis)]).

In this paper, we show the following.

Theorem 3.1. Let $N \geq 0$ be an integer. Assume that there exists $E \in C$ such that $|E(K)_{(l)}| = l^N$ and $\det(I - \rho(\sigma)) \equiv 0 \pmod{l^{N+1}}$ for all $\sigma \in G_K$. Then, the following hold.
(i) There exists an elliptic curve $E_1 \in \mathcal{C}$ and a $K$-isogeny $f : E \to E_1$ of degree $l$ such that $|E_1(K)(l)| = l^{N+1}$.

(ii) If $E(K)(l)$ is not cyclic, then there exists an elliptic curve $E' \in \mathcal{C}$ such that $E'(K)(l)$ is cyclic and $|E'(K)(l)| < l^{N}$.

Note that $E$ has at most $l+1$ $K$-isogenies of degree $l$ up to $K$-isomorphisms. On account of Theorem 2.3 (i), given $K$, $E$ and $l$, we can find a sequence of $K$-isogenies of degree $l$, which will allow us in practice to find an elliptic curve $E' \in \mathcal{C}$ with $|E'(K)(l)| = l^{M}$, where $l^{M} := \sup_{E \in \mathcal{C}} |E(K)(l)|$.

Put $l^{m} := \inf_{E \in \mathcal{C}} |E(K)(l)|$ and let $l^{n}$ be the number of $l$-power-th roots of unity in $K$. We also show that $m \geq \min\{n, M/2\}$ (Proposition 3.3) and that if $T_l(E)$ is irreducible and $M > 2n$, then $m = n$ (Theorem 4.4).

Finally, let $E(K)(l) \cong Z/l^s Z \oplus Z/l^t Z$ with $s \geq t \geq 0$; when $E$ runs over $\mathcal{C}$, we describe the range where $(s, t)$ can appear.

It is to be noted that the groups $E(K)(l)$ $(E \in \mathcal{C})$ correspond to the $G_K$-stable lattices in $T_l(E) \otimes Q_l$. Putting

$$ V := T_l(E) \otimes Q_l \quad \text{and} \quad G := \rho(G_K), $$

we see that Theorem 5.1 follows from Theorem 2.3 which is deduced from the properties of $G$-stable lattices in $V$ (see the following section). In order to prove Theorem 2.3 (i), we only need two lemmas (Lemmas 2.1 and 2.2) from elementary linear algebra. A theorem of Katz (Theorem 1, see also Remark 2.4 (1)) is a direct corollary of Theorem 2.3 (i). It follows that we give another proof of the theorem of Katz, which is simpler and more elementary than that given in [1].

Remark 1.2. It is easy to see that Theorem 5.1 (i) implies Theorem 1.1. Katz [1] also considered abelian varieties of dimension greater than 1, for which Theorem 1.1 does not hold in general (see Introduction in [1]). Hence, Theorem 5.1 (i) does not hold in general either for higher dimensional abelian varieties.

Notation. Let $K$ be a number field and $l$ a prime number. Fix the $K$-isogeny class $\mathcal{C}$ of an elliptic curve over $K$. Denote by $l^n$ the number of $l$-power-th roots of unity in $K$. Put

$$ v := \sup\{N \in Z : E(K) \supset Z/l^{N} Z, \ E \in \mathcal{C}\} $$

and put

$$ l^{M} := \sup_{E \in \mathcal{C}} |E(K)(l)|, \quad l^{m} := \inf_{E \in \mathcal{C}} |E(K)(l)|, $$

where $E(K)(l)$ denotes the $l$-primary part of the torsion subgroup $E(K)_{\text{tors}}$.

2. Maximal and minimal torsion

Let $k$ be a field. We begin by an elementary lemma.

Lemma 2.1. Let $A, B \in M_2(k)$ be $2 \times 2$ matrices with the coefficients in $k$ such that $\det A = \det B = 0$. Then, for all $\alpha, \beta \in k$ we have

$$ \det(A + B) = \det(A + B + A \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} B). $$
The proof of the lemma needs only an elementary calculation, that we leave to the reader.

We define subspaces of \( M_2(k) \) by
\[
W_\alpha := \left\{ \begin{pmatrix} \alpha a \\ a \end{pmatrix} \in M_2(k) : a \in k^2 \right\} \quad (\alpha \in k)
\]
and
\[
W_\infty := \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} \in M_2(k) : a \in k^2 \right\}.
\]

**Lemma 2.2.** Let \( U \) be a subspace of \( M_2(k) \) such that \( \det A = 0 \) for all \( A \in U \). Then, \( U \) is contained in either \( W_\alpha \) or \( tW_\alpha := \left\{ tA : A \in W_\alpha \right\} \) for some \( \alpha \in k \cup \{\infty\} \).

**Proof.** For \( A = \begin{pmatrix} a \\ b \end{pmatrix} \in M_2(k) \), let \( p(A) := b \in k^2 \).

If \( \dim p(U) = 0 \), then \( U \subset W_\infty \). If \( \dim p(U) = 2 \), then \( U \) contains
\[
A_1 = \begin{pmatrix} u & 0 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & v \\ 0 & 1 \end{pmatrix}
\]
for some \( u, v \in k \). Since \( \det(A_1 + A_2) = 0 \), we have \( u = v \). Hence we have \( U \subset W_\alpha \).

