CASSELS' LEMMA

PETE L. CLARK

Theorem 1. *(Cassels' Lemma) Let K be a complete local field with finite residue field $\mathbb{F}_q$. Let $\Psi : A \to A'$ be an isogeny of abelian varieties defined over K. We assume that A (hence also A') has good reduction and that* $\deg \Psi$ *is coprime to q. Then the image $\mathcal{K}$ of the Kummer map*

$$A'(K)/\Psi(A(K)) \to H^1(K, A[\Psi])$$

is equal to the subgroup $H^1(K^{\mathrm{unr}}/K, A[\Psi])$ of $H^1(K, A[\Psi])$ consisting of classes killed by restriction to the maximal unramified extension K^{unr} of K.

First proof: We have a commutative diagram with exact rows

$$0 \to A'(K)/\Psi(A(K)) \xrightarrow{\alpha} H^1(K, A[\Psi]) \xrightarrow{\beta} H^1(K, A)[\Psi] \to 0$$

$$0 \to A'(K^{\mathrm{unr}})/\Psi(A(K^{\mathrm{unr}})) \xrightarrow{\alpha'} H^1(K^{\mathrm{unr}}, A[\Psi]) \xrightarrow{\beta'} H^1(K^{\mathrm{unr}}, A)[\Psi] \to 0.$$

Step 1: Let $\xi \in H^1(K, A[\Psi])$ be a class which is in the image of the Kummer map; equivalently, $\beta(\xi) = 0$. We will show that $\operatorname{res} \xi = 0$. Because of the commutativity of the diagram, we have $\beta' \operatorname{res} \xi = \operatorname{res} \beta\xi = \operatorname{res} 0 = 0$. We claim that β' is injective, which suffices. Indeed, we will show:

Lemma 2. *With hypotheses above, we have*

$$A'(K^{\mathrm{unr}})/\Psi(A(K^{\mathrm{unr}})) = 0.$$

Proof. Since $A[\Psi] \subset A[\deg \Psi]$, it suffices to show the result for $\Psi = [n]$ on A with n a positive integer coprime to the residue characteristic, p. Let $\tilde{A}$ be the (good!) reduction of A modulo the maximal ideal of $\mathcal{O}_K$. We consider the base change to K^{unr}: reduction gives a short exact sequence

$$0 \to A^0(K^{\mathrm{unr}}) \to A(K^{\mathrm{unr}}) \to \tilde{A}(\overline{\mathbb{F}_q}) \to 0.$$

Certainly $\tilde{A}(\overline{\mathbb{F}_q})$, being the group of points of a connected group scheme over an algebraically closed field, is divisible. On the other hand, the theory of formal groups gives an isomorphism

$$A^0(K^{\mathrm{unr}}) \cong (\mathcal{O}_{K^{\mathrm{unr}}}, +) \bigoplus T_p,$$

where T_p is a p-primary torsion abelian group. Since n is a unit in the ring $\mathcal{O}_{K^{\mathrm{unr}}}$, its additive group is n-divisible. Therefore $A(K^{\mathrm{unr}})$, being an extension of n-divisible abelian groups, is itself n-divisible. □

Step 2: So far we know that $\mathcal{K}$, the image of the Kummer map, is a subgroup of $H^1(K^{\mathrm{unr}}/K, A[\Psi])$. It is easy to see that the latter is a finite abelian group – indeed, the set of continuous cocycles from the topologically cyclic group $\mathrm{Gal}(K^{\mathrm{unr}}/K)$ to the finite abelian group $A[\Psi]$ is finite. Hence $\mathcal{K}$ is also finite, and if $H \subset G$ are finite abelian groups, to show that $H = G$ it suffices to show that $\#H = \#G$.

We recall the following result of basic Galois cohomology of $\hat{\mathbb{Z}} = \mathrm{Gal}(K^{\mathrm{unr}}/K)$. If M is a finite $\hat{\mathbb{Z}}$-module, then

$$H^1(\hat{\mathbb{Z}}, M) \cong M/(F-1)M,$$

where F is the Frobenius map, the distinguished topological generator of $\hat{\mathbb{Z}}$. Reduction induces an isomorphism on the n-torsion, so $A[\psi](\overline{K}) = A[\psi](K^{\mathrm{unr}})$; we abbreviate this as $A[\psi]$ and write $A[\psi](K)$ for the subgroup of K-rational points, which is precisely the kernel of $F-1$. So we have

$$H^1(K^{\mathrm{unr}}/K, A[\Psi]) \cong A[\psi]/(F-1)A[\Psi].$$

Next a tiny piece of pure algebra: let M be a finite abelian group and φ an endomorphism of M. Then contemplation of the short exact sequence

$$0 \to \ker\varphi \to M \xrightarrow{\varphi} M \to \operatorname{coker}\varphi \to 0$$

gives $\#\ker\varphi = \#\operatorname{coker}\varphi$. Applying this with $M = A[\varphi]$ and φ equal to $F-1$, we get

$$\#H^1(K^{\mathrm{unr}}/K, A[\Psi]) = \#A[\Psi]/(F-1)A[\Psi] = \#\operatorname{coker}\varphi = \#ker\varphi = \#A[\Psi](K) = \#\tilde{A}[\Psi](\mathbb{F}_q).$$

On the other hand, because Ψ is surjective on the kernel of reduction, we have

$$\#\mathcal{K} = \#A'(K)/\Psi(A(K)) = \#\tilde{A}'(\mathbb{F}_q)/\tilde{\Psi}\tilde{A}(\mathbb{F}_q).$$

Note that since $\tilde{A}$ and $\tilde{A}'$ are $\mathbb{F}_q$-rationally isogenous, $\#\tilde{A}(\mathbb{F}_q) = \#\tilde{A}'(\mathbb{F}_q)$. Therefore, applying a similar counting argument to the exact sequence

$$0 \to \tilde{A}(\mathbb{F}_q)[\tilde{\Psi}] \to \tilde{A}(\mathbb{F}_q) \to \tilde{A}'(\mathbb{F}_q) \to \#\tilde{A}'(\mathbb{F}_q)/\tilde{\Psi}\tilde{A}(\mathbb{F}_q) = 0,$$

we conclude

$$\#H^1(K^{\mathrm{unr}}/K, A[\Psi]) = \#\tilde{A}(\mathbb{F}_q)[\tilde{\Psi}] = \#\tilde{A}'(\mathbb{F}_q)/\tilde{\Psi}\tilde{A}(\mathbb{F}_q) = \#\mathcal{K},$$

qed.