Lecture 14: Galois Cohomology of Abelian Varieties over Finite Fields

William Stein

Feb 12, 2010

See also Pete Clark's `http://math.uga.edu/~pete/wcnotes.pdf`.

1 Principal Homogenous Spaces for Abelian Varieties

An *abelian variety* A over a field k is a projective group variety, i.e., a projective variety that is equipped with a group structure $A \times A \to A$ and $1_A : k \to A$. Perhaps the first basic theorem about abelian varieties is that their group structure is commutative. We will not prove this here, since it requires too much algebraic geometry (for a complete proof readable by anybody who has read Hartshorne's *Algebraic Geometry*, see Milne's *Abelian Varieties* article in Cornell-Silverman).

A *principal homogenous space* for an abelian variety A over a field k is a variety X over k and a morphism $\iota : A \times X \to X$ that satisfies the axioms of a simply transitive group action.

If F is any field such that $X(F) \neq \emptyset$, then $A_F \approx X_F$, so we can view the principal homogenous spaces for A as twists of A as algebraic varieties (not as abelian varieties). Two principal homogenous spaces are equivalent if there is a morphism $X \to Y$ such that natural compatibility holds.

Given principal homomogenous spaces X and Y, the *Baer sum* defines a new principal homogenous space. Define an action of A on $X \times Y$ by $(a, x \times y) = (a, x) \times (-a, y)$. The Baer sum of X and Y is the quotient of $X \times Y$ by this action. The diagonal action $a.(x \times y) = ax \times ay$ then gives the Baer sum the structure of principal homogeneous space for A.

The collection of isomorphism classes of principal homomogenous spaces for a fixed abelian variety A over k equipped with Baer sum is an abelian group, called the *Weil-Chatalet* group of A, and denoted $\mathrm{WC}(A/k)$.

Theorem 1.1 (Lang-Tate, 1958)**.** *There is a natural isomorphism* $\mathrm{WC}(A/k) \to \mathrm{H}^1(k, A)$.

Sketch of Proof. Given a principal homogenous space X for A, we construct an element of $\mathrm{H}^1(k, A)$ as follows. Since X is a variety of positive dimension, there is a finite extension of k such that $X(F) \neq \emptyset$. Fix a choice of $P \in X(F)$. For $a \in A$ and $x \in X$, write $a + x$ for the image of (a, x) under the principal homogenous space map $A \times X \to X$. Define a map $f : G_k \to A$ by sending $\sigma \in G_k$ to

$$\sigma(P) - P$$

which means "the unique element $a \in A$ such that

$$a + P = \sigma(P).$$

The map f is a 1-cocycle because

$$f(\sigma) + \sigma f(\tau) = \sigma(P) - P + \sigma(\tau(P) - P) = \sigma(\tau(P)) - P = f(\sigma\tau),$$

where we have used the axioms that the principal homogenous space structure satisfy.

Conversely, constructing a principal homogenous space from a cycle f, is called "descent of the base field". The idea is that we find a finite extension F such that $f|_{G_F} = 0$, i.e., an extension that splits f. Then the data of (A_F, f_{G_F}) is "descent datum", which determines an algebraic variety X over k. See Serre *Algebraic Groups and Class Fields*, Section ???, for more details. □

Example 1.2. If A has dimension 1 then A is an elliptic curve. The principal homogenous spaces X for A are genus 1 curves with $\mathrm{Jac}(X) = A$. If A is defined over a number field k, then the nonzero elements of $Ш(A)$ are in bijection with the set of equivalence classes of principal homogenous spaces X such that $X(k_v) \neq \emptyset$ for all places v of k, yet $X(k) = \emptyset$. Thus $Ш(A)$ measures the obstruction to a local-to-global principal.

2 Galois Cohomology of Abelian Varieties over Finite Fields

Let A be an abelian variety over a finite field k.

The following theorem was proved by Lang in 1956. A more modern prove is given in the first few sections of Chapter VI of Serre's *Algebraic Groups and Class Fields*. Note that Lang actually proved a more general result about algebraic groups.

Theorem 2.1 (Lang, 1956)**.** *Let A be any connected algebraic group over a finite field (e.g., an abelian variety). Then $\mathrm{H}^1(k, A) = 0$.*

Proof. The following proof is based on what Pete Clark posted in the notes mentioned above. This proof has the advantage that it uses techniques that fit very nicely in the context of the rest of this course.

