Divisibility of Points in Algebraic Groups

Sebastiano Tronto

March 30, 2020

1 Algebraic Groups

References: J. S. Milne, *Algebraic Groups*, online lecture notes (also a published book now).

Let's start with an uncommon definition of group.

Definition 1. *A group is a set G with maps*

$$e : \{0\} \to G \qquad i : G \to G \qquad m : G \times G \to G$$

such that the appropriate diagrams commute.

An algebraic group is the same thing, but in the category of algebraic varieties!

Definition 2. *An algebraic group over a field k is an algebraic variety G over k with regular maps*

$$e : \operatorname{Spec} k \to G \qquad i : G \to G \qquad m : G \times G \to G$$

defined over k such that the appropriate diagrams commute.

Basically, the set of points of G (as an algebraic variety) has a group law, and the multiplication is a regular map (defined over k.

Example 3. Example of algebraic groups include:

- Elliptic curves and, more generally, abelian varieties.
- The multiplicative group $\mathbb{G}_m$ and, more generally, GL_n.

Abelian varieties are projective (and abelian) while GL_n is affine (and non-abelian for $n > 1$).

1.1 Points

From now on you can think of algebraic varieties as either affine or projective, so that we can freely talk about (projective or affine) coordinates. In this setting, given an (affine or projective) algebraic variety V over k, we can consider the set

$$V(k) = \{P \in V \mid P \text{ has coordinates in } k\}$$

or more generally

$$V(L) = \{P \in V \mid P \text{ has coordinates in } L\}$$

where L is any field extension.

What we are considering here is called "functor of points", and it is in fact a functor

$$\{\text{Extensions of } k\} \to \textsc{Set}$$

which completely determines our variety V (if we allow "extension" to mean "commutative, unitary k-algebra").

If we have an algebraic group G, since k-morphisms send point defined over L to points defined over L (for any field extension L of k), the set $G(L)$ is a group. In fact, algebraic groups are precisely those algebraic varieties those functor of points factors via Grp. This means, for example, that we can define GL_n as follows: it is the unique algebraic group over k such that, for any commutative k-algebra R, $\mathrm{GL}_n(R)$ is the group of invertible matrices with coefficients in R.

All this abstraction is just to say: if you are not comfortable with algebraic varieties, think of algebraic groups as functors $\mathrm{alg}_k \to \textsc{Grp}$.

1.2 Galois action

Now fix a finite Galois extension L of k and let $\Gamma = \mathrm{Gal}(L \,|\, k)$. Consider an algebraic group G over k. It's easy to see that Γ acts on $G(L)$ coordinate-wise, and that this action is compatible with the group operations on G. Thus, if G is commutative, $G(L)$ is a Γ-module.

2 The Local-Global Principle for Divisibility

References: Wikipedia (for the Grunwald-Wang theorem) and R. Dvorinicich, U. Zannier, *Local-GLobal Divisibility of Rational Points in some Commutative Algebraic Groups*, 2001.

In this section we fix a number field K, a commutative and connected algebraic group A over K and an integer N. We denote the multiplication $m : (P, Q) \mapsto m(P, Q)$ by $P + Q$.

2.1 Divisibility

There exists a map

$$\begin{aligned} N = [N] : A &\to A \\ P &\mapsto \underbrace{P + P + \cdots + P}_{N \text{ times}} \end{aligned}$$

given by repeated addition, which we call *multiplication by N*. We may want to call a point "N-divisible" if it lies in the image of this map, but this is not an interesting concept!

Lemma 4. *For $n \neq 0$, the multiplication by N map is surjective on $\overline{K}$-points.*

Proof for $A = \mathbb{G}_m$. A point $P \in \mathbb{G}_m = \overline{K}^\times$ certainly admits an N-th root in $\overline{K}^\times$. □

It is much more interesting to ask this question on the level of K-points, or of L-points for some extension L of K.

