Algebraic geometry

Lectures delivered by Xinwen Zhu
Notes by Akhil Mathew

Spring 2012, Harvard

Contents

Introduction

Xinwen Zhu taught a course (Math 232b) on the geometry of algebraic curves at Harvard in Spring 2012. These are my "live-TEXed" notes from the course.

Conventions are as follows: Each lecture gets its own "chapter," and appears in the table of contents with the date.

Of course, these notes are not a faithful representation of the course, either in the mathematics itself or in the quotes, jokes, and philosophical musings; in particular, the errors are my fault. By the same token, any virtues in the notes are to be credited to the lecturer and not the scribe.

Please email corrections to `amathew@college.harvard.edu`.

Lecture 1
2/6

This is the first meeting of Math 232b. This class will continue into reading period because we started two weeks late. This semester, we're trying to study abelian varieties.

§1 Indefinite integrals

What I say today is going to be kind of vague, without proofs, but we will come back to rigorous mathematics next time. Consider the integral

$$\int \frac{dx}{\sqrt{1-x^2}}.$$

It is known that this indefinite integral can be represented as $\sin^{-1}(x) + C$, and so the trigonometric functions can be used to solve it. Consequently, if we consider the definite integral

$$\int_0^u \frac{dx}{\sqrt{1-x^2}} + \int_0^u \frac{dx}{\sqrt{1-x^2}}$$

we can write it as:

$$\int_0^{F(u,v)} \frac{dx}{\sqrt{1-x^2}}$$

for some function $F(u,v) = u\sqrt{1-v^2} + v\sqrt{1-u^2}$.

Later on, people were interested in the circumference of more complicated curves:

1. The lemniscate defined by $(x^2+y^2)^2 = x^2 - y^2$.
2. Ellipses (defined by $\frac{x^2}{u^2} + \frac{y^2}{v^2} = 1$.

To calculate the length, one had to calculate integrals of the form

$$\int \frac{dx}{\sqrt{1-x^4}}, \quad \int \frac{1-k^2x^2}{\sqrt{p(x)}}dx,\ p(x) = (1-x^2)(1-k^2x^2).$$

It is known that such integrals (called *elliptic integrals*) cannot be done in terms of elementary functions.

However, Euler was still able to construct addition formulas for the elliptic integrals. Consider the integral $\int_0^u \frac{dx}{\sqrt{p(x)}}$ where $p(x)$ is a degree four polynomial of the above form $p(x) = (1-x^2)(1-k^2x^2)$.

Euler proved the **addition formula**:

$$\int_0^u \frac{dx}{\sqrt{p(x)}} + \int_0^v \frac{dx}{\sqrt{p(x)}} = \int_0^{F(u,v)} \frac{dx}{\sqrt{p(x)}} \tag{1}$$

where $F(u,v) = \frac{u\sqrt{p(v)}+u\sqrt{p(u)}}{1-k^2u^2v^2}$.

If we use the modern point of view of algebraic geometry, we can see why the addition formula exists. Consider the algebraic curve E given by $y^2 = p(x)$; there is a *group law* on E given by

$$(u, \sqrt{p(u)}) \oplus (v, \sqrt{p(v)}) := (F(u,v), \sqrt{p(F(u,v))}$$

and E is in fact an elliptic curve. The Jacobi form of an elliptic curve is $y^2 = (1 - x^2)(1 - k^2x^2)$ as given. (**N.B.** We all were a bit confused, expecting a cubic equation for an elliptic curve.)

We can also define the **Abel-Jacobi map** $E \to \mathbb{C}$ given by

$$(u, \sqrt{p(u)}) \to \int_0^u \frac{dx}{\sqrt{p(x)}}.$$

When we define such a map, it is a *group homomorphism.* However, you have to be careful, because when you integrate this, you're integrating a meromorphic function with poles at $\pm 1, \pm \frac{1}{k}$. So when you integrate from 0 to u, you should choose a path not passing through the poles.

So, more properly, the Abel-Jacobi map is a map

$$AJ : E \to \mathbb{C}/L$$

for L the *period lattice* $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. What you really get is that the integral is well-defined when considered as an element of a certain complex torus. This map is an *isomorphism*, and represents the algebraic curve E as a complex torus. Thus, the complex torus acquires the structure of an algebraic variety.

§2 Abel's work

Later on, Abel generalized this elliptic integral to more complex integrals, so-called abelian integrals. Let us state it in modern language. Let X be an algebraic curve of genus $g \geq 1$.

If you really try to understand the Abel-Jacobi map as before, we consider the group $\mathrm{Pic}^0(X)$ of divisor classes on X of degree zero, and we get a map

$$AJ : \mathrm{Pic}^0(X) \to H^0(X, \Omega_X)^\vee / L$$

as follows. Given a divisor $\sum p_i - q_i$ on X of degree zero, it goes to the map $H^0(X, \Omega_X) \to \mathbb{C}$ sending a global differential ω to $\sum_i \int_{p_i}^{q_i} \omega$. As before, the map is only well-defined modulo a certain lattice[1] L, because there are many paths connecting p_i and q_i. The lattice L is the image of $H_1(X, \mathbb{Z}) \to H^0(, \Omega_X)^\vee$, where the map just given is integration along a path. This is a well-defined map, and it induces an *isomorphism.* From its definition, it is an isomorphism of groups.

1.1 Definition. We denote $H^0(X, \Omega_X)^\vee / L$ by $J(X)$ and call it the **Jacobian variety** of X.

[1] It will be briefly seen below that L is a lattice.

In fact:

1.2 Theorem. *$J(X)$ is a compact complex torus, and has a natural (unique) structure as a projective variety.*

The first part of the theorem is a little bit of Hodge theory, but the second part is much more complicated. Today, let's just give a sketch of what's going on. We need to show that the image of

$$H_1(X;\mathbb{Z}) \to H^0(X,\Omega_X)^\vee \tag{2}$$

is in fact a lattice. This is because there is a map $H_1(X,\mathbb{Z}) \to H^1_{DR}(X;\mathbb{R})^\vee$ by the same pairing (integration), and this imbeds $H_1(X;\mathbb{Z})$ is a lattice inside $H^1_{DR}(X;\mathbb{R})^\vee$. However, by a little Hodge theory, we have

$$H^1(X;\mathbb{R}) \simeq H^0(X,\Omega_X).$$

This map is compatible with (2).

Now we use the following criterion for when a complex torus is algebraic:

1.3 Theorem. *Let $\dim_{\mathbb{C}} V = n$. Let $Y = V/\Lambda$ for $\Lambda \subset V$ a lattice, so Y is a compact complex manifold. Then the following are equivalent:*

1. *Y can be imbedded into a projective space.*
2. *There exists an algebraic variety X and an isomorphism of analytic spaces $X^{an} \simeq Y$ (i.e., Y comes from an algebraic variety).*
3. *There exist n algebraically independent meromorphic functions on Y.*
4. *There exists a positive-definite hermitian form $H : V \times \overline{V} \to \mathbb{C}$ such that $\Im H|_\Lambda$ takes values in $\mathbb{Z}$.*

Using this theorem, let's see (loosely) why the Jacobian $J(X)$ admits the structure of an algebraic variety. The fourth statement of the quoted theorem is the easiest, so let's try to find a hermitian form on $H^0(X,\Omega_X)^\vee$ satisfying the above properties. So, we'll need a lemma from linear algebra:

1.4 Lemma. *Let V be a complex vector space and let $V_{\mathbb{R}}$ be the underlying real vector space. There is a one-to-one bijection between hermitian forms on V and symplectic*[2] *forms on $V_{\mathbb{R}}$ such that $\omega(ix,iy) = \omega(x,y)$.*

Proof. The construction sends H to $\omega := \Im H$. ▲

As a result, to see that $J(X)$ is an algebraic variety, we need to construct a symplectic pairing

$$H_1(X,\mathbb{Z}) \times H_1(X,\mathbb{Z}) \to \mathbb{Z}$$

which satisfies certain properties to be elucidated. If we have such a symplectic pairing, it gives a hermitian form on $H^0(X,\Omega_X)^\vee = H_1(X,\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C}$ and the corresponding hermitian form takes integral values on the lattice. The required properties should imply that the corresponding hermitian form is positive-definite. This pairing will be given by the intersection pairing.

[2] Here we use "symplectic" to mean skew-symmetric, not necessarily nondegenerate.

§3 Abelian varieties

Given an algebraic curve X, we saw that we can get a Jacobian variety $J(X)$. It is a complex torus (so that it has a natural group structure), and it also has the structure of a projective variety. These two structures are in fact compatible with each other: the addition law is a morphism between algebraic varieties.

This motivates:

1.5 Definition. An **abelian variety over** $\mathbb{C}$ is a projective variety X with a group law in the category of varieties, i.e. a multiplication law and an inversion law which are morphisms of algebraic varieties.

1.6 Example. To each algebraic curve X, we get an abelian variety $J(X)$.

1.7 Example (Relevant in number theory)**.** Consider a totally real extension $F/\mathbb{Q}$ (where F is a number field), $[F : \mathbb{Q}] = g$. Let E/F be a quadratic imaginary extension. In this case, we say that $E/\mathbb{Q}$ is a **CM field.**

We consider the set of field imbeddings $\mathrm{Hom}(E, \mathbb{C})$; this set will have exactly $2g$ elements and there is a natural action of complex conjugation on the set. Namely, if you have an imbedding $i : E \to \mathbb{C}$, you can post-compose it with complex conjugation. We digress for a definition.

1.8 Definition. A **CM type** is a choice of $\Phi \subset \mathrm{Hom}(E, \mathbb{C})$ such that $|\Phi| = g$ and $\Phi \cup \overline{\Phi} = \mathrm{Hom}(E, \mathbb{C})$. In other words, we choose one element of each orbit of the conjugation action.

If we consider $E \otimes_{\mathbb{Q}} \mathbb{R}$, then via this choice of Φ, we get an isomorphism

$$E \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{C}^{\Phi}, \quad (e \otimes r) \mapsto (r\phi(e))_{\phi \in \Phi}$$

Inside here we have the ring of integers $\mathcal{O}_E$, which is a lattice. In fact, we have:

1.9 Theorem. *$\mathbb{C}^{\Phi}/\mathcal{O}_F$ is an abelian variety.*

To prove this, again, we need a hermitian pairing on $\mathcal{O}_F$, whose restriction to the lattice has integral imaginary parts. A sketch of the proof is as follows. Choose $\alpha \in \mathcal{O}_E$ totally imaginary in E, and such that $\Im \phi(\alpha)$, the imaginary part, is positive for $\phi \in \Phi$. (This is possible by the "approximation theorem.") Define a pairing

$$E \times E \to \mathbb{Q}, \quad (x, y) \mapsto \mathrm{Tr}_{E/\mathbb{Q}}(\alpha x y^*)$$

where $*$ is the automorphism of E over F. When restricted to $\mathcal{O}_E \times \mathcal{O}_E$, it lands in $\mathbb{Z}$. It's an exercise (in number theory) to see that gives a positive-definite hermitian form on $E \otimes_{\mathbb{Q}} \mathbb{R}$. These abelian varieties have **complex multiplication.**

Let's now go back to some more concrete examples in dimension one.

1.10 Example. Let $\Gamma \subset \mathbb{C}$ be *any* lattice; then $\mathbb{C}/\Lambda$ is an abelian variety. In dimension one, there are no restrictions on the lattice.

Proof. Write $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ for $\tau \in \mathbb{C}, \Im\tau > 0$ (by rescaling we can do this). Define a hermitian form

$$H : \mathbb{C} \times \mathbb{C} \to \mathbb{C}, \quad (z, w) \mapsto H(z, w) := \frac{z\overline{w}}{\Im\tau}.$$

This is clearly positive-definite and you can check that $\Im H(1, 1) = \Im H(\tau, \tau) = 0, \Im H(\tau, 1) = -1$. This means that $\Im H|_\Lambda$ takes values in $\mathbb{Z}$, so by the theorem, we're done. ▲

There are two questions now.

1. Is it true for any lattice $\Lambda \subset \mathbb{C}^n, n > 1$, the manifold $\mathbb{C}^n/\Lambda$ is an abelian variety?
2. Are all abelian varieties complex tori?

It turns out that the answer to the question to the first question is no, and that the answer to the second question is yes. In fact, even for any $n > 2$, the quotient $\mathbb{C}^n/\Lambda$ is almost always *not* an abelian variety (as Λ varies). It's a good exercise to show that for $n = 2$ using the lattice condition. The answer to the second question is yes, and we'll begin with that next time.

Lecture 2
2/8

§1 Abelian varieties are complex tori

Last time, we defined an **abelian variety** over $\mathbb{C}$ to be a projective variety equipped with a group law. All the examples we gave were of the form V/Λ for V is a complex vector space and $\Lambda \subset V$ a lattice, i.e. a free abelian subgroup of maximal rank $2\dim_{\mathbb{C}} V$. The natural question we asked last time was whether every abelian variety was of this form. In fact:

2.1 Proposition. *Let X be a connected compact complex Lie group; then X must be of the form V/Λ as above. In particular, any abelian variety*[3] *must be of this form.*

Proof. We should first show that X is commutative. Let V be the Lie algebra $\mathrm{Lie}(X)$; this is a vector space of dimension $n = \dim_{\mathbb{C}} X$. We want to show that X is commutative, so we look at the adjoint representation

$$\mathrm{Ad} : X \to \mathrm{GL}(V), \quad g \mapsto \mathrm{Ad}_g(\xi) := g\xi g^{-1}.$$

This action comes from the conjugation action of X on itself; each $g \in X$ acts on X via $h \mapsto ghg^{-1}$. The differential at the identity of this conjugation action gives the adjoint representation Ad.

Anyway, the point of this construction is that the adjoint representation is a holomorphic map, because we are working with *complex* Lie groups. But X is compact, and $\mathrm{GL}(V)$ is "affine," so any holomorphic map $X \to \mathrm{GL}(V)$ is constant. (In fact, any holomorphic map from X to a complex vector space—e.g. $\mathrm{End}(V)$—is constant, by

[3] Any abelian variety gives via analytification a compact complex Lie group.

looking at coordinates: any holomorphic function on a compact complex manifold is constant.) Therefore, the adjoint representation must be trivial.

Since the adjoint representation is trivial, and the group is connected, the conjugation action of X on itself must be trivial. In particular, X is commutative. In general, if you have a connected compact Lie group, it is a torus. Let's recall the proof. There is always a morphism

$$\exp : T_e(X) = V \to X$$

which is normally just a smooth (or holomorphic) map, but when X is commutative this is actually a group homomorphism. It is in fact a covering map, since the differential at e is the identity. It follows that $X \simeq V/\Lambda$ for $\Lambda \subset V$ discrete, and Λ is of full rank by compactness of X. ▲

In some sense, the examples we gave of complex abelian varieties are kind of general: all of them are of this form, V/Λ. In particular, the topology of a complex abelian variety is easy.

2.2 Corollary. *Let X be an abelian variety over $\mathbb{C}$ (or more generally a complex torus) of dimension g. Then X is commutative and divisible. Multiplication by n, $n_X : X \to X$, is a surjective group homomorphism whose kernel is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$.*

Proof. In fact, the kernel of multiplication by n is precisely $\frac{1}{n}\Lambda/\Lambda \subset V/\Lambda$. ▲

We can also deduce:

2.3 Corollary. $\pi_1(X) \simeq H_1(X;\mathbb{Z}) \simeq \Lambda \simeq \mathbb{Z}^{2g}$.

2.4 Corollary. *Let X, Y be abelian varieties, and let $\operatorname{Hom}(X,Y)$ be the group of morphisms of complex Lie groups.*[4] *The natural map*

$$\operatorname{Hom}(X,Y) \to \operatorname{Hom}(H_1(X;\mathbb{Z}), H_1(Y;\mathbb{Z}))$$

is injective.

Proof. The reason is simply that if $X = V_X/\Lambda_X, Y = V_Y/\Lambda_Y$, then

$$\operatorname{Hom}(X,Y) \subset \operatorname{Hom}_{\mathbb{C}}(V_X, V_Y)$$

is the collection of maps which take $\Lambda_X = H_1(X;\mathbb{Z})$ to $\Lambda_Y = H_1(Y;\mathbb{Z})$. ▲

Remark. The map $\operatorname{Hom}(X,Y) \to \operatorname{Hom}(H_1(X;\mathbb{Z}), H_1(Y;\mathbb{Z}))$ is not bijective. A map on homology groups $\Lambda_X \to \Lambda_Y$ induces a map of $\mathbb{R}$-vector spaces $\Lambda_X \otimes_{\mathbb{Z}} \mathbb{R} \to \Lambda_Y \otimes_{\mathbb{Z}} \mathbb{R}$, but it's not necessarily a morphism of $\mathbb{C}$-vector spaces.

[4] Recall that every holomorphic map between projective varieties is algebraic.

§2 Abelian varieties over general fields

Now we're going to switch to a more general situation.

2.5 Definition. An **abelian variety** over the field k is a smooth, complete (i.e. proper[5]) k-variety X together with a multiplication map

$$m : X \times X \to X$$

and an inverse map

$$i : X \to X$$

and a k-point

$$e : \mathrm{Spec} k \to X$$

such that X forms a group object with these multiplication, inversion, and identity maps.

2.6 Definition. Let X, Y be two abelian varieties over k. Then a **homomorphism** $f : X \to Y$ is a morphism of algebraic varieties which commutes with the various structure maps. In other words, we should have commutative diagrams of the following form:

$$\begin{tikzcd} X \times X \arrow[r, "m"] \arrow[d, "f\times f"] & X \arrow[d, "f"] \\ Y \times Y \arrow[r, "m"] & Y \end{tikzcd}.$$

We can thus form a *category* of abelian varieties and homomorphisms, which we denote by $\mathbf{AV}_k$.

§3 Natural questions

What kinds of questions do we want to study?

1. What is the group structure on $X(\overline{k})$, the set of geometric points?

   We will later prove that $X(\overline{k})$ is a commutative, divisible group and the multiplication-by-n map $n_X : X \to X$ is a group homomorphism whose kernel on $\overline{k}$-points is

   $$\ker n_X = \begin{cases} (\mathbb{Z}/n\mathbb{Z})^{2g} & \text{if } p := \mathrm{char} k \nmid n \\ (\mathbb{Z}/p^m\mathbb{Z})^i & \text{if } n = p^m,\ 0 \le i \le g. \end{cases}$$

   We have already seen this for $k = \mathbb{C}$.

2. The structure of the k-points is harder. The *Mordell-Weil theorem* states that if k is a number field, then $X(k)$ is a finitely generated abelian group. We may or may not be able to prove this result, depending on time constraints.

[5] We will later show that this implies projectivity.

3. What is $\mathrm{Hom}(X, Y)$? We said something about this when X, Y were complex abelian varieties. This is an abelian group (since Y is a commutative group object), and we might ask about the structure of this group. We saw that when $k = \mathbb{C}$, $\mathrm{Hom}(X, Y)$ is a finitely generated, *free* abelian group (a subgroup of $\mathrm{Hom}_{\mathrm{Ab}}(H_1(X; \mathbb{Z}), H_1(Y; \mathbb{Z}))$.

   We will see that, in general, $\mathrm{Hom}(X, Y)$ is a finitely generated free abelian group, not just for $k = \mathbb{C}$.

   Here is the idea. Let $l \neq p = \mathrm{char} k$ be a prime. We can consider the kernel

   $$X[l^n] := \ker l_X^n \subset X(\overline{k}) \simeq (\mathbb{Z}/l\mathbb{Z})^{2g}.$$

   This is a finite abelian group with an action of the Galois group $\mathrm{Gal}(\overline{k}/k)$. and there is a natural map

   $$X[l^{n+1}] \xrightarrow{l_X} X[l^n].$$

   2.7 Definition. The **l-adic Tate module** $T_l(X) := \varprojlim X[l^n]$; this is a free $\mathbb{Z}_l$-module (of rank $2g$) with a continuous action of the Galois group.

   The Tate module is somehow the replacement for the first homology group for an abelian variety. We have the following:

   2.8 Theorem. *If $f : X \to Y$ is a morphism of abelian varieties, it induces a map $T_l(f) : \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))$. The induced map*

   $$\mathrm{Hom}(X, Y) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))$$

   is injective.

   The proof of this result is much harder than the complex analog. Determining the image is tricky. The image has to lie in the collection of Galois-equivariant homomorphisms $T_l(X) \to T_l(Y)$, so we get a map

   $$\mathrm{Hom}(X, Y) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))^{\mathrm{Gal}} \tag{3}$$

   The famous *Tate conjecture* states the following:

   Tate conjecture: If k is finitely generated over its prime field, then the map $\mathbb{Z}_l \otimes \mathrm{Hom}(X, Y) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))^{\mathrm{Gal}}$ obtained from (3) is an isomorphism.

   Tate's conjecture is true when $k = \mathbb{F}_q$ (as proved by Tate), and when k is a number field (Faltings). The proofs are quite difficult, and depend a lot on the structure of the Picard group of an abelian variety.

4. We will study the Picard group of an abelian variety. We have the following:

   2.9 Theorem. *There is a short exact sequence*

   $$0 \to \mathrm{Pic}^0(X) \to \mathrm{Pic}(X) \to NS(X) \to 0$$

   *where $\mathrm{Pic}^0(X)$ has a natural structure as an abelian variety, usually denoted $\hat{X}$ (and called the **dual abelian variety**), and the **Neron-Severi group** $NS(X)$ is a finitely generated free abelian group.*

5. We will probably study, in this class, the *cohomology* of line bundles on abelian varieties, and in particular Riemann-Roch problems. Here is one example theorem:

   2.10 Theorem. *Let $\mathcal{L}$ be an ample line bundle on the abelian variety X.*[6] *Then the cubic power $\mathcal{L}^{\otimes 3}$ is very ample, i.e. it gives an imbedding of X into some projective space.*

   This is very important in constructing the *moduli space* of abelian varieties.

That's roughly the introduction of this course.

§4 Starting out

Let's begin with the first question.

As stated before, we have:

2.11 Theorem. *An abelian variety is commutative.*

Proof. One can modify the earlier proof via the adjoint representation, but let's prove it by another method.

We need the following *rigidity lemma.*

2.12 Proposition. *Let X be a complete variety, and Y, Z some varieties. Let $f : X \times Y \to Z$ be a morphism such that $f(X \times \{y_0\})$ is a point $z_0 \in Z$, for some $y_0 \in Y$. Then, there is a morphism $g : Y \to Z$ such that f is just projection plus g; in particular, $f(X \times \{y_1\}) = *$ for all y_1.*

The picture is that there is a point $y_0 \in Y$ such that the whole "vertical" fiber goes to a single point. Then the claim is that *all* the vertical fibers go each to one point (which varies with the fiber).

As a consequence of this rigidity lemma, we can see that any morphism of abelian varieties is, up to translation, a group homomorphism.

2.13 Corollary. *Let X, Y be two abelian varieties, and let $f : X \to Y$ a morphism of algebraic varieties, then $f(x) = m(h(x), a)$ for some morphism $h : X \to Y$ of abelian varieties and $a \in Y$.*

Proof. Without loss of generality, we can assume that f maps the identity to the identity. Then we have to show that f is already a homomorphism of abelian varieties. (This is very convenient.) Consider the map $g : X \times X \to Y$ sending

$$g(x, y) := f(xy)(f(x)f(y))^{-1}.$$

We notice that $g(x, y)$ sends the vertical fiber $X \times \{e\}$ and the horizontal fiber $\{e\} \times X$ into the identity element of Y. By the rigidity lemma, it must be constant on all vertical fibers, and on all horizontal fibers; it must thus be just the identity. It follows that f is a homomorphism. ▲

[6] These exist, as we will later show.

We can now see very easily that X is commutative: consider the inversion map $i : X \to X$. This sends the identity to itself, and it is thus a homomorphism; thus X is commutative. ▲

We will prove the rigidity lemma next time.

Lecture 3
2/10

§1 The rigidity lemma again

So, last time we proved that any abelian variety is commutative, modulo a *rigidity lemma.* Here was the picture. If X is a complete variety, Y, Z any varieties,[7] and we have a map

$$f : X \times Y \to Z$$

such that f maps one of the fibers $X \times \{y_0\}$ to a single point[8] $z_0 \in Z$, then the lemma states that f maps *every* $X \times \{y\}$ to a single point. In fact, there is a morphism $g : Y \to Z$ such that $f = g \circ p_2$ for p_2 the second projection. We stated this formally last time.

Proof. The idea is to consider an open affine neighborhood $U \subset Z$ of z_0. We can consider the pre-image of U, $f^{-1}(U) \subset X \times Y$. The pre-image necessarily contains the fiber $X \times \{y_0\}$. This pre-image is open, so the complement $W = X \times Y - f^{-1}(U)$ is closed.

Since X is complete, the projection $pr_2(W) \subset Y$ is closed and, moreover, it cannot be all of Y: in particular, $y_0 \notin pr_2(W)$. Thus $pr_2(W)$ is a *proper* closed subset of Y, not containing y_0, and we can take an open neighborhood $V = Y \setminus p_2(W)$ of y_0.

But, by definition, from this construction, for any point $y \in V$, the map $f : X \times Y \to Z$ sends the fiber $X \times \{y\}$ into U. Now the fibers $X \times \{y\}$ and U is affine, which means that f must be *constant* on the fibers $X \times \{y\}, y \in V$.

From this we want to show that f is constant on all the fibers, and is in fact of the form $g \circ p_2$. Pick $x_0 \in X$ and consider the map

$$g : Y \to Z, \quad y \mapsto f(x_0, y).$$

We want to show that $f = g \circ p_2$. But, for any $(x, v) \in X \times V$, we know that $f(x, v) = f(x_0, v)$ (since f contracts the fiber $X \times \{v\}$ to a point), and consequently

$$f|_{X \times V} = g \circ p_2|_{X \times V}.$$

By separatedness, this must be true everywhere. ▲

[7] We always assume varieties to be separated.

[8] Here by "point" we mean "closed point."

§2 The multiplication-by-n map — a sketch

We now know, in particular, that any abelian variety A is commutative. As a result, we shall write them *additively*, and write the inversion as $(-1)_A$. We can define, more generally, for each $n \in \mathbb{Z}$, a morphism of abelian varieties

$$n_A : A \to A, \quad x \mapsto nx.$$

So, now we want to study n_A. There are two things to show: first, n_A is surjective (so as an abstract group A is divisible), and second, we want to determine the kernel. Let's give an easy argument for the surjectivity.

3.1 Lemma. *If $p \nmid n$ (where $p = \operatorname{char} k$), then $[n]_A$ is surjective.*

Sketch. We can look at the differential of the addition map at the origin. In fact, the derivative $(dn_A)_0 : T_0 A \to T_0 A$ is given by multiplication by n. Therefore, $p \nmid n$, the map dn_A is an isomorphism, This implies that n_A is a smooth morphism, and in particular surjective (since A is proper). ▲

We will have another argument later, to include the case where $p \mid n$. In that case, multiplication by n is zero on the Lie algebra.

§3 The theorem of the cube

We will need to study line bundles on an abelian variety A.

3.2 Theorem (Theorem of the cube)**.** *Let X, Y be complete varieties, and let Z be any variety. Let us fix $x_0 \in X, y_0 \in Y, z_0 \in Z$. Let $\mathcal{L}$ be a line bundle on the product $X \times Y \times Z$. If the restriction*

$$\mathcal{L}|_{\{x_0\} \times Y \times Z}, \ \mathcal{L}|_{X \times \{y_0\} \times Z}, \ \mathcal{L}|_{X \times Y \times \{z_0\}}$$

are all trivial, then $\mathcal{L}$ itself is trivial.

Eventually, we will give a proof of the surjectivity of multiplication by n on an abelian variety using this. Before proving the theorem of the cube, let's make some remarks.

Remark. What does this theorem mean? Let us denote by $\mathcal{P}_k^+$ the category of pointed complete varieties over k. Objects here are complete varieties X together with a k-point $x_0 \in X(k)$. Morphisms are morphisms of varieties preserving the basepoint. Let $T : \mathcal{P}_k^+ \to \mathbf{Ab}$ be a contravariant functor from this category to the category of abelian groups.

Suppose we are given $n+1$ objects $X_0, \ldots, X_n \in \mathcal{P}_k^+$. For each i, we have projections

$$\pi_i : X_0 \times \cdots \times X_n \to X_0 \times \cdots \times \hat{X}_i \times \cdots \times X_n$$

and the inclusions

$$\sigma_i : X_0 \times \cdots \times \hat{X}_i \times \cdots \times X_n \to X_0 \times \cdots \times X_n$$

in the other direction. We have maps of abelian groups $T(\pi_i)$ and $T(\sigma_i)$. We can define a product map

$$\alpha_n = \sum T(\pi_i) : \prod_i T(X_0 \times \cdots \times \hat{X}_i \times \cdots \times X_n) \to T(X_0 \times \cdots \times X_n)$$

We have a map in the other direction

$$\beta_n = \prod T(\sigma_i) : \prod_i T(X_0 \times \cdots \times \hat{X}_i \times \cdots \times X_n) \to T(X_0 \times \cdots \times X_n).$$

We have a general categorical fact (valid in any pointed category).

3.3 Lemma. *The abelian group $T(X_0 \times \cdots \times X_n)$ decomposes as a direct sum, the image of α_n and the kernel of β_n.*

We say that the functor T is **of order** n (if $n = 1$, linear; if $n = 2$, quadratic), if β_n is surjective, or if α_n is surjective. What the theorem of the cube is saying is that the Pic functor from $\mathcal{P}_k^+ \to \mathbf{Ab}$ is a *quadratic functor* (actually, it says a little more, since one of the varieties didn't have to be complete).

3.4 Example. Here is an example of a linear functor. Let A be an abelian variety; we send it to $\mathrm{Hom}_{\mathcal{P}_k^+}(\cdot, A)$, defining a contravariant functor $\mathcal{P}_k^+ \to \mathbf{Ab}$. This is a linear functor. To see this, we will show that if $X, Y \in \mathcal{P}_k^+$, then the map

$$\mathrm{Hom}(X \times Y, A) \to \mathrm{Hom}(X, A) \times \mathrm{Hom}(Y, A)$$

is injective. This is the definition of a linear functor. In fact, this map is a *bijection*; we leave the surjectivity as an exercise. To see that the map is injective, we apply the rigidity lemma: if we have a map $X \times Y \to A$, and the restrictions to $X \times \{y_0\}, \{x_0\} \times Y$ map to zero, then $X \times Y$ maps entirely to zero.

