Division fields and an effective version of the local-global principle for divisibility

Laura Paladino

laura.paladino@unical.it

Università della Calabria

Specialisation and Effectiveness in Number Theory
28 Aug - 2 Sept BIRS

Joint work with Roberto Dvornicich (University of Pisa)

Introduction

- K a field with $\mathrm{char}(K) \neq 2, 3$;
- $\overline{K}$ the algebraic closure of K;
- $\mathcal{E}$ an elliptic curve with Weierstrass form

$$\mathcal{E}: \quad y^2 = x^3 + Ax + B, \quad \text{where } A, B \in K;$$

- $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$, for every positive integer m.

- K a field with $\mathrm{char}(K) \neq 2, 3$;
- $\overline{K}$ the algebraic closure of K;
- $\mathcal{E}$ an elliptic curve with Weierstrass form

$$\mathcal{E}: \quad y^2 = x^3 + Ax + B, \quad \text{where } A, B \in K;$$

- $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$, for every positive integer m.

- K a field with $\mathrm{char}(K) \neq 2, 3$;
- $\overline{K}$ the algebraic closure of K;
- $\mathcal{E}$ an elliptic curve with Weierstrass form

$$\mathcal{E}: \quad y^2 = x^3 + Ax + B, \quad \text{where } A, B \in K;$$

- $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$, for every positive integer m.

- K a field with $\mathrm{char}(K) \neq 2, 3$;
- $\overline{K}$ the algebraic closure of K;
- $\mathcal{E}$ an elliptic curve with Weierstrass form

$$\mathcal{E}: \quad y^2 = x^3 + Ax + B, \quad \text{where } A, B \in K;$$

- $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$, for every positive integer m.

Definition

The m-division field $K(\mathcal{E}[m])$ of $\mathcal{E}$ over K is the field generated over K by the coordinates of the m-torsion points of $\mathcal{E}$. We will also denote it by K_m.

It is well-known that $\mathcal{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two of the m-torsion points of $\mathcal{E}$, forming a basis of $\mathcal{E}[m]$. Then

$$K_m = K(x_1, x_2, y_1, y_2).$$

By the Weil Pairing we have

$$K(\zeta_m) \subseteq K_m.$$

Definition

The m-division field $K(\mathcal{E}[m])$ of $\mathcal{E}$ over K is the field generated over K by the coordinates of the m-torsion points of $\mathcal{E}$. We will also denote it by K_m.

It is well-known that $\mathcal{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two of the m-torsion points of $\mathcal{E}$, forming a basis of $\mathcal{E}[m]$. Then

$$K_m = K(x_1, x_2, y_1, y_2).$$

By the Weil Pairing we have

$$K(\zeta_m) \subseteq K_m.$$

Definition

The m-division field $K(\mathcal{E}[m])$ of $\mathcal{E}$ over K is the field generated over K by the coordinates of the m-torsion points of $\mathcal{E}$. We will also denote it by K_m.

It is well-known that $\mathcal{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two of the m-torsion points of $\mathcal{E}$, forming a basis of $\mathcal{E}[m]$. Then

$$K_m = K(x_1, x_2, y_1, y_2).$$

By the Weil Pairing we have

$$K(\zeta_m) \subseteq K_m.$$

Definition

The m-division field $K(\mathcal{E}[m])$ of $\mathcal{E}$ over K is the field generated over K by the coordinates of the m-torsion points of $\mathcal{E}$. We will also denote it by K_m.

It is well-known that $\mathcal{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two of the m-torsion points of $\mathcal{E}$, forming a basis of $\mathcal{E}[m]$. Then

$$K_m = K(x_1, x_2, y_1, y_2).$$

By the Weil Pairing we have

$$K(\zeta_m) \subseteq K_m.$$

Definition

The m-division field $K(\mathcal{E}[m])$ of $\mathcal{E}$ over K is the field generated over K by the coordinates of the m-torsion points of $\mathcal{E}$. We will also denote it by K_m.

It is well-known that $\mathcal{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two of the m-torsion points of $\mathcal{E}$, forming a basis of $\mathcal{E}[m]$. Then

$$K_m = K(x_1, x_2, y_1, y_2).$$

By the Weil Pairing we have

$$K(\zeta_m) \subseteq K_m.$$

Definition

The m-division field $K(\mathcal{E}[m])$ of $\mathcal{E}$ over K is the field generated over K by the coordinates of the m-torsion points of $\mathcal{E}$. We will also denote it by K_m.

