Abelian Varieties

Lectures delivered by Sug Woo Shin
Notes by Holden Lee

Fall 2012, MIT

Last updated Tue. 12/11/12

Contents

Introduction

Sug Woo Shin taught a course (18.787) on Abelian Varieties at MIT in Fall 2012. These are my "live-TEXed" notes from the course. The template is borrowed from Akhil Mathew.

Please email corrections to holden1@mit.edu.

Lecture 1
Thu. 9/6/12

Course website: `http://math.mit.edu/~swshin/Fall12-18787`

§1 Overview

In this course, we will cover abelian varieties and p-divisible groups, also known as Barsotti-Tate groups. We first build some basic knowledge and apply it to some interesting problems in number theory. Our main reference is Abelian Varieties, by Mumford. We will

1. *classify* abelian varieties over finite fields $\mathbb{F}_p$ and algebraic closures of finite fields $\overline{\mathbb{F}_p}$ (Honda-Tate Theory). We will also classify p-divisible groups up to isogeny (Dieudonné, Manin).

   With some more work, we can get classification up to isomorphism.

   Studying a variety over finite fields helps us understand abelian varieties over global fields, because when we study a global problem, one way to get information is to reduce modulo a prime and study over the variety over the special fiber.

2. go from characteristic p ($\mathbb{F}_p$) to characteristic 0 (e.g. $\mathbb{Q}_p$) using *deformations*.[1]

   - The Serre-Tate Theorem will tell us that deformations of abelian varieties are basically deformations of p-divisible groups.
   - The theory of Grothendieck-Messing will reduce deformations of p-divisible groups to some linear algebra.

To understand abelian varieties and p-divisible groups, we first need to understand group schemes. An abelian variety is a special type of group scheme, while a p-divisible group is an inductive limit of group schemes.

§2 Review: Yoneda Lemma and T-valued points

This is not part of the lecture. I include this section as a reference.

2.1 The Yoneda Lemma

Lemma 1.1 (Yoneda Lemma)**:** lem:yoneda Let $\mathcal{C}$ be a locally small category. Let h_A denote the functor $\mathrm{Hom}(\bullet, A) : \mathcal{C} \to (\mathrm{Sets})$ and h^A denote the contravariant functor $\mathrm{Hom}(A, \bullet)$ (i.e. it is a functor $\mathcal{C}^{\mathrm{op}} \to (\mathrm{Sets})$).

[1] Note: we ran out of time to actually cover this.

1. (Covariant version) Let F be functor from $\mathcal{C}$ to (Sets). As functors $(\text{Set})^{\mathcal{C}} \times \mathcal{C} \to (\text{Set})$, we have $\text{Nat}(h^A, F) \cong F(A)$. ($F$ is in $(\text{Set})^{\mathcal{C}}$, A is in $\mathcal{C}$, and $\text{Nat}(h^A, F) \cong F(A)$ is a set.)

2. (Contravariant version) Let F be a contravariant functor from $\mathcal{C}$ to (Sets). As functors $(\text{Set})^{\mathcal{C}^{\text{op}}} \times \mathcal{C} \to (\text{Set})$, we have $\text{Nat}(h_A, F) \cong F(A)$.

Corollary 1.2 (Yoneda Embedding)**:** cor:yoneda

1. The embedding $h^\bullet : \mathcal{C}^{\text{op}} \to (\text{Set})^{\mathcal{C}}$ given by sending $A \mapsto h^A = \text{Hom}_{\mathcal{C}}(A, \bullet)$ is fully faithful. (The morphism $f : A \to B$ gets sent to $f \circ \bullet$.)

2. The embedding $h_\bullet : \mathcal{C} \to (\text{Set})^{\mathcal{C}^{\text{op}}}$ given by sending $A \mapsto h_A = \text{Hom}_{\mathcal{C}}(\bullet, A)$ is fully faithful. (The morphism $f : A \to B$ gets sent to $\bullet \circ f$.)

Remark:
- A category is **locally small** if homomorphisms between any two objects form a set.
- $(\text{Set})^{\mathcal{C}^{\text{op}}}$ is the category of *contravariant functors* $\mathcal{C} \to (\text{Set})$.
- $\text{Hom}(A, B)$ has just the structure of a set.
- $\text{Nat}(G, F)$ denotes the set of natural transformations between G and F.
- A functor Φ is **fully faithful** if $\Phi_{A,B} : \text{Hom}(A, B) \to \text{Hom}(\Phi(A), \Phi(B))$ is bijective for any objects A and B. This basically means that Φ embeds the first category into the second, and there aren't any "extra" maps between embedded objects that are present in B but not A.
- We say a functor $F : \mathcal{C} \to (\text{Set})$ is **representable** if $F \cong h^A$ for some A (and ditto for the contravariant case).

Proof of Corollary 1.1. We show (2) of the lemma implies (2) of the corollary; (1) is entirely analogous. Set $F = h_B$ to get

$$\text{Nat}(h_A, h_B) \cong h_B(A).$$

Now a natural transformation is just a morphism in the functor category, so $\text{Nat}(h_A, h_B) = \text{Hom}_{(\text{Set})^{\mathcal{C}^{\text{op}}}}(h_A, h_B)$, and by definition $h_B(A) = \text{Hom}(A, B)$, so we get

$$\text{Hom}_{(\text{Set})^{\mathcal{C}^{\text{op}}}}(h_A, h_B) \cong \text{Hom}(A, B).$$

This is exactly the condition to be fully faithful. □

One way to think of this is that an object is determined by how other objects map into it.[2]

[2] As mentioned here `http://mathoverflow.net/questions/3184/philosophical-meaning-of-the-yoneda-lemma/3223#3223`, if one thinks of objects of a category as particles and morphisms as ways to smash one particle into another particle, then the Yoneda lemma says that it is possible to determine the identity of a particle by smashing other particles into it.

2.2 T-valued points

Definition 1.3: Let X and T be objects in a locally small category. Define the set of **T-valued points** of X to be

$$T(X) := \mathrm{Hom}(T, X).$$

In many cases we can think of "T-valued points" as a generalization of "points" of X. For example, suppose T is a singleton set $\{\cdot\}$ and X is a set, then a T-valued point is just a point of X.

The main application to algebraic geometry can be seen through the following example.

Example 1.4: ex:T-points Let R be an integral domain and V a variety over R. Let $T = \mathrm{Spec}(R)$ and X be the scheme corresponding to V. Then the T-points of X are exactly the points of V.

To see this, it's sufficient just to consider the affine case. Suppose $V \in R^n$ is defined by $f_1, \ldots, f_m$. By Lemma 1.5, to give a morphism

$$T = \mathrm{Spec}(R) \to X = \mathrm{Spec}\left(\frac{R[x_1, \ldots, x_n]}{(f_1, \ldots, f_m)}\right)$$

is the same as giving a R-algebra homomorphism

$$\frac{R[x_1, \ldots, x_n]}{(f_1, \ldots, f_m)} \to R,$$

which is just an assignment

$$(x_1, \ldots, x_n) \mapsto (a_1, \ldots, a_n) \text{ such that } f_i(x_1, \ldots, x_n) = 0 \text{ for some } i,$$

i.e. a point of V.

Lemma 1.5 (cf. Hartshorne, II, Exercise 2.4)**:** lem:spec-fff Let R be a ring. Then Spec is a fully faithful contravariant functor from the category of R-algebras to schemes over $\mathrm{Spec}(R)$.

Example 1.4 is the most intuitive example. However, the power of the viewpoint of $X(T)$ is that we can consider more generalized points. For instance, letting R be a field k,

- a $\mathrm{Spec}(k[t])$ point is a one-parameter family of k-points, and
- a $\mathrm{Spec}\left(\frac{k[t]}{(t^2)}\right)$ point is a k-point with a Zariski tangent vector.

The Yoneda Embedding tells us that we can identify a scheme X with the **functor of points** $h_X(\bullet) = X(\bullet)$—i.e. with $X(T)$, the T-points of X, as T ranges over all schemes—without losing any information. A functor $X \to Y$ becomes a natural transformation $h_X = X(\bullet) \to h_Y = Y(\bullet)$, i.e. maps of sets $X(T) \to Y(T)$ for each T, that are functorial over T.

§3 Group schemes

3.1 Definition of group schemes

We will define group schemes over a fixed scheme S.

Definition 1.6: Let S be a scheme. Define (Sch/S), the category of **S-schemes**, as follows.

- The objects are schemes T with a structure map to S, $\begin{array}{c} T \\ \downarrow \\ S \end{array}$.
- The morphisms are

$$\mathrm{Hom}\left(\begin{array}{cc} T & T' \\ \downarrow f, & \downarrow f' \\ S & S \end{array}\right) = \left\{ g : \begin{array}{ccc} T & \xrightarrow{\quad g \quad} & T' \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f'} & \\ & S & \end{array} \quad \text{commutes} \right\}$$

  called S-morphisms.

For short we'll write $\mathrm{Hom}_S(T, T')$, the maps f, f' being implicit.

We now apply the philosophy of the previous section: to study X we study $h_X = X(\bullet)$. If $X \in (\mathrm{Sch}/S)$ we get canonically

$$\begin{aligned} h_X : (\mathrm{Sch}/S) &\to (\mathrm{Sets}) \\ T &\mapsto \mathrm{Hom}_S(T, X). \end{aligned}$$

Since T and X are S-schemes, we define the T-points of X to be $X(T) := \mathrm{Hom}_S(T, X)$. The functor h_X sends

$$(T \xrightarrow{f} T') \mapsto (\mathrm{Hom}_S(T, X) \xleftarrow{h_X(f) = \bullet \circ f} \mathrm{Hom}_S(T', X)).$$

The Yoneda Embedding 1.2 tells us that $h_\bullet$ is a fully faithful contravariant functor

$$\begin{aligned} h_\bullet : (\mathrm{Sch}/S) &\to \mathrm{Fun}^{\mathrm{op}}((\mathrm{Sch}/S), (\mathrm{Sets})) = (\mathrm{Sets})^{(\mathrm{Sch}/S)^{\mathrm{op}}} \\ X &\mapsto h_X. \end{aligned}$$

We say $h \in \mathrm{Fun}^{\mathrm{op}}((\mathrm{Sch}/S), (\mathrm{Sets}))$ is **representable** (by the scheme X) if $h \cong h_X$.

We have several equivalent definitions for a group scheme. The Yoneda Embedding gives the equivalence of the 2nd and 3rd definitions.

Definition 1.7: A **group scheme** G over S' any of the following three equivalent objects.

1. a group object in (Sch/S), i.e. it is $(G, \widetilde{h_G})$ where $G \in (\mathrm{Sch}/S)$ and the following commutes:

$$\begin{array}{ccc} (\mathrm{Sch}/S) & \xrightarrow{\widetilde{h_G}} & (\mathrm{Gps}) \\ & {\scriptstyle h_G} \searrow \quad \swarrow {\scriptstyle \text{forgetful}} & \\ & (\mathrm{Set}) & \end{array}$$

2. (G, h_G) equipped with the following maps of sets

   - e_T (identity): $\{\cdot\} \to G(T)$
   - i_T (inverse): $G(T) \to G(T)$
   - m_T (multiplication): $G(T) \times G(T) \to G(T)$.

   such that $G(T)$ is a *group* under these operations, namely,

   (a) (Associativity) The following commutes:

$$\begin{array}{ccc} G(T) \times G(T) \times G(T) & \xrightarrow{(m_T, \mathrm{id})} & G(T) \times G(T) \\ \downarrow{\scriptstyle (\mathrm{id}, m_T)} & & \downarrow{\scriptstyle m_T} \\ G(T) \times G(T) & \xrightarrow[m_T]{} & G(T). \end{array}$$

   Note: This represents associativity because going clockwise we get $(xy)z$ and going counterclockwise we get $x(yz)$.

   (b) (Inverse)

$$\begin{array}{ccccc} & & G(T) \times G(T) & & \\ & {\scriptstyle (\mathrm{id}, i_T)} \nearrow & & \searrow {\scriptstyle m_T} & \\ G(T) & \xrightarrow{\text{structure}} & G(S) & \xrightarrow{e_T} & G(T) \\ & {\scriptstyle (i_T, \mathrm{id})} \searrow & & \nearrow {\scriptstyle m_T} & \\ & & G(T) \times G(T) & & \end{array}$$

   Note: The top, middle, and bottom give xx^{-1}, e, and $x^{-1}x$, respectively, so commutativity gives $xx^{-1} = e = x^{-1}x$.

   (c) (Identity) Let $e'_T : G(T) \to G(T)$ be the composition of the structure map with $e : G(S) \to G(T)$.

$$\begin{array}{ccccc} & & G(T) \times G(T) & & \\ & {\scriptstyle (\mathrm{id}, e'_T)} \nearrow & & \searrow {\scriptstyle m_T} & \\ G(T) & & \xrightarrow{\mathrm{id}} & & G(T) \\ & {\scriptstyle (e'_T, \mathrm{id})} \searrow & & \nearrow {\scriptstyle m_T} & \\ & & G(T) \times G(T) & & \end{array}$$

Note: This gives $x \cdot e = x = e \cdot x$.

and these group operations are *functorial*, namely for all $T \xrightarrow{f} T'$ in (Sch/S),

- $$\begin{array}{ccc} \{\cdot\} & \xrightarrow{e_T} & G(T) \\ & \searrow^{e_{T'}} & \uparrow{\scriptstyle h_G(f)} \\ & & G(T') \end{array}$$
- $$\begin{array}{ccc} G(T) & \xrightarrow{i_T} & G(T) \\ {\scriptstyle h_G(f)}\uparrow & & \uparrow{\scriptstyle h_G(f)} \\ G(T') & \xrightarrow{i_{T'}} & G(T') \end{array}$$
- $$\begin{array}{ccc} G(T) \times G(T) & \xrightarrow{i_T} & G(T) \\ {\scriptstyle h_G(f)}\uparrow & & \uparrow{\scriptstyle h_G(f)} \\ G(T') \times G(T') & \xrightarrow{i_{T'}} & G(T') \end{array}$$

3. (G, e, i, m) where $G \in (\mathrm{Sch}/S)$,

$$\begin{aligned} e &: S \to G \\ i &: G \to G \\ m &: G \times G \to G \end{aligned}$$

and we have the analogues of the group laws in the 2nd definition, but with fiber product instead of product and with e, i, m instead of e_T, i_T, m_T.

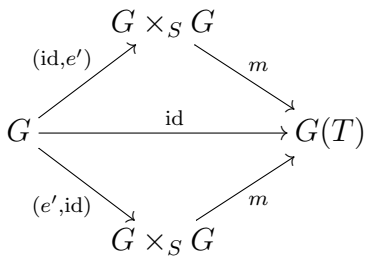
(a) (Associativity)

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{(m,\mathrm{id})} & G \times_S G \\ \downarrow{\scriptstyle (\mathrm{id},m)} & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow[m]{} & G. \end{array}$$

(b) (Inverse)

$$\begin{array}{ccccc} & & G \times_S G & & \\ & \overset{(\mathrm{id},i)}{\nearrow} & & \overset{m}{\searrow} & \\ G & \xrightarrow{\text{structure}} & S & \xrightarrow{e} & G \\ & \underset{(i,\mathrm{id})}{\searrow} & & \underset{m}{\nearrow} & \\ & & G \times_S G & & \end{array}$$

(c) (Identity) Let $e' : G \to G$ be the composition of the structure map with $e : S \to G$.



Proof of equivalence. The 1st and 2nd definition are equivalent: In the 2nd definition, the first set of conditions simply say $G(T)$ is a group, and the second set of conditions say that $\widetilde{h_G}$ is a functor; i.e. it sends the scheme morphism f to a group homomorphism $\widetilde{h_G}(f)$.

The 2nd and 3rd definitions are equivalent: We go between G to $G(T)$ by the Yoneda embedding, and between i, e, m and i_T, e_T, m_T by

- $i_T(f) = (h_T(f))(i) = i \circ f$.
- $m_T(f, g) = (h_T(f \times_T g))(m) = m \circ (f \times_S g)$.
- $e_T(f) = (h_T(f))(e) = e \circ f$.

□

The 3rd definition is the scheme viewpoint, and the 2nd definition is the functor of points viewpoint. In the following examples, we'll see how to switch between these viewpoints.

3.2 Examples of group schemes

Let $G = \operatorname{Spec} A$ and $S = \operatorname{Spec} R$. Suppose A is an R-algebra, so there is a natural structure map $G \to S$. We have by Lemma 1.5 that Spec is a contravariant fully faithful functor from (R-algebras) to (Sch/ $\operatorname{Spec} R$):

$$\begin{array}{ccc} (\text{rings}) & \xrightarrow{\text{Spec}} & (\text{Sch}) \\ \uparrow & & \uparrow \\ (R\text{-algebras}) & \xrightarrow[\text{Spec}]{\text{f.f.}} & (\text{Sch}/\operatorname{Spec} R) \end{array}$$

(Note the categories on the bottom are not full subcategories of the top.) As Lemma 1.5 says, S-morphisms between schemes over $\operatorname{Spec} R$ are nothing but R-algebra homomorphisms in the opposite direction, so we can be more concrete. So giving $G = \operatorname{Spec} A$ a group scheme structure, i.e. giving e, i, m for G, amounts to giving R-algebra maps (note $\operatorname{Spec}(A \otimes_R A) = \operatorname{Spec} A \times_{\operatorname{Spec} R} \operatorname{Spec} A$)

$$\begin{aligned} e &: A \to R \\ i &: A \to A \\ m &: A \to A \otimes_R A. \end{aligned}$$

such that R-algebra version of (a), (b), and (c) hold. (Just invert all the arrows in (a), (b), and (c), and replace the rings with schemes. A satisfying these axioms is called a **Hopf algebra**.)

We can give some common, concrete examples of group varieties.

Example 1.8: Define the additive group scheme $\mathbb{G}_{a,\operatorname{Spec} R}$ as follows. (First we consider the 3rd definition.) Let $A = R[t]$ and let $\mathbb{G}_{a,\operatorname{Spec} R} = \operatorname{Spec} A$ be the scheme with e, i, and m induced by the R-algebra homomorphisms

$$\begin{aligned} e &: R[t] \to R & f &\mapsto f(0) \\ i &: R[t] \to R[t] & f &\mapsto f(-t) \\ m &: R[t] \to R[t'] \otimes_R R[t''] \cong R[t', t''] & f &\mapsto f(t' + t'') \end{aligned}$$

(We abuse notation and let e, i, m denote these maps and the corresponding morphisms on schemes.)

Now we show that

$$\mathbb{G}_{a,\operatorname{Spec} R}(\operatorname{Spec} R') = (R', +) \text{ for any } R\text{-algebra } R'.$$

To see this, let $T = \operatorname{Spec} R'$, and note that

1. As a set, $\mathbb{G}_{a,\operatorname{Spec} R}(\operatorname{Spec} R')$ is the set of $\operatorname{Spec}(R)$-morphisms $\operatorname{Spec}(R') \to \operatorname{Spec}(R[t])$, i.e. the set of R-algebra homomorphisms $f : R[t] \to R'$. These homomorphisms are bjiection with the elements of R', by the map $f \mapsto f(t)$.

2. To find the group structure, note that $m_T(f, g) = m \circ (f \times_S g)$. Suppose $f \in \mathbb{G}_{a,\operatorname{Spec} R}(T)$ corresponds to the point a and $g \in \mathbb{G}_{a,\operatorname{Spec} R}(T)$ corresponds to the point b. Then

$$\begin{array}{lcc} & f : \operatorname{Spec}(R') \to \operatorname{Spec}(R[t]) & g : \operatorname{Spec}(R') \to \operatorname{Spec}(R[t]) \\ \text{correspond to} & R' \leftarrow R[t] & R' \leftarrow R[t] \\ & a \leftarrow\!\shortmid\, t & b \leftarrow\!\shortmid\, t. \end{array}$$

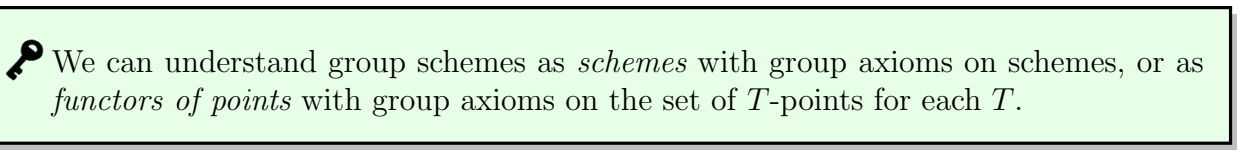
and we have

$$m \circ (f \times_{\operatorname{Spec} R} g) : \operatorname{Spec} R' \xrightarrow{f \times_{\operatorname{Spec} R} g} \operatorname{Spec} R[t'] \otimes R[t''] = \operatorname{Spec} R[t'] \times_{\operatorname{Spec} R} \operatorname{Spec} R[t''] \xrightarrow{m} \operatorname{Spec} R[t]$$

corresponds to

$$\begin{array}{ccccc} R' & \longleftarrow & R[t'] \otimes_R R[t''] & \xleftarrow{m} & R[t] \\ & & t' + t'' & \longleftarrow\!\shortmid & t \\ a & \longleftarrow\!\shortmid & t' & & \\ b & \longleftarrow\!\shortmid & t'' & & \\ a + b & \longleftarrow\!\shortmid & & & t \end{array}$$

The example shows the power of the "functor of points" perspective of group schemes. We don't need to view $(R', +)$ as a different scheme for each R'. Instead we can realize that they come from the same gadget $\mathbb{G}_{a,\operatorname{Spec} R}(\bullet)$—the functor of points associated to the scheme $\mathbb{G}_{a,\operatorname{Spec} R}$.


We can understand group schemes as *schemes* with group axioms on schemes, or as *functors of points* with group axioms on the set of T-points for each T.

Example 1.9: Define the multiplicative group scheme $\mathbb{G}_{m,\operatorname{Spec} R}$ as follows. Let $A = R[t, t^{-1}]$; let $\mathbb{G}_{m,\operatorname{Spec} R}$ be the scheme with e, i, m induced by the R-algebra homomorphisms

$$\begin{aligned} e &: f \mapsto f(1) \\ i &: f \mapsto f(t^{-1}) \\ m &: f \mapsto f(t't''). \end{aligned}$$

(Note 1 is the multiplicative identity so we look at $f(1)$ not $f(0)$.)

We similarly get

$$\mathbb{G}_{m,\operatorname{Spec} R}(\operatorname{Spec} R') = (R'^{\times}, \cdot).$$

(When we consider $\operatorname{Spec} R' \to \operatorname{Spec} R[t, t^{-1}]$, i.e. maps $R[t, t^{-1}] \to R'$, the image of t must be an invertible element.)

Remark: For any ring R, $\mathbb{G}_{a,\operatorname{Spec} R} \cong \mathbb{G}_{a,\operatorname{Spec} \mathbb{Z}} \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} R$, by defining an isomorphism on the level of points. The same is true for $\mathbb{G}_{m,\operatorname{Spec} R}$.

Example 1.10: To define the additive and multiplicative group schemes for general S, we need to use relative Spec.

$$\begin{aligned} \mathbb{G}_{a,S} &:= \underline{\operatorname{Spec}}(\mathscr{O}_S[t]) \\ \mathbb{G}_{m,S} &:= \underline{\operatorname{Spec}}(\mathscr{O}_S[t, t^{-1}]). \end{aligned}$$

with e, i, and m defined similarly. (See `http://en.wikipedia.org/wiki/Spectrum_of_a_ring#Global_Spec` for review on relative spec. Basically, if $S = \bigcup_i \operatorname{Spec}(A_i)$, then $\underline{\operatorname{Spec}}(\mathscr{O}_S[t]) := \bigcup_i \operatorname{Spec}(A_i[t])$, glued in the natural way.) Generalizing the affine case, we have that the T-points are just global sections and invertible global sections, respectively:

$$\begin{aligned} \mathbb{G}_{a,S}(T) &= \mathscr{O}_T(T) \\ \mathbb{G}_{m,S}(T) &= \mathscr{O}_T(T)^{\times}. \end{aligned}$$

Define

$$\mathrm{GL}_{n,S} := \underline{\operatorname{Spec}}(\mathscr{O}_S[\{x_{ij} : 1 \le i, j \le n\}, y]/(\det(x_{ij})y - 1))$$

so that

$$\mathrm{GL}_{n,S}(T) = \mathrm{GL}_n(\mathscr{O}_T(T)) = M_n(\mathscr{O}_T(T))^{\times}$$

Taking $n = 1$, we recover the multiplicative group scheme: $\mathrm{GL}_{1,S} = \mathbb{G}_{m,S}$.

Problem 1.1: Show that $\mathbb{G}_{a,S}(T) = \mathscr{O}_T(T)$, $\mathbb{G}_{m,S}(T) = \mathscr{O}_T(T)^\times$, and $\mathrm{GL}_{n,S}(T) = \mathrm{GL}_n(\mathscr{O}_T(T))$. We showed this when S and T are affine; glue to get the general case.

Example 1.11: Define

$$\mu_{n,S} = \underline{\mathrm{Spec}}\mathscr{O}_S[t]/(t^n - 1).$$

Here e, i, m are the same as for $\mathbb{G}_{m,S}$. Alternatively,

$$\mu_{n,S}(T) = \{x \in \mathscr{O}_T(T) : x^n = 1\}.$$

(The image of t should satisfy $t^n = 1$.)

Example 1.12: Define the constant group scheme as follows: let H be a group. Define

$$\underline{H}(T) = \mathrm{Hom}(\pi_0(T), H) = \mathrm{Hom}_{\mathrm{cont}}(T, H)$$

where $\pi_0(T)$ denotes the connected components of T and H is given the discrete topology in the last expression. Note $T \to T'$ gives a map $\underline{H}(T') \to \underline{H}(T)$.

$\underline{H}$ is a group scheme as the given functor of points is represented as follows. Let S_h be copies of S; we have

$$\underline{H} = \coprod_{h \in H} S_h.$$

The multiplication map is $\coprod_{h\in H} S_h \times_S \coprod_{h'\in H} S_{h'} \to \coprod_{h''\in H} S_{h''}$ induced by the natural maps $S_h \times_S S_{h'} \to S_{hh'}$ (induced by the identity map).

Example 1.13: Let Γ be an abstract commutative group, and

$$G = \underline{\mathrm{Spec}} \underbrace{\mathscr{O}_S[\Gamma]}_{\text{group algebra}}.$$

(If S is an affine scheme, we just get the group algebra.) Here

$$\mathscr{O}_S[\Gamma] = \bigoplus_{\gamma \in \Gamma} \mathscr{O}_S \cdot \gamma.$$

Define

$$\begin{aligned} e &: \mathscr{O}_S[\Gamma] \to \mathscr{O}_S & \gamma &\mapsto 1 \\ i &: \mathscr{O}_S[\Gamma] \to \mathscr{O}_S[\Gamma] & \gamma &\mapsto \gamma^{-1} \\ i &: \mathscr{O}_S[\Gamma] \to \mathscr{O}_S[\Gamma] \otimes \mathscr{O}_S[\Gamma] & \gamma &\mapsto \gamma \otimes \gamma. \end{aligned}$$

Problem 1.2: Check that this is a group scheme.
Check that if $\Gamma = \mathbb{Z}/n\mathbb{Z}$ we get μ_n, and if $\Gamma = \mathbb{Z}$ we get $\mathbb{G}_m$.

3.3 Morphisms between group scheme

The natural next step is to define a notion of morphisms between group schemes. As we've said, the objects of (Gp/S) to be the group schemes over S. The morphisms are

$$\begin{aligned}
&\mathrm{Hom}_{(\mathrm{Gp}/S)}(G, G') \\
&:= \mathrm{Hom}(\widetilde{h_G}, \widetilde{h_{G'}}) \text{ in } \mathrm{Fun}((\mathrm{Sch}/S), (\mathrm{Gp})) \\
&= \left\{ \begin{array}{ccc} G & \longrightarrow & G' \\ & \searrow \quad \swarrow & \\ & S & \end{array} \quad : G(T) \to G'(T) \text{ is a group homomorphism, for every } T \in (\mathrm{Sch}/S) \right\}
\end{aligned}$$

Definition 1.14: A **subgroup scheme** is a subscheme $H \subseteq G$ such that $H(T) \subseteq G(T)$ (subgroup) for all $T \in (\mathrm{Sch}/S)$. Equivalently, a subgroup scheme is (H, e_H, i_H, m_H) such that $H \subseteq G$, and the following commute:

$$\begin{array}{ccc} S & \xrightarrow{e_H} & H \\ & \searrow^{e_G} & \downarrow \\ & & G \end{array} \qquad \begin{array}{ccc} H & \xrightarrow{i_H} & H \\ \downarrow & & \downarrow \\ G & \xrightarrow{i_G} & G. \end{array} \qquad \begin{array}{ccc} H \times H & \xrightarrow{m_H} & H \\ \downarrow & & \downarrow \\ G \times G & \xrightarrow{m_G} & G. \end{array}$$

We want to define kernels and cokernels. Cokernels are more difficult; let's do kernels first.

Definition 1.15: Let $G \xrightarrow{f} H$ be in (Gp/S). Define the kernel K/S to be the functor $K(\bullet)$ such that

$$K(T) = \ker(G(T) \xrightarrow{f(T)} H(T))$$

for all T/S.

Proof of well-definedness. It's not obvious that this functor is represented by a scheme! So let's call the functor $F(T) := \ker(G(T) \xrightarrow{f(T)} H(T))$ for now; we have to show there exists a scheme K such that $K(T) = F(T)$, i.e. we need to show F is represented by a scheme K. We do this by constructing K. Define $K := G \times_H S$, so we have the following diagram.

$$\begin{array}{ccc} K & \longrightarrow & G \\ \downarrow & & \downarrow f \\ S & \xrightarrow{e_H} & H \end{array} \qquad \begin{array}{ccc} T & & \\ & \searrow & \\ & & K \longrightarrow G \\ & & \downarrow \quad \downarrow f \\ & & S \xrightarrow{e_H} H \end{array}$$

Now take T-points and check that

$$K(T) = G(T) \times_{H(T)} S(T) = \left\{ g \in G(T) : f(g) = 1_{H(T)} \right\} = \ker f(T).$$

The first equality is from definition of the fiber product (Here, $\times_{H(T)}$ denotes the set-theoretic pullback). $\square$

Quotients are hard; we'll get to them later.