3.5 Example. Say $k = \mathbb{C}$. The second cohomology $H^2(\cdot, \mathbb{Z}) : \mathcal{P}_{\mathbb{C}}^+ \to \mathbf{Ab}$ is quadratic. H^1 is a linear functor.

Let's give some corollaries of the theorem of the cube.

3.6 Corollary. *Let X, Y, Z be complete varieties. Then every line bundle on $X \times Y \times Z$ is of the form $p_{12}^*(\mathcal{L}_3) \otimes p_{23}^*(\mathcal{L}_1) \otimes p_{13}^*(\mathcal{L}_2)$ where $\mathcal{L}_3$ is a line bundle on $X \times Y$, $\mathcal{L}_1$ on $Y \times Z$, and $\mathcal{L}_2$ on $X \times Z$.*

Proof. In fact, this follows by the lemma above: the map α_3 is surjective since Pic is quadratic. ▲

3.7 Corollary. *Let A be an abelian variety and X some variety. Consider $f, g, h : X \to A$, three morphisms of varieties. For any line bundle $\mathcal{L}$ on A, we have the following isomorphism*

$$(f + g + h)^*\mathcal{L} \simeq (f + g)^*\mathcal{L} \otimes (g + h)^*\mathcal{L} \otimes (f + h)^*\mathcal{L} \otimes f^*L^{-1} \otimes g^*\mathcal{L}^{-1} \otimes h^*\mathcal{L}^{-1}. \quad (4)$$

This formula is a bit complicated, but later we're going to apply it to a special case.

Proof. In fact, we need to consider the "universal" case, where $X = A \times A \times A$, and the three maps f, g, h are the projections $p_1, p_2, p_3 : A \times A \times A \to A$. Let us make some notations. We have these projections $p_{ij} : A \times A \times A \to A \times A$, for $i, j \in \{1, 2, 3\}$, in addition to the projections p_i. We let $m : A \times A \to A$ be the multiplication map on A, and $n : A \times A \times A \to A$ the triple multiplication.

What we want to show is the following:

$$n^*\mathcal{L} \simeq (m \circ p_{12})^*\mathcal{L} \otimes (m \circ p_{23})^*\mathcal{L} \otimes (m \circ p_{13})^* \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1} \otimes p_3^*\mathcal{L}^{-1}.$$

We just need to handle this universal case. To check it, though, we can apply the theorem of the cube. We just need to check that the two line bundles on the left on the right are the same on

$$\{0\} \times A \times A, \ A \times \{0\} \times A, \ A \times A \times \{0\}.$$

By symmetry, let's just check it on the first. In fact, $n^*\mathcal{L}$ becomes $m^*\mathcal{L}$ on $\{0\} \times A \times A$. On the right, a bunch of things cancel. We have $(m \circ p_{12})^*\mathcal{L}|_{\{0\} \times A \times A} = p_1^*\mathcal{L}$, for example. And so on for the others—it is a bit tedious to write out, but easy to check. ▲

What we really want is:

3.8 Corollary. *Let $\mathcal{L}$ be a line bundle on A. Then*

$$n_A^*\mathcal{L} = \mathcal{L}^{\frac{n^2+n}{2}} \otimes (-1)^*\mathcal{L}^{\frac{n^2-n}{2}}.$$

Proof. We will use (4). In that equation, we let $f = n_A, g = 1_A = \mathrm{id}_A, h = (-1)_A$. If we plug it into the formula, we get

$$n_A^*\mathcal{L} = (n+1)_A^*\mathcal{L} \otimes 1 \otimes (n-1)_A^*\mathcal{L} \otimes n_A^*\mathcal{L}^{-1} \otimes \mathcal{L}^{-1} \otimes (-1)^*\mathcal{L}.$$

We can rewrite this a little as:

$$(n+1)_A^*\mathcal{L} \otimes n_A^*\mathcal{L}^{-1} = (n_A^*\mathcal{L} \otimes (n-1)_A^*\mathcal{L}^{-1}) \otimes (\mathcal{L} \otimes (-1)_A^*\mathcal{L}^{-1}).$$

If we denote $\mathcal{M}_n := n_A^*\mathcal{L} \otimes (n-1)^*\mathcal{L}^{-1}$, we get

$$\mathcal{M}_{n+1} = \mathcal{M}_n \otimes (\mathcal{L} \otimes (-1)_A^*\mathcal{L}).$$

As a result, we get

$$\mathcal{M}_n = (\mathcal{L} \otimes (-1)_A^*\mathcal{L})^{n-1} \otimes \mathcal{L}.$$

Since

$$n_A^*\mathcal{L} = \mathcal{M}_n \otimes \mathcal{M}_{n-1} \otimes \cdots \otimes \mathcal{M}_1,$$

we are done. ▲

We get from this:

3.9 Corollary. *If $\mathcal{L}$ is symmetric in the sense that $(-1)_A^*\mathcal{L} \simeq \mathcal{L}$, then*

$$n_A^*\mathcal{L} \simeq \mathcal{L}^{n^2}.$$

For the next corollary, we introduce some notation. If $x \in A$, we let $T_x : A \to A$ the translation by x map, $a \mapsto a + x$.

3.10 Corollary (Theorem of the square)**.** *For any $x, y \in A$, and any line bundle $\mathcal{L}$ on A, we have*

$$T_{x+y}^*\mathcal{L} \otimes \mathcal{L} = T_x^*\mathcal{L} \otimes T_y^*\mathcal{L}.$$

Proof. If we consider $f : A \to A$ as the map sending $f(A) = \{x\}$, $g : A \to A$ sending $g(A) = \{y\}$, and $h : A \to A$ the identity, then we apply (4) to f, g, h. We're out of time, but the result is now easy to check. ▲

The corollary allows us to make the following definition.

3.11 Definition. Let $\mathcal{L}$ be a line bundle on A. We can define the map $\phi_{\mathcal{L}} : A \to \mathrm{Pic}(A)$, $x \mapsto T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. This is a group homomorphism, by the theorem of the square.

This is a very important map, and we'll continue from here next week.

Lecture 4
2/13

Last time, we stated an important theorem—the *theorem of the cube*—and some applications. We are going to outline the main steps in the proof of this theorem. We will need a few facts about the cohomology of coherent sheaves on a scheme, and today we're going to review this theory.

§1 Quasi-coherent sheaves

Let X be a scheme.

4.1 Definition. It makes sense to talk about the category of *quasi-coherent sheaves* on X; this will be denoted $\mathrm{QCoh}(X)$. If X is noetherian, we can also talk about the category $\mathrm{Coh}(X)$ of *coherent sheaves* on X.

Recall that if $f : X \to Y$ is a morphism between schemes, we have an adjunction between $f^* : \mathrm{QCoh}(Y) \to \mathrm{QCoh}(X)$ and the right adjoint $f_* : \mathrm{QCoh}(X) \to \mathrm{QCoh}(Y)$ (in nice cases). The f_* has a so-called *derived functor.*

4.2 Definition. The **derived functors** of f_* will be denoted by $\left\{R^i f_*\right\}_{i \geq 0}$; these are additive functors

$$R^i f_* : \mathrm{QCoh}(X) \to \mathrm{QCoh}(Y).$$

We won't review the definition, but we will review the most important properties. The $R^i f_*$ are equipped with natural boundary maps $\delta^i : R^i f_*\mathcal{F}'' \to R^{i+1} f_*\mathcal{F}'$ for each exact sequence

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0.$$

So, in reality, we have a collection of functors $R^i f_*$, *together with* such natural transformations for each short exact sequence. We have the following properties:

1. $R^0 f_* = f_*$.
2. For any short exact sequence $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$, we have a long exact sequence of sheaves
$$\cdots \to R^i f_* \mathcal{F}' \to R^i f_* \mathcal{F} \to R^i f_* \mathcal{F}'' \xrightarrow{\delta^i} R^{i+1} f_* \mathcal{F}' \to R^{i+1} f_* \mathcal{F} \to \dots .$$
3. If we have a morphism of short exact sequences
$$\begin{tikzcd} 0 \arrow[r] & \mathcal{F}' \arrow[r] \arrow[d] & \mathcal{F} \arrow[r] \arrow[d] & \mathcal{F}'' \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathcal{G}' \arrow[r] & \mathcal{G} \arrow[r] & \mathcal{G}'' \arrow[r] & 0 \end{tikzcd}$$
then the associated diagram of long exact sequences commutes.
4. If Y is affine, $Y = \mathrm{Spec} R$, then $R^i f_* \mathcal{F}$ is the sheaf associated to the cohomology $H^i(X, \mathcal{F})$ (which is an R-module).

It is not immediately obvious that there *exists* such a sequence of functors, but such a sequence does exist, and the right one can be characterized by a universal property. Instead of going through all the details, let us describe how to actually *calculate* these functors.

The way to calculate the $R^i f_* \mathcal{F}$ is as follows. First assume Y is affine, $Y = \mathrm{Spec} R$; then we are trying to calculate the *cohomology* of this sheaf $\mathcal{F}$ (as an R-module). We will assume that X is *separated*, which implies that the intersection of two open affines in X is still affine.

Let $\mathfrak{A} = \{U_i\}_{i \in I}$ be a cover of X by open affines, so each $U_i \subset X$ is an affine open subscheme. Fix an order on the indexing set I.

4.3 Definition. We define the **Cech complex** $C^\bullet(\mathfrak{A}, \mathcal{F})$ of X as follows. We define
$$C^p(\mathfrak{A}, \mathcal{F}) = \prod_{i_0 < \cdots < i_p} \Gamma(U_{i_0} \cap \cdots \cap U_{i_p}, \mathcal{F}).$$

In particular,
$$C^0(\mathcal{A}, \mathcal{F}) = \prod_{i \in I} \Gamma(U_i, \mathcal{F}), \quad C^1(\mathfrak{A}, \mathcal{F}) = \prod_{i<j} \Gamma(U_i \cap U_j, \mathcal{F}).$$

We can define the differentials in this complex,
$$d^p : C^p(\mathfrak{A}, \mathcal{F}) \to C^{p+1}(\mathfrak{A}, \mathcal{F})$$
by sending an element $\sigma = (\sigma_{i_0 \dots i_p})_{i_0 < \cdots < i_p}$ to an element
$$(d\sigma)_{i_0 \dots i_{p+1}} = \sum_{j=0}^{p+1} (-1)^j \sigma_{i_0 \dots \hat{i_j} \dots i_{p+1}} |_{U_{i_0} \cap \cdots \cap U_{i_{p+1}}} \in \Gamma(U_{i_0} \cap \cdots \cap U_{i_{p+1}}, \mathcal{F}).$$

The hat means that something is omitted.

4.4 Example. Let us consider the first case of the Cech complex. The map $d : C^0(\mathfrak{A}, \mathcal{F}) \to C^1(\mathfrak{A}, \mathcal{F})$ sends an element $\sigma = (\sigma_i)_{i \in I}$ to the element $d\sigma$ defined via

$$(d\sigma)_{ij} = \sigma_i|_{U_i \cap U_j} - \sigma_j|_{U_i \cap U_j} \in \Gamma(U_i \cap U_j, \mathcal{F}).$$

We have:

4.5 Theorem. *If X is separated and $\mathcal{F}$ quasi-coherent on X, then $H^i(X, \mathcal{F}) = H^i(C^\bullet(\mathfrak{A}, \mathcal{F}))$ for any cover $\mathfrak{A}$ of X by open affines.*

4.6 Corollary (Künneth formula)**.** *Let X, Y be two separated schemes over a field k. Let $\mathcal{F} \in \mathrm{QCoh}(X), \mathcal{G} \in \mathrm{QCoh}(Y)$. Then we have the relation*

$$H^n(X \times Y, \mathcal{F} \boxtimes \mathcal{G}) = \bigoplus_{i+j=n} H^i(X, \mathcal{F}) \otimes_k H^j(Y, \mathcal{G}).$$

Here $\boxtimes$ means the tensor product of the pull-backs. This can be proved by observing that if one forms an open affine cover $\{U_i\}$ of X and an open affine cover $\{V_j\}$ of Y, one gets an open affine cover $\{U_i \times_k V_j\}$ of $X \times Y$, and the Cech complex of $\mathcal{F} \boxtimes \mathcal{G}$ is the tensor product of the Cech complexes of $\mathcal{F}, \mathcal{G}$.

4.7 Example. Let us compute $H^0(X, \mathcal{F})$ via the Cech complex. In fact, from the earlier example, we see that

$$H^0(C^\bullet(\mathfrak{A}, \mathcal{F}) = \ker(C^0(\mathfrak{A}, \mathcal{F}) \to C^1(\mathfrak{A}, \mathcal{F}))$$

consists of systems of elements $\sigma_i \in \Gamma(U_i, \mathcal{F})$ which agree on the intersections $U_i \cap U_j$. As a result, the kernel consists precisely of global sections, $H^0(X, \mathcal{F}) = \Gamma(X, \mathcal{F})$. This is good.

4.8 Example. What is $H^1(X, \mathcal{F})$? We can present such an element via a system of elements $(\sigma_{ij})_{i<j}$ (defined over $U_i \cap U_j$) satisfying the *cocycle condition*

$$\sigma_{jk}|_{U_i \cap U_j \cap U_k} - \sigma_{ik}|_{U_i \cap U_j \cap U_k} + \sigma_{ij}|_{U_i \cap U_j \cap U_k} = 0, \quad i < j < k.$$

These are the cocycles in the Cech complex. We have to quotient by the elements (σ_{ij}) that are (co)boundaries: i.e., those that can be presented as $\sigma_i - \sigma_j$ for some $(\sigma_i)_{i \in I}$.

The two important things for us are the long exact sequence in cohomology and the possibility of actual calculation using the Cech complex.

§2 Theorems on cohomology

Let us now review some of the important theorems on cohomology, without proof. First, we have a finiteness theorem.

4.9 Theorem. *Let $f : X \to Y$ be a proper morphism of noetherian schemes. Suppose $\mathcal{F} \in \mathrm{Coh}(X)$. Then the $R^i f_* \mathcal{F}$ are coherent sheaves on Y (not just quasi-coherent). In particular, if $Y = \mathrm{Spec} k$ for k a field, then $H^i(X, \mathcal{F})$ is a finite-dimensional k-vector space.*

We won't say anything about the proof, because it is hard. What we are mostly interested in is the case where $X \to \mathrm{Spec} k$ and X is a complete variety.

4.10 Theorem. *Let $f : X \to Y$ be a proper morphism of noetherian schemes, as above, and let $\mathcal{F} \in \mathrm{Coh}(X)$ be flat over Y.*[9] *Then, there exists finite complex*

$$0 \to K^0 \to \cdots \to K^n \to 0$$

of locally free $\mathcal{O}_Y$-modules of finite rank (over Y) with the following property.

For every morphism $u : S \to Y$, draw a cartesian square

$$\begin{tikzcd} X \times_Y S \arrow[r, "v"] \arrow[d, "g"] & X \arrow[d, "f"] \\ S \arrow[r, "u"] & Y \end{tikzcd} .$$

Then we have that

$$R^i g_* v^* \mathcal{F} = H^i(u^* K^\bullet) \in \mathrm{Coh}(S).$$

The theorem is a little abstract, but what it is saying is that the cohomology of any pull-back of $\mathcal{F}$ can be represented via this nice complex $K^\bullet$.

Let us give some examples.

4.11 Example. First, let's elucidate the flatness assumption. Consider $X \times_k T \to T$, for X, Y over a field k, then any vector bundle $\mathcal{E}$ on $X \times_k T$ is flat over T. This is typically the situation we want to use. This is because projections in this case will be flat.

Before we can give another example, we need a definition.

4.12 Definition. Let $X \to \mathrm{Spec} k$ be a proper map (i.e. X is a complete variety). Then each $H^i(X, \mathcal{F})$ (for $\mathcal{F} \in \mathrm{Coh}(X)$) is a finite-dimensional k-vector space by the previous theorem, and we let

$$\chi(X, \mathcal{F}) = \sum (-1)^i \dim_k H^i(X, \mathcal{F}).$$

This is the **Euler characteristic** of $\mathcal{F}$.

We will now show that in a flat family of coherent sheaves, the Euler characteristic is locally constant.

4.13 Corollary. *Let $f : X \to Y$ and $\mathcal{F} \in \mathrm{Coh}(X)$ as in the previous theorem (so f proper, $\mathcal{F}$ flat over Y). Then for $y \in Y$,*

$$\chi_y(\mathcal{F}) := \chi(\mathcal{F}_y)$$

is a locally constant function on Y. (Here $\mathcal{F}_y = \mathcal{F}|_{X_y}$ is a scheme proper over $\mathrm{Spec} k(y)$*, so the Euler characteristic makes sense.)*

[9] This means that for every point $x \in X$, the stalk $\mathcal{F}_x$ is a flat $\mathcal{O}_{Y,f(x)}$-module.

Proof. In fact, by the main theorem, we can associate to $\mathcal{F}$ a complex

$$0 \to K^0 \to \cdots \to K^n \to 0$$

of locally free $\mathcal{O}_Y$-modules. We will apply the statement of the theorem to the following situation

$$\begin{tikzcd} X_y \arrow[r] \arrow[d] & X \arrow[d, "f"] \\ \mathrm{Spec} k(y) \arrow[r] & Y \end{tikzcd} .$$

By the theorem, we know that we can calculate the cohomology $H^i(X_y, \mathcal{F}_y)$ as the cohomology $H^i(K^\bullet \otimes_Y k(y))$ of a complex. Therefore, the Euler characteristic of $\mathcal{F}_y$ can be written as

$$\chi(\mathcal{F}_y) = \sum (-1)^i \dim_{k(y)} H^i(K^\bullet \otimes_Y k(y))$$

and this can calculated via

$$\sum (-1)^i \dim_{k(y)} K^i \otimes k(y).$$

However, this is clearly a locally constant function on Y, because the K^i are locally free. Therefore, the Euler characteristics are locally constant. ▲

Here is another corollary:

4.14 Corollary (Semicontinuity)**.** *Let $f : X \to Y, \mathcal{F}$ be as before. Then*

$$y \mapsto h^i(y, \mathcal{F}) := \dim_{k(y)} H^i(X_y, \mathcal{F}_y)$$

is an upper semicontinuous function on Y.[10]

Proof. Again, we are in the situation of the main theorem. We observe that

$$h^i(y, \mathcal{F}) = \dim H^i(K^\bullet \otimes k(y)).$$

In other words, it is the dimension of the kernel of

$$d^i \otimes k(y) : K^i \otimes k(y) \to K^{i+1} \otimes k(y)$$

minus the dimension of the image of

$$d^{i-1} \otimes k(y) : K^{i-1} \otimes k(y) \to K^i \otimes k(y).$$

We can write this equivalently as

$$h^i(y, \mathcal{F}) = \dim(K^i \otimes k(y)) - \dim \mathrm{Im}(d^i \otimes k(y)) - \dim \mathrm{Im}(d^{i-1} \otimes k(y)).$$

We know that the first term is locally constant, so to prove that the whole thing is upper semicontinuous, we need only prove that the terms $\dim \mathrm{Im}(d^i \otimes k(y))$ are *lower* semicontinuous. That is, we need to show that for each n, the set

$$\left\{ y \in Y : \dim \mathrm{Im}(d^i \otimes k(y)) \le n \right\} \tag{5}$$

[10] That is, for any n, the set of $y \in Y$ such that $h^i(Y, \mathcal{F}) \ge n$ is closed.

is closed. However, we are dealing with maps of locally free sheaves $d^i : K^i \to K^{i+1}$ which can be given by matrices, at least locally. The statement that the dimension of the image is $\leq n$ is saying that certain determinants vanish (namely, the $n \times n$ minors), and that's a closed condition. In other words, the sets (5) are cut out by determinantal conditions, hence closed. ▲

We have one more corollary which we want to use later on. This will give us a criterion to check when the derived push-forwards are locally free.

4.15 Corollary. *Assume Y is reduced, and let $f, X, \mathcal{F}$ be as above. The following are equivalent.*

1. *$h^i(y, \mathcal{F})$ is locally constant on Y.*
2. *$R^i f_* \mathcal{F}$ is locally free of finite rank on Y, and the natural map*

$$R^i f_* \mathcal{F} \otimes k(y) \to H^i(X_y, \mathcal{F}_y)$$

is an isomorphism, for $y \in Y$.

Proof. Of course, the fact that the second condition implies the first is obvious. We want to show conversely if $h^i(y, \mathcal{F})$ is locally constant, then we get the local freeness. In fact, we have as before a piece of the complex

$$K^{i-1} \overset{d^{i-1}}{\to} K^i \overset{d^i}{\to} K^{i+1}$$

and we have $\mathrm{Im} d^{i-1} \subset \ker d^i$, and we have $\mathrm{Im} d^i \subset K^{i+1}$.

If $h^i(y, \mathcal{F})$ is locally constant, then the two functions

$$\dim(d^i \otimes k(y)), \dim(d^{i-1} \otimes k(y))$$

are locally constant, *by the previous proof.* (Both are lower semicontinuous.) This implies (by reducedness of Y) that $\mathrm{Im} d^i, \mathrm{Im} d^{i-1}$ are locally free sheaves. This means that there's locally a splitting of this complex, and from this the result follows (i.e. taking cohomology will commute with tensoring with k). ▲

Lecture 5
2/15

Today, we will prove the theorem of the cube, using the cohomology theory we developed last time.

§1 The seesaw theorem

We will start with the following.

5.1 Theorem. *Let k be algebraically closed, X a complete k-variety,*[11] *T/k any variety. Let $\mathcal{L}$ be a line bundle on the product $X \times_k T$. Then if*

$$T_1 = \left\{ t \in T : \mathcal{L}|_{X \times \{t\}} \textit{ is trivial } \right\},$$

then $T_1 \subset T$ is closed, and furthermore, there exists a line bundle $\mathcal{M}$ on T_1 (given the reduced subscheme structure) such that $\mathcal{L}|_{X \times T_1} = p_2^* \mathcal{M}$.

Here p_2 is the projection $X \times T_1 \to T_1$, and the theorem states that since the line bundle is trivial on the fibers of $X \times T_1$, it arises as a pull-back.

Proof. Let us first observe that if Z is any complete variety, then a line bundle $\mathcal{L}_0$ on Z is trivial if and only if $\Gamma(Z, \mathcal{L}_0) \neq 0$ and $\Gamma(Z, \mathcal{L}_0^{-1}) \neq 0$. The reason is that a trivial line bundle obviously satisfies this, and conversely if these nonvanishing conditions hold, then there are nontrivial maps

$$\mathcal{O}_Z \to \mathcal{L}_0, \quad \mathcal{L}_0 \to \mathcal{O}_Z.$$

Composing them in either order gives nonzero maps $\mathcal{O}_Z \to \mathcal{O}_Z$, which must be nonzero constants (in fact, $\Gamma(Z, \mathcal{O}_Z) = k$ in view of completeness). This means that $\mathcal{O}_Z \to \mathcal{L}_0$ is an isomorphism.

As a result, we can characterize T_1. T_1 is the set of all $t \in T$ such that $H^0(X \times \{t\}, \mathcal{L}|_{X \times \{t\}}) \neq 0$ and $H^0(X \times \{t\}, \mathcal{L}^{-1}|_{X \times \{t\}}) \neq 0$. However, by the semicontinuity theorem proved last time, we now find that T_1 must be closed.

Now, let's prove the second part. Consider the projection

$$p_2 : X \times T_1 \to T_1.$$

Consider $(p_2)_* \mathcal{L}$. We know that for $t \in T_1$, $\dim_k H^0(X \times \{t\}, \mathcal{L}|_{X \times \{t\}} = 1$. Since the cohomology along the fibers is constant, and since T is reduced, we find that $(p_2)_* \mathcal{L}$ is locally free of rank one (by yesterday's results). We write $\mathcal{M} := (p_2)_* \mathcal{L}$, and we get by adjunction a map

$$p_2^* \mathcal{M} \to \mathcal{L}$$

which is an isomorphism. In fact, it is an isomorphism on each fiber. ▲

Remark. If k is not algebraically closed, then the set T_1 as defined is still closed, but it is not true that $\Gamma(Z, \mathcal{O}_Z) = k$ for a complete k-variety Z. The above theorem turns out to be still true after an appropriate base-change of k.

§2 The theorem of the cube

Now, let's prove the main result. Recall the statement. We had varieties $X, Y, Z/k$ with points x_0, y_0, z_0 such that X, Y were complete. $\mathcal{L}$ was a line bundle on $X \times_k Y \times_k Z$ whose restriction to the "coordinate planes" $X \times Y \times \{z_0\}, X \times \{y_0\} \times Z, \{x_0\} \times Y \times Z$, were all trivial. We want to show that $\mathcal{L}$ is trivial.

[11] A *variety* is an integral, separated scheme of finite type over a field.

Proof of the theorem of the cube. We start with a reduction to the case of X a smooth projective curve:

5.2 Lemma. *For every two points $x_0, x_1 \in X$, there exists an irreducible curve $C \subset X$ containing x_0, x_1.*

As a result of this, we can assume X is a smooth projective curve. Indeed, in the theorem of the cube, to show that the line bundle $\mathcal{L}$ is trivial, we need to show that $\mathcal{L}|_{\{x\}\times Y\times\{z\}}$ is trivial for all $x \in X, z \in Z$. This is in virtue of the seesaw principle: if we have proved this, then $\mathcal{L}$ arises as a pull-back of something on $X \times Z$. But this line bundle is trivial because $\mathcal{L}|_{X\times\{y_0\}\times Z}$ is trivial, so we can then conclude that $\mathcal{L}$ is trivial.

To prove this, though, we can connect any point in X to x_0 with a curve. So we have reduced to proving it for X a curve. We can replace the curve with its normalization, and then reduce to the case of X a *smooth* curve. This is a bit tricky, but the observation is that showing $\mathcal{L}|_{\{x\}\times Y\times\{z\}}$ is trivial, we can replace X by something that surjects onto X.

Now, we can prove the theorem of the cube, with the assumption X is a smooth curve of genus g. Pick a divisor E on X of degree g such that

$$H^0(X, \Omega_X(-E)) = 0,$$

which is to say by Serre duality that $H^1(X, \mathcal{O}(E)) = 0$. (*Exercise*: this can always be done.)

Let $\mathcal{M} = p_1^*\mathcal{O}(E)\otimes\mathcal{L}$. To show that $\mathcal{L}$ is trivial, we have to show that $\mathcal{M} \simeq p_1^*\mathcal{O}(E)$. Consider the projection

$$p_{23} : X \times Y \times Z \to Y \times Z.$$

Consider the derived push-forward $R^1p_{23*}\mathcal{M}$; the support is a closed subset W of $Y\times Z$. But in fact, we claim that $W \cap Y \times \{z_0\}$ is empty.

The reason is that $H^1(X \times \{y\} \times \{z_0\}, \mathcal{M}|_{X\times\{y\}\times\{z_0\}}) = 0$, as the restriction to there is $\mathcal{O}(E)$. Consequently, this is true for nearby points (upper semicontinuity), and then we can apply the cohomology and base change theorems from last time.

Anyway, we find that the projection of W to the Z factor is a closed subset of Z which does not contain z_0. It is closed by properness of Y. In other words, there exists an open subset $Z' \subset Z$ which is *open*, containing z_0, such that $R^1p_{23*}\mathcal{M}$ is zero on $Y \times Z'$. (This again is because $Y \times \{z_0\} \cap W = \emptyset$.)

So now it is enough to prove the theorem for $X \times Y \times Z'$, by the see-saw theorem (the set of (x, z) such that the restriction to $\{x\} \times Y \times \{z\}$ is trivial is closed). We can *replace* Z by Z': we never assumed Z to be complete, so this is ok. In other words, we can *assume* that

$$R^1p_{23*}\mathcal{M} = 0.$$

This will imply that $p_{23*}\mathcal{M}$ is locally free of rank one on $Y \times Z$: in fact, the Euler characteristic $\chi(\mathcal{M}|_{X\times\{y\}\times\{z\}})$ does not change in y, z, and since H^1 of the fibers is always zero, we find that H^0 of the fibers is constant. When we choose $y = y_0, z = z_0$, we just compute $\chi(\mathcal{O}(E)) = 1 - g + \deg E = 1$. So the Euler characteristics along all the fibers is one.

Let us write

$$\mathcal{N} = p_{23*}\mathcal{M}$$

so that $\mathcal{N}$ is a line bundle. We are trying to show that $\mathcal{M}$ is isomorphic to the pullback of $\mathcal{O}(E)$. Let $\{U_i\}$ be an open cover of $Y \times Z$ such that $\mathcal{N}|_{U_i}$ is trivial; choose trivializations $\mathcal{N}|_{U_i} \simeq \mathcal{O}_{U_i}$. So we can produce a bunch of sections $\alpha_i \in \Gamma(U_i, \mathcal{N}) = \Gamma(X \times U_i, \mathcal{M})$.

Let D_i be the set of zeros of this section $\alpha_i(1)$. The claim is that the D_i can be glued together to get a closed subset of codimension one in the triple product. On $U_i \cap U_j$, we note that $\alpha_i = f_{ij}\alpha_j$ differ by an invertible function. That implies that the sets of zeros are the same. So one can define a subset $D \subset X \times Y \times Z$ such that $D|_{X \times U_i} = D_i$. Intuitively, what is this D? For each (y, z), we have a line bundle on the fiber; the global section gives a set of zeros along the fiber. As you move the fiber, the set of zeros varies and forms a closed subset D in $X \times Y \times Z$. In other words, the restriction of D to each fiber over (y, z) is the nonzero section of $\mathcal{M}|_{X \times \{y\} \times \{z\}}$.

To show that $\mathcal{L}$ is trivial, we are reduced to showing that $\mathcal{M} \simeq p_1^*\mathcal{O}(E)$, which is to say that D is linearly equivalent to $E \times Y \times Z$. That is what we want to show.