It is well-known that $\mathcal{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two of the m-torsion points of $\mathcal{E}$, forming a basis of $\mathcal{E}[m]$. Then

$$K_m = K(x_1, x_2, y_1, y_2).$$

By the Weil Pairing we have

$$K(\zeta_m) \subseteq K_m.$$

Questions:

1. In which cases $K(\zeta_m) = K(\mathcal{E}[m])$?

2. What about number fields $K(\mathcal{E}[m])$, when $K(\zeta_m) \subsetneq K(\mathcal{E}[m])$? Other generating systems? Degrees? Galois groups $\mathrm{Gal}(K(\mathcal{E}[m])/K)$? Discriminant? Etc.

Questions:

1. In which cases $K(\zeta_m) = K(\mathcal{E}[m])$?

2. What about number fields $K(\mathcal{E}[m])$, when $K(\zeta_m) \subsetneq K(\mathcal{E}[m])$? Other generating systems? Degrees? Galois groups $\mathrm{Gal}(K(\mathcal{E}[m])/K)$? Discriminant? Etc.

Questions:

1. In which cases $K(\zeta_m) = K(\mathcal{E}[m])$?

2. What about number fields $K(\mathcal{E}[m])$, when $K(\zeta_m) \subsetneq K(\mathcal{E}[m])$?
Other generating systems? Degrees? Galois groups $\mathrm{Gal}(K(\mathcal{E}[m])/K)$? Discriminant? Etc.

Questions:

1. In which cases $K(\zeta_m) = K(\mathcal{E}[m])$?

2. What about number fields $K(\mathcal{E}[m])$, when $K(\zeta_m) \subsetneq K(\mathcal{E}[m])$? Other generating systems? Degrees? Galois groups $\mathrm{Gal}(K(\mathcal{E}[m])/K)$? Discriminant? Etc.

Elliptic curves with $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\mathcal{E}[m])$

Theorem (Merel, Stein, 2001 + Rebolledo 2013)

Let p be a prime number.

If $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$ then $p \in \{2, 3, 5\}$.

The fundamental fact in Merel's proof is showing the existence of modular curves with a rational point of prime order $p \in \{2, 3, 5\}$. But no numerical example were given.

Theorem (Merel, Stein, 2001 + Rebolledo 2013)

Let p be a prime number.

If $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$ then $p \in \{2, 3, 5\}$.

The fundamental fact in Merel's proof is showing the existence of modular curves with a rational point of prime order $p \in \{2, 3, 5\}$. But no numerical example were given.

Theorem (P.,2010)

We have $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ *if and only if* $\mathcal{E}$ *belongs to the family*

$$\mathcal{F}_{\beta,h}: \qquad y^2 = x^3 + A_{\beta,h}x + B_{\beta,h}, \qquad \beta, h \in \mathbb{Q} \setminus \{0\},$$

$$A_{\beta,h} = -\frac{27\beta^4}{h^4} + \frac{18\beta^3}{h^2} - \frac{9\beta^2}{2} + \frac{3\beta h^2}{2} - \frac{3h^4}{16},$$

$$B_{\beta,h} = \frac{54\beta^6}{h^6} - \frac{54\beta^5}{h^4} + \frac{45\beta^4}{2h^2} - \frac{15\beta^2 h^2}{8} - \frac{3\beta h^4}{8} - \frac{1}{32h^6}$$

Elliptic curves with $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\mathcal{E}[m])$

Theorem (Gonzáles-Jiménez, Lozano-Robledo, 2016)

If $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\zeta_m)$ *then* $m \in \{2, 3, 4, 5\}$.

Theorem (Gonzáles-Jiménez, Lozano-Robledo, 2016)

If $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ *is abelian, then* $m = 2, 3, 4, 5, 6,$ *or* 8.

Theorem (González-Jiménez, Lozano-Robledo, 2016)

If $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\zeta_m)$ then $m \in \{2, 3, 4, 5\}$.

Theorem (González-Jiménez, Lozano-Robledo, 2016)

If $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is abelian, then $m = 2, 3, 4, 5, 6,$ or 8.