Lecture 2
Tue. 9/11/12

Last time we introduced group schemes. Let S be a scheme; then $(\mathrm{Gp}/S) \subseteq (\mathrm{Sch}/S)$ (but it is not a full subscheme). For $\varphi : H \to G$ in (Gp/S) we defined $\ker \varphi$ by

$$(\ker \varphi)(T) = \ker(\varphi(T) : H(T) \to G(T)).$$

and saw it was representable. What is the cokernel $\operatorname{coker} \varphi$ (when the image of φ is a normal group)? The naive idea is to find $Q \in (\mathrm{Sch}/S)$ such that

$$Q(T) = \operatorname{coker}(\varphi(T) : H(T) \to G(T)).$$

However this doesn't quite work. For example, consider the multiplication-by-n map

$$\begin{aligned} [n] : \mathbb{G}_m &\to \mathbb{G}_m \\ g &\mapsto g^n \end{aligned}$$

Think of this as ($\mathbb{G}_m$ appears n times)

$$\begin{array}{ccc} \mathbb{G}_m & \xrightarrow{\text{diagonal}} & \mathbb{G}_m \times \cdots \times \mathbb{G}_m \\ & \searrow^{[n]} & \downarrow \\ & & \mathbb{G}_m. \end{array}$$

We write $Q(K)$ as short for $Q(\operatorname{Spec} K)$. Now $Q(\operatorname{Spec}(\mathbb{Q})) = \mathbb{Q}^\times/(\mathbb{Q}^\times)^n$, and this is not contained in $Q(\operatorname{Spec}(\overline{\mathbb{Q}})) = \{1\}$. However, if Q were a scheme, when we pass to a larger field, we should get more points! (Since $\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}$, we have $\operatorname{Spec}(\overline{\mathbb{Q}}) \hookrightarrow \operatorname{Spec}(\mathbb{Q})$, and hence $Q(\mathbb{Q}) \hookrightarrow Q(\overline{\mathbb{Q}})$.)

There doesn't exist such a scheme Q, in other words, the functor $Q(\bullet)$ is not representable.

Today we'll talk about quotients, and see how to remedy this problem. There are three ways.

1. Take *categorical quotients*.
2. Take *geometric quotients* (geometric invariant theory).
3. Take the *fppf quotient*. We enlarge the category of schemes to fppf sheaves, and try to solve the problem there. Sheafify in the fppf topology and hope it's represented by a scheme.

Or we could enlarge the category to stacks...

Recall that taking the quotient of sheaves was subtle, too; we had have to sheafify. Something similar is at play here.

We follow [7, §4].

§1 Group scheme actions

It is actually no harder to study a group scheme action

$$G \circlearrowright X$$

where G is a group scheme over S and X is a scheme over S. If you're Grothendieck, then you can study something even more general, the quotient by any kind of equivalence relation (we won't cover this). Specializing to the left or right action of a subgroup scheme on a group scheme,

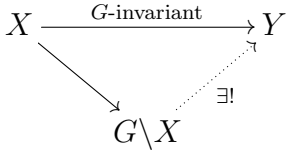
$$H \circlearrowright G$$

where $H \subseteq G$ in (Gp/S), we get quotient group schemes.

The idea for 1 (categorical quotients) and 2 (geometric quotients) is as follows. Consider the analogous case where a group G acts on a topological space X:

$$G \circlearrowright X.$$

1. The quotient space is the space $G\backslash X$ such that for any space Y and G-invariant map $X \to Y$ there exists a unique continuous map making the diagram commute.



2. Define $G\backslash X$ as a topological space to be $X/\sim$ where $x \sim gx$ for every $g \in G$, with the quotient topology. The topology is such that the continuous functions on $C(G\backslash X)$ are exactly those that come from G-invariant continuous functions on X.

$$C(G\backslash X) = C(X)^G$$

Taking categorical quotients is akin to 1; taking geometric quotients is akin to 2.

1.1 Group action on schemes

Definition 2.1: Let $G \in (\mathrm{Gp}/S)$ and $X \in (\mathrm{Sch}/S)$. A (left) action of X is one of the two equivalent things:

1. For every $T \in (\mathrm{Sch}/S)$, a map

$$G(T) \times X(T) \to X(T)$$

that is a group action, and that is functorial in T.

2. a morphism $\mu : G \times_S X \to X$ such that the following composition is the identity

$$X = S \times_S X \xrightarrow{(e,\mathrm{id}_X)} G \times_S X \xrightarrow{\mu} X$$
$$\mathrm{id}_X$$

and

$$\begin{array}{ccc} G \times_S G \times_S X & \xrightarrow{(m,\mathrm{id}_X)} & G \times_S X \\ {\scriptstyle (\mathrm{id}_G,\mu)}\downarrow & & \downarrow{\scriptstyle \mu} \\ G \times_S X & \xrightarrow{\mu} & X \end{array}$$

(This says $g_1(g_2x) = (g_1g_2)x$.)

Again, the equivalence holds by the Yoneda Embedding. In the first action, when we say $G(T) \times X(T) \to X(T)$ is a group action, we mean that an analogous diagram to the diagram in the 2nd definition holds (with $G(T)$ and $X(T)$ instead of G and T).

Definition 2.2: Given a group action on a scheme $G \circlearrowright X$, we say that a map $X \to Y$ in (Sch/S) is G**-invariant** if one of the following equivalent conditions hold.

1. $G(T) \circlearrowright X(T) \to Y(T)$ is $G(T)$-invariant for all T (i.e. $f(x) = f(gx)$).

2. The following diagram commutes. (p_i is the projection to the ith component.)

$$\begin{array}{ccccc} & & X & & \\ & {\scriptstyle p_2}\nearrow & & \searrow{\scriptstyle f} & \\ G \times_S X & & & & Y \\ & {\scriptstyle \mu}\searrow & & \nearrow{\scriptstyle f} & \\ & & X & & \end{array}$$

i.e. $f \circ p_2 = f \circ \mu$.

§2 Categorical quotient

We can now define a categorical quotient of X by G.

Definition 2.3: A **categorical quotient** of X by G is $(Y, X \xrightarrow{\pi} Y)$ such that for any G-invariant map $X \to Y'$, there exists a unique dotted morphism making the following commute.

$$\begin{array}{ccc} X & \xrightarrow{G\text{-invariant}} & Y' \\ & {\scriptstyle \pi}\searrow & \nearrow{\scriptstyle \exists!} \\ & Y & \end{array}$$

In other words,

$$\mathrm{Hom}_{(\mathrm{Sch}/S)}(Y, Y') = \ker(\ \mathrm{Hom}(X, Y') \underset{\mu^*}{\overset{p_2^*}{\rightrightarrows}} \mathrm{Hom}(G, Y') \times \mathrm{Hom}(X, Y')\ )$$
$$f \mapsto f \circ \pi.$$

By ker we actually mean the universal equalizer, so the RHS is the set of functions g satisfying $p_2 \circ g = \mu \circ g$. We have $p_2 \circ (f \circ \pi) = \mu \circ (f \circ \pi)$. The uniqueness and existence of f making the diagram commute says that the map is a bijection.

This is a flexible definition, because we can do the same in other categories. We work within any given category without enlarging it. Because of this, this approach also has its limitations.

We choose the best object to be the quotient, in the category of schemes. This quotient may or may not have the nice properties we may want.

We revisit our example.

Example 2.4: We have

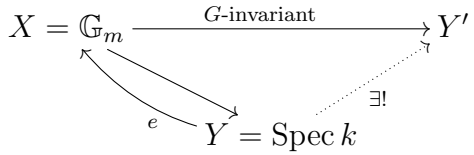
$$\mu : \mathbb{G}_m \times_S \mathbb{G}_m \to \mathbb{G}_m$$
$$(g, x) \mapsto g^n x$$

For simplicity we take $S = \operatorname{Spec} k$ where k is a field. We can show that $(\operatorname{Spec} k, \mathbb{G}_m \xrightarrow{\text{trivial}} \operatorname{Spec} k)$ is the categorical quotient of $\mathbb{G}_m$ by $\mathbb{G}_m$ under this action. Then for any T,

$$[\mathrm{coker}(\mathbb{G}_m \xrightarrow{[n]} \mathbb{G}_m)](T) = \{1\}.$$

We expect this—as $\mathbb{G}_m \xrightarrow{[n]} \mathbb{G}_m$ is surjective over an algebraically closed field (captured in our fake definition where the quotient had a single point over an algebraically closed field), we suspect that the quotient should just be a point over *any* field and actually any scheme.

Observe that given a G-invariant map $X \to Y'$, the unique map $Y \to Y'$ making the diagram commute is the composition of $e : Y \to X$ with $X \to Y'$:



Problem 2.1: Check these assertions.

§3 Geometric quotient

The geometric quotient is nicer, in the sense that we can construct, not just characterize it.

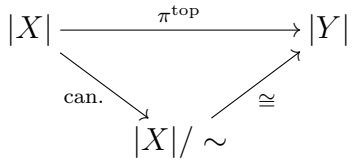
As a warm-up we consider the following simple case.

Lemma 2.5: Let Γ be a finite group, and $X = \operatorname{Spec} A$. Consider the group action

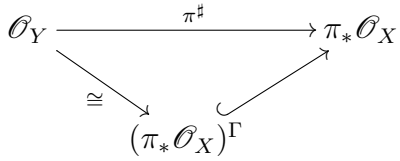
$$\Gamma \circlearrowright X = \operatorname{Spec} A \quad (S = \operatorname{Spec} k).$$

Let $Y = \operatorname{Spec} A^\Gamma \xleftarrow{\pi} X$ be induced by the inclusion $A^\Gamma \subseteq A$.

1. A is integral over A^Γ.
2. The map $Y = \operatorname{Spec} A^\Gamma \xleftarrow{\pi} X$ gives
   (a) the map on topological spaces



   and
   (b) the map on sheaves



Note also that π is a closed map.

Think of Y as the scheme whose topological space has the quotient topology, and whose sections are the Γ-invariant functions.

Let's prove it in this special case.

Proof. 1. Every $a \in A$ is a root of $\prod_{\gamma\in\Gamma}(X - \gamma(a)) \in A^\Gamma[X]$, so A is integral over A^Γ.

2. We need to show
   (a) $\Gamma\backslash|X| \to |Y|$ is well defined: Given $\mathfrak{p} \in \operatorname{Spec}(A)$, its image in A^Γ is $\mathfrak{p} \cap A^\Gamma$. We need $\mathfrak{p} \cap A^\Gamma = \gamma(\mathfrak{p}) \cap A^\Gamma$; this holds because Γ doesn't do anything on the Γ-invariant subset of $\mathfrak{p}$.

   Surjectivity follows from the fact that A is integral over A^Γ and the going-up theorem, which says that every prime ideal of A^Γ comes from a prime ideal of A.

   Theorem 2.6 (Going up)**:** Let $R \subseteq R'$ be an integral extension of rings, and $\mathfrak{p}$ a prime of R. Then there exists a prime $\mathfrak{q}$ of R' such that $\mathfrak{q} \cap R = \mathfrak{p}$.

Injectivity: Assume $\mathfrak{p} \cap A^\Gamma = \mathfrak{p}' \cap A^\Gamma$. Then for every $x \in \mathfrak{p}'$, we have $x \mid \prod_{\gamma\in\Gamma} \gamma(x) \in \mathfrak{p}' \cap A^\Gamma = \mathfrak{p} \cap A^\Gamma$, so $\gamma(x) \in \mathfrak{p}$ for some γ, i.e.

$$\mathfrak{p}' \subseteq \bigcup_{\gamma\in\Gamma} \gamma(\mathfrak{p}).$$

We use the following theorem from commutative algebra.

Theorem 2.7 (Prime avoidance)**:** Suppose $\mathfrak{a}$ is a subset of a ring R stable under addition and multiplication (e.g. an ideal). Suppose $\mathfrak{p}_j$ are prime ideals. If $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

This tells us that actually $\mathfrak{p}' \subseteq \gamma(\mathfrak{p})$ for some γ. By symmetry, $\mathfrak{p} \subseteq \delta(\mathfrak{p}')$ for some δ. This shows $\gamma(\mathfrak{p}) = \mathfrak{p}'$, i.e. $\mathfrak{p}$ and $\mathfrak{p}'$ lie in the same Γ-orbit, i.e. are the same in $\Gamma\backslash|X|$.

(b) The map on sheaves: Because the distinguished open sets $D_f := \operatorname{Spec}(A^\Gamma)_f$ for $f \in A^\Gamma$ form a basis for the topology on the affine scheme $Y = \operatorname{Spec} A^\Gamma$, it suffices to check the isomorphism on the D_f. On D_f we have the map

$$(A^\Gamma)_f = \mathscr{O}_Y(D_f) \to \pi_*\mathscr{O}_X(D_f).$$

The image is $(A_\Gamma)_f = (A_f)^\Gamma = (\pi_*\mathscr{O}_X)^\Gamma(D_f)$, as needed.

□

Because we actually constructed Y, the geometric quotient is a more hands-on approach.

We considered the affine case; to discuss the more general case where G is group scheme and X not necessarily affine, we need to enlarge our playground to *ringed spaces*.

We constuct a ringed space that looks like a candidate for the quotient, and show it is represented by scheme when possible.

We'll still assume $G \circlearrowright X$ where G is a finite flat group scheme over S and X is a scheme over S. This suffices for many purposes.

We have

$$(\mathrm{Sch}/S) \subset (\text{locally rings spaces}/S) \subset (\text{ringed spaces}/S)$$

We write (LRS/S) and (RS/S) in shorthand. The left inclusion is a full subcategory while the right one is not.

We'll construct a candidate for the quotient in the category (RS/S) and try to show it's actually in (Sch/S).

We assume the following hypothesis on orbits (essential in this approach):

- For any closed point $x \in X$, $G \cdot x \subseteq |X|$ is contained in an open affine subscheme of X.

Definition 2.8: Let $G \circlearrowright X$ where G is a group scheme over S and X is a scheme over S. Define the **geometric quotient** of X by G as the ringed space

$$(G\backslash X)_{rs} = (|X|/\sim, (\pi_{rs*}^{\text{top}}\mathscr{O}_X)^G)$$

where $\sim$ is given by the G-action, $\pi_{rs}^{\text{top}} : |X| \twoheadrightarrow |X|/\sim$ is the canonical quotient map and for every open $V \subseteq |X|/\sim$,

$$(\pi_{rs*}^{\text{top}}\mathscr{O}_X)^G(V) = \left\{a \in \pi_*^{\text{top}}\mathscr{O}_X(V) = \mathscr{O}_X(\pi^{\text{top}-1}(V)) : p_2^\sharp(a) = \mu^\sharp(a)\right\} \subseteq (\pi_{rs*}^{\text{top}}\mathscr{O}_X)^G(V).$$

Here the condition $p_2^\sharp(a) = \mu^\sharp(a)$ says that a is a G-invariant function. Recall that p_2 and μ were maps

$$G \times X \underset{p_2}{\overset{\mu}{\rightrightarrows}} X.$$

Next time, we'll show that under the hypothesis, this ringed space is actually a scheme.

Why do we assume such a hypothesis? The hypothesis says that the orbits of a closed point is contained in an affine neighborhood, so it allows us to reduce to the affine case.

If $\pi^{\text{top}} : |X| \to |X|/\sim = |Y|$ is affine (i.e. any inverse image of affine scheme is affine), for $x \in |X|$ mapping to $y \in |Y|$, there exists $V \ni y$ affine such that $\pi^{\text{top}-1}(V) \subseteq X$ is affine. But $\pi^{\text{top}-1}(V)$ contains the orbit of x, i.e. some affine neighborhood contains the orbit of x. Because the quotient morphism will often be affine, it is helpful to assume such a hypothesis.

Lecture 3
Thu. 9/13/12

Today we prove that under the hypothesis on orbits, the geometric quotient is a scheme.

Recall our hypothesis: for all $x \in X$ closed, $G \cdot x \subseteq |X|$ is contained in an open affine. We can write $G \cdot x$ another way, as

$$G \cdot x = \mu(p_2^{-1}(x))$$

Recall that we defined the geometric quotient $(|X|/\sim, (\pi_*^{\text{top}}\mathscr{O}_X)^G) \in (RS/S)$, where $\pi^{\text{top}} : |X| \to |X|/\sim$ is the quotient map and $(\pi_*^{\text{top}}\mathscr{O}_X)^G$ gives the collection of functions such that $p_2^\sharp(a) = \mu^\sharp(a)$.

More precisely, thinking of X as a space of functions, the G-invariance condition tells us that for $a \in (\pi_*^{\text{top}}\mathscr{O}_X)^G$, after pulling back a by the projection and multiplication maps $p_2, \mu : G \times_S X \to X$, we get the same thing: $p_2^\sharp(a) = \mu^\sharp(a)$.

§1 Geometric quotient, continued

Our goal today is to prove the following theorem.

Theorem 3.1: ([7, 4.16]) thm:geo-q Let G a finite locally free scheme over S and $G \circlearrowright X$ be a group scheme action. Under the hypothesis on orbits,

1. There exists $Y \in (\mathrm{Sch}/S)$ and $\pi : X \to Y$ such that $(Y, \pi) \cong ((X/G)_{rs}, \pi_{rs})$.
2. (Y, π) is a categorical quotient as well.
3. $\pi : X \to Y$ is integral, quasi-finite, and surjective. (Quasi-finite means that the fibers have dimension 0, i.e. $f^{-1}(y)$ is finite for each point $y \in Y$.)
4. If S is locally noetherian and X is locally of finite type over S, then π is a finite morphism.
5. The formation of the quotient (geometric or categorical) commutes with flat base change, namely base change to S' where $S' \to S$ is flat.[3] Namely, letting $X' := X \times_S S$, we have
$$(G\backslash X)'_{rs} \cong (G'\backslash X')_{rs}.$$

If we have a group action G on S, to form a quotient over S' there are two things we can do.

1. Base change to S' and take the quotient, or
2. take the quotient and base change.

The last point says that we have a natural isomorphism between these two objects.

Remark: ([7, 4.6] The condition that G be finite (over S) is essential. Consider
$$\mathbb{G}_m \circlearrowright \mathbb{A}^1_k = \mathbb{G}_m \cup \{0\},$$
where $S = \operatorname{Spec} k$ and $k = \overline{k}$. The categoric quotient is $\mathbb{A}^1_k \to \operatorname{Spec} k$, but the geometric quotient does not exist (the quotient map would have to map $\mathbb{A}^1_k \backslash \{0\}$ to a single point; since this is dense it maps all of $\mathbb{A}_k$ to a single point; but there whould be two points because there are two orbits). There doesn't exist a categorical quotient, but we suspect some quotient might still exist.

Proof sketch. (See [7, 4.18–4.25] for the details.)

We first reduce to the affine case by using the hypothesis to show X can be covered by G-stable open affine subschemes. We use that G is finite locally free in the reduction step. See [7, 4.18–19].

In the affine case $G = \operatorname{Spec} R$, $X = \operatorname{Spec} A$, $S = \operatorname{Spec} Q$. R is locally free over Q. By localizing, we may assume R is finite free of rank r over Q. Now
$$G \times_S X \underset{\mu}{\overset{p_2}{\rightrightarrows}} X \quad \text{induces} \quad R \otimes_Q A \underset{\mu}{\overset{p_2}{\leftleftarrows}} A$$

[3] A flat morphism $X \to Y$ is a morphism such that the induced map on every stalk is a flat map of rings, i.e. $f_p : \mathscr{O}_{Y,f(p)} \to \mathscr{O}_{X,p}$ is flat for all $p \in X$.

Define

$$B := \left\{ a \in A : p_2^\sharp(a) = \mu^\sharp(a) \right\}.$$

Part 1–3: We will show that $(Y = \operatorname{Spec} B,\ X \xrightarrow{\pi} Y)$, where π is induced by $B \hookrightarrow A$, is the geometric quotient. One main step is the following.

Claim 3.2: ([7, 4.20]) clm:787-3-1 *A is integral over B.*

We want to produce a monic polynomial with $a \in A$ as root. We have that $\mu^\sharp(a)$ acts by multiplication on $R \otimes_Q A$, a free A-module of rank r. Let $\chi(X)$ be the characteristic polynomial in $A[X]$.

Observe that $\mu^\sharp$ is injective because we have $\mu \circ (e, \mathrm{id}_X) = \mathrm{id}$:

$$\begin{array}{ccccc} & & \overset{\mathrm{id}}{\frown} & & \\ S \times_S X = X & \xrightarrow{(e,\mathrm{id}_X)} & G \times_S X & \xrightarrow{\mu} & X \\ x & \longmapsto & (e, x) & \longmapsto & x \end{array}$$

On rings, we have $(e, \mathrm{id}_X)^\sharp \circ \mu^\sharp = \mathrm{id}$, so $\mu^\sharp$ is injective.

If suffices to prove $\chi(X) \in B[X]$. By Cayley-Hamilton, $\chi(\mu^\sharp(a)) = 0$. Now, we can switch χ and $\mu^\sharp$ exactly when the coefficients are in B; for $b \in B$, $\mu^\sharp(b) = 1 \otimes b = p_2^\sharp(b)$. The fact that $\chi(X) \in B[X]$ gives $\mu^\sharp(\chi(a)) = 0$, which, by injectivity of $\mu^\sharp$, gives $\chi(a) = 0$.

This shows a is integral over B, which is exactly what we want to prove.

Let's prove $\chi(X) \in B[X]$. We need to show

$$eq : chi - in - B[X] p_2^\sharp(\chi(X)) = \mu^\sharp(\chi(X)) \tag{1}$$

in $R \otimes_Q A[X]$. We write

$$\chi(X) = (\mu^\sharp(a) \circlearrowright R \otimes_Q A \text{ as } A\text{-module}).$$

to mean that $\chi(X)$ is the characteristic polynomial of multiplication-by-$\mu^\sharp(a)$ on $R \otimes A$ considered as a A-module. To show (1), we transfer $\chi(X)$ to a characteristic polynomial on $R \otimes_Q R \otimes_Q A$ in two ways, and show they are equal.

1. We first transfer the action of A on $R \otimes_Q A$ to an action of $R \otimes_Q A$ on $R \otimes_Q R \otimes_Q A$ via the horizontal maps $p_2^\sharp$ and $m \otimes \mathrm{id}$:

$$\begin{array}{ccc} A & \xrightarrow{p_2^\sharp} & R \otimes_Q A \\ {\scriptstyle p_2^\sharp}\downarrow & & \downarrow{\scriptstyle 1\otimes\mathrm{id}} \\ R \otimes_Q A & \xrightarrow{m\otimes\mathrm{id}} & R \otimes_Q R \otimes_Q A. \end{array}$$

From this we get

$$eq : 787 - 3 - 1 p_2^\sharp(\chi(X)) = ((m \otimes 1)(\mu^\sharp(a)) \circlearrowright R \otimes_Q R \otimes_Q A \text{ as } R \otimes_Q A\text{-module}). \tag{2}$$

2. Next we transfer the action of A on $R \otimes_Q A$ to an action of $R \otimes_Q A$ on $R \otimes_Q R \otimes_Q A$ via the horizontal maps $\mu^\sharp$ and $\mathrm{id} \otimes \mu^\sharp$:

$$\begin{array}{ccc} A & \xrightarrow{\mu^\sharp} & R \otimes_Q A \\ {\scriptstyle p_2^\sharp}\downarrow & & \downarrow{\scriptstyle 1\otimes \mathrm{id}} \\ R \otimes_Q A & \xrightarrow{\mathrm{id}\otimes\mu^\sharp} & R \otimes_Q R \otimes_Q A. \end{array}$$

From this we get

$$eq : 787 - 3 - 2 \mu^\sharp \chi(X) = ((1 \otimes \mu^\sharp)(\mu^\sharp(a)) \circlearrowleft R \otimes R \otimes A \text{ as } R \otimes A\text{-module}). \tag{3}$$

Here, $R \otimes A$ acts on the 2nd and 3rd coefficients of $R \otimes_Q R \otimes_Q A$.

The group action axiom

$$\begin{array}{ccc} G \times G \times X & \xrightarrow{m\otimes 1} & G \times X \\ {\scriptstyle 1\otimes\mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ G \times X & \xrightarrow{\mu} & X \end{array}$$

now gives

$$(1 \otimes \mu^\sharp)(\mu^\sharp(a)) = (m^\sharp \otimes 1)(\mu^\sharp(a)).$$

This means (2) and (3) are equal, and we get (1), as needed. This proves Claim 3.2.

We know A integral over B, so $X \to Y$ is integral. By basic facts in commutative algebra, π is quasi-finite, closed, and surjective. (See for instance Chapter 5 of Atiyah-MacDonald.) Namely, use Cohen-Seidenberg theory: Going up gives surjectivity, etc.

It is not hard to show from here

$$(Y = \operatorname{Spec} B, \pi : \operatorname{Spec} A \to \operatorname{Spec} B) \cong (|X|/\sim, (\pi_*^{\mathrm{top}} \mathscr{O}_X)^G)$$

and that this is the categorical quotient. For details, see [7, 4.21–22].

Part 4: Let G be a locally finite type over S. Again reduce to the affine case. We can assume that A is a finite B-module. $X = \operatorname{Spec}(A)$, $Y = \operatorname{Spec}(B)$, $S = \operatorname{Spec}(Q)$, and A is a finitely generated Q-algebra. Then Because A is finitely generated Q-algebra, A is also a finitely generated B-algebra. Since A is integral over B, this means that A is finitely generated B-module, so π is finite.

Part 5: Reduce to the affine case; suppose $\operatorname{Spec} Q' = S' \to S = \operatorname{Spec} Q$ is flat. Say $X = \operatorname{Spec} A$. A function on X is given by $a \in A$. A G-invariant element is given by $(p_2^\sharp - \mu^\sharp)(a) = 0$. This operation commutes with base change in the following sense:

$$\ker((p_2^\sharp - \mu^\sharp) \otimes_Q Q') = \ker((p_2^\sharp - \mu^\sharp)) \otimes_Q Q'$$

We simply use the fact that tensoring by something flat is an exact functor. □

§2 Free group actions

We haven't imposed any conditions on the action itself. The group action is nicer when every point has trivial stabilizer. Our actual definition of a free group action is the following.

Definition 3.3: The group action $G \circlearrowright X$ where $G \in (\mathrm{Gp}/S)$ and $X \in (\mathrm{Sch}/S)$ is **(strictly) free** if

$$\begin{aligned}(\mu, p_2) : G \times_S X &\to X \times_S X \\ (g, x) &\mapsto (gx, x)\end{aligned}$$

is a closed immersion.

There is a special case where the action is always free.

Lemma 3.4: Let $G \subseteq H$ be a closed subscheme in (Gp/S). Let $G \circlearrowright H$ act by left translation. Then this action is strictly free.

Proof. We have

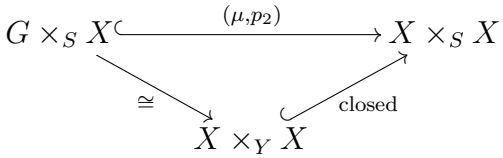
$$\begin{aligned}G \times_S H \hookrightarrow H \times_S H &\xrightarrow{\cong} H \times_S H \\ (h_1, h_2) &\longmapsto (h_1 h_2, h_2).\end{aligned}$$

where the left map is the basechange of $G \hookrightarrow H$, hence closed. □

When we impose more conditions on the action, we get stronger results, such as the following theorem (which we won't prove in complete generality)

Theorem 3.5: thm:gsx=xyx Let $G \circlearrowright X$ be a strictly free group action, G be finite locally free, and X be locally free of finite type. Suppose that the hypothesis on $G \cdot x$ is satisfied. Let Y be the geometric quotient. Then

1. $X \to Y$ is finite and locally free.
2. We have the following factorization.



Proof. We can check this locally. Let $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, $S = \operatorname{Spec} Q$, and $G = \operatorname{Spec} R$. Suppse R is free over Q of rank r.

Because $G \times_S X \hookrightarrow X \times_S X$ is a closed immersion, the corresponding map on rings is surjective:

$$R \otimes_Q A \twoheadleftarrow A \otimes_Q A.$$

Because $b \in B$, we have $\mu^\sharp(b) = p_2^\sharp(b)$ so

$$\mu^\sharp(a_1 \cdot b)p_2^\sharp(a_2) = \mu^\sharp(a_1)p_2^\sharp(b \cdot a_2).$$

This means that we can move b between the two factors in $A \otimes_Q A$ without affecting the image in $R \otimes_Q A$, i.e. we can factor

$$\begin{array}{ccc} eq : 787 - 3 - 3\ R \otimes_Q A & \twoheadleftarrow & A \otimes_Q A \\ & {\scriptstyle\varphi}\nwarrow \quad \nearrow{\scriptstyle q} & \\ & A \otimes_B A & \end{array} \tag{4}$$

The diagram shows φ is onto. We want to show that A is locally free over B. To do this, we localize at a prime $\mathfrak{q} \subset B$.

$A_\mathfrak{q}$ is semilocal (has a finite number of maximal ideals) since $X \to Y$ is quasi-finite.

We show that $A_\mathfrak{q}$ is free of rank r over $B_\mathfrak{q}$. This fact that A is locally free of rank r over B gives that A is free of rank r over B. See [7, 4.25] for details.

We get part 2 because we know φ is onto by (4). It is enough to show $(\ker\varphi)_\mathfrak{q} = \ker\varphi_\mathfrak{q}$ is 0. Using Nakayama's Lemma we can work over $B_\mathfrak{q}/\mathfrak{q}$-modules; $B_\mathfrak{q}/\mathfrak{q}$ is a field. A vector space map of dimension r that is onto must be an injection. We get $\ker\varphi_\mathfrak{q} = 0$ for all $\mathfrak{q}$, so Nakayama's lemma gives that the kernel itself is 0. □

Lecture 4
Tue. 9/18/12

Suppose we have a strictly free group action $G \circlearrowright X$, i.e. a group action such that the following map is closed:

$$\begin{array}{ccc} G \times_S X & \xrightarrow{\text{closed}} & X \times_S X \\ (g, x) & \longmapsto & gx. \end{array}$$

Let the quotient map be $X \xrightarrow{\pi} Y$. Our goal today is to relate quasi-coherent sheaves on X and on Y:

$$\mathrm{QCoh}(X) \underset{\pi^*}{\overset{\pi_*}{\rightleftarrows}} \mathrm{QCoh}(Y)\ .$$

In actuality rather than have $\mathrm{QCoh}(X)$ on the left-hand side, we have $\mathrm{QCoh}^G(X)$, the category of *G-equivariant sheaves* on X. We'll define what this means, and then show how G-invariant quasi-coherent sheaves[4] on X correspond to quasi-coherent sheaves on Y.

How will this be useful? Later on, when we construct dual abelian varieties, we will have to mod out by a group scheme, and we'll want to consider line bundles over the quotient scheme.

[4]Recall that a sheaf of $\mathcal{O}_X$-modules is **quasi-coherent** if X can be covered by open affine subsets $U_i = \operatorname{Spec} A_i$ such that for each i there is an A_i-module M_i with $\mathscr{F}|_{U_i} = \widetilde{M_i}$. See Hartshorne [2, §II.5]

§1 G-equivariance for vector bundles

sec:g-eq-vb

To motivate the definition of G-invariant sheaves, we first give several equivalent definitions of G-invariant vector bundles. This will be a kind of "toy model" for use to play with.

