LOCAL-GLOBAL QUESTIONS FOR DIVISIBILITY IN COMMUTATIVE ALGEBRAIC GROUPS

Laura Paladino
laura.paladino@unical.it

UNIVERSITÀ DELLA CALABRIA

Italy

Symposium on Arithmetic Geometry and its Applications
February 09, 2023

Joint work with Jessica Alessandrì (Università degli Studi dell'Aquila)
and Rocco Chirivì (Università di Lecce)

Joint work with Roberto Dvornicich (Università di Pisa)

Notation

k	a number field
$\bar{k}$	the algebraic closure of k
G_k	the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$
M_k	the set of places $v \in k$
k_v	the completion of k at v

k	a number field
$\bar{k}$	the algebraic closure of k
G_k	the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$
M_k	the set of places $v \in k$
k_v	the completion of k at v

k	a number field
$\bar{k}$	the algebraic closure of k
G_k	the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$
M_k	the set of places $v \in k$
k_v	the completion of k at v

k	a number field
$\bar{k}$	the algebraic closure of k
G_k	the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$
M_k	the set of places $v \in k$
k_v	the completion of k at v

k	a number field
$\bar{k}$	the algebraic closure of k
G_k	the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$
M_k	the set of places $v \in k$
k_v	the completion of k at v

$\mathcal{A}$	a commutative algebraic group defined over k
p	a prime number
l	a positive integer
$\mathcal{A}[p^l]$	the p^l-torsion subgroup of $\mathcal{A}$
$K := k(\mathcal{A}[p^l])$	the number field obtained by adding to k the coordinates of the points in $\mathcal{A}[p^l]$

$\mathcal{A}$	a commutative algebraic group defined over k
p	a prime number
l	a positive integer
$\mathcal{A}[p^l]$	the p^l-torsion subgroup of $\mathcal{A}$
$K := k(\mathcal{A}[p^l])$	the number field obtained by adding to k the coordinates of the points in $\mathcal{A}[p^l]$

$\mathcal{A}$	a commutative algebraic group defined over k
p	a prime number
l	a positive integer
$\mathcal{A}[p^l]$	the p^l-torsion subgroup of $\mathcal{A}$
$K := k(\mathcal{A}[p^l])$	the number field obtained by adding to k the coordinates of the points in $\mathcal{A}[p^l]$

$\mathcal{A}$	a commutative algebraic group defined over k
p	a prime number
l	a positive integer
$\mathcal{A}[p^l]$	the p^l-torsion subgroup of $\mathcal{A}$
$K := k(\mathcal{A}[p^l])$	the number field obtained by adding to k the coordinates of the points in $\mathcal{A}[p^l]$

$\mathcal{A}$	a commutative algebraic group defined over k
p	a prime number
l	a positive integer
$\mathcal{A}[p^l]$	the p^l-torsion subgroup of $\mathcal{A}$
$K := k(\mathcal{A}[p^l])$	the number field obtained by adding to k the coordinates of the points in $\mathcal{A}[p^l]$

It is well known that

$$\mathcal{A}[p^l] \simeq (\mathbb{Z}/p^l\mathbb{Z})^n, \text{ where } n \text{ depends only on } \mathcal{A},$$

$$G_k \text{ acts on } \mathcal{A}[p^l] \text{ as a subgroup } G \text{ of } \mathrm{GL}_n(\mathbb{Z}/p^l\mathbb{Z}),$$

$$G_{k_v} := \mathrm{Gal}(\bar{k}_v/k_v) \text{ acts on } \mathcal{A}[p^l] \text{ as a subgroup } G_v \text{ of } G.$$

It is well known that

$$\mathcal{A}[p^l] \simeq (\mathbb{Z}/p^l\mathbb{Z})^n, \text{ where } n \text{ depends only on } \mathcal{A},$$

$$G_k \text{ acts on } \mathcal{A}[p^l] \text{ as a subgroup } G \text{ of } \mathrm{GL}_n(\mathbb{Z}/p^l\mathbb{Z}),$$

$$G_{k_v} := \mathrm{Gal}(\bar{k}_v/k_v) \text{ acts on } \mathcal{A}[p^l] \text{ as a subgroup } G_v \text{ of } G.$$