Generators for $K(\mathcal{E}[m])$

Theorem (Reynolds, 2011)

Let m be divisible by an integer $d \geq 3$. Then

$$K_m = K\left(x_1, y\left(\frac{m}{d}P_1\right), x_2, y\left(\frac{m}{d}P_2\right)\right),$$

where $y\left(\frac{m}{d}P_i\right)$ denotes the ordinate of the point $\frac{m}{d}P_i$, for $i = 1, 2$.

Since K_m/K is a Galois extension, then by the Primitive Element Theorem we have that it is monogenous. Anyway, it is not easy to find explicitly $\alpha \in K_m$ such that $K_m = K(\alpha)$. Then we searched for minimal generating sets inside $\{x_1, x_2, \zeta_m, y_1, y_2\}$.

Theorem (Bandini, P., 2016)

Let $\mathcal{E}$, P_1 and P_2 as above. For every odd integer $m \geq 5$ we have

$$K_m = K(x_1, \zeta_m, y_2).$$

If m is an even number, then either $K_m = K(x_1, \zeta_m, y_2)$ or $K_m = K(x_1, \zeta_m, y_1, y_2)$ and $\mathrm{Gal}(K_m/K(x_1, \zeta_m, y_2))$ is generated by the element mapping P_2 to $\frac{m}{2}P_1 + P_2$.

Since K_m/K is a Galois extension, then by the Primitive Element Theorem we have that it is monogenous. Anyway, it is not easy to find explicitly $\alpha \in K_m$ such that $K_m = K(\alpha)$. Then we searched for minimal generating sets inside $\{x_1, x_2, \zeta_m, y_1, y_2\}$.

Theorem (Bandini, P., 2016)

Let $\mathcal{E}$, P_1 and P_2 as above. For every odd integer $m \geq 5$ we have

$$K_m = K(x_1, \zeta_m, y_2).$$

If m is an even number, then either $K_m = K(x_1, \zeta_m, y_2)$ or $K_m = K(x_1, \zeta_m, y_1, y_2)$ and $\mathrm{Gal}(K_m/K(x_1, \zeta_m, y_2))$ is generated by the element mapping P_2 to $\frac{m}{2}P_1 + P_2$.

Since K_m/K is a Galois extension, then by the Primitive Element Theorem we have that it is monogenous. Anyway, it is not easy to find explicitly $\alpha \in K_m$ such that $K_m = K(\alpha)$. Then we searched for minimal generating sets inside $\{x_1, x_2, \zeta_m, y_1, y_2\}$.

THEOREM (BANDINI, P., 2016)

Let $\mathcal{E}$, P_1 and P_2 as above. For every odd integer $m \geq 5$ we have

$$K_m = K(x_1, \zeta_m, y_2).$$

If m is an even number, then either $K_m = K(x_1, \zeta_m, y_2)$ or $K_m = K(x_1, \zeta_m, y_1, y_2)$ and $\mathrm{Gal}(K_m/K(x_1, \zeta_m, y_2))$ is generated by the element mapping P_2 to $\frac{m}{2}P_1 + P_2$.

Since K_m/K is a Galois extension, then by the Primitive Element Theorem we have that it is monogenous. Anyway, it is not easy to find explicitly $\alpha \in K_m$ such that $K_m = K(\alpha)$. Then we searched for minimal generating sets inside $\{x_1, x_2, \zeta_m, y_1, y_2\}$.

Theorem (Bandini, P., 2016)

Let $\mathcal{E}$, P_1 and P_2 as above. For every odd integer $m \geq 5$ we have

$$K_m = K(x_1, \zeta_m, y_2).$$

If m is an even number, then either $K_m = K(x_1, \zeta_m, y_2)$ or $K_m = K(x_1, \zeta_m, y_1, y_2)$ and $\mathrm{Gal}(K_m/K(x_1, \zeta_m, y_2))$ is generated by the element mapping P_2 to $\frac{m}{2}P_1 + P_2$.

Galois representations

Let p be an odd prime number and consider the following statement.

Lemma (Bandini, P., 2016)

For any prime $p \geqslant 5$ one has

$$[K_p : K(x_1, \zeta_p)] \leq 2p.$$

Moreover the Galois group $\mathrm{Gal}(K_p/K(x_1, \zeta_p))$ is cyclic, generated by a power of

$$\eta = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Let p be an odd prime number and consider the following statement.