Definition 4.1: Let $G \circlearrowright X$ be a group acting on discrete G-set. A **vector bundle** on X is a vector space V_x for each $x \in X$. Let $V = \bigcup_{x\in X} V_x$. A **G-equivariant** vector bundle is V along with any one of the following equivalent structures, called G-invariant structures.

1. A group action $G \circlearrowright V$, and a map $\phi : V \to X$ sending V_x to x such that ϕ is G-equivariant:
$$\phi(gv) = g\phi(v).$$
2. A collection of "multiplication by g maps" $\left\{\lambda_x(g) : V_x \xrightarrow{\sim} V_{gx}\right\}_{g\in G, x\in X}$ such that
$$\lambda_x(1) = \mathrm{id}$$
$$\lambda_x(g_1g_2) = \lambda_{g_2x}(g_1) \circ \lambda_x(g_2)$$
where the second condition is says that $\lambda_x(g)$ is a group action, and comes from the following composition:
$$eq : 787 - 4 - cocycle \quad V_x \xrightarrow{\lambda_x(g_2)} V_{g_2x} \xrightarrow{\lambda_{g_2x}(g_1)} V_{g_1g_2x}. \qquad (5)$$
$$\lambda_x(g_1g_2) \text{ (curved arrow, } \sim\text{)}$$

We want to couch this in the language of the whole space, not individual fibers. To do this, we need to collect all the maps $\lambda_x(g)$ into a single map. This motivates our next equivalent definition.

Consider the two maps
$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \xmapsto{p_2} & x \\ & \xmapsto{\mu} & gx. \end{array}$$

Using these two maps, we construct two vector bundles over $G \times X$, p_2^*V and μ^*V. The fiber over (g, x) in p_2^*V is V_x, and the fiber over (g, x) in μ^*V is V_{gx}.

We now "assemble" the map $\lambda_x(g)$ into a single map λ on vector bundles over $G \times X$:
$$p_2^*V \xrightarrow[\cong]{\lambda} \mu^*V \ .$$

To express the cocycle condition (5), we consider 3 maps
$$\begin{array}{ccc} G \times G \times X & \longrightarrow & X \\ (g_1, g_2, x) & \xmapsto{p_3} & x \\ & \xmapsto{\xi} & g_2x \\ & \xmapsto{\eta} & g_1g_2x. \end{array}$$

3. An G-equivariant structure is a map λ on vector bundle over $G \times X$,

$$p_2^* V \xrightarrow[\cong]{\lambda} \mu^* V \ .$$

such that the following commutes (the cocycle condition)

$$\begin{array}{ccccc} p_3^* V & \xrightarrow{p_{23}^*\lambda} & \xi^* V & \xrightarrow{(\mathrm{id}_G \times \mu)^*\lambda} & \eta^* V. \\ & \underset{(\mu\times \mathrm{id}_X)^*\lambda}{\overset{\cong}{\searrow}} & & \overset{\cong}{\nearrow} & \end{array}$$

where p_{23} is passing to the second and third components.

Taking the fiber at (g_1, g_2, x), we recover (5).

Now we pull back the definition above to $\{g\} \times X \subseteq G \times X$.

4. Define $T_g : X \xrightarrow{\cong} X$ by $T_g(x) = gx$. A G-invariant structure on G is a collection of maps $\left\{\lambda_g : V \xrightarrow{\cong} T_g^* V\right\}_{g\in G}$ satisfying the following cocycle condition

$$\begin{array}{ccccc} eq : df4 - cocyle\ V & \xrightarrow{\lambda_{g_2}} & T_{g_2}^* V & \xrightarrow{T_{g_2}^*\lambda_{g_1}} & T_{g_2}^* T_{g_1}^* V \\ & \searrow^{\lambda_{g_1 g_2}} & & & \| \\ & & & & T_{g_1 g_2}^* V. \end{array} \tag{6}$$

Why do we need G to be free?

Suppose $G \circlearrowright X$ is a free action of a group on a set, i.e. $\mathrm{Stab}_G(x) = \{1\}$. (We also say that X is a principal homogeneous space under G.) Let $\pi : X \to X/G$ be the quotient map. Then we have an equivalence

$$\begin{array}{c} eq : 787 - 4 - vb \left\{\begin{array}{c}\text{vector bundles over} \\ X/G\end{array}\right\} \xrightarrow{\cong} \left\{\begin{array}{c}G\text{-equivariant vector bundle} \\ \text{over } X\end{array}\right\}. \\ V \mapsto \pi^* V \end{array} \tag{7}$$

This is an exercise. The idea is that by knowing the fiber over point, we can use the action of G on X to copy that fiber on the whole orbit of x.

Remark: If G is not free and $|G| > 1$, then we wouldn't expect such an equivalence. For instance, take $X = \{\cdot\}$ and let G act on X trivially. We still have a map as in (7), but it is no longer surjective.

On the left-hand side, a vector bundle over $X/G = \{\cdot\}$ is just a vector space. On the right-hand side, a G-equivariant vector bundle over $\{\cdot\}$ is a vector space with G-action. The map is no longer surjective, because V and hence $\pi^* V$ can only have the trivial action, but there are non-trivial G-actions on vector spaces.

In general, to get around the "strictly free" condition, we use stacks instead of schemes. However we will always restrict to free case, so that we can stay within scheme theory.

Our main examples of interest are closed group subschemes acting on schemes. The action is always strictly free in this case.

We've made a toy model; now let's go back to reality.

§2 G-equivariance for sheaves

Definition 4.2: Let $G \circlearrowright X$ be a group scheme over S acting on a scheme X over S, and $\mathscr{F} \in \mathrm{QCoh}(X)$.[5] A **$G$-equivariant sheaf** is a sheaf $\mathscr{F}$ with either of the following equivalent structures (called G-equivariant structures):

1. a map $p_2\mathscr{F} \xrightarrow{\lambda, \cong} \mu^*\mathscr{F}$ such that the following commutes

$$p_3^*\mathscr{F} \xrightarrow[\cong]{p_{23}^*} \xi^*\mathscr{F} \xrightarrow{(\mathrm{id}_G \times \mu)^*\lambda} \eta^*\mathscr{F}.$$
$$\underset{(\mu \times \mathrm{id}_G)^*\lambda}{\overset{\cong}{\curvearrowright}}$$

   in $\mathrm{QCoh}(G \times_S G \times_S X)$, where the maps are the analogues of the maps in Section 1, for schemes instead of vector bundles.

2. a collection

$$\left\{ \mathscr{F}_T : \mathscr{F}_T \xrightarrow{\cong} T_g^*\mathscr{F}_T \right\}_{T \in (\mathrm{Sch}/S),\, g \in G(T)}$$

   in $\mathrm{QCoh}(X_T)$ where X_T is the basechange $X \times_S T$, $T_g : X_T \xrightarrow{\cong} X_T$ is the translation map $x \mapsto gx$, and the maps are functorial in T. Moreover, this collection satisfies the cocycle condition (we require the same kind of diagram as in 6).

A structure in item 1 gives a structure in item 2 just by pulling back. To see a structure in item 2 gives a structure in item 1, we have to use descent theory (omitted).

Compare these two definitions with definitions 3 and 4 in Section 1.

Now that we've made the basic definitions, we'd like to see how it applies to quotient schemes. Actually, we'll look at a more general case.

2.1 Construction of G-equivariant structure

Let $\pi : G \circlearrowright X \to Y$ be a G-invariant map, i.e. a map such that if $p_2, \mu : G \times_S X \to X$ are the projection and multiplication maps, the G-equivariance condition

$$\pi \circ p_2 = \pi \circ \mu$$

[5] We could work with other sheaves too; however, our proofs will only work for quasicoherent sheaves.

holds. (For instance, π could be the quotient map.) We know that there is a pullback map from quasicoherent sheaves on Y to quasicoherent sheaves on X,

$$\begin{aligned}\pi^* : \mathrm{QCoh}(Y) &\to \mathrm{QCoh}(X)\\ g &\mapsto \pi^* g.\end{aligned}$$

However, we also want to equip $\pi^* g$ with a natural G-equivariant structure, so that $\pi^* g$ is in the category of G-equivariant sheaves

$$\mathrm{QCoh}^G(X) = \left\{\begin{matrix}G\text{-equivariant sheaves}\\ \text{on } X\end{matrix}\right\}.$$

Is there a natrual G-equivariant structure that we can equip $\pi^* g$ with? Yes.

Note that if $X \xrightarrow{f} Y \xrightarrow{g} Z$ are scheme morphisms, $\mathscr{F} \in \mathrm{QCoh}(X)$ and $\mathscr{H} \in \mathrm{QCoh}(Z)$, then

$$(g \circ f)^* \mathscr{H} \cong f^*(g^* \mathscr{H})$$

and

$$(g \circ f)_* \mathscr{F} = g_*(f_* \mathscr{F}).$$

For $W \subseteq Z$, the sections on $(g \circ f)_* \mathscr{F}$ are $\mathscr{F}(f^{-1}(g^{-1}(W)))$. We will define the G-equivariant structure by examining the sections of $(g \circ f)_* \mathscr{F}$.

By assumption on π, we have $\pi \circ p_2 = \pi \circ \mu$. Thus we can λ as the map making the following diagram commute:

$$\begin{array}{ccc} p_2^*(\pi^* \mathscr{G}) & \xrightarrow{\lambda} & \mu^*(\pi^* \mathscr{G}) \\ \| & & \| \\ \cong (\pi \circ p_2)^* \mathscr{G} & = & (\pi \circ \mu)^* \mathscr{G}. \end{array}$$

A tedious check shows that $\lambda : p_2^*(\pi^* \mathscr{G}) \to \mu^*(\pi^* \mathscr{G})$ satisfies the cocycle condition and is functorial in $\mathscr{G}$, so we do have a G-invariant structure on $\pi^* \mathscr{G}$.

Going in the opposite direction, suppose we have a G-equivariant sheaf on X, $\mathscr{F} \in \mathrm{QCoh}^G(X)$. What happens to the G-equivariant structure when we push forwards, using π_*?

In general, $\pi^* \pi_*$ is not the identity; the rank may increase when we pull back and push forward. We'd like to modify π_* so that we *do* get the identity.

Thus, we don't just push forwards: we push forward *and* take the *G-invariant sections.* We will define the map

$$\begin{aligned}\pi_*(\cdot)^G : \mathrm{QCoh}^G(X) &\to \mathrm{QCoh}(Y)\\ (\mathscr{F}, \lambda) &\mapsto (\pi_* \mathscr{F})^G.\end{aligned}$$

This takes the sheaf $\mathscr{F}$ on X with G-invariant structure to a $\mathscr{O}_Y$-submodule of $\pi_* \mathscr{F}$ consisting of G-invariant sections, defined formally below.

Definition 4.3: Let $\pi : G \circlearrowright X \to Y$ be a **G-invariant map**. Let $V \subseteq Y$ be open. We say that a section $s \in \pi_*\mathscr{F}(V) = \mathscr{F}(\pi^{-1}(V))$ is **G-invariant** if

$$\lambda(p_2^*(s)) = \mu^*(s),$$

i.e. s gets mapped to the same element when we follow the two maps below:

$eq : 787 - 4 - 4$

$$\begin{array}{ccc} & & (p_2^*\mathscr{F})(p_2^{-1}(\pi^{-1}(V))) \\ & \overset{p_2^*}{\nearrow} & \| \cong \lambda \\ \mathscr{F}(\pi^{-1}(V)) & & \| \\ & \underset{\mu^*}{\searrow} & \| \\ & & (\mu^*\mathscr{F})(\mu^{-1}(\pi^{-1}(V))). \end{array} \tag{8}$$

Define $(\pi_*\mathscr{F})^G$ by having $(\pi_*\mathscr{F})^G(V)$ consist of the G-invariant sections on V.

Note that the blue sets above are the same because of G-invariance. Moreover, $(\pi_*\mathscr{F})^G$ is actually a $\mathscr{O}_Y$-submodule because the condition $\lambda(p_2^*(s)) = \mu^*(s)$ is stable under $\mathscr{O}_Y$ action.

Example 4.4: The sheaves $\mathscr{O}_G, \Omega^1_{G/S}$ carry natural G-invariant structures. This is easiest to see on the level of T-points. For all $g \in G(T)$, are there maps $\mathscr{O}_G \xrightarrow{\cong} T_g^*\mathscr{O}_G$ and $\Omega^1_{G/S} \cong T_g^*\Omega^1_{G/S}$ that satisfy the cocycle condition? Yes, because we know the translation T_g induces an isomorphism on these spaces.

For instance, (?)

$$\{\text{invariant global differentials on } G\} \cong \{G\text{-invariant section of } \Omega^1_{G/S} \text{ over } G\}$$

In the case of elliptic curves, we get the invariant differential on elliptic curves.

Remark: Given any vector bundle, in general there is not necessarily a G-invariant structure. The same is true of sheaves: given a quasi-coherent sheaf, there may not be G-equivariant structure, or there may be more than 1.

Theorem 4.5: Let X be a scheme locally of finite type over S. Let G be a locally free group scheme over S, and suppose we have a strictly free action $G \circlearrowright X$. Then there are 2 maps π^* and $\pi_*(\cdot)^G$ which induce categorical equivalences (top of diagram below)

$$\begin{array}{ccc} \mathrm{QCoh}(Y) & \underset{\pi_*(\cdot)^G}{\overset{\pi^*}{\rightleftarrows}} & \mathrm{QCoh}(X)^G \\ \uparrow & & \uparrow \\ \{\text{locally free of rank } a\} & \longleftrightarrow & \{\text{locally free of rank } a\} \end{array}$$

Moreover, they also induce a bijection on the subcategories of locally free sheaves of a given rank a.

Remark: The $a = 1$ case is already important; they give line bundles.

We will be specially interested in the case where Y is a quotient scheme, $Y = X/G$.

Proof sketch. For the complete proof, see [4, p. 70 and p. 114-118].

Reduce to affine case $G = \mathrm{Spec}(R)$. Because G is locally free, we can assume by localizing further that R is free of rank r over Q.

$$\begin{aligned} G &= \mathrm{Spec}(R) & X &= \mathrm{Spec}(A) \\ S &= \mathrm{Spec}(Q) & Y &= \mathrm{Spec}(B). \end{aligned}$$

Then $\mathscr{F}$ corresponds to an A-module M, i.e. $\mathscr{F} = \widetilde{M}$.

We can rewrite (8) in terms of modules (recall that defining pullback involves tensor product), to get the triangle on the LHS below:

$eq : 787 - 4 - 5$

$$\begin{array}{ccccc} M \otimes_A (R \otimes_Q A) & \xleftarrow[\psi]{\cong} & M \otimes_A (A \otimes_B A) & \xlongequal{m\otimes a\otimes 1 \leftarrow\!\shortmid a\otimes m} & A \otimes_B M \\ \uparrow \cong \lambda & & \cong \uparrow & & \cong \uparrow \lambda' \\ M & & & & \\ \downarrow \cong \lambda & & \cong \downarrow & & \cong \downarrow \lambda' \\ M \otimes_A (R \otimes_Q A) & \xleftarrow[\psi]{\cong} & M \otimes_A (A \otimes_B A) & \xlongequal{m\otimes 1\otimes a \leftarrow\!\shortmid m\otimes a} & M \otimes_B A. \end{array} \tag{9}$$

The maps in the left triangle carry $m \mapsto m \otimes 1$. Note that the two tensor products $M \otimes_A (R \otimes_Q A)$ are formed differently, though: the top one is formed via the map $p^* : A \to R \otimes_Q A$ sending $a \mapsto 1 \otimes a$ and bottom one is formed via the map $\mu^* : A \to R \otimes_Q A$. The sheaf $(\pi_* \mathscr{F})^G$ corresponds to the module

$$M^G = \{m \in M : \lambda(m \otimes 1) = m \otimes 1\}.$$

We will use two facts from last time.

1. By Theorem 3.5, we have an isomorphism $G \times_S X \xrightarrow{\cong} X \times_Y X$ sending $(g, x) \mapsto (gx, x)$. This gives a ring isomorphism

$$\begin{aligned} A \otimes_B A &\xrightarrow{\psi, \cong} R \otimes_Q A \\ a_1 \otimes a_2 &\mapsto \mu^*(a_1) p_2^*(a_2) = \mu^*(a_1)(1 \otimes a_2). \end{aligned}$$

   This gives us the middle square in (9). Here, the tensor product in the upper $M \otimes_A (A \otimes_B A)$ is formed by the map $A \to A \otimes_B A$ given by $a \mapsto 1 \otimes a$, and the tensor product in the lower $M \otimes_A (A \otimes_B A)$ is given by $a \mapsto a \otimes 1$. This is because $1 \otimes a$ is sent to $p_2^*(a)$ and $a \otimes 1$ is sent to $\mu^*(a)$.

2. If A is projective of rank r over B and integral over B, then A is faithfully flat over B. reference

We need to show two things.

1. We have an isomorphism
$$\pi^*((\pi_*\mathscr{F})^G) \xrightarrow{\cong} \mathscr{F}.$$
This is equivalent to having an isomorphism
$$\begin{aligned} M^G \otimes_B A &\xrightarrow{\cong} M \\ m \otimes a &\mapsto am \end{aligned}$$

2. For $\mathscr{G}$ on Y, we have an isomorphism
$$\mathscr{G} \xrightarrow{\cong} (\pi_*(\pi^*\mathscr{G}))^G.$$
If $\mathscr{G} = \widetilde{N}$, this is equivalent to having an isomorphism
$$N \xrightarrow{\cong} (N \otimes_B A)^G.$$

THIS IS UNEDITED. Fix after I understand the proof in Mumford. M projective over A iff M^G is projective over B If we show these are true we will be done very soon.

How to deduce theorem from 3 and 4.

(i) $\pi_*(\pi^*\mathscr{G})^G \cong \mathscr{G}$ canonically using adjunction. On modules, $(N \otimes_B A)^G \cong N$ for all B-modules N.

$N \otimes_B A \to (N \otimes_B A)^G \otimes_Q A \xrightarrow{\cong} N \otimes_B A$. isomorphism by 3. composition is identity [XYMATRIX] Thus LHS canonical map is isomorphism.

$$N \otimes_B A \xrightarrow{\cong} (N \otimes_B A)^G \otimes_B A.$$

implies A faithfully flat over B. It must be an isomorphism to begin with,

$$N \xrightarrow{\cong} (N \otimes_B A)^G.$$

(ii) Use part 4+ locally free=projective. Projective corresponds to projective. + check equality of rank, easy given part 3.

Refer to Mumford section 12. He works over algebraically closed field. $S = \mathrm{Spec}(k)$, k alg closed, but works in generality.

□

Next time we can will finally talk about abelian varieties and schemes.

Lecture 5
Thu. 9/20/12

Today we will (finally) talk about abelian schemes. We'll start by recalling some terminology from scheme theory.

§1 Review of scheme theory

Definition 5.1: 1. $X \in (\mathrm{Sch})$ is **locally noetherian** if for all open affine $U \subseteq X$, $U = \operatorname{Spec} A$ for some noetherian ring A.

2. $f : X \to Y$ is **locally of finite type**, **locally of finite presentation** if for all open affine $V = \operatorname{Spec} A \subseteq X$, for all $U = \operatorname{Spec} B \subseteq f^{-1}(V)$, B is an algebra of finite type (finitely generated), of finite presentation, respectively. The first means $V \cong A[x_1, \ldots, x_n]/\mathfrak{a}$, and the second means that in addition $\mathfrak{a}$ is finitely generated.

3. $f : X \to Y$ is **quasi-compact** if for all $V \subseteq Y$ open affine (quasi-compact), $f^{-1}(V)$ is quasi-compact.

Remark: It is enough that there exist some open covering that has the property (i.e., the properties are affine-local properties).

Definition 5.2: A morphism is

1. **noetherian** if it is locally noetherian and quasi-compact.

2. **of finite type** if it is locally of finite type and quasi-compact

3. **of finite presentation** if it is locally of finite presentation and quasi-compact.

Proposition 5.3: Let $f : X \to Y$ be a morphism such that Y is (locally) noetherian and f is (locally) of finite type. Then X is (locally) noetherian and f is (locally) of finite presentation.

Proof. In the affine case, this says that a finitely generated algebra over a noetherian ring is noetherian and finitely presented. This is true by the Hilbert Basis Theorem.

Glue for the general case. □

One of many definitions for smooth is the following.

Definition 5.4: f is **smooth** if f is locally of finite presentation, flat, and has geometrically regular fibers.

A flat morphism $f : X \to Y$ is one such that if $f(x) = y$, then $\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is a flat algebra.

Geometrically regular fibers means that for all scheme-theoretic points $y \in Y$, the bottom map is regular.

$$\begin{array}{ccc} X_y & \xrightarrow{f_y} & y = \operatorname{Spec} k(y) \\ \uparrow & & \uparrow \\ X_{\overline{y}} & \xrightarrow{\text{regular}} & \operatorname{Spec} \overline{k(y)} \end{array}$$

Regular means that the local rings at every point is regular, i.e. we have the correct dimension for the tangent space at every point.

Definition 5.5: Let k be a field. $X \in (\mathrm{Sch}/k)$ is a **variety** if X is integral (reduced and irreducible), of finite type, and separated.

We have the following fact.

Fact 5.6: $X \times_k k'$ is reduced/irreducible/connected for all field extensions k'/k iff $X \times_k \overline{k}$ is reduced/irreducible/connected for some algebraic closure $\overline{k}$. We say that X is **geometrically** reduced/irreducible/connected.

Definition 5.7: A morphism f is **proper** if it is separable, of finite type, and universally closed.

Fact 5.8: Let k be a field, and X/k be proper and geometrically connected and reduced. Then the global sections are

$$H^0(X, \mathscr{O}_X) \cong k.$$

§2 Abelian schemes

Definition 5.9: df:787-5-1 Let S be any scheme. An scheme $A \in (\mathrm{Sch}/S)$ with $\pi : A \to S \in (\mathrm{Sch}/S)$ is an **abelian scheme** if it satisfies either of the following equivalent conditions.

1. π is smooth, proper, and has geometrically connected fibers (for all $s \in S$, A_s is G-connected).

2. if π is proper, flat, and of finite presentation with smooth geometrically regular fibers.[6]

Proof of equivalence. Observe that (2) $\implies$ (1) is by definition: smooth means locally of finite presentation, flat, and having geometric regular fibers.

For (1) $\implies$ (2), everything is clear except finite presentation. Note that a smooth morphism is locally of finite presentation, and a proper morphism is of finite type, hence quasi-compact. A morphism that is locally of finite presentation and quasi-compact is of finite presentation. □

Remark: "Geometrically" can be removed in condition 1: If X/k is a connected scheme with $X(k) \neq \phi$, then X is automatically geometrically connected. Apply this fact to $X = A_s = A \times_S \operatorname{Spec} k(s) \underset{e_{A_s}}{\rightleftarrows} \operatorname{Spec} k(s)$ where e_{A_s} is the identity section.

Definition 5.10: df:787-5-2 (Mumford's definition) Let $k = \overline{k}$. Then an **abelian variety** over k is a proper group variety over k.

[6] A scheme is regular if it is covered by affine opens $\operatorname{Spec} A$ with A regular, i.e., noetherian and such that the localization at every prime ideal is a regular local ring.

We would like an abelian scheme over $\operatorname{Spec} k$ (where $k = \overline{k}$) that is a variety to be an abelian variety over k.

Proof of equivalence. Definition 5.9(1) $\implies$ Definition 5.10: Because X is proper, X is separated of finite type. We want X to be integral (reduced and irreducible). We use the following facts for schemes over a field k:

- connected and smooth together imply geometrically irreducible,
- smooth implies geometrically reduced.

Thus an abelian scheme over k is a variety.

Definition 5.10 $\implies$ 5.9(1): We use the following fact: Let X/k be reduced and locally of finite type, where k is a perfect field. Then the smooth locus $X_{sm} \subseteq X$ is open dense.

Now X_{sm} is open dense but also stable under group translation, so $X_{sm} = X$ and X is smooth. □

Thus our definitions 5.9 and 5.10 are healthy!

An example of an abelian variety is an elliptic curve.

Why do we impose these conditions? To see this, let's look at some nonexamples.

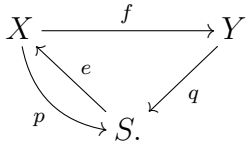
Example 5.11: The schemes $\mathbb{G}_{m,S}$, $\mathbb{G}_{a,S}$, and $GL_{n,S}/S$ are not abelian because they are not proper. ($\mathbb{G}_{m,S}$ and $GL_{n,S}/S$ are not of finite type, while $\mathbb{G}_{a,S}$ is not universally closed.)

The constant group scheme $(\mathbb{Z}/n\mathbb{Z})_S$ is not an abelian scheme: it is smooth and proper but not geometrically connected. It has n points over each fiber.

§3 Rigidity lemma and applications

So far we haven't imposed a condition that the group law be abelian. A natural question is: if the group law abelian for abelian schemes? Yes; our definitions in fact force it to be abelian, but the proof is somewhat technical, relying on the following lemma.

Lemma 5.12 (Rigidity lemma)**:** lem:rigid Let X, Y, S be locally noetherian (over S), let $f : X \to Y$ be a morphism, and let $e : S \to X$ be a section. Suppose $p : X \to S$ is proper and flat (with geometrically reduced fibers?), S is connected, q is finite separated, and $p \circ e = \mathrm{id}_S$. We have the following diagram

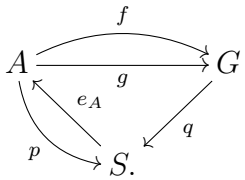


If $f(X_s) = \{y\}$ as a set for some $s \in S$, then $f = \eta \circ p$ where $\eta = f \circ e$, and $S \to Y$ is a section of q.

In other words, when we impose a property for one fiber, then we get the property over all S. We'll postpone the proof to next lecture, and focus instead on the consequences.

> The rigidity lemma allows us to take a property over one fiber of S and show it holds over all of S.

Corollary 5.13: cor:rigid1 Suppose we have scheme morphisms



where A is an abelian scheme, $q : G \to S$ is separated of finite presentation, and f, g are morphisms in (Sch/S) (not necessarily in (Gp/S)). If for some $s \in S$, $f_s = g_s$, then $f = \mu_G \circ ((\eta \circ p) \times g)$ for some section $\eta : S \to G$ (in fact $\eta = f \circ e_A$).

The idea is as follows. We can take a difference of morphisms, because G is a group scheme. We have that "$f - g$" is constant over a fiber; hence by the rigidity lemma it is constant everywhere.

Proof. By generalities in EGA IV we can reduce to the locally noetherian case. We can apply the rigidity lemma to

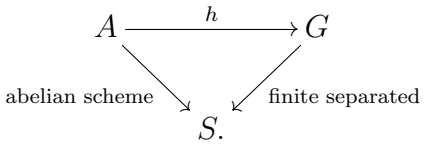
$$A \xrightarrow{(f, i_G \circ g)} G \times_S G \xrightarrow{\mu} G$$

sending

$$x \mapsto (f(x), g(x)^{-1}) \mapsto f(x)g(x)^{-1}.$$

We have $h(A_s) = \{e_G(s)\}$ (the identity on G). By the rigidity lemma, $h = \eta \circ p$ and $\eta = h \circ e_A$. Another way to write this is $f = \mu_G \circ ((\eta \circ p) \times g)$.[7] □

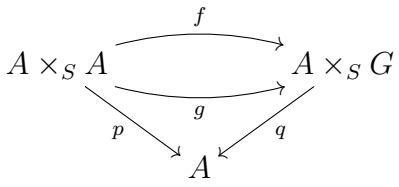
Corollary 5.14: cor:rigid2 Suppose A is an abelian scheme over S and G is finite separated group scheme over S:



If h sends the identity element of A to the identity element of G, i.e. $h \circ e_A = e_G$, then h is a group homomorphism.

[7] Taking T-points, we have $f(x)g^{-1}(x) = h(e_A)$ becomes $f(x) = g(x)h(e_A)$. This is equivalent to saying $h = \mu_G \circ (f, i_G \circ g) = \mu_G \circ (f, i_G \circ g) \circ e_A \circ p$ implies $f = \mu_G \circ (\mu_G \circ (f, i_G \circ g) \circ e_A \circ p, g) = \mu \circ (f \circ e_A \circ p, g)$.

Proof. Let p, q be the projections to the first component. Apply Corollary 5.14 to



where we let f and g be the maps

$$(x_1, x_2) \mapsto (x_1, h(x_1 x_2))$$
$$(x_1, x_2) \mapsto (x_1, h(x_2))$$

and p, q are projections onto the first component. Note that $p = q \circ f$.

The corollary gives

$$f = \mu_G \circ ((\eta \circ p) \times g)$$

Unraveling the definitions, we get

$$(x_1, h(x_1 x_2)) = (x_1, \eta_0(x_1)) \cdot_G (x_1, h(x_2))$$
$$\implies h(x_1 x_2) = \eta_0(x_1) h(x_2).$$

Take $x_2 = \mathrm{id}$ to get $h(x_1) = \eta_0(x_1)$. Hence we get

$$h(x_1 x_2) = h(x_1) h(x_2).$$

□

Now we show that an abelian scheme is well-named.

Corollary 5.15: Let $A \to S$ be an abelian scheme. Then A has commutative group law.

Proof. Commutativity is equivalent to the the inverse map $x \mapsto x^{-1}$ being a homomorphism. Apply Corollary 5.14 to $A \xrightarrow{i_A} A$, $x \mapsto x^{-1}$. This morphism sends e_A to e_A so it is a group hoomorphism. Hence A is abelian. □

For example, consider an elliptic curve, which is a smooth proper genus 1 curve. Choose a basepoint, i.e., declare a point to serve as the identity. Then the group law is determined. We generalize this.

Corollary 5.16: Let (A, e_A, i_A, μ_A) and (A, e_A, i'_A, μ'_A) in (Gp/S) be two abelian scheme structures on the same scheme, with the same identity element.

Then $i_A = i'_A$ and $\mu_A = \mu'_A$, i.e. the abelian schemes are the same.

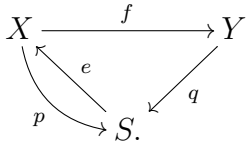
Proof. Apply Corollary 5.14 to $A \xrightarrow{\mathrm{id}} A$. It is an automorphism of schemes; hence it is a group homomorphism by the Corollary, and the group structures are compatible. □

We give the proof of the rigidity lemma next time.

Lecture 6
Tue. 9/25/12

Last time we saw why the rigidity lemma is so useful. For instance, it told us that if we fix the identity element of an abelian scheme, then it has only one possible group structure.