It is well known that

$$\mathcal{A}[p^l] \simeq (\mathbb{Z}/p^l\mathbb{Z})^n, \text{ where } n \text{ depends only on } \mathcal{A},$$

$$G_k \text{ acts on } \mathcal{A}[p^l] \text{ as a subgroup } G \text{ of } \mathrm{GL}_n(\mathbb{Z}/p^l\mathbb{Z}),$$

$$G_{k_v} := \mathrm{Gal}(\bar{k}_v/k_v) \text{ acts on } \mathcal{A}[p^l] \text{ as a subgroup } G_v \text{ of } G.$$

The local-global divisibility problem

Theorem. (Hasse, 1923-1924)

If $x \in k$ is a square in all but finitely many fields k_v, with $v \in M_k$, then x is a square in k.

What about p^l-powers instead squares?

Grunwald-Wang Theorem, 1950: the local-global principle holds for all powers p^l, with $p > 2$ and powers 2^l, with $l \leq 2$.

Trost, 1948: the local-global principle fails for all powers 2^l, with $l > 2$.

Considering such a local-global principle in k is like considering the principle on a torus of dimension 1 over k.

Theorem. (Hasse, 1923-1924)

If $x \in k$ is a square in all but finitely many fields k_v, with $v \in M_k$, then x is a square in k.

What about p^l-powers instead squares?

Grunwald-Wang Theorem, 1950: the local-global principle holds for all powers p^l, with $p > 2$ and powers 2^l, with $l \leq 2$.

Trost, 1948: the local-global principle fails for all powers 2^l, with $l > 2$.

Considering such a local-global principle in k is like considering the principle on a torus of dimension 1 over k.

Theorem. (Hasse, 1923-1924)

If $x \in k$ is a square in all but finitely many fields k_v, with $v \in M_k$, then x is a square in k.

What about p^l-powers instead squares?

Grunwald-Wang Theorem, 1950: the local-global principle holds for all powers p^l, with $p > 2$ and powers 2^l, with $l \leq 2$.

Trost, 1948: the local-global principle fails for all powers 2^l, with $l > 2$.

Considering such a local-global principle in k is like considering the principle on a torus of dimension 1 over k.

Theorem. (Hasse, 1923-1924)

If $x \in k$ is a square in all but finitely many fields k_v, with $v \in M_k$, then x is a square in k.

What about p^l-powers instead squares?

Grunwald-Wang Theorem, 1950: the local-global principle holds for all powers p^l, with $p > 2$ and powers 2^l, with $l \leq 2$.

Trost, 1948: the local-global principle fails for all powers 2^l, with $l > 2$.

Considering such a local-global principle in k is like considering the principle on a torus of dimension 1 over k.

Theorem. (Hasse, 1923-1924)

If $x \in k$ is a square in all but finitely many fields k_v, with $v \in M_k$, then x is a square in k.

What about p^l-powers instead squares?

Grunwald-Wang Theorem, 1950: the local-global principle holds for all powers p^l, with $p > 2$ and powers 2^l, with $l \leq 2$.

Trost, 1948: the local-global principle fails for all powers 2^l, with $l > 2$.

Considering such a local-global principle in k is like considering the principle on a torus of dimension 1 over k.

What about other commutative algebraic groups?

LOCAL-GLOBAL DIVISIBILITY PROBLEM. (DVORNICICH, ZANNIER)

Let $P \in \mathcal{A}(k)$. Suppose for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = p^l D_v$. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$?

What about other commutative algebraic groups?

Local-Global Divisibility Problem. (Dvornicich, Zannier)

Let $P \in \mathcal{A}(k)$. Suppose for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = p^l D_v$. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$?

Let $W \in \mathcal{A}(\bar{k})$ such that $W = p^l P$. Then the cocycle $Z = \{Z_\sigma\}_{\sigma \in G}$, where

$$Z_\sigma := \sigma(W) - W, \quad \sigma \in G,$$

vanishes in $H^1(G, \mathcal{A}[p^l])$ if and only if there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$.

The triviality of $H^1(G, \mathcal{A}[p^l])$ implies an affirmative answer to the local-global divisibility by p^l.