Lemma (Bandini, P., 2016)

For any prime $p \geqslant 5$ one has

$$[K_p : K(x_1, \zeta_p)] \leq 2p.$$

Moreover the Galois group $\mathrm{Gal}(K_p/K(x_1, \zeta_p))$ is cyclic, generated by a power of

$$\eta = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

By the previous lemma, we have

$$[K_p : K] \le \frac{p^2-1}{2} \cdot (p-1) \cdot 2p = (p^2-p)(p^2-1) = |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|.$$

If K is a number field and $\mathcal{E}$ has no complex multiplication, then, by the famous Serre's theorem, the Galois representation

$$\rho_{\mathcal{E},p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

is surjective for all $p > p(\mathcal{E})$, where $p(\mathcal{E})$ is a prime depending on $\mathcal{E}$.

Since $\mathrm{Gal}(\overline{K}/K) \simeq \mathrm{Gal}(K_p/K)$, then for all but finitely many p the set $\{x_1, y_2, \zeta_p\}$ is a minimal set of generators for K_p/K (among those contained in $\{x_1, x_2, y_1, y_2, \zeta_p\}$).

By the previous lemma, we have

$$[K_p : K] \leq \frac{p^2-1}{2} \cdot (p-1) \cdot 2p = (p^2-p)(p^2-1) = |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|.$$

If K is a number field and $\mathcal{E}$ has no complex multiplication, then, by the famous Serre's theorem, the Galois representation

$$\rho_{\mathcal{E},p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

is surjective for all $p > p(\mathcal{E})$, where $p(\mathcal{E})$ is a prime depending on $\mathcal{E}$.

Since $\mathrm{Gal}(\overline{K}/K) \simeq \mathrm{Gal}(K_p/K)$, then for all but finitely many p the set $\{x_1, y_2, \zeta_p\}$ is a minimal set of generators for K_p/K (among those contained in $\{x_1, x_2, y_1, y_2, \zeta_p\}$).

By the previous lemma, we have

$$[K_p : K] \leq \frac{p^2-1}{2} \cdot (p-1) \cdot 2p = (p^2-p)(p^2-1) = |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|.$$

If K is a number field and $\mathcal{E}$ has no complex multiplication, then, by the famous Serre's theorem, the Galois representation

$$\rho_{\mathcal{E},p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

is surjective for all $p > p(\mathcal{E})$, where $p(\mathcal{E})$ is a prime depending on $\mathcal{E}$.

Since $\mathrm{Gal}(\overline{K}/K) \simeq \mathrm{Gal}(K_p/K)$, then for all but finitely many p the set $\{x_1, y_2, \zeta_p\}$ is a minimal set of generators for K_p/K (among those contained in $\{x_1, x_2, y_1, y_2, \zeta_p\}$).

Definition

For an elliptic curve $\mathcal{E}/K$ and a prime p we say that p is *exceptional* for $\mathcal{E}$ if $\rho_{\mathcal{E},p}$ is not surjective, i.e., if $[K_p : K] < |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|$.

For exceptional primes the Galois group $\mathrm{Gal}(K_p/K)$ is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Hence it falls in one of the following cases.

Definition

For an elliptic curve $\mathcal{E}/K$ and a prime p we say that p is *exceptional* for $\mathcal{E}$ if $\rho_{\mathcal{E},p}$ is not surjective, i.e., if $[K_p : K] < |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|$.

For exceptional primes the Galois group $\mathrm{Gal}(K_p/K)$ is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Hence it falls in one of the following cases.

Lemma (Serre, 1972)

Let $G \lneq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Then one of the following holds:

1. *G is contained in a Borel subgroup;*
2. *G is a Cartan subgroup;*
3. *G is contained in the normalizer of a Cartan subgroup, but it is not a Cartan subgroup;*
4. *the image of G under $\pi : \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is contained in a subgroup which is isomorphic to A_4 or A_5 or S_4.*

Lemma (Larson, Vaintrob, 2014)

If $p \geq 53$ is unramified in $K/\mathbb{Q}$ and exceptional for $\mathcal{E}$, then $\mathrm{Gal}(K_p/K)$ does not verify 4.

Lemma (Serre, 1972)

Let $G \lneq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Then one of the following holds:

1. *G is contained in a Borel subgroup;*
2. *G is a Cartan subgroup;*
3. *G is contained in the normalizer of a Cartan subgroup, but it is not a Cartan subgroup;*
4. *the image of G under $\pi : \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is contained in a subgroup which is isomorphic to A_4 or A_5 or S_4.*

Lemma (Larson, Vaintrob, 2014)

If $p \geq 53$ is unramified in $K/\mathbb{Q}$ and exceptional for $\mathcal{E}$, then $\mathrm{Gal}(K_p/K)$ does not verify **4**.