Proposition 6.1 (Rigidity lemma 5.12, again)**:** Let X, Y, S be locally noetherian (over S), let $f : X \to Y$ be a morphism, and let $e : S \to X$ be a section. Suppose $p : X \to S$ is proper and flat (with geometrically reduced fibers?), S is connected, q is finite separated, and $p \circ e = \mathrm{id}_S$. We have the following diagram



If $f(X_s) = \{y\}$ as a set for some $s \in S$, then $f = \eta \circ p$ where $\eta = f \circ e$, and $S \to Y$ is a section of q.

Today prove the lemma and then talk about isogenies.

§1 Proof of rigidity lemma

The idea is to first prove the lemma when S consists of a point. In the general case we get that the lemma holds in a neighborhood of a point; then we show that the neighborhood where the lemma holds is both open and closed, hence all of S.

We follow [5, p. 115] but give more details.

Proof. Part 1: Let S consist of 1 point $\{s\}$. On topological space, it is clear that

$$f = \eta \circ p = f \circ e \circ p.$$

We show that this is true on the sheaf of rings too ($f^\sharp = (\eta \circ p)^\sharp$), using the following claim.

Claim 6.2: The map $p^\sharp : \mathscr{O}_S \xrightarrow{\cong} p_*\mathscr{O}_X$ is an isomorphism.

Since S has just one point, this is the same as saying we have an isomorphism

$$p^\sharp : \mathscr{O}_S(S) \xrightarrow{\cong} \mathscr{O}_X(X).$$

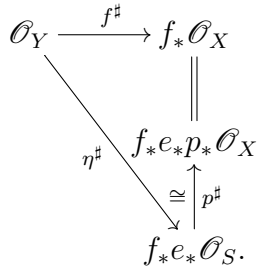
Proof. Injectivity: p is faithfully flat, so $\mathscr{O}_X(X)$ is a faithfully flat $\mathscr{O}_S(S)$ algebra, so $\mathscr{O}_S(S) \to \mathscr{O}_X(S)$ must be injective.

Surjectivity: Over the special fiber we have an isomorphism

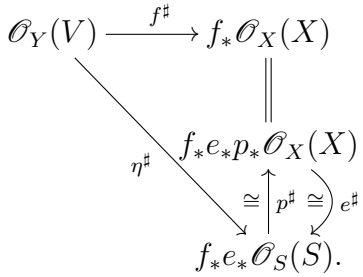
$$\mathscr{O}_S(S)/\mathfrak{m}_S \xrightarrow{\cong} \mathscr{O}_X(X)/\mathfrak{m}_S$$

The left-hand side is $\operatorname{Spec} k(s)$ and the right-hand side is $H^0(X_s, \mathscr{O}_{X_s})$, the space of global sections. (These are equal because we assumed something...) By Nakayama we get a surjection without the mod $\mathfrak{m}_S$.

From here the rest of the proof is formal. We will show that the following commutes.



Relationship between two diagrams? Why need to show 2nd to show 1st (why not just obvious?) To see this, look at the sections on an open $V \subseteq Y$ such that $y \in V \subseteq Y$. We have, for all $V \subseteq Y$



We get a map $e^\sharp$ that is the inverse of $p^\sharp$ because by hypothesis $p \circ e = \mathrm{id}$. The outer diagram commutes because $\eta^\sharp = e^\sharp f^\sharp$.

Thus we get $f^\sharp = p^\sharp \eta^\sharp = (\eta \circ p)^\sharp$, as needed. □

Part 2: Consider the general case. The idea is to define Z to be the largest closed subscheme of X on which $f = \eta \circ p$, and try to show that $Z = X$. Rigorously, we define Z as the following fiber product

$$\begin{array}{ccc} Z & \longrightarrow & X \\ \downarrow & & \downarrow{\scriptstyle (f,\eta\circ p)} \\ Y & \xrightarrow{\Delta} & Y \times_S Y \end{array}$$

By definition of the fiber product Z is exactly the "subscheme where $f = \eta \circ p$." To see Z is a closed subscheme, note that because Y is separated, the map $Y \xrightarrow{\Delta} Y \times_S Y$ is a closed immersion. Since closed immersions are stable under base extension, $Z \to X$ is closed.

Observe the following.

1. The fiber over s is contained in Z as a set:
$$p^{-1}(s) \subseteq Z.$$
(Note $X_s = p^{-1}(s)$ as sets.) This follows from step 1, applied to
$$\begin{array}{ccc} X_s & \xrightarrow{f_s} & Y_s \\ & \searrow \quad \swarrow & \\ & \operatorname{Spec} k(s). & \end{array}$$
(We have $\operatorname{Spec} k(s) = \{s\}$.)

2. For all $t \in S$ such that $p^{-1}(t) \subseteq Z$, we can "spread it out" to a whole open neighborhood (subscheme): there exists an open subscheme $W \subseteq S$ containing t such that $p^{-1}(W) \subseteq Z$ as an open subscheme.

   To be precise, when we write $p^{-1}(W)$ we mean the fiber product $W \times_S X$ where the map $X \to S$ is given by p. We will postpone the proof.

How can we finish given these two facts? Define
$$V := \left\{ t \in S : p^{-1}(t) \subseteq Z \right\}.$$
By item 1, V is nonempty, and by item 2, V is open.

The picture is as follows.

Diagram (see notebook)

We check the following.

- p is surjective. This follows from existence of e.
- p is open. Proper implies finite type and hence locally of finite type. A flat morphism locally of finite presentation is open.

Now note $S = V \cup p(X \backslash Z)$. We have V and $p(X \backslash Z)$ are both open and disjoint. Since S is connected and $V \neq \phi$, this means $X \backslash Z = \phi$, and set-theoretically, $Z = X$.

By part 1, the local rings must be isomorphic, and $Z = X$ as schemes. This shows the proposition is true.

We now show item 2. We need some technical considerations. Assume that $p^{-1}(t) \subseteq Z$. Consider the *thickened* point $T = \operatorname{Spec} \mathscr{O}_{S,t}/\mathfrak{m}_t^N \hookrightarrow S$. (As a set, $T = \{t\}$.) Note we are proceeding like in item 1 but more generally, because we're allowing nonreduced points. This is what allows us to get a neighborhood in Z rather than just a point in Z.

We show that there is a open neighborhood contained in Z, containing $p^{-1}(t)$. Applying part 1 to
$$\begin{array}{ccc} X \times_S T = p^{-1}(T) & \xrightarrow{f \times_S T} & Y \times_S T \\ & \searrow \quad \swarrow & \\ & T, & \end{array}$$
we see that $p^{-1}(T) \subseteq Z$.

Claim 6.3: There exists U such that $p^{-1}(T) \subseteq U \subseteq Z \subseteq X$ where $p^{-1}(T) \subseteq U$ is a subscheme and $U \subseteq Z$ is an open subscheme.

Proof. It suffices to prove an isomorphism of local rings: for all $z \in p^{-1}(t)$,

$$\mathscr{O}_{X,z} \twoheadrightarrow \mathscr{O}_{Z,z}$$

is an isomorphism. (It is surjective becaue $Z \subseteq X$ is a closed subscheme.) Consider ideal of definition for closed subscheme. Being zero at z. Being 0 is an open property, so 0 in neighborhood. (Why is showing this sufficient?)

For this, we need some algebra on local rings.

We have the commutative diagram (note $p^{-1}(T) := T \times_S X$)

$$\begin{array}{ccccc} p^{-1}(T) & \overset{\text{closed}}{\hookrightarrow} & Z & \overset{\text{closed}}{\hookrightarrow} & X \\ {\scriptstyle p}\downarrow & & & & \downarrow{\scriptstyle p} \\ T & & \xhookrightarrow[\text{closed}]{} & & S. \end{array}$$

For $z \in p^{-1}(T)$, we have on local rings that

$$\begin{array}{ccccc} \mathscr{O}_{X,z}/\mathfrak{m}_z^N = \mathscr{O}_{p^{-1}(T),z} & \twoheadleftarrow & \mathscr{O}_{Z,z} & \twoheadleftarrow & \mathscr{O}_{X,z} \\ \uparrow & & & & \uparrow \\ \mathscr{O}_{S,t}/\mathfrak{m}_t^N & = & \mathscr{O}_{T,t} & \twoheadleftarrow & \mathscr{O}_{S,t} \end{array}$$

where, because the map on the right is a local homomorphism, we have that $\mathfrak{m}_t \subset \mathscr{O}_{S,t}$ in the lower right is mapped to $\mathfrak{m}_z \subset \mathscr{O}_{X,z}$ in the upper right.

Define

$$\mathfrak{a} := \ker(\mathscr{O}_{X,z} \twoheadrightarrow \mathscr{O}_{Z,z}).$$

We have

$$\mathfrak{a} \subseteq \ker(\mathscr{O}_{X,z} \twoheadrightarrow \mathscr{O}_{Z,z}/\mathfrak{m}_t^N) = \mathfrak{m}_t^N \mathscr{O}_{X,z} \subseteq \mathfrak{m}_z^N \text{ for all } N \geq 1$$

since this works for any N. Thus $\mathfrak{a} \subseteq \bigcap_{N\geq 1} \mathfrak{m}_z^N$. By Krull's Theorem for noetherian rings, $\bigcap_{N\geq 1} \mathfrak{m}_z^N = (0)$. Hence $\mathscr{O}_{X,z} \to \mathscr{O}_{Z,z}$ is an isomorphism, and the claim follows. □

We've shown there exists U so that $p^{-1}(T) \subseteq U \subseteq Z$.

But we want a neighborhood downstairs, in S, as in item 2. To obtain a neighborhood in S, rather than in Z, we use take complement of U and use the fact that f is a closed map.

Because p is proper so $p(X\backslash U)$ is closed in S, and $S\backslash p(X\backslash U)$ is open. Thus exists an open set $W \subseteq S\backslash p(X\backslash U)$ containing t, such that

$$p^{-1}(W) \subseteq U \subseteq Z.$$

This is true not just as sets but as open subschemes.

This shows item 2, as needed. □

§2 Isogenies

We have $(\mathrm{Ab}/S) \subseteq (\mathrm{Gp}/S)$ as a full subcategory. The most important class of morphisms between abelian schemes are *isogenies*.

Recall that an abelian scheme over S is just a group scheme $\pi : A \to S$ that is smooth and proper and has geometrically connnected fibers.

Lemma 6.4: lem:787-6-1 Let $f : A \to A'$ be a morphism in (Ab/S). Then the following are equivalent.

1. f is finite and faithfully flat.
2. f is quasi-finite and surjective on points.

(A scheme is quasi-finite if it is finite type with 0-dimensional fibers.)

The second condition is weaker.

Definition 6.5: Any such f is called an **isogeny**.

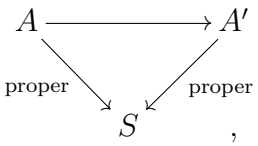
Fact 6.6: The following conditions are equivalent.

- finite
- quasi-finite and proper
- affine and proper.

The advantage of 2 in lemma is that it can be checked fiberwise.

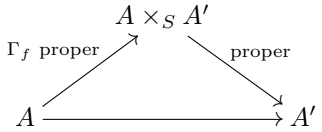
Proof. (1) $\implies$ (2) is clear.

For (2) $\implies$ (1) we need some Grothendieck-style lemmas. First, if we have a map $A \to A'$ with A and A' proper over S,



then $A \to A'$ is proper.[8] Since we assumed $f : A \to A'$ is quasi-finite, by the fact we get f is finite.

[8]Proof: See Hartshorne [2, Exercise 4.8e]. A proper map is separated, and separated means that the diagonal map is closed immersion. Basechange is proper, so $A \times_S A' \to A'$ and the graph morphism $\Gamma_f : A \to A \times_S A'$ is proper. The composition of proper morphisms is proper.

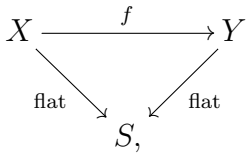


Hence $A \to A'$ is proper.

To see that f is flat, note the following two facts.

1. Fiberwise flatness:

   Proposition 6.7: pr:fiberwise-flatness If we have

   and X, Y are locally noetherian or X, Y are locally of finite presentation over S (in particular, if they are abelian varieties), then f is flat iff for all $s \in S$, f_s is flat.

   The proof comes down to a statement in commutative algebra for local noetherian rings.

   Thus, in our case, it suffices to prove $f_s : A_s \to A'_s$ is flat for all s.

2. Generic flatness:

   Proposition 6.8: pr:generic-flatness For X, Y nonempty, if either

   - $f : X \to Y$ is of finite type, and Y is integral and locally noetherian, or
   - $X \to Y$ is of finite presentation and Y is integral,

   then there exists nonempty $U \subseteq Y$ open dense such that

   $$f|_{f^{-1}(U)} : f^{-1}(U) \to Y$$

   is flat.

These theorems are stated in EGA. In fact, fiberwise and generic flatness are two of the most often cited facts from EGA. If it's flat extension, then already flat before taking the ff base extension. Spec $\overline{k(s)} \to$ Spec $k(s)$ is faithfully flat so it's okay.

In our case, A_s and A'_s are locally noetherian, A'_s is a variety, so integral, and $A_s \to A'_s$ is of finite type. Hence we can apply item 2 to see that $f_s : A_s \to A'_s$ is flat for an open dense subset of A_s. Using group translation, we find that f_s is flat. Why can't we work with A?

Figure 3

□

We now give examples of isogenies.

Example 6.9 (Multiplication by n)**:** Multiplication by n is an isogeny:

$$\begin{aligned}[n] : A &\to A \\ x &\mapsto \underbrace{x + \cdots + x}_{n}.\end{aligned}$$

This is not obvious; we will prove it later.

Example 6.10 (Quotient scheme)**:** Let A be an abelian variety, and H be a finite locally free subgroup scheme of A. $A \to A/H$ is surjective, flat and finite by Theorem 3.1, it is an isogeny.

Example 6.11 (Frobenius map)**:** In characteristic p, the relative Frobenius map

$$\text{Frob} : A \to A^{(p)} = A \times_S S$$

is an isogeny, where in the right the map $S \to S$ is the Frobenius map given as follows: Frob : $S \to S$ is the identity on topological space and maps $x^p \leftarrow\!\shortmid x$. We will check later (Example 16.1) that this is an isogeny.

For L an ample line bundle we have a map $\phi_L : A \to A^\vee$. We'll see later that this is an interesting isogeny.

Lemma 6.12: lem:787-6-2 Let $f : A \to A'$ be an isogeny. Then $\ker f$ is a finite locally free (commutative) group scheme over S.

Thus the example of $A \to A/H$ illustrates is a general phenomenon: the kernel is always a nice group scheme.

Proof. To see that $\ker f$ is finite, note that the kernel is given by the following fiber product.

$$\begin{array}{ccc} \ker f & \longrightarrow & A \\ \downarrow & & \downarrow{\scriptstyle f'} \\ S & \xrightarrow{e_{A'}} & A' \end{array}$$

Finiteness and flatness are stable under basechange, so the fact that the right-hand map is finite flat means the left-hand map is finite flat. Thus $\ker f$ is finite flat over S. □

Fact 6.13: If X, Y are locally of finite presentation over S, then $X \to Y$ is locally of finite presentation.

$$\begin{array}{ccc} X & \longrightarrow & Y \\ & {\scriptstyle \text{lfp}}\searrow \quad \swarrow{\scriptstyle \text{lfp}} & \\ & S. & \end{array}$$

Then X is finite flat over S iff it is finite and locally free over S.

Proof. The strategy is the same as that for properness: Use the diagonal morphism $Y \to Y \times Y$, which is locally of finite presentation. See Hartshorne [2, Exercise 4.8e]. □

Lecture 7
Thu. 9/27/12

§1 Isogenies

Recall the definition of an isogeny: a morphism $f : A \to A'$ in (Ab/S) is an **isogeny** if f is quasi-finite and surjective on points.

We showed f quasi-finite and surjective is equivalent to f being finite faithfully flat (Lemma 6.4). Note the second set of conditions is can be checked fiberwise, hence is easier to work with. In particular, f is an isogeny iff $f_s : A_s \to A'_s$ is isogeny for all $s \in S$, where $A_s := A \times_S \operatorname{Spec} k(s)$.

Equivalently to f being quasi-finite, $\ker f$ is quasi-finite over S. Indeed, if we knew every fiber over 0 were finite, then by group translation the fiber over every point is finite.

Moreover, the fact that f is an isogeny implies $\ker f$ is a finite flat locally free commutative group scheme over S (Lemma 6.12). We see that finite flat group schemes arise naturally in this context.

We would like a notion of rank or dimension for abelian schemes.

Definition 7.1: Define the function $\mathrm{rank} : S \to \mathbb{Z}_{\geq 0}$ by mapping $s \mapsto \mathrm{rank}(\ker f_s)$.

The rank is locally constant in the topological sense. If S is connected, then the rank is constant. It is natural to ask: what does an isogeny do the the rank?

It is clear that the composition of two isogenies is an isogeny and an isomorphism is an isogeny. We'll now show an isogeny preserves a natural invariant in geometry, the dimension.

Definition 7.2: We say $A \in (\mathrm{Ab}/S)$ has **relative dimension** $d \in \mathbb{Z}_{\geq 0}$ over S if for all $s \in S$, $\dim A_s = d$.

As a reminder, the dimension is the maximum length of closed subsets on the scheme, or the dimension of the corresponding ring in the sense of Krull dimension.

Note that the dimension may not be defined, For instance if A_1 has relative dimension 1 over S_1 and A_2 has relative dimension of dimension 2 over S_2. Then $A = A_1 \coprod A_2$ over $S = S_1 \coprod S_2$ does not have a dimension.

Definition 7.3: An **elliptic curve** is an abelian variety of dimension 1.

Lemma 7.4: let $f : A \to A'$ be an isogeny. For all $s \in S$, $\dim A_s = \dim A'_s$.

Proof. Let's import the following fact.

Lemma 7.5: lem:787-7-1 For varieties X and Y over a field k, if $\phi : X \to Y$ is an open morphism then for all $y \in \phi(X)$, $\dim \phi^{-1}(y)$ is the same. In fact,

$$\dim X = \dim Y + \dim \phi^{-1}(y).$$

Proof. See [1, Th. 14.114 and Pr. 14.102]. □

Reduce to the case where $S = \operatorname{Spec} k$ and apply to $f : A \to A'$ varieties over k. Then f is quasi-finite; it is open because it is flat and locally of finite presentation ([1][Th. 14.33]). Now $\dim f^{-1}(y) = 0$ because f is quasi-finite. Thus we get $\dim A = \dim A'$. □

What about the converse? If the dimensions are the same, can we say that the map is an isogeny? We'll need some more conditions.

Lemma 7.6: lem:787-7-2 Let $f : A \to A'$ be a morphism in (Ab/S). Assume $\dim A_s = \dim A'_s$ for all $s \in S$. Then the following are equivalent.

1. f is an isogeny.
2. f is quasi-finite.
3. f is surjective.

Recall f is an isogeny if it is quasi-finite and surjective. This lemma says that if the dimensions are the same, we can just check one of the conditions.

Proof. Since (1) is by definition just (2) and (3) combined, it suffices to prove (2) $\iff$ (3).

Reduce to the case where $S = \operatorname{Spec} k$.

Let $B := \overline{f(A)} \subseteq A'$ where $f(A)$ is the scheme-theoretic image of A and A' is irreducible containing $\overline{f(A)}$. We have

$$eq : 787 - 7 - 1 \quad \dim B = \dim A' \iff B = A' \text{ as a set} \iff f(A) = A' \tag{10}$$

because f is proper. (A morphism between two proper schemes is proper.)

Applying generic flatness 6.8 to $f : A \to B \subseteq A'$, we get that f is flat on the inverse image of an open dense subset $V \subseteq B$.

Note $f^{-1}(V) \neq \phi$ because f has dense image in B. Because f on $f|_{f^{-1}(V)}$ is flat and locally of finite presentation, it is open. (Why?) This means we can apply our imported result 7.5.

We have the following chain of equivalences.

1. f is quasi-finite (on one fiber, or on all fibers).
2. $\dim f^{-1}(V) = \dim V$. (To go between statements 1 and 2, use Lemma 7.5; quasifiniteness says $\dim f^{-1}(y) = 0$.)
3. $\dim A = \dim B$. (Note $\dim A = \dim f^{-1}(V)$ and $\dim B = \dim V$ because these are open dense subsets.)
4. f is surjective. (To go between 3 and 4, use (10).)

□

Now for an application.

Example 7.7: To check the relative Frobenius map Frob : $A \to A^{(p)} = A \times_S S$ (where $S \to S$ is given by the Frobenius map) and $[n] : A \to A$ are isogenies, we can work over an algebraically closed field (if a morphism is quasi-finite over a field extension, then it is already quasi-finite before base extension) and check it is either quasi-finite or surjective.

We summarize how we can check a morphism f is an isogeny.

Checking that f is an isogeny can be checked fiberwise. To check quasi-finiteness, we can just check the fiber over 0, i.e., check $\ker f$ is quasi-finite over S. Moreover, if the fibers of A, A' have the same dimension, it suffices to check just either surjectivity or quasi-finiteness.

§2 Motivation: Classification

We'll give some motivations, and then talk about line bundles.

When we're studying any type of geometric objects, the first problem is that of classification. We want to classify abelian varieties in some sensible manner.

1. Let A be an abelian scheme. We will assume that $A[n] := \ker[n]$ is quasi-finite over S. Then $A[n]$ is a finite locally free commutative group scheme over S by Lemma 6.12. Hence a good first step is to study or classify finite locally free commutative group scheme over S.

Of particular interest to us is the case $S = \operatorname{Spec} k$ (or the Spec over a ring of mixed characteristic such as $\mathbb{Z}_p$). Regarding $A[n]$, we could work with one prime at a time, by considering the p-power torsion of the group schemes:

$$A[p^\infty] = \bigcup_{n \geq 1} A[p^n]$$

over S. More precisely, interpret the RHS as a directed system $\varinjlim_n A[p^n]$. We call these objects **p-divisible groups**. p-divisible groups are simpler than abelian schemes, so we can study these objects first and then use them to classify abelian schemes.

For number theory, we can try $S =$ Spec of $\mathbb{F}_{p^r}$, $\overline{\mathbb{F}_p}$, $\mathbb{Z}_p$, $\mathbb{W}(\overline{\mathbb{F}_p})$, and then $\mathbb{Q}_p$, $\overline{\mathbb{Q}_p}$, $\mathbb{Q}$, and $\overline{\mathbb{Q}}$. We're interested in rational points of abelian varieties over number fields; this is still a mysterious topic and we don't know much.

Let's look at the classification problem from a different perspective. By introducing isogenies, we can go about classification as follows.

1. The dimension is invariant, so let's fix the dimension.
2. An isogeny gives an equivalence relation. We classify isogeny classes within each dimension.

3. An isogeny is strictly weaker than isomorphism. Thus we now classify isomorphism classes within each isogeny class.

Related to problem 2 is

2′. Classify isogeny classes of p-divisible groups.

It's easier solve the related problem for p-divisible groups: The theory is already very rich here. Then we can use the solution for p-divisible groups to solve the problem for abelian varieties.

We could also study $\mathrm{Hom}(A, B)$, $\mathrm{Isog}(A, B)$, and so forth (and do the same for p-divisible groups, etc.).

Example 7.8: Let the dimension be $d = 1$, and $S = \operatorname{Spec} \overline{\mathbb{F}_p}$. Then A is an elliptic curve over $\overline{\mathbb{F}_p}$. We classify according to the isogeny type of $A[p^\infty]$. We have exactly 2 possibilities, corresponding to 2 isogeny classes:

1. A is **ordinary** if (as a group)
$$A[p](\overline{\mathbb{F}_p}) \cong \mathbb{Z}/p\mathbb{Z}.$$
2. A is **supersingular** if
$$A[p](\overline{\mathbb{F}_p}) \cong \{0\}.$$

The isogeny class determine many properties of the elliptic curve.

If we consider isogeny types over A itself, we get a much richer theory.

§3 Line bundles

Let's study line bundles over abelian varieties. (It's easier to work with Spec of a field.)

We will talk about the following.

1. Abelian varieties are projective over fields, Theorem 9.4. (To prove projectivity we need to find ample line bundles.)
2. Duality theory: This imposes a strict condition on what the torsion group scheme should be.
3. Polarization
4. As a byproduct we'll see that $[n]$ is an isogeny.

We're entering Mumford [4, §6]. We'll try to just work over fields, rather than algebraically closed fields as Mumford does.

Theorem 7.9 (Theorem of the cube)**:** thm:cubeLet X and Y be proper varieties over k and Z be a variety over k. Let $x \in X$, $y \in Y$, and $z \in Z$ be scheme-theoretic points. Let L be a line bundle over $X \times_k Y \times_k Z$. If $L|_{\{x\}\times Y\times Z}$, $L|_{X\times\{y\}\times Z}$, and $L|_{X\times Y\times\{z\}}$ are trivial, then L is trivial. (By $\{x\} \times Y \times Z$ we mean the pullback of the line bundle along the closed immersion $\{x\} \times Y \times Z$, and so forth.)

We'll postpone the proof and treat this theorem as a black box for now.

Corollary 7.10: Let $A \in (\mathrm{Ab}/k)$ where k is any field. Define the maps

$$\begin{array}{ccc} A \times_k A \times_k A & \longrightarrow & A \\ (x_1, x_2, x_3) & \overset{\substack{p_{123} \\ p_{ij}}}{\longmapsto} & x_1 + x_2 + x_3 \\ & \overset{p_i}{\searrow} & x_i + x_j \\ & & x_i. \end{array}$$

Then $\Theta(L) := p_{123}^* L \otimes \left(\bigotimes_{i<j} p_{ij}^* L^{-1}\right) \otimes \left(\bigotimes_i p_i^* L\right)$ is trivial.

We try to restrict this line bundle to subschemes of the form $\{x\} \times X \times Y$ and show it's trivial. For x we choose the natural distinguished point—the identity. Then by the Theorem of the Cube we can get the line bundle to be trivial over the triple product.

Proof. We show that $\Theta(L)|_{\{e_A\}\times A\times A}$ is trivial (Restrict to $x_1 = 0$ part), and show the same for the other restrictions.

We will compute $i_{23}^*\Theta(L)$, where $i_{23} : \{e_A\} \times A \times A \hookrightarrow A \times A \times A$ is the obvious inclusion.

For example, to compute $i_{23}^* p_{123}^* L = (p_{123} \circ i_{23})^* L$, note we have the commutative diagram

$$\begin{array}{ccc} \{e_A\} \times A \times A & \hookrightarrow & A \times A \times A \\ & \overset{\substack{\mu \\ (x_2,x_3)\mapsto x_2+x_3}}{\searrow} & \downarrow{\scriptstyle p_{123}} \\ & & A \end{array}$$

Picture!

We can similarly compute the others, and cancel nicely! When restrict to $x_1 = 0$, $p_{123} = p_{23}$ cancel out, $p_{12} = p_2$ cancel out, $p_{13} = p_3$ cancel out, and $p_1 = 0$, so everything vanishes. □

Corollary 7.11: cor:787-7-2 Let $Y \in (\mathrm{Sch}/k)$ and $A \in (\mathrm{Ab}/k)$. Let $f_1, f_2, f_3 \in \mathrm{Hom}_{\mathrm{Sch}/k}(Y, A)$. Then define

$$\begin{aligned} f_{123} = f_1 + f_2 + f_3 &= p_{123} \circ (f_1, f_2, f_3) \\ f_{ij} = f_i + f_j &= p_{ij} \circ (f_1, f_2, f_3). \end{aligned}$$

(The image has group structure so can make sense of adding—map to $A\times A\times A$ and compose with p_{123}.) Let $L \in \mathrm{Pic}(A)$. Then

$$f_{123}^* L \otimes \left(\bigotimes_{i<j} f_{ij}^* L^{-1}\right) \otimes \left(\bigotimes_i f_i^* L\right)$$

is trivial.

Proof. This equals $(f_1, f_2, f_3)^*\Theta(L)$ so it is trivial by the previous corollary. □

Corollary 7.12: cor:787-7-3 We have $[n]^*L = L^{\otimes \frac{n(n+1)}{2}} \otimes [-1]^*L^{\otimes \frac{n(n-1)}{2}}$ where A and L are as before.

Proof. The idea is to use Corollary 7.11 along with induction.

Apply the corollary to $f_1 = [n]$, $f_2 = [1]$ (the identity map), and $f_3 = [-1] := i_A$. (Note $[n]$ is defined for all $n \in \mathbb{Z}$.) We get that

$$[n]^*L \otimes ([n+1]^*L^{-1} \otimes [n-1]^*L^{-1} \otimes \underbrace{[0]^*L^{-1}}_{\text{trivial}}) \otimes [n]^*L \otimes \underbrace{[1]^*L}_{L} \otimes [-1]^*L \text{ is trivial.}$$

In $\mathrm{Pic}(A)$, we have $[n+1]^*L - 2[n]^*L + [n-1]^*L = L + [-1]^*L$. Use induction (plug in $n = 1, 2, 3, \ldots$ and $-1, -2, -3, \ldots$) to get the result. □

Lecture 8
Tue. 10/2/12

§1 Line bundles on abelian varieties

Recall last time we used Corollary 7.11 to prove Corollary 7.12, which tells us how the multiplication-by-n map acts on line bundles in $\mathrm{Pic}(A)$.

Definition 8.1: We say that L is **symmetric** if $[-1]^*L \cong L$, and **anti-symmetric** if $[-1]^*L \cong L^{-1}$.

Note that Corollary 7.12 says that

$$[n]^*L = \begin{cases} n^2 L, & L \text{ is symmetric} \\ nL, & L \text{ is anti-symmetric} \end{cases}$$

If L is any line bundle, then we can easily produce a symmetric and antisymmetric line bundle:

$$L \otimes [-1]^*L \text{ is symmetric}$$
$$L \otimes [-1]^*L^{-1} \text{ is anti-symmetric}$$

Corollary 8.2: cor:[n]=isogeny Let $A \in (\mathrm{Ab}/k)$ satisfy the following hypothesis.

- A has a ample line bundle.[9]

[9] Equivalently, A is projective over k, rather than just proper.

Then $[n] : A \to A$ is an isogeny.

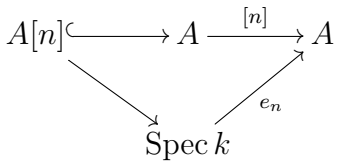
Later, we will show that the hypothesis is always satisfied. Here, projectivity helps us because it allows us to use facts about ample line bundles.

Proof. Since $[n]$ is a map between abelian schemes of the same dimension, it suffices to show either $[n]$ is quasi-finite or $[n]$ is surjective (Lemma 7.5). We will show that $\ker[n] := A[n]$ is quasi-finite over k.

We make the following observations.

1. $[n]^*$ is ample: Because L is ample, $[-1]^*L$ is ample (automorphisms preserve line bundles). Because the tensor product of ample line bundles is ample, using Corollary 7.12 we get $[n]^*L$ is ample.