Definition 5. *Let $P \in A(K)$ be a rational point and L be a field extension of K. We say that P is N-divisible over L if there exists $Q \in A(L)$ such that $P = nQ$.*

2.2 The Local-Global principle

Consider a rational point $P \in A(K)$. If it is N-divisible over K, i.e. if there is $Q \in A(K)$ such that $P = NQ$, then clearly it is N-divisible over any field extension L of K, as $Q \in A(K) \subseteq A(L)$. In particular, it is divisible over $K_\mathfrak{p}$ for every "prime" $\mathfrak{p}$ of K (here I also include the so called "infinite primes", i.e. archimedean valuations).

We can ask the following question, which we refer to as the **local-global principle**:

Assume that P is N-divisible over $K_\mathfrak{p}$ for almost all primes $\mathfrak{p}$ of K (i.e. for all but finitely many of them). Can we conclude that P is N-divisible over K?

This question has been studied in this generality by Dvornicich and Zannier in 2006, and by other people in the following years. But the motivation comes from a classical theorem, which can be seen as an example for this in case $A = \mathbb{G}_m$.

A positive answer would be useful in practice, because it is possible to check the existence of division points everywhere locally in an effective way, combining Hensel's Lemma with some known bounds on the number of points over finite fields.

2.3 The Grunwald-Wang Theorem

In 1933 Grunwald proved the following theorem.

Theorem 6. *Let $a \in K^\times$ assume that $a \in (K_\mathfrak{p}^\times)^N$ for almost all places $\mathfrak{p}$ of K. Then $a \in (K^\times)^N$.*

A second proof was published by Whaples in 1942. However, in 1948 Wang found a mistake in the proof and produced the following counterexample.

Example 7. The number $16 \in \mathbb{Q}^\times$ is an 8-th power in $\mathbb{Q}_p$ for all $p \neq 2$, but it is not an 8-th power in $\mathbb{Q}$. In fact, consider the factorization

$$X^8 - 16 = (X^2 - 2)(X^2 - 2)(X^2 - 2X + 2)(X^2 + 2X + 2).$$

Notice that the first factor (respectively second, third) has a root in $\mathbb{Q}_p$ if and only if 2 (respectively -2, -1) is a square in $\mathbb{Q}_p$. Since for $p > 2$ the subgroup of squares is in $\mathbb{Z}_p^\times$ has index two, we conclude that either 2, -2 or -1 is a square in $\mathbb{Q}_p$. Hence $X^8 - 16$ has a root in $\mathbb{Q}_p$ for all $p > 2$.

One can construct an even worse counterexample, i.e. find a number that is an 8-th power over *all* completions, but not an 8-th power over K: just consider $K = \mathbb{Q}(\sqrt{7})$ and $16 \in K^\times$. Then 16 is an 8-th power over all $K_\mathfrak{p}$ with $\mathfrak{p} \nmid 2$ by what we have shown, and this time it is also an 8-th power over $K_{\mathfrak{p}_2}$, where $\mathfrak{p}_2$ is the only (ramified) prime above 2. However, 16 is not an 8-th power in K.

Wang was also able to detect exactly the cases in which the theorem fails and provided a necessary and sufficient condition to fix the statement.

2.4 Results of Dvornicich and Zannier

Fact. We let $A[m] := \{P \in A(\overline{K}) \,|\, mP = 0\} = \ker m$. This is an algebraic group over K and actually a Galois module. We have $A[m] \cong (\mathbb{Z}/m\mathbb{Z})^{n_A}$ for some integer n_A depending only on A.

