Attribution Key

for more information see: http://open.umich.edu/wiki/AttributionPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

PD-GOV **Public Domain – Government**: Works that are produced by the U.S. Government. (17 USC § 105)

PD-EXP **Public Domain – Expired**: Works that are no longer protected due to an expired copyright term.

PD-SELF **Public Domain – Self Dedicated**: Works that a copyright holder has dedicated to the public domain.

ZERO **Creative Commons – Zero Waiver**

BY **Creative Commons – Attribution License**

BY-SA **Creative Commons – Attribution Share Alike License**

BY-NC **Creative Commons – Attribution Noncommercial License**

BY-NC-SA **Creative Commons – Attribution Noncommercial Share Alike License**

GNU-FDL **GNU – Free Documentation License**

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

PD-INEL **Public Domain – Ineligible**: Works that are ineligible for copyright protection in the U.S. (17 USC § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

FAIR USE **Fair Use**: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (17 USC § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Lecture 4: Abelian varieties (algebraic theory)

This lecture covers the basic theory of abelian varieties over arbitrary fields. I begin with the basic results such as commutativity and the structure of torsion. Then I discuss the dual abelian variety. Next I prove the weak Mordell–Weil theorem, as the same ideas will be important for us later on. Last is Poincaré irreducibility, and its interpretation in terms of the isogeny category.

A good reference for today is Mumford's "Abelian varieties" (MR282985) or Milne's notes.

1 General facts about abelian varieties

Fix a field k. Many of the results about abelian varieties over $\mathbf{C}$ continue to hold over k. However, the proofs are quite different and more complicated. We give some indications as to how the theory is developed, but omit most of the arguments.

1.1 Commutativity

We begin by explaining the most basic fact: commutativity. One can establish this using an argument similar to the one we used in the complex case. We present a different argument here, which provides a more general result. It is based on the following general fact:

Theorem 1 (Rigidty Lemma)**.** *Let X be a complete variety, let Y and Z be arbitrary varieties, and let $f\colon X \times Y \to Z$ be a map of varieties. Suppose there exists $x_0 \in X$ and $y_0 \in Y$ such that the restriction of f to each of $X \times \{y_0\}$ and $\{x_0\} \times Y$ is constant. Then f is constant.*

Corollary 2. *Let X and Y be abelian varieties and let $f\colon X \to Y$ be any map of varieties such that $f(0) = 0$. Then f is a morphism of abelian varieties, i.e., it respects the group structure.*

Proof. Consider the map $h\colon X \times X \to Y$ given by $(x, y) \mapsto f(x+y) - f(x) - f(y)$. Then $h(x, 0) = h(0, x) = 0$ for all $x \in X$, and so by the Rigidity Lemma $h = 0$, i.e., f is a homomorphism. □

Corollary 3. *An abelian variety is commutative.*

Proof. The map $x \mapsto -x$ takes 0 to 0 and is therefore a homomorphism, which implies commutativity. □

1.2 Theorem of the cube

Theorem 4 (Theorem of the cube)**.** *Let X, Y, and Z be varieties, with X and Y complete, and let $x_0 \in X$, $y_0 \in Y$, and $z_0 \in Z$ be points. Let L be a line bundle on $X \times Y \times Z$, and suppose the restrictions of L to each of $X \times Y \times \{z_0\}$, $X \times \{y_0\} \times Z$, and $\{x_0\} \times Y \times Z$ are trivial. Then L is trivial.*

Remark 5. This can be thought of as a version of the rigidity lemma for maps to the stack $\mathrm{B}\mathbf{G}_m$. □

Corollary 6. *Let A be an abelian variety. Let $p_i\colon A \times A \times A \to A$ denote the projection map, and let $p_{ij} = p_i + p_j$ and $p_{123} = p_1 + p_2 + p_3$. Let L be a line bundle on A. Then the line bundle*

$$p_{123}^* L \otimes p_{12}^* L^{-1} \otimes p_{13}^* L^{-1} \otimes p_{23}^* L^{-1} \otimes p_1^* L \otimes p_2^* L \otimes p_3^* L$$

on $A \times A \times A$ is trivial.

These are notes for Math 679, taught in the Fall 2013 semester at the University of Michigan by Andrew Snowden.