2. $[n]^*L|_{A[n]}$ is trivial: We have that following commutes



   So pulling back by $[n]$ is the same as pulling back to $\operatorname{Spec} k$ and then to $A[n]$. $\operatorname{Spec} k$ has trivial Picard group, so the pullback of L to $\operatorname{Spec} k$ is trivial.

3. $[n]^*L|_{A[n]}$ is ample: The pullback of an ample line bundle via an immersion is ample.

4. We use the following fact.

   Fact 8.3 (Line bundle criterion for finiteness)**:** fct:787-8-1 Let X be a proper variety over k. Let L be an ample and trivial line bundle on X. Then $\dim(X) = 0$.

   Proof. If the dimension is positive, can choose line bundle with trivial sections. Since L is ample, tensoring a high power of it should give a lot of sections. But becase L is trivial, doesn't do anything. Can't produce more sections, contradiction. □

   Now apply this to $[n]^*L|_{A[n]}$.

□

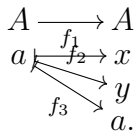
Corollary 8.4 (Theorem of the Square)**:** cor:squareLet $A \in (\mathrm{Ab}/k)$ and let L be a line bundle over A. Let $T_x : A \to A$ be given by $y \mapsto x + y$. Then the following hold.

1. Let $x, y \in A(k)$. Then
$$T_{x+y}^*L \otimes L \cong T_x^*L \otimes T_y^*L.$$

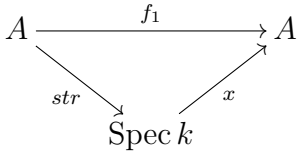
2. Suppose $x, y \in A(T)$, and $T \in (\mathrm{Sch}/k)$. Then
$$T_{x+y}^* L \otimes L \cong T_x^* L \otimes T_y^* L \otimes p_2^*(\text{stuff}).$$
where T_x is given by
$$\begin{aligned} A \times_k T &\xrightarrow{T_x} A \times_k T \\ (a, t) &\mapsto (a + x(t), t) \end{aligned}$$
and p_2 is the projection $A \times_k T \to T$.

Note (1) is just a special case of (2).

Proof. Apply Corollary 7.11 to the maps



where $f_{123} = T_{x+y}$, $f_{13} = T_x$, $f_{23} = T_y$, and $f_3 = \mathrm{id}_A$, i.e., f_1 is the map such that



commutes, and similarly for f_2. The corollary gives us that
$$f_{123}^* L \otimes f_3^* L \cong f_{13}^* L \otimes f_{23}^* L \otimes (\cdots)$$
In the case of (1), the last term is trivial. (2) is left as an exercise. (In this case the last term is not necessarily trivial.) □

As a consequence of Corollary 8.4, the map $\phi_L : A(k) \to \mathrm{Pic}(A)$ given by $x \mapsto T_x L \otimes L^{-1}$ is a group homomorphism. It is easy to check $\phi_{L_1 \otimes L_2} = \phi_{L_1} + \phi_{L_2}$ where the addition on the RHS is in $\mathrm{Pic}\, A$.

Taking $y \in A(k)$ we have $\phi_{T_y^* L} = \phi_L$ by Corollary 8.4. This is because
$$\begin{aligned} \phi_{T_y^* L}(x) &= T_x^*(T_y^* L) \otimes (T_y^* L)^{-1} \\ &= (\underbrace{T_y \circ T_x}_{T_{x+y}})^* L \otimes (T_y^* L)^{-1} \\ &= (T_x^* L \otimes T_y^* L \otimes L^{-1}) \otimes (T_y^* L)^{-1} \qquad \text{by Theorem of the Square 8.4} \\ &= T_x^* L \otimes L^{-1} = \phi_L(x). \end{aligned}$$

Next time we'll upgrade ϕ_L from a group homomorphism to a morphism of group schemes (on the left-hand side we would consider A as a scheme, and on the right-hand side we can give $\mathrm{Pic}(A)$ the structure of a scheme, called the Picard scheme of A). We will make sense of the kernel $K(L)$ as a closed subgroup scheme of A.

§2 Seesaw Theorem and $K(L)$

We will need the Seesaw Theorem to make sense of $K(L)$ as a subgroup scheme.

In Mumford, the Seesaw Theorem is used to prove the Theorem of the Cube. It is easier to understand the Seesaw Theorem using the theory of Picard schemes (which we'll take as a black box for now).

Theorem 8.5 (Seesaw Theorem)**:** thm:seesaw Let X be a proper variety over k, Y a scheme over k, and $\mathscr{L}$ a line bundle over $X \times_k Y$. Then there exists a unique closed subscheme $Y_0 \subseteq Y$ such that

1. $\mathscr{L}|_{X\times Y_0} \cong p_2^* M$ for some $M \in \mathrm{Pic}(Y_0)$. (I.e., the restriction is trivial on X.)
2. For all $f : T \to Y$ such that $(1_X \times f)^* \mathscr{L} \cong p_2^* K$ for some $K \in \mathrm{Pic}(T)$,

$$\begin{array}{ccc} X \times_k T & \xrightarrow{1_X \times f} & X \times_k Y \\ & \searrow^{p_2} & \\ & & T, \end{array}$$

there exists a unique map $T \to Y_0$ making the following commute

$$\begin{array}{ccc} T & \longrightarrow & Y \\ & \overset{\exists!}{\searrow} & \uparrow \\ & & Y_0 \end{array}$$

Moreover, for any scheme T over k,

$$eq : 787 - 8 - 1 Y_0(T) = \{f \in Y(T) : (1_X \times f)^* \mathscr{L} \cong p_2^* M \text{ for some } M \text{ over } T\}. \qquad (11)$$

Why is this called Seesaw?

Think of item 2 as saying that Y_0 is the largest closed subscheme of Y such that $\mathscr{L}|_{X\times Y_0}$ is $p_2^*(M)$ for some $M \in \mathrm{Pic}(Y_0)$.

There are two interesting applications of the Seesaw Theorem.

1. Proof of Theorem of the Cube. (See [4, §6].)
2. Definition of $K(L) \subseteq A$ as a closed subgroup scheme, such that

$$K(L)(k) = \ker \phi_L.$$

Remark: The Seesaw Theorem gives the Theorem of the Cube with its corollaries. The Theorem of the Cube and the Seesaw Theorem give the definition $K(L) \subseteq A$ as a closed subgroup scheme. The definition of $K(L)$ then means that for L ample we can define the dual abelian scheme

$$A^\vee := A/K(L).$$

In this way we can avoid the big theory of Picard schemes; we can show that with this definition $A^\vee$ satisfies properties that we expect a moduli space to satisfy.

Then $\phi_L : A \to A^\vee$ is just the quotient map. We do have to check we get the same object for different choices of L.

Alternatively, if you accept the theory of Picard schemes as in [7], we get the Seesaw Theorem and the Theorem of the Cube as before. Now directly from the theory of Picard schemes, we get $A^\vee = \mathrm{Pic}^0(A)$, $\phi_L : A \to A^\vee$, and then we define $K(L) := \ker \phi_L$.

We'll talk about both approaches.

We can apply the Seesaw Theorem 8.5 to $X = Y = A \in (\mathrm{Ab}/k)$ and the "Mumford" line bundle $\mathscr{L} = \mu^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$, where $p_1, p_2, \mu : A \times A \to A$ are the projection and multiplication maps. We get a closed subscheme $K(L) \subseteq A$ satisfying the property

$$K(L)(T) = \{x \in A(T) : (1_A \times x)^* \mathscr{L}\} = p_2(\mathscr{L}).$$

What's not clear yet is that this is a sub*group* scheme. We will use the Theorem of the Cube to show this.

Lemma 8.6: $K(L) \subseteq A$ is a closed subgroup scheme.

Proof. There is another way to describle the T-points of $K(L)$.

Claim 8.7: clm:787-8-1

$$K(L)(T) = \left\{x \in A(T) : T_x^* L_T \otimes L_T^{-1} \cong p_2^*(M) \text{ for some line bundle } M \text{ over } T\right\}.$$

Here, $L_T := p_1^* L$ where $p_1 : A \times T \to A$ is the projection.

We now show that if the claim is true then $K(L)(T)$ is a *group* scheme by the Theorem of the Square, so $K(L)(T)$ is a sub*group* scheme.

For $x, y \in K(L)(T)$, we have by the Theorem of the Square 8.4 that

$$\begin{aligned} T_{x+y}^* L_T \otimes L_T^{-1} &\cong (T_x^* L_T \otimes L_T^{-1}) \otimes (T_y^* L_T \otimes L_T^{-1}) \\ &= p_2^*(M_1) \otimes p_2^*(M_2) \cong p_2^*(M_1 \otimes M_2) \end{aligned}$$

for some M_1, M_2. Thus $x + y \in K(L)(T)$. That $x \in K(L)(T)$ implies $-x \in K(L)(T)$ is left as an exercise.

It remains to show that the condition on $\mathscr{L} = \mu^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$ in 11 gives the condition on L in Claim 8.7.

Proof of Claim 8.7. It suffices to prove that $(1_A \times x)^* \mathscr{L}$ and $T_x^* L_T \otimes L_T^{-1}$ differ by $p_2^*(M)$ for some M.

We first verify that $(1_A \times x)^* \mu^* \mathscr{L} \cong T_x^* L_T$. We have

$$A \times T \xrightarrow{1_A \times x} A \times A \xrightarrow{\mu} A$$

$$\begin{aligned}(1_A \times x)^*\mu^* L &\cong (\mu(1_A \times x))^* L \\ &\cong (p_1 \circ T_x)^* L \qquad\qquad \mu \circ (1_A \times x) = p_1 \circ T_x \\ &\cong T_x^* p_1^* L \\ &\cong T_x^* L_T.\end{aligned}$$

Then

$$\begin{aligned}(1_A \times x)^*\mathscr{L} &= (1_A \times X)^*(\mu^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}) \\ &= (T_x^* L_T) \otimes \underbrace{(1_A \times x)^* p_1^* L^{-1}}_{L_T^{-1}} \otimes \underbrace{(1_A \times x)^* p_2^* L^{-1}}_{p_2^*(x^* L)^{-1}}.\end{aligned}$$

□

□

Lecture 9
Thu. 10/4/12

Today we will prove that abelian varieties are projective. Recall that a scheme X over S is **projective** if it factors as $X \hookrightarrow \mathbb{P}^n_S \to S$ where the first map is a closed immersion. A scheme X is projective if and only if we can find an ample invertible sheaf on X (see Hartshorne, [2, §II.7], specifically Theorem II.7.6). We will prove projectivity by finding an ample invertible sheaf.

§1 Abelian varities are projective

Let k be a field and $A \in (\mathrm{Ab}/k)$. Let D be an effective divisor (you can think of D as a Weil divisor—sums of subvarieties of codimension 1—or a Cartier divisor—a global section of the sheaf of total quotient rings). Let $L := L(D)$ be the associated line bundle.

Set theoretically, define

$$H(D) := \left\{x \in A(\overline{k}) : T_x^* D = D\right\} \subseteq A(\overline{k}).$$

(Note the condition is equality, not equivalence in divisor class.) Here $T_x : A \to A$ is translation by x. To work scheme-theoretically, we equip $H(D)$ with the reduced closed subscheme structure of A. Note $H(D)$ is Zariski closed because the equality is a closed condition. Note it is also a sub*group* scheme; this is clear.

1.1 An equivalence

Proposition 9.1: pr:787-9-1 Assume $k = \overline{k}$. Let $f : A \to \operatorname{Spec} k$ be the structure map. Then the following are equivalent.

1. $H(D)$ is finite.
2. $K(L)$ is finite.
3. The linear system $|2D|$ has no basepoint and defines a finite morphism $A \to \mathbb{P}(f*L^{\otimes 2})$.
4. L is ample over A.

Here "finite" means either finite over $\operatorname{Spec} k$, or having dimension 0, or having finitely many points (the conditions are equivalent).

Remark: To show that an abelian variety is projective, we will use (i) $\implies$ (iv). In practice we most often use (ii) $\implies$ (iv).

Proof. We show that (ii) $\implies$ (i) $\implies$ (iii) $\implies$ (iv) $\implies$ (ii).

For (ii) $\implies$ (i), just note $H(D) \subseteq K(L)$. This is because $H(D)$ is the set of D such that T_x^*D, and $K(L)$ is the set of L such that $T_x^*L \otimes L^{-1}$ is trivial (i.e. $T_x^*L \sim L$), which is a weaker condition.

We'll skip (i) $\implies$ (iii).

(iii) $\implies$ (iv) is standard.

(iv) $\implies$ (ii): The idea is to take the identity component. $K(L)$ is reduced closed subscheme but not necessarily connected. There will be finitely many connected components. The proof will comes down to showing that the identity component is trivial.

Let

$$Y := (K(L)^\circ)_{\text{red}} \subseteq A \,/k$$

($H(D)$ is reduced by definition, but $K(L)$ may not be.) We will show that Y is a point (i.e. has dimension 0). To do this, we show it's a subvariety, and then use ample line bundles.

Claim 9.2: Y is a sub-abelian variety of A.

Proof. We first show Y is a subgroup scheme of A. We know $K(L)$ is a subgroup scheme in A. It is equipped with the multiplication and inverse maps that are the restriction of the corresponding maps μ, i for A.

We need to show Y is stable under μ. We have the diagram

$$\begin{array}{ccccc}
 & & (K(L)\times K(L))^\circ_{\text{red}} & & \\
 & & \| & & \\
 & & Y\times Y & \hookrightarrow & K(L)\times K(L) \\
 & \swarrow & \downarrow & & \downarrow \mu \\
Y = (K(L)^\circ)_{\text{red}} & \hookrightarrow & K(L)^\circ & \hookrightarrow & K(L).
\end{array}$$

Because Y is connected, μ factors through $Y \times Y \to K(L)^\circ$. A map from a reduced scheme factors through the reduced version of the target (Hartshorne [2][Exer. II.2.3c]), so μ further factors through Y. The proof for i is similar.

Next we need to show Y is integral and proper over k. Because Y if locally of finite type and reduced over k, the smooth locus $Y_{sm} \neq \phi$ is open dense. Using group translation, we can propagate it to all of Y, so $Y_{sm} = Y$. Because Y is smooth and connected, it is irreducible. Because Y is smooth and irreducible, it is an integral variety. Now $Y \subseteq A$ is a closed immersion so Y is a proper variety over k. Thus Y is an abelian variety over k. □

What good is knowing this? We want to show $\dim(Y) = 0$ and Y reduces to a point, using the fact that there's a ample line bundle on A. To use the line bundle, we have to pull it back to Y and then use Fact 8.3. (Actually we will work with a line bundle on $A \times A$.)

We have the canonical map $i : Y \hookrightarrow A$, with $L|_Y := i^*L$ ample. Consider the map

$$eq : 787 - 9 - 1 j : Y \times Y \xrightarrow{\mathrm{id},i} Y \times Y \subseteq A \times Y \subseteq A \times K(L) \subseteq A \times A \tag{12}$$

that sends $y \mapsto (y, -y)$. Consider the Mumford line bundle

$$M(L) := \mu^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}.$$

We pull back the Mumford line bundle to Y and see what happens. Observe (we have $p_1 \circ (\mathrm{id}, i)$ is the identity, $p_2 \circ (\mathrm{id}, i)$ is the inverse map, and $\mu \circ (\mathrm{id}, i)$ is the trivial map)

$$j^* M(L) \cong L|_Y \otimes [-1]^* L_Y.$$

This is still ample, because the tensor product of ample sheaves is ample.

On the other hand, we claim the following.

Claim 9.3: thm:jML-trivial $j^*M(L)$ is trivial.

From the claim and ampleness of $j^*M(L)$, we by Fact 8.3 that $\dim(Y \times Y) = 0$ and $\dim(Y) = 0$. Hence $\dim K(L) = 0$ as well, i.e. (ii) holds.

Note we work with $M(L)$ because as we will see in the proof of Claim 9.3, it allows us to use the Seesaw Theorem.

Proof of Claim 9.3. We just compute the pullback. We might as well prove that the pullback to any intermediate step in (12) is trivial; we show it's already trivial when pulled back to $A \times K(L)$.

By definition of $K(L)$ in Seesaw Theorem 8.5,

$$eq : 787 - 9 - 2 M(L)|_{A \times K(L)} \cong p_2^* N \tag{13}$$

for some line bundle N over $K(L)$. We have the commutative diagram

$$\begin{array}{ccc} \{e_A\} \times K(L) & \xrightarrow{\varepsilon} & A \times K(L) \\ \cong \downarrow & & \downarrow p_2 \\ K(L) & \xrightarrow{\mathrm{id}} & K(L). \end{array}$$

Pull back (13) via ε to get

$$\varepsilon^*(\mu^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}) \cong \varepsilon^* p_2^* N \cong (p_2 \circ \varepsilon)^* N = N$$

because $p_2 \circ \varepsilon = \mathrm{id}$.

$$\begin{array}{ccc} K(L) & \xhookrightarrow{\varepsilon} & A \times K(L) \\ & & \downarrow{\scriptstyle p_2} \\ & & K(L). \end{array}$$

It suffices to show that the LHS is trivial. But what is it? We compute that it equals

$$(\mu \circ \varepsilon)^* L \otimes (p_1 \circ \varepsilon)^* L^{-1} \otimes (p_2 \circ \varepsilon)^* L^{-1}$$

which is trivial because $\mu \circ \varepsilon = p_2 \circ \varepsilon$ and $p_1 \circ \varepsilon$ is trivial. □

This finishes the proof of Proposition 9.1. □

1.2 Proof of Projectivity

We can now show that every abelian variety is projective over its basefield.

Theorem 9.4: thm:ab-var-proj An abelian variety over any field k is projective over k.

Proof. We can reduce to $k = \overline{k}$ without too much difficulty (see [3] or [7]).

Here's a cool fact which we'll justify later.

Fact 9.5: fct:787-9-1 Let X be a proper variety over k and $U \subseteq X$ be a (normal)[10] affine open subscheme. Then $D := X \backslash U$ is a divisor (its irreducible components have codimension 1).[11]

The fact lies at the heart of the proof because it gives us the ample line bundle we need.

As we've mentioned, to prove projectivity it is enough to produce an ample line bundle or divisor, because we obtain a very ample line bundle by taking a high power. By the equivalence in Proposition 9.1, L is ample iff $H(D)$ or $K(L)$ is finite. We will show construct a divisor D such that $H(D)$ is finite.

Choose U and D as above. We may assume that $0 \in U$ by translation. Recall that

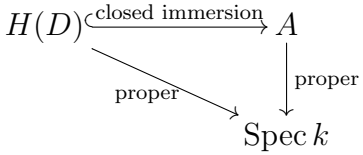
$$H(D)(\overline{k}) = \left\{ s \in A(\overline{k}) : T_x^* D = D \right\}.$$

The condition is equivalent to $T_x^* U = U$. Now $0 \in U$ implies $H(D) \subseteq U$. Now $x \in H(D)$ means that U is T_x-stable. We have this wonderful fact. Recall $H(D) \subseteq A$ is a closed

[10] This condition makes the fact easier to check. Without the condition it is still true (see EGA IV).

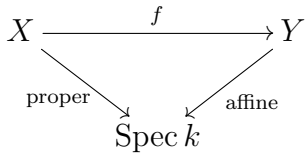
[11] Something like $\mathbb{A}^2 - \{(0,0)\}$ fails this criterion because it is not affine.

immersion (as it has the reduced closed subscheme structure) and $A \to \operatorname{Spec} k$ is proper, so $H(D) \to \operatorname{Spec} k$ is proper.



However it is very difficult for a proper scheme to live in an affine scheme.

Fact 9.6: fct:proper-to-affine Suppose $X \to \operatorname{Spec} k$ is proper, $Y \to \operatorname{Spec} k$ is affine, and $f : X \to Y$ is a morphism. Then the image of f is finite (0-dimensional).



The upshot is that $\dim H(D) = 0$ (finite), so L is ample and A is projective over k. □

Let's justify cool fact 9.5.

Proof. Let $X \backslash U = Z \cup Z'$. Assume Z has codimension at least 2 in X and Z' is closed. We want to show $Z = \phi$. We can reduce to the case where X and U are both affine.

Let $V \subseteq X \backslash Z'$ be the open affine neighborhood of the generic point for Z. Then $U \cap V \subseteq V$ is open and $U \cap V, V$ are affine. (The intersection of a separated affine subscheme and an affine subscheme is affine.) It is integral because X is integral (it is a variety) and these are open subsets of X. We use the following key fact from commutative algebra.

Fact 9.7 (18.705 notes, 23.11; [2], Pr. II.6.3A)**:** Let A be a noetherian integral domain. If A is normal iff $A = \bigcap_{\mathfrak{p} \text{ height } 1} A_{\mathfrak{p}}$. (The intersection is taken in $\operatorname{Frac}(A)$.)

Let $U \cap V = \operatorname{Spec} B$ and $V = \operatorname{Spec} A$. The complement of $U \cap V \subseteq V$ has codimension at least 2 in V. We have

$$\bigcap_{\mathfrak{p} \in U} A_{\mathfrak{p}} = A \subseteq B = \bigcap_{\mathfrak{p} \in U \cap V} A_{\mathfrak{p}} \overset{(*)}{\subseteq} \bigcap_{\mathfrak{p} \text{ height } 1} A_{\mathfrak{p}} = A$$

The middle inclusion (*) is from the fact that $U \backslash U \cap V$ has codimension at least 2. Then we have $B = A$, and hence $U \cap V = V$. This means $Z = \phi$. □

Consider $A \in (\mathrm{Ab}/k)$ where k is any field. Before, we assumed A was projective over k to prove that $[n] : A \to A$ is an isogeny (Corollary 8.2). But now we know that A is always projective, so $[n]$ is an isogeny for any abelian variety.

§2 Rank of $A[n]$

We now know $A[n]$ is a finite group scheme over k. It is natural to ask what the rank of $A[n]$ over k is.

$$\operatorname{rank}_k A[n] = ?$$

Mumford takes 2 approaches.

1. intersection theory,
2. cohomology of line bundles (or coherent sheaves). (Look at Hilbert polynomials; the rank pops out as the top degree coefficient.)

We'll sketch the first approach.

Choose an ample line bundle $L_0 = L(D_0)$ where D_0 is an effective ample divisor. We make it ample and *symmetric*:

$$L = L_0 \otimes [-1]^* L_0 \leftrightarrow D$$

(by this notation, we mean: suppose that L corresponds to D). For a symmetric line bundle we know that

$$[n]^* L \cong L^{\otimes n^2} \leftrightarrow [n]^* D = n^2 D.$$

(For D we use additive notation.) We now invoke the following theorem from intersection theory for proper varieties over k. We may assume $k = \overline{k}$.

Fact 9.8: Let $f : X \twoheadrightarrow Y$ be proper varieties of the same dimension g over k. Say $\deg f = [k(Y) : k(X)]$ where $D_1, \ldots, D_g$ are Cartier divisors. Then we have[12]

$$(f^* D_1 \cdots f^* D_g)_X = (\deg f)(D_1 \cdots D_g)_Y.$$

Now plug in $X = Y = A$ and $f = [n]$ to get

$$\underbrace{[n]^* D \cdots [n]^* D}_{g} = (\deg[n])(\underbrace{D \cdots D}_{g})$$

We have $n^2 D = [n]^* D$ so the LHS is $n^{2g}(D \cdots D) \neq 0$. Hence we get $\deg[n] = n^{2g}$. If $\operatorname{char} k \nmid n$, then this gives $\operatorname{rank}_k A[n] = 2g$.

We have shown the following.

Theorem 9.9 (Degree of multiplication-by-n map)**:** thm:deg-A[n] Let A be an abelian variety of dimension g over a field k. Then the following hold.

1. The multiplication-by-n map has degree
$$\deg[n] = n^{2g}.$$
2. If $\operatorname{char} k \nmid n$ then $\operatorname{rank}_k A[n] = 2g$ and $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

[12] See [2][Ex. II.6.6.2] for definitions of the intersection divisor.

Lecture 10
Thu. 10/11/12

Last time we showed that abelian varieties over a field k are projective by exhibiting an ample line bundle. If we have an abelian scheme over S of relative dimension g, we showed that $A[n]$ is finite locally free subgroup scheme over S of A of rank $2g$ (Theorem 9.9). We reduced to the case of fields, then to the the case of algebraically closed fields, and finally computed certain intersection numbers given by ample divisors.

Today we'll start a new topic.

§1 Picard schemes

Recall that for $A \in (\mathrm{Ab}/k)$, we produced a group homomorphism

$$\begin{aligned} A(k) &\to \mathrm{Pic}(A) \\ x &\mapsto T_x^* L \otimes L^{-1}. \end{aligned}$$

where $\mathrm{Pic}(A)$ is the group of isomorphism classes of line bundles over A and T_x is translation by x. This was a group homomorphism by the Theorem of the Square 8.4.

We now upgrade this map to a morphism of group schemes. We'd like to give $\mathrm{Pic}(A)$ some geometric structure, and make it into a Picard scheme.

Definition 10.1: Let $X \in (\mathrm{Sch}/S)$. The **absolute Picard functor** is the functor

$$\begin{aligned} \underline{\mathrm{Pic}}_X : (\mathrm{Sch}/S) &\to (\mathrm{Gp}/S) \\ T &\mapsto \mathrm{Pic}(X \times_S T) = \left\{ \begin{matrix} \text{line bundles} \\ \text{over } X \times_S T \end{matrix} \right\} / \cong \end{aligned}$$

We are in the moduli space situation: We write down a functor, which we want to be represented by a scheme. Unfortunately, this functor is never representable by a scheme. To see this, note the following fact.

Fact 10.2 (Gluing morphisms)**:** Every scheme is a Zariski sheaf. For $Y \in (\mathrm{Sch}/S)$ and $T = \bigcup U_i \in (\mathrm{Sch}/S)$, the sequence

$$Y(T) \to \prod_i Y(U_i) \rightrightarrows \prod_{i,j} Y(U_i \cap U_j)$$

is exact. The left map is injective.

In other words, defining morphisms $U_i \to Y$ in a compatible is the same as giving a map from Y to T.

As the following shows, a Picard functor is not a Zariski sheaf, so it cannot be representable.

Example 10.3: Let $X = S$, suppose $\mathrm{Pic}(S) \neq (0)$ and take a fine enough covering $S = \bigcup U_i$. Consider

$$\underline{\mathrm{Pic}}_S(S) \to \prod_i \underline{\mathrm{Pic}}_S(U_i).$$

The LHS is just $\mathrm{Pic}(S)$. The factors in the RHS are $\mathrm{Pic}(U_i)$, which are trivial. (Invertible sheaves are trivialized if we choose a fine enough open covering.) Hence the map is not injective.

One way to deal with this is to define Picard stacks. However, we want to work within the category of schemes, so we need to use a different definition. To remedy our problem, we'll kill line bundles coming from S.

Definition 10.4: df:rel-pic Given $X \to S$, define the **relative Picard functor** by

$$\begin{aligned} \underline{\mathrm{Pic}}_{X/S} : (\mathrm{Sch}/S) &\to (\mathrm{Gps}) \\ T &\mapsto \mathrm{Pic}(X \times_S T)/p_2^* \mathrm{Pic}(T). \end{aligned}$$

where p_2 is the map $X \times_S T \to T$.

This is not the best definition but it works in many cases, including the case of abelian schemes.

If we make some additional hypotheses will be a good definition, i.e. $\underline{\mathrm{Pic}}_{X/S}$ will now be a Zariski sheaf.

- $f : X \to S$ is proper, flat, and has geometrically integral fibers, and there exists a section $e : S \to X$ so that $f \circ e = \mathrm{id}_S$.

In the more general case, if $\underline{\mathrm{Pic}}_{X/S}$ is not a Zariski sheaf, we want to sheafify it in some way. Sheafification in the Zariski topology is not enough; we have to use the étale or fppf topology (Grothendieck topologies). We get a better candidate which is theoretically more natural.

However, in the case of abelian schemes, the hypothesis holds, so the extra technology is not necessary.

Theorem 10.5: thm:pic-rep Under the above hypothesis, if $S = \mathrm{Spec}\, k$, then $\underline{\mathrm{Pic}}_{X/k}$ is representable by a group scheme over k that is locally of finite type (denoted $\mathrm{Pic}_{X/k}$).

If we want to work with finite objects, it's natural to work with the connected component or something slightly larger than the connected component. We write $\mathrm{Pic}^\circ_{X/k} := (\mathrm{Pic}_{X/k})^\circ$ to mean the connected component containing the identity.

Example 10.6: In the special case that X be a proper curve over k, we define this to be the **Jacobian**:

$$\mathrm{Jac}(X/k) = \mathrm{Pic}^\circ_{X/k}\,.$$

We now give a general definition over a scheme S.

Definition 10.7: Assume the hypothesis. Define

$$\underline{\mathrm{Pic}}^{\circ}_{X/S}(T) = \left\{ L \in \underline{\mathrm{Pic}}_{X/S}(T) : L_s \in \mathrm{Pic}^{\circ}_{X_s/k(s)}(T_s) \text{ for all } s \in S \right\}.$$

This is a subfunctor of $\underline{\mathrm{Pic}}_{X/S}$.
We have the following complement to Theorem 10.5.

Theorem 10.8: thm:pic0-rep If $\pi : X \to S$ is an abelian scheme, then $\underline{\mathrm{Pic}}^{\circ}_{X/S}$ is represented by an abelian scheme.

We'll use this theorem as a black box.

Definition 10.9: Call the scheme representing $\underline{\mathrm{Pic}}^{\circ}_{X/S}$ the **dual abelian scheme** of X, and denote it by

$$\pi^{\vee} : X^{\vee} \to S.$$

Definition 10.10: Suppose $A \in (\mathrm{Ab}/S)$. Then

$$A^{\vee}(A^{\vee}) = \mathrm{Pic}^{\circ}_{A/S}(A^{\vee}) \subseteq \mathrm{Pic}_{A/S}(A^{\vee}) = \mathrm{Pic}(A \times_S A^{\vee})/p_2^* \mathrm{Pic}(A^{\vee}).$$

There is a distinguished element in the LHS, the identity morphism $\mathrm{id}_{A^{\vee}}$. Define the **Poincaré line bundle** $\mathcal{P}$ as the image of $\mathrm{id}_{A^{\vee}}$ on the RHS.

Lemma 10.11: lem:787-10-1 Suppose $A \in (\mathrm{Ab}/S)$, $T \in (\mathrm{Sch}/S)$. Suppose that under the inclusion

$$A^{\vee}(T) \subseteq \mathrm{Pic}(A \times_S T)/p_2^* \mathrm{Pic}(T),$$

y is sent to $L(y)$. Then

$$L(y) \cong (\mathrm{id}, y)^* \mathcal{P} \bmod p_2^* \mathrm{Pic}(T).$$

This is how an object is supposed to work in a moduli problem.