Given a set of points $S \subseteq A(\overline{K})$ we can define the field $K(S)$ obtained by adjoining to K all the coordinates of points in S (if A is projective, we have to take affine coordinates). More precisely this can be defined as the extension fixed by the subgroup

$$\left\{\sigma \in \mathrm{Gal}(\overline{K} \,|\, K) \,|\, \sigma(P) = P \,\forall P \in S\right\}$$

of the absolute Galois group of K. We define

$$K_m := K(A[m])$$

to be the m-th *torsion field* (or *division field*) of A, which is a finite Galois extension of K. These field extensions have been studied extensively using the theory of Galois representations. In fact, given that the Galois group acts $\mathbb{Z}/m\mathbb{Z}$ linearly on $A[m]$, we have an injective map

$$\mathrm{Gal}(K_m \,|\, K) \to \mathrm{GL}_{n_A}(\mathbb{Z}/m\mathbb{Z}).$$

Definition 8. *Let Γ be a group and M be a Γ-module. We define the following subgroup ("locally trivial" cocycles):*

$$H^1_{\mathrm{loc}}(\Gamma, M) := \bigcap_{C \leq \Gamma \text{ cyclic}} \ker\left(\mathrm{res}_C : H^1(\Gamma, M) \to H^1(C, M)\right).$$

We may restrict to the case $N = \ell^n$ is a prime power. We have the following result:

Theorem 9 (Dvornicich, Zannier)**.** *Let $P \in A(K)$ be such that for all but finitely many primes $\mathfrak{p}$ of K there is $Q_\mathfrak{p} \in A(K_\mathfrak{p})$ such that $P = \ell^n Q_\mathfrak{p}$.*

(1) If $H^1_{\mathrm{loc}}(\mathrm{Gal}(K_{\ell^n} \,|\, K), A[\ell^n]) = 0$, then there exists $Q \in A(K)$ such that $P = \ell^n Q$;

(2) if $H^1_{\mathrm{loc}}(\mathrm{Gal}(K_{\ell^n} \,|\, K), A[\ell^n]) \neq 0$ but $H^1(\mathrm{Gal}(K_{\ell^n} \,|\, K), A(K_{\ell^n})) = 0$, then there exists some $P' \in A(K)$ that is ℓ^n-divisible over $K_\mathfrak{p}$ for all but finitely many $\mathfrak{p}$, but ℓ^n-divisible in K.

With this we can explain the failure of Grunwald-Wang theorem in some cases.

Example 10. Let $K = \mathbb{Q}$ and $A = \mathbb{G}_m$ and $\ell^n = 8$. Then some computations show that

$$H^1_{\mathrm{loc}}(\mathrm{Gal}(\mathbb{Q}(\zeta_8) \,|\, \mathbb{Q}), \mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

while $H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_8) \,|\, \mathbb{Q}), \mathbb{Q}(\zeta_8)) = 0$ by Hilbert's Theorem 90. We conclude that there must be a counterexample to the local-global principle.

3 Divisibility in Field Extensions

Let K and A be as before. Again we restrict to the case where $N = \ell^n$ is a prime power.

An interesting phenomenon is that of rational points that are not ℓ^n-divisible, but may become ℓ^n-divisible over a certain field extension.

Lemma 11. *Let $L \supseteq K$ be a finite Galois extension with Galois group G and let ℓ^n be a prime power. Then there is an exact sequence of abelian groups*

$$0 \to \ell^n A(K) \to A(K) \cap \ell^n A(L) \to H^1(G, A[\ell^n](L)) \to H^1(G, A(L)).$$

Proof. Consider the short exact sequence of G-modules

$$0 \to A[\ell^n](L) \to A(L) \to \ell^n A(L) \to 0$$

and the beginning of the long exact sequence induced in cohomology (i.e. taking $H^*(G, -)$)

$$0 \to (A[\ell^n](L))^G \to (A(L))^G \to (\ell^n A(L))^G \to H^1(G, A[\ell^n](L)) \to H^1(G, A(L)).$$

Notice that

$$(A[\ell^n](L))^G = A[\ell^n](K), \qquad (A(L))^G = A(K), \qquad (\ell^n A(L))^G = A(K) \cap \ell^n A(L)$$

and that

$$A(K)/A[\ell^n](K) \cong \ell^n A(K)$$

and the conclusion follows. □

In particular, if $H^1(G, A[\ell^n](L)) = 0$, then if there is a point $Q \in A(L)$ such that $\ell^n Q \in A(K)$, then actually $Q \in A(K)$.