Let Σ be the subset of M_k containing all the places v of k satisfying the assumptions of the problem.
Then the hypotheses of the problem assure the vanishing of Z in $H^1(G_v, \mathcal{A}[p^l])$, for every $v \in \Sigma$.

Let $W \in \mathcal{A}(\bar{k})$ such that $W = p^l P$. Then the cocycle $Z = \{Z_\sigma\}_{\sigma \in G}$, where

$$Z_\sigma := \sigma(W) - W, \quad \sigma \in G,$$

vanishes in $H^1(G, \mathcal{A}[p^l])$ if and only if there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$.

The triviality of $H^1(G, \mathcal{A}[p^l])$ implies an affirmative answer to the local-global divisibility by p^l.

Let Σ be the subset of M_k containing all the places v of k satisfying the assumptions of the problem.
Then the hypotheses of the problem assure the vanishing of Z in $H^1(G_v, \mathcal{A}[p^l])$, for every $v \in \Sigma$.

Let $W \in \mathcal{A}(\bar{k})$ such that $W = p^l P$. Then the cocycle $Z = \{Z_\sigma\}_{\sigma \in G}$, where

$$Z_\sigma := \sigma(W) - W, \quad \sigma \in G,$$

vanishes in $H^1(G, \mathcal{A}[p^l])$ if and only if there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$.

The triviality of $H^1(G, \mathcal{A}[p^l])$ implies an affirmative answer to the local-global divisibility by p^l.

Let Σ be the subset of M_k containing all the places v of k satisfying the assumptions of the problem.
Then the hypotheses of the problem assure the vanishing of Z in $H^1(G_v, \mathcal{A}[p^l])$, for every $v \in \Sigma$.

Let $W \in \mathcal{A}(\bar{k})$ such that $W = p^l P$. Then the cocycle $Z = \{Z_\sigma\}_{\sigma \in G}$, where

$$Z_\sigma := \sigma(W) - W, \quad \sigma \in G,$$

vanishes in $H^1(G, \mathcal{A}[p^l])$ if and only if there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$.

The triviality of $H^1(G, \mathcal{A}[p^l])$ implies an affirmative answer to the local-global divisibility by p^l.

Let Σ be the subset of M_k containing all the places v of k satisfying the assumptions of the problem.
Then the hypotheses of the problem assure the vanishing of Z in $H^1(G_v, \mathcal{A}[p^l])$, for every $v \in \Sigma$.

$$H^1_{\mathrm{loc}}(G,\mathcal{A}[p^l]) := \bigcap_{v\in\Sigma} \ker\{H^1(G,\mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_v,\mathcal{A}[p^l])\}.$$

Proposition. (Dvornicich, Zannier, 2001)

Let $\Sigma = \{v \in M_k | v \text{ is unramified in } K\}$. If $H^1_{\mathrm{loc}}(G,\mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

Proposition. (Dvornicich, Zannier, 2001)

Let $\Sigma = \{v \in M_k | v \text{ is unramified in } K\}$. If $H^1_{\mathrm{loc}}(G,\mathcal{A}[p^l]) \neq 0$, then the local-global divisibility by p^l fails in $\mathcal{A}$ over a finite extension of k.

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) := \bigcap_{v\in\Sigma} \ker\{H^1(G, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_v, \mathcal{A}[p^l])\}.$$

Proposition. (Dvornicich, Zannier, 2001)

Let $\Sigma = \{v \in M_k | v \text{ is unramified in } K\}$. If $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

Proposition. (Dvornicich, Zannier, 2001)

Let $\Sigma = \{v \in M_k | v \text{ is unramified in } K\}$. If $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) \neq 0$, then the local-global divisibility by p^l fails in $\mathcal{A}$ over a finite extension of k.

$$H^1_{\mathrm{loc}}(G,\mathcal{A}[p^l]) := \bigcap_{v\in\Sigma} \ker\{H^1(G,\mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_v,\mathcal{A}[p^l])\}.$$

Proposition. (Dvornicich, Zannier, 2001)

Let $\Sigma = \{v \in M_k | v \text{ is unramified in } K\}$. If $H^1_{\mathrm{loc}}(G,\mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

Proposition. (Dvornicich, Zannier, 2001)

Let $\Sigma = \{v \in M_k | v \text{ is unramified in } K\}$. If $H^1_{\mathrm{loc}}(G,\mathcal{A}[p^l]) \neq 0$, then the local-global divisibility by p^l fails in $\mathcal{A}$ over a finite extension of k.