Proof. The map $T \to A^{\vee}$ induces

$$y^* : A^{\vee}(A^{\vee}) \to A^{\vee}(T)$$

given by precomposing with y. Because $\underline{\mathrm{Pic}}_{A/S}$ is a functor we have the commutative diagram

$$\begin{array}{ccc} A^{\vee}(A^{\vee}) & \hookrightarrow & \mathrm{Pic}(A \times A^{\vee})/p_2^* \mathrm{Pic}(A^{\vee}) \\ \downarrow{\scriptstyle y^*} & & \downarrow{\scriptstyle (\mathrm{id},g)^*} \\ A^{\vee}(T) & \hookrightarrow & \mathrm{Pic}(A \times T)/p_2^* \mathrm{Pic}(T). \end{array}$$

We have that $\mathrm{id} \in A^{\vee}(A^{\vee})$ is mapped as follows:

$$\begin{array}{ccc} \mathrm{id} & \hookrightarrow & \mathcal{P} \\ \downarrow{\scriptstyle y^*} & & \downarrow{\scriptstyle (\mathrm{id},g)^*} \\ y & \hookrightarrow & L(y). \end{array}$$

Thus $L(y) = (\mathrm{id}, y)^* \mathcal{P} \bmod p_2^* \mathrm{Pic}(T)$. □

Corollary 10.12 (Criterion for line bundle/T-points to be trivial)**:** The following are equivalent.

- The map $y : T \to A^\vee$ factors through $e_{A^\vee} : S \to A^\vee$.
- $L(y) = (\mathrm{id}, y)^*\mathcal{P}$ is trivial mod $p_2^* \operatorname{Pic}(T)$.

Proof. This follows from Lemma 10.11. □

§2 λ_L and $K(L)$

Recall the following notation. For $A \in (\mathrm{Ab}/S)$ we have maps

$$p_1, \mu, p_2 : A \times_S A \to A$$

and maps $\pi : A \to S$, $e_A : S \to A$.

Let $L \in \operatorname{Pic}(A)$. Consider the Mumford line bundle

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

We have because $\underline{\operatorname{Pic}}_{A/S}$ is represented by $\operatorname{Pic}_{A/S}$ that

$$\operatorname{Pic}(A \times_S A)/p_2^*(\operatorname{Pic}(A)) = \operatorname{Pic}_{A/S}(A) = \operatorname{Hom}_{(\mathrm{Sch}/S)}(A, \operatorname{Pic}_{A/S}).$$

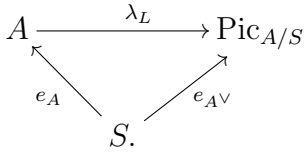
Definition 10.13: Define λ_L to be the image of $M(L)$ in $\operatorname{Hom}_{(\mathrm{Sch}/S)}(A, \operatorname{Pic}_{A/S})$.

A priori, an element of $\operatorname{Hom}_{(\mathrm{Sch}/S)}(A, \operatorname{Pic}_{A/S})$ is a morphisms of scheme, not necessarily of group schemes. We show an element corresponding to a line bundle is a morphism of group schemes.

Lemma 10.14: 1. λ_L is morphism of group schemes over S.

2. λ_L lands in $\operatorname{Pic}^\circ_{A/S} \subseteq \operatorname{Pic}_{A/S}$.

Proof. 1. By the rigidity lemma (specifically Corollary 5.14), a morphism which takes id to id is a group homomorphism. Thus it suffices to show λ_L takes the identity element to the identity element, i.e., the following commutes:



(?) What is the universal line bundle? Letting $\mathcal{P}$ be the universal line bundle over $A \times_S \operatorname{Pic}_{A/S}$, it suffices to prove $(\mathrm{id}, \lambda_L \circ e_A)^*\mathcal{P}$ is trivial mod $p_2^* \operatorname{Pic}(T)$. . We have

$$(\mathrm{id}_A, e_A)^* \underbrace{(\mathrm{id}_A, \lambda_L)^*\mathcal{P}}_{M(L)}.$$

We see compute $\mu(L)$. Get element of $p_2 p_{12}(T)$.

2. This follows because A is fiberwise geometrically connected.

The upshot is that for L a line bundle over A, we get a map $\lambda : A \to A^\vee$ in (Ab/S). $\square$

Definition 10.15: An isogeny $\lambda : A \to A^\vee$ in (Ab/S) is a **polarization** if for all $s \in S$,

$$\lambda_{\overline{s}} = \lambda \times_S \operatorname{Spec} \overline{k(s)}$$

is of the form $\lambda_{L(\overline{s})}$ for some ample line bundle $L(\overline{s})$ over $A_{\overline{s}}$. Implicit we identify $(A^\vee)_{\overline{s}} = (A_{\overline{s}})^\vee$.

A polarization is **principal** if it is an isomorphism.

Remark: A polarization λ is quasi-finite. To see this, note $L(\overline{s})$ is ample iff $\ker \lambda_{\overline{s}}$ is finite over $k(\overline{s})$. If $\ker \lambda_{\overline{s}}$ is finite over $k(\overline{s})$, then $\lambda_{\overline{s}}$ is quasi-finite. Since quasi-finiteness can be checked on fibers, this implies λ is quasi-finite.

The dual $A^\vee$ has the same or larger dimension as A.

§3 Duality

Here are natural questions.

1. Give $f : A \to B$ in (Ab/S), is there a dual morphism $f^\vee : B^\vee \to A^\vee$?
2. Is $\dim A = \dim A^\vee$? (relative dimension)
3. If f is an isogeny, is $f^\vee$ an isogeny? Is $\deg f = \deg f^\vee$?
4. Is there a canonical map $A \to (A^\vee)^\vee$ and is it an isomorphism? Is $(f^\vee)^\vee = f$ if we identify $A = (A^\vee)^\vee$
5. Is polarization an isogeny?
6. Is there a relationship between $\ker f$ and the *Cartier dual* $(\ker f)^\vee$? (A Cartier dual is the dual of a finite flat group schemes; we will define this in Lecture 12.)

We'll enhance our understanding of dual abelian varieties by answering these questions. We'll just give some partial answers today.

1. Given $f, T \in (\mathrm{Sch}/S)$, we have a map $\operatorname{Pic} B \times_S T \xrightarrow{f^*} \operatorname{Pic}(A \times_S T)$:

$$\begin{array}{ccc}
B^\vee(T) & \dashrightarrow & A^\vee(T) \\
\big\downarrow & & \big\downarrow \\
\operatorname{Pic}(B \times_S T)/p_2^*T & \xrightarrow{f^*} & \operatorname{Pic}(A \times_S T)/p_2^*T \\
\cup & & \cup \\
L & \longmapsto & f^*L
\end{array}$$

Thus we can define a map $B^\vee(T) \to A^\vee(T)$ making the above commute. Since B is fiberwise connected, we get a map

$$\begin{array}{ccc} B^\vee(T) & \xrightarrow{f^\vee} & A^\vee(T) \\ \big\downarrow & & \big\downarrow \\ \mathrm{Pic}^\circ_{B/S}(T) & \longrightarrow & \mathrm{Pic}^\circ_{A/S}(T) \end{array}$$

Note that (2) $\implies$ (5): Same dimension and quasifinite imply isogeny.

For (4), we construct a canonical map $A \to (A^\vee)^\vee$ as follows. We have

$$(A^\vee)^\vee(A) = \mathrm{Pic}^\circ_{A^\vee/S}(A) \subseteq \mathrm{Pic}(A^\vee \times_S A)/p_2^*A \ni \mathcal{P}.$$

We can check that $\mathcal{P}$ is actually in $\mathrm{Pic}^\circ_{A^\vee/S}(A)$. Then $\mathcal{P}$ is associated to a canonical map $K_A : A \to (A^\vee)^\vee$.

Lecture 11
Thu. 10/18/12

Today we'll continue talking about duality of abelian schemes (duality strikes back!).

This section is a mess. See Mumford [4, §13] or [7, §7.2].

§1 Complements on Pic

Last time we worked modulo p_2^* all the way. Today we'll give a slightly different but equivalent definition of Pic. Let $A \in (\mathrm{Ab}/S)$. To avoid confusion, write

$$\begin{aligned} \mathrm{Line}(A) &= \{\text{line bundles over } A\} \\ \mathrm{Pic}(A) &= \mathrm{Line}(A)/\cong . \end{aligned}$$

Definition 11.1: Define

$$\mathrm{Pic}_{e,A/S} : (\mathrm{Sch}/S) \to (\mathrm{Sets})$$

by mapping

$$T \mapsto \left\{ \begin{array}{c} (L, \varepsilon) : \ L \in \mathrm{Line}(A \times_S T) \\ \varepsilon : \mathscr{O}_T \xrightarrow{\cong} e_{A,T}^* L \end{array} \right\} / \cong$$

where $e_{A,T}$ is a section ($p_2 \circ e_{A,T} = \mathrm{id}_T$), e_A is a section ($f \circ e_A = \mathrm{id}_S$), and $p_1 \circ e_{A,T} = e_A \circ g$:

$$\begin{array}{ccc} A & \xleftarrow{p_1} & A \times_S T \\ {\scriptstyle e_A}\uparrow\big\downarrow{\scriptstyle f} & & {\scriptstyle p_2}\big\downarrow\uparrow{\scriptstyle e_{A,T}} \\ S & \xleftarrow{g} & T. \end{array}$$

Think of Definition 10.4 as the point variant of this definition. Here we put some condition. We can show that

$$\begin{aligned}\mathrm{Pic}_{e,A/S} &\cong \mathrm{Pic}_{A/S}\\ (L,\varepsilon) &\mapsto L.\end{aligned}$$

$$T \mapsto \frac{\mathrm{Pic}(A \times_S T)}{p_2^* \mathrm{Pic}(T)}.$$

arbitrary line bundle, no chance such iso in general, bc L lots line bundles in generl. But can mod by $p_2^*\,\mathrm{Pic}(T)$ and go back.Careful in choose what want.

Recall that we defined a subfunctor $\mathrm{Pic}^\circ_{A/S}$. Let the image of $\mathrm{Pic}^\circ_{A/S}$ under the above isomorphism be $\mathrm{Pic}^0_{e,A/S}$. We can take either definition as the dual abelian scheme $A^\vee$ of A.

Our black-box theorem 10.8 tells us $A^\vee \in (\mathrm{Ab}/S)$. The definition was fiberwise: $\mathrm{Pic}^\circ_{A/S}$ is basically the bundles in the connected components of every fiber.

We have an isomorphism

$$A^\vee(A^\vee) \cong \mathrm{Pic}^\circ_{e,A/S}(A^\vee) = \left\{(L,\varepsilon) : L \in \mathrm{Line}(A \times_S A^\vee), \varepsilon : \mathscr{O}_{A^\vee} \xrightarrow{\cong} e^*_{A,A^\vee} L\right\}$$

sending id_A to $(\mathcal{P}_A, \varepsilon_A)$ where $\mathcal{P}_A$ is the Poincaré line bundle. ε is called a **rigidification**.

only way get line bundle on $A \times T$. $A \times T \to A \times A^\vee$. Identity on A and given map on T.

Now what is $f \in A^\vee(T)$ sent to under the isomorphism $A^\vee(T) \cong \mathrm{Pic}^\circ_{e,A/S}(T)$? We saw above what $\mathrm{id}_A \in A^\vee(A^\vee)$ got sent to under $A^\vee(A^\vee) \cong \mathrm{Pic}^\circ_{e,A/S}(A^\vee)$. Now the only way to get a line bundle on $A \times T \to A \times A^\vee$ is to use the map $A \times T \to A \times A^\vee$, which is the identity on A and the given map on T. This motivates the following lemma.

Lemma 11.2: We have that under the isomorphism $A^\vee(T) \cong \mathrm{Pic}^\circ_{e,A/S}(T)$, f is sent to $(1 \times f)^* \mathcal{P}_A$:

$$\begin{array}{ccc} A^\vee(T) & = & \mathrm{Pic}^\circ_{e,A/S}(T) \\ \| & & \\ \mathrm{Hom}_S(T, A^\vee) & & \cup \\ \cup & & \\ f & \longmapsto & (1 \times f)^* \mathcal{P}_A. \end{array}$$

Recall that given $f : A \to B$, we had an associated dual map $f^\vee : B^\vee \to A^\vee$. We also constructed a canonical map $K_A : A \to (A^\vee)^\vee$.

Problem 11.1: Show that if we have maps of abelian varieties $A \xrightarrow{f} B \xrightarrow{g} C$, then

$$(g \circ f)^\vee = f^\vee \circ g^\vee.$$

§2 Duality theorems

Let $A, B \in (\mathrm{Ab}/S)$ be of relative dimension g. Let $f : A \to B$ be a morphism.

Proposition 11.3: pr:787-11-1 Let A be an abelian variety of relative dimension g. Then

$$\dim(A) = \dim(A^\vee) = g.$$

Proposition 11.4: pr:787-11-2

1. If f is an isogeny, then $f^\vee$ is an isogeny.
2. $\deg f = \deg f^\vee$.
3. K_A is an isomorphism.

We have

$$(\mathrm{Ab}/S) \underset{\vee}{\overset{\vee}{\rightleftarrows}} (\mathrm{Ab}/S)^{\mathrm{op}}$$

giving that $\mathrm{id} \cong ((\bullet)^\vee)^\vee$.

Proof. Step 1 is to reduce to the case where $S = \operatorname{Spec} k$. Because A and $A^\vee$ are the same dimension by Proposition 11.3, it suffices to check $f^\vee$ is an isogeny fiberwise.

If know fiberwise isomorphism, then ?

For (3), check K_A is an isogeny fiberwise. Also $\ker K_A$ has rank 1, $\deg K_A = 1$. Why isogeny of degree 1 an isomorphism (exercise). This gives isomorphism

Problem 11.2: Exercise: An isogeny of degree 1 is an isomorphism. We have $\ker f \to S$ is locally free of rank 1. However we have a section:

$$\begin{array}{c} \ker f \\ {\scriptstyle e_A}\uparrow\downarrow \\ S \end{array}$$

Hence $\ker f \cong S$. Using this, one can show Algebra, locally free of rank 1, but already have copy of A, show rest is 0.

$$\begin{array}{c} B = A \oplus (\cdot) \\ \uparrow \\ A \end{array}$$

$(\cdot) = 0$.

We can now work over fields. When $S = \operatorname{Spec} k$, Then (L, ε), and (L, ε') are always related by an isomorphism. Hence we can forget about ε; only the existence of ε matters. (Exercise. Mumford §13) Isomorphism without specify. Pullback along id section trivial. □

Let's start the proof of Proposition 11.3. One proof uses cohomology of abelian varieties with line bundles as coefficients.

Proof of Proposition 11.3. We'll need 2 black boxes in our proof of Propositions 11.3 and 11.4.

Fact 11.5 (Black box 1, [4, §12.2])**:** fct:787-11-1 Let $A \in (\mathrm{Ab}/S)$ be of relative dimension 0. Then

$$\dim_k H^i(A, \mathscr{O}_A) = \binom{g}{i}.$$

In particular, there is no cohomology for $i > g$.

The proof involves a Koszul complex computation. It looks like a differential complex. The differential maps are all trivial. See Mumford for the construction of the complex.

We'll only need to use Fact 11.5 for H^1. Then Proposition 11.3 follows from the next proposition

Proposition 11.6: pr:787-11-1' $T_eA^\vee \cong H^1(A, \mathscr{O}_A)$ as k-vector spaces. ($T_eA^\vee$ is the tangent space at the identity.)

Because A is smooth, this implies $\dim A^\vee = g$. Now as k-vector spaces, letting $S = \operatorname{Spec} k[\varepsilon]/\varepsilon^2$,

$$\begin{aligned} T_eA^\vee &= \left\{\phi \in \operatorname{Hom}(\operatorname{Spec} k[\varepsilon]/\varepsilon^2, A^\vee) : \phi|_{\operatorname{Spec} k} = e_{A^\vee}\right\} \\ &= \ker(\operatorname{Pic}(A \times S)/p_2^* \operatorname{Pic}(k[\varepsilon]/\varepsilon^2) \to \operatorname{Pic}(A)/p_2^* \operatorname{Pic}(k) \\ &= \ker(H^1(A \times S, \mathscr{O}_{A\times S}^\times) \to H^1(A, \mathscr{O}_A^\times)) \end{aligned}$$

identifying Pic with H^1 cohomology (see Hartshorne [2, Exercise III.4.5]) and noting that $\operatorname{Pic}(k[\varepsilon]/\varepsilon^2)$ is trivial.

As a topological space, $A \times S = A$. To find the kernel of the above map, we form a long exact sequence.

$$1 \to 1 + \varepsilon\mathscr{O}_A \to \mathscr{O}_{A\times S}^\times \to \mathscr{O}_A^\times \to 1.$$

This is like looking at $R \otimes_k k[\varepsilon]/\varepsilon^2$. We get a long exact sequence

$$\begin{array}{ccccc} & & H^0(\mathscr{O}_{A\times S}^\times) & \twoheadrightarrow & H^0(\mathscr{O}_A^\times) \\ & \swarrow & & & \\ H^1(1+\varepsilon\mathscr{O}_A) & \longrightarrow & H^1(\mathscr{O}_{A\times S}^\times) & \longrightarrow & H^1(\mathscr{O}_A^\times). \end{array}$$

Note that as sheaves of abelian groups , we have an isomorphism

$$\mathscr{O}_A \xrightarrow{s} 1 + \varepsilon\mathscr{O}_A, \qquad a \mapsto 1 + \varepsilon a.$$

(This is just like a map $R \otimes_k k[\varepsilon]/\varepsilon^2 \to R$.)

We conclude that $H^1(A, \mathscr{O}_A) \cong T_eA^\vee$ as (abstract) groups. It is left as an exercise to upgrade this to an isomorphism as k-vector spaces. □

Now we give the proof of Proposition 11.4.

Proof. Again, we need some input from cohomology. Let $A \in (\mathrm{Ab}/k)$ and $L \in \mathrm{Line}(A)$. We define the Euler characteristic by

$$\chi(L) = \chi_A(L) := \sum_{i \geq 0} (-1)^i \dim H^i(A, L) \in \mathbb{Z}.$$

Studying the Euler characteristic is much easier than studying cohomology spaces, and it behaves nicely.

Fact 11.7 (Black box 2)**:** 1. We have that

$$\chi_{A \times A^\vee}(\mathcal{P}_A) = (-1)^g.$$

2. For $f : A \to B$ isogeny, $M \in \mathrm{Line}(B)$,

$$\chi_A(f^* L) = (\deg f) \chi_B(L).$$

This is proved in Mumford [4, §13.1–2]. In fact the cohomology is concentrated in degree g.:

$$H^i(A \times A^\vee, \mathcal{P}_A) = \begin{cases} k & \text{if } i = g \\ 0 & i \neq g. \end{cases}$$

Now recall the definition of $f^\vee : B^\vee \to A^\vee$. For all $T \in (\mathrm{Sch}/k)$ (or over S, in general), we defined $f^\vee$ to make the diagram below commute.

$$\begin{array}{ccccc} B^\vee(T) & = & \mathrm{Hom}(T, B^\vee) & \hookrightarrow & \mathrm{Pic}_e(B \times T) \\ \downarrow{\scriptstyle f^\vee} & & \downarrow{\scriptstyle f^\vee \circ (\bullet)} & & \downarrow{\scriptstyle (f \times 1)^*} \\ A^\vee(T) & = & \mathrm{Hom}(T, A^\vee) & \hookrightarrow & \mathrm{Pic}_e(A \times T). \end{array} \tag{14}$$

Notes

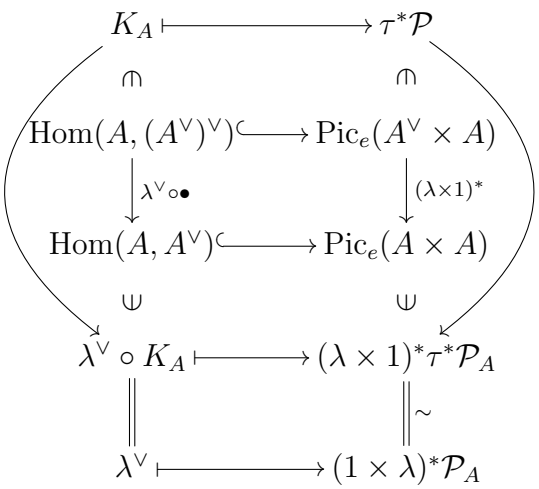
Lemma 11.8: lem:787-11-2 For all $\lambda : A \to A^\vee$, we have the commutative triangle

$$\begin{array}{ccc} A & \xrightarrow{K_A} & (A^\vee)^\vee, \\ & {\scriptstyle \lambda} \searrow \quad \swarrow {\scriptstyle \lambda^\vee} & \\ & A^\vee & \end{array}$$

i.e., $\lambda = \lambda^\vee \circ K_A$.

Proof. Plug into (14). We have $B = A^\vee$, $f = \lambda$, and $T = A$. □

Now we have a diagram



Corollary 11.9: If $\lambda : A \to A^\vee$ is an isogeny then $\lambda^\vee$ is an isogeny.

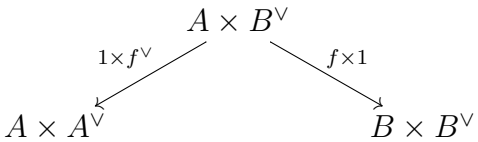
Proof. Since the dimensions of A and $A^\vee$ are the same, to show λ is an isogeny it suffices to show λ is surjective.

If λ is surjective, then $\lambda^\vee$ is also surjective by Lemma 11.8. □

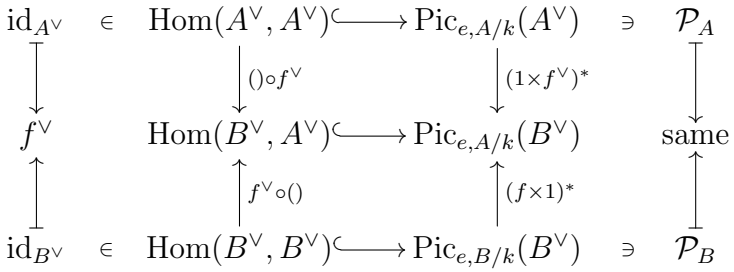
Lemma 11.10: lem:2poincare-bundle

$$(1\times f^\vee)^*\mathcal{P}_A \cong (f\times 1)^*\mathcal{P}_B.$$

where



We have $\mathcal{P}_A$ lives on the LHS and $\mathcal{P}_B$ lives on the RHS. We now have



Top comes from def pic, bottom from EQ. Same on rhs.

Corollary 11.11: If f and $f^\vee$ are isogenies, then $\deg f = \deg f^\vee$.

Proof. We have

$$\chi((1 \times f^\vee)^* \mathcal{P}_A) = \chi((f \times 1)^* \mathcal{P}_B).$$

The LHS is

$$\deg(1 \times f^\vee)\chi(\mathcal{P}_A) = \deg(f^\vee)\chi(\mathcal{P}_A)$$

while the RHS is

$$\deg(1 \times f^\vee)\chi(\mathcal{P}_B) = \deg(f)\chi(\mathcal{P}_B).$$

But $\chi(\mathcal{P}_A) = \chi(\mathcal{P}_B)$ (why) so $\deg f = \deg f^\vee$. □

Corollary 11.12: K_A is an isomorphism.

Proof.

$$\begin{array}{ccc} A & \xrightarrow{K_A} & (A^\vee)^\vee \\ & {\scriptstyle \lambda_L} \searrow \quad \swarrow {\scriptstyle \lambda_L^\vee} & \\ & A^\vee & \end{array}.$$

Choose an ample line bundle $L \in \mathrm{Line}(A)$. Then λ_L is an isogeny because $K(L)$ is finite over k. So $\lambda_L^\vee$ is an isogeny. K_A is also an isogeny, since $\ker K_A \subseteq \ker \lambda_L$. Now

$$\deg(\lambda_L) = \deg(\lambda_L^\vee \circ K_A) = \deg(\lambda_L^\vee)\deg(K_A)$$

think in terms of algebras, this is like B locally free rank m over A and C locally free rank n over B, then C locally free rank mn over A. Hence $\deg(K_A) = 1$, and K_A is an isomorphism. □

If remains the prove the following.

Lemma 11.13: If f is an isogeny, then $f\vee$ is an isogeny.

Remark: (maybe better) show $\ker f^\vee$ is Cartier dual $\ker f$.

Here's an exercise: The following commutes.

$$\begin{array}{ccc} A & \xrightarrow{K_A} & (A^\vee)^\vee \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle (f^\vee)^\vee} \\ B & \xrightarrow{K_B} & (B^\vee)^\vee \end{array}$$

I.e. "$f = (f^\vee)^\vee$". Since the across maps are iso, if f is an isogeny then f is surjective, $\dim A = \dim B$, $(f^\vee)^\vee$ is surjective. If $f^\vee : B^\vee \to A^\vee$ not isogeny then not surjective. Then $f^\vee(B^\vee) \subseteq A^\vee$, subabelian variety of dimension less than g. image proper group subvariety.

But dimension less than g can't surject to dimension g, contradiction.

$$B^\vee \to f^\vee(B^\vee) \to A^\vee$$

where $f^\vee(B^\vee)$ has dimension less than g.

$$(B^\vee)^\vee \leftarrow ()^\vee \leftarrow (A^\vee)^\vee$$

dim $< g$ in middle, $(f^\vee)^\vee$ surjective. dim g on left. Contradiction, end proof of Prop. 2. $\square$

Lecture 12
Tue. 10/23/12

sec:cartier

(I was absent today. Notes are borrowed from John Binder.)

Last time we proved duality results for abelian schemes over S. Given a morphism $f : A \to B$ in (Ab/S), we had morphisms

$$\begin{array}{ccc} & A \times B^\vee & \\ {\scriptstyle 1\times f^\vee}\swarrow & & \searrow{\scriptstyle f\times 1} \\ A \times A^\vee & & B \times B^\vee \end{array}$$

and we saw that the Poincaré line bundles on $A \times A^\vee$ and $B \times B^\vee$ are related by the following (Lemma 11.10):

$$(1 \times f^\vee)^* \mathcal{P}_A \cong (f \times 1)^* \mathcal{P}_B.$$

Theorem 12.1 (Poincaré reducibility)**:** thm:poincare-reducibility Suppose X is an abelian variety and Y is an abelian subvariety, $Y \hookrightarrow X$. Then there is an abelian subvariety $Z \hookrightarrow X$ such that the multiplication map

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

is an isogeny.

To prove this, we need the following lemma.

Lemma 12.2: lem:laf*l Let $L \in \mathrm{Line}(X)$ be a line bundle on an abelian variety X. Let $f : Y \to X$ be a morphism in (Ab/k). Then

$$\lambda_{f^*L} = f^\vee \circ \lambda_L \circ f.$$

In other words, the following diagram commutes.

$$\begin{array}{ccccccc} Y & \xrightarrow{f} & X & \xrightarrow{\lambda_L} & X^\vee & \xrightarrow{f^\vee} & Y^\vee. \\ & \searrow & & & & \nearrow & \\ & & & {\scriptstyle \lambda_{f^*L}} & & & \end{array}$$

Proof. The morphism λ_{f^*L} is characterized by

$$(1 \times \lambda_{f^*L})^* \mathcal{P}_Y \cong M(f^*L) := \mu^*(f^*L) \otimes p_1(f^*L)^{-1} \otimes p_2(f^*L)^{-1}.$$

We need to show that

$$(1 \times \lambda_{f^*L})^* \mathcal{P}_Y = (1 \times (f^\vee \circ \lambda_L \circ f))^* \mathcal{P}_Y,$$

which by Lemma 11.10 is equivalent to

$$(1 \times f)^* (1 \times \lambda_L)^* (1 \times f^*)^* = \mathcal{P}_Y \cong M(f^*L).$$

The left-hand side is

$$(1 \times f)^* \underbrace{(1 \times \lambda_L)^* \mathcal{P}_X}_{M(L)}.$$

and this is isomorphic to the RHS (exercise). Hint: The following commutes.

$$\begin{array}{ccc} Y \times Y & \xrightarrow{(f,f)} & X \times X \\ {\scriptstyle \mu_Y}\downarrow & & \downarrow{\scriptstyle \mu_X} \\ Y & \xrightarrow{\quad f \quad} & X. \end{array}$$

□

Now we prove Theorem 12.1.

Proof of Theorem 12.1. Given $i : Y \hookrightarrow X$ choose an ample line bundle $L \in \mathrm{Line}(X)$. Let

$$Z' := \ker(X \xrightarrow{\lambda_L} X^\vee \xrightarrow{i^\vee} Y^\vee) \subseteq X.$$

Now $Z' \cap Y$ is finite over k since by Lemma 12.2,

$$Z' \cap Y = \ker(i^\vee \circ \lambda_L \circ i) = \ker(\lambda_{i^*L}) = K_{i^*L}$$

which is finite over k. Take $Z = (Z'_{\mathrm{red}})^\circ$.

Fact 12.3: [7, 5.31] Let Y be an abelian variety over a field k. If $Z \hookrightarrow Y$ is a closed subgroup scheme, then Z° is an open and closed subgroup scheme of Y that is geometrically irreducible. The reduced underlying scheme Z°_{red} is an abelian subvariety of Y. Z is an abelian subvariety of X and $\dim Z' = \dim X - \dim Y$.

Observe that $\mu_X : Y \times Z \to X$ is an isogeny:

1. $\ker \mu_X \subseteq (Y \cap Z) \times (Y \cap Z)$ is finite, and
2. $\dim(Y \times Z) = \dim Y - \dim Z = \dim Y - \dim Z' \geq \dim X$.

Definition 12.4: $A \in (\mathrm{Ab}/k)$ is **simple** if there is no proper nontrivial abelian subvariety $B \subseteq A$.

Proposition 12.5: If $A \to B$ is an isogeny and A is simple, then B is simple.

Corollary 12.6: Given $A \in (\mathrm{Ab}/k)$, there exist simple $A_1, \dots, A_r \in (\mathrm{Ab}/k)$ and $n_1, \dots, n_r \in \mathbb{N}$ and an isogeny

$$A_1^{n_1} \times \cdots \times A_r^{n_r} \to A.$$

Moreover the A_i, n_i are unique.

Remark: A is k-simple does not imply that $A \times_k k'$ is k'-simple. Simplicity is not preserved under base change (corresponding to tensor product of algebras).

□

§1 Cartier duality

We studied the dual functor $A \mapsto A^\vee$ on (Ab/S). Now we define Cartier duality, which is a functor on the category of finite locally free group schemes over S. We give two approaches.