For any \( B \notin W_\alpha \) with \( \det B = 0 \), there exists \( A \in W_\alpha \) such that \( \det(A + B) \neq 0 \).

Therefore, we have \( U = W_\alpha \).

If \( \dim p(U) = 1 \), then there exists a non-zero vector \( c \in k^2 \) such that
\[
A_t := \begin{pmatrix} tc \\ c \end{pmatrix} \in U \quad \text{for} \quad t \in k.
\]

Take any \( A = \begin{pmatrix} b \\ c \end{pmatrix} \in U \). If \( \lambda \neq 0 \), then \( b \in kc \). If \( \lambda = 0 \), then
\[
0 = \det(A + A_t) = \det\left( \begin{pmatrix} b \\ c \end{pmatrix} \right),
\]
which implies that
\[
U \subset \left\{ \begin{pmatrix} xc \\ yc \end{pmatrix} : x, y \in k \right\} = tW_\alpha
\]
for some \( \alpha \in k \cup \{\infty\} \). \( \square \)

Let \( l \) be a prime number and \( V \) a two-dimensional \( \mathbb{Q}_l \)-vector space. Let \( G \subset \text{Aut}_{\mathbb{Q}_l}(V) \) be a compact subgroup. Denote by \( \mathcal{L} \) the set of \( G \)-stable lattices in \( V \).

For \( L = \mathbb{Z}_l x \oplus \mathbb{Z}_l y \), let
\[
\rho : G \rightarrow \text{GL}_2(\mathbb{Z}_l)
\]
be the representation attached to \( \{x, y\} \). For \( w \in L \) and an integer \( i \geq 0 \), \( w \mod l^i \) is considered to be in \( V/L \) by the inclusion
\[
L/l^i L \simeq l^{-i} L/L \subset V/L.
\]
The torsion subgroup \( T(G, L) \subset V/L \) is defined by
\[
T(G, L) := (V/L)^G.
\]

Thus, \( \alpha x + \beta y \mod l^i \) is in \( T(G, L) \) if and only if
\[
(I - \rho(\sigma)) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{l^i} \quad \text{for all} \quad \sigma \in G,
\]
where \( I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \). If \( T(G, L) \) contains a subgroup of order \( l^N \), then
\[
\det(I - \rho(\sigma)) \equiv 0 \pmod{l^N}
\]
for all \( \sigma \in G \).

**Theorem 2.3.** Let \( N \geq 0 \) be an integer. Assume that there exists a lattice \( L \in \mathcal{L} \) such that \( T(G, L) \) is a finite group of order \( l^N \) and \( \det(I - \rho(\sigma)) \equiv 0 \pmod{l^{N+1}} \) for all \( \sigma \in G \). Then, the following hold:

(i) There exists a sublattice \( L_1 \subset L \) in \( \mathcal{L} \) of index \( l \) such that \( |T(G, L_1)| = l^{N+1} \).

(ii) If \( T(G, L) \) is not cyclic, then there exists a lattice \( L' \in \mathcal{L} \) such that \( T(G, L') \) is cyclic and \( |T(G, L')| < l^N \).

**Proof.** (i) Choose a basis \( \{x, y\} \) for \( L \) such that
\[
T(G, L) = \langle x \pmod{l^s} \rangle \oplus \langle y \pmod{l^t} \rangle
\]
with \( s + t = N, s \geq t \geq 0 \). Then, for \( \sigma \in G \) the attached representation \( \rho \) has the form
\[
\rho(\sigma) = I + A_\sigma \begin{pmatrix} l^s & 0 \\ 0 & l^t \end{pmatrix} \quad \text{with} \quad A_\sigma := \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \in M_2(\mathbb{Z}).
\]

Our assumption implies that \( \det A_\sigma \equiv 0 \pmod{l} \) for all \( \sigma \in G \). Since
\[
A_{\sigma\sigma'} = A_\sigma + A_{\sigma'} + A_\sigma \begin{pmatrix} l^s & 0 \\ 0 & l^t \end{pmatrix} A_{\sigma'},
\]
we have
\[
\det(A_\sigma + A_{\sigma'}) \equiv 0 \pmod{l}
\]
for all \( \sigma, \sigma' \in G \) by Lemma \[2.2\]. Let \( U_\rho \) be the subspace of \( M_2(\mathbb{Z}/l\mathbb{Z}) \) generated by \( A_\sigma \pmod{l} \) for \( \sigma \in G \). Every element \( A \in U_\rho \) is of the form
\[
A = \sum_{i=1}^{r} A_{i}, \quad \text{where} \quad A_i = A_{\sigma_i} \pmod{l}
\]
with \( \sigma_i \in G \ (i = 1, \ldots, r) \). Since \( \det A_i = \det(A_i + A_j) = 0 \) for all \( 0 \leq i, j \leq r \), every element \( A \in U_\rho \) satisfies \( \det A = 0 \) by linearity. Hence by Lemma \[2.2\], we see that for some \( \alpha \in \mathbb{Z}/l\mathbb{Z} \cup \{\infty\} \),
\[
U_\rho \subset W_\alpha \quad \text{or} \quad U_\rho \subset \mathbb{Z}/l\mathbb{Z}.
\]

