European Journal of Mathematics (2022) 8 (Suppl 2):S599–S628
https://doi.org/10.1007/s40879-022-00567-z

REVIEW ARTICLE

Local-global questions for divisibility in commutative algebraic groups

Roberto Dvornicich[1] · **Laura Paladino**[2]

Received: 12 May 2021 / Revised: 4 June 2022 / Accepted: 12 June 2022 /
Published online: 7 September 2022

Abstract

This is a survey focusing on the Hasse principle for divisibility of points in commutative algebraic groups and its relation with the Hasse principle for divisibility of elements of the Tate–Shavarevich group in the Weil–Châtelet group. The two local-global subjects arose as a generalization of some classical questions considered respectively by Hasse and Cassels. We describe the deep connection between the two problems and give an overview of the long-established results and the ones achieved during the last twenty years, when the questions were taken up again in a more general setting. In particular, by connecting various results about the two problems, we describe how some recent developments in the first of the two local-global questions imply an answer to Cassels' question, which improves all the results published before about that problem. This answer is best possible over $\mathbb{Q}$. We also describe some links with other similar questions, for example the Support Problem and the local-global principle for existence of isogenies of prime degree in elliptic curves.

Keywords Hasse principle · Local-global divisibility problem · Elliptic curves · Tate–Shafarevich group

Mathematics Subject Classification 11G05 · 11G07 · 11G10 · 11E72

✉ Laura Paladino
laura.paladino@unical.it

Roberto Dvornicich
roberto.dvornicich@unipi.it

[1] Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo 5, 56126 Pisa, Italy

[2] Dipartimento di Matematica e Informatica, Università della Calabria, Ponte Pietro Bucci, Cubo 30B, 87036 Arcavacata di Rende (CS), Italy

1 Introduction

In 1923–1924 Hasse generalized to all number fields a result shown by Minkowski over $\mathbb{Q}$.

Hasse–Minkowski Theorem *Let k be a number field and let $F(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ be a quadratic form. If F represents 0 non-trivially in k_v, for all completions k_v of k, then $F = 0$ has a non-trivial solution in k.*

This theorem is also known as the Hasse principle on quadratic forms. The assumption that F is isotropic in k_v *for all but finitely many completions* (implying the same conclusion) gives a stronger form of the principle. Since then, many mathematicians have been concerned with similar so-called local-global problems, i.e. they have been questioning if, given a global field k, the validity of some properties for all but finitely many local fields k_v could ensure the validity of the same properties for k (see among others [13, 25, 31, 50, 54, 58, 82, 83]). When the answer to such a problem is affirmative, one says that there is a local-global principle or a Hasse principle. Along with the classical Hasse principle on quadratic forms, one of the most famous local-global principles is the Albert–Brauer–Hasse–Noether Theorem on central simple algebras, often referred to as the Brauer–Hasse–Noether Theorem (see for instance [86]).

Theorem 1.1 (Albert, Hasse, Brauer, Noether, 1932) *Let k be a number field and let $\mathfrak{A}$ be a central simple algebra over k. Then $\mathfrak{A}$ splits over k if and only if $\mathfrak{A}$ splits over k_v, for all places v of k.*

Brauer proved that the tensor product equips the set of equivalence classes of central simple algebras over k with the structure of an abelian group, which is called the Brauer group of k and is denoted by $\mathrm{Br}(k)$ (see the recent monograph [30] written by Colliot-Thélène and Skorobogatov). The cohomological description of $\mathrm{Br}(k)$ is $H^2(k, \bar{k}^*)$, where $\bar{k}$ is the separable closure of k, and can be extended in the case of a variety X defined over k, giving rise to the Brauer–Grothendieck group $\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_{m,X})$ (see [30, 91] for further details). In [64], Manin showed that in many cases the failure of the Hasse principle of the existence of k-rational points on X can be explained by a reciprocity law imposed by $\mathrm{Br}(X)$ on the set of adelic points on X. For further details see [37], in which Creutz shows that the Brauer–Manin obstruction explains all failures of the Hasse principle of existence of k-rational points for torsors under abelian varieties (see also [64, Théorème 6], where a similar statement was proved under the hypothesis of finiteness of the Tate–Shafarevich group, that we will define in the following).

Local-global questions have often an equivalent formulation in terms of principal homogeneous spaces under some group schemes $\mathcal{G}$ over k, that are classified by the first cohomology group $H^1(k, \mathcal{G}) := H^1(\mathrm{Gal}(\bar{k}/k), \mathcal{G}(\bar{k}))$ (see for instance [51, 91]). In these cases, when the hypotheses require that the assertion holds in *all* completions k_v, one can study the behaviour of the Tate–Shafarevich group $Ш(k, \mathcal{G})$ to get information about the validity or the failure of the principle. In fact, this group is the intersection of the kernels of the restriction maps $\mathrm{res}_v : H^1(k, \mathcal{G}) \to H^1(k_v, \mathcal{G})$, as v varies in the set M_k of places of k, and its vanishing ensures a positive answer to the question.

On the other hand, by answering the problem in some cases, one can get information about $Ш(k, \mathcal{G})$. When the hypotheses of a local-global question require its validity in *all but finitely many* completions k_v, the group that interprets the hypotheses of the problem in the cohomological context is not exactly $Ш(k, \mathcal{G})$, but a similar group, i.e., the intersection of the kernels of the maps $H^1(k, \mathcal{G}) \to \prod_{v\in\Sigma} H^1(k_v, \mathcal{G})$, as v varies in a subset Σ of M_k containing all but finitely many places v (see Sect. 3 for further details). The two groups often coincide, but there are some examples in which they differ (see Sects. 4 and 7.1 for further details). In various cases it suffices to study the behaviour of one of them to understand the structure of the other (see Sect. 4).

In this paper we will be concerned with the following local-global problems and their relation.

Problem 1.2 Let k be a number field, M_k the set of the places v of k and $\mathcal{G}$ a commutative and connected algebraic group defined over k. Let $P \in \mathcal{G}(k)$ and let q be a positive integer. Assume that for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{G}(k_v)$ such that $P = qD_v$. Is it possible to conclude that there exists $D \in \mathcal{G}(k)$ such that $P = qD$?

Problem 1.2 was stated by the first author and Zannier in 2001 [43] and it was named the *local-global divisibility problem*. It is the $r = 0$ case of the following problem.

Problem 1.3 Let k be a number field, M_k the set of the places v of k and $\mathcal{G}$ a commutative and connected algebraic group defined over k. Let q be a positive integer, let $\sigma \in H^r(k, \mathcal{G})$ and let $\mathrm{res}_v \colon H^r(k, \mathcal{G}) \to H^r(k_v, \mathcal{G})$ be the restriction map. Assume that for all but finitely many $v \in M_k$ there exists $\tau_v \in H^r(k_v, \mathcal{G})$ such that $q\tau_v = \mathrm{res}_v(\sigma)$. Can we conclude that there exists $\tau \in H^r(k, \mathcal{G})$ such that $q\tau = \sigma$?

In a slightly different form, i.e. with the assumption that the local divisibility holds for all $v \in M_k$, Problem 1.3 was stated in 2016 by Creutz [36]. In fact, when $r = 1$, a similar question was firstly posed by Cassels in 1962 only in the case when $\mathcal{G}$ is an elliptic curve [14].

Cassels' question Let k be a number field and $\mathcal{E}$ an abelian variety of dimension 1 defined over k. 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?

Here infinitely divisible by p means divisible by p^l, for all positive integers l. Thus, if one wonders about the divisibility by every power p^l of p in Problem 1.3, then this problem can be considered as a generalization of Cassels' question to all commutative algebraic groups. Both Problems 1.2 and 1.3 are generally studied in the case when $q = p^l$, with p a prime number and l a positive integer. In fact, an answer for all powers of prime numbers suffices to have an answer for a general integer q, by using the unique factorization in $\mathbb{Z}$ and Bézout's identity.

Since 1972, Cassels' question was considered in abelian varieties and not only in elliptic curves, firstly by Bašmakov [11, 12] and in the last few years by Çiperiani and Stix [26, 27] and by Creutz [35].

In this paper we carefully explain the connection between these problems and between some groups that interpret the hypotheses of Problem 1.2 and respectively

Problem 1.3 in a cohomological context (among them being some Tate–Shafarevich groups). The relation between these groups was sometimes hinted in the literature, but never explained in details. We will also give a comprehensive overview of all the results achieved for those questions, with particular emphasis on the case of elliptic curves. In fact, in this last case there is a recent answer to Problem 1.2 [78, 79] which implies an affirmative answer to the mentioned Cassels' question for every $p > (3^{[k:\mathbb{Q}]/2}+1)^2$ over a number field $k \neq \mathbb{Q}$ and for every $p \geqslant 5$ over $\mathbb{Q}$ (see Theorem 6.5). This answer is best possible over $\mathbb{Q}$. The way of deducing such an answer to Cassels' question (see Sect. 6.1) has not been explicitly described in other papers. The answer itself for $k \neq \mathbb{Q}$ has not been explicitly stated in other papers. When $k = \mathbb{Q}$ it is instead mentioned in [36] as a consequence of [79].

In addition observe that if the point P in the statement of Problem 1.2 is the zero point in the group law of $\mathcal{G}$ and we require that neither D nor D_v, for all but finitely many v, is the zero point itself, then the question can be reformulated as follows: *if $\mathcal{G}$ admits a k_v-rational torsion point of order q, for all but finitely many places $v \in M_k$, can we conclude that $\mathcal{G}$ admits a k-rational torsion point of order q*? Thus, the question is somehow related with some other famous problems about torsion points or reductions of torsion points in abelian varieties, as the *Support Problem* studied by Corrales-Rodrigáñez and Schoof in [32] or the question studied by Katz in [55] about the group of k-rational torsion points of an abelian variety. Owing to the connection between the existence of isogenies of prime degree p and the existence of k-rational p-torsion points, the question is also linked to the local-global problem for the existence of isogenies of prime degree in elliptic curves, studied by Sutherland in [92]. We will describe these and some other related problems and the main results obtained about them in Sect. 6.

The paper is structured as follows. At first we give a historical overview of the formulation of the two problems and their classical solutions. Then we describe a cohomological interpretation for Problem 1.2 and give more details about the link between Problems 1.2, 1.3 and Cassels' question, that is discussed in Sect. 4. Section 5 is dedicated to Problem 1.3 and Cassels' question. In Sects. 6 and 7 we describe the affirmative results achieved for the three problems and respectively the known counterexamples. As mentioned above, in the last part of the paper we illustrate some questions similar or somehow related to the three problems, among them the Support Problem [32], the problem studied by Katz about the existence of a torsion point of a prescribed order [55] and the local-global principle for the existence of isogenies of prime degree [92]. We give a brief overview of the main results achieved for those problems too and explain their connections with Problems 1.2 and 1.3.

2 Classical problems and classical solutions

In the case of a quadratic form $X^2 + rY^2$, where r is a rational number, the Hasse principle is equivalent to the statement "if a rational number is a square in k_v, for all but finitely many v, then it is a square in k". It is natural to ask if such a principle still holds for q-powers of rational numbers, where q is a general positive integer, and not only for rational squares. The answer to such a question was given by the

Grunwald–Wang Theorem (see for example [4, Chapters IX and X]). Here we state the theorem in its classical form, i.e. in the more general case when k is a global field. Through all the paper, for every positive integer q, we denote by ζ_q a primitive q-th root of the unity. Furthermore, for every positive integer s, let $\hat{\zeta}_{2^s}$ be a 2^s-th root of the unity such that $\hat{\zeta}_{2^{s+1}} = \hat{\zeta}_{2^s}$, and let $\eta_s := \hat{\zeta}_{2^s} + (\hat{\zeta}_{2^s})^{-1}$. In particular, for every field k, there exists an integer $s_k \geqslant 2$ such that $\eta_{s_k} \in k$, but $\eta_{s_k+1} \notin k$.

Theorem 2.1 (Grunwald–Wang, 1933–1950) *Let k be a global field, let q be a positive integer and let Σ be a set containing all but finitely many places v of k. Consider the group $P(q, \Sigma) = \{x \in k \mid x \in k_v^q \text{ for all } v \in \Sigma\}$. Then $P(q, \Sigma) = k^q$ except under the following conditions:*

(1) *k is a number field;*
(2) *-1, $2 + \eta_{s_k}$ and $-(2 + \eta_{s_k})$ are non-squares in k;*
(3) *$q = 2^t q'$, where q' is odd and $t > s$;*
(4) *$v \notin \Sigma$, for all $v \mid 2$ where -1, $2 + \eta_{s_k}$ and $-(2 + \eta_{s_k})$ are non-squares in k_v.*

In this special case $P(q, \Sigma) = k^q \cup \eta_{s_k+1}^q k^q$.

In particular, when $k = \mathbb{Q}$, the principle for q-powers of rational numbers could fail only when q is divided by 2^t, with $t \geqslant 3$. The first example violating the principle was shown by Trost in 1934 (see [95]).

Theorem 2.2 (Trost, 1948) *The equation $x^8 = 16$ has a solution in the p-adic field $\mathbb{Q}_p$, for every $p \neq 2$, but it has no solutions in $\mathbb{Q}_2$ and in $\mathbb{Q}$.*

Similar examples can be constructed for all powers 2^t, with $t \geqslant 3$ and, consequently, for all integers $q = 2^t q'$, where q' is odd and $t \geqslant 3$, as in the statement of the theorem. For further details about the formulation of the Grunwald–Wang Theorem, the reader can see the survey [86] by Roquette.