It suffices to show that $\mathrm{H}^1(k, A)[n] = 0$ for every positive integer n. The Kummer sequence associated to $0 \to A[n] \to A \to A \to 0$ is

$$0 \to A(k)/nA(k) \to \mathrm{H}^1(k, A[n]) \to \mathrm{H}^1(k, A)[n] \to 0.$$

It thus sufficies to prove that

$$\#(A(k)/nA(k)) = \#\,\mathrm{H}^1(k, A[n]).$$

We have an exact sequence of finite abelian groups

$$0 \to A(k)[n] \to A(k) \xrightarrow{[n]} A(k) \to A(k)/nA(k) \to 0.$$

Thus

$$\#A(k)[n] = \#(A(k)/nA(k)),$$

so now we just have to show that

$$\#\,\mathrm{H}^1(k, A[n]) = \#A(k)[n].$$

We have

$$\#\hat{\mathrm{H}}^0(F/k, A(F)[n]) = \#\hat{\mathrm{H}}^1(F/k, A(F)[n])$$

for all finite extensions F of k. In particular let F be any extension of $k(A[n])$ of degree divisible by n. Because the norm map is multiplicative in towers, we have

$$\mathrm{Tr}_{F/k}(A[n]) = \mathrm{Tr}_{k(A[n])/k}(\mathrm{Tr}_{F/k(A[n])}(A[n])) = \mathrm{Tr}_{k(A[n])/k}([n]A[n]) = \mathrm{Tr}_{k(A[n])/k}(0) = 0.$$

Thus

$$\hat{\mathrm{H}}^0(F/k, A[n](F)) = A(k)[n]/\mathrm{Tr}_{F/k}(A[n]) = A(k)[n],$$

where here we write Tr instead of the usual "norm" to denote the element $\sum \sigma^i$, where $\mathrm{Gal}(F/k) = \langle\sigma\rangle$. Thus for all finite extensions of F, we have

$$\#\hat{\mathrm{H}}^1(F/k, A[n](F)) = \#A(k)[n].$$

By taking compositums, we see that *every* extension of k is contained in a finite extension of F, so

$$\#\,\mathrm{H}^1(k, A[n]) = \#\varinjlim_{M/F} \hat{\mathrm{H}}^1(M/k, A[n]) = \#A(k)[n].$$

This proves the theorem. □

Remark 2.2. When A is an elliptic curve the Hasse bound and Theorem 1.1 imply the theorem. Indeed, any $X \in \mathrm{WC}(A/k)$ is a genus 1 curve over the finite field k, hence

$$|\#X - \#k - 1| \leq 2\sqrt{\#k}.$$

It follows that $\#X \geq \#k + 1 - 2\sqrt{\#k} > 0$.

We have the following incredibly helpful corollary:

Corollary 2.3. *If $0 \to A \to B \to C \to 0$ is an exact sequence of abelian varieties over a finite field k, then $0 \to A(k) \to B(k) \to C(k) \to 0$ is also exact.*

Proof. The cokernel of $B(k) \to C(k)$ is contained in $\mathrm{H}^1(k, A) = 0$. □

Example 2.4. Suppose E is an optimal elliptic curve quotient of $J = J_0(N)$ and $p \nmid N$ is a prime. Then for any integer $n \geq 1$, the induced natural map

$$J(\mathbb{F}_{p^n}) \to E(\mathbb{F}_{p^n})$$

is surjective. If $E[\ell]$ is irreducible, one can use Ihara's theorem to also prove that $J(\mathbb{F}_{p^2})^{\mathrm{ss}}(\ell) \to E(\mathbb{F}_{p^2})(\ell)$ is surjective, where $J(\mathbb{F}_{p^2})^{\mathrm{ss}}$ is the group generated by supersingular points.

Corollary 2.5. *We have $\mathrm{H}^q(k, A) = 0$ for all $q \geq 1$. (In fact, we have $\hat{\mathrm{H}}^q(k, A) = 0$ for all $q \in \mathbb{Z}$.)*

Proof. Suppose F is any finite extension of the finite field k. Then $\mathrm{Gal}(F/k)$ is cyclic, so by a result we proved before (lecture 13), we have

$$\#\hat{\mathrm{H}}^q(F/k, A(F)) = \#\hat{\mathrm{H}}^1(F/k, A(F)) = 1$$

for all $q \in \mathbb{Z}$. □

Corollary 2.6. *If F/k is a finite extension of finite fields, and A is an abelian variety, then the natural trace map*

$$\mathrm{Tr}_{F/k} : A(F) \to A(k)$$

is surjective.

Proof. By Corollary 2.5 and the definition, we have

$$0 = \hat{\mathrm{H}}^0(F/k, A(F)) = A(k)/\,\mathrm{Tr}_{F/k}(A(F)).$$

□

Let A be an abelian variety over a number field K, and v a prime of K, with residue class field $k = k_v$. The Néron model $\mathcal{A}$ of A is a smooth commutative group scheme over the ring $\mathcal{O}_K$ of integer of K with generic fiber A such that for all smooth commutative group schemes S the natural map

$$\mathcal{A}(S) \to A(S_K)$$

is an isomorphism. Reducing modulo v we have an exact sequence

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \Phi_{A,v} \to 0, \tag{2.1}$$

where $\mathcal{A}_k^0$ is the connected component that contains the identity and $\Phi_{A,v}$ is a finite flat group scheme over k, called the *component group* of A at v.

Proposition 2.7. *For every integer q, we have*

$$\hat{\mathrm{H}}^q(k, \mathcal{A}_k) = \hat{\mathrm{H}}^q(k, \Phi_{A,v}).$$

Proof. Take Galois cohomology associated to the exact sequence (2.1), and use Corollary 2.5. □