Case 1. If \( U_\rho \subset W_\infty \), then for \( \sigma \in G \) the matrix \( A_{\sigma} \) has the form
\[
A_{\sigma} = \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix} A'_\sigma \quad \text{with} \quad A'_\sigma := \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \in M_2(\mathbb{Z}).
\]
Let \( L_1 := \mathbb{Z}_l x + \mathbb{Z}_l l y \). Then \( L_1 \in \mathcal{L} \) and for \( \sigma \in G \) the attached representation
\[
\rho_1(\sigma) := \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}^{-1} \rho(\sigma) \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}
\]
has the form
\[
\rho_1(\sigma) = I + A'_\sigma \begin{pmatrix} l^s & 0 \\ 0 & l^{t+1} \end{pmatrix}.
\]
Therefore, we have
\[
T(G, L_1) \cong \mathbb{Z}/l^s\mathbb{Z} \oplus \mathbb{Z}/l^{t+1}\mathbb{Z}.
\]
Next, if \( U_\rho \subset W_\alpha \) for some \( \alpha \in \mathbb{Z}/l\mathbb{Z} \), we may assume that \( U_\rho \subset W_0 \), since
\[
\begin{pmatrix}
1 & \alpha \\
0 & 1
\end{pmatrix}^{-1} W_\alpha \begin{pmatrix}
1 & l^{s-t} \alpha \\
0 & 1
\end{pmatrix} = W_0
\]
and
\[
\begin{pmatrix}
l^s & 0 \\
0 & l^t
\end{pmatrix} \begin{pmatrix}
1 & \pi \\
0 & 1
\end{pmatrix} = \begin{pmatrix}
1 & l^{s-t} \pi \\
0 & 1
\end{pmatrix} \begin{pmatrix}
l^s & 0 \\
0 & l^t
\end{pmatrix},
\]
where \( \pi \) denotes the representative of \( \alpha \) in \( \{0,1,\ldots,l-1\} \). Hence by the same argument as above, we have
\[
T(G, L_2) \simeq \mathbb{Z}/l^{s+1} \mathbb{Z} \oplus \mathbb{Z}/l^t \mathbb{Z} \quad \text{with} \quad L_2 := l x + Z_l y \in \mathcal{L}.
\]

Case 2. If \( U_\rho \subset W_\infty \), then for \( \sigma \in G \) the representation \( \rho \) has the form
\[
\rho(\sigma) = I + A_\sigma \begin{pmatrix}
l^s & 0 \\
0 & l^{t+1}
\end{pmatrix}
\]
with \( A_\sigma := \begin{pmatrix}
a_\sigma & b_\sigma \\
c_\sigma & d_\sigma
\end{pmatrix} \in M_2(\mathbb{Z}) \),
and we have \( T(G, L) \simeq \mathbb{Z}/l^s \mathbb{Z} \oplus \mathbb{Z}/l^t \mathbb{Z} \), which contradicts the assumption. Similarly, the case where \( U_\rho \subset \mathbb{Z}/l\mathbb{Z} \) for some \( \alpha \in \mathbb{Z}/l\mathbb{Z} \) cannot happen. This completes the proof of (i).

(ii) Suppose that \( T(G, L) \) is not cyclic. This implies that
\[
T(G, L) \simeq \mathbb{Z}/l^s \mathbb{Z} \oplus \mathbb{Z}/l^t \mathbb{Z} \quad \text{with} \quad s \geq t > 0.
\]
It suffices to show that there exists \( L' \in \mathcal{L} \) such that
\[
T(G, L') \simeq \mathbb{Z}/l^s \mathbb{Z} \quad \text{or} \quad T(G, L') \simeq \mathbb{Z}/l^t \mathbb{Z}.
\]
By the consideration in (i), we may assume that
\[
U_\rho \subset W_\infty \quad \text{or} \quad U_\rho \subset W_0.
\]
If \( U_\rho \subset W_\infty \), put
\[
L' := l x' + Z_l y' \in \mathcal{L} \quad \text{with} \quad (x', y') := (l^t x, y).
\]
Then, for \( \sigma \in G \) the attached representation
\[
\rho'(\sigma) := \begin{pmatrix}
l^t & 0 \\
0 & 1
\end{pmatrix}^{-1} \rho(\sigma) \begin{pmatrix}
l^t & 0 \\
0 & 1
\end{pmatrix}
\]
has the form
\[
\rho'(\sigma) = I + \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix} A_\sigma \begin{pmatrix}
l^s & 0 \\
0 & 1
\end{pmatrix} \quad \text{with} \quad A_\sigma := \begin{pmatrix}
a_\sigma & b_\sigma \\
c_\sigma & d_\sigma
\end{pmatrix} \in M_2(\mathbb{Z}),
\]
where \( c_\sigma \equiv d_\sigma \equiv 0 \pmod{l} \) for all \( \sigma \in G \). Since \( T(G, L) \simeq \mathbb{Z}/l^s \mathbb{Z} \oplus \mathbb{Z}/l^t \mathbb{Z} \) implies that \( (a_\sigma, b_\sigma) \) mod \( l \) (\( \sigma \in G \)) generates \( \mathbb{Z}/l^2 \mathbb{Z} \), we have
\[
T(G, L') = (x' \mod l^s) \simeq \mathbb{Z}/l^s \mathbb{Z}.
\]
If \( U_\rho \subset W_0 \), then we similarly have
\[
T(G, L') \simeq \mathbb{Z}/l^t \mathbb{Z} \quad \text{with} \quad L' := l x + Z_l l^s y.
\]
This completes the proof of Theorem \( \spadesuit \).