If we denote by $\mathbb{G}_m$ the multiplicative group over k, then the Grunwald–Wang Theorem holds in the commutative group $\mathbb{G}_m$ as well as in k. By questioning if its validity still holds for a general commutative algebraic group $\mathcal{G}$ instead of $\mathbb{G}_m$, we get nothing but Problem 1.2, i.e. the *local-global divisibility problem in commutative algebraic groups*. So in the cases when the answer to Problem 1.2 is affirmative, we have a kind of a generalization of the Hasse principle for squares of k-rational numbers. The answer to the local-global divisibility depends on k as well as on q and this is already shown by the Grunwald–Wang Theorem in the case when $\mathcal{G}$ is $\mathbb{G}_m$.

As stated in the introduction, the more general Problem 1.3 also was motivated by a classical problem, i.e. Cassels' question. This question was formulated in 1962 in the third paper of Cassels' famous series *Arithmetic on curves of genus* 1 (see [17, Problem (b)] and [16, Problem 1.2]; for the whole series of the mentioned Cassels' papers see [14–22]). An affirmative answer to the local-global divisibility only by p for elements in $H^1(k, \mathcal{E})$ was soon given by Cassels and Tate (see [17, Lemma 6.1 and its corollary] and see also [16, Theorem 8.1]). In particular Cassels deduced the validity of the local-global divisibility by p from the following lemma.

Lemma 2.3 (Tate, 1962) *Let k be a number field with algebraic closure $\bar{k}$ and absolute Galois group $G_k := \mathrm{Gal}(\bar{k}/k)$. Let M be a G_k-module that is isomorphic to*

$\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. Then an element of $H^2(G_k, M)$ is trivial if it is everywhere locally trivial.

Here *everywhere locally trivial* means that, for all v, the element vanishes in $H^2(G_{k_v}, M(\overline{k_v}))$, where $\overline{k_v}$ is the algebraic closure of k_v and $G_{k_v} := \mathrm{Gal}(\overline{k_v}/k_v)$. Assume that $\mathcal{G}$ is a smooth commutative algebraic group and that the multiplication-by-q map $[q]$ is étale, then we have the exact sequence

$$0 \longrightarrow \mathcal{G}[q] \longrightarrow \mathcal{G} \xrightarrow{[q]} \mathcal{G} \longrightarrow 0,$$

where $\mathcal{G}[q]$ is the q-torsion subgroup of $\mathcal{G}$, which implies the long-exact sequence of Galois cohomology

$$\begin{aligned}\cdots \longrightarrow \mathcal{G}(k) &\longrightarrow H^1(k, \mathcal{G}[q])\\ &\longrightarrow H^1(k, \mathcal{G}) \xrightarrow{[q]_*} H^1(k, \mathcal{G}) \longrightarrow H^2(k, \mathcal{G}[q]) \longrightarrow \cdots.\end{aligned}$$

In the case of an elliptic curve $\mathcal{E}$, since $\mathcal{E}[p] \simeq \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$, then the local-global divisibility by p holds in $H^1(k, \mathcal{E})$, as a consequence of Tate's lemma. On the contrary, for powers p^l, with $l \geqslant 2$, the problem remained open for decades, even in the case of elliptic curves defined over $\mathbb{Q}$. In this last case, an affirmative answer for all powers $p \geqslant 5$ has been lately proved. We will describe it in Sect. 6.1, as a consequence of some answers given to Problem 1.2.

3 A cohomological interpretation of Problem 1.2

When $\mathcal{G} \neq \mathbb{G}_m$ a useful way to attack Problem 1.2 was shown in [43], in which the authors gave a cohomological interpretation of the problem. For every positive integer q, we denote by $K := k(\mathcal{G}[q])$ the number field generated over k by the coordinates of the points in the q-torsion subgroup $\mathcal{G}[q]$ of $\mathcal{G}$. Since K is the splitting field of the q-division polynomials, then K/k is a Galois extension, whose Galois group we denote by G. Let $P \in \mathcal{G}(k)$ and let $D \in \mathcal{G}(\bar{k})$ be a q-divisor of P, i.e. $P = qD$. Let F be the extension of K generated by the coordinates of D. Two q-divisors of P differ by a q-torsion point of $\mathcal{G}$. Then we have that F/k is a Galois extension (it is the splitting field of the polynomials whose roots are the coordinates of the points $\widetilde{D} \in \mathcal{G}$ satisfying $q\widetilde{D} = P$) and we denote by Γ its Galois group $\mathrm{Gal}(F/k)$ (see also [43]). For every $\sigma \in \Gamma$, we have

$$q\sigma(D) = \sigma(qD) = \sigma(P) = P.$$

Thus the points $\sigma(D)$ and D differ by a point in $\mathcal{G}[q]$ and we can define a cocycle $\{Z_\sigma\}_{\sigma\in\Gamma}$ of Γ with values in $\mathcal{G}[q]$ by

$$Z_\sigma := \sigma(D) - D. \tag{3.1}$$

Proposition 3.1 *The class of the cocycle* $\{Z_\sigma\}_{\sigma\in\Gamma}$ *defined in* (3.1) *vanishes in* $H^1(\Gamma, \mathcal{G}[q])$ *if and only if there exists* $D' \in \mathcal{G}(k)$ *such that* $qD' = P$.

Proof Assume that $\{Z_\sigma\}_{\sigma\in\Gamma}$ vanishes in $H^1(\Gamma, \mathcal{G}[q])$, then there exists $W \in \mathcal{G}[q]$ such that $\sigma(W) - W = Z_\sigma = \sigma(D) - D$, for all $\sigma \in \Gamma$. We have $\sigma(D - W) = D - W$, for all $\sigma \in \Gamma$. Thus $D' := D - W \in \mathcal{G}(k)$, since $qD' = qD - qW = qD = P$. The reverse implication is trivial. □

As mentioned above, the vanishing of some specific first cohomology group often ensures an affirmative answer to this kind of problems. This is quite a standard way of proceeding in local-global questions, so we stated the proof of Proposition 3.1 for the reader's convenience. The goal in [43] was to consider a subgroup of $H^1(G, \mathcal{G}[q])$, whose vanishing still ensures an affirmative answer to Problem 1.2.

Definition 3.2 Let Σ be the subset of M_k containing the valuations v that are unramified in K. For every $v \in \Sigma$, let $G_v := \mathrm{Gal}(K_w/k_v)$, where w is a place of K extending v. We call the *first local cohomology group* (of G with values in $\mathcal{G}[q]$) the following subgroup of $H^1(G, \mathcal{G}[q])$:

$$H^1_{\mathrm{loc}}(G, \mathcal{G}[q]) := \bigcap_{v\in\Sigma} \ker\left(H^1(G, \mathcal{G}[q]) \xrightarrow{\mathrm{res}_v} H^1(G_v, \mathcal{G}[q])\right). \tag{3.2}$$

The first local cohomology group portrays the hypotheses of the problem in the cohomological context. In fact, observe that if there exists a point $D_v \in \mathcal{G}(k_v)$ such that $P = qD_v$, then as in (3.1) we can define a cocycle of G_v with values in $\mathcal{G}[q]$ vanishing in $H^1(G_v, \mathcal{G}[q])$. The elements of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ are represented by cocycles that vanish in $H^1(G_v, \mathcal{G}[q])$, for all $v \in \Sigma$. We can say that the cocycles representing a class in $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ are *locally coboundaries*. The group $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ was firstly defined by Tate, as stated by Serre in [88], where the group was introduced (and denoted by $H^1_*(G, \mathcal{G}[q])$). It is very similar to the Tate–Shafarevich group $Ш(k, \mathcal{G}[q])$ up to isomorphism (see Sect. 4 for further details). Observe that, by the Chebotarev Density Theorem (see [60, 94]), the local Galois group G_v varies over all cyclic subgroups of G as v varies in Σ. Then, for every $\sigma \in G$, there exists $v \in \Sigma$, such that $G_v = \langle\sigma\rangle$. Thus, if $\{Z_\sigma\}_{\sigma\in G} \in H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$, then for every $\sigma \in G$ there exists $W_\sigma \in \mathcal{G}[q]$ such that $Z_\sigma = (\sigma - 1)W_\sigma$. As stated in [43, Definition on p. 321], we have the following equivalent definition of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$.

Definition 3.3 A cocycle $\{Z_\sigma\}_{\sigma\in G} \in H^1(G, \mathcal{G}[q])$ satisfies the *local conditions* if, for every $\sigma \in G$, there exists $W_\sigma \in \mathcal{G}[q]$ such that $Z_\sigma = (\sigma - 1)W_\sigma$. The subgroup of $H^1(G, \mathcal{G}[q])$ formed by all the cocycles satisfying the local conditions is the first local cohomology group $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$.

This second definition shows explicitly the kind of cocycles that one has to check if they are coboundaries or not. Such a description was useful to get a solution to the problem both in cases when the answer is affirmative and in cases when it is negative. In fact, the triviality of the first cohomology group assures an affirmative answer to Problem 1.2.

Theorem 3.4 (Dvornicich, Zannier, 2001) *If $H^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = 0$, then the local-global divisibility by q holds in $\mathcal{G}$ over k.*

On the other hand, in the cases when such a group is nontrivial we have counterexamples over a finite extension of k. In Sect. 7 we state such a converse of Theorem 3.4 over a finite extension L of k (i.e. Theorem 7.1) and describe its proof, which gives an explicit method to find counterexamples over L. In the case of elliptic curves, this method was successfully applied to find counterexamples over k itself. In Sect. 7 we also discuss when one can find a counterexample over k or not.

Remark 3.5 To apply the Chebotarev Density Theorem, it suffices to have a subset of M_k of Dirichlet density 1. So the hypotheses of Problem 1.2 can be reformulated by asking that the local divisibility holds for a set of places v of Dirichlet density 1. Indeed we have

$$H^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = \bigcap_{v \in S} \ker\left(H^1(G, \mathcal{G}[q]) \xrightarrow{\mathrm{res}_v} H^1(G_v, \mathcal{G}[q])\right),$$

where S is a subset of Σ such that G_v varies over all cyclic subgroups of G as v varies in S. If we are able to find such a set S, then we can replace the hypotheses of Problem 1.2 about the validity of the local divisibility for all but finitely many $v \in M_k$ with the assumption of the validity of the local divisibility for every $v \in S$. Notice that in particular S is finite, being G finite (on the contrary Σ is not finite). So it suffices to have that the local divisibility by q holds for a finite number of suitable places to get the global divisibility by q. An explicit set S is produced in [42] for elliptic curves defined over $\mathbb{Q}$.

4 First local-cohomology group and Tate–Shafarevich group

As stated in the previous sections, the definition (3.2) of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ is very similar to the classical definition of the Tate–Shafarevich group $Ш(k, \mathcal{G}[q])$ up to isomorphism. The Tate–Shafarevich group was firstly introduced in the case of an abelian variety, but the definition can be generalized to the case of a commutative algebraic group $\mathcal{G}$. We have already defined

$$Ш(k, \mathcal{G}) := \bigcap_{v \in M_k} \ker\left(H^1(k, \mathcal{G}) \xrightarrow{\mathrm{res}_v} H^1(k_v, \mathcal{G})\right).$$

More generally, for every $r \geqslant 0$, one can define

$$Ш^r(k, \mathcal{G}) := \bigcap_{v \in M_k} \ker\left(H^r(k, \mathcal{G}) \xrightarrow{\mathrm{res}_v} H^r(k_v, \mathcal{G})\right),$$

where $H^r(k, \mathcal{G}) := H^r(G_k, \mathcal{G}(\bar{k}))$ and $H^r(k_v, \mathcal{G}) := H^r(G_{k_v}, \mathcal{G}(\overline{k_v}))$. Clearly, $Ш(k, \mathcal{G}) = Ш^1(k, \mathcal{G})$. If we consider the G_k-module $\mathcal{G}[q]$ instead of $\mathcal{G}$, in the same

way we get

$$Ш(k, \mathcal{G}[q]) := \bigcap_{v \in M_k} \ker\left(H^1(k, \mathcal{G}[q]) \xrightarrow{\text{res}_v} H^1(k_v, \mathcal{G}[q])\right)$$

(and respectively $Ш^r(k, \mathcal{G}[q])$, with $r \geqslant 0$). Let Σ be the subset of M_k containing the valuations that are unramified in K and consider the following modified Tate–Shafarevich group:

$$Ш_\Sigma(k, \mathcal{G}[q]) := \bigcap_{v \in \Sigma} \ker\left(H^1(k, \mathcal{G}[q]) \xrightarrow{\text{res}_v} H^1(k_v, \mathcal{G}[q])\right) \tag{4.1}$$

(see also [87], in which the author considered similar modified Tate–Shafarevich groups, with a slightly different notation; in the notation used in [87] the group in (4.1) would be denoted by $Ш_{M_k \setminus \Sigma}$). Clearly, $Ш(k, \mathcal{G}[q]) \subseteq Ш_\Sigma(k, \mathcal{G}[q])$ and in particular the triviality of $Ш_\Sigma(k, \mathcal{G}[q])$ implies the triviality of $Ш(k, \mathcal{G}[q])$. It is well known that $H^1_{\text{loc}}(G, \mathcal{G}[q])$ is isomorphic to $Ш_\Sigma(k, \mathcal{G}[q])$ and we have the following Proposition 4.1, that is proved for instance in [34, Proof of Lemma 3.3] and [68, Chapter I, Lemma 9.3]. We firstly recall that as a consequence of Chevalley's Theorem on the classification of the commutative algebraic groups in characteristic zero, we have a group isomorphism $\mathcal{G}[q] \simeq (\mathbb{Z}/q\mathbb{Z})^n$, where n is a positive integer depending only on $\mathcal{G}$ (see [89] and [43, Section 2]). In the case when $\mathcal{G}$ is an abelian variety of dimension g, it is well known that $n = 2g$. Therefore we have a representation of G_k in the general linear group $\text{GL}_n(\mathbb{Z}/q\mathbb{Z})$

$$\rho\colon G_k \hookrightarrow \text{GL}_n(\mathbb{Z}/q\mathbb{Z}).$$

The image $\rho(G_k)$ is isomorphic to $G = \text{Gal}(k(\mathcal{G}[q])/k) = \text{Gal}(K/k)$, and we still denote by G such an image. The group G_k acts on $\mathcal{G}[q]$ as G and the q-torsion subgroup $\mathcal{G}[q]$ is a G_k-module as well as a G-module. We have $G \simeq G_k/\ker(\rho)$ and by the inflation map, the group $H^1(G, G[q])$ is isomorphic to a subgroup of $H^1(k, G[q])$. Similarly, the group $H^1(G_v, G[q])$ is isomorphic to a subgroup of $H^1(k_v, G[q])$, for every $v \in \Sigma$. By the injection given by the inflation map, the group $H^1_{\text{loc}}(G, \mathcal{G}[q])$ is isomorphic to a subgroup of $Ш_\Sigma(k, \mathcal{G}[q])$.