Proof. This follows immediately from the theorem of the cube. For example, if we restrict to $A \times A \times \{0\}$ then $p_{123}^* L = p_{12}^* L$, $p_{13}^* L = p_1^* L$, and $p_3^* L = 1$, so all factors cancel. $\square$

Corollary 7. *Let A be an abelian variety, let X be any variety, let $f, g, h \colon X \to A$ be maps, and let L be a line bundle on A. Then the line bundle*

$$(f+g+h)^* L \otimes (f+g)^* L^{-1} \otimes (f+h)^* L^{-1} \otimes (g+h)^* L^{-1} \otimes f^* L \otimes g^* L \otimes h^* L$$

on X is trivial.

Proof. This follows from the previous corollary by considering the map $X \to A \times A \times A$ given by (f, g, h). $\square$

1.3 Structure of torsion

Proposition 8. *Let L be a line bundle on an abelian variety A. Then*

$$[n]^* L = L^{(n^2+n)/2} \otimes [-1]^* L^{(n^2-n)/2}.$$

In particular, if L is symmetric ($[-1]^* L = L$) then $[n]^* L = L^{n^2}$, while if L is anti-symmetric ($[-1]^* L = L^{-1}$) then $[n]^* L = L^n$.

Proof. Applying Corollary 7 to the maps $[n]$, $[1]$, and $[-1]$, we find

$$[n]^* L \otimes [n+1]^* L^{-1} \otimes [n-1]^* L^{-1} \otimes [n]^* L \otimes L \otimes [-1]^* L$$

is trivial. In other words,

$$[n+1]^* L = [n]^* L^2 \otimes [n-1]^* L^{-1} \otimes L \otimes [-1]^* L.$$

The result now follows by induction. $\square$

Proposition 9. *The map $[n]$ is an isogeny, i.e., it is surjective with finite kernel.*

Proof. One can show that abelian varieties are projective. Let L be an ample line bundle on A. Replacing L by $L \otimes [-1]^* L$, we can assume L is symmetric. Since $[n]^* L = L^{n^2}$, it is ample. However, the restriction of this to the n-torsion is obviously trivial. Since the n-torsion is a complete variety on which the trivial bundle is ample, it must be finite. This implies that $[n]$ is surjective, by reasoning with dimension. $\square$

Proposition 10. *The degree of $[n]$ is n^{2g}.*

Proof. Let $f \colon X \to Y$ be a finite map of complete varieties of degree d. If $D_1, \ldots, D_n$ are divisors on Y, where $n = \dim(X) = \dim(Y)$, then there is an equality of intersection numbers:

$$(f^* D_1 \cdots f^* D_n) = d(D_1 \cdots D_n).$$

Now, let D be an ample divisor such that $[-1]^* D$ is linearly equivalent to D (e.g., the divisor associated to the line bundle used above). Then $[n]^* D$ is linearly equivalent to $n^2 D$. We thus find

$$\deg([n])(D \cdots D) = ((n^2 D) \cdots (n^2 D)) = n^{2g}(D \cdots D).$$

Since D is ample, $(D \cdots D) \neq 0$, and thus $\deg([n]) = n^{2g}$. $\square$

One can show that $[n]\colon A \to A$ induces multiplication by n on the tangent space. This shows that $[n]$ is separable if and only if n is prime to the characteristic. Combined with the above (and the usual induction argument), we see that:

Corollary 11. *If n is prime to the characteristic, then $A[n](\overline{k})$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^{2g}$.*

Corollary 12. *If ℓ is a prime different from the characteristic then $T_\ell A$ is isomorphic to $\mathbf{Z}_\ell^{2g}$.*

Since $[p]$ is not separable, $A[p](\overline{k})$ must have fewer than p^{2g} points. In fact, we when we study group schemes we will see that it can have at most p^g points.

1.4 Theorem of the square

Theorem 13 (Theorem of the square)**.** *Let L be a line bundle on an abelian variety A, and let x and y be two points of A. Then*

$$t_{x+y}^*L \otimes L = t_x^*L \otimes t_y^*L.$$

Here t_x denotes translation by x.

Proof. Apply the f, g, h proposition with $f = x$ (constant map), $g = y$, and $h = \mathrm{id}$. $\square$

Define $\mathrm{Pic}(A)$ to be the set of isomorphism classes of line bundles on A. For a line bundle L, let $\phi_L\colon A(k) \to \mathrm{Pic}(A)$ be the map $\phi_L(x) = t_x^*L \otimes L^{-1}$. The theorem of the square exactly states that ϕ_L is a group homomorphism.