The group $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l])$ is very similar to the Tate-Shafarevich group.

Let

$$Ш_\Sigma(k, \mathcal{A}[p^l]) := \bigcap_{v \in \Sigma} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

Then

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) \simeq Ш_\Sigma(k, \mathcal{A}[p^l]).$$

In particular the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l])$ implies the triviality of $Ш_\Sigma(k, \mathcal{A}[p^l])$, which contains the Tate-Shafarevich group:

$$Ш(k, \mathcal{A}[p^l]) := \bigcap_{v \in M_k} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

The group $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l])$ is very similar to the Tate-Shafarevich group.

Let

$$Ш_{\Sigma}(k, \mathcal{A}[p^l]) := \bigcap_{v \in \Sigma} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

Then

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) \simeq Ш_{\Sigma}(k, \mathcal{A}[p^l]).$$

In particular the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l])$ implies the triviality of $Ш_{\Sigma}(k, \mathcal{A}[p^l])$, which contains the Tate-Shafarevich group:

$$Ш(k, \mathcal{A}[p^l]) := \bigcap_{v \in M_k} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

The group $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l])$ is very similar to the Tate-Shafarevich group.

Let

$$Ш_\Sigma(k, \mathcal{A}[p^l]) := \bigcap_{v \in \Sigma} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

Then

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) \simeq Ш_\Sigma(k, \mathcal{A}[p^l]).$$

In particular the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l])$ implies the triviality of $Ш_\Sigma(k, \mathcal{A}[p^l])$, which contains the Tate-Shafarevich group:

$$Ш(k, \mathcal{A}[p^l]) := \bigcap_{v \in M_k} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

The group $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l])$ is very similar to the Tate-Shafarevich group.

Let

$$Ш_\Sigma(k, \mathcal{A}[p^l]) := \bigcap_{v \in \Sigma} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

Then

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) \simeq Ш_\Sigma(k, \mathcal{A}[p^l]).$$

In particular the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l])$ implies the triviality of $Ш_\Sigma(k, \mathcal{A}[p^l])$, which contains the Tate-Shafarevich group:

$$Ш(k, \mathcal{A}[p^l]) := \bigcap_{v \in M_k} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

In fact we have the following diagram given by inflation-restriction exact sequences where Σ_K denotes the set of places w of $K = k(\mathcal{A}[p^l])$ extending the places $v \in \Sigma$.

$$\begin{array}{ccccccc}
0 & \to & H^1(G, \mathcal{A}[p^l]) & \xrightarrow{inf} & H^1(G_k, \mathcal{A}[p^l]) & \xrightarrow{res} & H^1(G_K, \mathcal{A}[p^l]) \\
 & & \Big\downarrow \prod res_v & & \Big\downarrow \prod res_v & & \Big\downarrow \prod res_w \\
0 & \to & \prod_{v\in\Sigma} H^1(G_v, \mathcal{A}[p^l]) & \xrightarrow{inf} & \prod_{v\in\Sigma} H^1(G_{k_v}, \mathcal{A}[p^l]) & \xrightarrow{res} & \prod_{w\in\Sigma_K} H^1(G_{K_w}, \mathcal{A}[p^l])
\end{array}$$

The vertical map on the right is injective because of G_K acting trivially on $\mathcal{A}[p^l]$ and by the Chebotarev Density Theorem.

$$\begin{tikzcd}
0 \arrow[r] & H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) \arrow[r, "\sim"] \arrow[d] & Ш_{\Sigma}(k, \mathcal{A}[p^l]) \arrow[r] \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & H^1(G, \mathcal{A}[p^l]) \arrow[r, "inf"] \arrow[d, "\prod res_v"] & H^1(G_k, \mathcal{A}[p^l]) \arrow[r, "res"] \arrow[d, "\prod res_v"] & H^1(G_K, \mathcal{A}[p^l]) \arrow[d, "\prod res_w"] \\
0 \arrow[r] & \prod_{v \in \Sigma} H^1(G_v, \mathcal{A}[p^l]) \arrow[r, "inf"] & \prod_{v \in \Sigma} H^1(G_{k_v}, \mathcal{A}[p^l]) \arrow[r, "res"] & \prod_{w \in \Sigma_K} H^1(G_{K_w}, \mathcal{A}[p^l])
\end{tikzcd}$$

Cassels' question

Let $\mathcal{E}$ be an elliptic curve defined over k. Then the triviality

$$Ш(k, \mathcal{E}[p^l]), \text{ for every } l \geq 1,$$

implies an affirmative answer to the following question stated by Cassels in the third of his famous series of papers *Arithmetic of curves of genus 1*.