Theorem (Bandini, P., 2016)

Assume that $p \geq 5$ is exceptional.
If $\mathrm{Gal}(K_p/K)$ is contained in a Borel subgroup or in the normalizer of a split Cartan subgroup, then

- *if $p \not\equiv 1 \pmod 3$, then $K_p = K(\zeta_p, y_2)$;*
- *if $p \equiv 1 \pmod 3$, then $[K_p : K(\zeta_p, y_2)]$ is 1 or 3.*

If $\mathrm{Gal}(K_p/K)$ is contained in the normalizer of a non-split Cartan subgroup, then

- *if $p \equiv 1 \pmod 3$, then $K_p = K(\zeta_p, y_2)$;*
- *if $p \not\equiv 1 \pmod 3$, then $[K_p : K(\zeta_p, y_2)]$ is 1 or 3.*

When $m = p^n$, with $n \geq 2$, the generating set $\{x_1, \zeta_{p^n}, y_2\}$ of K_m/K is not minimal and can be improved as follows.

Theorem (Dvornicich, P., 2022)

Let $m = p^n$, where p is a prime and n is a positive integer. Then

$$K_{p^n} = K(x_1, \zeta_p, y_2).$$

THEOREM (DVORNICICH, P., 2022)

Let $F := K(x_1, y_1)$. For all $p > 3$ and $r \geq 1$, we have

$$K(\mathcal{E}[p^n])/F = F(\zeta_{p^n}, \sqrt[m_1]{a}),$$

with $a \in F(\zeta_{p^n})$ and $\mathrm{Gal}(K(\mathcal{E}[p^n])/F) = C_{m_1}.C_{m_2}$, where m_1, m_2 are positive integers such that $m_1 | p^n$ and $m_2 | p^{n-1}(p-1)$.

In the representation of $\mathrm{Gal}(K(\mathcal{E}[p^n])/F)$ in $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, the group C_{m_1} is generated by a power of

$$\omega := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Theorem (Dvornicich, P., 2022)

Let $F := K(x_1, y_1)$*. For all* $p > 3$ *and* $r \geq 1$*, we have*

$$K(\mathcal{E}[p^n])/F = F(\zeta_{p^n}, \sqrt[m_1]{a}),$$

with $a \in F(\zeta_{p^n})$ *and* $\mathrm{Gal}(K(\mathcal{E}[p^n])/F) = C_{m_1}.C_{m_2}$*, where* m_1*,* m_2 *are positive integers such that* $m_1 | p^n$ *and* $m_2 | p^{n-1}(p-1)$*.*

In the representation of $\mathrm{Gal}(K(\mathcal{E}[p^n])/F)$ *in* $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$*, the group* C_{m_1} *is generated by a power of*

$$\omega := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

A bound for the discriminant of $K(\mathcal{E}[m])$

Theorem (Dvornicich, P., 2022)

Let $D_{K_m/K}$ denote the discriminant of the extension K_m/K and let $h(D_{K_m/K})$ be its logarithmic height. For every $m \geq 3$, we have

$$h(D_{K_m/K}) \leq \begin{cases} 3(m^2-1)^4(m^2-3)(\log m + h(A) + h(B)), & \text{if } m \text{ is odd;} \\ 3(m^2-4)^4(m^2-6)(\log m + h(A) + h(B)), & \text{if } m \text{ is even.} \end{cases}$$

Theorem (Lagarias, Montgomery, Odlyzko, 1979)

For any number field K, any finite Galois extension L/K, with $L \neq \mathbb{Q}$ and any conjugacy class C in $\mathrm{Gal}(L/K)$, there exists a prime v of K which is unramified in L, for which the Artin symbol $\left(\frac{L|K}{v}\right)$ is equal to C and

$$N_{K/\mathbb{Q}}(v) \leq |D_{L/\mathbb{Q}}|^{C_1}.$$

To have an explicit effective version one has to know explicitly C_1 and the discriminant $D_{L/\mathbb{Q}}$ or an upper bound for it.