Proposition 4.1 *Let Σ be the subset of M_k containing the valuations v that are unramified in K. The groups $H^1_{\text{loc}}(G, \mathcal{G}[q])$ and $Ш_\Sigma(k, \mathcal{G}[q])$ are isomorphic. In particular, if $H^1_{\text{loc}}(G, \mathcal{G}[q]) = 0$, then $Ш(k, \mathcal{G}[q]) = 0$.*

Proof Let Σ_K denote the set of places w of K extending the places $v \in \Sigma$. Consider the following diagram given by inflation-restriction exact sequences:

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1(G, \mathcal{G}[q]) & \xrightarrow{\text{inf}} & H^1(G_k, \mathcal{G}[q]) & \xrightarrow{\text{res}} & H^1(G_K, \mathcal{G}[q]) \\
 & & \downarrow{\scriptstyle \prod \text{res}_v} & & \downarrow{\scriptstyle \prod \text{res}_v} & & \downarrow{\scriptstyle \prod \text{res}_w} \\
0 & \longrightarrow & \prod_{v\in\Sigma} H^1(G_v, \mathcal{G}[q]) & \xrightarrow{\text{inf}} & \prod_{v\in\Sigma} H^1(G_{k_v}, \mathcal{G}[q]) & \xrightarrow{\text{res}} & \prod_{w\in\Sigma_K} H^1(G_{K_w}, \mathcal{G}[q]).
\end{array}$$

The kernel of the vertical map on the left is $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ and the kernel of the central vertical map is $Ш_\Sigma(k, \mathcal{G}[q])$. The vertical map on the right is injective because of G_K acting trivially on $\mathcal{G}[q]$ and by the Chebotarev Density Theorem. Then we have

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1_{\mathrm{loc}}(G, \mathcal{G}[q]) & \xrightarrow{\inf} & Ш_\Sigma(k, \mathcal{G}[q]) & \xrightarrow{\mathrm{res}} & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^1(G, \mathcal{G}[q]) & \xrightarrow{\inf} & H^1(G_k, \mathcal{G}[q]) & \xrightarrow{\mathrm{res}} & H^1(G_K, \mathcal{G}[q]) \\
 & & \downarrow \prod \mathrm{res}_v & & \downarrow \prod \mathrm{res}_v & & \downarrow \prod \mathrm{res}_w \\
0 & \longrightarrow & \prod_{v\in\Sigma} H^1(G_v, \mathcal{G}[q]) & \xrightarrow{\inf} & \prod_{v\in\Sigma} H^1(G_{k_v}, \mathcal{G}[q]) & \xrightarrow{\mathrm{res}} & \prod_{w\in\Sigma_K} H^1(G_{K_w}, \mathcal{G}[q])
\end{array}$$

and $H^1_{\mathrm{loc}}(G, \mathcal{G}[q]) \simeq Ш_\Sigma(k, \mathcal{G}[q])$. In particular, if $H^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = 0$, then $Ш_\Sigma(k, \mathcal{G}[q]) = 0$, implying $Ш(k, \mathcal{G}[q]) = 0$. □

The group $Ш(k, \mathcal{G}[q])$ itself is often isomorphic to $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ and this is in particular the case when $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ is trivial, which surely happens for p sufficiently large [11, 12, 36]. Anyway, in a few cases, the two groups may differ. If the local-global principle fails and there is a point locally divisible for all places but a finite number of them (unramified in K) for which the local divisibility does not hold and this point is not globally divisible as well, then there is a nontrivial class in $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$, whose image in $Ш_\Sigma(k, \mathcal{G}[q])$ does not belong to $Ш(k, \mathcal{G}[q])$ (see Sect. 7.1 for some examples in elliptic curves defined over $\mathbb{Q}$). The most of the results obtained for Problems 1.2 and 1.3 are produced by showing the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ or $Ш(k, \mathcal{G}[q])$ [11, 12, 27, 43, 78, 79], etc.

5 On Problem 1.3 and Cassels' question

In this section we give some more information about Problem 1.3 and Cassels' question. As mentioned above, in the more general case of an abelian variety $\mathcal{A}$, Cassels' question was firstly considered by Bašmakov in [11, 12], since 1972. Anyway, even if he stated the problem for abelian varieties, in his papers he focused especially on elliptic curves. In the recent papers [26, 27], Çiperiani and Stix gave a very detailed analysis of Cassels' questions, both in the case of elliptic curves and in the case of general abelian varieties. Quite at the same time with [26], the question for abelian varieties was also considered in [35], in which Creutz stated the following result (see also [27, Proposition 4.3]).

Theorem 5.1 (Creutz, 2013) *Let $\mathcal{A}$ be an abelian variety defined over a number field k. Let $\mathcal{A}^\vee$ be its dual and $\mathcal{A}[q]^\vee$ the Cartier dual of $\mathcal{A}[q]$, where q is a positive integer. In order to have that $Ш(k, \mathcal{A}) \subseteq qH^1(k, \mathcal{A})$ it is necessary and sufficient that the image of the natural map $Ш(k, \mathcal{A}[q]^\vee) \to Ш(k, \mathcal{A}^\vee)$ is contained in the maximal divisible subgroup of $Ш(k, \mathcal{A}^\vee)$.*

The maximal divisible subgroup $\mathrm{div}(H^1(k,\mathcal{A}^\vee))$ of $Ш(k,\mathcal{A}^\vee)$ is the right kernel of the pairing

$$Ш(k,\mathcal{A}) \times Ш(k,\mathcal{A}^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z},$$

known as Cassels–Tate pairing, since it was defined by Tate in [93] as a generalization of Cassels' pairing on the Tate–Shafarevich group of an elliptic curve (see also [35]). More generally there is the following Cassels–Tate pairing:

$$Ш^i(k,\mathcal{A}) \times Ш^{2-i}(k,\mathcal{A}^\vee) \to \mathbb{Q}/\mathbb{Z},$$

whose left and right kernels are the maximal divisible groups of $Ш^i(k,\mathcal{A})$ and respectively $Ш^{2-i}(k,\mathcal{A}^\vee)$, for $0 \leqslant i \leqslant 2$ [69, Theorem 8.6.7], [27]. Observe that if $Ш(k,\mathcal{A}^\vee[q])$ is trivial, then the image of the map $Ш(k,\mathcal{A}[q]^\vee) \to Ш(k,\mathcal{A}^\vee)$ is contained in $\mathrm{div}(H^1(k,\mathcal{A}^\vee))$. On the contrary, the nontriviality of $Ш(k,\mathcal{A}^\vee[q])$ does not assure in general that $Ш(k,\mathcal{A}) \not\subseteq qH^1(k,\mathcal{A})$. The proof of Theorem 5.1, is based on the Cassels–Tate pairing. Consider again the exact sequence

$$0 \longrightarrow \mathcal{A}[q] \longrightarrow \mathcal{A} \xrightarrow{[q]} \mathcal{A} \longrightarrow 0,$$

which implies the long-exact sequence of cohomology

$$\cdots \to H^r(k,\mathcal{A}[q]) \to H^r(k,\mathcal{A}) \xrightarrow{[q]_*} H^r(k,\mathcal{A}) \xrightarrow{\delta_r} H^{r+1}(k,\mathcal{A}[q]) \to \cdots \tag{5.1}$$

An element $\sigma \in H^r(k,\mathcal{A})$ is locally divisible by q if and only if its image under δ_r is in $Ш^{r+1}(k,\mathcal{A}[q])$ and it is globally divisible by q if and only if $\delta_r(\sigma) = 0$. Therefore, if $Ш^{r+1}(k,\mathcal{A}[q]) = 0$, then the local-global divisibility by q holds in $H^r(k,\mathcal{A})$. It is known that $Ш^{r+1}(k,\mathcal{A}[q]) = 0$, for all $r \geqslant 2$ [93, Theorem 3.1]. Then Theorem 5.1 implies the following statement too [36].

Theorem 5.2 (Creutz, 2016) *Assume any of the following:*

(1) $r = 0$ *and* $Ш(k,\mathcal{A}[q]) = 0$*;*
(2) $r = 1$ *and* $Ш(k,\mathcal{A}[q]^\vee) = 0$*;*
(3) $r \geqslant 2$.

Then the local-global divisibility by q holds in $H^r(k,\mathcal{A})$.

Theorem 5.2 has an extension to the case when k has positive characteristic, that was implemented by Creutz and Voloch in [38]. The triviality of $Ш(k,\mathcal{A}[p^l])$, for every $l \geqslant 1$, implies an affirmative answer in $\mathcal{A}^\vee$ over k to Cassels' question for p and to Problem 1.3 for every power of p. When $\mathcal{A}$ is a principally polarized abelian variety, then $\mathcal{A} \simeq \mathcal{A}^\vee$. In this last case, the triviality of $Ш(k,\mathcal{A}[p^l])$, for every l, is a sufficient condition to have an affirmative answer to Cassels' question for p in $\mathcal{A}$.

Corollary 5.3 *Let $\mathcal{A}$ be a principally polarized abelian variety defined over a number field k. If $Ш(k,\mathcal{A}[p^l]) = 0$, for some prime number p and some positive integer l, then the local-global divisibility by p^l holds in $H^r(k,\mathcal{A})$, for every $r \geqslant 0$.*

In addition, Creutz proved that if $\mathcal{A}$ is principally polarized and $Ш(k, \mathcal{A})$ is finite, then the condition $Ш(k, \mathcal{A}[p^l]) \neq 0$ implies that for some $r \geqslant 0$ the local-global divisibility by p^l fails in $H^r(k, \mathcal{A})$ [36, Proposition 2.2.].

In [27], Çiperiani and Stix gave some sufficient conditions to have $Ш(k, \mathcal{A}[p^l]) = 0$, for every $l \geqslant 0$.

Theorem 5.4 (Çiperiani, Stix, 2015) *Let $\mathcal{A}$ be an abelian variety defined over a number field k and let p be a prime number. If*

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

then

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

To prove these results and the other ones in their mentioned papers [26, 27], the authors use Galois representations, characters of representations, Poitou–Tate duality and especially sequences in cohomology and maps between cohomology groups, that allow them to deduce the triviality of $Ш(k, \mathcal{A}[p^l])$. The vanishing of this group also assures an affirmative answer to Problem 1.2 by part (1) of Theorem 5.2 (recall that Problem 1.2 is the $r = 0$ case of Problem 1.3 as mentioned in Sect. 1). By investigating certain exact sequences [27, (4.4) and (2.1)] involving the group $Ш(k, \mathcal{A}[p^l])$ and the group $Ш(k, \mathcal{A})[p^l]$, i.e. the p^l-torsion part of the group $Ш(k, \mathcal{A})$, Çiperiani and Stix also get the same conclusion by showing that Theorem 5.4 implies the following equality, for all l:

$$\left\{P \in \mathcal{A}(k) \mid P \in p^l A(k_v) \text{ for all } v \in M_k\right\} = p^l \mathcal{A}(k).$$

Thus Theorem 5.4 gives sufficient conditions to have an affirmative answer to Problem 1.2 in abelian varieties. In view of Theorem 5.2, if $\mathcal{A}$ is a principally polarized abelian variety, then Theorem 5.4 gives sufficient conditions to have an affirmative answer to Cassels' question for p, to Problem 1.3 for every power of p and to Problem 1.2 for every power of p. Till now, Cassels' question has not been investigated in a general commutative algebraic group $\mathcal{G}$.