Let $p \in X$ be a point, $p \notin E$. Consider $D \cap \{p\} \times Y \times Z$. This is a closed subset of $Y \times Z$, and it cannot be the whole thing because it does not contain $\{p\} \times Y \times \{z_0\}$, because when you restrict $D_{X \times \{y\} \times \{z_0\}}$ you just get E, and $p \notin E$.

So we get a proper closed subset D in $\{p\} \times Y \times Z$. Furthermore, the projection of $D \cap p \times Y \times Z$ to the Z factor is a closed subset not containing z_0. That means $D \cap \{p\} \times Y \times Z$, since it is codimension one, must be of the form $\{p\} \times Y \times T$ for T of codimension one. But on the other hand, this intersection does not contain $p \times \{y_0\} \times Z$ becasue the line bundle is trivial there. We find that $T = \emptyset$. Thus D does not intersect $\{p\} \times Y \times Z$, which forces that D is contained in $E \times Y \times Z$.

The proof, modulo the lemma, is now complete.

Proof of the lemma. Assume $\dim X > 1$, or there is nothing to prove.

For any two points $x_0, x_1 \in X$, we want to find an irreducible curve containing them. By induction, we just need to find an irreducible subvariety of codimension one containing both. Now X is complete. By Chow's lemma, we can assume that X is projective. (Chow's lemma says that there is a projective variety projecting birationally and surjectively onto any complete variety.) Let $\widetilde{X}$ be the blow-up of X at the two points $\{x_0\}, \{x_1\}$ so that $\widetilde{X}$ is still projective, and we can imbed $\widetilde{X} \hookrightarrow \mathbb{P}^N$ for some N. By Bertini's theorem, we can find a general hyperplane section H such that $H \cap \widetilde{X}$ is irreducible of codimension one in $\widetilde{X}$. If $f : \widetilde{X} \to X$ is the projection, then $\dim f^{-1}(x_0), f^{-1}(x_1) \geq 1$, so $H \cap f^{-1}(x_i) \neq \emptyset$ for each i. We can then finish by induction, by projecting these intersections to X. ▲

▲

The proof of the theorem of the cube was long and tricky. Over $\mathbb{C}$, there is a very easy proof: we look at the exponential sequence

$$0 \to \mathbb{Z} \to \mathcal{O}_X \to \mathcal{O}_X^* \to 1,$$

and the line bundles are classified by $H^1(X, \mathcal{O}_X^*)$. We have an exact sequence

$$H^1(\mathcal{O}_X) \to H^1(X, \mathcal{O}_X^*) \to H^2(X, \mathbb{Z})$$

and the outside functors are quadratic (in fact, the first is linear), which means that the middle is linear in X.

Lecture 6
2/17

Last time, we proved the theorem of the cube, and today we will apply it to deduce some deep results on abelian varieties.

§1 $\mathrm{Pic}^0(A)$

Let A be an abelian variety over an algebraically closed field k,[12] $\mathcal{L} \in \mathrm{Pic}(A)$. We recall that if $T_x, x \in A$ denotes translation by x, then we have the *theorem of the square* (a consequence of the theorem of the cube)

$$T_{x+y}^* \mathcal{L} \otimes \mathcal{L} \simeq T_x^* \mathcal{L} \otimes T_y^* \mathcal{L}, \quad x, y \in A(k).$$

Consequently, as before, we get a *group homomorphism* depending on $\mathcal{L}$:

$$\phi_{\mathcal{L}} : A(k) \to \mathrm{Pic}(A), \quad x \mapsto T_x^* \mathcal{L} \otimes \mathcal{L}^{-1}.$$

It is easy to check that $\phi_{\mathcal{L}_1 \otimes \mathcal{L}_2} = \phi_{\mathcal{L}_1} \otimes \phi_{\mathcal{L}_2}$. Consequently, we have a homomorphism

$$\mathrm{Pic}(A) \xrightarrow{\phi} \mathrm{Hom}(A(k), \mathrm{Pic}(A)).$$

6.1 Definition. We let $\mathrm{Pic}^0(A) = \ker \phi$, i.e. the collection of $\mathcal{L} \in \mathrm{Pic}(A)$ such that $T_x^* \mathcal{L} \simeq \mathcal{L}$ for all $x \in A$ (i.e. the translation-invariant line bundles).

Any line bundle of the form $T_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$ is translation-invariant (by the theorem of the square), and consequently lands in $\mathrm{Pic}^0(A)$. We have thus an exact sequence

$$0 \to \mathrm{Pic}^0(A) \to \mathrm{Pic}(A) \xrightarrow{\phi} \mathrm{Hom}(A(k), \mathrm{Pic}^0(A)).$$

We will later see that there is an underlying abelian variety whose k-rational points form the group $\mathrm{Pic}^0(A)$.

Here is another criterion for a line bundle to belong to $\mathrm{Pic}^0(A)$.

6.2 Lemma. $\mathcal{L} \in \mathrm{Pic}^0(A)$ *if and only if, for* $m : A \times A \to A$ *the multiplication map, we have*

$$m^* \mathcal{L} \simeq p_1^* \mathcal{L} \otimes p_2^* \mathcal{L} = \mathcal{L} \boxtimes \mathcal{L} \in \mathrm{Pic}(A \times A).$$

[12] Professor Zhu stated things in slightly more general, but I was behind while TEXing notes.

Proof. Of course, if $m^*\mathcal{L} \simeq p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}$, then we can pull back along any inclusion

$$\{x\} \times A \to A \times A$$

and pulling $m^*\mathcal{L}$ along the imbedding gives $T_x^*\mathcal{L}$. Pulling back $\mathcal{L} \boxtimes \mathcal{L}$ gives $\mathcal{L}$. For the other direction, suppose $\mathcal{L} \in \mathrm{Pic}^0(A)$, and we consider the line bundle

$$\mathcal{M} = m^*\mathcal{L} \otimes (\mathcal{L}^{-1} \boxtimes \mathcal{L}^{-1}),$$

which we have to prove is trivial. By hypothesis it is trivial on each $A \times \{x\}$ and each $\{x\} \times A$. Now we can apply the "see-saw" lemma to conclude that $\mathcal{M}$ is trivial. ▲

Fix a line bundle $\mathcal{L} \in \mathrm{Pic}(A)$.

6.3 Definition. We let $K(\mathcal{L}) = \{x \in A(k) : T_x^*\mathcal{L} \simeq \mathcal{L}\}$, so that $K(\mathcal{L})$ is the kernel of $\phi_{\mathcal{L}}$. So $K(\mathcal{L})$ consists of those points in A such that $\mathcal{L}$ is invariant under translation by that point; if $\mathcal{L} \in \mathrm{Pic}^0(A)$, then $K(\mathcal{L}) = A$, and conversely.

First, we note that:

6.4 Lemma. *$K(\mathcal{L}) \subset A$ is closed.*

Proof. We look at $\mathcal{M} = m^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1}$ on $A \times A$ (where $m : A \times A$ is the multiplication map); then $K(\mathcal{L})$ consists exactly of those x such that when you restrict to $A \times \{x\}$, $\mathcal{M}$ is trivial. By the see-saw lemma, we find thus that $K(\mathcal{L})$ is closed. ▲

Thus $K(\mathcal{L})$ has in fact the structure of an *algebraic group.*

§2 A criterion for ampleness

Let A be an abelian variety, as before.

Here is the main theorem:

6.5 Theorem. *Let $\mathcal{L} = \mathcal{O}(D)$ for D an effective divisor on A. Then the following are equivalent:*

1. *$\mathcal{L}$ is ample.*
2. *$K(\mathcal{L})$ is finite.*[13]
3. *The set $H(D) = \{x \in A : x + D = D\}$ is finite.*
4. *The linear system $|2D|$ is base-point free and defines a finite morphism $A \to \mathbb{P}^N$.*

Before proving this, let us give a deep corollary:

6.6 Corollary. *Every abelian variety is projective.*

[13] So ampleness is at the opposite extreme from being in $\mathrm{Pic}^0(\mathcal{L})$.

Proof. We need to find an ample line bundle on A. Pick an affine open $U \subset A$ containing $0 \in A$, and let $D = A \setminus U$ (we can assume D is a divisor by removing parts of U). If we want to show that the associated line bundle is ample, we need to show that the collection $H(D)$ of points translation by which leaves D invariant is finite. Clearly $H(D) \subset U$ because translation by an element of $H(D)$ must leave U invariant. On the other hand, $H(D) \subset A$ is closed, and hence a complete variety: this implies that $H(D)$ is finite. We can thus use $\mathcal{O}(D)$ as our ample line bundle on A, by the previous theorem. ▲

We initially defined an abelian variety to be *complete* (or proper) rather than projective, but by the above corollary, we may as well have defined an abelian variety to have been projective. But historically, that's not the case. In the 1940s, Weil announced a proof of the Riemann hypothesis for algebraic curves over finite fields using the theory of Jacobians: that didn't exist at the time, so Weil had to construct it. Weil was unable to show that the Jacobian was projective, and he spend five years trying to rewrite the foundations of algebraic geometry to introduce abstract varieties. In particular, the Jacobian he constructed was an abstract complete variety. Later on, in the 1950s, it was proved that every abelian variety was projective anyway, but this is a deep theorem.

Let's now prove the theorem.

Proof of the ampleness criterion. Let's start by showing that 1 implies 2: if $\mathcal{L}$ is ample, we have to show that $K(\mathcal{L})$ is finite. If not, then the connected component $K(\mathcal{L})^0$ at zero is an abelian variety of positive dimension. By definition, $\mathcal{L}|_{K(\mathcal{L})^0}$ is translation-invariant, i.e.

$$\mathcal{L}|_{K(\mathcal{L})^0} \in \mathrm{Pic}^0(K(\mathcal{L})^0).$$

Equivalently, $m^*\mathcal{L}|_{K(L)^0 \times K(\mathcal{L})^0} \simeq (\mathcal{L} \boxtimes \mathcal{L})_{K(\mathcal{L})^0 \times K(\mathcal{L})^0}$. This is bad, though. When you restrict $\mathcal{L}$ to the abelian variety $K(\mathcal{L})^0$, it is still ample.

In fact, consider the map $K(\mathcal{L})^0 \to K(\mathcal{L})^0 \times K(\mathcal{L})^0$, $x \mapsto (x, -x)$. If we pull back the isomorphism $m^*\mathcal{L}|_{K(L)^0 \times K(\mathcal{L})^0} \simeq (\mathcal{L} \boxtimes \mathcal{L})_{K(\mathcal{L})^0 \times K(\mathcal{L})^0}$ to $K(\mathcal{L})^0$, we find that $\mathcal{O}_{K(\mathcal{L})^0} \simeq \mathcal{L} \otimes (-1)^*\mathcal{L}$. This means that $\mathcal{O}_{K(\mathcal{L})^0}$ is ample, a contradiction (if the trivial line bundle is ample, then the variety is quasi-affine). Obviously 2 implies 3.

Let's now show that 3 implies 4. We need to show that if $H(D)$ is finite, then $|2D|$ has no base points. Recall that by the theorem of the square, for $x, y \in A$, we have

$$(x + y + D) + D \sim (x + D) + (y + D).$$

If we let $y = -x$, then

$$2D \sim (x + D) + (-x + D),$$

and the divisors $(x+D)+(-x+D)$ all belong to the linear system $|2D|$. We'll use this to construct lots of elements of this linear system and show that it is base-point free. For any u, we want to find some x such that $u \notin x + D, -x + D$. This is equivalent to saying that $x \notin -u + D, x \notin -u - D$. But we can always find such an x for such a u. This shows that $|2D|$ has no base-points. (In fact, we have not used 3 yet: the base-point-freeness of $|2D|$ is *always* true for any effective divisor D.)

We now have to show that, under the hypotheses of 3, the induced morphism $\phi : A \to |2D|^*$ (where $|2D|^*$ denotes a projective space) is actually finite. This is really a morphism and not a rational map because the divisor has no base points. Since ϕ is proper, to show finiteness, it suffices to show that the fibers are finite. That is, for $p \in |2D|^*$, we have to show that $\phi^{-1}(p)$ is finite. Well, how should we show that? Otherwise, ϕ would contract a curve $C \subset A$ to a point.

Let $E \in |2D|$ be an element: then either $E \cap C \supset C$ or $E \cap C = \emptyset$. This is because the pull-back of the linear system $|2D|^*$ to C (the collection of hyperplane sections in C) has to be trivial. For generic E, we must have $E \cap C = \emptyset$ then.

Now we have:

6.7 Lemma. *Let $C \subset A$ be an irreducible curve. Let E be a divisor on A such that $C \cap E = \emptyset$. Then for every $x, y \in C$, we have*

$$x - y + E = E.$$

If we prove this lemma, we will be done with the proof that 3 implies 4, because we can take $E = x + D + (-x + D)$ for generic x and the set of $z \in A$ such that $z + E = E$ is finite by hypothesis. So we just need to prove the lemma.

Proof. Let $\mathcal{L}$ be the line bundle on A given by E, i.e. $\mathcal{L} = \mathcal{O}(E)$. By this assumption, we have that $\mathcal{L}|_C = \mathcal{O}_C$. This implies that $T_x^*\mathcal{L}, x \in C$ forms a family of line bundles on C: we have a multiplication $m : C \times A \to A$, and the pull-back $m^*\mathcal{L}$ is a line bundle on $C \times A$. For any $x \in A$, the Euler characteristic $\chi(m^*\mathcal{L}_{C\times\{x\}}) = \chi(\mathcal{O}_C)$, because the Euler characteristic is constant in a family. So we have that $\chi(T_x^*\mathcal{L}) \simeq \chi(\mathcal{L})$ for all $x \in A$, which means that

$$\deg T_x^*\mathcal{L} = \deg \mathcal{O}_C = 0, \quad \forall x \in C$$

by Riemann-Roch. This means in particular that $-x + E$ (global a section of the line bundle $T_x^*\mathcal{L}$) either contains C or does not intersect C (since a global section over C must be either zero or nonvanishing).

Fix $x, y \in C, z \in E$. Let us look at the divisor $(x - z) + E$: it contains x (as $z \in E$): therefore, by this argument, $x - z + E \supset C$ (because it intersects C at x). So it contains y, and then we are done. ▲

Finally, we should show that 4 implies 1. We have a finite morphism

$$\phi : A \to \mathbb{P}^N = |2D|^*.$$

We have that $\phi^*\mathcal{O}(1) = \mathcal{L}^{\otimes 2}$. We need to show that $\mathcal{L}$ is ample. But the pull-back of an ample line bundle by a finite morphism is ample, so $\mathcal{L}^{\otimes 2}$, hence $\mathcal{L}$, is ample.[14] ▲

We can now show that abelian varieties are divisible.

6.8 Corollary. *For any $n \in \mathbb{Z} \setminus \{0\}$, the multiplication by n map $n_A : A \to A$ is surjective.*

[14] This is slightly different from the argument in class.

Proof. Equivalently, we show that $\ker n_A$ is finite (by the dimension theorem). Choose an ample line bundle $\mathcal{L}$ on A; we have

$$n_A^*\mathcal{L} = \mathcal{L}^{(n^2+n)/2} \otimes (-1)^*\mathcal{L}^{(n^2-n)/2}$$

and this is thus ample on A. On the other hand, $n_A^*\mathcal{L}|_{\ker n_A}$ is a trivial line bundle, so the trivial line bundle is ample on $\ker n_A$. This implies that $\ker n_A$ is finite. ▲

Let us just state the following result, which we will prove next time:

Recall that the *degree* of a dominant morphism of algebraic varieties of the same dimension is the degree of the associated field extension.

6.9 Theorem. *The degree of $n_A : A \to A$ is n^{2g} for $g = \dim A$. Consequently, if n_A is separable (which is true iff $p \nmid n$), then $\ker n_A$ has cardinality n^{2g}. The inseparable degree of p_A is at least p^g.*

Lecture 7
2/22

§1 A correction

First, a correction. Last time, we gave an argument that if $D \subset A$ was a divisor on the abelian variety A such that

$$H(D) := \{x \in A : x + D = D\}$$

was finite, then the associated map

$$A \to |2D|^*$$

was finite.

We had the lemma that if $E \subset A$ was a divisor and $C \subset A$ a curve such that $C \cap E = \emptyset$, then for any $x, y \in C$, we had $(x - y) + E = E$.

Let us now reprove that the lemma implies the finiteness of $A \to |2D|^*$.

Proof. We showed that if $A \to |2D|^*$ was not finite, then there would be a curve C such that $C \cap D = \emptyset$.

Write $D = \sum D_i$ for the D_i irreducible divisors. For generic $x \in A$, we know that C does not intersect $(x + D) \cup (-x + D)$. In particular, for each i, we have that

$$C \cap (x + D_i) = C \cap (-x + D_i) = \emptyset.$$

This implies (by the lemma) that for any $y, z \in C$, we have that $(y-z)+(x+D_i) = x+D_i$ and $(y - z) + (-x + D_i) = -x + D_i$. This implies that $(y - z) + D = D$.

Consequently, for every $y, z \in C$, we get that $y-z \in H(D)$, which is a contradiction. ▲

§2 Isogenies

If A is an abelian variety, we have a map $n_A : A \to A$ given by multiplication by A. We saw last time that n_A was surjective and $\ker n_A$ was finite.

Here is a more general situation:

7.1 Definition. Let A, B be abelian varieties. A homomorphism $\alpha : A \to B$ is called an **isogeny** if it is surjective and the kernel is finite (which means that α is finite).

So, n_A is an isogeny $A \to A$. The composite of two isogenies is an isogeny. Later, we will see that if one has an isogeny $A \to B$, then there is an isogeny in the other direction such that the composition is a multiplication by n map.

§3 The degree of n_A

We now want to compute the degree of n_A.

7.2 Theorem. $\deg n_A = n^{2g}$ *for* $g = \dim A$.

To prove this, we use the following:

7.3 Definition. Let X be a complete variety of dimension g, and $\mathcal{L}$ a line bundle on X. Let $\mathcal{F}$ be a coherent sheaf on X. Consider the Euler characteristics $\chi(\mathcal{F} \otimes \mathcal{L}^n)$, and write

$$P_{\mathcal{L}}(\mathcal{F}, n) := \chi(\mathcal{F} \otimes \mathcal{L}^{\otimes n});$$

this is a polynomial of degree $\leq g$. If $\mathcal{L}$ is ample, then this is the usual Hilbert polynomial.[15] Let $d_{\mathcal{L}}(\mathcal{F})$ be $g!$ times the leading coefficient of $P_{\mathcal{L}}(\mathcal{F}, \cdot)$ and let

$$d_{\mathcal{L}} := d_{\mathcal{L}}(\mathcal{O}_X).$$

We will need the following:

7.4 Proposition.

1. *Let $\mathcal{F}$ be a coherent sheaf on X with generic rank r. Then $d_{\mathcal{L}}(\mathcal{F}) = r d_{\mathcal{L}}$.*
2. *Let $f : X \to Y$ be a dominant morphism of complete varieties of the same dimension, and let $\mathcal{L}$ be a line bundle on Y. Then* $(\deg f) d_{\mathcal{L}} = d_{f^*\mathcal{L}}$.

We postpone the proof.

Proof of the theorem. Let $\mathcal{L}$ be ample on the abelian variety A. We can assume that $\mathcal{L}$ is symmetric, $\mathcal{L} \simeq (-1)^*\mathcal{L}$ (by replacing $\mathcal{L}$ with $\mathcal{L} \otimes (-1)^*\mathcal{L}$). In this case, we have that

$$n_A^*\mathcal{L} \simeq \mathcal{L}^{n^2}.$$

Now if we compare the degrees, we have that

$$\deg n_A \deg \mathcal{L} = \deg \mathcal{L}^{n^2} = n^{2g} \deg \mathcal{L},$$

and since $\deg \mathcal{L} > 0$ ($\mathcal{L}$ being ample), we are done. (Note that $\deg \mathcal{L}^k = k^g \deg \mathcal{L}$ by substitution.) ▲

[15] We will only use this case, in fact.

Let us now prove the proposition.

Proof. We will assume that X is smooth, which is the only case that we needed. We will also assume that, in the second statement, the map f is finite.

Let us start by proving the first claim. If $\mathcal{F}$ has generic rank r, then that means that there is an open $U \subset X$ such that $\mathcal{F}|_U \simeq \mathcal{O}_U^r$. So, $D = X \setminus U$ can be chosen to be a divisor. Since X is smooth, we have a line bundle $\mathcal{M} = \mathcal{O}(D) = \mathcal{I}_D^{-1}$ is the inverse of the ideal sheaf of D; this has a natural section $\sigma \in \Gamma(X, \mathcal{M})$ whose zero locus is precisely D.

For any $m \in \Gamma(U, \mathcal{F})$, there exists some n such that $m\sigma^n$ extends to a section of $\mathcal{F} \otimes \mathcal{M}^n$. Choose a basis $e_1, \dots, e_r$ for $\Gamma(U, \mathcal{F})$ (which is a free module over $\Gamma(U, \mathcal{O}_U)$), and choose $N \gg 0$ such that each $e_i \otimes \sigma^N$ extends to a section of $\mathcal{F} \otimes \mathcal{M}^N$ on X. Then we have r global sections of $\mathcal{F} \otimes \mathcal{M}^N$ and we get a map

$$\mathcal{O}_X^r \to \mathcal{F} \otimes \mathcal{M}^N.$$

The quotient is supported on D, and the map is injective because it is injective on U. Consequently, we get an exact sequence

$$0 \to (\mathcal{M}^{-N})^r \to \mathcal{F} \to \mathcal{T} \to 0$$

and we can compare the Hilbert polynomials. We find

$$d_{\mathcal{L}}(\mathcal{F}) = r d_{\mathcal{L}}(\mathcal{M}^{-N})$$

because the torsion sheaf has no degree (it is supported on a smaller dimension set). However, $d_{\mathcal{L}}(\mathcal{M}) = d_{\mathcal{L}}(\mathcal{O})$ (again because they differ by a subset of proper codimension), so we are done.

Now let's prove the second claim. We want to calculate $\deg f^*\mathcal{L}$ but let's first calculate $\chi(f^*\mathcal{L}^n)$. We know that

$$H^i(X, f^*\mathcal{L}^n) = H^i(Y, f_*f^*\mathcal{L}^n) = H^i(Y, f_*\mathcal{O}_X \otimes \mathcal{L}^n).$$

and therefore

$$\chi(f^*\mathcal{L}^n) = \chi(f_*\mathcal{O}_X \otimes \mathcal{L}^n).$$

Consequently, we find

$$d_{f^*\mathcal{L}} = d_{\mathcal{L}}(f_*\mathcal{O}_X)$$

and $f_*\mathcal{O}_X$ has generic rank $\deg f$. So this follows from the first claim. ▲

§4 The inseparability degree

Anyway, we have now given a complete proof of the fact that

$$\deg n_A = n^{2g}.$$

But there is another question we might ask. If L/K is a finite extension of fields, then we can always write it as a composite of a purely inseparable extension and a separable extension. The degree of the first component is called the *purely inseparable* degree. We want to determine the inseparable degree of n_A.

7.5 Theorem. *If $p \nmid n$, then n_A is separable. The inseparable degree of p_A is at least p^g.*

Proof. First, let's assume $p \nmid n$. We want to show that $n_A : A \to A$ is separable. But this is equivalent to saying that n_A is smooth and that follows because n_A is smooth at the origin: $(dn_A)_0 : T_0A \to T_0A$ is multiplication by n and is surjective.

(Alternatively, we can argue by noting that the degree of n_A, as computed earlier, is not divisible by p, and consequently there can be no purely inseparable component of the field extension.)

Next, we have to look at the inseparable degree of p_A. Note that

$$(dp_A)_0 : T_0A \to T_0A$$

is multiplication by p, and is consequently zero. That means that the pull-back map $p_A^*\Omega_{A/k} \to \Omega_{A/k}$ is zero. At the rational differentials, this means that

$$p_A^* : \Omega_{k(A)/k} \to \Omega_{k(A)/k}$$

is zero. Consequently, if we have a rational function $f \in k(A)$, this means that $p_A^* df = 0$, or $d(p_A^* f) = 0$. But that means $p_A^*(f) \in k(A)^p k$. The kernel of

$$k(A) \to \Omega_{k(A)/k}$$

is exactly this. Therefore, p_A^* of $k(A)$ lands in $k(A)^p$ (if k is perfect). This means that the inseparable degree of p_A^* must be at least p^g. ▲

7.6 Corollary. *If $A[n]$ denotes the n-torsion points of A, then*

$$A[n] = \begin{cases} (\mathbb{Z}/n\mathbb{Z})^{2g} & p \nmid n \\ (\mathbb{Z}/p^m\mathbb{Z})^i, & n = p^m, 0 \leq i \leq g. \end{cases}$$

Proof. We know that the cardinality of $A[n]$ is just the number of points in the fiber at zero, or the number of points in a generic fiber: that's the separable degree of $n_A : A \to A$. In particular, for any ℓ prime, we have that

$$\mathrm{card} A[\ell] = \begin{cases} \ell^{2g} & \ell \neq p \\ \ell^i & \ell = p, \ 0 \leq i \leq g \end{cases}$$

because in the second case, the separable degree is $p^i, 0 \leq i \leq g$. But now, we have that for any ℓ, there is an exact sequence

$$0 \to A[\ell] \to A[\ell^{n+1}] \xrightarrow{\ell} A[\ell] \to 0$$

and by induction the corollary follows (because each $A[\ell]$ is annihilated by ℓ). ▲

Lecture 8
2/24

Let us briefly make the main claim for the next few lectures. So far, we've basically managed to answer the first question made at the beginning: abelian varieties are *abelian*, and we described the torsion points. Next, we're going to study the dual abelian variety $\mathrm{Pic}^0(A)$ of an abelian variety. To start, we'll study the general theory of group schemes, and then we'll move to dual abelian varieties.

§1 Group schemes

Fix a scheme S (locally noetherian).

8.1 Definition. A **group scheme** G over S, $G \to S$, is a group object in the category of schemes over S.

What is the meaning of this definition? If $\mathcal{C}$ is a category, we can construct a new category $\hat{\mathcal{C}}$, the category of contravariant functors $\mathcal{C} \to \mathbf{Set}$. So

$$\hat{\mathcal{C}} = \{F : \mathcal{C}^{op} \to \mathbf{Sets}\}.$$

There is a natural imbedding

$$h : \mathcal{C} \to \hat{\mathcal{C}}$$

which sends an object X to the functor h_X sending $h_X(Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$. The **Yoneda lemma** states that this functor $h : \mathcal{C} \to \hat{\mathcal{C}}$ is fully faithful. The essential image of h (i.e. the functors isomorphic to h_X for some X) are called **representable functors.**

We can now define the notion of a **group object** in $\mathcal{C}$.

8.2 Definition. If we had a functor $G : \mathcal{C}^{op} \to \mathbf{Grp}$ to the category of groups (instead of to the category of sets), we can call this a **group functor.** To give a group functor is to give an object of $\hat{\mathcal{C}}$ together with some additional structure on it.

A **group object** in $\mathcal{C}$ is a triple (G, X, α) where $G : \mathcal{C}^{op} \to \mathbf{Grp}$ is a group functor, and α is an isomorphism in $\hat{\mathcal{C}}$ between $G \overset{\alpha}{\simeq} h_X$.

This means that X is a group object if for every $Y \in \mathcal{C}$, the set $h_X(Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$ is equipped with a group structure which is natural in Y: that is, for any $Z \to Y$, the corresponding map

$$\mathrm{Hom}(Y, X) \to \mathrm{Hom}(Z, X)$$

is a group homomorphism.

Assume now that $\mathcal{C}$ has finite products (including a terminal object $*$, which is the empty product). In this case, we can give a characterization of group objects totally inside $\mathcal{C}$.

In this case, a group object in $\mathcal{C}$ is the same thing as the following data:

1. An object $X \in \mathcal{C}$.

2. Maps $m : X \times X \to X$ ("multiplication"), $s : X \to X$ ("inversion"), $e : * \to X$ ("identity").

3. The maps are required to satisfy the usual axioms for a group. For instance, we should have associativity, which means that the following should commute:

$$\begin{tikzcd} X \times X \times X \arrow[r, "m\times 1"] \arrow[d, "1\times m"] & X \times X . \arrow[d, "m"] \\ X \times X \arrow[r, "m"] & X \end{tikzcd}$$

Similarly, we should have the commutativity of:

$$\begin{tikzcd} X \arrow[r, "1\times s"] \arrow[d] & X \times X \arrow[d, "m"] \\ * \arrow[r, "e"] & X \end{tikzcd}$$

The point is that the usual definition of a group can be expressed solely in terms of diagrams, and these diagrams make sense in any category with products. This is another way of defining a group object. If we have data as above, then for every Y, we get a natural map

$$m : h_{X\times X}(Y) = h_X(Y) \times h_X(Y) \to h_X(Y)$$

and an inversion map

$$s : h_X(Y) \to h_X(Y)$$

and a unit map

$$e : h_*(Y) = * \to h_X(Y).$$

So this gives a group object structure on X. Conversely, using the Yoneda lemma, if we have a group object, we can get diagrams as above.

With this in mind, we can understand a group scheme over S in two ways.

1. It can be understood as a scheme $G \to S$ together with various maps $m : G \times_S G \to G, s : G \to G$, and $e : S \to G$ (since S is the final object in the category of schemes over S).

2. For every T over S, the set $G(T)$ of T-points (over S—that is, $\mathrm{Hom}_S(T, G)$) has a natural group structure.

If $S' \to S$ is any morphism, then base-change gives a new group scheme $G_{S'}$ over S'. Note that we can talk about **group subschemes** in a natural sense. It also makes sense to talk about **morphisms** between group schemes: if G, H are group schemes over S, then a morphism $G \to H$ is a morphism of schemes $f : G \to H$ which commutes with the group structure. We will soon give some examples.

8.3 Definition. If we have a morphism $f : G \to H$ of group schemes, we define the **kernel** $\ker f$ to be the pull-back

$$\begin{tikzcd} \ker f \arrow[r] \arrow[d] & G \arrow[d, "f"] \\ S \arrow[r, "e"] & H \end{tikzcd}$$

If e is a closed imbedding, then $\ker f$ is a closed group subscheme of S.