Theorem (Lagarias, Montgomery, Odlyzko, 1979)

For any number field K, any finite Galois extension L/K, with $L \neq \mathbb{Q}$ and any conjugacy class C in $\mathrm{Gal}(L/K)$, there exists a prime v of K which is unramified in L, for which the Artin symbol $\left(\frac{L|K}{v}\right)$ is equal to C and

$$N_{K/\mathbb{Q}}(v) \leq |D_{L/\mathbb{Q}}|^{C_1}.$$

To have an explicit effective version one has to know explicitly C_1 and the discriminant $D_{L/\mathbb{Q}}$ or an upper bound for it.

Theorem (Ahn, Kwon, 2019)

For any number field K, any finite Galois extension L/K, with $L \neq \mathbb{Q}$ and any conjugacy class C in $\mathrm{Gal}(L/K)$, there exists a prime v of K which is unramified in L, for which the Artin symbol $\left(\frac{L|K}{v}\right)$ is equal to C and

$$N_{K/\mathbb{Q}}(v) \leq |D_{L/\mathbb{Q}}|^{12577}.$$

An effective version of the hypotheses of the local-global divisibility

Problem (Dvornicich, Zannier, 2001)

Let $P \in \mathcal{E}(K)$. Assume that for all but finitely many places $v \in K$, there exists $D_v \in \mathcal{E}(K_v)$ such that $P = mD_v$, where K_v is the completion of K at the place v. Is it possible to conclude that there exists $D \in \mathcal{E}(K)$ such that $P = mD$?

It suffices to solve the problem for $m = p^n$ to get an anwer for a general m.

Problem (Dvornicich, Zannier, 2001)

Let $P \in \mathcal{E}(K)$. Assume that for all but finitely many places $v \in K$, there exists $D_v \in \mathcal{E}(K_v)$ such that $P = mD_v$, where K_v is the completion of K at the place v. Is it possible to conclude that there exists $D \in \mathcal{E}(K)$ such that $P = mD$?

It suffices to solve the problem for $m = p^n$ to get an anwer for a general m.

- Tate 1962; (reproved by Dvornicich, Zannier in 2001 and by Wong in 2001): YES , for all p, when $n = 1$;
- Dvornicich, Zannier, 2007: YES , for all $p > 163$, $n \geq 1$, when $k = \mathbb{Q}$;
- P., Ranieri, Viada, 2012: YES , for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, $n \geq 1$;
- P., Ranieri, Viada, 2014: YES , for all $p > 3$, $n \geq 1$, when $k = \mathbb{Q}$;
- Creutz, 2016: NO , for $p = 2, 3$ and $n \geq 2$.

- Tate 1962; (reproved by Dvornicich, Zannier in 2001 and by Wong in 2001): YES , for all p, when $n = 1$;
- Dvornicich, Zannier, 2007: YES , for all $p > 163$, $n \geq 1$, when $k = \mathbb{Q}$;
- P., Ranieri, Viada, 2012: YES , for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, $n \geq 1$;
- P., Ranieri, Viada, 2014: YES , for all $p > 3$, $n \geq 1$, when $k = \mathbb{Q}$;
- Creutz, 2016: NO , for $p = 2, 3$ and $n \geq 2$.

- Tate 1962; (reproved by Dvornicich, Zannier in 2001 and by Wong in 2001): YES , for all p, when $n = 1$;
- Dvornicich, Zannier, 2007: YES , for all $p > 163$, $n \geq 1$, when $k = \mathbb{Q}$;
- P., Ranieri, Viada, 2012: YES , for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, $n \geq 1$;
- P., Ranieri, Viada, 2014: YES , for all $p > 3$, $n \geq 1$, when $k = \mathbb{Q}$;
- Creutz, 2016: NO , for $p = 2, 3$ and $n \geq 2$.

- Tate 1962; (reproved by Dvornicich, Zannier in 2001 and by Wong in 2001): YES , for all p, when $n = 1$;
- Dvornicich, Zannier, 2007: YES , for all $p > 163$, $n \geq 1$, when $k = \mathbb{Q}$;
- P., Ranieri, Viada, 2012: YES , for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, $n \geq 1$;
- P., Ranieri, Viada, 2014: YES , for all $p > 3$, $n \geq 1$, when $k = \mathbb{Q}$;
- Creutz, 2016: NO , for $p = 2, 3$ and $n \geq 2$.