6 Known affirmative results about the local-global divisibility problem and Cassels' question

We are going to give an overview of all the results achieved for Problem 1.2, Cassels' question and Problem 1.3 since their formulations. We will also describe in which cases some affirmative results to Problem 1.2 implied affirmative results to Cassels' question and to Problem 1.3, thanks to the connection between the three problems, that we explained in the previous sections.

6.1 Local-global divisibility in elliptic curves

In the case when $\mathcal{G}$ is an elliptic curve $\mathcal{E}$, the local-global divisibility of points has been widely studied during the last fifteen years. Having explicit equations satisfied by torsion points of such commutative algebraic groups was useful to describe the extension K/k and the group $H^1_{\text{loc}}(G, \mathcal{E}[q])$ in various examples. By Tate's Lemma 2.3 and the exact sequence (5.1) (for $r = 1$), the local-global divisibility by p holds in elliptic curves defined over number fields. This result was reproved in [43, 98]. In [98], Wong studied a problem similar to Problem 1.2, that we will state in Sect. 8 (see Problem 8.8).

Regarding the local-global divisibility by powers p^l, with $l \geqslant 2$, we summarize the results of the main statements of [78, 79] in the next theorem.

Theorem 6.1 (Paladino, Ranieri, Viada, 2012–2014) *Let p be a prime number, ζ_p a primitive p-th root of the unity and $\overline{\zeta_p}$ its complex conjugate. Let $\mathcal{E}$ be an elliptic curve defined over a number field k that does not contain the field $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. Suppose that at least one of the following conditions holds:*

(1) *$\mathcal{E}$ has no k-rational torsion points of exact order p;*
(2) *$k(\mathcal{E}[p]) \neq k(\zeta_p)$;*
(3) *there does not exist any cyclic k-isogeny of degree p^3 between two elliptic curves defined over k that are k-isogenous to $\mathcal{E}$.*

Then, the local-global principle for divisibility of points by p^l holds in $\mathcal{E}$ over k, for all positive integers l.

The hypothesis that k does not contain the field $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ is necessary, for all the conditions (1), (2), (3) in Theorem 6.1, as shown by an example produced in [79, Section 6]. The proof is based on showing the triviality of the first local cohomology group by the use of Galois representations. Observe that when $k = \mathbb{Q}$, in view of Mazur's Theorem on the possible subgroups $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ of rational torsion points of elliptic curves [65], condition (1) implies that the local-global divisibility by p^l, with $l \geqslant 1$ holds for $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geqslant 11$. Furthermore, Merel and Stein [67] and Rebolledo [85] proved that if $\mathbb{Q}(\mathcal{E}[p]) \neq \mathbb{Q}(\zeta_p)$ then $p \in \{2, 3, 5\}$ or $p > 1000$. Therefore condition (2) implies that the local-global divisibility by p^l, with $l \geqslant 1$, holds for $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geqslant 7$. Finally, in [56], Kenku proved that there does not exist any rational isogeny of degree 5^3 in elliptic curves over $\mathbb{Q}$, by showing that the modular curve $Y_0(125)$ has no rational points. Then Theorem 6.1 implies that the local-global divisibility by p^l, with $l \geqslant 1$, holds in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geqslant 5$.

Corollary 6.2 (Paladino, Ranieri, Viada, 2012–2014) *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $p \geqslant 5$. Then the local-global divisibility by p^l, with $l \geqslant 1$, holds in $\mathcal{E}$ over $\mathbb{Q}$.*

This result is best possible, since for powers p^l, with $p \in \{2, 3\}$ and $l \geqslant 2$, there are counterexamples, as we will see in Sect. 7.1. A second proof of Corollary 6.2 for $p \geqslant 11$ was given in [27] and a third one for $p \geqslant 5$ was given in [62, Theorem 24]. In this last paper Lawson and Wuthrich list all cases when $H^1(G, \mathcal{E}[p^l]) \neq 0$ and from

them they deduce Corollary 6.2. Some of their techniques of proof are similar to the ones in [78, 79], namely the use of the existence of an isogeny of prime degree and Galois representations. But they also use some exact sequences in cohomology, that allow them to shorten the proofs.

For a general k, condition (1) in Theorem 6.1 is also very interesting in view of Merel's Theorem on torsion points of elliptic curves. Here we recall its statement [66].

Theorem 6.3 (Merel, 1994) *For every positive integer d, there exists a constant $B(d) \geqslant 0$ such that for all elliptic curves $\mathcal{E}$ over a number field k, with $[k:\mathbb{Q}] = d$, we have*

$$|\mathcal{E}_{\text{tors}}(k)| \leqslant B(d).$$

In his very cited but unpublished paper [72], Oesterlé showed that Merel's constant $B([k:\mathbb{Q}])$ can be taken as $(3^{[k:\mathbb{Q}]/2}+1)^2$. Thus Theorem 6.1, combined with Theorem 6.3, implies the next statement.

Corollary 6.4 (Paladino, Ranieri, Viada, 2012–2014) *Let $\mathcal{E}$ be an elliptic curve defined over a number field k. Then there exists a number $B(d)$, depending only on the degree $d = [k:\mathbb{Q}]$ of k over $\mathbb{Q}$, such that the local-global principle for divisibility of points by p^l in $\mathcal{E}$ over k holds for every prime number $p > B(d)$ and every $l \geqslant 1$. In addition $B(d) \leqslant (3^{d/2}+1)^2$.*

Observe that the statement of Corollary 6.4 holds for all k and not only for number fields that do not contain $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. In fact the number $B(d)$ can be chosen as $\max\{p_0, (3^{d/2}+1)^2\}$, where p_0 is the largest prime such that k contains the field $\mathbb{Q}(\zeta_{p_0} + \overline{\zeta_{p_0}})$. Since $p_0 \leqslant 2[k:\mathbb{Q}]+1$, then $B([k:\mathbb{Q}]) \leqslant (3^{[k:\mathbb{Q}]/2}+1)^2$.

Gillibert and Ranieri considered the restriction of Problem 1.2 to torsion points of elliptic curves over number fields and showed that in this case the answer is affirmative for all powers of every $p \geqslant 3$ [46]. Their result is best possible, since for powers of 2 the local-global principle fails even in this case.

In the case of global fields of positive characteristic, the problem was treated by Creutz and Voloch in the mentioned [38]. In particular they showed some counterexamples to Problem 1.2 in elliptic curves and also some counterexamples to Cassels' question. An analogue of Problem 1.2 for Drinfeld modules and respectively Carlitz modules was studied in [52, 70]. In [52], van der Heiden considered the problem for Drinfeld modules of rank 1 and rank 2 over function fields. The answer is affirmative in many cases, but there are counterexamples too (see in particular [52, Theorem 18]). In [70], Dong Quan Ngoc Nguyen studied a generalization of such a problem for Carlitz modules over function fields and generalizes van der Heiden's results by giving some sufficient conditions to have an affirmative answer.

Regarding Cassels' question, as showed in Proposition 4.1, the triviality of $H^1_{\text{loc}}(G, \mathcal{E}[q])$ implies the triviality of $Ш(k, \mathcal{E}[q])$. For elliptic curves we have $\mathcal{E}[q] \simeq \mathcal{E}[q]^\vee$ and consequently $Ш(k, \mathcal{E}[q]) \simeq Ш(k, \mathcal{E}[q]^\vee)$. Then, in view of Theorem 5.1, Corollary 6.1 (see also Corollary 6.2) assures an affirmative answer to Cassels' question over $\mathbb{Q}$ for all prime numbers $p \geqslant 5$. We have also an affirmative answer to Problem 1.3, for all $r \geqslant 0$, for every $q = p^l$, with $p \geqslant 5$ and $l \geqslant 1$.

Furthermore, for a general number field k, Theorem 6.1, combined with Corollary 6.4, imply an affirmative answer to Cassels' question (respectively to Problem 1.3, for all r) in elliptic curves over k, for every $p > (3^{[k:\mathbb{Q}]/2}+1)^2$ (resp. for all powers p^l of every $p > (3^{[k:\mathbb{Q}]/2}+1)^2$). A description of how to reach these conclusions by combining the cited theorems does not appear in the literature before. The conclusions themselves for $k \neq \mathbb{Q}$ do not appear in the literature too (the case when $k = \mathbb{Q}$ is mentioned in [36] as a consequence of [79]). Here we explicitly resume all these conclusions for Cassels' question in the next theorem.

Theorem 6.5 *Let $\mathcal{E}$ be an elliptic curve defined over a number field k. Then Cassels' question has an affirmative answer for all $p > (3^{[k:\mathbb{Q}]/2}+1)^2$ in $\mathcal{E}$ over k. In addition, when $k = \mathbb{Q}$, Cassels' question has an affirmative answer for all $p \geqslant 5$.*

In [27], the authors proved a similar result.

Theorem 6.6 (Çiperiani, Stix, 2015) *Let $\mathcal{E}$ be an elliptic curve defined over a number field k. Let $B(d)$ be the constant in Theorem 6.3, where $d = [k:\mathbb{Q}]$. Then Cassels' question has an affirmative answer in the following two cases:*

(1) $p > \max\{B(d), (2^d + 2^{d/2})^2\}$;
(2) $p \geqslant 3$, $[k(\zeta_p):k] \neq 2$ *and* $\mathcal{E}[p]$ *is an irreducible* G_k*-representation.*

The bound $p > (3^{[k:\mathbb{Q}]/2}+1)^2$ in Theorem 6.5 is better than the bound $p > (2^{[k:\mathbb{Q}]} + 2^{[k:\mathbb{Q}]/2})^2$ in Theorem 6.6. In fact, we have already observed that $B(d)$ can be taken $\leqslant (3^{d/2}+1)^2$. Then $\max\{B(d), (2^d+2^{d/2})^2\} = (2^d+2^{d/2})^2$. Both Theorem 6.1 and Theorem 6.6 give a criterion to establish the validity of Cassels' question for p in $\mathcal{E}$ over k. Observe that if $k \neq k(\zeta_p)$, then the condition $[k(\zeta_p):k] \neq 2$ implies $\mathbb{Q}(\zeta_p + \overline{\zeta_p}) \nsubseteq k$ in the second part of Theorem 6.6. Moreover the irreducibility of $\mathcal{E}[p]$ as a G_k-module implies that $\mathcal{E}$ has no k-rational p-torsion points, as required in Theorem 6.1. We do not know if the bound $p > (3^{[k:\mathbb{Q}]/2}+1)^2$ is sharp, when $k \neq \mathbb{Q}$. When $k = \mathbb{Q}$, such a bound is not sharp, since Cassels' question has an affirmative answer for all $p \geqslant 5$; so we may expect that it can be improved for other number fields too. The bound $p \geqslant 5$ is sharp. In fact, when $k = \mathbb{Q}$, there are counterexamples to Cassels' question (resp. Problem 1.3), for $p \in \{2, 3\}$ (respectively for powers p^l, with $p \in \{2, 3\}$ and $l \geqslant 2$), see Sect. 7.1.1 for further details. When $k = \mathbb{Q}$, in [27] the authors give another proof of Theorem 6.5 for $p \geqslant 11$.

6.2 Local-global divisibility in algebraic tori

The study of Problem 1.2 in algebraic tori began in [43]. Illengo gave a more complete description in [53], by proving the following statement.

Theorem 6.7 (Illengo, 2008) *Let $\mathcal{T}$ be an algebraic torus, defined over k, of dimension*

$$n < 3(p-1).$$

Then the local-global divisibility by p holds in $\mathcal{T}$ over k.

Illengo also showed that his bound is best possible, since for all $n \geqslant 3(p-1)$ there are counterexamples (see Sect. 7.2 below). For powers of p the question is open. Cassels' question is also open in algebraic tori, as well as Problem 1.3 for $r \geqslant 1$.

6.3 Local-global divisibility in abelian varieties

When $\mathcal{G}$ is an abelian variety $\mathcal{A}$, we have some more information about Problem 1.2, provided by Gillibert and Ranieri in [47].

Theorem 6.8 (Gillibert, Ranieri, 2017) *Let $\mathcal{A}$ be an abelian variety defined over a number field k and let p be a prime. Suppose that there exists an element $\sigma \in \mathrm{Gal}(k(\mathcal{A}[p])/k)$, with order dividing $p-1$ and not fixing any nontrivial element of $\mathcal{A}[p]$. Moreover suppose that $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p]) = 0$. Then the local-global divisibility by p^l holds in $\mathcal{A}$ over k and $Ш(k, \mathcal{A}[p^l]) = 0$, for every $l \geqslant 1$.*

The same authors studied the local-global divisibility especially in the case of abelian varieties of GL_2-type [46, 48].

Along with Theorem 5.1, one of the main results about Cassels' question in abelian varieties is the mentioned Theorem 5.4, proved by Çiperiani and Stix (see also [26]).

Observe that both the conclusion of Theorem 5.4 and the conclusion of Theorem 6.8 hold under the assumption that $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p])$ is trivial. As discussed above, the vanishing of this group implies the validity of the local-global divisibility by p in $\mathcal{A}$ over k and in $H^1(k, \mathcal{A})$. Therefore the case of the divisibility by p is not covered either by Theorem 5.4 or by Theorem 6.8. In [47, Theorem 1.3], Gillibert and Ranieri gave sufficient conditions to have an affirmative answer to Problem 1.2 in principally polarized abelian varieties, without assuming $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p]) = 0$. Anyway the question for the divisibility by p remained open in abelian varieties that are not principally polarized, as well as in a general commutative algebraic group.