§2 Examples of group schemes

8.4 Example. If A is an abelian variety over a field k, then A becomes a group scheme over Spec$k$. (Incidentally, the definitions given today make precise the definition of an abelian variety.)

8.5 Example. If S is a scheme, the **additive group** $\mathbb{G}_a = \mathrm{Spec}\mathcal{O}_S[T]$ is $\mathbb{A}^1_S$, together with the group structure

$$\mathbb{G}_a \times_S \mathbb{G}_a \to \mathbb{G}_a$$

given by the pull-back morphism on functions (recall that there is an equivalence of categories between affine S-schemes and quasi-coherent sheaves of algebras)

$$\mathcal{O}_S[T] \to \mathcal{O}_S[T] \otimes_{\mathcal{O}_S} \mathcal{O}_S[T], \quad T \mapsto T \otimes 1 + 1 \otimes T.$$

The unit map comes from setting $T = 0$ and the inverse map corresponds to $T \to -T$.

For any scheme $X \to S$, we have

$$\mathbb{G}_a(X) = \Gamma(X, \mathcal{O}_X)$$

with the usual addition (exercise).

8.6 Example. Similarly, we can define the **multiplicative group** $\mathbb{G}_m$ over S, which is defined as Spec$\mathcal{O}_S[T, T^{-1}]$ whose codiagonal map is (on the level of algebras) $T \mapsto T \otimes T$ and whose inversion map is $T \mapsto T^{-1}$. Then $\mathbb{G}_m(X) = \Gamma(X, \mathcal{O}_X^*)$ with the usual multiplication.

For an abelian group scheme G, and $n \in \mathbb{Z}$, we can define multiplication by $n : G \to G$. This can be done on the level of functors of points. For instance, we can describe multiplication by n on $\mathbb{G}_m$ by

$$\mathbb{G}_m(X) \to \mathbb{G}_m(X), \quad \Gamma(X, \mathcal{O}_X^*) \overset{s \mapsto s^n}{\to} \Gamma(X, \mathcal{O}_X^*).$$

8.7 Example. We can consider the kernel of this map $n : \mathbb{G}_m \to \mathbb{G}_m$, and it turns out to be

$$\mathbb{G}_m[n] = \ker n = \mathrm{Spec}\mathcal{O}_S[t]/(t^n - 1).$$

This is often denoted μ_n. For a scheme X over S, we have that $\mu_n(S)$ is the collection of nth roots of unity in the ring of global sections.

8.8 Example. Here is a group functor. Let $X \to S$ be a scheme over S. We can define

$$\mathrm{Pic}_{X/S} : \mathrm{Sch}/S \to \mathbf{Grp}$$

sending any T to the set of isomorphism classes of $X \times_S T$ modulo isomorphism classes of line bundles on T. This is called the **Picard functor.**

In general, when you give a group functor, it need not be representable. If $\mathrm{Pic}_{X/S}$ is representable, then the corresponding scheme is called the **Picard scheme** of X. We will study this in the case in the case of X an abelian variety over a field.

§3 Vector fields

From now on, we assume that $G \to S$ is locally of finite type. We have the *coherent* sheaf $\Omega_{G/S}$ on G: we could describe it such that

$$\operatorname{Hom}_{\mathcal{O}_S}(\Omega_{G/S}, \mathcal{F}) = \operatorname{Der}_{\mathcal{O}_S}(\mathcal{O}_G, \mathcal{F})$$

for any quasicoherent $\mathcal{F}$. In particular, elements of

$$\operatorname{Hom}_{\mathcal{O}_S}(\Omega_{G/S}, \mathcal{O}_X) = \operatorname{Der}_{\mathcal{O}_S}(\mathcal{O}_G, \mathcal{O}_G)$$

are called **vector fields.**

Let's say we have a vector field D on G (so a derivation on functions). After a base-change along S via $u : T \to S$, we get a pull-back maps from

$$\operatorname{Hom}(\Omega_{G/S}, \mathcal{O}_S) \to \operatorname{Hom}(\Omega_{G_T/T}, \mathcal{O}_T)$$

and consequently we can get a new derivation (or vector field) u^*D.

Now we're going to start using the group structure.

8.9 Definition. We say that D is a **right-invariant** vector field if for any $g \in G(T)$ and $f \in \mathcal{O}_G$, $D(R_g^*(f)) = R_g^*D(f)$.

We require this for any T because we might not have enough sections $S \to G$.

8.10 Definition. We denote the set of right-invariant vector fields on G by $\operatorname{Lie}(G)$.

Note that this construction commutes well with pull-backs along S. In fact, $\operatorname{Lie}(G)$ is a *sheaf* of $\mathcal{O}_S$-modules on S.

The next lemma shows that we get a Lie bracket.

8.11 Lemma. *Let $D_1, D_2 \in \operatorname{Lie}(G)$; then $[D_1, D_2] \in \operatorname{Lie}(G)$. If $p\mathcal{O}_S = 0$, then $D_1^p \in \operatorname{Lie}(G)$.*

The point is that the commutator is always a derivation (which is even right-invariant if we start with invariant things), and the pth power ends up being a derivation too, basically because of the binomial theorem and the fact that $\binom{p}{i} \equiv 0 \mod p$ for $i \in \{1, 2, \dots, p-1\}$.

So:

8.12 Corollary. $\operatorname{Lie}(G)$ *is a restricted Lie algebra.*

Lecture 9
2/27

§1 The Lie algebra again

Let us now study group schemes in the case where the base is a field.

Let $S = \operatorname{Spec} k$ for k a field. Let G/k be a group scheme. We defined the **Lie algebra** $\operatorname{Lie}(G)$ to be the set of left-invariant vector fields on G. (We said last time right-invariant, but left-invariant is more standard.) In other words, we were looking for k-derivations

$$D : \mathcal{O}_G \to \mathcal{O}_G$$

such that $DL_x^* = L_x^* D$. This is a k-vector space. (In general, we get a sheaf of $\mathcal{O}_S$-modules.) As we saw, if we have two left-invariant derivations $D_1, D_2 \in \mathrm{Lie}(G)$, then $[D_1, D_2] \in \mathrm{Lie}(G)$; we also saw that if $p = \mathrm{char} k$, then $D^p \in \mathrm{Lie}(G)$. The conclusion is that $\mathrm{Lie}(G)$ is actually a restricted Lie algebra (also called a p-Lie algebra).

To say that $\mathrm{Lie}(G)$ is a **restricted Lie algebra** means that there are two operations on $\mathrm{Lie}(G)$:

1. The bracket $[\cdot, \cdot] : \mathrm{Lie}(G) \times \mathrm{Lie}(G) \to \mathrm{Lie}(G)$ which is k-linear, skew-symmetric, and satisfies the Jacobi identity. This gives rise to the adjoint representation of $\mathrm{Lie}(G)$ on itself.

2. There is a p-th power operation $(\cdot)^p : \mathrm{Lie}(G) \to \mathrm{Lie}(G)$ such that $(\lambda X)^{(p)} = \lambda^p X^{(p)}$ for $\lambda \in k, X \in \mathrm{Lie}(G)$.

3. $\mathrm{Ad} X^p = (\mathrm{Ad} X)^p$.

4. $(X+Y)^{(p)} = X^{(p)} + Y^{(p)} + F_p(\mathrm{Ad}X, \mathrm{Ad}Y)Y$ for some universal "noncommutative" polynomial F_p. (The explicit expression is not important for us, but F_p has no constant term.)

In general, a **restricted Lie algebra** is a k-vector space endowed with the above structure of a Lie bracket and a pth power operation. Note that if a restricted Lie algebra is abelian, then $(\cdot)^{(p)}$ is a group homomorphism (though not k-linear).

Remark. If G is an abelian variety, then $\mathrm{Lie}(G)$ turns out to be abelian, and the pth power map turns out to be a pretty important group homomorphism.

Sometimes it is more convenient to define the Lie algebra of a Lie group as the tangent space at the origin. Let $T_e G$ be the tangent space of G at the identity $e \in G$. Alternatively, this is $\mathrm{Hom}_k(\mathfrak{m}_e/\mathfrak{m}_e^2, k)$. From Grothendieck's point of view, this is $\mathrm{Hom}_k(\mathrm{Spec} k[\epsilon]/\epsilon^2 \to G)$, or the set of maps

$$\mathrm{Spec} k[\epsilon]/\epsilon^2 \to G$$

which maps the closed point into e. When G is a group scheme, this can be written as

$$\ker(G(\mathrm{Spec} k[\epsilon]/\epsilon^2) \to G(k)).$$

(Note: in general, if $T_1 \to T_2$ is a morphism of schemes, then we get a group homomorphism $G(T_2) \to G(T_1)$). In particular, we get the multiplicative structure on the kernel purely from the functorial point of view.

9.1 Proposition. *There is a restriction map* $\mathrm{Lie}(G) \to T_e(G)$ *sending a vector field to its restriction at e. In other words, a vector field D is sent to the map $\mathfrak{m}_e/\mathfrak{m}_e^2 \to k$ sending $f \mapsto (Df)(e)$. This restriction map is an isomorphism.*

Proof. We start with the following. Let $\Lambda = k[\epsilon]/\epsilon^2$.

9.2 Lemma. *Let X/k be a scheme. To give a vector field or derivation $D : \mathcal{O}_X \to \mathcal{O}_X$ is the same thing as giving an automorphism of Λ-algebras $\widetilde{D} : \mathcal{O}_X \otimes_k \Lambda \to \mathcal{O}_X \otimes_k \Lambda$ which reduces to the identity.*

Proof. In fact, to give a map $\widetilde{D} : \mathcal{O}_X \otimes_k \Lambda \to \mathcal{O}_X \otimes_k \Lambda$, then we have to give a map $\mathcal{O}_X \oplus \epsilon\mathcal{O}_X \to \mathcal{O}_X \oplus \epsilon\mathcal{O}_X$ and the second component gives a derivation. ▲

So we can think of the map $\widetilde{D}$ as giving an automorphism of the scheme $\widetilde{X} = X \times_k \Lambda$ which restricts to the identity on X. Intuitively, vector fields give "infinitesimal automorphisms" of X (i.e. automorphisms of $\widetilde{X}$).

Anyway, if $X = G$ is a group scheme, then a vector field D is left-invariant if and only if the following diagram commutes:

$$\begin{tikzcd}
\widetilde{G} \times \widetilde{G} \arrow[r, "1\times\widetilde{D}"] \arrow[d, "m"] & \widetilde{G} \times \widetilde{G} \cdot \arrow[d, "m"] \\
\widetilde{G} \arrow[r, "\widetilde{D}"] & \widetilde{G}
\end{tikzcd}$$

(Exercise.)

So now we need to construct the inverse map. Given an element of T_eG, we need an element of $\mathrm{Lie}(G)$. Right now, we get an element of $\ker(G(\Lambda) \to \ker G(k))$, and once we have a point of $G(\Lambda)$, we get a right translation map $\widetilde{G} \to \widetilde{G}$. This is associated to a left-invariant vector field on G, which is what we want. ▲

Another application is the following. Let $\Lambda' = \Lambda \otimes_k \Lambda = k[\epsilon_1, \epsilon_2]/(\epsilon_1^2, \epsilon_2^2)$; this has two projections

$$p_1, p_2 : \mathrm{Spec}\Lambda' \rightrightarrows \mathrm{Spec}\Lambda$$

but there is also a third one $p_3 : \mathrm{Spec}\Lambda' \to \mathrm{Spec}\Lambda$ coming from the map $\epsilon \mapsto \epsilon_1\epsilon_2$.

In differential geometry, we know that to calculate the bracket of x, y, we have to form $\exp(tx)\exp(sy)\exp(-tx)\exp(-sy)$ and take its derivative at zero. In algebraic geometry, we can imitate this with s, t replaced by ϵ_1, ϵ_2 (and nilpotency allows us to imitate all this).

9.3 Lemma. *Let $D_1, D_2 \in \mathrm{Lie}(G)$, $D_3 = [D_1, D_2]$. Then, as automorphisms of $G \times_k \Lambda'$, we have $p_1^*\widetilde{D}_1 p_2^*\widetilde{D}_2 p_1^*\widetilde{D}_1^{-1} p_2^*\widetilde{D}_2^{-1} = p_3^*\widetilde{D}_3$.*

Here p_1^*, p_2^*, p_3^* refers to the operation of pulling back automorphisms (base change). We'll omit the proof.

9.4 Corollary. *If G is commutative (e.g. for an abelian variety), then the Lie algebra* $\mathrm{Lie}(G)$ *is abelian.*

Proof. As we saw in the previous proof, the infinitesimal automorphisms $\widetilde{D_i}$ are associated to right translations, so they all commute with each other. ▲

§2 General facts

Now let us give some general facts. Let G/k be a group scheme, locally of finite type. Let G^0 be the connected component at the identity.

9.5 Proposition. *G^0 is open and closed and is a subgroup scheme of G. G^0 is geometrically irreducible and is of finite type.*

Sketch of proof. G^0 is a connected component, so it is closed; it is also open by general topology (for noetherian spaces).

A connected scheme locally of finite type over a scheme containing a rational point is geometrically connected (this is a general fact which we won't prove); this implies that G^0 is geometrically connected.

To see that it is a group scheme, we need to check that the multiplication map $G^0 \times G^0 \to G$ factors through G^0, but $G^0 \times_k G^0$ is connected, so this is easy.

To prove that G^0 is geometrically connected, we can base change to the algebraic closure $\overline{k}$. The reduced subscheme $(G^0 \times_k \overline{k})_{red}$ becomes a group scheme over $\overline{k}$. Now we find that $(G^0 \times_k \overline{k})_{red}$ contains a nonsingular point; since we have a group structure, this is a smooth scheme over $\overline{k}$. Since it is connected, it must be irreducible.

To see that G^0 is of finite type, there is a little trick to show that it is quasi-compact. For any nonempty open $U \subset G^0$, the map $m : U \times U \to G^0$ turns out to be surjective. (The counterpart of this observation in the theory of Lie groups is that they are generated by a small neighborhood of the identity, if they are connected.) ▲

Notice that we did not claim that G^0 is smooth. There are lots of nonreduced group schemes. However, in characteristic zero, we have:

9.6 Theorem. *If* $\mathrm{char} k = 0$*, any group scheme is automatically smooth (and therefore reduced).*

Sketch of proof. To show that it is smooth, we can base-change to $\overline{k}$ and we may just assume that k is algebraically closed, as a result. So we just need to show that the scheme is nonsingular. Alternatively, we need to show that the completed local ring at a point is a power series ring. We can reduce to showing that $\widehat{\mathcal{O}_{G,e}}$ is a power series ring.

Let $dx_1, \dots, dx_n$ form a basis for $\mathfrak{m}_e/\mathfrak{m}_e^2$, the cotangent space at the identity. We want to show that the completion $\widehat{\mathcal{O}_{G,e}}$ is the power series ring in $x_1, \dots, x_n \in \mathfrak{m}$. OK, choose a dual basis $\delta_1, \dots, \delta_n \in T_e(G)$. This gives us left invariant vector fields $D_1, \dots, D_n \in \mathrm{Lie}(G)$.

Let $A = \widehat{\mathcal{O}_{G,e}}$ be the completed local ring at x. There is a natural map

$$k[[x_1, \dots, x_n]] \to A$$

and we want to construct an inverse map. But we can send any $f \in A$ to $\sum_\alpha \frac{1}{\alpha} D^\alpha f$ as α ranges over multi-indices and $D^\alpha = D_1^{\alpha_1} D_2^{\alpha_2} \dots D_n^{\alpha_n}$. (**Question**: the D's don't commute.) One can check that these two constructions are inverse to each other. ▲

This fails in characteristic p. Consider for instance $\mu_p = \mathrm{Spec} k[z]/(z^p - 1) = \mathrm{Spec} k[z]/(z-1)^p$. This isn't reduced. We can also define $\alpha_p = \mathrm{Spec} k[t]/t^p$ where multiplication is $\Delta(t) = 1 \otimes t + t \otimes 1$.

Lecture 10
2/29

§1 The Picard scheme

We shall assume that X/k is a **projective variety**, by which we mean something which is geometrically integral and which has a rational point $* \in X(k)$. We can introduce a functor

$\mathrm{Pic}_{X/k}(T) = \{\text{iso classes of line bundles on } X \times T\} \,/\, \{\text{iso classes of line bundles of the form } p^*\mathcal{L}, \mathcal{L} \in \mathrm{Pic}(T$

This is a group functor on the category of schemes over k.

The following lemma is straightforward.

10.1 Lemma. *We can interpret* $\mathrm{Pic}_{X/k}(T)$ *this as the set of pairs* $(\mathcal{L}, \alpha)$ *where* $\mathcal{L}$ *is a line bundle on* $X \times T$ *and* $\alpha : \mathcal{L}|_{*\times T} \simeq \mathcal{O}_T$ *(modulo isomorphism).*

So we have to have a line bundle on $X \times T$ and a given trivialization on one fiber. This is the description of the Picard functor that we will use in the sequel.

10.2 Theorem (Grothendieck)**.** $\mathrm{Pic}_{X/k}$ *is represented by a scheme (which is automatically a group scheme), locally of finite type,*

The connected component $\mathrm{Pic}^0_{X/k}$ *at the identity is a quasi-projective variety; it is projective if* X *is smooth.*

We will treat this theorem as a black box.

10.3 Example. The k-points of $\mathrm{Pic}_{X/k}$, or $\mathrm{Pic}_{X/k}(k)$, can be described as pairs of line bundles $\mathcal{L}$ on X and a trivialization $\mathcal{L}|_* \simeq k$. The need to have the trivialization is to prevent line bundles from having nontrivial automorphisms. (As a set, this is the same as the set of isomorphism classes of line bundles.)

When we just work with all line bundles, it is better to treat them not as a set but a *groupoid*, because there are nontrivial automorphisms. Requiring the trivialization gets rid of this and makes the Picard functor a functor to sets.

10.4 Example. In general, $\mathrm{Pic}_{X/k}(T) = \mathrm{Hom}(T, \mathrm{Pic}_{X/k})$. If we take $T = \mathrm{Pic}_{X/k}(X)$, we have the identity map

$$1 : \mathrm{Pic}_{X/k} \to \mathrm{Pic}_{X/k}$$

which leads to a *universal* line bundle $\mathcal{L}_{univ}$ on $X \times \mathrm{Pic}_{X/k}$ together with a trivialization $\alpha_{univ} : \mathcal{L}_{univ}|_{*\times \mathrm{Pic}_{X/k}} \simeq \mathcal{O}_{\mathrm{Pic}_{X/k}}$. This is sometimes called the **Poincaré line bundle.**

In general, if we are given any map $T \to \mathrm{Pic}_{X/k}$, we can pull back $\mathcal{L}_{univ}, \alpha_{univ}$ to get a line bundle and a trivialization. This is the pair corresponding to $T \to \mathrm{Pic}_{X/k}$.

This representability theorem tells us the existence of a scheme $\mathrm{Pic}_{X/k}$ representing this functor; equivalently, it tells us we get a universal line bundle and universal trivialization such that any such data on any scheme is a pull-back of such.

For instance, for each point $\lambda \in X(k)$, then we can pull-back $(\mathcal{L}_{univ}, \alpha_{univ})$ over $X \times \mathrm{Pic}_{X/k}$ to X to get a line bundle over X (this is what we said before: the k-points are in bijection with isomorphism classes of line bundles).

Anyway, we'll assume the existence of such a scheme, but we'll do everything else.

§2 $\mathrm{Pic}^0_{X/k}$

Keep the same notations of the previous section. We'll throughout assume that X has a rational point.

10.5 Definition. Let $\mathcal{M}, \mathcal{N}$ be two line bundles on X. We say that $\mathcal{M}, \mathcal{N}$ are **algebraically equivalent** if there exist:

1. Connected schemes $T_1, \dots, T_n$ of finite type over k
2. Pairs of geometric points $(s_1, t_1), (s_2, t_2), \dots,$, for $(s_i, t_i) \in T_i(\overline{k})$.
3. $\mathcal{L}_i \in \mathrm{Pic}(X \times T_i)$.

We require:

1. $\mathcal{L}_1|_{X \times \{s_1\}} \simeq \mathcal{M}_{\overline{k}}$.
2. $\mathcal{L}_i|_{X \times \{t_i\}} \simeq \mathcal{L}_{i+1}|_{X \times \{s_i\}}$.
3. $\mathcal{L}_n|_{X \times \{t_n\}} \simeq \mathcal{N}_{\overline{k}}$.

In fact, what this means is that in an algebraic sense, they can be connected (at least geometrically) by a family of line bundles (the the line bundles on $X \times T_i$ are these families).

We can now give a criterion for when a point on the Picard scheme, corresponding to a line bundle on X, lands in the connected component at zero.

10.6 Lemma. *Let $\mathcal{L}$ be a line bundle on X and let $\lambda \in \mathrm{Pic}_{X/k}$ be the corresponding k-point. Then λ lands in the connected component $\mathrm{Pic}^0_{X/k}$ if and only if $\mathcal{L}$ is algebraically equivalent to the trivial line bundle.*

Proof. First, let's show that if $\lambda, 0$ are in the same connected component in $\mathrm{Pic}_{X/k}$ (that is, $\mathrm{Pic}^0_{X/k}$), then we have a *geometrically irreducible* (by last time) algebraic variety $\mathrm{Pic}^0_{X/k}$ connecting $\lambda, 0$. There is a line bundle (the restriction of the Poincaré bundle) on $X \times \mathrm{Pic}^0_{X/k}$ whose restrictions to X over $\lambda, 0$ are given by $\mathcal{L}, \mathcal{O}_X$. The relevant "family of line bundles" making $\lambda, 0$ algebraically equivalent is just then the Poincaré bundle over $\mathrm{Pic}^0_{X/k}$. So $\mathcal{L}, \mathcal{O}_X$ are algebraically equivalent.

(We can even find a curve connecting the two points in $\mathrm{Pic}^0_{X/k}$, so the two line bundles are algebraically equivalent by a curve.)

Suppose now that $\mathcal{L}, \mathcal{O}_X$ are algebraically equivalent. Then we can find the connected schemes $T_1, \dots, T_n$ and geometric points (s_i, t_i) and line bundles $\mathcal{L}_i|_{X \times T_i}$ which "connect" $\mathcal{L}$ and $\mathcal{O}_X$. These families[16] each give maps $T_i \to \mathrm{Pic}_{X/k}$ which must land in a connected component of $\mathrm{Pic}_{X/k}$. We find that T_n must be mapped to Pic^0 (because one of its points goes to the origin), and inductively $T_{n-1}, \dots, T_1$ all map to the origin. Then finally, the point corresponding to s_1, i.e. λ, goes to $\mathrm{Pic}^0_{X/k}$. ▲

As we've thus seen, if two line bundles are algebraically equivalent, we can find a *single curve* to fit them two in a family.

[16] The Picard functor can be defined as either line bundles on the product modulo a certain relation, or isomorphism classes of line bundles with a trivialization along the fibers.

§3 The dual abelian variety

The special case we're interested in is the case $X = A$ for an abelian variety over k, so it has a rational point 0. Thus we can apply the previous theory.

10.7 Definition. We let $\hat{A} = \mathrm{Pic}^0_{A/k}$; this is a projective group scheme over k. We'll soon prove that $\hat{A}$ is smooth, and therefore it is an abelian variety. We call $\hat{A}$ the **dual abelian variety.**

According to this lemma, $\hat{A}$ parametrizes all line bundles on the abelian variety A which are algebraically equivalent to zero.

Remark. If char$k = 0$, then $\hat{A}$ is automatically smooth (group schemes are smooth in characteristic zero).

Earlier, we defined $\mathrm{Pic}^0(A)$ as the collection of line bundles $\mathcal{L} \in \mathrm{Pic}(A)$ which were translation-invariant. In other words, it was the kernel of the map defined earlier

$$\eta : \mathrm{Pic}(A) \to \mathrm{Hom}(A, \mathrm{Pic}(A)), \quad \eta(\mathcal{L})(x) = T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}.$$

We now show that this notation is justified.

10.8 Theorem. *A line bundle $\mathcal{L} \in \mathrm{Pic}(A)$ is algebraically equivalent to zero (i.e. the k-points of $\mathrm{Pic}^0_{A/k}$) if and only if it belongs to $\mathrm{Pic}^0(A)$ (i.e. it is translation-invariant).*

Proof. Let us first show that $\mathrm{Pic}^0_{A/k}(k) \subset \mathrm{Pic}^0(A)$, that is a line bundle algebraically equivalent to zero is translation-invariant.

To say that $\mathcal{L}$ is translation-invariant is to say that

$$m^*\mathcal{L} \simeq p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}, \quad m : A \times A \to A. \tag{6}$$

(This was by the see-saw lemma.) Let $\mathcal{P}$ be the universal Poincaré bundle on $A \times \hat{A}$.

There are maps:

$$A \times A \times \hat{A} \to A \times \hat{A}$$

which are given by m, p_1, p_2. Consider

$$\mathcal{M} = m^*\mathcal{P} \otimes p_1^*\mathcal{P}^{-1} \otimes p_2^*\mathcal{P}^{-1}.$$

If we show that $\mathcal{M}$ is trivial, then it will follow that any line bundle from $\hat{A}$ satisfies (6). But we already have a trivialization

$$\mathcal{M}_{\{0\}\times A \times \hat{A}_{red}}, \ \mathcal{M}|_{A\times\{0\}\times\hat{A}_{red}}, \mathcal{M}_{A\times A\times\{0\}}$$

because the universal line bundle $\mathcal{P}$ is trivial on $\{0\} \times \hat{A}$. If we use the theorem of the cube, it follows that $\mathcal{M}$ is trivial, which is what we want.

Next, we want to show the other direction: a translation-invariant line bundle is algebraically equivalent to zero. We first show that a nontrivial line bundle in $\mathrm{Pic}^0(A)$ (i.e., translation-invariant) has no cohomology.

10.9 Lemma. *Let $\mathcal{L} \in \mathrm{Pic}^0(A)$ be nontrivial. Then $H^i(A, \mathcal{L}) = 0$ for all i.*

Proof. First, $H^0(A,\mathcal{L})=0$ because if a global section σ existed, we can get a contradiction as follows. The map $A \overset{x\mapsto(x,-x)}{\to} A \overset{m}{\to} A \to A$, is constant so pulls back $\mathcal{L}$ to zero. However, since $\mathcal{L}\in\mathrm{Pic}^0$, this is just $\mathcal{L}\otimes(-1)^*\mathcal{L}$. This means that $\mathcal{L}\otimes(-1)^*\mathcal{L}$ must be trivial. But $\mathcal{L}$ has a section, and consequently $(-1)^*\mathcal{L}$ has a section. Tensoring these sections gives a section of the trivial line bundle which consequently vanishes *nowhere*; thus our given section of $\mathcal{L}$ must nowhere vanish as well.

In general, let k be the smallest integer such that $H^k(A,\mathcal{L})\neq 0$. Idea: consider $H^k(A\times A, m^*\mathcal{L})$, and there is a sequence of maps composing to the identity

$$A \overset{x\mapsto(0,x)}{\to} A\times A \overset{m}{\to} A$$

and this gives a sequence

$$H^k(A,\mathcal{L})\to H^k(A\times A,m^*\mathcal{L})\to H^k(A,\mathcal{L}).$$

The composition is the identity. Thus $H^k(A\times A,m^*\mathcal{L})\neq 0$. Now we can use the Künneth theorem and $H^k(A\times A,m^*\mathcal{L})\simeq H^k(A\times A,p_1^*\mathcal{L}\otimes p_2^*\mathcal{L})\simeq\bigoplus_{i+j=k}H^i(A,\mathcal{L})\otimes_k H^j(A,\mathcal{L})$. But now this is necessarily zero since k is the smallest integer for which $H^i(A,\mathcal{L})\neq 0$ and $H^0=0$. ▲

Next time, we'll prove the rest of this theorem. ▲

Lecture 11
3/2

Last time, we were trying to prove that the k-points $\hat{A}(k)$ of $\mathrm{Pic}^0_{A/k}=\hat{A}$ were the same as the translation-invariant line bundles, i.e. those in $\mathrm{Pic}^0(A)$.

We showed one direction. Now we need to show that a line bundle in $\mathrm{Pic}^0(A)$ is actually algebraically equivalent to zero.

§1 Completion of the proof of equivalence

We will deduce the other direction from:

11.1 Theorem. *Let $\mathcal{L}$ be an ample line bundle. Then the map*

$$\phi_{\mathcal{L}}:A(\overline{k})\to\mathrm{Pic}^0(A_{\overline{k}}),\ x\mapsto T_x^*\mathcal{L}\otimes\mathcal{L}^{-1}$$

is surjective.

Proof. Assume without loss of generality that k is algebraically closed.

Assume $\mathcal{M}\in\mathrm{Pic}^0(A)$ is *not* of the form $T_x^*\mathcal{L}\otimes\mathcal{L}^{-1}$. We consider

$$\mathcal{N}=m^*\mathcal{L}\otimes p_1^*\mathcal{L}^{-1}\otimes p_2^*(\mathcal{L}^{-1}\otimes\mathcal{M}^{-1}).$$

We want to calculate the cohomology of this line bundle. There are two projections $p_1,p_2:A\times A\to A$. We will use the Leray spectral sequence for these two projections to calculate the cohomology.

The spectral sequence goes

$$H^i(A, R^j p_{1*}\mathcal{N}) \implies H^{i+j}(A \times A, \mathcal{N}).$$

We can also get another spectral sequence

$$H^i(A, R^j p_{2*}\mathcal{N}) \implies H^{i+j}(A \times A, \mathcal{N}).$$

Let's first look at the first projection p_1. What is this sheaf $R^j p_{1*}\mathcal{N}$? Because of cohomology and base change, we might try to understand the cohomology $H^\bullet(A, \mathcal{N}|_{\{x\}\times A})$ for each x, that is the cohomology along the fiber (in this case, the vertical fiber). So, what is $\mathcal{N}|_{\{x\}\times A}$? This is $T_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \otimes \mathcal{M}^{-1}$. This is nontrivial and in $\mathrm{Pic}^0(A)$ (because $T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is in Pic^0 by the theorem of the square). However, we showed last time that for a nontrivial sheaf in Pic^0, all of the cohomologies vanish. By cohomology and base-change, it follows that $R^j p_{1*}\mathcal{N} = 0$ for all j. (Once we know that the cohomology along the fibers is constant, that implies that the derived push-forwards are locally free of that rank.)