2 The dual variety

Over the complex numbers, we can write an abelian variety A as V/M, where V is a complex vector space and M is lattice. We defined the dual abelian variety $A^\vee$ as $\overline{V}^*/M^\vee$. We would like to be able to define the dual variety over any field, but this definition obviously does not carry over. The key idea is to reinterpret $A^\vee$ in terms of line bundles.

Recall that over $\mathbf{C}$ we showed that the set $A^\vee$ was canonically in bijection with the set $\mathrm{Pic}^0(A)$. Furthermore, although our definition of $\mathrm{Pic}^0(A)$ was originally topological (and does not generalize to other fields), we characterized $\mathrm{Pic}^0(A)$ as the translation invariant line bundles (which does generalize to other fields). We therefore have a possible method of defining the dual.

2.1 Definition of the dual

Let k be an arbitrary field, and let A be an abelian variety over k. We defined $\mathrm{Pic}(A)$ above to be the set of isomorphism classes of line bundles on A. We now define $\mathrm{Pic}^0(A)$ to be the subgroup consisting of those line bundles L which are translation invariant, i.e., which satisfy $t_x^*(L) \cong L$ for all $x \in A$. Motivated by the complex case, we want to define $A^\vee$ to be an abelian variety with point-set $\mathrm{Pic}^0(A)$. However, it is not good enough to just define the points of a variety over a field: we must define its functor of points.

For a variety T, let $F(T)$ be the of isomorphism classes of line bundles L on $A \times T$ satisfying the following two conditions: (a) for all $t \in T$, the restriction of L to $A \times \{t\}$ belongs to $\mathrm{Pic}^0(A)$; and (b) the restriction of L to $\{0\} \times T$ is trivial. Thus $F(k) = \mathrm{Pic}^0(A)$. We define the dual abelian variety $A^\vee$ to be the variety that represents F, if it exists. If it does exist, then it automatically comes with a universal bundle $\mathcal{P}$ on $A \times A^\vee$, which is called the Poincaré bundle.

2.2 Construction of the dual

Let L be an ample bundle on A. We then have the map $\phi_L\colon A \to \mathrm{Pic}^0(A)$. (The theorem of the square implies the image is in Pic^0.) Over the complex numbers, we saw that this map was an isogeny of tori. In general, one can prove the it is surjective, and has finite kernel $K(L)$. In fact, one can give $K(L)$ a natural scheme structure. This suggests that $A^\vee$ should be the quotient $A/K(L)$, and one can show that this is indeed the case.

2.3 Another approach to the dual

Let L be in $\mathrm{Pic}^0(A)$. Then, by definition, $t_x^*(L)$ and L are isomorphic for all $x \in A$. Choose an isomorphism ϕ_x. Then $\phi_y t_y^*(\phi_x)$ and ϕ_{x+y} are two isomorphisms $t_{x+y}^*(L) \to L$, and thus differ by an element $\alpha_{x,y}$ of $\mathrm{Aut}(L) = \mathbf{G}_m$. It is obvious that α is a 2-cocycle of A with coefficients in $\mathbf{G}_m$, and thus defines a central extension $\mathcal{G}(L)$ of A by $\mathbf{G}_m$. In fact, $\mathcal{G}(L)$ is a commutative group.

Here is a different construction of $\mathcal{G}(L)$. One can show that L being translation invariant is equivalent to $p_1^*L \otimes p_2^*L$ being isomorphic to m^*L, where m is the multiplication map $A \times A \to A$ and p_i are the projection maps. The fiber at (x, y) of this isomorphism is an identification $L_x \otimes L_y \to L_{x+y}$. In other words, there is a natural map $L \times L \to L$ (identifying L with its total space) over the multiplication map on A. The group $\mathcal{G}(L)$ is then just L minus its zero section, with this multiplication.

We have thus constructed a map $\mathcal{G}\colon \mathrm{Pic}^0(A) \to \mathrm{Ext}^1(A, \mathbf{G}_m)$, where Ext^1 is taken in the category of commutative group varieties. Serre showed (MR0103191, Chapter VII, Section 3) that this map is an isomorphism. Forming Ext^1 in the category of fppf sheaves allows one to recover the functor of points of $A^\vee$.