6.4 Some remarks about the local-global divisibility of points in other commutative algebraic groups

We have seen that the local-global divisibility by p holds when $\mathcal{G}$ is a torus isomorphic to $\mathbb{G}_m$ and when $\mathcal{G}$ is an elliptic curve. This is not true in general for a commutative algebraic group $\mathcal{G}$, as shown by some counterexamples that we will describe in the next section and as underlined in [43, Remark 3.6]. In particular they show that for abelian varieties of dimension higher than 1 and for algebraic tori of dimension higher than 1, it is not true in general that the local-global divisibility by a prime p holds. Furthermore, we have just observed at the end of the previous section, that Theorems 5.4 and 6.8 do not give information about the local-global divisibility by p in abelian varieties that are not principally polarized. A result in [77] gives conditions on $\mathcal{G}[p]$ ensuring the validity of the local-global divisibility by p, for a general commutative algebraic group $\mathcal{G}$. It underlines that the reducibility of $\mathcal{G}[p]$ as a G_k-module or as an H-module, for any subnormal subgroup H of G_k is the greatest obstruction to the local-global divisibility by p. In particular every class of Galois groups $\mathrm{Gal}(k(\mathcal{G}[p])/k)$ for which the local-global divisibility by p may fail in $\mathcal{G}$ is shown in that paper.

7 Counterexamples

The triviality of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ is not exactly a necessary condition for the local-global divisibility by q in $\mathcal{G}$ over k. In fact, the existence of a cocycle of G with values in $\mathcal{G}[q]$ that satisfies the local conditions and it is not a coboundary ensures the existence of a counterexample over a *finite extension* of k. Here is the precise statement, proved in [45].

Theorem 7.1 (Dvornicich, Zannier, 2007) *Let q be a positive integer and let $K = k(\mathcal{G}[q])$ be the q-division field of a connected commutative algebraic group $\mathcal{G}$ defined over a number field k. Let $\{Z_\sigma\}_{\sigma\in G}$ be a cocycle with values in $\mathcal{G}[q]$ representing a nontrivial element in $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$. Then there exist a number field L such that $L \cap K = k$ and a point $P \in \mathcal{G}(L)$ which is divisible by q in $\mathcal{G}(L_v)$ for all places v of L, but not divisible by q in $\mathcal{G}(L)$.*

Therefore, the nontriviality of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ is an obstruction to the validity of the principle in finite extensions of k.

A method to obtain explicit counterexamples from a nontrivial class in $\{Z_\sigma\}_{\sigma\in G} \in H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ is given by considering the equality (3.1) with $D \in \mathcal{G}(\bar{k})$ (and $\{Z_\sigma\}_{\sigma\in G}$ such a nontrivial element in $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$). When we know explicit equations for the group law of $\mathcal{G}$, as for instance in the case of elliptic curves, we get an explicit system of equations in the coordinates of D, as variables. When $\mathcal{G}$ is an elliptic curve, we have a system of two equations in two variables. In the proof of Theorem 7.1 in [45], the authors show that, as σ varies in G, that system defines an algebraic variety $\mathcal{B}$ that is isomorphic to $\mathcal{G}$ over K. Furthermore, they show that every k-rational point of $\mathcal{B}$ corresponds to a point $D \in \mathcal{G}(K)$, such that $P = qD$ is a k-rational point of $\mathcal{G}$ violating the Hasse principle for divisibility by q. This construction clarifies why in certain cases the non-vanishing of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ is not a necessary condition; it depends on the existence of a k-rational point on the variety $\mathcal{B}$. In the case when $\mathcal{B}$ has no k-rational points, we are not able to find a counterexample over k. However an L-rational point of $\mathcal{B}$, where L is a finite extension of k linearly disjoint from K over k, corresponds to a point $D \in \mathcal{G}(LK)$ such that $P = qD$ is an L-rational point of $\mathcal{G}$ violating the Hasse principle for divisibility by q. Theorem 7.1 ensures the existence of an L-rational point in $\mathcal{B}$ and consequently assures the existence of a counterexample to Problem 1.2 in a finite extension of k linearly disjoint from K (in some cases we also have that L is k itself, as stated above).

Once we have a counterexample for p^l, a method to find counterexamples to the local-global divisibility by p^{l+s}, for every $s \geqslant 0$, is shown by the second author in [75]. It is based on producing maps between $H^1_{\mathrm{loc}}(G, \mathcal{G}[p^l])$ and $H^1_{\mathrm{loc}}(\mathrm{Gal}\,(k(\mathcal{G}[p^{l+s}]/k), \mathcal{G}[p^{l+s}])$ that are injective under certain conditions. This method has been applied to produce explicit counterexamples for 2^l and 3^l, with $l \geqslant 2$, respectively over $\mathbb{Q}$ and over $\mathbb{Q}(\zeta_3)$ (see Sect. 7.1 for further details). It works both to prove the existence of counterexamples and to find explicitly some of them.

Remark 7.2 The most interesting case for counterexample is when $k = \mathbb{Q}$, since a counterexample over $\mathbb{Q}$ gives also a counterexample over all but finitely many number fields k. In fact, assume that P is a point giving a counterexample to the local-global

divisibility by q in $\mathcal{G}$ over $\mathbb{Q}$ and let D be a q-divisor of P, i.e. $P = qD$. Let $\mathbb{Q}(\mathcal{G}[q])(D)$ be the extension of $\mathbb{Q}$ obtained by adding to $\mathbb{Q}(\mathcal{G}[q])$ the coordinates of D. As stated in Sect. 3, since two different q-divisors of the same point differ by a q-torsion point in $\mathcal{G}$, then $\mathbb{Q}(\mathcal{G}[q])(D)/\mathbb{Q}$ is a Galois extension. If k is a number field linearly disjoint from $\mathbb{Q}(\mathcal{G}[q])(D)/\mathbb{Q}$ over $\mathbb{Q}$, then P is locally divisible by q in all but finitely many completions k_v, with $v \in M_k$ (because it is locally divisible by q in all but finitely many p-adic fields $\mathbb{Q}_p$), but it is not divisible by q in k (since the coordinates of the q-divisors of P lie in $\mathbb{Q}(\mathcal{G}[q])(D)/\mathbb{Q}$).

Concerning the link between counterexamples to Problem 1.2 and counterexamples to Problem 1.3 and Cassels' question, observe that, by Theorem 5.1, if we have counterexamples to Cassels' question in an abelian variety $\mathcal{A}$, then the image of the map $Ш(k, \mathcal{A}[q]^\vee) \to Ш(k, \mathcal{A}^\vee)$ is not contained in the maximal divisible subgroup $\mathrm{div}(H^1(k, \mathcal{A}^\vee))$ of $Ш(k, \mathcal{A}^\vee)$. In particular $Ш(k, \mathcal{A}[q]^\vee)$ is nontrivial, implying $H^1_{\mathrm{loc}}(G, \mathcal{A}[q]^\vee) \neq 0$ too. Therefore a counterexample to Cassels' question in $\mathcal{A}$ gives a counterexample to the local-global divisibility in $\mathcal{A}^\vee$, but the converse is not true. In fact, the Tate–Shafarevich group $Ш(k, \mathcal{A}^\vee)$ could vanish even if the first cohomology group $H^1_{\mathrm{loc}}(G, \mathcal{A}[q]^\vee)$ does not vanish and, in any case, even the nontriviality of $Ш(k, \mathcal{A}[q]^\vee)$ does not imply that the image of the map $Ш(k, \mathcal{A}[q]^\vee) \to Ш(k, \mathcal{A}^\vee)$ is not contained in $\mathrm{div}(H^1(k, \mathcal{A}^\vee))$. If $\mathcal{A}$ is principally polarized (that in particular happens when $\mathcal{A}$ is an elliptic curve), we also have that a counterexample to Cassels' question in $\mathcal{A}$ gives a counterexample to the local-global divisibility in $\mathcal{A}$, but the converse it is not true in general.

7.1 Counterexamples about Problem 1.2 and Cassels' question in elliptic curves

The first paper dedicated exclusively to the counterexamples to the local-global divisibility of points of elliptic curves is [44]. The authors produced explicit counterexamples to the local-global divisibility by 4 in some elliptic curves over $\mathbb{Q}$. They use equation (3.1) and the method explained above. One of the counterexamples is given by the curve $y^2 = (x + 15)(x - 5)(x - 10)$, with its rational point $P = (1561/12^2, 19459/12^3)$, that is locally divisible by 4 in $\mathbb{Q}_p$, for all $p \neq 2$, but it is not divisible by 4 in $\mathbb{Q}$ and in $\mathbb{Q}_2$. This is one of the cases when $H^1_{\mathrm{loc}}(G, \mathcal{E}[4])$ and $Ш(k, \mathcal{E}[4])$ are different, since the point P comes out from a notrivial class $\{Z_\sigma\}_{\sigma \in G}$ in $H^1_{\mathrm{loc}}(G, \mathcal{E}[4])$, which does not belong to $Ш(k, \mathcal{E}[4])$, being P not divisible by 4 in $\mathbb{Q}_2$. In [44] the authors also show that the point

$$P = (5086347841/1848^2, -35496193060511/1848^3)$$

of the curve $y^2 = (x + 2795)(x - 1365)(x - 1430)$ is locally divisible by 4 in all $\mathbb{Q}_p$, but it is not globally divisible by 4 in $\mathbb{Q}$. Similar counterexamples appear in [36, 73]. As mentioned above, in [75] it was shown that the first cited counterexample to the divisibility by 4, given by $P = (1561/12^2, 19459/12^3)$ in $y^2 = (x+15)(x-5)(x-10)$, can be raised to counterexamples to the local-global divisibility by 2^l, for all $l \geqslant 2$. In particular, the point $2^{l-2}P$ gives a counterexample to the local-global divisibility by 2^l.

Even when the question about the local-global divisibility is restricted only to the torsion points of an elliptic curve, for $p = 2$ there are still counterexamples, as shown by Gillibert and Ranieri in [46].

The first counterexamples to the local-global divisibility by 3^l, for some $l \geqslant 2$, were produced in [74]. They are counterexamples to the local-global divisibility by 3^2, but the points giving the counterexamples have rational abscissas only, whereas the ordinates are not rational and are defined over $\mathbb{Q}(\zeta_3)$. Those counterexamples to the local-global divisibility by 3^2 imply counterexamples to the local-global divisibility by 3^l, for all $l \geqslant 2$, in elliptic curves over $\mathbb{Q}(\zeta_3)$ [75]. In 2016, Creutz produced the first counterexamples to the local-global divisibility by 3^l, for all $l \geqslant 2$, in elliptic curves over $\mathbb{Q}$ [36]. Those examples are given by the elliptic curve $\mathcal{E} : x^3 + y^3 + 30z^3 = 0$ defined over $\mathbb{Q}$ (with distinguished point $P_0 = (1 : -1 : 0)$) and the rational point $P = (1523698559 : -2736572309 : 826803945)$. For every $l \geqslant 2$, the point $3^{l-1}P$ is locally divisible by 3^l in all p-adic fields $\mathbb{Q}_p$ but it is not divisible by 3^l in $\mathbb{Q}$. The techniques used to find those counterexamples are different from the one illustrated above. Creutz considered a 3-covering C of $\mathcal{E}$ over $\mathbb{Q}$. The 3-coverings of $\mathcal{E}$ over $\mathbb{Q}$ are parametrized up to isomorphism by $H^1(\mathbb{Q}, \mathcal{E}[3])$ [33, Proposition 1.14]. He took into account the exact sequence

$$\cdots \to \mathcal{E}(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, \mathcal{E}[3]) \to H^1(\mathbb{Q}, \mathcal{E}) \to \ldots$$

and the class $\xi \in H^1(\mathbb{Q}, \mathcal{E}[3])$ associated to C. The images $\mathrm{res}_v(\xi)$ are in $\delta(\mathcal{E}(\mathbb{Q}_p)[3])$, for every p. On the other hand he took a rational point on C and calculated its image in $\mathcal{E}$, which is P. Therefore $\xi = \delta(P)$ and by showing $\xi \neq 0$ he got the conclusion.

Another counterexample to the local-global divisibility by 9 in elliptic curves over $\mathbb{Q}$ appears in [62]. Lawson and Wuthrich show that the point $(-2, 3)$ on the elliptic curve $y^2 + y = x^3 + 20$ is locally divisible by 9 in $\mathbb{Q}_p$, for all $p \neq 3$, but it is not divisible by 9 in $\mathbb{Q}$ and in $\mathbb{Q}_3$. To find this counterexample, they considered elliptic curves admitting a 3-isogeny where either the kernel has a rational 3-torsion point or the kernel of the dual isogeny has a rational 3-torsion point. In fact in [45] it is essentially shown that the non-existence of an isogeny of degree p for $\mathcal{E}$ is a sufficient condition to the local-global divisibility of points by p^l, for every $l \geqslant 1$ over fields k not containing $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ (indeed the proof is carried on in the case when $k = \mathbb{Q}$, but it can be easily generalized to every number field $k \not\supseteq \mathbb{Q}(\zeta_p + \overline{\zeta_p})$; see also [78] where this last condition has been explicitated). For each of those $\mathcal{E}$, Lawson and Wuthrich computed the pair $(a_p(\mathcal{E}), p)$ modulo 9, for all $p < 1000$, where $a_p(\mathcal{E})$ is the trace of the Frobenius element of $\mathrm{Gal}(k(\mathcal{E}[p])/k)$. On the other hand, they considered the pairs $(\mathrm{tr}(\sigma), \det(\sigma))$, formed by trace and determinant of matrices $\sigma \in \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, such that the kernel of the map $H^1(G, \mathcal{E}[9]) \to \prod_{v \in \Sigma} H^1(G_v, \mathcal{E}[9])$ is nontrivial. In the cases when a pair of the first type coincided with a pair of the second type, they got a curve $\mathcal{E}$, which was a good candidate for a counterexample. Then they checked that for the candidate with the smallest conductor, the local divisibility by 9 holds for all but finitely many v, but the global divisibility does not hold.