Anyway, the Leray spectral sequence now gives us that $H^\bullet(A \times A, \mathcal{N}) = 0$.

Now, on the other hand, let's try to look at the *second* spectral sequence. Let's try to figure out what $R^j p_{2*}\mathcal{N}$ is. Again, we can try to look at the fibers. Along a fiber $A \times \{y\}$, the sheaf $\mathcal{N}|_{A\times\{y\}}$ is $T_y\mathcal{L} \otimes \mathcal{L}^{-1}$. The sheaf can be trivial at only finitely many points because $\left\{y \in A : T_y^*\mathcal{L} \simeq \mathcal{L}\right\}$ is exactly the finite set $K(\mathcal{L})$ (because $\mathcal{L}$ is ample). We proved this earlier.

Anyway, we find that $T_y^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is nontrivial except on a finite set. Thus, for all y outside this finite set, we must have $H^\bullet(A, \mathcal{N}|_{A\times\{y\}}) = 0$, again by yesterday's lemma. It follows that $R^j p_{2*}\mathcal{N}$ is supported on a zero-dimensional scheme (i.e. $K(\mathcal{L})$). It follows that the Leray spectral sequence for p_{2*} degenerates and gives

$$\Gamma(A, R^j p_{2*}\mathcal{N}) = H^j(A, R^j p_{2*}\mathcal{N}).$$

Since $R^j p_{2*}\mathcal{N}$ was supported on a finite set, we get that $R^j p_{2*}\mathcal{N} \equiv 0$ for all j.

Now we can go in reverse by cohomology and base change. If $R^j p_{2*}\mathcal{N} \equiv 0$ for all j, we find that the fiberwise cohomology must be trivial. For all y, we must have that $H^\bullet(A, \mathcal{N}|_{A\times\{y\}}) = 0$.[17] But this is absurd: set $x = 0$ and $\mathcal{N}|_{A\times\{0\}}$ is trivial. So H^0 cannot be zero. ▲

The theorem now implies that any element of $\mathrm{Pic}^0(A)$ is algebraically equivalent to zero. Pick an ample line bundle $\mathcal{L}$ on A; then we get a composite diagram

$$\phi_{\mathcal{L}} : A(\overline{k}) \to \mathrm{Pic}^0_{A/k}(\overline{k}) \to \hat{A}(\overline{k})$$

and the composite is surjective. Each $T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is clearly algebraically equivalent to zero.

We have now seen that there are two interpretations of $\hat{A}$.

1. It classifies line bundles algebraically equivalent to zero.

2. It classifies translation-invariant line bundles.

[17] Here is a fact: if $R^i f_*\mathcal{F}$ is locally free and $R^i f_*\mathcal{F} \otimes k(y) \simeq H^i(X_y, \mathcal{F}_y)$, then this implies that $R^{i-1} f_*\mathcal{F} \otimes k(y) \simeq H^{i-1}(X_y, \mathcal{F}_y)$ in cohomology and base change.

§2 Smoothness of the dual

We now show that the dual variety is smooth. In general, the Picard scheme is not smooth (though it is for curves).

11.2 Theorem. *$\hat{A}$ is a smooth variety (in particular, reduced).*

Proof. Let $\mathcal{L}$ be a line bundle.

We have a map

$$\phi_{\mathcal{L}} : A(\overline{k}) \to \hat{A}(\overline{k})$$

which can be defined not only at the level of $\overline{k}$-points, but in fact at the level of S-points for any S. We can define for any $\alpha : S \to A$, we can define a family of line bundles over $S \times A$ with the appropriate trivialty conditions. Anyway, as a result we get a map of *group schemes*

$$\phi_{\mathcal{L}} : A \to \mathrm{Pic}_{A/k}.$$

(E.g. we just have to check the universal case.)

Because A is connected, the map lands in $\hat{A} = \mathrm{Pic}^0_{A/k}$. Choosing $\mathcal{L}$ to be ample, we can choose $\phi_{\mathcal{L}} : A \to \hat{A}$ to be *surjective* with finite kernel. So

$$\dim A = \dim \hat{A}.$$

(By the fiber dimension theorem.) Therefore, to prove smoothness of $\hat{A}$, it's enough to show that $\dim T_0\hat{A} \leq \dim A$.

What is $T_0\hat{A}$? This is, by definition, the kernel of

$$\hat{A}(k[\epsilon]/\epsilon^2) \to \hat{A}(k) = \ker(\mathrm{Pic}_{A/k}(k[\epsilon]/\epsilon^2) \to \mathrm{Pic}_{A/k}(k)).$$

Let $\Lambda = k[\epsilon]/\epsilon^2$. Therefore, $T_0\hat{A}$ consists of pairs $(\mathcal{L}, \alpha)$ where $\mathcal{L}$ is a line bundle on $A \times \Lambda$ and α is a trivialization on $\{0\} \times \Lambda$ which are trivial on $A \times \{0\}$. Isomorphism classes of line bundles on X, for any X, is given by $H^1(X, \mathcal{O}_X^*)$. Let's look at $\mathcal{O}_{A\times\Lambda}^*$; this is a sheaf on the underlying topological space of A. There is an exact sequence

$$0 \to \mathcal{O}_A \overset{f\mapsto 1+\epsilon f}{\to} \mathcal{O}_{A\times\Lambda}^* \to \mathcal{O}_A^* \to 1$$

which is in fact split. Consequently, $H^1(A \times \Lambda, \mathcal{O}_{A\times\Lambda}^*) = H^1(A, \mathcal{O}_A^*) \oplus H^1(A, \mathcal{O}_A)$. If we require the thing to be trivial along $A \times \{0\}$, we get that the tangent space to $\hat{A}$ is $H^1(A, \mathcal{O}_A)$.

Anyway, the point is now to show that $\dim H^1(A, \mathcal{O}_A) \leq \dim A$.

Let X be a complete variety over k. Suppose that $H^0(X, \mathcal{O}_X) = k$. We can define

$$H_X = \bigoplus_i H^i(X, \mathcal{O}_X)$$

and try to study this graded vector space. This is a graded-commutative k-algebra (this is generally true) with the product structure given by cup-product. Now, if $X = A$ is an abelian variety, we have more structure. H_A is a *cocommutative* coalgebra. There is a map

$$H_A \to H_A \otimes H_A$$

which is given by the pull-back along multiplication $H_A \to H_{A\times A} \simeq H_A \otimes H_A$ (the last thing is the Künneth formula). The antipode comes from the action of $(-1)^*$. So we get a *graded Hopf algebra* structure on H_A, which is finite-dimensional.

Examples of Hopf algebras: if G/k is an affine group scheme, then $k[G] = \Gamma(G, \mathcal{O}_G)$ is a Hopf algebra where the comultiplication comes from dualizing the multiplication on G. This is a commutative Hopf algebras. (In fact, the category of commutative Hopf algebras is antiequivalent to the category of affine group schemes.) If G is commutative, then this Hopf algebra is cocommutative.

(**We are out of time here.**) ▲

Lecture 12
3/5

§1 Hopf algebras

Let k be a field.

12.1 Definition. A **Hopf algebra** is a tuple $(H, m, \delta, \Delta, \epsilon, s)$ where

1. H is a k-vector space .
2. $m : H \otimes_k H \to H$, $\delta : k \to H$ make H a k-algebra.
3. $\epsilon : H \to k$, $\Delta : H \to H \otimes_k H$ makes H into a k-coalgebra.
4. m is a coalgebra homomorphism and Δ is an algebra homomorphism.
5. $s : H \to H$ is an algebra anti-homomorphism and coalgebra anti-homomorphism making the diagram commute:

$$\begin{tikzcd}
 & H \arrow[ld] \arrow[r, "\Delta"] & H \otimes H \arrow[dd, "s\otimes 1"] \\
k \arrow[rd, "\delta"] & & \\
 & H & H \otimes H \arrow[l, "m"]
\end{tikzcd} .$$

If we don't have the last map s, we say that we have a **bialgebra.**

We have:

12.2 Proposition. *There is an antiequivalence of categories between commutative Hopf algebras over k and affine group schemes over k.*

This provides an easy way to remember the axioms.

12.3 Definition. A **graded Hopf algebra** is the same thing, except H is now required to be a *graded* vector space and all the maps should be morphisms of graded vector spaces. For instance, the unit should be in degree zero.

We say that H is **graded-commutative** if

$$ab = (-1)^{\deg a \deg b} ba$$

for a, b homogeneous. Similarly we can define **graded-cocommutative.**

12.4 Example. As we said before, the commutative group scheme $\mathbb{G}_a = \operatorname{Spec} k[t]$ corresponds to a commutative, cocommutative Hopf algebra such that

$$\Delta(t) = 1 \otimes t + t \otimes 1.$$

We can make this graded-commutative if we impose a grading where $\deg t = 2n$. (We didn't write down all the extra maps.)

12.5 Example. We can talk about the quotient Hopf algebra $\alpha_{p^n} = \operatorname{Spec} k[t]/t^{p^n}$ (still with $\Delta(t) = 1 \otimes t + t \otimes 1$); this is still graded-commutative and cocommutative if t is in even degree.

12.6 Example. Let $\Lambda_k[t] = k \oplus kt$ with the degree of t odd, $t^2 = 0$, and $\Delta(t) = 1 \otimes t + t \otimes 1$. Since $\deg t$ is odd, we actually get a graded Hopf algebra. In fact, we have

$$\Delta(t)^2 = (1 \otimes t + t \otimes 1)^2 = 0$$

because the grading gives an extra sign when this is expanded out. This is where the oddness of $\deg t$ was used.

(**Question**: So, a graded Hopf algebra is not a special type of Hopf algebra: it's a Hopf algebra object internal to graded vector spaces?)

12.7 Example. Let H_1, H_2 are two graded-commutative, cocommutative Hopf algebras, then $H_1 \otimes H_2$ is one as well. For instance, with the notation of the previous example, $\Lambda_k[t_1] \otimes \Lambda_k[t_2]$ is the exterior algebra $\bigwedge^\bullet(kt_1 \oplus kt_2)$.

We have the following:

12.8 Theorem (Borel)**.** *Let k be a perfect field and let H be a nonnegative, graded commutative and cocommutative k-bialgebra. Suppose $H_0 = k$ and each H_n is finite-dimensional. Then H is the tensor product $H_1 \otimes H_2 \otimes \cdots \otimes H_n$ with each H_i one of the forms of the previous examples. (I.e., each H_i a polynomial algebra, an exterior algebra, or some quotient.)*

§2 Applications to abelian varieties

As a result, we can tie up a loose end from last time.

12.9 Corollary. *Suppose A is an abelian variety of dimension g. Then $H^1(A, \mathcal{O}_A) = g$ and the natural map $\bigwedge^\bullet H^1(A, \mathcal{O}_A) \to H^\bullet(A, \mathcal{O}_A)$ is an isomorphism.*

Proof. Assume k algebraically closed, by base change.

The point is that $H^n(A, \mathcal{O}_A) = 0$ for $n > g$ (according to Grothendieck's vanishing theorem). Consequently, the bialgebra

$$H_A = \bigoplus H^i(A, \mathcal{O}_A)$$

does not have any polynomial factors. Thus, by Borel's theorem, we can write $H_A = \bigwedge^\bullet V \otimes k[t_1, \dots, t_n]/(t_1^{p^{m_1}}, \dots, t_n^{p^{m_n}})$ where the graded vector space V has terms in odd degrees. But of course, the degree one part of V_1 must then have dimension $\leq g$ because otherwise exterior powers in dimension $\geq g+1$ would be nonzero, contradicting the vanishing theorem. Since $H^1(A, \mathcal{O}_A) \subset V_1$, we have

$$\dim H^1(A, \mathcal{O}_A) \leq g.$$

We also had the other inequality previously, $\dim H^1(A, \mathcal{O}_A) \geq g$ (by interpreting the H^1 as a tangent space). So we have equality. Thus $V_1 = H^1(A, \mathcal{O}_A)$ and this has dimension g.

If there were any other factors in this, say some V_d or t_i, then there would be terms in H_A of degree $> g$. So these don't exist. ▲

In particular, we've seen that there is a canonical isomorphism (by cup-product)

$$\bigwedge^i H^1(A, \mathcal{O}_A) \simeq H^i(A, \mathcal{O}_A)$$

for each i, and in particular, $h^i(A, \mathcal{O}_A) = \binom{g}{i}$.

We have in particular proved, in view of what we saw last time:

12.10 Corollary. *The dual abelian variety $\hat{A}$ is smooth.*

Let us give another application of the Picard scheme. Let $\mathcal{L}$ be a line bundle. We defined a map

$$\phi_{\mathcal{L}} : A \to \hat{A}$$

and we know that if $\mathcal{L}$ is ample, then $\ker \phi_{\mathcal{L}}$ is finite. Since the two abelian varieties have the same dimension, $\phi_{\mathcal{L}}$ is an *isogeny.* It turns out that if $\mathcal{L}$ is ample and $\mathcal{L}_0 \in \mathrm{Pic}^0$, then $\phi_{\mathcal{L}} = \phi_{\mathcal{L} \otimes \mathcal{L}_0}$. Different line bundles can give the same $\phi_{\mathcal{L}}$.

12.11 Definition. A **polarization** of an abelian variety A is an isogeny $\lambda : A \to \hat{A}$ such that after you base change to $\overline{k}$, it is $\phi_{\mathcal{L}}$ for some ample $\mathcal{L}$.

This isogeny is more fundamental than the ample line bundle $\mathcal{L}$ itself: even if $\mathcal{L}$ can't be defined over k, the isogeny might be.

12.12 Definition. A polarization λ is called a **principal polarization** if it is an isomorphism (i.e. if it has degree one).

Here is an example of a principally polarized abelian variety.

12.13 Example. Let X be a complete curve over k with a rational point $x_0 \in X(k)$. Then, we know that $\mathrm{Pic}_{X/k}$ is represented by a scheme, and we define the **Jacobian variety**

$$J(X) = \mathrm{Pic}^0_{X/k}.$$

We know that the $\overline{k}$-points of $J(X)$ parametrizes line bundles algebraically equivalent to zero, or those who have degree zero. (A line bundle is algebraically equivalent to zero if and only if the degree is zero: this is because in an algebraic family of line bundles, the Euler characteristic does not change.) The tangent space

$$T_0 J(X) = H^1(X, \mathcal{O}_X)$$

by the same argument as before. In particular $J(X)$ has dimension $\leq g$.

For every d, we have the Abel-Jacobi map

$$\mathrm{AJ}^d : X^d \to J(X).$$

X^d parametrizes families of ordered d-tuples of points; it goes to the line bundle $\mathcal{O}(x_1 + \cdots + x_d - dx_d)$. If you want to do it scheme-theoretically, you can do so using divisors. If $d > 2g - 2$, then the Abel-Jacobi map is a surjection and the fibers are projective spaces of dimension $d - g$. For, what is a fiber $(\mathrm{AJ}^d)^{-1}(\mathcal{L})$? It's the projectivization of some space of sections. When d is large, the fibers have constant dimension. We can use this to see again that $\dim J(X) \geq g$. Consequently, $J(X)$ is smooth, and we get another abelian variety.

12.14 Theorem. *$J(X)$ admits a canonical principal polarization.*

We will construct an ample divisor on $J(X)$, which gives the polarization, and then one can show that it is principal. Let Θ be the scheme-theoretical image of AJ^{g-1}. This is the locus of those line bundles $\mathcal{L} \in J(X)$ such that $\Gamma(\mathcal{L}(g-1)x_0) \neq 0$. The claim is that Θ is an ample divisor on $J(X)$ and the map ϕ_Θ is a principal polarization of the Jacobian.

A special case is when $X = E$ is an elliptic curve. Then $x_0 = 0 \in E$ (we can choose this), and $J(X) \simeq E$, and Θ is just $\{x_0\}$. In fact, Θ consists of line bundles $\mathcal{O}(x - x_0)$ with nonzero global sections, and these are trivial precisely when $x = x_0$. So Θ is ample, because any positive divisor on an elliptic curve is ample.

Lecture 13
3/8

§1 The polarization of the Jacobian

Recall that a map $A \to \hat{A}$ is a **polarization** if after tensoring with the algebraic closure, λ becomes the map $\phi_{\mathcal{L}}$ for $\mathcal{L}$ an ample bundle over $A \times_k \overline{k}$. The choice of $\mathcal{L}$ is not unique; changing it by an element of $\mathrm{Pic}^0(A \times_k \overline{k})$ won't do anything. The polarization is **principal** if it is an isomorphism.

13.1 Example. An example from last time is the case of $A = E$ an elliptic curve, in which case $\hat{A} = E$ again. We can take $\mathcal{L} = \mathcal{O}(\{0\})$ to be the divisor at the origin; then the map

$$\phi_{\mathcal{L}} : E \to E$$

sends $x \mapsto -x$. If you translate $\mathcal{L}$ by x, one gets $\mathcal{O}(-x)$. In this case, the polarization is an isomorphism (i.e., it is a principal polarization).

The analog of a higher-dimensional elliptic curve is not just an abelian variety, but a polarized abelian variety.

13.2 Example. If X is a curve (smooth, projective), then the Jacobian $J(X) = \mathrm{Pic}^0(X)$ turns out to be an abelian variety—in particular, reduced. There is a canonical divisor Θ on $J(X)$. This is the image

$$\Theta = \mathrm{Im}(AJ^{g-1} : X^{g-1} \to J(X))$$

where the Abel-Jacobi map AJ maps $(x_1, \dots, x_{g-1})$ to $\mathcal{O}(x_1 + \dots + x_{g-1} - (g-1)x_{g-1})$. It turns out that Θ gives a principal polarization on $J(X)$.

To say that Θ is ample, we argue as follows. Consider the first Abel-Jacobi map $AJ : X \to J(X)$; by functoriality, we get a map on Picard schemes

$$\tau : J(\hat{X}) = \mathrm{Pic}^0_{J(X)/k} \to \mathrm{Pic}^0_{X/k} = J(X).$$

The claim is that this map is an isomorphism. We will see that $\tau \circ \phi_\Theta = -1$; this in turn will mean that ϕ_Θ is injective, and consequently Θ is ample and ϕ_Θ is an isomorphism.

Consider the following general situation. Let S be a noetherian scheme, and consider $\pi : X \times S \to S$ and a line bundle $\mathcal{L} \in \mathrm{Pic}(X \times S)$. According to what we have seen, the cohomology of $\mathcal{L}$ can be represented by a complex on S. There exists a 2-term complex $K^\bullet$ on S of locally frees of finite rank. For each $s \in S$, the fiber $\mathcal{L}|_{X_s}$ has two cohomology groups $H^0(X, \mathcal{L}|_{X_s}), H^1(X, \mathcal{L}|_{X_s})$. What we want is a line bundle on S is the determinant of these two vector spaces, at each $s \in S$. How should we do that? We can't do it fiberwise, but we can use the complex $K^\bullet = K^0 \to K^1$ of locally frees on S representing the cohomology. We can take

$$\det \mathcal{L} := \bigwedge^{top} K^0 \otimes (\bigwedge^{top} K^1)^{-1} \in \mathrm{Pic}(S).$$

It's easy to see that this is independent of the choice of $K^\bullet$. This is called the **determinant line bundle**; its formulation commutes with arbitrary base-change.

Exercise: if $S = X$, and we have the projection $p_2 : X \times X \to X$, and $\mathcal{L} = \mathcal{O}(-\Delta)$, then what is $\det_{\mathcal{L}}$? The claim is that it is trivial. If $\mathcal{L} = \mathcal{O}(\Delta)$, you'll get the canonical sheaf of X, or its inverse, $\omega_X^{\pm 1}$. This is a good exercise.

The claim is that the line bundle on $J(X)$ associated to the theta-divisor is the determinant line bundle of something. We have the Poincaré line bundle $\mathcal{P}$ on

$$X \times J(X)$$

which is canonically trivialized on $\{x_0 0\} \times J(X)$ (where x_0 is a point in X). Let $\mathcal{M} = \mathcal{P} \otimes p_1^* \mathcal{O}((g-1)x_0)$. The restriction of $\mathcal{M}$ to each fiber $X \times a$ is $\mathcal{P}|_{X \times a} \otimes \mathcal{O}((g-1)x_0)$. By Riemann-Roch, the Euler characteristic of $\mathcal{M}|_{X \times a}$ is always zero.

Now consider the two-term complex $K^0 \to K^1$ over $J(X)$ representing the cohomology of $\mathcal{M}$. For any a, the dimension difference $\dim K^0 \otimes k(a) - \dim K^1 \otimes k(a) = \chi(\mathcal{M}|_{X \times a}) = 0$. In particular, we have

$$\mathrm{rank} K^0 = \mathrm{rank} K^1.$$

We have a map of two vector bundles of the same rank, which is locally represented by some matrix. We can ask for the locus where the matrix is not of full rank. In fact, we have a map given by the complex:

$$\psi : \bigwedge^{top} K^0 \to \bigwedge^{top} K^1.$$

Can ψ be identically zero? Consider those $a \in J(X)$ such that $\psi|_a = 0$; this set consists of those $a \in J(X)$ such that $K_a^0 \to K_a^1$ is not injective. This consists of $a \in J(X)$ such that $h^0(\mathcal{M}|_{X \times a}) = 0$. In other words, we have to consider a such that $h^0(\mathcal{P}_a \otimes \mathcal{O}((g-1)x_0)) > 0$. This is, however, *exactly* the image of the $g-1$ Abel-Jacobi map, which is a proper subscheme Θ. So ψ cannot be identically zero, and hence it is injective.

We find that

$$\det \mathcal{M} = \bigwedge^{top} K^0 \otimes (\bigwedge^{top} K^1)^{-1} \hookrightarrow \mathcal{O}_{J(X)}$$

is an ideal sheaf, and the quotient is supported on the Θ. It follows that this determinant line bundle $\det \mathcal{M}^{-1}$ is a positive *multiple* of the Θ divisor.

OK, so now we want to show that

$$\tau \circ \phi_{\det \mathcal{M}^{-1}} = -1 : J(X) \to J(X).$$

If this is true, then we're done. In fact, it will also show that $\det \mathcal{M}^{-1}$ cannot be divisible in the Picard group, so it must be exactly $\mathcal{O}(\Theta)$ (or $\phi_{\det \mathcal{M}^{-1}}$ would have a nontrivial kernel).

What is the meaning of this identity? It states that for any $a \in J(X)$, then $\tau\phi_{\det^{-1} \mathcal{M}}(a)) = -a$. In other words, we have to prove

$$\tau(T_a^*(\det \mathcal{M}^{-1}) \otimes \det \mathcal{M}) = a.$$

But what is τ? It is a map $\widehat{J(X)} \to J(X)$ which sends a line bundle $\mathcal{L}$ on $J(X)$ to the pull-back under the Abel-Jacobi map $AJ : X \to J(X)$. So, when we restrict to X, we claim that

$$T_{AJ(a)}^* \det AJ^* \mathcal{M}^{-1} \otimes \det AJ^* \mathcal{M} = -a.$$

OK, what is $(T_a^* \det |_{\mathcal{M}})|_{AJ}$? It is the same thing as $\det \mathcal{M}|_{AJ^1(X)-a}$. Now the formation of the determinant bundle commutes with base change so this is $\det \mathcal{M}|_{AJ^1(X)-a}$. Here we have a map

$$X \times X \overset{1, AJ-a}{\to} X \times J(X)$$

and we are pulling $\mathcal{M}$ back via this, and then taking the determinant cohomology with respect to the second projection. It is a calculation to show that $\mathcal{M}$ restricted to $X \times X$ is just $\mathcal{O}(\Delta - \{x_0\} \times X) \otimes p_1^* \mathcal{O}((g-1)x_0) \otimes p_1^* \mathcal{P}_a$.

13.3 Lemma. *Let $\mathcal{L}$ be a line bundle on X, and let $\mathcal{J} = \mathcal{O}(\Delta) \otimes p_1^*\mathcal{L}$ on $X \times X$; then* $\det \mathcal{L}$ *(with respect to the second projection) is* $\det_{\mathcal{O}(\Delta)} \otimes \mathcal{L}$*.*

If we believe this, then we can compute the appropriate determinant bundles...?
(I was sufficiently confused here that I couldn't really keep taking notes.)

Lecture 14
3/9

§1 Biduality

For an abelian variety A, we constructed the dual abelian variety $\hat{A}$ which parametrizes line bundles on A algebraically equivalent to zero. That is, $\hat{A} = \mathrm{Pic}^0_{A/k}$. What is $\hat{\hat{A}}$? We fully expect that we get back to A. Our goal is to prove this fact.

Given the association

$$A \mapsto \hat{A}$$

we can think of it as a contravariant functor somewhat analogous to the duality functor on vector spaces.

§2 Duality for finite group schemes

Let's start with something a little easier. Let G be a *finite* group scheme over k. So G is affine and the ring of functions $\Gamma(G, \mathcal{O}_G)$ is a finite-dimensional k-vector space. As before, let's write

$$H = \Gamma(G, \mathcal{O}_G);$$

this is a finite-dimensional commutative Hopf algebra over k. Let's consider the more specific case now when G is *commutative*; this means that H is also *cocommutative.*

14.1 Example. μ_p, α_p.

H is a Hopf algebra, so it has a multiplication m, comultiplication Δ, unit ϵ, counit δ, and antipode S. The dual $H^* = \mathrm{Hom}_k(H, k)$ thus inherits the dual of this structure: we get, for instance, a map

$$m^* : H^* \to H^* \otimes H^*$$

and a map

$$\epsilon^* : H^* \to k$$

and so on. Here we have essentially used the fact that H is *finite-dimensional.* It is easy to see that m^* now becomes a cocommutative comultiplication, Δ^* becomes a commutative multiplication, and so on. In other words, the structure H^* with the duals to all these maps is also a commutative, cocommutative Hopf algebra over k.

14.2 Definition. We denote $\hat{G}$ as $\mathrm{Spec} H^*$ as above; this is called the **Cartier dual.** It is also a finite, commutative group scheme over k.

We thus have a nice duality functor on the category of finite commutative group schemes over k to k, and ˆ is clearly an anti-involution.

Let us define the following. Let G_1, G_2 be two commutative group schemes over a base S. Then we can define $\underline{hom}(G_1, G_2)$ as a functor from $\mathrm{Sch}/S \to \mathbf{Ab}$ which sends an S-scheme to the set of all group-homomorphisms

$$\underline{\mathrm{Hom}}_T(G_{1T}, G_{2T})$$

(which is an abelian group).

14.3 Proposition. *$\hat{G}$ represents the group functor $\underline{\mathrm{Hom}}(G, \mathbb{G}_m)$.*

This tells us that, while we defined $\hat{G}$ somewhat indirectly by its ring of functions, we can also describe $\hat{G}$ by its points. Each point is represented by a morphism from G to $\mathbb{G}_m$.

Proof. We want to show that for every test k-scheme $T = \mathrm{Spec} R$, which we'll assume (wlog) affine, that

$$\hat{G}(R) \simeq \mathrm{Hom}(G \times_k R, \mathbb{G}_m \times_k R).$$

What is $\hat{G}(R)$? By definition, it consists of k-algebra homomorphisms

$$H^* \to R.$$

These are the same as R-algebra homomorphisms

$$H_R = H^* \otimes_k R \to R.$$

But $\mathrm{Hom}_R(H^* \otimes_k R, R) \subset \mathrm{Hom}_{R-\mathrm{linear}}(H_R^*, R) = H_R$ (because H_R is finite free over R). Consequently, an R-point of $\hat{G}$ is given by an element of H_R, but not every element will give us such a thing.

Consider an element $\phi \in \mathrm{Hom}_{R-\mathrm{linear}}(H_R^*, R) = H_R$. Given such a thing, ϕ is an algebra-homomorphism if and only if $\phi(ab) = \phi(a)\phi(b)$ and $\phi(1) = 1$. If you write it out, this is equivalent to $\Delta_R^*(a \otimes b) = \phi(a)\phi(b)$. ($\Delta^*$ was the multiplication on H^*.) Anyway, this is equivalent to

$$(\Delta_R(\phi))(a \otimes b) = \phi(a)\phi(b) = (\phi \otimes \phi)(a \otimes b).$$

So this implies that

$$\Delta_R(\phi) = \phi \otimes \phi \in H_R \otimes_R H_R.$$

To say that $\phi(1) = 1$, this states that $\epsilon_R(\phi) = 1$. So the elements of H_R that arise in this way (which are actually algebra-homomorphisms) ϕ is *group-like.*

This is equivalent to saying that $\Delta_R(\phi) = \phi \otimes \phi$ and ϕ is invertible in H_R. To see this, we note that $\epsilon_R \otimes \epsilon_R \circ \Delta_R : H_R \to H_R$ is equal to ϵ_R (by dualizing group scheme diagrams). So if ϕ is invertible, then we get

$$\epsilon_R(\phi) = (\epsilon_R \otimes \epsilon_R) \circ \Delta_R(\phi) = \epsilon_R(\phi)^2$$

and invertibility implies $\epsilon_R(\phi) = 1$. Conversely, let's say we know that $\Delta_R(\phi) = \phi \otimes \phi$ and $\epsilon_R(\phi) = 1$. Consider the diagram

$$\begin{tikzcd}
G_R \arrow[r, "1\times S"] \arrow[d] & G_R \times G_R \arrow[d] \\
\mathrm{Spec} R \arrow[r] & G_R
\end{tikzcd}$$

where the composite is the identity. We dualize to get a commutative diagram

$$\begin{tikzcd}
H_R & H_R \otimes H_R \arrow[l] \\
R \arrow[u] & H_R \arrow[l, "R", "\epsilon"'] \arrow[u]
\end{tikzcd}$$

and this implies that if ϕ is group-like, then $\phi S(\phi) = 1$ (since we assumed that $\epsilon_R(\phi) = 1$).