1.1 Concrete approach

Suppose we are in the affine case, so we can write $S = \mathrm{Spec}(Q)$ and $G = \mathrm{Spec}\, R$. A morphism $G \to S$ corresponds to a algebra homomorphism $Q \to R$.

First, we give a basic definition.

Definition 12.7: A **Hopf algebra** R over Q is an algebra equipped with the following functions. (Note items 1 and 2 are part of the definition for an algebra.)

1. Ring multiplication $m : R \otimes_Q R \to R$
2. Structure map (unit): $\delta : Q \to R$ (corresponding to $G \to S$)
3. $i^\sharp : R \to R$ corresponding to $i : G \to G$.
4. Counity $e^\sharp : R \to Q$ corresponding to $e : S \to G$.
5. Comultiplication $\Delta : R \to R \otimes_Q R$ corresponding to $G \times G \to G$.

What happens when we dualize? Define $R^\vee = \mathrm{Hom}_{Q\text{-alg}}(R, Q)$. This is equipped with maps dual to the ones in the definition: (we drop the $\sharp$ for notational convenience)

1. $R^\vee \to R^\vee \otimes_Q R^\vee$
2. $R^\vee \to Q^\vee \cong Q$ (canonically; $\mathrm{Hom}_Q(Q, Q) = Q$)

3. $R^\vee \xrightarrow{i^\vee} R^\vee$
4. $Q^\vee \xrightarrow{e^\vee} R^\vee$
5. $R^\vee \otimes R^\vee \xrightarrow{m^\vee} R^\vee$.

Now $G^\vee = (\operatorname{Spec} R^\vee, \mu^\vee, e^\vee, i^\vee)$ is a group scheme over S; in fact it is a finite locally free commutative group scheme.

We see that $G \to G'$ ($\operatorname{Spec} R \to \operatorname{Spec} R'$) gives $G'^\vee \to G^\vee$ ($\operatorname{Spec} R' \to \operatorname{Spec} R$). You can check that this is a morphism of group schemes.

Problem 12.1: Show that $(G^\vee)^\vee \xrightarrow{\cong} G$ functorially in G.

For general schemes S, we glue from the affine case.

Example 12.8: We have $(\mathbb{Z}/n\mathbb{Z})^\vee \cong \mu_n$ when $S = \operatorname{Spec} k$. (Recall that $\underline{\mathbb{Z}/n\mathbb{Z}} = \operatorname{Spec}\left(\bigoplus_{x\in\mathbb{Z}/n\mathbb{Z}} k\right)$.) Here the multiplication map is

$$\mu^\sharp : \bigoplus_\gamma k \to \bigoplus_{(\delta,\delta')\in(\mathbb{Z}/n\mathbb{Z})^2} k$$
$$(a_\gamma) \mapsto (a_{\delta\neq\delta'}).$$

We claim that $\mu_n = \operatorname{Spec}(k[t]/(t^n-1))$ and $\mu^\sharp : t \to t \otimes t$. Note $\bigoplus_\gamma k^\vee \cong k[\mathbb{Z}/n\mathbb{Z}] \cong k[t]/(t^n-1)$ via the maps

$$((a_n) \mapsto a_m) \leftarrow\!\shortmid \underbrace{m}_{\mathbb{Z}/n\mathbb{Z}} \leftarrow\!\shortmid t^m.$$

as k vector-spaces, as k-algebras, and as Hopf algebras.

1.2 Second approach to $G^\vee$

Theorem 12.9: Let G be a finite locally free abelian group scheme over S. Then the functor

$$\underline{G^\vee} : (\mathrm{Sch}/S) \to (\mathrm{Gps})$$
$$T \mapsto \operatorname{Hom}_{(\mathrm{Gp}/T)}(G \times T, \mathbb{G}_{m,T})$$

is representable by $\underline{G^\vee}$.

Proof. Observe that $\underline{G^\vee}$ is a Zariski sheaf so we can reduce to $S = \operatorname{Spec} Q$, $G = \operatorname{Spec} R$, $G' = \operatorname{Spec} R'$, and $T = \operatorname{Spec} Q'$. It suffices to show

$$\underline{G^\vee}(\operatorname{Spec} Q') \cong G^\vee(\operatorname{Spec} Q')$$

for all Q-algebras Q', and that this is functorial in Q'. Note

$$\begin{aligned}\underline{G^\vee}(R') &\subseteq \operatorname{Hom}_{(\mathrm{Sch}/S)}(\operatorname{Spec} R \otimes Q', \operatorname{Spec} Q'[t,t^{-1}]) \\ &= \operatorname{Hom}_{Q\text{-alg}}(Q'[t,t^{-1}], R \otimes_Q Q') \cong R^\times_{Q'}\end{aligned}$$

the last via $\varphi \mapsto \varphi(t)$. (We use $R_{Q'}$ to denote $R \otimes_Q Q'$.) Consider

$$eq : 787 - 12 - 1 \quad G^\vee(R') = \left\{\alpha \in R_{Q'}^\times : \mu^\sharp(\alpha) \equiv \alpha \otimes \alpha\right\} \tag{15}$$

Claim 12.10:

$$eq : 787 - 12 - 2 \quad G^\vee(Q') = \left\{\alpha \in R_{Q'} : \mu^\sharp = \alpha \otimes \alpha,\ e^\sharp(\alpha) \equiv 1\right\}. \tag{16}$$

Proof. (15)⊆(16): The following commute.

$$\begin{array}{ccccc} G \times S & \xrightarrow{(\mathrm{id},e)} & G \times G & \xrightarrow{\mu} & G \\ & \searrow^{\mathrm{id}} & & & \nearrow \end{array} \qquad \begin{array}{ccccc} G & \xrightarrow{(\mathrm{id},i)} & G \times G & \xrightarrow{\mu} & G \\ & \searrow & & \nearrow_{e} & \\ & & S & & \end{array}$$

We get $R \to R \otimes_Q R = R$, $\alpha \mapsto (\mathrm{id}, e)^\sharp(\mu^\sharp \alpha) = \alpha$. $(\mathrm{id}, e)^\sharp(\mu^\sharp \alpha) = (\mathrm{id}, e)^\sharp(\alpha \otimes \alpha) = \alpha \otimes e^\sharp \alpha$ by (1).(?) Hence (15)⊆(16).

(16)⊆(15): We have the diagram

$$\begin{array}{ccccc} G & \xrightarrow{(\mathrm{id},i)} & G \times G & \xrightarrow{\mu} & G \\ & \searrow & & \nearrow_{e} & \\ & & S & & \end{array}$$

This gives $\alpha i^\sharp \alpha = e^\sharp \alpha = 1$ using (1), so $\alpha \in R_Q^\times$. □

Now we prove the theorem. We want to show $\underline{G^\vee}(Q') = G^\vee(Q')$. The LHS is in $R_{Q'}$ and the RHS is in $\mathrm{Hom}(R_{Q'}^\vee, Q')$, [under arrow] duality of Q' modules. Claim the isomorphism restricts to the bijection. The LHS (i) corresponds to multiplication preserving, the RHS (ii) identity preserving... See Mumford. □

Lecture 13
Thu. 10/25/12

Last time we defined the Cartier dual for finite locally free group schemes over S. We gave 2 definitions. One was

$$\vee : G \mapsto \underline{G}^\vee := \mathrm{Hom}_{(\mathrm{Gp}/S)}(G, \mathbb{G}_m)$$

represented by $G^\vee = \underline{\mathrm{Spec}}\mathscr{O}_G^\vee$ where we take the $\mathscr{O}_S$-mod dual. This has all the structure we need for a group scheme. Multiplication is comultiplication, identity is coidentity, and inverse is inverse (also called antipodal map).

§1 Cartier dual and dual isogenies

Our main result is the following.

Theorem 13.1: If $f : A \to B$ is an isogeny in (Ab/S), then we have a canonical isomorphism

$$(\ker f)^\vee \cong \ker(f^\vee).$$

Proof. Our plan is to show

$$\begin{aligned}\ker(f^\vee) &= \ker(\mathrm{Pic}^\circ_e B \to \mathrm{Pic}^\circ_e A)\\ &\overset{\iota}{\subseteq} \ker(\mathrm{Pic}_e B \to \mathrm{Pic}_e A) := K'\\ &\cong K^\vee.\end{aligned}$$

Everything is clear except the last line, which is the key step. To conclude the theorem from these equations, we use $\deg f = \deg f^\vee$ to get $\mathrm{rank}(\ker(f^\vee)) = \mathrm{rank}(K^\vee)$, getting $\ker(f^\vee) \cong K^\vee$. Alternatively, we can show ι is an isomorphism directly; see Mumford.

We now show the key isomorphism, $K' \cong K^\vee$. We need a better description of the kernel, in terms of points. For all $T \in (\mathrm{Sch}/S)$, we have

$$K'(T) = \ker(\mathrm{Pic}_e B(T) \xrightarrow{(f\times 1)^*} \mathrm{Pic}_e A(T))$$

where $\mathrm{Pic}_e B(T) = \mathrm{Pic}_e(B \times T)$ and $\mathrm{Pic}_e A(T) = \mathrm{Pic}_e(A \times T)$. Note

$$\mathrm{Pic}_e B(T) = \mathrm{Pic}_e(B \times T) = \left\{L \in \mathrm{Pic}(B \times T) : e^*_{B,T} L \cong \mathscr{O}_T\right\}.$$

Then we have (under $(f \times 1)^* L \cong \mathscr{O}_{A\times T}$)

$$K'(T) = \ker(\mathrm{Pic}(B \times T) \to \mathrm{Pic}(A \times T)).$$

Note

$$e^*_{B,T} L = e^*_{A,T}(f \times 1)^* L \cong \mathscr{O}_T$$

using commutative triangle

$$\begin{array}{ccc} A_T & \xrightarrow{(f\times 1)^*} & B_T \\ & {\scriptstyle e_{A,T}}\nwarrow \quad \nearrow{\scriptstyle e_{B,T}} & \\ & T & \end{array}$$

$K'(T)$ is isomorphic to the set of K-equivariant structures on $\mathscr{O}_{A\times T}$. Recall that we have $A \times_S T$? $A_T \xrightarrow{f_T} B_T \bmod K_T$. Recall that we have

$$\mathrm{QCoh}^{K_T}(A_T) \to\leftarrow \mathrm{QCoh}(B_T)$$

pushforward increases rank in general. To get equivalence, we have to take K_T-invariant sections after pushing forward. Right: $f_{T,*}(\cdot)^{K_T}$, Left: f_T^*. How many in kernel. All should be $\mathscr{O}_{A_T}$, different L different choices of K_T-equivariant structure. Le have

$$\mathrm{QCoh}(B_T) \ni L \in \ker(\mathrm{Pic}(B_T) \to \mathrm{Pic}(A_T))$$

Condition to be in kernel is $f_T^* \cong \mathscr{O}_{A_T}$. Trying to count how many nonisomorphic L, same as number of nonisomorphic K_T invar structure by categ equivalence.

We have $f^*L \cong \mathscr{O}_{A_T}$. We need to prove

$$\left\{\begin{matrix}K_T\text{-equivariant structure} \\ \text{on } \mathscr{O}_{A\times T}\end{matrix}\right\} \cong K^\vee(T) = \mathrm{Hom}_{\mathrm{Gp}/T}(K_T^\vee, \mathbb{G}_{m,T}).$$

use a diff interp of line bundle. Use geo intuition. General facts. A line bundle L on X is $X \times \mathbb{A}^1 \to X$. Given a K-action on X, a K-equivariant equivariant structure on L ($\mu^*L \cong p_2^*L$) is $X \times \mathbb{A}^1 \to X \to X$ K-equivariant, K acting on both.

For us, $p_1 : A_T \times_T \mathbb{A}^1_T \to A_T$. Downstairs, K-action? Upstairs how give K-equivariant structure. Condition map downward equivariant just means diagram commutes.

$$\begin{array}{ccc} K_T \times A_T \times \mathbb{A}^1_T & \xrightarrow{?} & A_T \times_T \mathbb{A}^1_T \\ \downarrow & & \downarrow{\scriptstyle p_1} \\ K_T \times_T \mathbb{A}_T & \xrightarrow{\mu_{A,T}} & A_T \end{array}$$

(Bottom: $(k, x) \mapsto k + x$.)

To commute, we need to give on T'-points

$$(k, x, a) \mapsto (x + k, \lambda(k, x, a)).$$

Now $\lambda(k, x, a)$ has to be linear in the a component, so we can write

$$\lambda(k, x, a) = \lambda(k, x)a$$

Now we realize that $\lambda(k, x)$ depends only on k.

We now use the fact that every map $K_T \times A_T \to \mathbb{A}^1_T$ factors through K_T:

$$\begin{array}{ccc} K_T \times A_T & \longrightarrow & \mathbb{A}^1_T \\ & \searrow \quad \nearrow & \\ & K_T & \end{array}$$

Indeed, $\pi : A_T \to T$ proper means that $\pi_* \mathscr{O}_{A_T} \cong \mathscr{O}_T$ and $\pi_* \mathscr{O}_{A_T \times K_T} \cong \mathscr{O}_{K_T}$. Then to be an action,

$$\begin{aligned} \lambda(0, \cdot) &= 1 \\ \lambda(k + k', x) &= \lambda(k, x)\lambda(k', k + x). \end{aligned}$$

This looks like a cocycle condition. But because λ doesn't depend on x, this reduces to just a homomorphism condition; we get

$$(\lambda \mapsto \lambda(k, \cdot)) \in K^\vee(T) = \mathrm{Hom}_{\mathrm{Gp}/T}(K_T, \mathbb{G}_{m,T}).$$

everything lands in invertible element of $\mathbb{G}_m$.

If have element can go backwards to define action, so can go both forwards and backwards.

You have to actually keep track of group operations (we proved it's a set theoretic bijections). □

Corollary 13.2: Let A be an abelian variety. Then $A[n]^v \cong A^\vee[n]$. Moreover, the following commutes

$$\begin{array}{ccc} A[n]^\vee & \xrightarrow{\cong} & A^\vee[n] \\ \downarrow & & \downarrow \\ A[nm]^\vee & \xrightarrow{\cong} & A^\vee[nm] \end{array}$$

Thus we can put this information together to organize into a limit object.

§2 p-divisible groups, p-adic Tate modules

Recall that for $A \in (\mathrm{Ab}/S)$, $A[n]$ is a finite locally free commutative group scheme over S of rank n^{2g}.

Let's restrict to $S = \operatorname{Spec} k$ for now. We have the following.

Fact 13.3: Let G be a finite commutateive group scheme over k. Let $k := \operatorname{rank}_k G$.

- If $(\operatorname{char} k, r) = 1$ then G is étale over k (it is the Spec of a finite product of finite seperable extensions of k).
- If G is étale over k and $k = \overline{k}$, then $G \cong \underline{\Gamma}$ for some finite abstract group Γ ($|\Gamma| = r$).
- If $k = \overline{k}$, $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ if $(\operatorname{char} k, n) = 1$.

Caution? For instance if $\dim A = 1$, $A[4] = (\mathbb{Z}/2)^4$ but $|A[2]| \neq 2^2$. $(\mathbb{Z}/4)^2$?

Remark: If $\operatorname{char} k = p$, then

$$A[p^m](\overline{k}) \mid (p^m)^{\dim A}.$$

Only half the size expect in other case. Still correct size as group scheme. In $\overline{k}$, some points clustered in one place, don't have points separated from each other. One way to see half size is that if you have physical points, can show have to contain $(\mathbb{Z}/p^m\mathbb{Z})$ type objects. As soon as have, also have to contain its dual μ_{p^m}. (you can show using theorem) However, only 1 point in μ_{p^m} in characteristic p. Mumford discussion p-rank in section 15.

We make a provisional definition.

Definition 13.4: Let $A \in (\mathrm{Ab}/k)$ be an abelian variety over a field. The **p-divisible group** associated with A is the inductive system

$$A[p^\infty] = \left(A[p] \hookrightarrow A[p^2] \hookrightarrow A[p^3] \hookrightarrow \cdots\right)$$

Later we'll see that we can make sense of this as a FPPF scheme (?).

Definition 13.5: Define the p-adic Tate module by

$$T_pA := \varinjlim_n A[p^n](\overline{k}) = \varinjlim_n A(\overline{k})[p^n] = \left(A[p](\overline{k}) \xleftarrow{p} A[p^2](\overline{k}) \xleftarrow{p} \cdots\right)$$

If $(p, \operatorname{char} k) = 1$, then $T_pA \cong \mathbb{Z}_p^{2g}$ as a $\mathbb{Z}_p$-module (note we have (diagram with $\mathbb{Z}/p^n$ action)).

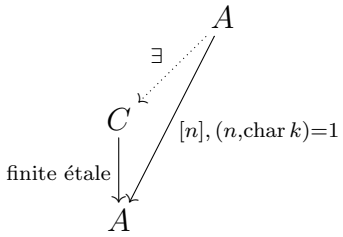
Remark: If $\operatorname{char} k \neq p$, then we usually study T_pA. If $\operatorname{char} k = p$, then we usually study $A[p^\infty]$ or its Dieudonné module $\mathbb{D}(A[p^\infty])$. If $\neq p$, then T_pA has torsion free, lots possibility work with rather than $\mathbb{Q}_p/\mathbb{Z}_p$ to some power.

Note $T_pA : \mathbb{D}(A[p^\infty]) = H^1_{\text{ét}} : H^1_{\text{cris}}$. Étale cohom when char$\neq p$, Crystalline cohomology when $= p$.

We have a fancy interpretation of T_pA. It is the p-primary part of the étale fundamental group

$$\pi_1^{\text{ét}}(A \times_k \overline{k}).$$

Fundamental group pro-p etale covering. (???) The underlying idea is that if you have A and some étale covering $C \to A$, then you can majorize it by some $A \xrightarrow{[n]} A$:



THink about this we can have a universal cover.

Readmore in Mumford section 18.

What's important in number theory is that we have this Galois representation (assuming $(\operatorname{char} k, p) = 1$)

$$G(\overline{k}/k) \to \mathrm{GL}_{\mathbb{Z}_p}(T_pA) \cong \mathrm{GL}_{2g}(\mathbb{Z}_p).$$

Galois action commuates with everything, p-mult in limit, $\mathbb{Z}_p$ structure

Note that if we have Tate modules for 2 different abelian varieties, then it induces a homomorphism

$$\operatorname{Hom}_{\mathbb{Z}_p[G(\overline{k}/k)]-\text{module}}(T_pA, T_pB).$$

Falting's proof of Mordell's conjecture. Also proved bijection when number field. This is a bijection when

- k is a finite field (Tate, mid 1960's).
- k is a number field (Faltings, early 1980's).

We'll aim to cover the proof when k is a finite field.

Conjecture 13.6: This is a bijection if k is finitely generated over $\mathbb{F}_p$ or $\mathbb{Q}$. (See Tate's article.)

For any field, it is generally known to be injective. We'll prove this.

What about local fields?? When $k = \mathbb{Q}_\ell$, and A, B have good reduction mod ℓ, then $T_pA \circlearrowleft G(\overline{Q}_\ell/\mathbb{Q}_\ell)$ factors through $\mathrm{Frob}_\ell^{\widehat{Z}}$. Too weak to cut out homomorphism.

§3 Structure of Hom and End

We follow Mumford, section 19. Let (Ab/k) be the category of abelian varieties over k up to isomorphism, as usual. Let

$$(\mathrm{Ab}/k)^\circ = \left\{ \begin{array}{c} \text{Objects: Abelian varieties}/k \\ \text{Morphisms: } \mathrm{Hom}_k^\circ(A,B) \\ := \mathrm{Hom}_{\mathrm{Gp}/k}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q} \end{array} \right\}.$$

Here $\mathrm{Hom}_{\mathrm{Gp}/k}(A,B)$ is a $\mathbb{Z}$-module, $\mathrm{Hom}_k^\circ(A,B)$ is a $\mathbb{Q}$-vector space. $f \in (\mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q})^\times$ is called a **quasi-isogeny**. For instance, n^{-1} is not a map, but it is a quasi-isogeny. Every isogeny is a quasi-isogeny.

If $f : A \to B$ is an isogeny. There exists an isogeny $g : B \to A$ such that $f \circ g = [n]$, $g \circ f = [n]$. (We sort-of proved this. See also Mumford.) Basically, we'd like to learn more about the structure of these guys, for instance, when $A = B$, we have $\mathrm{End}(A)$, $\mathrm{End}^0(A)$. Are they finite-dim, torsion-free? What algebras?Next week.

Lecture 14
Tue. 10/30/12

§1 Structure of Hom and End

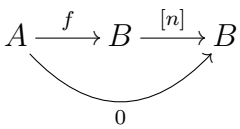
Recall that (Ab/k) denotes the category of abelian varieties over k, while $(\mathrm{Ab}/k)^0$ denotes the category of abelian varieties, but with morphisms $\mathrm{Hom}^0(A,B) := \mathrm{Hom}_{(\mathrm{Gp}/k)}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$. An isogeny becomes a morphism in the new category.

Now $\mathrm{Hom}^0(A,B)$ is a $\mathbb{Q}$-vector space and $\mathrm{End}^0(A)$ is a $\mathbb{Q}$-algebra (with multiplication as composition), but we don't know that they are finite-dimensional yet. We'll show this today.

Lemma 14.1: 1. $\mathrm{Hom}(A,B)$ is a torsion-free $\mathbb{Z}$-module.

2. $\mathrm{Hom}(A,B) \subseteq \mathrm{Hom}^0(A,B)$.

Proof. We want to show that if $[n] \circ f = 0$ then $f = 0$.



Suppose $\dim A = g$. Now $\operatorname{im} f \subseteq B[n]$ has dimension 0, so $\ker f$ has dimension g. This means $\ker f = A$, because the only subscheme of an irreduced irreducible scheme with same dimension is the scheme itself.

(1) implies (2) directly. □

Recall that an abelian variety A is k-simple if there is no abelian subvariety $B \subset A$ with $B \neq 0$.

Lemma 14.2: If A is simple then $\operatorname{End}^0(A)$ is a division ring.

Proof. We need to show every nonzero morphism is invertible: if $0 \neq f \in \operatorname{End}^0(A)$, is $f \in \operatorname{End}^0(A)^\times$?

There exists $n \in \mathbb{N}$ such that $[n] \circ f \in \operatorname{End}(A)$; we have $[n] \circ f \neq 0$ because $\operatorname{End}(A)$ is torsion-free. We have $[n] \in \operatorname{End}^0(A)^\times$ because its inverse is $\frac{1}{n}$. The fact that A is simple implies that every nonzero endomorphism is invertible, so $[n]f \in \operatorname{End}^0(A)^\times$ (being an isogeny). Hence $f \in \operatorname{End}^0(A)^\times$. □

This tells us something about the structure of the endomorphism algebra. Recall that Poincaré reducibility tells us that A is isogenous to some product of simple varieties:

$$A \sim A_1^{n_1} \times \cdots \times A_r^{n_r}$$

with $A_i \not\sim A_j$ for $i \neq j$ and with $n_i \geq 1$. This tells us that the endomorphism ring decomposes

$$\operatorname{End}^0(A) \cong \prod_{i=1}^{r} \mathcal{M}_{n_i}(D_i), \qquad \text{where } D_i = \operatorname{End}^0(A_i)$$

(Because the A_i are simple, there is no map between different A_i's except zero.) The D_i are division $\mathbb{Q}$-algebras. We've reduced the study of the $\operatorname{End}(A)$ to the case when A is simple. The basic questions are the following.

1. Is $\dim_{\mathbb{Q}} \operatorname{End}^0(A) < \infty$?
2. Is $\operatorname{Hom}(A, B)$ a finitely generated $\mathbb{Z}$-module?

If item 2 is true, then because we know $\operatorname{Hom}(A, B)$ is torsion-free, $\operatorname{Hom}(A, B)$ is actually a finite free $\mathbb{Z}$-module.

We now answer these questions.

Theorem 14.3 (Mumford [4], Theorem 19.3)**:** thm:787-HomAB

1. $\operatorname{Hom}(A, B)$ is a finitely generated $\mathbb{Z}$-module.
2. Assume that $(\ell, \operatorname{char} k) = 1$. Then

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \operatorname{Hom}(A, B) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$$

is injective.

We'll see why we need $(\ell, \operatorname{char} k) = 1$ in the proof. We don't expect the map $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \operatorname{Hom}(A, B) \to \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$ to be a bijection. Consider when $A = B$ are elliptic curves over $\mathbb{C}$. Then $\operatorname{End}(A) = \mathbb{Z}$ or $\mathbb{Z} \oplus \mathbb{Z}$, a rank 2 module in an imaginary quadratic field. The RHS has rank 4 over $\mathbb{Z}_\ell$, while the LHS has rank 1 or 2. Galois invariance prevents this from being bijective.

When the field is finitely generated over $\mathbb{Q}$, conjecturally, the image is the commutant of Galois.

Corollary 14.4: 1. $\operatorname{rank}_{\mathbb{Z}}(\operatorname{Hom}(A, B)) = \dim_{\mathbb{Q}} \operatorname{Hom}^0(A, B) \leq 4 \dim A 4 \dim B$.

2. $\operatorname{End}^0(A)$ is a finite-dimensional semisimple algebra.

Proof. We have $T_\ell A \cong \mathbb{Z}_\ell^{2 \dim A}$ and $T_\ell B \cong \mathbb{Z}_\ell^{2 \dim B}$. Just multiply the dimensions. □

We'll prove the theorem starting in 2 steps. As preparation, we'll prove the following.

Theorem 14.5 (Mumford [4], Theorem 19.2)**:** thm:deg-poly The map

$$\begin{aligned} \operatorname{End}(A) &\to \mathbb{Z} \\ \phi &\mapsto \deg \phi \end{aligned}$$

(where $\deg \phi := 0$ if ϕ is not an isogeny) extends to a homogeneous polynomial f of degree $2g$ on $\operatorname{End}^0(A)$, i.e., for any $\phi, \psi \in \operatorname{End}^0(A)$, the following function

$$\begin{aligned} \mathbb{Q}^2 &\to \mathbb{Q} \\ (m, n) &\mapsto f(m\phi + n\psi) \end{aligned}$$

is a homogeneous polynomial of degree $2g$.

Proof. We recall some facts.

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

(ii) $\chi_A(f^* L) = (\deg f)\chi_A(L)$. (Both sides are 0 if f is not an isogeny.)

(iii) If L and M are ample line bundles then the function

$$n \mapsto \chi(L^{\otimes n} \otimes M)$$

is a polynomial in n of degree at most g.

In fact there is a precise Riemann-Roch type formula for $\chi_A(L)$ in Mumford [4], Section 16.

1. We have by (i) that

$$\deg(n\phi) = \deg n \deg \phi = n^{2g} \deg \phi.$$

This shows homogeneity.

2. We will show $n \mapsto \deg(n\phi + m\psi)$ is a polynomial in n.

Together 1 and 2 give us what we want, namely, $\det(n\phi + m\psi)$ is a polynomial in m and n, homogeneous of degree $2g¿$

Let's show item 2. We will use the Euler characteristic of the line bundle. Choose an ample line bundle L. Then $\chi(L) \neq 0$. This comes from $H^i(A, L) = 0$ for $i > 0$. (See Mumford [4], Section 16.)

We know by (ii) that

$$\deg(n\phi + \psi) = \frac{\chi((n\phi + \psi)^* L)}{\chi(L)}.$$

It suffices to show that

$$n \mapsto \chi(\underbrace{(n\phi + \psi)^* L}_{=:L(n)})$$

is a polynomial. The idea is to get an expression in terms of a tensor power of L, using Theorem of the Cube 7.9. Apply the Theorem of the Cube to $f_1 = (n-1)\phi + \psi$ and $f_2 = f_3 = \phi$. We get a recursive formula which we solve to get

$$L(n) := L_1^{\frac{n(n-1)}{2}} \otimes L_2^n \otimes L_3.$$

Now 2 applications of Then we can appeal to (iii) to conclude that $\chi(L(n))$ is a polynomial in n: (iii) implies

$$(m, n) \mapsto \chi(L_1^m \otimes L_2^n \otimes L_3)$$

is a polynomial in m and n, so $n \mapsto \chi(L(n))$ is a polynomial in n, of degree at most $2g$. □

Let's get back to the proof of Theorem 14.3.

Proof of Theorem 14.3. We prove this in two steps.

Step 1: Recall that $\mathrm{Hom}(A, B) \subset \mathrm{Hom}^0(A, B)$. For every finitely generated $\mathbb{Z}$-submodule M of $\mathrm{Hom}(A, B)$, $\mathbb{Q}M \cap \mathrm{Hom}(A, B)$ is a finitely generated $\mathbb{Z}$-module.

Step 2: Prove the injectivity of (ii).

Once we have steps 1 and 2, noting tensoring is an exact functor (?), tensoring with $\mathbb{Q}_\ell$ gives

$$\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}(A, B) = \mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathrm{Hom}^0(A, B) \hookrightarrow \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathrm{Hom}(T_\ell A, T_\ell B).$$

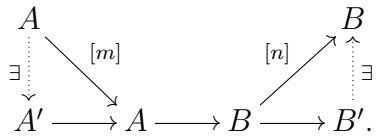
The RHS is finite dimensional, so $\mathrm{Hom}^0(A, B)$ is finite dimensional. Taking any M containing a $\mathbb{Q}$-basis of $\mathrm{Hom}^0(A, B)$, step 1 implies (1) and we'll be done.

We have to prove Steps 1 and 2. For step 1, we'll make use of the fact that the degree function is polynomial.

Step 1: (Proof) We use the following.

Lemma 14.6: Let $A' \to A$ and $B \to B'$ be isogenies. Then we have an injection $\mathrm{Hom}(A, B) \hookrightarrow \mathrm{Hom}(A', B')$.

Proof. Given $A' \to A$, we can find m such that $[m] : A \to A$ factors through $A' \to A$. Given $B \to B'$ we can find n such that $[n] : B \to B$ factors through $B \to B'$.



Then we find that $[n]f[m] = 0$. By torsion-freeness we have $f = 0$. □

We make some reduction steps. First we may assume A, B are simple. Poincaré reducibility tells us that for some finite product of simple abelian varieties we have $\prod A_i^{m_i} \to A$ and $B \to \prod_j B_j^{n_i}$. The lemma says that

$$\mathrm{Hom}(A, B) \hookrightarrow \prod_{i,j} \mathrm{Hom}(A_i^{m_i}, B_j^{n_j}) = \prod_{i,j} \mathcal{M}_{m_i \times n_j} \mathrm{Hom}(A_i, B_j).$$

If the conclusion true for each $\mathrm{Hom}(A_i, B_j)$, then it is true for $\mathrm{Hom}(A, B)$.

We can assume $A = B$: If there is no isogeny $B \to A$, then $\mathrm{Hom}(A, B) = 0$. If there is an isogeny $B \to A$, then $\mathrm{Hom}(A, B) \hookrightarrow \mathrm{Hom}(A, A)$. If conclusion of step 1 true for $\mathrm{Hom}(A, A)$, then true for $\mathrm{Hom}(A, B)$.