**Remark 2.4.** (1) Theorem \( \spadesuit \) immediately implies a theorem of Katz (\[1\] Theorem 1), which states the following:

If \( \text{det}(I - \rho(\sigma)) \equiv 0 \pmod{l^N} \) for all \( \sigma \in G \), then there exists a lattice \( L' \in \mathcal{L} \) such that \( T(G, L') \equiv 0 \pmod{l^N} \).
(2) Let $0 \leq M \leq \infty$ be the supremum of integers $N$ satisfying $\det(I - \rho(\sigma)) \equiv 0 \pmod{l^N}$ for all $\sigma \in G$. Then we see that $l^M = \sup_{L \in \mathcal{L}} |T(G, L)|$.

(3) Let $l^m := \inf_{L \in \mathcal{L}} |T(G, L)|$. If $m$ is finite and $m < M$, then Theorem 3.3(ii) implies that $T(G, L) \simeq \mathbf{Z}/l^m\mathbf{Z}$ for every $L \in \mathcal{L}$ with $|T(G, L)| = l^m$. In case $V$ is irreducible, the existence of a lattice $L \in \mathcal{L}$ such that $T(G, L) \simeq \mathbf{Z}/l^m\mathbf{Z}$ has been shown in [3, Lemma 3].

3. Possible types of torsion on elliptic curves

Let $K$ be a number field and $\overline{K}$ the algebraic closure of $K$. Denote by $G_K$ the Galois group $\text{Gal}(\overline{K}/K)$ of $\overline{K}$ over $K$. Let $l$ be a prime number. Fix the $K$-isogeny class $\mathcal{C}$ of an elliptic curve over $K$. For $E \in \mathcal{C}$, denote by $T_l(E)$ the $l$-adic Tate module of $E$ and by $\rho : G_K \to \text{Aut}(T_l(E))$ the corresponding $l$-adic representation. For $E, E' \in \mathcal{C}$, we know that $T_l(E) \otimes \mathbf{Q}_l \simeq T_l(E') \otimes \mathbf{Q}_l$ as $G_K$-modules. Hence, for an elliptic curve $E \in \mathcal{C}$ we put $V_l := T_l(E) \otimes \mathbf{Q}_l$, and for any $E' \in \mathcal{C}$ we regard $T_l(E')$ as a $G_K$-submodule of $V_l$. The finiteness of the $K$-isomorphism classes of elliptic curves in $\mathcal{C}$ allows us to let

$$l^M := \sup_{E \in \mathcal{C}} |E(K)_{(l)}| \quad \text{and} \quad l^m := \inf_{E \in \mathcal{C}} |E(K)_{(l)}|,$$

where $E(K)_{(l)}$ denotes the $l$-primary part of $E(K)_{\text{tors}}$. Then for $E \in \mathcal{C}$ we know that

$$\det(I - \rho(\sigma)) \equiv 0 \pmod{l^M} \quad \text{for all } \sigma \in G_K$$

(cf. [1, Introduction]). Moreover, a $G_K$-stable sublattice $L_1 \subset T_l(E)$ of index $l$ corresponds to an elliptic curve $E_1 \in \mathcal{C}$ with $T_l(E_1) = L_1$, and induces a $K$-isogeny $f : E \to E_1$ of degree $l$. Since

$$T_l(G, L) = E(K)_{(l)} \quad \text{for } L \supseteq T_l(E) \quad \text{and} \quad G := \rho(G_K),$$

Theorem 3.3 implies the following.

**Theorem 3.1.** Let $N \geq 0$ be an integer. Assume that there exists $E \in \mathcal{C}$ such that $|E(K)_{(l)}| = l^N$ and $\det(I - \rho(\sigma)) \equiv 0 \pmod{l^{N+1}}$ for all $\sigma \in G_K$. Then, the following hold.

(i) There exists an elliptic curve $E_1 \in \mathcal{C}$ and a $K$-isogeny $f : E \to E_1$ of degree $l$ such that $|E_1(K)_{(l)}| = l^{N+1}$.

(ii) If $E(K)_{(l)}$ is not cyclic, then there exists an elliptic curve $E' \in \mathcal{C}$ such that $E'(K)_{(l)}$ is cyclic and $|E'(K)_{(l)}| < l^N$.