Anyway, it's now clear that to give a group-like element ϕ in the Hopf algebra H_R is the same thing as giving a morphism of Hopf algebras $R[T, T^{-1}] \to H_R$ (sending $T \mapsto \phi$). That proves the result. ▲

14.4 Example. Take $G = \mathbb{Z}/n\mathbb{Z}$: this is the union of n points with the multiplication structure given discretely. This is a disconnected scheme. What is $\hat{G}$? We can think of it as maps of group schemes $G \to \mathbb{G}_m$. For any R, $\hat{G}(R)$ consists of maps $\mathrm{Hom}(G_R, \mathbb{G}_{mR})$ and this corresponds to elements $f \in R^*$ such that $f^n = 1$. Consequently,

$$\hat{\mathbb{Z}/n\mathbb{Z}} = \mu_n, \quad \hat{\mu_n} = \mathbb{Z}/n\mathbb{Z}.$$

14.5 Example. As an exercise, α_p is self-dual.

§3 Abelian varieties

This suggests that there is a connection between $\hat{G}$ and the dual abelian variety.

14.6 Theorem. *Let $f : A \to B$ be an isogeny of abelian varieties. In particular,* $\ker f$ *is a finite group scheme over k (not necessarily reduced). Then, $\hat{f} : \hat{B} \to \hat{A}$ is an isogeny and in fact $\widehat{\ker f} = \ker \hat{f}$.*

An isogeny $f : A \to B$ of abelian varieties is a surjective morphism. So we can write it as an exact sequence

$$0 \to \ker f \to A \to B \to 0$$

(at least formally), and duality gives

$$0 \to \widehat{\ker f} \to \hat{B} \to \hat{A} \to 0$$

(though the arrow seems to go in the wrong direction).

Let's now give another interpretation of the dual abelian variety, at least informally (though it can be made rigorous). $\hat{A}$ parametrizes line bundles $\mathcal{L}$ on A which are algebraically equivalent to zero, or such that $m^*\mathcal{L} \simeq \mathcal{L} \otimes \mathcal{L}$ on $A \times A$. (This was the see-saw lemma.) A line bundle on A is the same thing as a $\mathbb{G}_m$-torsor on A; this is by deleting the origin. Given $\mathcal{L}$, deleting the origin gives a $\mathbb{G}_m$-torsor $\mathcal{L} \setminus \{0\}$. So we are looking at $\mathbb{G}_m$-torsors L^- on A such that $m^*L^- \simeq L^- \boxtimes L^-$.

Let's say this again. If $\mathcal{L}$ is an invertible sheaf on X, then we can define its total space $L = \mathrm{tot}(\mathcal{L})$; this is a scheme affine over X. It is equipped with a canonical zero section. If you delete the zero section, then the resulting L^- is a $\mathbb{G}_m$-torsor. Torsors can be pulled back, and the total space pulls back nicely in the same way that line bundles do.

As a result, $\hat{A}$ really classifies a special type of $\mathbb{G}_m$-torsor over A. These are those for which there exists a commutative diagram

$$\begin{tikzcd}
L^- \times L^- \arrow[r] \arrow[d] & L^- \arrow[d] \\
A \times A \arrow[r, "m"] & A
\end{tikzcd}$$

which gives the scheme $\mathcal{L}^-$ the structure of a group scheme (which *lifts* the multiplication m over A). So L^- becomes a commutative group scheme fitting into the short exact sequence

$$1 \to \mathbb{G}_m \to L^- \to A \to 0.$$

This description is due to Grothendieck, that extensions of A by $\mathbb{G}_m$ are the same as multiplicative torsors. We usually write this as $\mathrm{Ext}^1(A, \mathbb{G}_m) = \hat{A}$.

Now, it's easy to understand the following: if

$$0 \to K \to A \to B \to 0$$

is a short exact sequence, then you can hom into $\mathbb{G}_m$ to get

$$0 \to \mathrm{Hom}(K, \mathbb{G}_m) \to \mathrm{Ext}^1(B, \mathbb{G}_m) \to \mathrm{Ext}^1(A, \mathbb{G}_m) \to 0.$$

(The reason for the zeros is that the first term would be $\mathrm{Hom}(A, \mathbb{G}_m) = 0$ because A is proper, and the last term can be shown to be zero as well.) This suggests why taking the dual abelian variety should send the kernel to the Cartier dual.

Anyway, this was just motivation.

To prove this theorem, we will try to analyze $\ker \hat{f}$ (of $f : A \to B$), by considering its S-points. These are those line bundles $\mathcal{L}$ on $B \times S$ (with a specified trivialization on $0 \times S$) such that $(f \times 1)^*\mathcal{L}$ is trivial. Of course, the rigidification was unnecessary, and

$$(\ker \hat{f})(S) = \{\mathcal{L} \in \mathrm{Pic}(B \times S) : (f \times 1)^*\mathcal{L} \simeq \mathcal{O}_{A \times S}\}.$$

14.7 Lemma. *If f is an isogeny, then f is faithfully flat (i.e. flat and surjective).*

Proof. We just have to show f is flat; this is because of "generic flatness." ▲

Now Grothendieck's theory of descent tells us that we can recover quasi-coherent sheaves on $B \times S$ in terms of quasi-coherent sheaves on $A \times S$ with some additional conditions. What we will do next time is to review this faithfully flat descent and then to translate this last condition in terms of it.

Lecture 15
3/19

§1 The dual of the kernel

Let's review what we did last time. Let G be a finite commutative group scheme over k. Then, its ring of functions is a finite-dimensional k-vector space. The ring of functions $H = k[G]$ is a commutative, cocommutative (finite-dimensional) Hopf algebra. Then, the dual $H^* = \mathrm{Hom}_k(H, k)$ becomes a commutative, cocommutative Hopf algebra too. That gives us another finite commutative group scheme over k, which we wrote

$$\hat{G} = \mathrm{Spec} H^*,$$

and called it the **Cartier dual.** The nice fact about this construction is that the dual group scheme $\hat{G}$ represents a nice functor, i.e.

$$\hat{G}(S) = \mathrm{Hom}(G_S, \mathbb{G}_{mS}),$$

and in fact we could have defined $\hat{G}$ in this way.

The theorem we want to prove is as follows.

15.1 Theorem. *Let $f : A \to B$ an isogeny of abelian varieties. Then the dual map $\hat{f} : \hat{B} \to \hat{A}$ induced (by pulling back line bundles) is also an isogeny and* $\ker \hat{f}$ *is a finite, commutative groups scheme over k, canonically isomorphic to the Cartier dual $\widehat{\ker f}$.*

Proof. We'll look at the S-points. What is $\ker \hat{f}(S)$? This just consists of sets of pairs $(\mathcal{L}, \alpha)$ where $\mathcal{L}$ is a line bundle on $B \times S$, α is a trivialization $\alpha : \mathcal{L}|_{\{0\} \times S} \to \mathcal{O}$ and we require that $f^*\mathcal{L} \simeq \mathcal{O}_{A \times S}$ (because it's in the kernel). This exactly consists of isomorphism classes of line bundles $\mathcal{L}$ on $B \times S$ such that $f^*\mathcal{L} \simeq \mathcal{O}_{A \times S}$. Now, we want to characterize this subset.

Now let's recall the theory of fppf descent. This is a basic theory in algebraic geometry due to Grothendieck. Let $f : X_0 \to Y$ be a faithfully flat, locally of finite presentation morphism morphism (i.e., fppf). From here, one can form the chain

$$X_2 \Rrightarrow X_1 \rightrightarrows X_0 \xrightarrow{f} f$$

where $X_1 = X_0 \times_Y X_0, X_2 = X_1 \times_{X_0} X_1$. In this case, we can construct the category of quasi-coherent sheaves on Y in terms of quasi-coherent sheaves on this whole diagram. Let $\mathcal{F} \in \mathrm{QCoh}(Y)$. If we pull back via f^*, we'll get $\mathcal{G} = f^*\mathcal{F} \in \mathrm{QCoh}(X_0)$. But it's more than that. The two pull-backs $p_1^*\mathcal{G}, p_2^*\mathcal{G}$ are canonically isomorphic via an isomorphism $\theta : p_1^*\mathcal{G} \simeq p_2^*\mathcal{G}$ (this is because $f \circ p_1 = f \circ p_2$). If you further pull back to X_2, you have the cocycle condition

$$p_{23}^*\theta \circ p_{12}^*\theta = p_{13}^*\theta. \tag{7}$$

Anyway, if you have a quasi-coherent sheaf on Y, you can produce a quasi-coherent sheaf on X_0 with an isomorphism θ satisfying a cocycle condition. When f is faithfully flat, you can go in the opposite direction.

15.2 Definition. Define a category of **descent data** $\mathrm{Desc}(X_0, Y)$ as follows. This is the category of pairs $(\mathcal{G}, \theta)$ where $\mathcal{G} \in \mathrm{QCoh}(X_0)$ and $\theta : p_1^*\mathcal{G} \simeq p_2^*\mathcal{G}$ is an isomorphism satisfying the cocycle condition.

Anyway, we have thus a functor

$$f^* : \mathrm{QCoh}(Y) \to \mathrm{Desc}(X_0, Y)$$

because the pull-back from Y to X_0 factors (canonically) through the category of descent data.

We have:

15.3 Theorem (Grothendieck)**.** *When f is fppf, then $f^* : \mathrm{QCoh}(Y) \to \mathrm{Desc}(X_0, Y)$ is an equivalence of categories.*

Anyway, in our situation we have a map

$$f : A \times S \to B \times S.$$

Let $X_0 = A \times S, Y = B \times S$. Then, in the previous notation, $X_1 = A \times S \times G$ for $G = \ker f$. The first map is projection and the second map comes from the action of $G = \ker f$ on A. Similarly, $X_2 = A \times S \times G \times G$ where the three maps $X_2 \Rrightarrow X_1$ are given by multiplication $G \times G \to G$, and the two actions of G on A. This is an exercise.

OK, so recall what we want to do. We'd like to describe those line bundles on $B \times S$ such that the pull-back to $A \times S$ is given by the structure sheaf. Note that f is an isogeny, so it's faithfully flat. We'd like to describe $\ker \hat{f}(S)$; by the theory of descent, it consists of line bundles on $B \times S$ whose pull-back is trivial; alternatively, it consists of pairs

$$(\mathcal{O}_{A \times S}, \theta)$$

where θ is a descent datum. But what is θ? Well,

$$\theta : p_1^*\mathcal{O}_{A \times S} \simeq p_2^*\mathcal{O}_{A \times S}$$

or in other words

$$\theta : \mathcal{O}_{A \times S \times G} \simeq \mathcal{O}_{A \times S \times G}$$

which means that θ is an invertible element of $\Gamma(A \times S \times G, \mathcal{O}_{A \times S \times G})$. But since A is an abelian variety, in particular projective, it's an element of $\Gamma(S \times G, \mathcal{O}^*_{S \times G})$. So θ is given exactly by a morphism of schemes $S \times G \to \mathbb{G}_{mS}$. The cocycle condition is then just that the map of schemes $S \times G \to \mathbb{G}_{mS}$ is a morphism of S-group schemes. In other words, this is the same as elements of $(\widehat{\ker f})(S)$.

Since we have seen that $\ker \hat{f}$ is a finite group scheme, it follows that $\hat{f}$ is an isogeny. ▲

If we have a short exact sequence

$$0 \to \ker f \to A \xrightarrow{f} B \to 1,$$

we can dualize it to get an exact sequence

$$1 \to \widehat{\ker f} \to \hat{B} \to \hat{A} \to 1.$$

15.4 Corollary. *If f is an isogeny, then* $\deg f = \deg \hat{f}$*.*

In fact, $\deg f$ is just the dimension of the coordinate ring of the kernel, and that's preserved under dualization.

§2 Biduality

Now, we'd like to put A and the dual $\hat{A}$ on a symmetric footing, just as with Cartier duality. For instance, we'd like to show that the double dual is canonically the identity.

15.5 Definition. Let A, B be two abelian varieties of the same dimension. A line bundle $\mathcal{Q}$ on $A \times B$ is said to be a **divisorial correspondence** if the $\mathcal{Q}|_{\{0\} \times B} \simeq \mathcal{O}_B$ and $\mathcal{Q}|_{A \times \{0\}}$ is isomorphic to $\mathcal{O}_A$.

A divisorial correspondence induces a homomorphism

$$\kappa_Q : B \to \hat{A}$$

(it's a morphism of abelian varieties because it sends 0 to 0 — see the rigidity lemma).

We can also swap the two factors via $\sigma : B \times A \to A \times B$, and we also get a map

$$\kappa_{\sigma^* Q} : A \to \hat{B}.$$

15.6 Example. Consider the Poincaré line bundle $\mathcal{P} \in \mathrm{Pic}(A \times \hat{A})$. By definition, $\kappa_{\mathcal{P}}$ is the identity $\hat{A} \to \hat{A}$. On the other hand, we get a biduality map

$$\gamma := \kappa_{\sigma^* \mathcal{P}} : A \to \hat{\hat{A}}.$$

15.7 Proposition. *Let $\mathcal{L}$ be a line bundle on A. Then we have a map $\phi_{\mathcal{L}} : A \to \hat{A}$. On the other hand, we have the map $\gamma : A \to \hat{\hat{A}}$ from the previosu example. Then the following diagram commutes:*

$$\begin{tikzcd} A \arrow[r, "\gamma"] \arrow[dr, "\phi_{\mathcal{L}}"'] & \hat{\hat{A}} \arrow[d, "\widehat{\phi_L}"] \\ & \hat{A} \end{tikzcd} .$$

Proof. We have a map

$$1 \times \phi_{\mathcal{L}} : A \times A \to A \times \hat{A}.$$

If you pull back the Poincaré line bundle $\mathcal{P}$ via this, we get

$$(1 \times \phi_{\mathcal{L}})^* \mathcal{P} \simeq m^* \mathcal{L} \otimes p_1^* \mathcal{L}^{-1} \otimes p_2^* \mathcal{L}^{-1} \in \mathrm{Pic}(A \times A).$$

The whole proposition is based on this observation. To prove it, we use the see-saw lemma: restrict to $A \times \{x\}$ for any point x. But $(1 \times \phi_{\mathcal{L}})^* \mathcal{P}$ restricted to $A \times \{x\}$ is just $T_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$; that's the same as $m^* \mathcal{L} \otimes p_1^* \mathcal{L}^{-1} \otimes p_2^* \mathcal{L}^{-1}|_{A \times \{x\}}$. The difference of these two line bundles is then something obtained by pull-back along the second factor. We just need to show now

$$(1 \times \phi_\alpha)^* \mathcal{P}|_{\{0\} \times A} \simeq (m^* \mathcal{L} \otimes p_1^* \mathcal{L}^{-1} \otimes p_2^* \mathcal{L}^{-1})|_{\{0\} \times A};$$

both, however, are trivial line bundles.

Now let's use this observation. We find that

$$(1 \times \phi_{\mathcal{L}})^* \mathcal{P}|_{\{x\} \times A} \simeq T_x^* \mathcal{L} \otimes \mathcal{L}^{-1}.$$

But what's this? The left-hand-side is $\widehat{\phi_{\mathcal{L}}} \circ \kappa_x$ (by chasing through the definitions) while the left hand side is $\phi_{\mathcal{L}}(x)$. ▲

(**I need to fix some notations here; I've used κ and γ to mean the same thing, having copied down some things wrongly.**)

15.8 Corollary. *$\kappa : A \to \hat{\hat{A}}$ is an isomorphism.*

Proof. Pick $\mathcal{L}$ ample. Then $\phi_{\mathcal{L}} = \widehat{\phi_{\mathcal{L}}} \circ \kappa$ so that κ is an isogeny. Looking at the degrees, we find that $\deg \kappa = 1$. ▲

In particular, we have a canonical biduality isomorphism

$$\kappa : A \simeq \hat{\hat{A}}$$

which identifies any abelian variety with its double dual. Under these identifications, we have that $\phi_{\mathcal{L}} = \widehat{\phi_{\mathcal{L}}}$.

15.9 Definition. A map $\lambda : A \to \hat{A}$ is called **symmetric** if $\lambda = \hat{\lambda}$ (under the identification via κ).

In particular, any polarization is symmetric. Not every isogeny is a polarization, because there exist non-symmetric isogenies.

Finally, let's mention the following thing.

15.10 Proposition. *Let $f : A \to B$ and $\mathcal{L}$ a line bundle on A. Then we have a commutative diagram*

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\phi_{f^*\mathcal{L}}"] & B \arrow[d, "\phi_{\mathcal{L}}"] \\
\hat{A} & \hat{B}. \arrow[l, "\hat{f}"]
\end{tikzcd}$$

Lecture 16
3/23

(I missed the lecture on 3/21.)

Last time, we considered the case char$k = p > 0$. If G is *any* group scheme, we have the absolute Frobenius

$$F : G \to G$$

(which exists for any k-scheme), making the following diagram commute:

$$\begin{tikzcd}
G \arrow[r] \arrow[d] & G \arrow[d] \\
\mathrm{Spec} k \arrow[r] & \mathrm{Spec} k
\end{tikzcd}$$

where the bottom map comes from $x \mapsto x^p$. In other words, the absolute Frobenius is identity on the underlying topological spaces and raises each function to the power p. This diagram factors

$$\begin{tikzcd}
G \arrow[r, "F^{(1)}"] \arrow[dr] & G^{(1)} \arrow[r] \arrow[d] & G \arrow[d] \\
 & \mathrm{Spec} k \arrow[r] & \mathrm{Spec} k
\end{tikzcd}$$

where $G^{(1)}$ is the pull-back. We define $G^{F^{(1)}} = \ker G \to G^{(1)}$; thus the kernel is a *local* scheme of height one. (In fact, it consists of exactly one point.) There is a factorization

$$G^{F^{(1)}} \to \mathrm{Spec}\mathcal{O}_{G,e} \to G.$$

To calculate the local group scheme $G^{F^{(1)}}$, we can write

$$k[G^{F^{(1)}}] = \mathcal{O}_{G,e}/\mathfrak{m}_e^{(p)}, \quad \mathfrak{m}_e^{(p)} = \{x^p, x \in \mathfrak{m}\}.$$

Thus everything in the maximal ideal has pth power zero (which justifies the "height one" claim). Moreover, the Lie algebra of $G^{F^{(1)}}$ equals the Lie algebra of G.

16.1 Definition. (This was done last time, but I missed it.) G is **height one** if it is a local scheme with one point, $G = \mathrm{Spec}A$ for A a local artinian ring, and $x^p = 0$ for all $x \in \mathfrak{m}$.

16.2 Theorem. *The functor $G \mapsto \mathrm{Lie}(G)$ is an equivalence of categories between height one groups and p-Lie algebras.*

Proof. (Sketch.) The construction of the inverse functor is done by sending a p-Lie algebra $\mathfrak{g}$ to the *universal enveloping algebra* $U\mathfrak{g}$—here U is the left adjoint of the forgetful functor from associative algebras to Lie algebras. In other words, $U\mathfrak{g} = T\mathfrak{g}/(x \otimes y - y \otimes x - [x,y])$. Moreover, $U\mathfrak{g}$ is a *Hopf algebra* where the comultiplication is defined by

$$\Delta(x) = 1 \otimes x + x \otimes 1, x \in \mathfrak{g}.$$

(There is a natural inclusion of $\mathfrak{g} \subset U\mathfrak{g}$.) The comultiplication extends to all of $U\mathfrak{g}$ uniquely. The Hopf algebra is cocommutative.

The elements $v \in U(\mathfrak{g})$ (i.e., the primitive elements) such that $\Delta(v) = v \otimes 1 + 1 \otimes v$ is exactly $\mathfrak{g}$.

If we have a p-Lie algebra, you can form the quotient $\mathfrak{U}\mathfrak{g} = U\mathfrak{g}/(x^p - x^{(p)}), x \in \mathfrak{g}$, so that the pth power of an element of $\mathfrak{g}$ becomes the same as the restricted pth power. Now, we get a *finite-dimensional* Hopf algebra. Finally, we take the dual $(\mathfrak{U}\mathfrak{g}^\vee$, which is a *commutative* finite-dimensional Hopf algebra. Now you just have to check that $(\mathfrak{U}\mathfrak{g})^\vee$ corresponds to a group scheme of height one. There is some checking to do, but it's in Mumford. ▲

Remark. In characteristic zero, $G \mapsto \mathrm{Lie}(G)$ is an equivalence of categories between "formal groups" and Lie algebras. The construction in the other direction is similar.

What we need is just the corollary of this theorem.

16.3 Corollary. *If G is commutative of height one, the multiplication by p map $p_G : G \to G$ is zero (i.e. it factors through* Spec$k$*).*

Proof. This is because multiplication by p is a group homomorphism and taking Lie of it gives the zero map (i.e., multiplication by p). ▲

16.4 Corollary. *Let G be local; then there exists n (in fact, a power of p) such that $n_G : G \to G$ is zero.*

Proof. We defined the relative Frobenius $F^{(1)} : G \to G^{(1)}$, and we can iterate this to get

$$G \to G^{(1)} \to G^{(2)} \to \dots$$

and you can define a chain of closed subgroups of G given by $\ker F^{(1)} \subset \ker F^{(2)} \subset \dots$ and since G is local, the chain will eventually terminate at G. (If you iterate the Frobenius a lot, you eventually get zero.) Then you can induct on the number of steps in the filtration. For instance, $G^{F^{(1)}}$ is killed by multiplication by p. This means that $G^{F^{(2)}}$ is killed by multiplication by p^2, because one can check that multiplication by p on $G^{F^{(2)}}$ has to factor through $G^{F^{(1)}}$. ▲

16.5 Corollary. *Let G be finite commutative. Then there exists n such that $n_G : G \to G$ is zero.*

Proof. Filter G as a local thing and an étale thing, and reduce to the local one. ▲

This fact looks trivial, but it's not easy to prove without invoking this whole theory. Let's give an application of this to abelian varieties.

16.6 Corollary. *Let $f : A \to B$ be an isogeny of abelian varieties. Then there exists some n and an isogeny $g : B \to A$ such that $g \circ f = n_A$.*

(In particular, if there exists an isogeny from $A \to B$, there exists one in the other direction.)

Proof. The proof will rely on the theory of descent. We reviewed descent for quasi-coherent sheaves. We also need another fact: schemes are sheaves in the fppf topology.

16.7 Theorem. *Let $U \to V$ be faithfully flat of finite presentation. (For instance, any isogeny between abelian varieties.) Let X be a scheme. Then*

$$\mathrm{Hom}(V, X) \to \mathrm{Hom}(U, X) \rightrightarrows \mathrm{Hom}(U \times_V U, X)$$

is exact (i.e., an equalizer diagram). In other words, given a map $U \to X$ such that the two pull-backs to $U \times_V U$ are equal, one gets a map $V \to X$.

Let's use this theorem to prove the corollary. Apply this theorem to $f : A \to B$ and $X = A$. We have a diagram

$$\ker f \to A \to B$$

and we want to construct a morphism $B \to A$ such that the pull-back to A is multiplication by n. To do this, we have to show that multiplication by n when pulled back in the two ways to $A \times_B A = A \times \ker f$ gives the same thing. The first map $A \times \ker f \to A$ is projection and the second map $A \times \ker f \to A$ is multiplication. So, choose n such that n_A kills $\ker f$, which we can do by the previous theory. If we choose such an n, then the two compositions

$$A \times_B A \to A \overset{n_A}{\to} A$$

are the same, and consequently we get a morphism $B \to A$ as desired (it is a homomorphism by the rigidity lemma).

(We can take $n = \deg f$, in fact.) ▲

16.8 Example. Consider the Frobenius $F : A \to A^{(1)}$ (in characteristic p), which is a morphism between two abelian varieties. The kernel A^F is height one and consequently is killed by multiplication by p. There is thus a factorization

$$A \to A^{(1)} \to A$$

such that the composite is p_A. There is a unique isogeny $V : A^{(1)} \to A$ such that the composite $A \to A^{(1)} \overset{V}{\to} A$ is p_A. You can easily show that $F^{(1)}V = p_{A^{(1)}}$. (To show this, just apply $F^{(1)}$ to both sides and cancel.) V is called the **Verschielung.** Constructing it for general commutative group schemes is harder.

Now let's move on to studying $A[n]$. If $n = n_1 p^m$ where $(n_1, p) = 1$, then we have

$$A[n_1] \times A[p^m] \to A[n],$$

which is an *isomorphism.* Let's prove this.

16.9 Lemma. *The Cartier dual* $\widehat{A[n]}$ *is* $\hat{A}[n]$.

Proof. We already did this for any homomorphism of abelian varieties, $\widehat{\ker f} = \ker \hat{f}$, so we just need to show that $\hat{n_A} = n_{\hat{A}}$. But this just means that if $\mathcal{L} \in \mathrm{Pic}^0(A)$, we have $n_A^* \mathcal{L} \simeq \mathcal{L}^{\otimes n}$. However, we know that for any $\mathcal{L}$, we have

$$n_A^* \mathcal{L} \simeq \mathcal{L}^{(n^2+n)/2} \otimes (-1)^* \mathcal{L}^{(n^2-n)/2}$$

and this reduces to the desired form when $\mathcal{L} \in \mathrm{Pic}^0(A)$ (as $(-1)^*\mathcal{L} = \mathcal{L}^{-1}$ for such $\mathcal{L}$). That is, the dual of multiplication by n is exactly multiplication by n, again. ▲

OK, anyway, to prove that $A[n_1] \times A[p^m] \to A[n]$ is an isomorphism, we need only prove it after base-changing to the algebraic closure, so we'll assume our ground field is algebraically closed. Here $A[n_1]$ is étale and dualizing gives something étale again (it's $\hat{A}[n_1]$). We can decompose $A[p^m]$ into a bunch of factors which are étale local and local étale and local local (**I don't really understand this here**), and we find that we have a decomposition of group schemes into four pieces (étale-étale, local-local, étale-local, local-étale).

Over an algebraically closed field, an étale-local group is something of the form $(\mathbb{Z}/p^m\mathbb{Z})$ (i.e. a product of p-power cyclic groups). A local-étale group is thus a sum of things of the form μ_{p^m}. In fact, we can show

$$A[p^m]_{\overline{k}} = (Z/p^m\mathbb{Z})^r \times \mu_{p^m}^s \times ()_{\text{loc,loc}}$$

r is called the p**-rank** of A.

Claim: The p-rank is invariant under isogeny.

16.10 Corollary. *$r = s$ (by the isogeny $A \to \hat{A}$).*

Lecture 17
3/26

Let's consider an abelian variety A, an integer n relatively prime to the characteristic p, and consider $A[n]$ as a finite étale scheme. We can regard it as a finite group $A[n](\overline{k}) = A[n](k^s)$ together with an action of the Galois group $\text{Gal}(k^s/k)$. We also know that the finite group is $(\mathbb{Z}/n\mathbb{Z})^{2g}$. If we pick $n = l^m$ for a prime $l \neq p$, then we get

$$A[l^m](k^s) = (\mathbb{Z}/l^m\mathbb{Z})^{2g}$$

and clearly we may reduce to this case, without loss of generality.

17.1 Definition. The **Tate module** $T_l(A)$ is defined as

$$T_l(A) = \varprojlim A[l^m](k^s).$$

Here the inverse limit is taken over the system $A[l^{n+1}](k^s) \to A[l^n](k^s)$ given by multiplication by l. As a group, $T_l(A) = \varprojlim(\mathbb{Z}/l^n\mathbb{Z})^{2g} = \mathbb{Z}_l^{2g}$. It is therefore a free $\mathbb{Z}_l$-module of rank $2g$, together with a continuous action of the Galois group.

(Recall that the Tate module and the Galois group are given the profinite topology.) We have a continuous homomorphism

$$\rho : \text{Gal}(k^s/k) \to \text{GL}_{2g}(\mathbb{Z}_l).$$

If $f : A \to B$ is a morphism, then it induces a morphism $T_l(f) : T_l(A) \to T_l(B)$ of Tate modules, so T_l is naturally a *functor* (of continuous $\mathbb{Z}_l$-representations of the Galois group).

Remark. Of course, this definition makes sense not just for abelian varieties, but for arbitrarily commutative group schemes. In particular, we can consider $T_l(\mathbb{G}_m) = \varprojlim \mu_{l^n}$ and we define it as $\mathbb{Z}_l(1)$. It's a free module of rank one over $\mathbb{Z}_l$ but it has a natural action of the Galois group (from the action of Gal on the roots of unity). This is a map $\text{Gal}(k^s/k) \to \mathbb{Z}_l^*$ (the cyclotomic character).

Let's make a few definitions.

17.2 Definition. We can consider the category of continuous representations of $\mathrm{Gal}(k^s/k)$ on finite, free $\mathbb{Z}_l$-modules. Let M be an object of this category. We define the **Tate twist**

$$M(n) = M \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(1)^{\otimes n}$$

where for $n < 0$, we define $(\mathbb{Z}_l(1))^{\otimes n} = (\mathbb{Z}_l(1)^\vee)^{\otimes -n}$. As a $\mathbb{Z}_l$-module, this changes nothing, but the action of the Galois group is twisted.

17.3 Proposition. $(T_l(A))^\vee \simeq T_l\hat{A}(1)$.

Proof. We just do it at the finite stage. There, we know that, as finite group schemes,

$$\widehat{A[l^m]} \simeq \hat{A}[l^m].$$

This means that

$$A[\hat{l^m}](k^s) = \mathrm{Hom}(A[l^m]_{k_s}, \mathbb{G}_{m,k^s}) = \mathrm{Hom}(A[l^m](k^s), \mu_{l^m}).$$

The last thing is just a hom-set in the category of groups. Everything here is compatible with the Galois action, and now we can just take the limit to get

$$T_l\hat{A} \simeq \mathrm{Hom}(T_lA, \mathbb{Z}_l(1)).$$

Now dualize. ▲

17.4 Proposition. *Let $f : A \to B$ be an isogeny, and let $N = \ker f$ (as a finite group scheme); then we have a natural short exact sequence of $\mathbb{Z}_l[\mathrm{Gal}(k^s/k)]$-modules*

$$0 \to T_l(A) \to T_l(B) \to N(k^s)_l \to 0$$

where $N_l(k^s)$ is the l-Sylow subgroup over $N(k^s)$.