There are no explicit counterexamples to the local-global divisibility by powers of $p \geqslant 5$ in elliptic curves over any number field k. Anyway, in [84], Ranieri exhibited

all possible subgroups G of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, such that there could exist an elliptic curve $\mathcal{E}$ with Galois group $\mathrm{Gal}(k(\mathcal{E}[p])/k)$ isomorphic to G, with a point violating the local-global divisibility by 5^l, for some positive integer l.

7.1.1 Counterexamples to Problem 1.3 and Cassels' question in elliptic curves

The first counterexample to Problem 1.3 appears in [35] and it is given by the curve

$$y^2 = x(x + 80)(x + 205),$$

such that $Ш(\mathbb{Q}, \mathcal{E}) \not\subseteq 4H^1(\mathbb{Q}, \mathcal{E})$.

To produce this example Creutz used Theorem 5.1. In [36], he showed that this example implies counterexamples to Problem 1.3 in elliptic curves, for every power 2^n, with $n \geqslant 2$. In the same paper he also shows counterexamples to Problem 1.3 in elliptic curves for every power 3^n, with $n \geqslant 2$. Those counterexamples also imply a negative answer to Cassels' question for $p \in \{2, 3\}$.

7.2 Counterexamples to Problem 1.2 in algebraic tori

As mentioned in Sect. 6.2, Illengo showed that the bound in Theorem 6.7 is best possible, since for all $n \geqslant 3(p - 1)$ there are counterexamples.

Theorem 7.3 (Illengo, 2008) *Let $p \neq 2$ be a prime and let $l \geqslant 3(p - 1)$. Let $\mathbb{F}_p^l$ be the field with p^l elements. There exists a p-group G in $\mathrm{SL}_n(\mathbb{Z})$ such that the map $H^1(G, \mathbb{F}_p^l) \to \prod H^1(C, \mathbb{F}_p^l)$, where the product is taken on all cyclic subgroups C of G, is not injective.*

Other counterexamples to the local-global divisibility by p in algebraic tori are produced in [43].

7.3 Counterexamples to Problems 1.2, 1.3 and Cassels' question in abelian varieties

In 1996 in [23, Chapter 6, Section 9, p. 61], Cassels and Flynn produced a counterexample to the local-global principle for divisibility by $p = 2$ in an abelian surface. They considered a curve $\mathcal{C}$ of genus 2 defined over $\mathbb{Q}$, with equation $y^2 = A(x)B(x)C(x)$, where $A(x)$, $B(x)$, $C(x) \in \mathbb{Q}[x]$ are quadratic polynomials with constant term equal to 1, irreducible over $\mathbb{Q}$, but splitting respectively over $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{17})$ and $\mathbb{Q}(\sqrt{34})$. They showed that the Jacobian $\mathcal{A}$ of $\mathcal{C}$ has a point P locally divisible by 2 over all p-adic fields $\mathbb{Q}_p$ and over $\mathbb{R}$, but not divisible by 2 over $\mathbb{Q}$. This is a counterexamples to Problem 1.2 (and to the $r = 0$ case of Problem 1.3) in abelian varieties and predates the counterexamples in elliptic curves. Since the local divisibility holds for all p, then we have $Ш(\mathbb{Q}, \mathcal{A}) \neq 0$. The abelian surface $\mathcal{A}$ is principally polarized and it is conjectured that $Ш(\mathbb{Q}, \mathcal{A})$ is finite. In this last case we also have a counterexample to the local-global disivibility by 2 in $H^r(\mathbb{Q}, \mathcal{A})$, for some r, as mentioned in Sect. 5.

More generally, in [35], Creutz showed some counterexamples to Problem 1.3 and to Cassels' question in abelian varieties for every p.

Theorem 7.4 (Creutz, 2013) *Let $k = \mathbb{Q}(\zeta_p)$. Let p, r be two prime numbers satisfying $r \equiv 1 \pmod{p^2}$ if p is odd or $r \equiv 1 \pmod 8$ if $p = 2$. Let*

$$f(x) = (x^p - \zeta_p)(x^p - r)(x^p - \zeta_p r) \cdots (x^p - \zeta_p^{p-1} r).$$

There are infinitely many classes $c \in k^*/(k^*)^p$ such that the Jacobian J of the cyclic cover of the projective line $\mathbb{P}^1(k)$ defined by $y^p = cf(x)$ satisfies $Ш(k, J) \not\subseteq pH^1(k, J)$. In particular there are infinitely many non-isomorphic abelian varieties over k with this property.

Those counterexamples are over the cyclotomic field $k = \mathbb{Q}(\zeta_p)$, but the author also deduces counterexamples over $\mathbb{Q}$, by restriction of scalars. To have counterexamples to Problem 1.2 for the divisibility by p in the Jacobian J of Theorem 7.4, one can take the class $c = 1$.

8 Other related problems

In the literature there are various classical problems and also recent ones somehow linked to Problems 1.2 and 1.3. We are going to recall briefly some of them. As already observed in the introduction, if the point P in the statement of Problem 1.2 is the zero point in the group law of $\mathcal{G}$ and we ask that neither D nor D_v, for all but finitely many v, is the zero point itself, then the question can be reformulated as follows.

Question 8.1 If $\mathcal{G}$ admits a k_v-rational torsion point of order q, for all but finitely many places $v \in M_k$, can we conclude that $\mathcal{G}$ admits a k-rational torsion point of order q?

This is one of the reasons why the local-global divisibility problem is related to the following problems about torsion points, number fields generated by the coordinates of torsion points, existence of isogenies in abelian varieties, etc. Through all this section, we denote by $\mathfrak{p}_v$ the prime ideal associated to the valuation v and by $\mathbb{F}_v$ the residue field.

(i). In [55], Katz studied this problem formulated by Lang.

Problem 8.2 (Lang, 1981) Let $q \geqslant 2$ be a positive integer. Let $\mathcal{A}$ be an abelian variety defined over a number field k and let $\mathcal{A}_{\text{tors}}(k)$ denote the set of k-rational torsion points of $\mathcal{A}$. For every $v \in M_k$, let $\widetilde{\mathcal{A}}_v$ be the reduction of $\mathcal{A}$ modulo v and let $N(v)$ denote the number of $\mathbb{F}_v$-rational points of $\widetilde{\mathcal{A}}_v$. Suppose that the congruence

$$N(v) \equiv 0 \pmod q$$

holds for a set of places v of Dirichlet density 1. Does there exist an abelian variety $\mathcal{A}'$ that is k-isogenous to $\mathcal{A}$ and such that

$$\#\mathcal{A}'_{\text{tors}}(k) \equiv 0 \pmod q?$$

Katz proved that when $\mathcal{A}$ is an elliptic curve or an abelian variety of dimension 2, then we have an affirmative answer to Problem 8.2. On the contrary, he produces counterexamples for every abelian variety of dimension $g \geqslant 3$ and every positive integer $q \geqslant 3$.

Assume that $\mathcal{E}$ is an elliptic curve with good reduction at v. If q is coprime with the characteristic of the residue field $\mathbb{F}_v$, then by [90, VII, Proposition 3.1], the group $\mathcal{E}(k_v)[q]$ of the k_v-rational q-torsion points of $\mathcal{E}$ injects into the group $\widetilde{\mathcal{E}}_v(\mathbb{F}_v)$ of the $\mathbb{F}_v$-rational points of $\widetilde{\mathcal{E}}_v$. Then the existence of a k_v-rational point of exact order q implies the existence of a subgroup of $\widetilde{\mathcal{E}}_v(\mathbb{F}_v)$ of order q. If $q \nmid N(v)$, then there are no k_v-rational q-torsion points in $\mathcal{E}$. Since $\mathcal{E}(k)[q]$ injects into $\mathcal{E}(k_v)[q]$, this also implies that there are no k-rational q-torsion points in $\mathcal{E}$. Therefore an affirmative answer to Problem 8.2 implies an affirmative answer to Question 8.1.

Katz reformulated Lang's question in terms of representations to prove some of his results (see also [39, 40]).

Problem (Lang, Katz, 1981) Let $q \geqslant 2$ be a positive integer. Let $\mathcal{A}$ be an abelian variety defined over a number field k. For every place v, denote by $T_v(\mathcal{A})$ the v-adic Tate module of $\mathcal{A}$, by ρ_v the associated v-adic representation and by $\bar{\rho}_v$ the associated mod v representation. If for every $\sigma \in G_k$, we have $\det(1 - \bar{\rho}_v(\sigma)) = 0$ in k_v, is it true that the semisimplification of $T_v(\mathcal{A}) \otimes k_v$ contains the trivial representation?

(ii). Owing again to the particular case when $P \in \mathcal{G}(k)$ is the zero point, Problem 1.2 is also linked to the famous *Support Problem*, considered by Corrales-Rodrigáñez and Schoof in [32]. The original question about integers was posed by Erdős in 1988, during a conference in number theory that took place in Banff.

Problem 8.3 (Support Problem, Erdős, 1988) Let x, y, q be positive integers such that $x^q \equiv 1 \pmod{p}$ if and only if $y^q \equiv 1 \pmod{p}$, for every prime number p. Can we conclude that $x = y$?

The name *Support Problem* is a consequence of the name *support* used to indicate the set of prime numbers dividing $x^q - 1$. In [32], Corrales-Rodrigáñez and Schoof answered affirmatively to Problem 8.3. Moreover they show that the answer is affirmative even with the hypotheses holding for all but finitely many prime numbers p. They also considered the question on a number field k and proved the following statement.

Theorem 8.4 (Corrales-Rodrigáñez, Schoof, 1997) *Let k be a number field and let $x, y \in k^*$. Assume that for almost all valuations v of k, and for all positive integers q one has*

$$y^q \equiv 1 \pmod{\mathfrak{p}_v} \quad \textit{whenever} \quad x^q \equiv 1 \pmod{\mathfrak{p}_v}.$$

Then y is a power of x.

In addition, they considered the same question in the case of elliptic curves.

Problem 8.5 (Corrales-Rodrigáñez, Schoof, 1997) Let $\mathcal{E}$ be an elliptic curve over a number field k. Let $P, Q \in \mathcal{E}(k)$. Assume that for every positive integer q and all but finitely many places v of k for which $\mathcal{E}$ has good reduction, we have

$$qP \equiv 0 \text{ in } \mathbb{F}_v \quad \text{whenever} \quad qQ \equiv 0 \text{ in } \mathbb{F}_v.$$

What can we conclude about P and Q?

One of the main differences between Question 8.1 or Problem 8.2 and the Support Problem is that in this last case one considers *two* points having the same behaviour with respect a certain property and wonders about their possible relation.

Corrales-Rodrigáñez and Schoof showed that two points P and Q satisfying the assumptions of Problem 8.5 are actually linked as follows.

Theorem 8.6 (Corrales-Rodrigáñez, Schoof,1997) *Let $\mathcal{E}$ be an elliptic curve defined over a number field k. Let $P, Q \in \mathcal{E}(k)$. If for every positive integer q and all but finitely many places v of k for which $\mathcal{E}$ has good reduction, one has*

$$qP \equiv 0 \text{ in } \mathcal{E}(\mathbb{F}_v) \quad \text{whenever} \quad qQ \equiv 0 \text{ in } \mathcal{E}(\mathbb{F}_v),$$

then either $Q = \phi(P)$, for some k-rational endomorphism ϕ of $\mathcal{E}$ or both P and Q are torsion points.

The same question was afterwards considered for abelian varieties by Larsen [61], by Demeyer and Perucca [41, 80, 81], by Banaszak, Gajda and Krasoń [5, 6] and by Barańczuk [10]. In particular in [61], Larsen proved this generalization of Theorem 8.6.

Theorem 8.7 (Larsen, 2003) *Let $\mathcal{A}$ be an abelian variety over a number field k. Let $P, Q \in \mathcal{A}(k)$. Assume that for every positive integer q and all but finitely many places v of k for which $\mathcal{A}$ has good reduction, we have*

$$qP \equiv 0 \text{ in } \mathcal{E}(\mathbb{F}_v) \implies qQ \equiv 0 \text{ in } \mathcal{E}(\mathbb{F}_v).$$

Then there exists a k-endomorphism ϕ of $\mathcal{A}$ and a positive integer m such that $\phi(P) = mQ$.