**Corollary 3.2.** Let

$$l^M := \sup_{E \in \mathcal{C}} |E(K)_{(l)}| \quad \text{and} \quad v := \sup\{N \in \mathbf{Z} : E(K) \supset E/|l^N\mathbf{Z}, E \in \mathcal{C}\}.$$ 

Then there exists an elliptic curve $E \in \mathcal{C}$ such that $E(K)_{(l)} \simeq \mathbf{Z}/l^v\mathbf{Z} \oplus \mathbf{Z}/l^{M-v}\mathbf{Z}$.

**Proof.** Let

$$w := \sup\{N \in \mathbf{Z} : E(K)_{(l)} \simeq \mathbf{Z}/l^v\mathbf{Z} \oplus \mathbf{Z}/l^{N}\mathbf{Z}, E \in \mathcal{C}\}.$$ 

Suppose that $v + w < M$. Then Theorem 3.1(i) implies that there exists $E_1 \in \mathcal{C}$ such that $E_1(K)_{(l)}$ is isomorphic either to

$$\mathbf{Z}/l^{v+1}\mathbf{Z} \oplus \mathbf{Z}/l^w\mathbf{Z} \quad \text{or} \quad \mathbf{Z}/l^v\mathbf{Z} \oplus \mathbf{Z}/l^{w+1}\mathbf{Z},$$

which contradicts the definition of $v$ or $w$, respectively. Hence we have $v + w = M$, which completes the proof of the corollary. \qed
Let $l^n$ be the number of $l$-power-th roots of unity in $K$. Since $\det \rho$ is the $l$-adic cyclotomic character of $K$, we have

$$
\det \rho(\sigma) \equiv 1 \pmod{l^n} \quad \text{for all } \sigma \in G_K \text{ and }
$$

$$
\det \rho(\tau) \not\equiv 1 \pmod{l^{n+1}} \quad \text{for some } \tau \in G_K.
$$

Next, we give a lower bound for $m$.

**Proposition 3.3.** \ $m \geq \min\{n, M/2\}$.

**Proof.** It suffices to show that if $m < n$, then $m \geq M/2$. We may assume that $m < M$; thus there exists $E \in \mathcal{C}$ such that $E(K)_{(l)} \cong \mathbb{Z}/l^m\mathbb{Z}$ by Remark 2.4 (3).

Choose a basis $\{x, y\}$ for $T_1(E)$ such that $E(K)_{(l)} = \langle x \pmod{l^m} \rangle$ with $y$ arbitrary. Then, for $\sigma \in G_K$ the attached representation $\rho$ has the form

$$
\rho(\sigma) = I + A_\sigma \begin{pmatrix} l^m & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{with } A_\sigma := \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \in M_2(\mathbb{Z}_l),
$$

where

$$(3.1) \quad (a_\sigma, b_\sigma) \pmod{l} (\sigma \in G_K) \text{ generates } (\mathbb{Z}/l\mathbb{Z})^2.
$$

Since $m < n$ and $\det \rho(\sigma) \equiv 1 \pmod{l^n}$ for all $\sigma \in G_K$, we see that

$$(3.2) \quad d'_\sigma := l^{-m}d_\sigma \in \mathbb{Z}_l, \quad a_\sigma + d'_\sigma \equiv 0 \pmod{l} \quad \text{for all } \sigma \in G_K.
$$

First, assume that $c_\sigma \equiv 0 \pmod{l^m}$ for all $\sigma \in G_K$. Let $E' \in \mathcal{C}$ correspond to $L' := \mathbb{Z}_l x + \mathbb{Z}_l l^m y \subset T_1(E)$.

Then, for $\sigma \in G_K$ the attached representation $\rho'$ has the form

$$
\rho'(\sigma) = I + A'_\sigma \begin{pmatrix} l^m & 0 \\ 0 & l^m \end{pmatrix}, \quad \text{with } A'_\sigma := \begin{pmatrix} a_\sigma & b_\sigma \\ c'_\sigma & d'_\sigma \end{pmatrix},
$$

where $c'_\sigma := l^{-m}c_\sigma \in \mathbb{Z}_l$. It follows from (3.1) that

$$
E'(K)_{(l)} \cong \mathbb{Z}/l^m\mathbb{Z} \oplus \mathbb{Z}/l^m\mathbb{Z}.
$$

If $m < M/2$, then $\det A'_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in G_K$, and from Lemma 2.2 and (3.1) we see that

$$
U_{\rho'} = W_{\alpha} \quad \text{for some } \alpha \in \mathbb{Z}/l\mathbb{Z} \cup \{\infty\},
$$

where $U_{\rho'}$ is the subspace of $M_2(\mathbb{Z}/l\mathbb{Z})$ generated by $A'_\sigma \pmod{l}$ for $\sigma \in G_K$. Hence, there exists $A \in U_{\rho'}$ such that $\text{tr} A \neq 0$, which contradicts (3.2). Therefore, we have $m \geq M/2$.