3 The Mordell–Weil theorem

Theorem 14 (Mordell–Weil)**.** *Let A be an abelian variety over the number field K. Then $A(K)$ is a finitely generated abelian group.*

The proof of this theorem usually proceeds in two steps: first, one shows that $A(K)/nA(K)$ is a finite group (the so-called weak Mordell–Weil theorem), and then one uses height functions to deduce the theorem. We will only discuss the proof of the first step. A complete proof, in the case of elliptic curves, is given in Chapter VII of Silverman's "The arithmetic of elliptic curves" (MR0817210).

Consider the exact sequence

$$0 \to A[n](\overline{K}) \to A(\overline{K}) \xrightarrow{n} A(\overline{K}) \to 0.$$

Taking Galois cohomology, one obtains an exact sequence

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

This is called the Kummer sequence, and is very important. To show that $A(K)/nA(K)$ is finite, it suffices to show that the middle cohomology group is finite. This is not quite true; however, one can show that the image of the first map only hits classes which are unramified outside a fixed finite set of places S, and so it's enough to establish finiteness for such classes, which is true. (The set S can be taken to be the set of places of bad reduction for A, together with those places above n.)

Let L/K be a finite Galois extension containing all the n-torsion of A, and enlarge S so that L/K is unramified outside S. Then one has the inflation–restriction sequence:

$$0 \to \mathrm{H}^1(\mathrm{Gal}(L/K), A[n](\overline{K})) \to \mathrm{H}^1(G_{K,S}, A[n](\overline{K})) \to \mathrm{H}^1(G_{L,S}, A[n](\overline{K})),$$

and so to prove finiteness of the middle group it suffices to prove finiteness of the outer groups. Finiteness of the group on the left comes for free, since $\mathrm{Gal}(L/K)$ and $A[n](\overline{K})$ are both finite. Since $G_{L,S}$ acts trivially on $A[n](\overline{K})$, the right group is just $\mathrm{Hom}(G_{L,S}, \mathbf{Z}/n\mathbf{Z})^{2g}$. Giving a map $G_{L,S} \to \mathbf{Z}/n\mathbf{Z}$ is (almost) the same as giving a $\mathbf{Z}/n\mathbf{Z}$ extension of L unramified outside of S. Since there are only finitely many such extensions unramified, the finiteness result follows.

4 Structure of the isogeny category

4.1 Poincaré reducibility

Theorem 15 (Poincaré reducibility)**.** *Let A be an abelian variety, and let B be an abelian subvariety. Then there exists an abelian subvariety C such that $B \cap C$ is finite and $B \times C \to A$ is an isogeny.*

Proof. Choosing polarizations on A and A/B to identify them with their duals, the dual to the quotient map $A \to A/B$ is a map $A/B \to A$. We let C be its image. The properties are easy to verify. □

We say that an abelian variety A is simple if the only abelian subvarieties are 0 and A.

Corollary 16. *Every abelian variety is isogenous to a product of simple varieties.*

4.2 The isogeny category

Define a category Isog as follows. The objects are abelian varieties. For two abelian varieties A and B, we put $\mathrm{Hom}_{\mathrm{Isog}}(A, B) = \mathrm{Hom}(A, B) \otimes \mathbf{Q}$. One can show that if $f \colon A \to B$ is an isogeny then there exists an isogeny $g \colon B \to A$ such that $gf = [n]$, for some n; it follows that $\frac{1}{n}g$ is the inverse to f in Isog. Thus isogenies become isomorphisms in Isog.

It is not difficult to see that Isog is in fact an abelian category. The simple objects of this category are exactly the simple abelian varieties. Poincar's theorem shows that Isog is semi-simple as an abelian category.

From this formalism, and general facts about abelian varieties, we deduce two results:

- The decomposition (up to isogeny) into a product of simple abelian varieties is unique (up to isogeny). (Reason: in any semi-simple abelian category, the decomposition into simples is unique up to isomorphism.)

- If A is a simple abelian variety then $\mathrm{End}(A) \otimes \mathbf{Q}$ is a division algebra over $\mathbf{Q}$. (Reason: if A is a simple object in an abelian category and $\mathrm{End}(A)$ contains a field k, then it is a division algebra over k.)