CASSELS' QUESTION. (1962)

Are the elements of $Ш(k, \mathcal{E})$ infinitely divisible by a prime p when considered as elements of the group $H^1(G_k, \mathcal{E})$?

Let $\mathcal{E}$ be an elliptic curve defined over k. Then the triviality

$$Ш(k, \mathcal{E}[p^l]), \text{ for every } l \geq 1,$$

implies an affirmative answer to the following question stated by Cassels in the third of his famous series of papers *Arithmetic of curves of genus 1*.

CASSELS' QUESTION. (1962)

Are the elements of $Ш(k, \mathcal{E})$ infinitely divisible by a prime p when considered as elements of the group $H^1(G_k, \mathcal{E})$?

Since 1972, Cassels' question was considered in abelian varieties and not only in elliptic curves, firstly by Bašmakov and in the last few years by Çiperiani and Stix and by Creutz.

If in Cassels' question one considers a general commutative algebraic group $\mathcal{A}$ instead of an elliptic curve and the divisibility by a fixed power of p, then one gets the following local-global question:

Local-Global Divisibility Problem on the Weil-Châtelet group.

Let $\sigma \in H^1(G_k, \mathcal{A})$. Assume that for all $v \in M_k$ there exists $\tau_v \in H^1(G_{k_v}, \mathcal{A})$, such that $p^l \tau_v = res_v(\sigma)$. Can we conclude that there exists $\tau \in H^1(G_k, \mathcal{A})$, such that $p^l \tau = \sigma$?

Since 1972, Cassels' question was considered in abelian varieties and not only in elliptic curves, firstly by Bašmakov and in the last few years by Çiperiani and Stix and by Creutz.

If in Cassels' question one considers a general commutative algebraic group $\mathcal{A}$ instead of an elliptic curve and the divisibility by a fixed power of p, then one gets the following local-global question:

Local-Global Divisibility Problem on the Weil-Châtelet group.

Let $\sigma \in H^1(G_k, \mathcal{A})$. Assume that for all $v \in M_k$ there exists $\tau_v \in H^1(G_{k_v}, \mathcal{A})$, such that $p^l \tau_v = res_v(\sigma)$. Can we conclude that there exists $\tau \in H^1(G_k, \mathcal{A})$, such that $p^l \tau = \sigma$?

THEOREM. (CREUTZ, 2013)

Let $\mathcal{A}$ be an abelian variety defined over a number field k. Let $\mathcal{A}^\vee$ be its dual and $\mathcal{A}[p^l]^\vee$ the Cartier dual of $\mathcal{A}[p^l]$. We have that

$$Ш(k, \mathcal{A}) \subseteq p^l H^1(k, \mathcal{A})$$

if and only if the image of the map

$$Ш(k, \mathcal{A}[p^l]^\vee) \to Ш(k, \mathcal{A}^\vee)$$

is contained in the maximal divisible subgroup of $Ш(k, \mathcal{A}^\vee)$.

For principally polarized abelian varieties $\mathcal{A}$ over k, we have $\mathcal{A}[p^l] \simeq \mathcal{A}[p^l]^\vee$ and then:

$$\begin{array}{ccc}
H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = 0, & \Longrightarrow & Ш(k, \mathcal{A}[p^l]) = 0, \\
\text{for all } l \geq 1 & & \text{for all } l \geq 1 \\
\Downarrow & & \Downarrow \\
\text{local-global divisibility by } p^l & & \text{affirmative answer to} \\
\text{in } \mathcal{A} \text{ over } k, & & \text{Cassels' question} \\
\text{for every } l \geq 1 & & \text{for } p
\end{array}$$