3.1 The Case of Elliptic Curves with $n = 1$ and $L = K_\ell$

If A is an elliptic curve, $n = 1$ and $L = K_\ell$, the interesting cohomology group is $H^1(\mathrm{Gal}(K_\ell \,|\, K), A[\ell])$, where $A[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ and $\mathrm{Gal}(K_\ell \,|\, K)$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Lemma 12. *Assume that A is an elliptic curve. The cohomology group $H^1(\mathrm{Gal}(K_\ell \,|\, K), A[\ell])$ is either trivial or cyclic of order ℓ. In case $\ell = 2$ it is always trivial.*

Proof. Since $\ell A[\ell] = 0$, we have $\ell H^1(\mathrm{Gal}(K_\ell \,|\, K), A[\ell]) = 0$. It follows from [2], Theorem IX.4, that we have an injective map $H^1(\mathrm{Gal}(K_\ell \,|\, K), A[\ell]) \to H^1(H, A[\ell])$, where H is an ℓ-Sylow subgroup of $\mathrm{Gal}(K_\ell \,|\, K)$. This is either trivial (in which case $H^1(\mathrm{Gal}(K_\ell \,|\, K), A[\ell]) = 0$) or cyclic of order ℓ, generated by $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

We can compute $H^1(\langle\sigma\rangle, A[\ell])$:

$$H^1(\langle\sigma\rangle, A[\ell]) = \frac{\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in A[\ell] \mid \sum_{i=0}^{\ell-1} \sigma^i \begin{pmatrix} x \\ y \end{pmatrix} = 0 \right\}}{(\sigma - 1)A[\ell]}$$

and since

$$\sum_{i=0}^{\ell-1}\sigma^i\begin{pmatrix}x\\y\end{pmatrix}=\sum_{i=0}^{\ell-1}\begin{pmatrix}x+iy\\y\end{pmatrix}=\begin{pmatrix}\ell x+\frac{1}{2}\ell(\ell-1)y\\\ell y\end{pmatrix}=\begin{cases}\begin{pmatrix}y\\0\end{pmatrix} & \text{if } \ell=2,\\ \begin{pmatrix}0\\0\end{pmatrix} & \text{otherwise}\end{cases}$$

and

$$(\sigma-1)A[\ell]=\left\{\begin{pmatrix}x\\0\end{pmatrix}\mid x\in\mathbb{Z}/\ell\mathbb{Z}\right\}$$

we get that $H^1(\langle\sigma\rangle, A[2])=0$ and $H^1(\langle\sigma\rangle, A[\ell])=\mathbb{Z}/\ell\mathbb{Z}$ for $\ell>2$. □

In particular, the case $K=\mathbb{Q}$ has been completely solved, and there are rather complete results in the case of number fields K such that $K\cap\mathbb{Q}(\zeta_\ell)=\mathbb{Q}$ (see [1]). It turns out that, over $\mathbb{Q}$, the group $H^1(\mathrm{Gal}(K_\ell\mid K), A[\ell])$ may only be non-zero for some classes of curves when $\ell=3,5$ or for exactly one curve when $\ell=11$. So the obstruction does appear in some situations.

It is in fact possible that some point $\alpha\in A(K)$ is not ℓ-divisible in $A(K)$, but becomes ℓ-divisible in $A(K_\ell)$. The smallest example I have found is the point $(23769/400, 3529853/8000)$ on the elliptic curve over $\mathbb{Q}$ with Cremona Label $17739g1$ given by the equation

$$y^2+y=x^3-216x-1861.$$

3.2 Eventual Divisibility in ℓ^n-Torsion Fields

Unfortunately, as we have seen, a point can become "more ℓ-divisible" over the ℓ-torsion field. But how much more ℓ-divisible can it become? And what about over the infinite tower of ℓ^n-torsion fields (for $n\to+\infty$)? Can a point become more and more ℓ-divisible in this tower? Luckily, in many interesting cases the answer is no.

