Rational ℓ-multiples of points over the ℓ-torsion field

Sebastiano Tronto

January 11, 2019

Let ℓ be a rational prime and let A be an abelian variety of dimension d over a number field K. Let $K_\ell = K(A[\ell])$ and let $\mathcal{T}_1 = \mathrm{Gal}(K_\ell \mid K)$.

Remark 1. For $m \geq 1$ we have $\#\,\mathrm{GL}_m(\mathbb{F}_\ell) = \prod_{i=0}^{\ell-1}(\ell^m - \ell^i)$. In fact, elements of $\mathrm{GL}_m(\mathbb{F}_\ell)$ are in bijection with bases of $\mathbb{F}_\ell^m$, and counting basis of a vector space over a finite field is a simple combinatorics exercise: first we pick any non-zero vector ($\ell^n - 1$ possibilities), then we pick any vector that is not in the $\mathbb{F}_\ell$-span on the first one ($\ell^n - \ell$ possibilities), then a third one that is not in the span of the first two...

In particular, $v_\ell\left(\#\,\mathrm{GL}_m(\mathbb{F}_\ell)\right) = \frac{1}{2}m(m-1)$.

Compare the next lemma with [1], Lemma 3.7.

Lemma 2. *There is an exact sequence*

$$0 \to \ell A(K) \to A(K) \cap \ell A(K_\ell) \to H^1(\mathcal{T}_1, A[\ell]).$$

In particular, if $H^1(\mathcal{T}_1, A[\ell]) = 0$ we have $A(K) \cap \ell A(K_\ell) = \ell A(K)$.

Proof. Consider the short exact sequence of $\mathcal{T}_1$-modules

$$0 \to A[\ell](K_\ell) \to A(K_\ell) \to \ell A(K_\ell) \to 0$$

and the induced long exact sequence in cohomology (i.e. take $H^*(\mathcal{T}_1, -)$)

$$0 \to A[\ell](K) \to A(K) \to A(K) \cap \ell A(K_\ell) \to H^1(\mathcal{T}_1, A[\ell]) \to \cdots$$

and the thesis follows by noticing that $A(K)/A[\ell](K) \cong \ell A(K)$. □

This leads us to study the group $H^1(\mathcal{T}_1, A[\ell])$. In particular, we would like to know in which cases it is trivial (and so we are happy). In particular, the case of elliptic curves has been completely solved if $K = \mathbb{Q}$, and there are rather complete results if $K \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$ (see [2]).

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 $17739g1$. A gp script that finds all the 12 examples of elliptic curves with conductor $< 10^5$ with a generator of the free part of the group of rational points that becomes 3-divisible over K_3 can be found in `test3.gp`.

The question now becomes: "How much" can a point $\alpha \in A(K)$ become ℓ-divisible in $A(K_{\ell^\infty})$? That is, can we find an (explicit) N such that there is no $\beta \in A(K_{\ell^\infty})$ with $\alpha = \ell^n\beta$ for $n \geq N$?

(If we could say $A(K) \cap \ell A(K_{\ell^\infty}) = A(K) \cap \ell A(K_{\ell^{n_0}})$ for some n_0, then we could use Petsche's results to explicitly bound N in terms of the height of P)

References

[1] R. Jones, J. Rouse, *Galois Theory of Iterated Endomorphisms*, preprint(?).

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