For principally polarized abelian varieties $\mathcal{A}$ over k, we have $\mathcal{A}[p^l] \simeq \mathcal{A}[p^l]^\vee$ and then:

$$\begin{array}{ccc}
\begin{array}{c} H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = 0, \\ \text{for all } l \geq 1 \end{array} & \Longrightarrow & \begin{array}{c} Ш(k, \mathcal{A}[p^l]) = 0, \\ \text{for all } l \geq 1 \end{array} \\
\Downarrow & & \Downarrow \\
\begin{array}{c} \text{local-global divisibility by } p^l \\ \text{in } \mathcal{A} \text{ over } k, \\ \text{for every } l \geq 1 \end{array} & & \begin{array}{c} \text{affirmative answer to} \\ \text{Cassels' question} \\ \text{for } p \end{array}
\end{array}$$

For principally polarized abelian varieties $\mathcal{A}$ over k, we have $\mathcal{A}[p^l] \simeq \mathcal{A}[p^l]^\vee$ and then:

$$\begin{array}{ccc} H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = 0, & \Longrightarrow & Ш(k, \mathcal{A}[p^l]) = 0, \\ \text{for all } l \geq 1 & & \text{for all } l \geq 1 \\ \Downarrow & & \Downarrow \\ \text{local-global divisibility by } p^l & & \text{affirmative answer to} \\ \text{in } \mathcal{A} \text{ over } k, & & \text{Cassels' question} \\ \text{for every } l \geq 1 & & \text{for } p \end{array}$$

For principally polarized abelian varieties $\mathcal{A}$ over k, we have $\mathcal{A}[p^l] \simeq \mathcal{A}[p^l]^\vee$ and then:

$$\begin{array}{ccc}
\begin{array}{c} H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = 0, \\ \text{for all } l \geq 1 \end{array} & \Longrightarrow & \begin{array}{c} Ш(k, \mathcal{A}[p^l]) = 0, \\ \text{for all } l \geq 1 \end{array} \\
\Downarrow & & \Downarrow \\
\begin{array}{c} \text{local-global divisibility by } p^l \\ \text{in } \mathcal{A} \text{ over } k, \\ \text{for every } l \geq 1 \end{array} & & \begin{array}{c} \text{affirmative answer to} \\ \text{Cassels' question} \\ \text{for } p \end{array}
\end{array}$$

For principally polarized abelian varieties $\mathcal{A}$ over k, we have $\mathcal{A}[p^l] \simeq \mathcal{A}[p^l]^\vee$ and then:

$$\begin{array}{ccc}
\begin{array}{c} H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = 0, \\ \text{for all } l \geq 1 \end{array} & \Longrightarrow & \begin{array}{c} Ш(k, \mathcal{A}[p^l]) = 0, \\ \text{for all } l \geq 1 \end{array} \\
\Downarrow & & \Downarrow \\
\begin{array}{c} \text{local-global divisibility by } p^l \\ \text{in } \mathcal{A} \text{ over } k, \\ \text{for every } l \geq 1 \end{array} & & \begin{array}{c} \text{affirmative answer to} \\ \text{Cassels' question} \\ \text{for } p \end{array}
\end{array}$$

Elliptic curves

Theorem. (P., Ranieri, Viada, 2012-2014)

Let $\mathcal{E}$ be an elliptic curve defined over k, then

- the local-global disivibility by p^l holds in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$ and $l \geq 1$;
- the local-global disivibility by p^l holds in $\mathcal{E}$ over k, for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ and $l \geq 1$, when $[k : \mathbb{Q}] > 1$.

Counterexamples

In elliptic curves over $\mathbb{Q}$ for all 2^l, with $l \geq 2$ (P., 2011);

in elliptic curves over $\mathbb{Q}$ for all 3^l, with $l \geq 2$ (Creutz, 2016).

THEOREM. (P., RANIERI, VIADA, 2012-2014)

Let $\mathcal{E}$ be an elliptic curve defined over k, then

- the local-global disivibility by p^l holds in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$ and $l \geq 1$;
- the local-global disivibility by p^l holds in $\mathcal{E}$ over k, for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ and $l \geq 1$, when $[k:\mathbb{Q}] > 1$.