Secondly, assume that $c_{\tau_1} \not\equiv 0 \pmod{l^m}$ for some $\tau_1 \in G_K$, which means that $m > 0$. Now, we have $b_{\tau_2} \in \mathbb{Z}_l^\times$ for some $\tau_2 \in G_K$ (by (3.1)) and the following relations:

$$
b_{\tau_1\tau_2} \equiv b_{\tau_1} + b_{\tau_2} \pmod{l^m},
$$

$$
c_{\tau_1\tau_2} \equiv c_{\tau_1} + c_{\tau_2} \pmod{l^m}.
$$

Therefore, one can find $\tau \in G_K$ such that $b_\tau c_\tau \not\equiv 0 \pmod{l^m}$, which implies that $m \geq M/2$. This completes the proof of Proposition 3.3 \qed

In case $V_l$ is irreducible, the following holds.

**Theorem 3.4.** Assume that $V_l$ is an irreducible $G_K$-module and that $M > 2n$. Then we have $m = n$.
Proof. This theorem is just a slight generalization of Lemma 2 in [2]. Assume that
\[ E(K)_{(l)} = \langle x \mod l^n \rangle \oplus \langle y \mod l^n \rangle \]
with \( s + t = M, s \geq t \geq 0 \). The assumption \( M > 2n \), together with the definition of \( n \), implies that
\[ s \geq M - n > n \geq t \]
and that for \( \sigma \in G_K \) the representation \( \rho \) attached to \( \{ x, y \} \) has the form
\[ \rho(\sigma) = I + \left( \begin{array}{cc}
  l^n a_{\sigma} & l^n b_{\sigma} \\
  l^n c_{\sigma} & l^n d_{\sigma}
\end{array} \right) \in I + \left( \begin{array}{cc}
  l^n Z_I & l^n Z_I \\
  l^n Z_I & l^n Z_I
\end{array} \right) , \]
where \( d_{\tau} \in Z_I^k \) for some \( \tau \in G_K \). Since the characteristic polynomial \( f(T) \) of the matrix \( \rho(\tau) \) satisfies
\[ f(T) \equiv \{ T - (1 + l^n a_{\tau}) \{ T - (1 + l^n d_{\tau}) \} \mod l^{2n+1}, \]
we have
\[ l^{-2n} f(T) \equiv (S - l^{-n} a_{\tau})(S - d_{\tau}) \equiv S(S - d_{\tau}) \mod l \]
with \( T = 1 + l^n S \). By Hensel’s lemma, there exist \( \mu_1, \mu_2 \in Z_l \) such that \( f(\mu_1) = f(\mu_2) = 0 \) and
\[ \mu_1 \equiv 1, \mu_2 \equiv 1 + l^n d_{\tau} \mod l^{n+1}. \]
Hence, one can choose
\[ P := \left( \begin{array}{cc}
  1 & b' \\
  l^n c' - n & l^n - t
\end{array} \right) \text{ with } b', c' \in Z_l \]
such that
\[ P^{-1} \rho(\tau) P = \left( \begin{array}{cc}
  \mu_1 & 0 \\
  0 & \mu_2
\end{array} \right) , \]
and for \( \sigma \in G_K \) the representation \( \rho_0(\sigma) := P^{-1} \rho(\sigma) P \) has the form
\[ \rho_0(\sigma) = I + \left( \begin{array}{cc}
  l^{M-n} a_{0,\sigma} & l^n b_{0,\sigma} \\
  l^{M-n} c_{0,\sigma} & l^n d_{0,\sigma}
\end{array} \right) \in I + \left( \begin{array}{cc}
  l^{M-n} Z_I & l^n Z_I \\
  l^{M-n} Z_I & l^n Z_I
\end{array} \right) . \]
Let \((x_0, y_0) := (x, y) P\). Since \( V_l \) is irreducible, there exists an integer \( r \) such that
\[ l^{M-n} c_{0,\sigma} \equiv 0 \mod l^r \text{ for all } \sigma \in G_K \text{ and } l^{M-n} c_{0,\sigma} \not\equiv 0 \mod l^{r+1} \text{ for some } \tau' \in G_K. \]
Let \((x', y') := (x_0, l^r y_0)\). Then, for \( \sigma \in G_K \) the attached representation \( \rho' \) has the form
\[ \rho'(\sigma) = I + \left( \begin{array}{cc}
  l^{M-n} a'_{\sigma} & l^n b'_{\sigma} \\
  l^n c'_{\sigma} & l^n d'_{\sigma}
\end{array} \right) \in I + \left( \begin{array}{cc}
  l^{M-n} Z_l & l^n Z_l \\
  Z_l & l^n Z_l
\end{array} \right) \]
with \( c'_{\sigma, \tau} \in Z_l ^k \). Since
\[ \rho'(\tau) = \left( \begin{array}{cc}
  \mu_1 & 0 \\
  0 & \mu_2
\end{array} \right) , \]
we see that \((c'_{\sigma, \tau}) \mod l \ (\sigma \in G_K) \) generates \((Z_l/Z)^2\). Hence, the elliptic curve \( E' \) corresponding to the lattice \( L' := Z_l x' \oplus Z_l y' \) satisfies
\[ E'(K)_{(l)} = \langle y' \mod l^n \rangle \simeq Z/l^n Z. \]
It follows from Proposition 3.3 that \( m = n. \)
Let
\[ E(K)(0) \simeq \mathbb{Z}/l^n \mathbb{Z} \oplus \mathbb{Z}/l^t \mathbb{Z} \] with \( s \geq t \geq 0 \).