In [41], Demeyer and Perucca showed an explicit m. In the same paper, as well as in [81] they also considered the question for tori. Moreover Li treated it for Drinfeld modules in [63]. In [57], Khare and Prasad studied the same local-global problem for endomorphisms of an abelian variety (and, more generally, of a commutative algebraic group) instead of points. Other similar problems are treated in [2, 59].

(iii). In [98], Wong considered the following question.

Problem 8.8 (Wong, 2000) Let $\mathcal{G}$ be an algebraic group defined over a number field k and $q > 1$ a positive integer. Denote by Λ a subset of M_k of density 1 and by U a finite subset of the set of k-rational points $\mathcal{G}(k)$ of $\mathcal{G}$. For every $v \in M_k$ let $\widetilde{\mathcal{G}}_v$ be the reduction of $\mathcal{G}$ modulo v. Assume that for every $v \in \Lambda$, there exists a non-zero point $P_v \in U$, whose image in $\widetilde{\mathcal{G}}_v(\mathbb{F}_v)$ is a q-th power of a point in $\widetilde{\mathcal{G}}_v(\mathbb{F}_v)$. Does U contain a q-th power of an element of $\mathcal{G}(k)$?

The answer clearly depends on U, as well as on k and q. When $U = \{P\}$, with P a k-rational point of $\mathcal{G}$, Problem 8.8 is similar to Problem 1.2, but here one considers the q-divisors of the image of P in $\widetilde{\mathcal{G}}_v(\mathbb{F}_v)$, instead of the q-divisors of P in $\mathcal{G}(k_v)$. Problem 8.8 was even formulated quite at the same time than Problem 1.2. It is also

related to Problem 8.5 in abelian varieties, in the case when P is the zero point. The main result about Wong's question is the following.

Theorem 8.9 (Wong, 2000) *Let $\mathcal{A}$ be an abelian variety defined over a number field k, let $U = \{P\}$, with $P \in \mathcal{A}(k)$ and let q be a positive integer. Assume that one of the following conditions hold:*

(a) $H^1(\mathrm{Gal}(k(\mathcal{A}[q])/k), \mathcal{A}[q]) = 0$;
(b) *$\mathcal{A}$ is an elliptic curve and $q = p$.*

If the image of P in $\widetilde{\mathcal{A}}(\mathbb{F}_v)$ is the q-th power of an element of $\widetilde{\mathcal{A}}(\mathbb{F}_v)$ for a set of places v of density 1, then P is the q-th power of a point in $\mathcal{A}(k)$.

(iv). Let $\mathcal{E}$ be an elliptic curve defined over k. It is well-known that there is a close connection between the existence of a k-rational torsion point of order p in $\mathcal{E}$ and the existence of a k-rational isogeny $\phi\colon \mathcal{E} \to \mathcal{E}$ of degree p. Therefore Question 8.1 (as well as the other mentioned problems) is also linked to the following local-global problem for existence of isogenies of prime degree in elliptic curves.

Problem 8.10 (Sutherland, 2012) Let k be a number field and $\mathcal{E}$ be an elliptic curve defined over k. Assume that $\mathcal{E}$ admits a k_v-rational isogeny of degree p, for all places v of k. Does $\mathcal{E}$ admit a k-rational isogeny of degree p?

As we recalled in Sect. 7, the connection between the existence of isogenies and Problem 1.2 is also underlined in [45]. The converse of Problem 8.10 is trivially true. Sutherland proved the following result.

Theorem 8.11 (Sutherland, 2012) *Let p be a prime number. Assume that $\sqrt{\left(\frac{-1}{p}\right)p} \notin k$ and that $\mathcal{E}$ admits a rational isogeny of degree p locally at a set of primes with density 1. Then $\mathcal{E}$ admits an isogeny of degree p at a quadratic extension of k. If $p \equiv 1 \pmod 4$ or $p < 7$, then $\mathcal{E}$ admits a k-rational isogeny of degree p.*

When $k = \mathbb{Q}$, he furthermore showed that the question has an affirmative answer for every prime $p \neq 7$. If $p = 7$ there exists only one counterexample up to isomorphism. The counterexample is given by the elliptic curve with the equation

$$y^2 + xy = x^3 - x^2 - 107x - 379,$$

admitting an isogeny of degree 7 locally at every prime of good reduction and over $\mathbb{R}$, but admitting no rational isogenies of degree 7. Anyway, according to Theorem 8.11, the curve admits a k-rational isogeny over a quadratic extension k of $\mathbb{Q}$. In addition, when k is a number field containing the quadratic subfield of $\mathbb{Q}(\zeta_p)$, the author gives a classification of the curves for which the principle fails.

The study was completed in [9] by Banwait and Cremona for number fields k that do not contain the quadratic subfield of $\mathbb{Q}(\zeta_p)$. In particular they showed all possible elliptic curves for which the principle fails when k is a quadratic extension.

In [3], Anni gives an upper bound for the primes p such that the local-global divisibility for existence of isogenies of degree p may fail in elliptic curves over a number field k. This bound depends only on the degree of k and on its discriminant.

In the recent paper [97], Vogt considers Problem 8.10 for rational isogenies of arbitrary degree q. In particular he shows that for a fixed number field k and a fixed positive integer q there are only finitely many non-isomorphic elliptic curves for which the local-global existence of a rational isogeny of degree q fails.

(v). Having investigated about the vanishing of two subgroups of $H^1(G, \mathcal{G}[p^l])$, we have to recall that a very interesting question is about the vanishing of this group itself. In the case of elliptic curves, this problem has been especially investigated in [24] and in the mentioned [62], in which the authors proved the following statement.

Theorem 8.12 (Lawson, Wuthrich, 2016) *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$. The group $H^1(G, \mathcal{E}[p])$ is trivial except in the following cases:*

(1) *$p = 3$, there is a rational point of order 3 on $\mathcal{E}$, and there are no other isogenies of degree 3 from $\mathcal{E}$ that are defined over $\mathbb{Q}$;*
(2) *$p = 5$ and the quadratic twist of $\mathcal{E}$ by $D = 5$ has a rational point of order 5, but no other isogenies of degree 5 defined over $\mathbb{Q}$;*
(3) *$p = 11$ and $\mathcal{E}$ is the curve labeled as 121c2 in Cremona's label, given by the global minimal equation $y^2 + xy = x^3 + x^2 - 3632x + 82757$.*

In each of these cases, $H^1(G, \mathcal{E}[p])$ has p elements.

For a general commutative algebraic group $\mathcal{G}$, sufficient conditions to the vanishing of $H^1(G, \mathcal{G}[p])$ are given by Nori in [71, Theorem E].

Theorem 8.13 (Nori, 1972) *There exists a constant $c(n)$ depending only on n such that if $p > c(n)$ and $G \leqslant \mathrm{GL}_n(\mathbb{F}_p)$ acts semisimply on $\mathbb{F}_p^n$, then*

$$H^1(G, \mathbb{F}_p^n) = 0.$$

Many other authors have investigated about the vanishing of the group $H^1(\Gamma, M)$, where Γ is a group and M is a Γ-module (see for examples among others [28, 29, 96]).

(vi). Another question, that is not a local-global one, but it is strongly related to Problem 1.2 (and consequently to Problem 1.3) is the classification of all q-division fields $k(\mathcal{G}[q])$, for a fixed integer q. In fact, information about the extension $k(\mathcal{G}[q])/k$ provides information about the Galois group $G = \mathrm{Gal}(k(\mathcal{G}[q])/k)$ and then about the local cohomology group $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ and the Tate–Shafarevich group $Ш(k, \mathcal{G}[q])$. In particular in [74] the interest of classifying all elliptic curves such that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ was motivated by the possible applications to Problem 1.2. Anyway, independently from the local-global divisibility, an interesting question is to understand when the field $k(\mathcal{E}[p])$ is as small as possible, i.e. $k(\mathcal{E}[p]) = k(\zeta_p)$. We have already mentioned that Merel and Stein [67] and Rebolledo [85] proved that $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$ implies $p \in \{2, 3, 5\}$ or $p > 1000$. The curves with $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\zeta_2)$ (resp. $k(\mathcal{E}[2]) = k(\zeta_2)$) are the ones with two rational (resp. k-rational) torsion points of order 2, that are linearly independent. All the curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ (resp. $k(\mathcal{E}[3]) = k(\zeta_3)$) are shown in [74] (resp. [8]). All the curves with $\mathbb{Q}(\mathcal{E}[5]) = \mathbb{Q}(\zeta_5)$ were lately classified in [49] by González-Jiménez and Lozano-Robledo.

They also proved that if $\mathbb{Q}(\mathcal{E}[q]) = \mathbb{Q}(\zeta_q)$, for any integer q, then $q \in \{2, 3, 4, 5\}$ and describe the family of elliptic curves such that $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\zeta_4)$. Moreover, they studied some properties of the extension $\mathbb{Q}(\mathcal{E}[q])/\mathbb{Q}$ in the case when it is abelian. In particular they described all possible abelian Galois groups $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[q])/\mathbb{Q})$ and proved the following statement.

Theorem 8.14 (González-Jiménez, Lozano-Robledo, 2016) *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let q be a positive integer. Assume that $\mathbb{Q}(\mathcal{E}[q])/\mathbb{Q}$ is abelian. Then $n \in \{2, 3, 4, 5, 6, 8\}$.*

A classification of all number fields $k(\mathcal{E}[q])$, for $q \in \{3, 4\}$, is given in [8] (see also [7] for number fields $\mathbb{Q}(\mathcal{E}[3])$ and [76] for number fields $k(\mathcal{E}[5])$, where $\mathcal{E}$ is an elliptic curve with complex multiplication with Weierstrass form $y^2 = x^3 + bx$ or $y^2 = x^3 + c$, where $b, c \in \mathbb{Q}$). In the same paper a new set of generators is provided for the extension $k(\mathcal{E}[q])$, when q is an odd number. Let ζ_q be a primitive q-th root of the unity as above and $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ two q-torsion points of $\mathcal{E}$ forming a basis of $\mathcal{E}[q]$. Then

$$k(\mathcal{E}[q]) = k(x_1, \zeta_q, y_2).$$

In addition, if $q = p^l$, with p odd, then $k(\mathcal{E}[p^l]) = k(x_1, \zeta_p, y_2)$, for every l [42], where ζ_p is a primitive p-th root of the unity and $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ two p^l-torsion points of $\mathcal{E}$ forming a basis of $\mathcal{E}[p^l]$. For some other information about q-division fields $k(\mathcal{E}[q])$, see also [1].

Acknowledgements A part of this paper was written when the second author was a guest at the Max Planck Institute for Mathematics in Bonn. She thanks for the hospitality and the excellent work conditions. The authors are very grateful to Brendan Creutz for some precious suggestions and for useful discussions. They also warmly thank Jacob Stix for helpful discussions. They are grateful to Igor Shparlinski and Boris Kunyavskii for having pointed out Remark 3.5. Furthermore the authors deeply thank the anonymous referees for many valuable comments and suggestions.

Funding Open access funding provided by Universitá della Calabria within the CRUI-CARE Agreement.

References

1. Adelmann, C.: The Decomposition of Primes in Torsion Points Fields. Lecture Notes in Mathematics, vol. 1761. Springer, Berlin (2001)
2. Ailon, N., Rudnik, Z.: Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$. Acta Arith. **113**(1), 31–38 (2004)
3. Anni, S.: A local-global principle for isogenies of prime degree over number fields. J. London Math. Soc. **89**(3), 745–761 (2014)