- Tate 1962; (reproved by Dvornicich, Zannier in 2001 and by Wong in 2001): YES , for all p, when $n = 1$;
- Dvornicich, Zannier, 2007: YES , for all $p > 163$, $n \geq 1$, when $k = \mathbb{Q}$;
- P., Ranieri, Viada, 2012: YES , for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, $n \geq 1$;
- P., Ranieri, Viada, 2014: YES , for all $p > 3$, $n \geq 1$, when $k = \mathbb{Q}$;
- Creutz, 2016: NO , for $p = 2, 3$ and $n \geq 2$.

In particular

$$Ш(K, \mathcal{E}[p^n]) = 0.$$

As a consequence of a result of Creutz of 2013, we have that the triviality of $Ш(K, \mathcal{E}[p^n])$, for every r, implies an affirmative answer to the following question posed by Cassels in 1962.

Cassels' question

Are the elements of $Ш(K, \mathcal{E})$ infinitely divisible by a prime p when considered as elements of the Weil-Châtelet group $H^1(K, \mathcal{E})$ of all classes of principal homogeneous spaces for $\mathcal{E}$ defined over K?

Creutz 2013 + P., Ranieri, Viada, 2012-2014 $\Rightarrow$ YES , for all $p > 3$, when $K = \mathbb{Q}$ and for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, when $K \neq \mathbb{Q}$.

In particular

$$Ш(K, \mathcal{E}[p^n]) = 0.$$

As a consequence of a result of Creutz of 2013, we have that the triviality of $Ш(K, \mathcal{E}[p^n])$, for every r, implies an affirmative answer to the following question posed by Cassels in 1962.

Cassels' question

Are the elements of $Ш(K, \mathcal{E})$ infinitely divisible by a prime p when considered as elements of the Weil-Châtelet group $H^1(K, \mathcal{E})$ of all classes of principal homogeneous spaces for $\mathcal{E}$ defined over K?

Creutz 2013 + P., Ranieri, Viada, 2012-2014 $\Rightarrow$ YES , for all $p > 3$, when $K = \mathbb{Q}$ and for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, when $K \neq \mathbb{Q}$.

In particular

$$Ш(K, \mathcal{E}[p^n]) = 0.$$

As a consequence of a result of Creutz of 2013, we have that the triviality of $Ш(K, \mathcal{E}[p^n])$, for every r, implies an affirmative answer to the following question posed by Cassels in 1962.

Cassels' question

Are the elements of $Ш(K, \mathcal{E})$ infinitely divisible by a prime p when considered as elements of the Weil-Châtelet group $H^1(K, \mathcal{E})$ of all classes of principal homogeneous spaces for $\mathcal{E}$ defined over K?

Creutz 2013 + P., Ranieri, Viada, 2012-2014 $\Rightarrow$ YES , for all $p > 3$, when $K = \mathbb{Q}$ and for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, when $K \neq \mathbb{Q}$.

In the proofs we need that v varies among all places unramified in K_{p^n} to have that the Galois group $G_v := \mathrm{Gal}((K_{p^n})_w/K_v)$, where $w|v$, varies over all cyclic subgroups of G.

By the Chebotarev Density Theorem the local Galois group G_v varies over all cyclic subgroups of G as v varies in a set of primes with Dirichlet density 1.

In the proofs we need that v varies among all places unramified in K_{p^n} to have that the Galois group $G_v := \mathrm{Gal}((K_{p^n})_w/K_v)$, where $w|v$, varies over all cyclic subgroups of G.

By the Chebotarev Density Theorem the local Galois group G_v varies over all cyclic subgroups of G as v varies in a set of primes with Dirichlet density 1.

Indeed G_v varies over all cyclic subgroups of G as v varies in a set of primes v such that $h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(p^n, A, B)$, where $B(p^n, A, B)$ is the upper bound showed above for $h(D_{\mathbb{Q}(\mathcal{E}[p^n])/\mathbb{Q}})$.

Corollary (Dvornicich, P., 2022)

Let $p \geq 5$ and $n \geq 1$. Let $P \in \mathcal{E}(\mathbb{Q})$ and let

$$S = \{v \in M_K | h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(p^n, A, B)\},$$

Assume that for all $v \in S$, there exists $D_v \in \mathcal{E}(\mathbb{Q}_v)$ such that $P = p^n D_v$. Then there exists $D \in \mathcal{E}(\mathbb{Q})$ such that $P = p^n D$.

Thank you for your attention!