Counterexamples

In elliptic curves over $\mathbb{Q}$ for all 2^l, with $l \geq 2$ (P., 2011);

in elliptic curves over $\mathbb{Q}$ for all 3^l, with $l \geq 2$ (Creutz, 2016).

THEOREM. (P., RANIERI, VIADA, 2012-2014)

Let $\mathcal{E}$ be an elliptic curve defined over k, then

- the local-global disivibility by p^l holds in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$ and $l \geq 1$;
- the local-global disivibility by p^l holds in $\mathcal{E}$ over k, for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ and $l \geq 1$, when $[k : \mathbb{Q}] > 1$.

Counterexamples

In elliptic curves over $\mathbb{Q}$ for all 2^l, with $l \geq 2$ (P., 2011);

in elliptic curves over $\mathbb{Q}$ for all 3^l, with $l \geq 2$ (Creutz, 2016).

Theorem. (P., Ranieri, Viada, 2012-2014)

Let $\mathcal{E}$ be an elliptic curve defined over k, then

- the local-global disivibility by p^l holds in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$ and $l \geq 1$;
- the local-global disivibility by p^l holds in $\mathcal{E}$ over k, for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ and $l \geq 1$, when $[k : \mathbb{Q}] > 1$.

Counterexamples

In elliptic curves over $\mathbb{Q}$ for all 2^l, with $l \geq 2$ (P., 2011);

in elliptic curves over $\mathbb{Q}$ for all 3^l, with $l \geq 2$ (Creutz, 2016).

THEOREM. (P., RANIERI, VIADA, 2012-2014)

Let $\mathcal{E}$ be an elliptic curve defined over k, then

- the local-global disivibility by p^l holds in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$ and $l \geq 1$;
- the local-global disivibility by p^l holds in $\mathcal{E}$ over k, for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ and $l \geq 1$, when $[k : \mathbb{Q}] > 1$.

Counterexamples

In elliptic curves over $\mathbb{Q}$ for all 2^l, with $l \geq 2$ (P., 2011);

in elliptic curves over $\mathbb{Q}$ for all 3^l, with $l \geq 2$ (Creutz, 2016).

THEOREM. (CREUTZ, LU, 2022)

The local-global divisibility by 7^l holds in elliptic curves over quadratic fields for every $l \geq 1$.

(TATE, 1962)

The elements of $Ш(k, \mathcal{E})$ are divisible by p in $H^1(G_k, \mathcal{E})$.

The question for the divisibility by powers of p remained open for 50 years, for every p.

COROLLARY. (P., RANIERI, VIADA, 2012-2014)

- Cassels' question has an affirmative answer in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$.
- Cassels' question has an affirmative answer in $\mathcal{E}$ over k, for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, when $[k : \mathbb{Q}] > 1$.

(Tate, 1962)

The elements of $Ш(k, \mathcal{E})$ are divisible by p in $H^1(G_k, \mathcal{E})$.

The question for the divisibility by powers of p remained open for 50 years, for every p.

Corollary. (P., Ranieri, Viada, 2012-2014)

- Cassels' question has an affirmative answer in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$.
- Cassels' question has an affirmative answer in $\mathcal{E}$ over k, for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$, when $[k : \mathbb{Q}] > 1$.

Abelian varieties

THEOREM. (GILLIBERT, RANIERI, 2017)

Let $\mathcal{A}$ be an abelian variety defined over a number field k. Suppose that there exists an element $\sigma \in G$, with order dividing $p-1$ and not fixing any nontrivial element of $\mathcal{A}[p]$. Moreover suppose that $H^1(G, \mathcal{A}[p]) = 0$. Then the local-global divisibility by p^l holds in $\mathcal{A}$ over k and $Ш(G_k, \mathcal{A}[p^l]) = 0$, for every $l \geq 1$.

THEOREM. (ÇIPERIANI, STIX, 2015)

Let $\mathcal{A}$ be an abelian variety defined over a number field k. Assume that

1) $H^1(G_k, \mathcal{A}[p]) = 0$ and
2) the G_k-modules $\mathcal{A}[p]$ and $\mathrm{End}(\mathcal{A}[p])$ have no common irreducible subquotients.