4. Artin, E., Tate, J.: Class Field Theory. W.A. Benjamin, New York (1968)
5. Banaszak, G., Gajda, W., Krasoń, P.: Support problem for the intermediate Jacobians of l-adic representations. J. Number Theory **100**(1), 133–168 (2003)
6. Banaszak, G., Gajda, W., Krasoń, P.: Detecting linear dependence by reduction maps. J. Number Theory **115**(2), 322–342 (2005)
7. Bandini, A., Paladino, L.: Number fields generated by the 3-torsion points of an elliptic curve. Monatsh. Math. **168**(2), 157–181 (2012)
8. Bandini, A., Paladino, L.: Fields generated by torsion points of elliptic curves. J. Number Theory **169**, 103–133 (2016)
9. Banwait, B.S., Cremona, J.: Tetrahedral elliptic curves and the local-global principle for isogenies. Algebra Number Theory **8**(5), 1201–1229 (2014)
10. Barańczuk, S.: On a generalization of the support problem of Erdős and its analogues for abelian varieties and K-theory. J. Pure Appl. Algebra **214**(4), 380–384 (2010)
11. Bašmakov, M.I.: On the divisibility of principal homogeneous spaces over Abelian varieties. Izv. Akad. Nauk SSSR Ser. Mat. **28**, 661–664 (1964) (in Russian)
12. Bašmakov, M.I.: The cohomology of abelian varieties over a number field. Russian Math. Surveys **27**(6), 25–70 (1972)
13. Bayer-Fluckiger, E., Parimala, R.: Classical groups and the Hasse principle. Ann. Math. **147**(3), 651–693 (1998)
14. Cassels, J.W.S.: Arithmetic on curves of genus 1. I. On a conjecture of Selmer. J. Reine Angew. Math. **202**, 52–99 (1959)
15. Cassels, J.W.S.: Arithmetic on curves of genus 1. II. A general result. J. Reine Angew. Math. **203**, 174–208 (1960)
16. Cassels, J.W.S.: Arithmetic on curves of genus 1. III. The Tate–Šafarevič and Selmer groups. Proc. London Math. Soc. **12**, 259–296 (1962)
17. Cassels, J.W.S.: Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. J. Reine Angew. Math. **211**, 95–112 (1962)
18. Cassels, J.W.S.: Arithmetic on curves of genus 1. V. Two counterexamples. J. London Math. Soc. **38**, 244–248 (1963)
19. Cassels, J.W.S.: Corrigendum: "Arithmetic on curves of genus 1. III. The Tate–Šafarevič and Selmer groups". Proc. London Math. Soc. **13**(3), 768 (1963)
20. Cassels, J.W.S.: Arithmetic on curves of genus 1. VI. The Tate–Šafarevič group can be arbitrarily large. J. Reine Angew. Math. **214–215**, 65–70 (1964)
21. Cassels, J.W.S.: Arithmetic on curves of genus 1. VII. The dual exact sequence. J. Reine Angew. Math. **216**, 150–158 (1964)
22. Cassels, J.W.S.: Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. J. Reine Angew. Math. **217**, 180–199 (1965)
23. Cassels, J.W.S., Flynn, E.V.: Prolegomena to a Middlebrow Arithmetic of Genus 2 Curves. London Mathematical Society Lecture Note Series, vol. 230. Cambridge University Press, Cambridge (1996)
24. Cha, B.: Vanishing of some cohomology groups and bounds for the Shafarevich–Tate groups of elliptic curves. J. Number Theory **111**(1), 154–178 (2005)
25. Chernousov, V.I.: The Hasse principle for groups of type E_8. Soviet. Math. Dokl. **39**(3), 592–596 (1989)
26. Çiperiani, M., Stix, J.: Weil–Châtelet divisible elements in Tate–Shafarevich groups I: The Bashmakov problem for elliptic curves over $\mathbb{Q}$. Compositio Math. **149**(5), 729–753 (2013)
27. Çiperiani, M., Stix, J.: Weil–Châtelet divisible elements in Tate–Shafarevich groups II: On a question of Cassels. J. Reine Angew. Math. **700**, 175–207 (2015)
28. Cline, E., Parshall, B., Scott, L.: Cohomology of finite groups of Lie type, I. Inst. Hautes Études Sci. Publ. Math. **45**, 169–191 (1975)
29. Cline, E., Parshall, B., Scott, L.: Cohomology of finite groups of Lie type. II. J. Algebra **45**(1), 182–198 (1977)
30. Colliot-Thélène, J.-L., Skorobogatov, A.N.: The Brauer–Grothendieck Group. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3, vol. 71. Springer, New York (2021)
31. Colliot-Thélène, J.-L., Skorobogatov, A.N., Swinnerton-Dyer, P.: Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points. Invent. Math. **134**(3), 579–650 (1988)
32. Corrales-Rodrigáñez, C., Schoof, R.: The support problem and its elliptic analogue. J. Number Theory **64**(2), 276–290 (1997)

33. Cremona, J.E., Fisher, T.A., O'Neil, C., Simon, D., Stoll, M.: Explicit n-descent on elliptic curves. I. Algebra. J. Reine Angew. Math. **615**, 121–155 (2008)
34. Creutz, B.: A Grunwald–Wang type theorem for abelian varieties. Acta Arith. **154**(4), 353–370 (2012)
35. Creutz, B.: Locally trivial torsors that are not Weil–Châtelet divisible. Bull. London Math. Soc. **45**(5), 935–942 (2013)
36. Creutz, B.: On the local-global principle for divisibility in the cohomology of elliptic curve. Math. Res. Lett. **23**(2), 377–387 (2016)
37. Creutz, B.: There are no transcendental Brauer–Manin obstructions on abelian varieties. Int. Math. Res. Not. **2020**(9), 2684–2697 (2020)
38. Creutz, B., Voloch, J.F.: Local-global principle for Weil–Chătelet divisibility in positive characteristic. Math. Proc. Cambridge Philos. Soc. **163**(2), 357–367 (2017)
39. Cullinan, J.: Local-global properties of torsion points on three-dimensional abelian varieties. J. Algebra **311**(2), 736–774 (2007)
40. Cullinan, J.: Points of small order on three-dimensional abelian varieties; with an appendix by Yuri Zarhin. J. Algebra **324**(3), 565–577 (2010)
41. Demeyer, J., Perucca, A.: The constant of the support problem for abelian varieties. J. Number Theory **133**(9), 2843–2856 (2013)
42. Dvornicich, R., Paladino, L.: On the division fields of an elliptic curve and an effective bound to the hypotheses of the local-global divisibility. Int. J. Number Theory **18**(7), 1567–1590 (2022)
43. Dvornicich, R., Zannier, U.: Local-global divisibility of rational points in some commutative algebraic groups. Bull. Soc. Math. France **129**(3), 317–338 (2001)
44. Dvornicich, R., Zannier, U.: An analogue for elliptic curves of the Grunwald–Wang example. C. R. Acad. Sci. Paris Ser. I **338**(1), 47–50 (2004)
45. Dvornicich, R., Zannier, U.: On local-global principle for the divisibility of a rational point by a positive integer. Bull. London Math. Soc. **39**(1), 27–34 (2007)
46. Gillibert, F., Ranieri, G.: On the local-global divisibility of torsion points on elliptic curves and GL_2 -type varieties. J. Number Theory **174**, 202–220 (2017)
47. Gillibert, F., Ranieri, G.: On the local-global divisibility over abelian varieties. Ann. Inst. Fourier (Grenoble) **68**(2), 847–873 (2018)
48. Gillibert, F., Ranieri, G.: On local-global divisibility over GL_2-type varieties. Acta Arith. **193**(4), 339–354 (2020)
49. González-Jiménez, E.: Lozano-Robledo, Á: Elliptic curves with abelian division fields. Math. Z. **283**(3–4), 835–859 (2016)
50. Harbater, D., Hartmann, J., Krashen, D.: Local-global principles for Galois cohomology. Commentarii Math. Helv. **89**(1), 215–253 (2014)
51. Harbater, D., Hartmann, J., Krashen, D.: Local-global principle for torsors over arithmetic curves. Amer. J. Math. **137**(6), 1559–1612 (2015)
52. van der Heiden, G.-J.: Local-global problem for Drinfeld modules. J. Number Theory **104**(2), 193–209 (2004)
53. Illengo, M.: Cohomology of integer matrices and local-global divisibility on the torus. J. Théor. Nombres Bordeaux **20**(2), 327–334 (2008)
54. Kato, K.: A Hasse principle for two-dimensional global fields. With an appendix by Jean-Louis Colliot-Thélène. J. Reine Angew. Math. **366**, 142–183 (1986)
55. Katz, N.M.: Galois properties on torsion points on abelian varieties. Invent. Math. **62**(3), 481–502 (1981)
56. Kenku, M.A.: On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$. J. London Math. Soc. **23**(3), 415–427 (1981)
57. Khare, C., Prasad, D.: Reduction of homomorphisms mod p and algebraicity. J. Number Theory **105**(2), 322–332 (2004)
58. Kneser, M.: Hasse principle for H^1 of simply connected groups. In: Borel, A., Mostow, G.D. (eds.) Algebraic Groups and Discontinuous Subgroups. Proceedings of Symposia in Pure Mathematics, vol. 9, pp. 159–163. American Mathematical Society, Providence (1966)
59. Kowalski, E.: Some local-global applications of Kummer theory. Manuscripta Math. **111**(1), 105–139 (2003)
60. Lagarias, J.C., Montgomery, H.L., Odlyzko, A.M.: A bound for the least prime Ideal in the Chebotarev density theorem. Invent. Math. **54**(3), 271–296 (1979)
61. Larsen, M.: The support problem for abelian varieties. J. Number Theory **101**(2), 398–403 (2003)

62. Lawson, T., Wuthrich, C.: Vanishing of some cohomology groups for elliptic curves. In: Loeffler, D., Zerbes, S.L. (eds.) Elliptic Curves, Modular Forms and Iwasawa Theory. Springer Proceedings in Mathematics & Statistics, vol. 188, pp. 373–399. Springer, Cham (2016)
63. Li, A.: On the support problem for Drinfeld modules. Comm. Algebra **34**(6), 2167–2174 (2006)
64. Manin, Yu.I.: Le groupe de Brauer–Grothendieck en géométrie diophantienne. Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1. 401–411. Gauthier-Villars, Paris (1971)
65. Mazur, B.: Rational isogenies of prime degree (with an appendix of D. Goldfeld). Invent. Math. **44**(2), 129–162 (1978)
66. Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. **124**, 437–449 (1996)
67. Merel, L., Stein, W.A.: The field generated by the points of small prime order on an elliptic curve. Internat. Math. Res. Notices **2001**(20), 1075–1082 (2001)
68. Milne, J.S.: Arithmetic Duality Theorems. Perspectives in Mathematics, vol. 1. Academic Press, Boston (1986)
69. Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields. Grundlehren der mathematischen Wissenschaften, vol. 323. Springer, Berlin (2000)
70. Nguyen, D.Q.N.: A Carlitz module analogue of the Grunwald–Wang theorem. Indiana Univ. Math. J. **67**(3), 1281–1297 (2018)
71. Nori, M.V.: On subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$. Invent. Math. **88**(2), 257–275 (1987)
72. Oesterlé, J.: Torsion des courbes elliptiques sur les corps de nombres. preprint
73. Paladino, L.: Local-global divisibility by 4 in elliptic curves defined over $\mathbb{Q}$. Ann. Mat. Pura Appl. **189**(1), 17–23 (2010)
74. Paladino, L.: Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9. J. de Théor. Nombres Bordeaux **22**(1), 139–160 (2010)
75. Paladino, L.: On counterexamples to local-global divisibility in commutative algebraic groups. Acta Arith. **148**(1), 21–29 (2011)
76. Paladino, L.: On 5-torsion of CM elliptic curves. Riv. Math. Univ. Parma (N.S.) **9**(2), 329–350 (2018)
77. Paladino, L.: Divisibility questions in commutative algebraic groups. J. Number Theory **205**, 210–245 (2019)
78. Paladino, L., Ranieri, G., Viada, E.: On local-global divisibility by p^n in elliptic curves. Bull. London Math. Soc. **44**(4), 789–802 (2012)
79. Paladino, L., Ranieri, G., Viada, E.: On minimal set for counterexamples to the local-global principle. J. Algebra **415**, 290–304 (2014)
80. Perucca, A.: Two variants of the support problem for products of abelian varieties and tori. J. Number Theory **129**(8), 1883–1892 (2009)
81. Perucca, A.: The multilinear support problem for products of abelian varieties and tori. Int. J. Number Theory **8**(1), 255–264 (2012)
82. Poonen, B.: An explicit algebraic family of genus one curves violating the Hasse principle. J. Théor. Nombres Bordeaux **13**(1), 263–274 (2001)
83. Prasad, G., Rapinchuk, A.S.: Local-global principles for embedding of the fields with involution into simple algebras with involution. Comment. Math. Helv. **85**(3), 583–645 (2010)
84. Ranieri, G.: Counterexamples to the local-global divisibility over elliptic curves. Ann. Mat. Pura Appl. **197**(4), 1215–1225 (2018)
85. Rebolledo Hochart, M.: Corps engendré par les points de 13-torsion des courbes elliptiques. Acta Arith. **109**(3), 219–230 (2003)
86. Roquette, P.: The Brauer–Hasse–Noether Theorem in Historical Perspective. Schriften der Mathematisch-Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften, vol. 15. Springer, Berlin (2005)
87. Sansuc, J.-J.: Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres. J. Reine Angew. Math. **327**, 12–80 (1981)
88. Serre, J.-P.: Sur les groupes de congruence des variétés abéliennes. Izv. Akad. Nauk SSSR. Ser. Mat. **28**, 3–20 (1964)
89. Serre, J.-P.: Algebraic groups and class fields. Graduate Texts in Mathematics, vol. 117. Springer, New York (1988)
90. Silverman, J.H.: The Arithmetic of Elliptic Curves. 2nd edn. Graduate Texts in Mathematics, vol. 106. Springer, Dordrecht (2009)

91. Skorobogatov, A.: Torsors and Rational Points. Cambridge Tracts in Mathematics, vol. 144. Cambridge University Press, Cambridge (2001)
92. Sutherland, A.V.: A local-global principle for rational isogenies of prime degree. J. Théor. Nombres Bordeaux **24**(2), 475–485 (2012)
93. Tate, J.: Duality theorems in Galois cohomology over number fields. In: Proceedings of the International Congress of Mathematicians (Stockholm 1962), pp. 288–295. Inst. Mittag-Leffler, Djursholm (1963)
94. Tschebotareff, N.: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. Math. Ann **95**(1), 191–228 (1926)
95. Trost, E.: Zur theorie des Potenzreste. Nieuw Archief voor Wiskunde **18**(2), 58–61 (1948)
96. University of Georgia VIGRE Algebra Group: First cohomology for finite groups of Lie type: Simple modules with small dominant weights. Trans. Amer. Math. Soc. **365**(2), 1025–1050 (2013)
97. Vogt, I.: A local-global principle for isogenies of composite degree. Proc. London Math. Soc. **121**(3), 1496–1530 (2020)
98. Wong, S.: Power residues on Abelian varieties. Manuscripta Math. **102**(1), 129–138 (2000)