Proof. What is the Tate module? We have

$$T_l(A) = \varprojlim A[l^n]$$

and this is equivalently

$$T_l(A) = \varprojlim \mathrm{Hom}(\mathbb{Z}/l^n\mathbb{Z}, A(\overline{k})] = \mathrm{Hom}(\varinjlim \mathbb{Z}/l^n\mathbb{Z}, A(\overline{k})) = \mathrm{Hom}(\mathbb{Q}_l/\mathbb{Z}_l, A(\overline{k})).$$

We have an exact sequence

$$0 \to N(\overline{k}) \to A(\overline{k}) \to B(\overline{k}) \to 0$$

of abelian groups (together with Galois-action). Now apply the functor $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}_l/\mathbb{Z}_l, \cdot)$ to this short exact sequence, to get

$$0 \to \mathrm{Hom}(\mathbb{Q}_l/\mathbb{Z}_l, N(\overline{k})) \to T_l(A) \to T_l(B) \to \mathrm{Ext}^1(\mathbb{Q}_l/\mathbb{Z}_l, N(\overline{k})) \to \mathrm{Ext}^1(\mathbb{Q}_l/\mathbb{Z}_l, A(\overline{k})).$$

The last term is zero because $A(\overline{k})$ is divisible, and hence an injective object in the category of abelian groups. The first term is zero because the Tate module of N is zero.

Finally, we need to identify $\mathrm{Ext}^1(\mathbb{Q}_l/\mathbb{Z}_l, N(\overline{k}))$. Here $N(\overline{k}) = N(k^s)$ is a finite group so it decomposes as the l-torsion plus stuff primary to l. That is, $N(\overline{k}) = N_l \times N^l$ where N_l is the l-torsion and N^l is prime to l. So we can write

$$\mathrm{Ext}^1(\mathbb{Q}_l/\mathbb{Z}_l, N(\overline{k})) = \mathrm{Ext}^1(\mathbb{Q}_l/\mathbb{Z}_l, N_l) \oplus \mathrm{Ext}^1(\mathbb{Q}_l/\mathbb{Z}_l, N^l)$$

where the second term is zero, because N^l is annihilated by something prime to l (which acts by isomorphisms on $\mathbb{Q}_l/\mathbb{Z}_l$). So, we just need to calculate the first term. We can do this using the short exact sequence

$$0 \to \mathbb{Z}_l \to \mathbb{Q}_l \to \mathbb{Q}_l/\mathbb{Z}_l \to 0$$

and applying $\mathrm{Hom}(\cdot, N_l)$ to this sequence. Since $\mathbb{Q}_l$ is injective, we get a natural isomorphism $\mathrm{Ext}^1(\mathbb{Q}_l/\mathbb{Z}_l, N_l) \simeq \mathrm{Hom}(\mathbb{Z}_l, N_l) = N_l$.

This gives the short exact sequence in the proposition. The action of the Galois group extends to all this. ▲

We will talk more about the Tate module later on.

How about the $l = p$ case? Here's a brief introduction. One can still define:

17.5 Definition. The **p-adic Tate module** is

$$T_{p,\mathrm{et}}(A) = \varprojlim A[p^m](\overline{k})$$

and this is a free $\mathbb{Z}_p$-module of rank r (r the p-rank). This is *not* the same as taking points over the separable closure because $A[p^m]$ is not étale (though it is ok if k is perfect).

It's not as good as the l-adic Tate module. You lose some information. In fact, you only see the étale quotient of this group (**wait, why?**) and you don't see the local part of the group from this. Instead, people introduce the following notation:

17.6 Definition. Let S be a base scheme. A **p-divisible group** X is an inductive system $\{X_n, \iota_n\}, n \geq 0$ (with $X_0 = S$) where X_n is commutative, finite flat over S and ι_n is a closed imbedding $X_n \hookrightarrow X_{n+1}$. We require that multiplication by p map $X_n \to X_n$, it factors through $\iota_{n-1} : X_{n-1} \to X_n$, so we get maps $\pi_n : X_n \to X_{n-1}$ factoring multiplication by p. Finally, we require that π_n be faithfully flat.

17.7 Example. Let A be an abelian variety. Then we can define a p-divisible group $A[p^\infty] = \{A[p^n], \iota_n\}$. Here ι_n is the natural closed imbedding $A[p^n] \hookrightarrow A[p^{n+1}]$.

For historical reasons, people tend to work with these sorts of inductive systems rather than projective systems. There are several facts to discuss. Let's make one more definition.

17.8 Definition. Consider X_1; this is killed by multiplication by p. Therefore, the rank of $\mathcal{O}_{X_1}$ over S is a power p^r of p. In fact, $\mathcal{O}_{X_1}$ is a locally free sheaf of Hopf algebras and taking the fiber over one point, we can see the claim (**wait, why?**). This rank r is called the **height** of the p-divisible group X. Inductively one sees that the rank of X_n is p^{nr}.

The height of $A[p^\infty]$ is p^{2g}.

We've just introduced some notation. This notation is a good substitute for the l-adic Tate module for l at p. But it contains more information than the p-adic Tate module.

Lecture 18
3/28

The category AV_k of abelian varieties over k and morphisms of abelian varieties is pretty complicated. Here is a simpler quotient category.

18.1 Definition. AV_k^0 is the category of abelian varieties up to isogeny.

1. Objects are abelian varieties.
2. Morphisms between A, B are given by $\mathrm{Hom}_{\mathrm{AV}_k^0}(A, B) = \mathrm{Hom}_{\mathrm{AV}_k}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Note that every isogeny is invertible in AV_k^0. This is because if $f : A \to B$ is any isogeny, there is an isogeny $g : B \to A$ such that $g \circ f$ is multiplication by n for some n. We can also find some $h : B \to A$ such that $f \circ h$ is multiplication by some m. We have inverted multiplication by n for every n. This means that f is an isomorphism in this category.

It's much simpler to study AV_k^0 than AV_k.

18.2 Theorem (Poincaré complete reducibility)**.** *Let $A \subset B$ be an abelian subvariety. Then there exists an abelian subvariety $C \subset B$ such that the natural map*

$$A \times C \to B$$

is an isogeny. In other words, in AV_k^0, every object can be decomposed as a product of irreducibles.

Proof. Consider an ample line bundle $\mathcal{L}$ on B. There is a map $A \hookrightarrow B$ which is a closed imbedding, so there is a commutative diagram

$$\begin{tikzcd} A \arrow[r] \arrow[d, "\phi_{\mathcal{L}|_A}"] & B \arrow[d, "\phi_{\mathcal{L}}"] \\ \hat{A} & \hat{B} \arrow[l] \end{tikzcd} .$$

The kernels of the vertical maps are finite because $\mathcal{L}$ and $\mathcal{L}|_A$ are ample. Let C be the connected component of the kernel of $B \to \hat{A}$, and we claim that the map $A \times C \to B$ is an isogeny.

To see that the kernel of $A \times C \to B$ is finite, we need to see that $A \cap C$ is is finite. But that's because anything in $A \cap C$ maps to zero in $\hat{A}$ and $A \xrightarrow{\phi_{\mathcal{L}}|_A} \hat{A}$ has finite kernel.

Now we need to see that the map is surjective. We can do this by counting dimensions. The map from $\hat{B} \to \hat{A}$ is surjective (because the map $A \to \hat{A}$ is already surjective), and the fibers have dimension $\dim B - \dim A$. Thus the fiber dimensions of $B \to \hat{A}$ have that dimension too. ▲

18.3 Definition. An abelian variety A is called **simple** if it does not contain any abelian subvariety other than $\{0\}$ or A.

18.4 Corollary. *Up to isogeny, every abelian variety is a product of simple abelian varieties. In fact,*

$$A \sim \prod A_i^{n_i}$$

where the A_i are simple, and the A_i, A_j are pairwise nonisogeneous. This decomposition is unique up to permutation.

Remark. If you work a little harder, you can show that AV_k^0 is a *semisimple abelian category.* We don't need this, though.

18.5 Definition (Notation)**.** We write Hom^0 for the Hom-set in AV_k^0 (i.e. $\mathrm{Hom}^0(A, B) = \mathrm{Hom}(A, B) \otimes \mathbb{Q}$).

If A is simple, then we can consider its endomorphism ring $\mathrm{End}^0(A) = \mathrm{Hom}^0(A, A)$ in AV_k^0; by Schur's lemma, this is a division algebra.

18.6 Corollary. *For every A, the ring* $\mathrm{End}^0(A)$ *is semisimple, and can be written as a tensor product of matrix algebras over division algebras.*

This follows from the decomposition of A up to isogeny.

We will see that these are in fact finite-dimensional over $\mathbb{Q}$.

Remark. Being simple is not necessarily preserved under base-extension. It refers to a particular field.

We will now construct an important structure on the endomorphism ring.

18.7 Definition. Let E a field, and V/E be a vector space (not necessarily finite-dimensional). A function $V \to E$ is called **homogeneous of degree** n if the restriction of f to any finite-dimensional subspace is a polynomial function, homogeneous of degree n. Equivalently, for any two vectors $v_1, v_2 \in V$, the function $f(\lambda_1 v_1 + \lambda_2 v_2)$ is homogeneous of degree d.

18.8 Definition. The *degree* of an endomorphism $f : A \to A$ is defined to be the ordinary degree if f is an isogeny and zero otherwise.

18.9 Theorem. *There is a unique way of extend the degree to a homogeneous polynomial of degree $2g$ as a function* $\mathrm{End}^0(A) \to \mathbb{Q}$*.*

To prove this claim, we note that there is a strong restriction on $\mathrm{End}^0(A)$ as a result. Clearly $\mathrm{End}(A) \subset \mathrm{End}^0(A)$ is a sub $\mathbb{Z}$-module of a $\mathbb{Q}$-vector space. A priori, it could be very divisible. But if there exists a polynomial function on this $\mathbb{Q}$-vector space which takes integer values on this $\mathbb{Z}$-module $\mathrm{End}(A)$, then $\mathrm{End}(A)$ cannot be very divisible.

Proof. We will give another interpretation of the degree. Pick an ample line bundle $\mathcal{L}$ on A such that $\chi(L) \neq 0$ (e.g. by taking a high tensor power). Then:

18.10 Lemma. *$\deg(f) = \chi(f^*\mathcal{L})/\chi(\mathcal{L})$.*

Let's assume this lemma and finish the proof.

Assuming the lemma, let's prove the theorem. The function $\deg : \mathrm{End}(A) \to \mathbb{Z}$ is homogeneous of degree $2g$ in the following sense: $\deg(nf) = n^{2g} \deg f$. In fact, if f is not an isogeny, then both are zero; if f is an isogeny, then we use the fact that $\deg([n]_A) = n^{2g}$. There is thus a unique extension $\deg : \mathrm{End}^0(A) \to \mathbb{Q}$ which is weakly homogeneous of degree $2g$—that is, such that $\deg(nf) = n^{2g} \deg f$. We still need to show that it is a polynomial function.

Now, we need to show that for any $f_1, f_2 \in \mathrm{End}(A)$, the degree $\deg(nf_1 + f_2)$ is a polynomial in n. This will suffice to show that the degree and its extension are polynomial functions.

By the lemma, $\deg(nf_1 + f_2) = \chi((nf_1 + f_2)^*\mathcal{L})/\chi(\mathcal{L})$. Therefore, it's enough to show that $\chi((nf_1+f_2)^*\mathcal{L})$ is a polynomial function (in n). But what is this line bundle? We can use the theorem of the cube. Given three maps $f, g, h : X \to A$, we have

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

where $+$ means $\otimes$. Let's apply this to nf_1, f_1, f_1.

Let $\mathcal{L}_n = (nf_1 + f_2)^*\mathcal{L}$. We find

$$\mathcal{L}_{n+2} = \mathcal{L}_{n+1} + \mathcal{L}_{n+1} + (2f_1)^*\mathcal{L} - \mathcal{L}_1 - f_1^*\mathcal{L} - f_1^*\mathcal{L}.$$

Using this, one gets

$$\mathcal{L}_n - \mathcal{L}_{n-1} =$$

▲

Lecture 19
3/30

Last time, we defined for an endomorphism f of an abelian variety A,

$$\deg f$$

to be either the degree of f as a morphism if f is an isogeny, or zero otherwise. We wanted to prove:

$$\deg f = \frac{\chi(f^*\mathcal{L})}{\chi(\mathcal{L})} \tag{8}$$

for $\mathcal{L}$ an ample line bundle with $\chi(\mathcal{L}) \neq 0$. There are two cases to check:

1. f is an isogeny.

2. f is not an isogeny.

More generally, in case 1:

Let G be a group scheme over k of finite type, X a scheme over k of finite type, equipped with the trivial G-action.

19.1 Definition. A **G-torsor** P over X is a G-scheme P (that is, a scheme with a right G-action) together with a G-equivariant morphism $\pi : P \to X$ such that the natural map $P \times_k G \to P \times_X P$ is an isomorphism. In other words, a principal G-bundle.

19.2 Example. If $f : A \to B$ is an isogeny, then it is a $N = \ker f$-torsor. The following diagram is cartesian:

$$\begin{tikzcd} A \times N \arrow[r] \arrow[d] & A . \arrow[d] \\ A \arrow[r] & B \end{tikzcd}$$

19.3 Theorem. *Let G be finite (e.g. N in the previous example), $\pi : P \to X$ a G-torsor, and X proper over a field. Then for any coherent sheaf $\mathcal{F}$,*

$$\chi(\pi^* \mathcal{F}) = (\deg \pi)\chi(\mathcal{F}).$$

Note that π is a finite morphism, so this makes sense. Of course, this theorem implies the first case of (8).

Proof. Dévissage.

This is similar to the idea we used before. By Noetherian induction, we can assume the theorem holds for dimension $< n$ and we can assume that X is irreducible. (This is because if the theorem holds for sheaves $\mathcal{F}_1, \mathcal{F}_2$, it holds for any extension of $\mathcal{F}_1, \mathcal{F}_2$, and any coherent sheaf has a filtration whose quotients are each supported on an irreducible component.) We can similarly assume X is reduced.

Let r be the generic rank of $\mathcal{F}$. We can assume $r > 0$, because if $r = 0$, then $\mathcal{F}$ is supported on a proper closed subscheme. There exists an open set $U \subset X$ such that $\mathcal{F}|_U \simeq \mathcal{O}_X^r$. There is a map $\mathcal{O}_U^r \to \mathcal{F}|_U \oplus \mathcal{O}_U^r$ given by this isomorphism plus the diagonal map. This gives a subsheaf of $(\mathcal{F} \oplus \mathcal{O}_X^r)|_U$ and we can extend this to a subsheaf $\mathcal{G} \subset \mathcal{F} \oplus \mathcal{O}_X^r$ (we can always extend subsheaves). Then we can consider the projection

$$\mathcal{G} \to \mathcal{F}$$

which is an isomorphism on U, so the kernel and cokernel are supported on subschemes of proper codimension. Similarly for $\mathcal{G} \to \mathcal{O}_X^r$. By the inductive hypothesis, we find that the statement for $\mathcal{F}$ is equivalent to the statement of $\mathcal{G}$, which is equivalent to $\mathcal{O}_X^r$. We just have to prove the theorem for any one sheaf of generic rank $r > 0$. In particular, we could just prove the theorem for $\pi_* \mathcal{O}_P$.

So, what is this for $\mathcal{O}_X$? Let $\mathcal{F} = \pi_* \mathcal{O}_P$. We want to show that $\chi(\pi^* \pi_* \mathcal{O}_P) = \deg \pi \chi(\pi_* \mathcal{O}_P)$. We have a cartesian diagram

$$\begin{tikzcd}
P \times G \arrow[r] \arrow[d] & P \arrow[d] \\
P \arrow[r] & X
\end{tikzcd}$$

and by flat base change, we find that $\pi^* \pi_* \mathcal{O}_P = \mathcal{O}_P \otimes k[G]$. This gives the result. ▲

Anyway, that proves one case of the result we wanted. Now suppose f is not an isogeny. We want to show that $\chi(f^* \mathcal{L}) = 0$. It turns out that this is not so easy to prove.

19.4 Proposition. *Let $\mathcal{L}$ be a line bundle on the abelian variety A. Then $\chi(\mathcal{L}^n)$ (a polynomial of degree $\leq g$) is a* homogeneous *polynomial of degree g, of the form $d\frac{n^g}{g!}$.*

Once we know that, we can prove that $\chi(f^* \mathcal{L}) = 0$. It follows that $\chi(f^* \mathcal{L}) = 0$ because $\chi(f^* \mathcal{L}^n) = d_{f^* \mathcal{L}} \frac{n^g}{g!}$. This is also $\chi(f_*(f^* \mathcal{L}^n)) = \chi(f_* \mathcal{O}_A \otimes \mathcal{L}^n)$ (projection formula), and $f_* \mathcal{O}_A$ is supported on a closed subscheme of A. This means that $\chi(f_* \mathcal{O}_A \otimes \mathcal{L}^n)$ is of degree $< g$.

Proof. We want to show that for all m, n

$$\chi(\mathcal{L}^{mn}) = m^g \chi(\mathcal{L}^n),$$

which is the homogeneity claimed. We might as well prove it for m^2 instead of m.

But this is true if $\mathcal{L}$ is *symmetric*, i.e. $\mathcal{L} = (-1)^* \mathcal{L}$. In this case we know that $m^* \mathcal{L} = \mathcal{L}^{m^2}$. Therefore

$$\chi(\mathcal{L}^{nm^2}) = \chi(m^* \mathcal{L}^n) = (\deg m) \chi(\mathcal{L}^n) = m^{2g} \chi(\mathcal{L}^n),$$

using the result we just proved on torsors. If $\mathcal{L} \in \mathrm{Pic}^0$, then we know that $\chi(\mathcal{L}) = 0$ (because $\mathcal{L}$ is algebraically zero, so $\chi(\mathcal{L}) = \chi(\mathcal{O}_A) = 0$; we also proved this earlier, via $h^i(A, \mathcal{L}) = 0$ for all i). However, taking powers preserves Pic^0.

Now, (see below) every line bundle can be written as $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2$ where $\mathcal{L}_1$ is symmetric and $\mathcal{L}_2 \in \mathrm{Pic}^0$. Thus, $\chi(\mathcal{L}^{m^2 n}) = \chi(\mathcal{L}_1^{m^2 n}) = m^{2g} \chi(\mathcal{L}_1^n) = m^{2g} \chi(\mathcal{L}^n)$. (We can replace $\mathcal{L}_2$ by $\mathcal{O}_A$ in the Euler characteristic because there is an algebraic family connecting them.)

19.5 Lemma. *Assume $k = \overline{k}$. Every line bundle $\mathcal{L} \in \mathrm{Pic}(A)$ is the tensor product of something in* Pic^0 *and a symmetric line bundle.*

Proof. We want to find an $\mathcal{L}_2$ such that $\mathcal{L} \otimes \mathcal{L}_2^{-1}$ is symmetric. That is,

$$(\mathcal{L} \otimes \mathcal{L}_2^{-1}) = (-1)^* (\mathcal{L} \otimes \mathcal{L}_2^{-1}).$$

This is equivalent to

$$\mathcal{L}_2^2 = \mathcal{L}_2 \otimes (-1)^* \mathcal{L}_2^{-1} = \mathcal{L} \otimes (-1)^* \mathcal{L}^{-1}.$$

So we need to find an $\mathcal{L}_2$ satisfying this. For this to happen, $\mathcal{L} \otimes (-1)^*\mathcal{L}^{-1}$ better be algebraically equivalent to zero; however, if we can show that $\mathcal{L} \otimes (-1)^*\mathcal{L}^{-1} \in \mathrm{Pic}^0$ because then $\mathcal{L}_2$ can be taken as the square root of $(\mathcal{L} \otimes (-1)^*\mathcal{L}^{-1})$. We can find a square root as Pic^0 is divisible.

Anyway, so we're reduced to proving that $(\mathcal{L} \otimes (-1)^*\mathcal{L}^{-1}) \in \mathrm{Pic}^0$. This means that this line bundle is translation-invariant, i.e.

$$T_x^*\mathcal{L} \otimes T_x^*(-1)^*\mathcal{L}^{-1} \simeq \mathcal{L} \otimes (-1)^*\mathcal{L}^{-1}.$$

This in turn is equivalent to

$$T_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \simeq (-1)^*(T_{-x}^*\mathcal{L} \otimes \mathcal{L}^{-1}).$$

The latter is the same thing as $T_{-x}^*\mathcal{L}^{-1} \otimes \mathcal{L}$ because the thing inside $(-1)^*$ is in Pic^0 (theorem of the square). We thus need to show

$$T_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \simeq T_{-x}^*\mathcal{L}^{-1} \otimes \mathcal{L},$$

which is the theorem of the square. Namely, the left side is a translation of the right side and the right side is in Pic^0. ▲

▲

Remark. We are almost there for Riemann-Roch formula on an abelian variety. We know that

$$\chi(\mathcal{L}^n) = \frac{d_{\mathcal{L}} n^g}{g!}$$

where $d_{\mathcal{L}}$ is the degree if $\mathcal{L}$ is very ample. If $\mathcal{L}$ is defining an imbedding in projective space, then $d_{\mathcal{L}}$ is just the degree of the abelian variety. In other words, $d_{\mathcal{L}}$ is the self-intersection D^g where D is the hyperplane class (the divisor associated to $\mathcal{L}$). So we can write, for $\mathcal{L}$ very ample,

$$\chi(\mathcal{L}) = \frac{D^g}{g!}.$$

In general, the right formula is the following: for every line bundle $\mathcal{L}$ on A, you can attach its first Chern class $c_1(\mathcal{L})$. If A is over $\mathbb{C}$, then this lives in $H^2(A;\mathbb{Z})$; in general, it is something in $\mathrm{Ch}^1(A)$ (the Chow group). (You can also take this in étale cohomology, if you like.) Anyway, all the Chow-groups, or the cohomology groups, have a ring structure. Then $\frac{c_1^g}{g!}$ lives in the top cohomology group. Anyway, the general Riemann-Roch formula is

$$\chi(\mathcal{L}) = \frac{c_1^g}{g!}.$$

Lecture 20
4/2

20.1 Theorem. *Let A, B be two abelian varieties over k. Then the natural map*

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_l \to \mathrm{Hom}(T_l(A), T_l(B))$$

is injective. In particular, $\mathrm{Hom}(A, B)$ *is a free $\mathbb{Z}$-module of finite rank.*

Proof. Consider isogenies $\prod A_i \to A$, $B \to \prod B_j$ where the A_i, B_j are simple. Then we know that $\mathrm{Hom}(A, B) \to \prod \mathrm{Hom}(A_i, B_j) \to \prod \mathrm{Hom}(T_l(A_i), T_l(B_j))$ and of course the first map is injective. There is a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}(A,B) \otimes \mathbb{Z}_l \arrow[r] \arrow[d] & \mathrm{Hom}(T_lA, T_lB) \arrow[d] \\
\prod \mathrm{Hom}(A_i, B_j) \otimes \mathbb{Z}_l \arrow[r] & \prod_{i,j} \mathrm{Hom}(T_lA_i, T_lB_j)
\end{tikzcd}.$$

From this, we see that we might as well prove the bottom map is injective. We can thus reduce to the case where A, B are *simple.* If A, B are not isogeneous, there is nothing to prove. If A, B are isogenous, we can compose with an isogeny to reduce to the case $B = A$.

These reductions show that we just need to prove the theorem for *simple* abelian varieties A, specifically that

$$\mathrm{Hom}(A, A) \otimes \mathbb{Z}_l \to \mathrm{Hom}(T_lA, T_lA)$$

is an injection. It's enough to show that for any finitely generated abelian group $M \subset \mathrm{Hom}(A, A)$, the map $M \otimes \mathbb{Z}_l \to \mathrm{Hom}(T_lA, T_lA)$ is injective.

Because of the polynomial function, any finitely generated subgroup can't be too divisible. Let $QM = \{f \in \mathrm{End}(A), \exists n, nf \in M\}$; that is, QM consists of all those f a multiple of which lands in M. The claim is that QM is also finitely generated. In fact, $QM = M \otimes \mathbb{Q} \cap \mathrm{End}(A)$ inside $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$. Here $M \otimes \mathbb{Q}$ is a finite-dimensional vector space over $\mathbb{Q}$ and we have this degree function deg on it. The degree is a nonzero integer for any element of $\mathrm{End}(A) \setminus \{0\}$.[18] Now we have a vector space $M \otimes \mathbb{Q}$ and a subgroup $QM \subset M \otimes \mathbb{Q}$ and a polynomial function deg on $M \otimes \mathbb{Q}$ such that the open neighborhood $\{\deg < 1\}$ does not intersect with QM. This means that QM must be discrete in $M \otimes \mathbb{R}$, hence finitely generated.

So, OK. It's enough to prove that if M is finitely generated and $M = QM$, then the map

$$M \otimes \mathbb{Z}_l \to \mathrm{End}(T_lA)$$

is injective. QM is free (it's torsion-free and finitely generated), so pick a $\mathbb{Z}$-basis $f_1, \dots, f_k$ be one. Suppose $\sum a_i T_l(f_i) = 0$ for some l-adic integers a_i; we want a contradiction. (If not all the a_i are zero.) We can assume that one of the a_i is not divisible by l (by dividing by l–everything here is a free $\mathbb{Z}_l$-module, after all). So assume there exists an a_i which is a unit in $\mathbb{Z}_l$.

Anyway, what does the condition $\sum a_i T_l(f_i) = 0$ mean? Replace each a_i by integers a_i' such that $a_i' \equiv a_i \mod l\mathbb{Z}_l$. Then the condition means that $\sum a_i' f_i$ sends $T_l(A)$ into to $lT_l(A)$, although one of the a_i' is not divisible by l.

So let $f = \sum a_i' f_i$ (this is an honest endomorphism of A, since the a_i' are *integers*), so $T_l(f)$ sends $T_l(A)$ into $lT_l(B)$. This implies in particular that $A[l] \subset \ker f$. However, by descent this means that $f = f' \circ l$, which is a contradiction as f was not divisible by l in $M = QM$. ▲

[18] This is because the degree of an isogeny is not zero: an endomorphism of a simple abelian variety is an isogeny or zero.

Recall the *Neron-Severi group* $NS(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ (line bundles mod algebraic equivalence), which maps (via ϕ) to $\mathrm{Hom}(A, \hat{A})$. This is injective, by definition. Since $\mathrm{Hom}(A, \hat{A})$ is of finite rank, we get:

20.2 Corollary. *$NS(A)$ is a finitely generated free abelian group.*

Finite generation is always true for any variety, but torsion-freeness is not.

20.3 Definition. The rank of the Neron-Severi group is called the **base number** of A.

20.4 Corollary. *$\mathrm{End}^0(A)$ is a finite-dimensional semisimple $\mathbb{Q}$-algebra.*

This means that $\mathrm{End}^0(A)$ can be written as $\prod M_{n_i}(D_i)$ for the D_i finite-dimensional division algebras over $\mathbb{Q}$. We understand finite-dimensional algebras over $\mathbb{Q}$ fairly well.

Let D be a finite-dimensional division algebra over $\mathbb{Q}$. Let $K = \mathrm{Cent}(D)$, so D is a *central* division algebra over K. Then $D \otimes_K \overline{K}$ is a finite-dimensional simple algebra over $\overline{K}$, central, so it is a matrix algebra $M_{d\times d}(\overline{K})$ (Artin-Wedderburn). So, getting a description of division algebras over K is a question of Galois descent. We'll take more about this later and classify all the possible $\mathrm{End}^0(A)$'s.

Let's remember the definition.

20.5 Definition. Let B be a finite-dimensional simple algebra over a field $\mathbb{Q}$. A function $N : B \to \mathbb{Q}$ is called a **norm form** if N is a polynomial function and $N(ab) = N(a)N(b)$. A function $T : B \to \mathbb{Q}$ is called a **trace form** if T is linear and $T(ab) = T(ba)$.

For example:

20.6 Proposition. *Let B be finite-dimensional simple over $\mathbb{Q}$ and let $K \subset B$ be the center.*[19] *Then there exists a unique norm form $N^0 : B \to K$ and a unique up to constant trace form $T^0 : B \to K$ such that, for any norm form $N : B \to \mathbb{Q}$ is of the form $(N_{K/\mathbb{Q}} \circ N^0)^i$ and any trace form $T : B \to \mathbb{Q}$ is of the form $\phi \circ T^0$) for some linear map $\phi : K \to \mathbb{Q}$.*

Proof. If $K = \mathbb{Q}$ (i.e. B is central), then we just base-change to $\overline{K}$ to construct the norm-form: here $B \otimes_K \overline{K} \simeq M_d(\overline{K})$. But a norm-form on a matrix algebra is just a power of the determinant. And then apply "Galois descent" to define the norm-form on B itself. Similarly for trace functions—any trace form on a matrix algebra factors through the quotient of $M_d(\overline{K})/[M_d(\overline{K}), M_d(\overline{K})]$. So we can use trace functions to descend as well.

In general, for any B, you consider $B \otimes_{\mathbb{Q}} \mathbb{Q} = B \otimes_K K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ and $K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is isomorphic to $\prod K_i$ for the K_i the Galois conjugates. So $B \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is isomorphic to $\prod M_d(\overline{K})$. A norm form induces a norm form here and we can classify norm forms on products of matrix algebras. So we are reduced to the case of norm forms on products of matrix algebras: these are given by products of the powers of the determinant on various factors. Using the action of the Galois, the various powers of the determinant are all the same. Similarly for the trace. ▲

[19] K is a field by the structure theorem: B is some matrix algebra over a division algebra.

(This was pure algebra, so we sketched it.)

20.7 Definition. N^0 is called the **reduced norm** and T^0 is called the **reduced trace**.

All this discussion holds for other fields, too, e.g. $\mathbb{Q}_l$.

We have a polynomial function deg on $\operatorname{End}^0(A) \to \mathbb{Q}$. If we base-change to $\mathbb{Q}_l$, we get a polynomial function on a $\mathbb{Q}_l$-vector space $\operatorname{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_l$. There is also another polynomial function: namely, $\operatorname{End}^0(A) \otimes_{\mathbb{Q}_l} \to \operatorname{End}(T_l A \otimes \mathbb{Q}_l) \overset{\det}{\to} \mathbb{Q}_l$. I.e., take the determinant of the action on the Tate module tensored with $\mathbb{Q}_l$.