We conclude this paper by describing the range where \((s, t)\) can appear, when \(E\) runs over \(C\).

(I) \( V_l \) is an irreducible \( G_l \)-module.

If \( M > 2n \), then for each \( N \) with \( n \leq N < M - n \) there exists \( E_N \in C \) such that \( E_N(K)(0) \simeq \mathbb{Z}/l^N \mathbb{Z} \). Indeed, for \( N = n \), Remark 2.3 (3) assures that there exists \( E \in C \) such that \( E(K)(0) \simeq \mathbb{Z}/l^n \mathbb{Z} \), since \( m = n \) by Theorem 3.4. For \( n < N < M - n \), let \( \{x', y'\} \) be as in the proof of Theorem 3.4.

Put
\[ L_N := Z_l x_N + Z_l y_N \]
for each \( N \), where
\[ (x_N, y_N) := (x', y') P_N \quad \text{with} \quad P_N := \begin{pmatrix} l^{N+n} & l^N \\ 0 & 1 \end{pmatrix}. \]

Let \( E_N \in C \) be the elliptic curve such that \( T_l(E_N) = L_N \). Then, for \( \sigma \in G_K \) we have
\[ \rho_N(\sigma) := P_N^{-1} \rho'(\sigma) P_N = I + B(\sigma), \]
where
\[ B(\sigma) = \begin{pmatrix} -c_\sigma & -d_\sigma \\ 0 & 0 \end{pmatrix} \quad \text{(or)} \quad \begin{pmatrix} -c_\sigma & -d_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \quad \text{if} \quad n = 0 \quad \text{(mod} \ l). \]

Since \((c_\sigma, d_\sigma) \mod l \ (\sigma \in G_K)\) generates \((\mathbb{Z}/l\mathbb{Z})^2\), we obtain
\[ E_N(K)(0) \equiv (x_N \mod l^n) \simeq \mathbb{Z}/l^N \mathbb{Z}, \]
hence we easily see that for each \( N \) with \( n \leq N < M - n \), each type of the groups
\[ \mathbb{Z}/l^N \mathbb{Z}, \mathbb{Z}/l^N \mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z}, \ldots, \mathbb{Z}/l^N \mathbb{Z} \oplus \mathbb{Z}/l^m \mathbb{Z} \]
can be realized as \( E(K)(0) \) for some \( E \in C \).

Now, assume that \( s + t = M \) and \( s < v \), where
\[ v := \sup \{ N \in \mathbb{Z} : E(K) \supset \mathbb{Z}/l^N \mathbb{Z}, \ E \in C \}. \]

Then we have \( M - n < v \), and by Corollary 3.2 there exists \( E' \in C \) such that
\[ E'(K)(0) \equiv (x' \mod l^v \oplus y' \mod l^{M-v}) \simeq \mathbb{Z}/l^v \mathbb{Z} \oplus \mathbb{Z}/l^{M-v} \mathbb{Z}. \]

For \( \sigma \in G_K \) the attached representation \( \rho' \) has the form
\[ \rho'(\sigma) = I + \begin{pmatrix} l^v a_{\sigma} & l^{M-v} b_{\sigma} \\ l^v c_{\sigma} & l^{M-v} d_{\sigma} \end{pmatrix} \in I + \begin{pmatrix} l^v Z_l & l^{M-v} Z_l \\ l^v Z_l & l^{M-v} Z_l \end{pmatrix}, \]
where \( b_{\tau_1}, c_{\tau_2} \in Z_l^{\times} \) for some \( \tau_1, \tau_2 \in G_K \). Hence, when we put
\[ E'_1 := E'/\langle y \mod l \rangle, \ E'_2 := E'/\langle y \mod l^2 \rangle, \ldots, E'_{M-v} := E'/\langle y \mod l^{M-v} \rangle, \]
the groups \( E'_1(K)(0), E'_2(K)(0), \ldots, E'_{M-v}(K)(0) \) are isomorphic respectively to
\[ \mathbb{Z}/l^v \mathbb{Z}, \mathbb{Z}/l^v \mathbb{Z} \oplus \mathbb{Z}/l^{M-v} \mathbb{Z}, \mathbb{Z}/l^v \mathbb{Z} \oplus \mathbb{Z}/l^{M-v} \mathbb{Z}, \ldots, \mathbb{Z}/l^v \mathbb{Z}, \]
when we put
\[ E''_1 := E'/\langle x \mod l \rangle, E''_2 := E'/\langle x \mod l^2 \rangle, \ldots, E''_{M-v} := E'/\langle x \mod l^{M-v} \rangle, \]
the groups \( E''_1(K)(0), E''_2(K)(0), \ldots, E''_{M-v}(K)(0) \) are isomorphic respectively to
\[ \mathbb{Z}/l^{v-1} \mathbb{Z} \oplus \mathbb{Z}/l^{M-v+1} \mathbb{Z}, \mathbb{Z}/l^{v-2} \mathbb{Z} \oplus \mathbb{Z}/l^{M-v+2} \mathbb{Z}, \ldots, \mathbb{Z}/l^v \mathbb{Z} \oplus \mathbb{Z}/l^{M-v} \mathbb{Z}. \]
Consequently, we obtain the following: 