Proposition 13. *Let A be an elliptic curve over a number field K, ℓ^n a prime power and $P\in A(K)$ a point of infinite order. Assume that for all $m\geq 1$, for all $T\in A[\ell^m](K)$ the point $P+T$ is not ℓ-divisible in $A(K)$ (i.e. that P is ℓ-indivisible even up to torsion). Assume moreover that for some $\delta\leq n$ the matrix $(\ell^\delta+1)I$ is contained in the image of the Galois representation $\mathrm{Gal}(K_{\ell^n}\mid K)\to\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Then P is at most ℓ^δ divisible in $A(K_{\ell^n})$ (i.e. there is no $Q\in A(K_{\ell^n})$ such that $P=\ell^{\delta+1}Q$).*

Proof. First we show that $H^1(\mathrm{Gal}(K_{\ell^n}\mid K), A[\ell^{\delta+1}])$ is killed by ℓ^δ. Let $\varphi:\mathrm{Gal}(K_{\ell^n}\mid K)\to A[\ell^{\delta+1}]$ be a cocycle. Then for any $g\in\mathrm{Gal}(K_{\ell^n}\mid K)$ we have

$$\varphi((\ell^\delta+1)I\cdot g)=\varphi((\ell^\delta+1)I)+(\ell^\delta+1)\varphi(g)$$

which, since $(\ell^\delta+1)I\in\mathcal{Z}(\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))$, is also equal to

$$\varphi(g\cdot(\ell^\delta+1)I)=\varphi(g)+g\varphi((\ell^\delta+1)I)$$

and from equating the two expressions we get

$$\ell^\delta\varphi(g)=g\varphi((\ell^\delta+1)I)-(\ell^\delta+1)I$$

which shows that $\ell^\delta\varphi$ is a coboundary. So $\ell^\delta H^1(\mathrm{Gal}(K_{\ell^n}\mid K), A[\ell^{\delta+1}])=0$.

But now by Lemma 11 we have an exact sequence

$$0\to\ell^{\delta+1}A(K)\to A(K)\cap\ell^{\delta+1}A(K_{\ell^n})\to H^1(G, A[\ell^{\delta+1}]).$$

So $(A(K)\cap\ell^{\delta+1}A(K_{\ell^n}))/\ell^{\delta+1}A(K)$ embeds in $H^1(G, A[\ell^{\delta+1}])$, so it must be killed by ℓ^δ. This means that $\ell^\delta(A(K)\cap\ell^{\delta+1}A(K_{\ell^n}))\subseteq\ell^{\delta+1}A(K)$.

Assume now by contradiction that there is $Q\in A(K_{\ell^n})$ such that $P=\ell^{\delta+1}Q$. This means that $P\in A(K)\cap\ell^{\delta+1}A(K_{\ell^n})$, so $\ell^\delta P\in\ell^{\delta+1}A(K)$. So there is $R\in A(K)$ such that $\ell^{\delta+1}R=\ell^\delta P$. But then $T:=\ell R-P\in A[\ell^\delta](K)$ is such that $P+T=\ell R$, a contradiction. □

Remark 14. If A does not have complex multiplication, Serre's Open Image Theorem [3] assures the existence of a $\delta\geq 1$, depending only on the prime ℓ, such that the assumption of the theorem holds. Moreover we can take $\delta=1$ for almost all primes ℓ.

References

[1] T. Lawson, C. Wuthrich, *Vanishing of some Galois cohomology groups for elliptic curves*, preprint(?).

[2] J.-P. Serre, *Local Fields*.

[3] J.-P. Serre, *Propriétés galoisiennes de points d'ordre fini des courbes elliptiques*, 1972