20.8 Theorem. *These two polynomial functions on* $\operatorname{End}^0(A) \otimes \mathbb{Q}_l$ *are the same.*

Proof. Both are norm forms.

Note that for any $f \in \operatorname{End}^0(A)$, then the l-adic absolute value of $\deg f$ is the same as the l-adic absolute value of the determinant of $T_l(A)$: that is, $|\deg f|_l = |\det T_l(f)|_l$. (**Why is this?**)

Together, these will imply the theorem. In fact, we reduce to the case of A simple, so that $\operatorname{End}^0(A)$ is *simple*, and then two norm forms are powers of a common one, so if they have the same absolute values, then they are the same. ▲

Lecture 21
4/4

We want to prove the following theorem.

21.1 Theorem. *The degree of any element* $\phi \in \operatorname{End}^0(A)$ *is the same as the determinant of* $T_l(\phi)$ *(where* ϕ *acts on* $T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$*).*

Proof. It's enough to show that this is true after taking the l-adic absolute value. Everything here is an l-adic number, and we're going to claim

$$|\deg \phi|_l = |\det T_l(\phi)|_l, \tag{9}$$

and we'll be done after that because both are norm forms on this finite-dimensional semisimple $\mathbb{Q}_l$-algebras $\operatorname{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_l$. In fact, if $\operatorname{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_l = B_1 \times \cdots \times B_r$ (the B_i simple), then deg is a product of powers of the reduced norms on the B_i. Similarly for $\det T_l$. If they have the same absolute value, this would imply that the exponents have to be the same. By continuity, we can reduce to showing this for ϕ an element of $\operatorname{End}^0(A)$, and in fact to ϕ an element of $\operatorname{End}(A)$ (since both sides are homogeneous of degree $2g$).

If ϕ is not an isogeny, then $T_l(\phi) \otimes \mathbb{Q}$ is not an isomorphism (the image is of smaller dimension). So everything is zero. Therefore, assume ϕ is an isogeny. Then there is an exact sequence

$$0 \to T_l(A) \overset{T_l(\phi)}{\to} T_l(A) \to (\ker \phi)_l \to 0.$$

(We saw this earlier.) This means precisely that the l-adic absolute value of $\det T_l(\phi)$ (which is the index of the image) is the order of $(\ker \phi)_l$. ▲

21.2 Theorem. *Let $\phi \in \operatorname{End}(A)$. We can define the polynomial $P(n) = \deg(n - \phi)$. Then this is the characteristic polynomial of the linear operator $T_l(\phi)$. In particular, $p(x) \in \mathbb{Z}[x]$ and the leading coefficient is one.*

Proof. This follows from the previous result: $\deg(n - \phi) = \det(n - T_l(\phi))$. Note that $p(n)$ is in $\mathbb{Z}$ always, so it has rational coefficients. But $T_l(\phi)$ comes from a map of $\mathbb{Z}_l$-modules, $T_l(A) \to T_l(A)$, so $p(n)$ has at least $\mathbb{Z}_l$ coefficients. We can do this for every l, not the characteristic, so the worst that can happen is that $p(n)$ has coefficients with denominators a power of the characteristic. This isn't quite sufficient.

Here's a complete argument. Because $\operatorname{End}(A)$ is finite over $\mathbb{Z}$, there exists a polynomial $q(x) \in \mathbb{Z}[x]$ with leading coefficient one so that $q(\phi) = 0$. Consequently, $q(T_l(\phi)) = 0$. This means that the roots of the characteristic polynomial of $T_l(\phi)$ are algebraic integers. Since the coefficients are in $\mathbb{Q}$, we win. ▲

So $p(x) = x^{2g} + a_1 x^{2g-1} + \dots$.

21.3 Definition. We call $p(x)$ the **characteristic polynomial** of ϕ. a_{2g} (the constant coefficient) is called the **norm** of ϕ. We call $-a_1$ the **trace** of ϕ.

OK, if we write

$$\operatorname{End}(A) = B_1 \times \cdots \times B_r, \quad B_i \text{ simple},$$

then the degree is a product of the reduced norm forms on B_i raised to various powers m_i. Then, $\operatorname{Tr}(\phi)$ is the sum of the reduced traces on B_i with factors of m_i.

Let A be *simple.* So $\deg : \operatorname{End}^0(A) \to \mathbb{Q}$ is a polynomial function of degree $2g$. If A is simple, then the degree $[\operatorname{End}^0(A) : K] = d^2$ if K is the center and $[K : \mathbb{Q}] = e$. The reduced norm then is a polynomial of degree de.

21.4 Corollary. *If A is simple, then $de \mid 2g$.*

(E.g. if $g = 1$ and A is an elliptic curve, then $d = 1, 2, e = 1, 2$.)

21.5 Proposition. *If $\operatorname{char} k = 0$, and A is simple over the algebraic closure, then $\dim \operatorname{End}^0(A) = d^2 e \mid 2g$.*

Proof. Can assume $k = \mathbb{C}$ ("Lefschetz principle"). Then $A = V/L$ for V a vector space and L a lattice. Then $L_{\mathbb{Q}} = L \otimes \mathbb{Q}$ is acted on by $\operatorname{End}^0(A)$. This is a division algebra over $\mathbb{Q}$ acting on $L_{\mathbb{Q}}$, so $L_{\mathbb{Q}}$ is thus an $\operatorname{End}^0(A)$ vector space. The dimension is

$$\dim_{\mathbb{Q}} L_{\mathbb{Q}} / \dim \operatorname{End}^0(A),$$

and this must be an integer. That means $2g / \dim \operatorname{End}^0(A) \in \mathbb{Z}$. ▲

In characteristic zero, this means that for an elliptic curve, $d = 1, e = 2$. For "supersingular" elliptic curves, $d = 2, e = 1$ (these only exist in characteristic p).

21.6 Definition. An **abelian variety** over k is called **of CM type** if there exists $F \hookrightarrow \operatorname{End}^0(A)$ with $F/\mathbb{Q}$ a field of degree $2g$.

If A is simple, then $\mathrm{End}^0(A)$ is a division algebra and the maximal subfield has degree de over $\mathbb{Q}$, and since $de \mid 2g$, we have that $de = 2g$ exactly.

If A is of CM type, then A must be isogeneous to a product $A \sim A_i^{n_i}$ for A_i simple (only one simple factor can occur). In fact, if F is such a subfield of degree $2g$ and $A = \prod A_i^{n_i}$, then F injects into $M_{n_i}(A_i)$ for some i. Any maximal subfield of $M_{n_i}(A_i)$ is of degree $n_i d_i g_i$ over $\mathbb{Q}$, so $2g \leq n_i d_i g_i \leq 2g$, which forces there to be one factor.

21.7 Definition. A is **potentially of CM type** if $A_{\overline{k}}$ is of CM type.

If $\mathrm{char} k = 0$ and A is potentially of CM type, then $\mathrm{End}^0(A) \subset \mathrm{End}^0(A_{\overline{k}})$ is a field. In fact, $\mathrm{End}^0(A_{\overline{k}})$ contains a field of degree $2g$, which must be the whole thing by the previous proposition, at least if A is geometrically simple.

Lecture 22
4/6

§1 Corrections

First, some corrections. Let's redefine a CM abelian variety. Let A be an abelian variety, of dimension $\dim A = g$.

22.1 Definition. We say that A is **of CM type (by** B**)** if the endomorphism ring of A tensored with $\mathbb{Q}$ contains a commutative semisimple algebra B of dimension $2g$ over $\mathbb{Q}$.

The following still holds.

22.2 Proposition. *If* A/k, $\mathrm{char} k = 0$, A *simple, then* $\dim_{\mathbb{Q}} \mathrm{End}^0(A) \mid 2g$.

Last time, we did this over $\overline{k}$.

Proof. By the Lefschetz principle, assume $\overline{k} = \mathbb{C}$. Then $\mathrm{End}(A) \hookrightarrow \mathrm{End}(A_{\overline{k}}) = \mathrm{End}(A_{\mathbb{C}})$. But $A_{\mathbb{C}} = V/L$ for a vector space V modulo a lattice L. Thus $\mathrm{End}^0(A)$ acts on $L \otimes \mathbb{Q}$, and since A is simple, $\mathrm{End}^0(A)$ is a division algebra. Thus, considering L as a vector space over $\mathrm{End}^0(A)$, we find that $\dim \mathrm{End}^0(A) \mid 2g$. ▲

If $\mathrm{char} k = 0$ and A is simple, of CM type, then $\mathrm{End}^0(A)$ is a *field* of degree $2g$ over $\mathbb{Q}$.

Correction: If A is CM by a field F, then A is isogeneous to $A_i^{n_i}$ for A_i simple and of CM type.

§2 Weil pairing

Now we need to talk about the *Weil pairing.* We mentioned earlier that there is an isomorphism

$$T_l \hat{A} \simeq (T_l A)^\vee(1).$$

The proof of this statement we gave was not quite complete (though the statement is correct). So let's recall the proof.

Proof. We just need to prove it at the finite level. We know that

$$\hat{A}[l^n] \simeq \widehat{A[l^n]}$$

as group schemes (where $\widehat{A[l^n]}$ denotes the Cartier dual). So

$$\hat{A}[l^n] \simeq \mathrm{Hom}(A[l^n], \mu_{l^n})$$

and we saw this earlier. Then, take the limit in l. But there's something to prove before you take the limit, which we ignored. One needs to check that this isomorphism is actually compatible in l.

In fact, the isomorphpism can be given as the bimultiplicative map

$$A[l^n] \times \hat{A}[l^n] \to \mu_{l^n},$$

and we need to see that this is compatible with changing l. That is, we need to show that there are commutative diagrams

$$\begin{tikzcd}
A[l^{n+1}] \times \hat{A}[l^{n+1}] \arrow[r] \arrow[d] & \mu_{l^{n+1}} . \arrow[d, "l"] \\
A[l^n] \times A[l^n] \arrow[r] & \mu_{l^n}
\end{tikzcd}$$

So, we need to understand this pairing map

$$e_n : A[n] \times \hat{A}[n] \to \mu_n.$$

This is induced from the isomorphism

$$\widehat{\ker\phi} \simeq \ker\hat{\phi}, \quad \phi : A \to B.$$

Let us recall how the isomorphism is constructed. Let's just look at this at the level of $\overline{k}$-points (since everything is étale). On $\overline{k}$-points, it's just a line bundle on B such that $\phi^*\mathcal{L} \simeq \mathcal{O}_A$. Given such a line bundle $\mathcal{L}$ and an element $x \in \ker\phi(\overline{k})$, we want to produce a number. This number can be given as follows: choose an isomorphism $\beta : \phi^*\mathcal{L} \simeq \mathcal{O}_A$. Compare the two trivializations when pulled back to $A \times \ker\phi$ by the two pull-backs. Namely, we get a new map $\phi^*\mathcal{L} \simeq (T_x)^*\phi^*\mathcal{L} \to T_x^*\mathcal{O}_B \simeq \mathcal{O}_A$. So, translating by β, we get a *new* isomorphism $\phi^*\mathcal{L} \simeq \mathcal{O}_A$. So, we get a number

$$e(x, \mathcal{L}) = T_x\beta\beta^{-1}.$$

Now, let $\mathcal{L} \in A[m](\overline{k})$ (so $m^*\mathcal{L}$ is trivial) and $x \in A[m](\overline{k}) \subset A[nm](\overline{k})$. We want to calculate the pairing $e_{nm}(x, \mathcal{L})$: the claim is that it is $e_m(nx, \mathcal{L})$. This will imply the claim. Choose an isomorphism $\beta : m^*\mathcal{L} \simeq \mathcal{O}_A$. Pulling back gives

$$n^*\beta : (nm)^*\mathcal{L} \simeq n^*\mathcal{O}_A \simeq \mathcal{O}_A.$$

Using this formula, $e_{nm}(x, \mathcal{L})$, is $T_x^*(n^*\beta)(n^*\beta)^{-1}$. But then this is $n^*(T_{nx}^*\beta\beta^{-1})$ and the claim follows. ▲

By the same argument (exercise), we find that if $\phi : A \to B$ is any morphism of abelian varieties, and e_{l^∞} is the Weil pairing on the Tate modules,

$$e_{l^\infty}(T_l\phi(x), y) = e_{l^\infty}(x, T_l\widehat{\phi}(y))$$

and this is checked at the finite level in a similar way.

Remember that

$$e_n(x, \mathcal{L}) = T_x^*\beta \circ \beta^{-1}.$$

Assume $\mathcal{L}$ is isomorphic to $\mathcal{O}(D)$ for some Cartier divisor D. To write as a line bundle as a line bundle associated to a Cartier divisor is the same is imbedding $i : \mathcal{L} \hookrightarrow \mathcal{K}_A$ (the sheaf of rational functions on A). A choice of trivialization β corresponds to a rational function on A. If we have $n^*\mathcal{L} \simeq \mathcal{O}_A$, then we get a rational function g by taking the image of 1 in $n^*K_A = K_A$. Then, the associated divisor of this rational function is $n^{-1}D$. So $e_n(x, \mathcal{L}) = T_x^*g/g$.

22.3 Theorem. *Fix a line bundle $\mathcal{L}$, and consider the pairing*

$$E^{\mathcal{L}} : T_lA \times T_lA \xrightarrow{\phi_{\mathcal{L}}} T_lA \times T_l\hat{A} \to \mathbb{Z}_l.$$

Then $E^{\mathcal{L}}$ is skew-symmetric.

In the theory of elliptic curves, there is a canonical pairing on the l-torsion points, called the Weil pairing. In higher dimensions, the natural pairing is with the Tate modules of A and $\hat{A}$. Elliptic curves have a canonical polarization (given by $\mathcal{O}(\{0\})$).

Proof. We need only prove that $E(x, \phi_{\mathcal{L}}(x)) = 1$ (where E is the ordinary Weil pairing). Let $\mathcal{L} = \mathcal{O}(D)$. Then $\phi_{\mathcal{L}}(x) = T_x^*\mathcal{L} \otimes \mathcal{L}^{-1} = \mathcal{O}(T_xD - D)$. Choose a rational function g such that g^{-1} has the divisor $n^{-1}(T_xD - D)$. We want $T_x^*g = g$. I.e., $g(z+x) = g(z), \forall z$. We write $x = ny$. Then, we know that (g^{-1}) is going to be $T_{-y}(n_A^{-1}D) - n_A^{-1}D$. So, in other words, $(g^{-1}) = T_{-y}E - E$. Then,

$$(T_{jy}^*(g^{-1})) = T_{-(j+1)y}E - T_{-jy}E.$$

Summing them all together gives

$$\left(\prod_0^{n-1} T_{jy}^*g^{-1}\right) = T_{-x}^*E - E = 0$$

because E is x-invariant. This means that $h = \prod_0^{n-1} T_{jy}^*g^{-1}$ is constant. So $h(z+y) = h(z)$, which implies $g(x+z) = g(x)$. ▲

So, we have a skew-symmetric pairing on the Tate module of an abelian variety, once we've chosen a line bundle. Let λ be a polarization of A; then $E^\lambda(x, y) = e_{l^\infty}(x, T_l\lambda y)$ is symplectic (skew-symmetric and nondegenerate). In fact, given any map $\phi : A \to \hat{A}$, we can form a bilinear pairing $E^\phi(x, y)$; when ϕ comes from a line-bundle, we get a skew-symmetric pairing. One might ask whether the converse is true: if E^ϕ is skew-symmetric, does ϕ come from a line bundle? For an algebraically closed field, this is true.

22.4 Lemma. *Let $\mathcal{P}$ be the Poincaré bundle on $A \times \hat{A}$. Then $T_l(A \times \hat{A}) = T_l A \times T_l \hat{A}$. Then*

$$E^P((x, \hat{x}), (y, \hat{y})) = e_{l^\infty}(x, \hat{y}) - e_{l^\infty}(y, \hat{x}).$$

22.5 Lemma. *Let $f : A \to B$. Then $E^{f^*\mathcal{L}}(x, y) = E^{\mathcal{L}}(T_l(f)(x), T_l(f)y))$.*

Lecture 23
4/9

23.1 Proposition. *If we consider the Weil pairing associated to the Poincaré line bundle on $A \times \hat{A}$, then it is given by*

$$E^{\mathcal{P}}((x, \hat{x}), (y, \hat{y})) = e_{l^\infty}(x, \hat{y}) - e_{l^\infty}(y, \hat{x}).$$

Proof. It's enough if we consider

$$E^{\mathcal{P}}((x, 0), (y, 0)) = E^{\mathcal{P}}((0, \hat{x}), (0, \hat{y})) = 0.$$

Also,

$$E^{\mathcal{P}}((x, 0), (0, \hat{y})) = e_{l^\infty}(x, \hat{y}).$$

Consider the pull-back $\iota : A \to A \times \hat{A}$, which is 1×0. Then $E^{\mathcal{P}}((x, 0), (y, 0)) = E^{\iota^{\mathcal{P}}}(x, y) = 0$ since $\iota^*\mathcal{P} = 0$. The other case is proved (somewhat) similarly. We need the fact that for abelian varieties A, B, we have a canonical isomorphism $\widehat{A \times B} = \hat{A} \times \hat{B}$: that is, Pic^0 is a linear functor. The map

$$\widehat{A \times B} \to \hat{A} \times \hat{B}$$

sends a line bundle $\mathcal{L}$ to $\mathcal{L}|_{A \times \{0\}}, \mathcal{L}|_{\{0\} \times B}$; this is injective because $\mathcal{L}$ is translation-invariant. It is an isomorphism by counting dimensions.

In particular,

$$\widehat{A \times \hat{A}} \simeq \hat{A} \times \hat{\hat{A}} \simeq \hat{A} \times A.$$

Under this isomorphism, $\phi_{\mathcal{P}}(x, \hat{x})$ goes to the pair $(\hat{x}, x)$. Hence, we find that $E^{\mathcal{P}}((x, 0), (0, \hat{y})) = e_{l^\infty}((x, 0), (\hat{y}, 0))$. (**I'm a little confused here—I should try to fix this later.**) ▲

23.2 Theorem. *Let $\phi : A \to \hat{A}$. The following are equivalent:*

1. *ϕ is symmetric.*[20]
2. *$e_{l^\infty}(\cdot, \phi(\cdot))$ is skew-symmetric.*
3. *2ϕ can be written as $\phi_{\mathcal{L}}$ for some $\mathcal{L}$.*
4. *Over the algebraic closure, ϕ can be written as $\phi_{\mathcal{L}'}$ for some $\mathcal{L}'$.*

Proof. We already know that 4 implies 1 (if something is symmetric over $\overline{k}$.

Suppose 1 is satisfied. Define $\mathcal{L} = (1 \times \phi)^*\mathcal{P}$. Then

$$E^{\mathcal{L}}(x, y) = E^{\mathcal{P}}((x, \phi(x)), (y, \phi(y)) = e_{l^\infty}(x, \phi(y)) - e_{l^\infty}(y, \phi(x)) = 2E^{\phi}(x, y)$$

by skew-symmetry. In particular, $E^{\mathcal{L}} = 2E^{\phi}$, which implies that $2\phi = \phi_{\mathcal{L}}$.

(There were some other parts of the proof, which I didn't follow.) ▲

[20] I.e., $\phi = \hat{\phi}$.

§1 The Rosati involution

We now are interested in finding possibilities for the division algebras $\mathrm{End}^0(A)$. Here is the **Rosati involution.**

23.3 Definition. Choose a polarization $\lambda : A \to \hat{A}$. Then one can define a map $\mathrm{End}^0(A) \to \mathrm{End}^0(A)$ sending ϕ to the map $\phi' : A \xrightarrow{\lambda} \hat{A} \xrightarrow{\hat{\phi}} \hat{A} \xrightarrow{\lambda^{-1}} A$. Here λ^{-1} is the formal inverse to λ in the category we are working in. One can check that $\phi \mapsto \phi'$ is an *anti-involution* on $\mathrm{End}^0(A)$. This needn't preserve the integral structure. Note that this depends on the polarization. However, two polarizations are related by an isomorphism in the isogeny category, so the anti-involution is defined *up to conjugacy.*

We have

$$E^\lambda(\phi x, y) = E^\lambda(x, \phi' y),$$

meaning that the anti=involution on $\mathrm{End}^0(A)$ corresponds to the duality anti-involution on $\mathrm{End}(T_l(A))$.

The really important theorem is:

23.4 Theorem. *The Rosati involution is positive, i.e. let* $\phi \in \mathrm{End}^0(A)$ *be nonzero. Then the trace of* $\phi\phi'$ *is positive.*

Lecture 24
4/11

We are going to prove the following theorem.

24.1 Theorem. *Fix a polarization* $\lambda : A \to \hat{A}$. *Then we get the Rosati involution*

$$' : \mathrm{End}^0(A) \to \mathrm{End}^0(A).$$

Then

$$\mathrm{Tr}(\phi\phi') > 0, \forall \phi.$$

Proof. We know that a polarization on a complex manifold is an ample line bundle, or a line bundle with a metric of positive curvature. Over a general field, we don't know how to formulate something like that, but for abelian varieties, this positivity of the Rosati involution. (This involution can be defined for any isogeny $\phi_{\mathcal{L}} : A \to \hat{A}$, but won't generally be positive.)

(Recall that the *characteristic polynomial* of any element of $\mathrm{End}^0(A)$ was defined, and the trace is the negative of the second coefficient.)

Assume that

$$\lambda = \phi_{\mathcal{L}}, \quad \mathcal{L} \text{ very ample.}$$

So $\mathcal{L} = \mathcal{O}(H)$ for a hyperplane section H. (We can do this by replacing $\mathcal{L}$ by a multiple thereof.) First, we want to give an expression of this trace. Then for $\phi \in \mathrm{End}(A)$,

$$\mathrm{Tr}(\phi\phi') = \frac{1}{H^g} 2g(H^{g-1}.\phi^{-1}(H)).$$

This will imply the theorem, because the intersection number is always positive.

Consider the line bundle $\mathcal{N} : \phi^*\mathcal{L}^{-1} \otimes \mathcal{L}^n$, which defines a map $\phi_{\mathcal{N}} : A \to \hat{A}$. What is the degree of this map? We can write

$$\begin{aligned}
&\deg \phi_{\mathcal{N}} \\
&\qquad = \deg(n\phi_{\mathcal{L}} - \phi_{\phi^*\mathcal{L}}) \\
&\qquad = \deg(\phi_{\mathcal{L}} n - \hat{\phi}\phi_{\mathcal{L}}\phi) \\
&\qquad = \deg(\phi_{\mathcal{L}} n - \phi_{\mathcal{L}}(\phi_L^{-1}\widehat{\phi}\phi_{\mathcal{L}}\phi)) = \deg(\phi_{\mathcal{L}}) \deg(n - \phi'\phi) = \deg(\phi_{\mathcal{L}})p(n)
\end{aligned}$$

for $p(n)$ the characteristic polynomial of the homomorphism $\phi'\phi$. So we need to understand the ratio of the degrees of these two maps.

We will show:

24.2 Theorem. *For any $\mathcal{L}$ nondegenerate (i.e. $K(\mathcal{L})$ finite),*

$$\deg \phi_{\mathcal{L}} = \chi(\mathcal{L})^2.$$

In view of this, we have

$$p(n) = \frac{\chi(\phi^*\mathcal{L}^{-1} \otimes \mathcal{L}^n)^2}{\chi(\mathcal{L})^2}.$$

But Riemann-Roch tells us how to compute these Euler characteristics. We have

$$\chi(\mathcal{L}) = \frac{c_1(\mathcal{L})^g}{g!}.$$

We find from all this

$$p(n) = \frac{((nH - \phi^{-1}(H))^g)^2}{(H^g)^2}.$$

The coefficient in front of n^{2g-1} is exactly

$$\frac{2gn^{2g-1}H^g H^{g-1}.\phi^{-1}(H)}{(H^g)^2}.$$

▲

Now we will compute the ratio of these degrees.

Proof of the theorem (or a weaker version). We calculate the pull-back of the Poincare line bundle to $A \times A$, i.e. given $\mathcal{L}$, we calculate $\chi((1 \times \phi_{\mathcal{L}})^*\mathcal{P})$ in two ways. As we mentioned below, this is $m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1}$ (if you forget it, apply see-saw). This is the Mumford line bundle and is denoted $M(\mathcal{L})$.

So, we'll calculate $\chi(M(\mathcal{L}))$ in two ways. First, since it is a pull-back, we have $\chi(M(\mathcal{L})) = \deg \phi_{\mathcal{L}}\chi(\mathcal{P})$. Here's another way. We can calculate the cohomology of the Mumford line bundle via the Leray spectral sequence under

$$A \times A \overset{p_1}{\to} A,$$

and notice that the cohomology is supported on $K(\mathcal{L})$. If you restrict to $y \times A$, you get $T_y^*\mathcal{L} \otimes \mathcal{L}^{-1}$, which is something algebraically equivalent to zero but for $y \notin K(\mathcal{L})$, all the cohomology vanishes. Thus, the cohomology occurs only on the $K(\mathcal{L})$'s, and this forms a finite set.

In particular, we find that

$$R^i p_{1*} M(\mathcal{L})$$

is supported on $K(\mathcal{L})$. (We have used this type of argument before.) Because of this, we know that the cohomology

$$H^i(A \times A, M(\mathcal{L})) = \Gamma(A, R^i p_{1*} M(\mathcal{L}))$$

as the Leray spectral sequence degenerates (the $R^i p_{1^*} M(\mathcal{L})$ have no higher cohomology). On the other hand, by the projection formula,

$$R^i p_{1*}(M(\mathcal{L})) = R^i p_{1^*}(m^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1} \otimes p_1^*\mathcal{L}^{-1}) = R^i p_{1*}(m^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1}) \otimes \mathcal{L}^{-1}.$$

Consequently, we find

$$R^i p_{1*}(m^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1})$$

is supported on a finite set. We have

$$H^i(A \times A, M(\mathcal{L})) = \Gamma(A, R^i p_{1*}(m^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1}).$$

From all this, we get

$$\chi(M(\mathcal{L})) = \chi(m^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1})$$

by comparing Leray spectral sequences. But, we consider the shearing isomorphism $A \times A \to A \times A$ under $m \times 1$ and $(m^* \otimes p_2^*)\mathcal{L}$ is just the pull-back of $\mathcal{L} \boxtimes \mathcal{L}$ under this. So

$$\chi(m^*\mathcal{L} \otimes p_2^*\mathcal{L}) = \chi(\mathcal{L} \boxtimes \mathcal{L}^{-1}) = \chi(\mathcal{L})\chi(\mathcal{L}^{-1})$$

by the Kunneth formula. But we know that χ of a line bundle is a homogeneous polynomial of degree g, so

$$\chi(m^*\mathcal{L} \otimes p_2^*\mathcal{L}) = (-1)^g \chi(\mathcal{L})^2.$$

As a result, we get

$$\chi(M(\mathcal{L})) = (-1)^g \chi(\mathcal{L})^2.$$

So

$$\deg \phi_{\mathcal{L}} \chi(\mathcal{P}) = (-1)^g \chi(\mathcal{L})^g.$$

Thus, one has to show that $\chi(\mathcal{P}) = (-1)^g$, but Michael will present a proof later. For our purposes, this is already enough; we just need to compute the ratios of degrees. ▲

OK, let's now assume A is simple. Let $D = \mathrm{End}^0(A)$; this is a finite-dimensional division algebra over $\mathbb{Q}$ with an anti-involution $'$ (the Rosati involution) such that $\mathrm{Tr}(\phi\phi') > 0$ (for $\mathrm{Tr} = \mathrm{Tr}_{D/\mathbb{Q}}$ the reduced trace, which is a positive multiple of the trace we used before). Now this is a purely algebraic problem. Given a finite-dimensional division algebra with anti-involution with this positivity condition, we might try to classify all such. (These are called **Albert algebras.**) The answer is yes. This is given by:

24.3 Theorem (Classification of Albert algebras, I)**.** *Let D be an Albert algebra with involution $'$. Let K be the center, and $K^0 = \{a \in K, a' = a\}$. Then K^0 is totally real, and K is either K^0 or a totally imaginary quadratic extension.*

(So, Albert *fields* are totally real or totally imaginary quadratic extensions thereof.) The proof is purely algebra, and we'll give it.

Proof. Consider the set of all real imbeddings $\sigma_i : K_0 \hookrightarrow \mathbb{R}$ for $i = 1, 2, \ldots, r_1$ and the set of non-conjugate complex imbeddings $\sigma_{r_1+j} : K_0 \hookrightarrow \mathbb{C}$, $j = 1, 2, \ldots, r_2$ (so $r_1 + 2r_2 = \deg K_0/\mathbb{Q}$). We want to show that $r_2 = 0$. Anyway, we have an isomorphism of algebras

$$K_0 \otimes \mathbb{R} \simeq \mathbb{R} \times \cdots \times \mathbb{R} \times \mathbb{C} \times \cdots \times \mathbb{C}.$$

The trace is just the sum of the real parts and the sum of the real parts of the complex pieces. We know that $\mathrm{Tr}_{K_0/\mathbb{Q}}(x^2) > 0$ for $x \in \mathbb{Q}$ (by positivity and the fact that $'$ fixes K_0) and we get a form $q(x) = \mathrm{Tr}_{K_0/\mathbb{Q}}(x^2)$ on $K_0 \otimes \mathbb{R}$ which is positive semidefinite. But it's also nondegenerate over $\mathbb{Q}$, hence nondegenerate over $\mathbb{R}$. This means that in fact, $q_{\mathbb{R}}$ is positive definite. But this implies that there can't be any complex parts.

So, if $K = K_0$ there's nothing to prove. Anyway, $[K : K_0] = 2$ so we have a quadratic extension $K_0(\sqrt{\alpha})$. We have to see that it is totally imaginary. We have to show that $\sigma_i(\alpha) < 0$ for all i, which will do it. Let's write $K \otimes \mathbb{R}$ as as $\prod_{\sigma_i} K \otimes_{K_0} \mathbb{R}$. Each of the factors is either $\mathbb{R} \times \mathbb{R}$ or $\mathbb{C}$ and the involution is either conjugation or flipping factors. Using the positivity condition, one finds that $\mathbb{R}$ can't happen. ▲