Put 
\[ \mu := \min\{n, [M/2]\}. \]  
Each type of the groups 
\[ \mathbb{Z}/l^v\mathbb{Z}, \mathbb{Z}/l^v\mathbb{Z} \oplus \mathbb{Z}/l^v\mathbb{Z}, \ldots, \mathbb{Z}/l^v\mathbb{Z} \oplus \mathbb{Z}/l^{M-v-1}\mathbb{Z}, \]  
\[ \mathbb{Z}/l^v\mathbb{Z} \oplus \mathbb{Z}/l^{M-v}\mathbb{Z}, \mathbb{Z}/l^{v-1}\mathbb{Z} \oplus \mathbb{Z}/l^{M-v+1}\mathbb{Z}, \ldots, \mathbb{Z}/l^{M-\mu}\mathbb{Z} \oplus \mathbb{Z}/l^{\mu}\mathbb{Z} \]  
can be realized as \( E(K)_l \) for some \( E \in \mathcal{C} \).

Therefore, in case \( V_l \) is irreducible, the range where \((s, t)\) can appear is as shown in Figure 1. Here, the integral points on the bold lines and in the solidly shaded region necessarily appear.

(i) \( n < M/2 \) \( (\implies m = n) \)  
(ii) \( n \geq M/2 \) \( (\implies M/2 \leq m) \)

\[ \begin{array}{c}
\text{Figure 1.} \\
\end{array} \]

(II) \( V_l \) is a reducible \( G_K \)-module.

Assume that \( E \) is an elliptic curve in \( \mathcal{C} \) such that its endomorphism ring \( \text{End}_K(E) \) over \( K \) is isomorphic to the maximal order in the imaginary quadratic field \( \text{End}_K(E) \otimes \mathbb{Q} \). Then \( T_l(E) \) is completely reducible, and the assumption \( E(K)_l \simeq \mathbb{Z}/l^v\mathbb{Z} \oplus \mathbb{Z}/l^v\mathbb{Z} \) implies that there exists a basis \( \{x, y\} \) for \( T_l(E) \) such that for \( \sigma \in G_K \),
\[ \rho(\sigma) = I + \begin{pmatrix} l^v a_{\sigma} & 0 \\ 0 & l^v d_{\sigma} \end{pmatrix} \in I + \begin{pmatrix} l^v \mathbb{Z}_l & 0 \\ 0 & l^v \mathbb{Z}_l \end{pmatrix}, \]
where \( a_{\tau}, d_{\tau} \in \mathbb{Z}_l^\times \) for some \( \tau \in G_K \). It follows from Remark 2.4 (2) that \( s + t = M \).

Define
\[ E_0 := E \quad \text{and} \quad E_i := E/(P_i), \]
where \( P_i := x + y \mod l^i \) (or \( \mod l^{r+i} \) for some integer \( r \geq 0 \) if \( s = t \)) with \( i = 1, \ldots, t \). Then, it is not difficult to show the following:

- If \( n < M/2 \), then \( s = M - n \) and \( t = n \).
- If \( n \geq M/2 \), then \( M \) is even and \( s = t = M/2 \).
- We have \( m \geq s \), \( E_t(K)_l \) is cyclic of order \( l^m \) and
\[ E_t(K)_l \simeq \mathbb{Z}/l^s\mathbb{Z} \oplus \mathbb{Z}/l^{t-i}\mathbb{Z}, \]
with \( s_i := \min\{s + i, m\} \) \( (i = 0, 1, \ldots, t) \), which exhaust all possible types of torsion groups \( E(K)_l \) in \( \mathcal{C} \).
Therefore, in case \( V \) is reducible, the range where \((s, t)\) can appear is as shown in Figure 2. Here, the integral points on the bold lines necessarily appear.

(i) \( n < M/2 \) \((\implies M/2 < M - n \leq m = v)\)  
(ii) \( n \geq M/2 \) \((\implies M/2 \leq m = v)\)

In particular, the possible types of maximal \( l \)-primary torsion in \( C \) are given as follows.

**Proposition 3.5.** In the \( K \)-isogeny class \( C \), the possible types of maximal \( l \)-primary torsion are exactly the following:

\[
\mathbb{Z}/l^n\mathbb{Z} \oplus \mathbb{Z}/l^{M-v}\mathbb{Z}, \mathbb{Z}/l^{v-1}\mathbb{Z} \oplus \mathbb{Z}/l^{M-v+1}\mathbb{Z}, \ldots, \mathbb{Z}/l^{M-\mu}\mathbb{Z} \oplus \mathbb{Z}/l^{\mu}\mathbb{Z},
\]

where \( \mu := \min\{n, [M/2]\} \).

**Acknowledgment**

We would like to thank the referee for helpful suggestions and comments.

**References**