Then

$$Ш(k, \mathcal{A}[p^l]) = 0, \text{ for every } l \geq 1.$$

Counterexamples

For every p, Cassels' question has a negative answer for infinitely many abelian varieties defined over $\mathbb{Q}$ (Creutz, 2013).

Theorem. (P., 2019)

Let $\mathcal{A}$ be a commutative algebraic group defined over k. Assume that $\mathcal{A}[p]$ is a very strongly irreducible G-module or a direct sum of very strongly irreducible G-modules.
If $p > \frac{n}{2} + 1$, then the local-global divisibility by p holds in $\mathcal{A}$ over k and $Ш(k, \mathcal{A}[p]) = 0$.

Furthermore, the proof shows exactly all the Galois representations of G_k in $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ for which the local-global divisibility may fail in $\mathcal{A}$.

Theorem. (P., 2019)

Let $\mathcal{A}$ be a commutative algebraic group defined over k. Assume that $\mathcal{A}[p]$ is a very strongly irreducible G-module or a direct sum of very strongly irreducible G-modules.
If $p > \frac{n}{2} + 1$, then the local-global divisibility by p holds in $\mathcal{A}$ over k and $\text{Ш}(k, \mathcal{A}[p]) = 0$.

Furthermore, the proof shows exactly all the Galois representations of G_k in $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ for which the local-global divisibility may fail in $\mathcal{A}$.

Algebraic tori

Illengo produced the following result about the local-global divisibility by p in algebraic tori.

THEOREM. (ILLENGO, 2008)

Let $\mathcal{T}$ be an algebraic torus of dimension n defined over a number field k.
Let $p \geq 3$ a prime number.
If $n < 3(p-1)$ then the local-global divisibility by p holds in $\mathcal{T}$.

Counterexamples

In algebraic tori of dimension $n \geq 3(p-1)$ for every p (Illengo, 2008).

Illengo produced the following result about the local-global divisibility by p in algebraic tori.

THEOREM. (ILLENGO, 2008)

Let $\mathcal{T}$ be an algebraic torus of dimension n defined over a number field k.
Let $p \geq 3$ a prime number.
If $n < 3(p-1)$ then the local-global divisibility by p holds in $\mathcal{T}$.

Counterexamples

In algebraic tori of dimension $n \geq 3(p-1)$ for every p (Illengo, 2008).

Theorem. (Alessandrì, Chirivì, P., 2022)

Let $p \geq 3$ be a prime number.

(A) Let k be a number field and let $\mathcal{T}$ be a torus defined over k. If $\mathcal{T}$ has dimension $n < p - 1$, then the local-global divisibility by p^l holds in $\mathcal{T}$ over k, for every $l \geq 1$.

(B) For each $n \geq p - 1$ there exists a torus defined over $\mathbb{Q}$ of dimension n and a finite extension $L/\mathbb{Q}$ such that the local-global divisibility by p^l does not hold for $\mathcal{T}(L)$ for any $l \geq 1$.

An effective version of the hypotheses of the local-global divisibility problem in elliptic curves

Theorem. (Dvornicich, P., 2022)

Let $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ and $l \geq 1$. Let $P \in \mathcal{E}(k)$ and let

$$S = \{v \in M_k | h(N_{k/\mathbb{Q}}(v)) \leq 12577 \cdot B(p^l, b, c)\},$$

Assume that for all $v \in S$, there exists $D_v \in \mathcal{E}(k_v)$ such that $P = p^l D_v$. Then there exists $D \in \mathcal{E}(k)$ such that $P = p^l D$.

Theorem. (Dvornicich, P., 2022)

Let $D_{K_m/k}$ denote the discriminant of the extension $k(\mathcal{E}[m])/k$ and let $h(D_{K_m/k})$ be its logarithmic height, for every positive integer $m \geq 3$. We have

$$h(D_{K_m/k}) \leq B(m, b, c),$$

where

$$B(m, b, c) = \begin{cases} 3(m^2-1)^4(m^2-3)(\log m + h(b) + h(c)), & \text{if } m \text{ is odd;} \\ 3(m^2-4)^4(m^2-6)(\log m + h(b) + h(c)), & \text{if } m \text{ is even.} \end{cases}$$

Thank you for your attention!

Campus UniCal

A view of Calabria

Happy $7 \cdot 17^2$!