Now we use use Theorem 14.5. Let M be a finitely generated $\mathbb{Z}$-submodule of $\mathrm{End}(A)$. We have to show $\Gamma := \mathbb{Q}M \cap \mathrm{End}(A) \subset \mathbb{Q} \cdot M \cong \mathbb{Q}^r$ is finitely generated. Now we claim that

$$\Gamma \cap \left\{\alpha \in \mathrm{End}^0(A) : |\deg(\alpha)| < 1\right\} = \{0\}.$$

Indeed, the degree is a polynomial on $\mathrm{End}^0(A)$. The reason is that on $\mathrm{End}(A)$, the degree function assumes integer values; we have $\deg \alpha = 0$ iff $\alpha = 0$. This shows $|\deg(\alpha)| < 1$ contains an open neighborhood of 0. Hence Γ is a disrete subgroup of $\mathbb{Q}M$. A standard fact shows that a discrete subgroup is finitely generated. This marks the end of step 1.

Step 2: Suppose by way of contradiction that the map is not injective. Then some element is sent to 0:

$$T_\ell : 0 \neq \sum_{i=1}^{r} \alpha_i \phi_i \mapsto 0, \qquad \alpha_i \in \mathbb{Z}_\ell,\ \phi_i \in \mathrm{Hom}(A, B).$$

Let $M := \mathbb{Z}\langle \phi_1, \ldots, \phi_r \rangle$. We may enlarge M such that

$$M = \mathbb{Q}M \cap \mathrm{Hom}(A, B).$$

Choose free generators $\phi_1, \ldots, \phi_r$ of M. However, it's difficult to work with homomorphisms with $\mathbb{Z}_\ell$ coefficients, so we approximate $\mathbb{Z}_\ell$ coefficients with $\mathbb{Z}$ coefficients. Choose $\beta_i \in \mathbb{Z}$ such that $\beta_i - \alpha_i \in \ell\mathbb{Z}_\ell$ (i.e., the β_i are a first-order ℓ-adic approximation to α_i). Then

$\phi = \sum_{i=1}^r \alpha_i\phi_i + (\beta_i - \alpha_i)\phi_i$ maps to $T_\ell(\phi) = 0 + \ell(\cdots)$. Now we have a commutative diagram

$$\begin{array}{ccc} T_\ell A & \xrightarrow{T_\ell(\phi)} & T_\ell B \\ {\scriptstyle \bmod \ell}\downarrow & & \downarrow{\scriptstyle \bmod \ell} \\ A[\ell](\overline{k}) & \xrightarrow{\phi} & B[\ell](\overline{k}). \end{array}$$

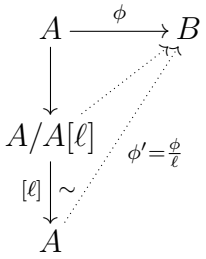
Going clockwise we have 0. However, the vertical maps are surjections, so we must have the lower map $\phi = 0$.

Now $\phi|_{A[\ell](\overline{k})} = 0$. Using $(\ell, \operatorname{char} k) = 1$, we have

$$\phi|_{A[\ell]\times_k \overline{k}} = 0.$$

This gives us $\phi|_{A[\ell]} = 0$. The rank of the kernel doesn't change from k to $\overline{k}$. If the kernel has full rank in either field, it has full rank in both fields.

We now have a map



in $\operatorname{Hom}(A, B) \cap \mathbb{Q}M = M$. Now $\phi' = \sum_{i=1}^r \alpha_i'\phi_i$. Thus $\sum \ell\alpha_i'\phi_i = \sum_{i=1}^r \beta_i\phi_i$. This implies that α_i should be infinitely divisible by ℓ: we may assume there exists i, $\ell \nmid \alpha_i$, using ℓ-torsion-freeness of the RHS. We we a contradiction because by iniital choice of β_i, there exists i so that $\ell \nmid \beta_i$. □

Next time we'll discuss the characteristic polynomial, Section 19 of Mumford [4].

Lecture 15
Thu. 11/1/12

Last time we showed that in (Ab/k), assuming $(\operatorname{char} k, \ell) = 1$, there is an injection

$$\mathbb{Z}_\ell \otimes \operatorname{Hom}_{(\mathrm{Gp}/k)}(A, B) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}_\ell\text{–module}}(T_\ell A, T_\ell B).$$

We have that $\operatorname{End}^0(A)$ is a finite dimensional semisimple algebra over $\mathbb{Q}$: decomposing $A \sim \prod_{i=1}^r A_i^{n_i}$ where A_i is simple, we get

$$\operatorname{End}^0(A) \cong \prod_{i=1}^r \mathcal{M}_{n_i}(\operatorname{End}^0(A_i)).$$

Here each $\operatorname{End}^0(A_i)$ is a finite division algebra over $\mathbb{Q}$, so $\operatorname{End}^0(A)$ is finite-dimensional semisimple.

§1 Central simple algebras

Definition 15.1: Let F be a field of characteristic 0, such as a finite extension of $\mathbb{Q}$ and $\mathbb{Q}_\ell$. A **central simple algebra (CSA)** D over F is a finite-dimensional simple F-algebra with center F.

Example 15.2: Any matrix algebra $D = \mathcal{M}_n(F)$ is a central simple algebra. In particular, for $n = 1$, $D = F$ is a central simple algebra over F.

We have the following facts.

Proposition 15.3: The following hold.

1. Every central simple algebra over F splits over the algebraic closure of F:
$$D \otimes_F \overline{F} \cong \mathcal{M}_n(\overline{F}).$$
2. $[D : F] = n^2$ for some $n \in \mathbb{Z}$.
3. $D \cong \mathcal{M}_r(D')$ for some central division algebra D'/F, and we have
$$r[D' : F]^{\frac{1}{2}} = [D : F]^{\frac{1}{2}}.$$

The central simple algebras are classified by the **Brauer group**

$$\mathrm{Br}(F) = \{\mathrm{CSA}/F\}/\sim$$

with multiplication given by $\otimes$ and equivalence relation $D \sim D'$ if $\mathcal{M}_r(D) \cong \mathcal{M}_{r'}(D')$ for some r, r'.

Just like we have a norm and trace for a field extension K/F, we have a norm and trace for a CSA D/F. We define the reduced norm and trace and then relate them to general norm and trace functions.

Normally we define the norm and trace as the determinant and trace of the multiplication map considered on the space itself D. But the dimension of D/F is n^2, which is too large. Hence we define the reduced norm and trace: we consider the multiplication map on $\overline{F}^n$ instead. We can do this becaue by Proposition **??**, $D \otimes_F \overline{F} \cong \mathcal{M}_n(\overline{F})$, and by Noether-Skolem, any automorphism of $\mathcal{M}_n(\overline{F})$ is given by an inner automorphism and doesn't change the determinant and trace.

Definition 15.4: Define the **reduced norm** $N^\circ_{D/F}$ and **reduced trace** $T^\circ_{D/F}$ by

$$N^\circ_{D/F}(a) := \det_{\overline{F}}(a \otimes 1|_{\overline{F}^n})$$
$$T^\circ_{D/F}(a) := \mathrm{Tr}_{\overline{F}}(a \otimes 1|_{\overline{F}^n})$$

where $n = [D : F]^{\frac{1}{2}}$.

One can check that $N^\circ_{D/F}(a)$ and $T^\circ_{D/F}(a)$ are invariant under $G(\overline{F}/F)$; hence they are in F.

Definition 15.5: Let D/F be a CSA, and F/E be a separable extension.

1. A **norm form** of D over E is a nonzero polynomial function $N : D \to E$ such that
$$N(x_1x_2) = N(x_1)N(x_2).$$
2. A **trace form** of D over E is a function $T : D \to E$ that is E-linear (in particular $T(x_1 + x_2) = T(x_1) + T(x_2)$) and such that $T(xy) = T(yx)$.

Why are we interested in norm and trace forms? Recall that we had a degree function on $\mathrm{End}(A)$, and we extended it to $\mathrm{End}^0(A)$. Because degree is multiplicative, it is a norm form.

By proving a classification theorem for norm forms, we can better understand deg.

Example 15.6: Let D/F be a CSA and F/E a separable extension.

- $N^\circ_{D/F}$ and $T^\circ_{D/F}$ are norm/trace forms on D/F.
- In the situation of the definition,
$$N^{\min}_{D/E} := \mathrm{Nm}_{F/E} \circ N^\circ_{D/F}$$
$$T^{\min}_{D/E} := \mathrm{Tr}_{F/E} \circ T^\circ_{D/F}$$
are norm/trace forms on D/E, called the **minimal norm** and **minimal trace**.

  This is a typical way to get a norm and trace form.

As the following shows, all norm and trace forms come from the minimal norm and trace.

Lemma 15.7 (Classification of norm/trace forms)**:** lem:classify-norm

- Any norm form N on D/E is in the form $(N^{\min}_{D/E})^m$, where $m \in \mathbb{Z}$.
- Any trace form T on D/E is in the form $\phi \circ T^\circ_{D/F}$, where $\phi : F \to E$ is a E-linear map.

Proof for the special case $E = F = \overline{F}$. We have $D \cong \mathcal{M}_n(F)$ by Proposition **??**(1) so N gives rise to a morphism of group schemes (actually algebraic groups) over F
$$\mathrm{GL}_n \to \mathbb{G}_m.$$
The fact that $N(x_1x_2) = N(x_1)N(x_2)$ means this is a group homomorphism, so a morphism of algebraic groups. We have
$$N(x_1x_2x_1^{-1}x_2^{-2}) = 1$$

by multiplicativity (because the target $\mathbb{G}_m$ is commutative). So $N = 1$ on the closed subgroup scheme SL_n generated by commutators. Thus the morphism factors

$$\begin{array}{ccc} \mathrm{GL}_n & \xrightarrow{N} & \mathbb{G}_m \\ \downarrow & \searrow^{N^{\min}_{D/F}} & \uparrow \\ \mathrm{GL}_n / \mathrm{SL}_n & \xrightarrow[\cong]{\det} & \mathbb{G}_m. \end{array} \quad \hat{}m,\ m \in \mathbb{Z}$$

But the only map $\mathbb{G}_m \to \mathbb{G}_m$ is the mth power map. A morphism $\mathbb{G}_m \to \mathbb{G}_m$ corresponds to a map $k[t, t^{-1}] \to k[t, t^{-1}]$; to be a morphism of group schemes it has to be the mth power map.

For the trace form, note $T(xy - yx) = 0$ for all $x, y \in \mathcal{M}_n(F)$, the elements $xy - yx$ generate the trace 0 part in $\mathcal{M}_n(F)$ (prove this by a hands-on approach), so we similarly get the trace form factors as follows.

$$\begin{array}{ccc} \mathcal{M}_n(F) & \xrightarrow{T} & E \\ \downarrow & \searrow^{T^{\circ}_{D/F}} & \uparrow \\ \frac{\mathcal{M}_n(F)}{\langle xy - yx \rangle} & \xrightarrow[\cong]{\mathrm{Tr}} & F. \end{array} \quad \exists E\text{–linear}$$

All maps in the diagram are E-linear, so the map $F \to E$ is E-linear. □

Theorem 15.8 (Mumford [4], Theorem 19.4)**:** Suppose $(\mathrm{char}\, k, \ell) = 1$, $A \in (\mathrm{Ab}/k)$ and $\dim A = g$. Suppose $f \in \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$; we have $T_\ell(f) \in \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell A)$. Then the following hold.

1. $\deg f = \det T_\ell f$
2. $P_f(n) := \deg([n] - f) = \det([n] - T_\ell(f))$ is a monic polynomial of degree $2g$ with coefficients in $\mathbb{Z}$.
3. $P_f(f) = 0$ in $\mathrm{End}(A)$.

Remark: The philosophy is that because f has geometric origin, $T_\ell(f)$ in a sense doesn't depend on ℓ. (2) implies that the $P_f(n)$ are independent of ℓ, and (1) implies that $\det T_\ell(f)$ is independent of ℓ.

In ℓ-adic étale cohomology, we often see independence of ℓ. Independence of ℓ questions are known in many cases (though not everywhere). You can interpret this theorem in the context of étale cohomology.

Proof. Part 1 is about the equality of 2 norm forms. Recall that we extended deg from $\mathrm{End}(A)$ to $\mathrm{End}^0(A)$; it is a norm form

$$N_1 : \mathrm{End}^0(A) \xrightarrow{\deg} \mathbb{Q}.$$

The determinant also gives a norm form

$$N_2 : \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\det T_\ell(\cdot)} \mathbb{Z}_\ell.$$

By Theorem 14.5, deg is homogeneous of degree $2g$; $\det T_\ell(\bullet)$ is also homogeneous of degree $2g$ because it is the determinant of an endomorphism of rank $2g$-modules.) We get two norm forms that are homogeneous of degree $2g$:

$$N_1, N_2 : \mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to \mathbb{Q}_\ell.$$

To prove part 1 we need to show $N_1 = N_2$. We do this in 2 steps.

Step 1: We show that N_1 and N_2 have the same ℓ-adic evaluation:

$$|N_1(\alpha)|_\ell = |N_2(\alpha)|_\ell \quad \text{for all } \alpha \in \mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

Write $\alpha = \ell^{-a}\alpha_0$ where $\alpha_0 \in \mathrm{End}\, A \otimes \mathbb{Z}_\ell$. Because N_1 and N_2 are homogeneous of the same degree, it suffices to show that

$$|N_1(\alpha_0)|_\ell = |N_2(\alpha_0)|_\ell \quad \text{for all } \alpha_0 \in \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell.$$

Now write

$$N_1(\alpha_0) = \ell^{n_1} \cdot u_1$$
$$N_2(\alpha_0) = \ell^{n_2} \cdot u_2$$

where $u_i \in \mathbb{Z}_\ell^\times$. We show that $n_1 = n_2$. To show this, consider α_0 as a map $A[\ell^N] \to A[\ell^N]$ for N finite; this gives us a description of n_1. The map on the Tate modules $T_\ell A \xrightarrow{T_\ell(\alpha_0)} T_\ell A$ gives us a description of n_2. By taking an inverse limit of the maps $A[\ell^N] \xrightarrow{\alpha_0} A[\ell^N]$, we can relate n_1 and n_2. For any $N \geq 0$, we have the exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker \alpha_0(N) & \longrightarrow & A[\ell^N] & \xrightarrow{\alpha_0(N)} & A[\ell^N] & \longrightarrow & \mathrm{coker}\, \alpha_0(N) \longrightarrow 0 \\
 & & \uparrow{\scriptstyle [\ell]} & & \uparrow{\scriptstyle [\ell]} & & \uparrow{\scriptstyle [\ell]} & & \uparrow{\scriptstyle \cong} \\
0 & \longrightarrow & \ker \alpha_0(N+1) & \longrightarrow & A[\ell^{N+1}] & \xrightarrow{\alpha_0(N+1)} & A[\ell^{N+1}] & \longrightarrow & \mathrm{coker}\, \alpha_0(N+1) \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

where $\alpha_0(N) := \alpha_0|_{A[\ell^N]}$. Here we're implicitly looking at $\overline{k}$-points, $A[\ell^N] = A(\overline{k})[\ell^N]$.

Taking the inverse limit we get the ℓ-adic Tate modules. Taking $N \gg 0$ large enough the kernel stabilizes:

$$\ker \alpha_0(N) = \ker \alpha_0(N+1) = \cdots$$

and has order equal to the ℓ-part of $|\ker \alpha_0| = \deg \alpha_0$, which is ℓ^{n_1}. When we take the inverse limit by multiplication by ℓ, we get 0, because a finite ℓ-group cannot be infinitely divisible.

When we take the limit we preserve the size of coker. The exact sequences give that

$$\frac{|\ker \alpha_0(N)|}{|A[\ell^N]|}\frac{|A[\ell^N]|}{|\operatorname{coker}\alpha_0(N)|} = 1,$$

so ker and coker have the same order. We get that for large enough N,

$$|\operatorname{coker}\alpha_0(N)| = \ell^{n_1}.$$

Taking the inverse limit $\varprojlim_N$ we get

$$0 \to T_\ell A \xrightarrow{T_\ell(\alpha_0)} T_\ell A \to \operatorname{coker} T_\ell(\alpha_0) \to 0$$

where the cokernel has order equal to $|\operatorname{coker}\alpha_0(N)| = \ell^{n_1}$. On the other hand, because $N_2(\alpha_0) = \det T_\ell(\alpha_0) = \ell^{n_2}u_2$ and the ℓ-adic unit acts like an isomorphism, we have

$$|\operatorname{coker} T_\ell(\alpha_0)| = |T_\ell A/T_\ell(\alpha_0)T_\ell A| = \ell^{n_2}.$$

Hence $\ell^{n_1} = \ell^{n_2}$, as needed. This proves step 1. (Note we used homogeneity, not yet the classification of norm forms.)

Step 2: We show $N_1(\alpha) = N_2(\alpha)$. Write $\operatorname{End}^0 A \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{j=1}^r D_j$, where the D_j are finite simple over $\mathbb{Q}_\ell$. We decompose N_i into norm forms $N_{i,j}$ as follows:

$$N_i = \prod_{j=1}^r N_{i,j}, \qquad N_{i,j} : D_j \to \mathbb{Q}_\ell,\ i = 1, 2.$$

By Lemma 15.7, we have

$$N_{i,j} = (N^{\min}_{D_j/\mathbb{Q}_\ell})^{\nu_{i,j}}, \qquad \nu_{i,j} \in \mathbb{Z}.$$

Plug in $\alpha = (1, \ldots, 1, \underbrace{\alpha_j}_{j}, 1, \ldots, 1) \in \operatorname{End}^0 A \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{j=1}^r D_j$ into Step 1 to get

$$|N^{\min}_{D_j/\mathbb{Q}_\ell}(\alpha_j)|^{\nu_{1,j}} = |N^{\min}_{D_j/\mathbb{Q}_\ell}(\alpha_j)|^{\nu_{2,j}}.$$

We are free to choose α_j, so $\nu_{1,j} = \nu_{2,j}$ for all j. Hence $N_1 = N_2$. This proves part 1.

For part 2, note $P_f(N)$ is the characteristic polynomial of $T_\ell(f)$. Hence it is monic of degree $2g$. *A priori* the coefficients are in $\mathbb{Z}_\ell$; we need to show they are in $\mathbb{Z}$.

First we show the coefficients are in $\mathbb{Q}$; then we show they are also algebraic integers, so they are in $\mathbb{Z}$.

The degree function assumes integer values on $\operatorname{End}(A)$. If $P_f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$, it's not hard to see that $P_f(X) \in \mathbb{Q}[X]$.

Note the $\mathbb{Z}$-subalgebra generated by f, $\mathbb{Z}[f] \subseteq \operatorname{End}(A)$, is a finite commutative $\mathbb{Z}$-algebra. ($\operatorname{End}(A)$ is finitely generated by Theorem 14.3(1), and any subgroup of finitely generated

abelian group is finitely generated.) Hence f is integral over $\mathbb{Z}$. $T_\ell f$ satisfies the same monic equation that f satisfies, with coefficients in $\mathbb{Z}$. In particular, the eigenvalues of $T_\ell\mathbb{Z}$, which are in $\overline{\mathbb{Q}}$, satisfy the same equation. By integrality, the eigenvalues are in $\overline{\mathbb{Z}}$. Hence $P_f(X) \in \overline{\mathbb{Z}}[X]$. Since the coefficients are also in $\mathbb{Q}$, we get $P_f(X) \in \mathbb{Z}[X]$. This proves part 2.

Now we prove part 3. If we plug an operator into its own characteristic polynomial, we get 0 (Cayley-Hamilton). Hence

$$T_\ell(P_f(f)) = P_f(T_\ell(f)) = 0.$$

By Theorem 14.3(2), T_ℓ is injective, so

$$P_f(f) = 0.$$

□

Definition 15.9: $P_f(X) \in \mathbb{Z}[X]$ is called the **characteristic polynomial** of f. Define the trace and norm of P_f to be the following coefficients:

$$P_f(X) = X^{2g} - \underbrace{a_{2g-1}}_{\mathrm{Tr}(f)} X^{2g-1} + \cdots + \underbrace{a_0}_{\mathrm{Nm}\, f = \deg f}.$$

Corollary 15.10: Let $A \in (\mathrm{Ab}/k)$ have dimension g and be simple. Let $F := Z(\mathrm{End}^0 A)$. Then $d = [\mathrm{End}^0 A : F]^{\frac{1}{2}}$ and $e = [F : \mathbb{Q}]$. Then $de \mid 2g$.

This really relies on the classification of norms.

Proof. By Lemma 15.7,

$$\mathrm{Nm}\, f = (N^{\min}_{\mathrm{End}^\circ A} f)^n$$

with $n \in \mathbb{Z}$. We look at the degree of both sides. The LHS is a polynomial f of degree $2g$. The degree of the RHS is $de \cdot n$. Hence

$$de \mid 2g.$$

□

Definition 15.11: A $\overline{k}$-simple abelian variety $A \in (\mathrm{Ab}/k)$ is of **CM-type** if $de = 2g$.

If A is an elliptic curve (of dimension 1) this says $de = 2$. In characteristic 0, it can only happen that $d = 1$ and $e = 2$. To understand the endomorphism algebra of elliptic curves, we need another fact on the endomorphism algebra: $\mathrm{End}^0(A)$ has a positive involution, called the **Rosati involution**. This gives us a finer classification of endomorphism algebras. In positive characteristic, $\mathrm{End}^0(A)$ can also be a central quaternion algebras over $\mathbb{Q}$, and we get supersingular elliptic cuves. We'll talk about this and give a classification of complex abelian varieties next time.

Lecture 16
Tue. 11/6/12

Given an abelian variety $A \in (\mathrm{Ab}/k)$ of dimension g, let $f \in \mathrm{End}(A)$. Recall that the characteristic polynomial $P_f(X) \in \mathbb{Z}[X]$ is monic of degree $2g$. It is given by, for $n \in \mathbb{Z}$,

$$P_f(n) = \deg([n] - f) = \det T_\ell([n] - f) \text{ on } T_\ell A.$$

The advantage of writing $P_f(n)$ is that we can do simple linear algebra, but on $\mathbb{Z}_\ell$. The LHS is independent of ℓ but we cannot do simple linear algebra there.

Example 16.1: ex:frobenius-morphism We define the Frobenius morphism. To do this, we need to specify the map on topological spaces and on sheaves of rings.

Let X be a $\mathbb{F}_q$-scheme, where $q = p^f$. Define the **Frobenius morphism** as the map

$$\mathrm{Frob}_q : X \to X$$

that is the identity on topological spaces

$$X_{\mathrm{top}} \xrightarrow{\mathrm{id}} X_{\mathrm{top}}$$

and such that the map on affine opens is given the qth power map

$$\begin{aligned} \mathscr{O}_X(U) &\leftarrow \mathscr{O}_X(U) \\ a^q &\leftarrow\!\shortmid a. \end{aligned}$$

For $A \in (\mathrm{Ab}/\mathbb{F}_q)$ we have $\mathrm{Frob}_q \in \mathrm{End}(A)$. By the rigidity lemma (Corollary 5.14) it suffices to show the identity is sent to the identity and that Frob_q is a finite morphism.

Note Frob_q is a finite morphism becase the map on rings is

$$\begin{aligned} \mathbb{F}_q[X_1, \dots, X_n]/(f_j) &\leftarrow \mathbb{F}_q[X_1, \dots, X_n]/(f_j) \\ X_i^q &\leftarrow\!\shortmid X_i. \end{aligned}$$

This is a finite algebra, so Frob_q is an isogeny.

We have the Riemann Hypothesis for abelian varieties.

Theorem 16.2 (Riemann Hypothesis for abelian varieities)**:** The roots of $P_{\mathrm{Frob}_q}(X)$ are algebraic integers α such that $\iota(\alpha)\overline{\iota(\alpha)} = q$ for all imbeddings $\iota : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$.

This was proved earlier than the Riemann hypothesis for general varieties over $\mathbb{F}_q$. The key point is that given an ample line bundle, there is a Rosati involution $\ddagger_L$. We show that

$$\alpha \cdot \alpha^\ddagger = q.$$

We will return to this.

One consequence of the Riemann hypothesis is that it gives a way to calculate the number of points of A over $\mathbb{F}_q$ as q varies. Because $1 - \mathrm{Frob}_q$ is a separable and hence étale, isogeny,

$$P_{\mathrm{Frob}_q}(1) = \deg(1 - \mathrm{Frob}_q) = \ker(1 - \mathrm{Frob}_q) = |A(\mathbb{F}_q)|.$$

We'll leave this discussion for now.

§1 Duality pairings

We will follow Mumford [4][§20].

Recall that for an isogeny f, we have

$$\ker(f^\vee) \cong (\ker f)^\vee.$$

There exists a canonical pairing

$$\begin{aligned} \ker f \times \ker(f^\vee) &\to \mathbb{G}_m \\ (g, \chi) &\mapsto \chi(g) \end{aligned}$$

from the functorial description of the Cartier dual.

We apply this to $f = [n]$ to get a pairing

$$\begin{aligned} A[n] \times A^\vee[n] &\to \mathbb{G}_m \\ (g, \chi) &\mapsto \chi(g) \in \mu_n. \end{aligned}$$

To be precise we identify $A^\vee[n] = A[n]^\vee$. Note we have $ng = 0$ so $\chi(g)^n = 1$. Thus we get a canonical duality pairing

$$A[n] \times A^\vee[n] \xrightarrow{\overline{e}_n} \mu_n.$$

We want to pass to Tate modules, and just study this pairing for powers of each prime. Let ℓ be a prime with $(\mathrm{char}\, k, \ell) = 1$. Take $\overline{k}$-points and take the inverse limit $\varprojlim$ over $n = \ell, \ell^2, \ell^3, \ldots$ To be precise, we have to check compatibility, i.e., we have to check the following diagram commutes.

$$\begin{array}{ccccc} A[n] \times A^\vee[n] & = & A[n] \times A[n]^\vee & \longrightarrow & \mu_n \\ {\scriptstyle [m]}\uparrow & & {\scriptstyle [m]}\uparrow & & {\scriptstyle [m]}\uparrow \\ A[mn] \times A^\vee[mn] & = & A[mn] \times A[mn]^\vee & \longrightarrow & \mu_{mn} \end{array}$$

namely,

$$\overline{e}_{mn}(x, y)^m = \overline{e}_n(mx, my).$$

Commutativity of the left square comes from "functoriality" of the isomorphism $\ker(f^\vee) \cong (\ker f)^\vee$ for $f = [n]$. (One has to do some work to check this, see Mumford, [4].) Commutativity of the right square comes from functoriality of Cartier dual; this is given to us by the definition of Cartier dual.

We obtain a pairing

$$T_\ell A \times T_\ell A^\vee \xrightarrow{\overline{e}_\ell} \varprojlim_n \mu_{\ell^n}(\overline{k}) =: \mathbb{Z}_\ell(1) \cong \mathbb{Z}_\ell.$$

Note the last isomorphism is noncanonical; there is no preferred root of unity. $\mathbb{Z}_\ell(1)$ is also written $T_\ell \mathbb{G}_m$. (Note: $\mathbb{Z}_\ell$ is often considered additively.)

We summarize the properties of this map, dropping the bar from now on.

Proposition 16.3: The Weil pairing is

- $\mathbb{Z}_\ell$-bilinear
- perfect.

Proof. Note $A[n] \times A^\vee[n] \xrightarrow{\overline{e}_n} \mu_n$ is $\mathbb{Z}/n\mathbb{Z}$-bilinear; hence when we take the limit we still have a bilinear map.

The map is also perfect, because $A^\vee[n] \cong \mathrm{Hom}(A[n], \mu_n)$. Taking the limit we still get a perfect map. □

Lemma 16.4: lem:eltl Let $A \in (\mathrm{Ab}/k)$ and $f \in \mathrm{End}(A)$. Then

$$e_\ell(T_\ell(f)x, y) = e_\ell(x, T_\ell(f^\vee)y)$$

for all $x \in T_\ell A$ and $y \in T_\ell A^\vee$.

Think of this as saying we can compute the pairing downstairs or upstairs in the following diagram:

$$\begin{array}{ccccc} T_\ell A & \times & T_\ell A^\vee & \longrightarrow & \mathbb{Z}_\ell(1) \\ {\scriptstyle T_\ell(f)}\downarrow & & \uparrow{\scriptstyle T_\ell(f^\vee)} & & \| \\ T_\ell A & \times & T_\ell A^\vee & \longrightarrow & \mathbb{Z}_\ell(1). \end{array}$$

To prove this, we have to unravel the definitions. projective limit at finite level

Proof. We make the convention to write f in place of $T_\ell f$ if this will not cause confusion. It suffices to check that equality holds at every finite level, $\overline{e}_{\ell^n}(fx, y) = \overline{e}_{\ell^n}(x, f^\vee y)$. We will reinterpret this equation in terms of line bundles, and get a character out of certain line bundles. Specifically, we use the interpretation

$$y \in A^\vee[n] \leftrightarrow \left\{ \begin{array}{c} L \in \mathrm{Pic}(A \times \overline{k}) \\ L^n \text{ trivial} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} A[n]\text{-equivariant structure} \\ \text{on } \mathscr{O}_{A \times \overline{k}} \end{array} \right\}.$$

The equivariant structure is given by an $A[n]$-action on $\mathbb{A}^1_k$; we have

$$A \times \mathbb{A}^1_k / A[n]\text{-action}.$$

The action (for $\gamma \in A[n]$)

$$\gamma : (g, a) \mapsto (g + \gamma, \chi(\gamma)a).$$

Here $\chi : A[n] \to \mathbb{G}_m$, $\in A[n]^\vee$.

The point is that

$$\overline{e}_n(x, y) = \chi(x)$$

with the correspondence $y \to x$ as above. We get

$$\overline{e}_n(fx, y) = \chi(fx) = (\chi \circ f)(x) = \overline{e}_n(x, f^\vee y).$$

(check $f^\vee y \to \chi \circ f$.)

It's just unraveling long but natural maps. □

We've developed the basic properties of the Weil pairing; it's enough to remember them.

§2 Riemann forms

Definition 16.5: Let $A \in (\mathrm{Ab}/k)$, with $(\mathrm{char}\, k, \ell) = 1$, and let $\lambda : A \to A^\vee$ be a homomorphism. We define the **Riemann form** associated to λ by

$$\begin{aligned} E^\lambda : T_\ell A \times T_\ell A &\to \mathbb{Z}_\ell(1) \\ (x, y) &\mapsto e_\ell(x, \lambda y). \end{aligned}$$

Given a line bundle L, define

$$E^L := E^{\lambda_L}.$$

Roughly speaking, pullback of Poincaré line bundle becomes Mumford line bundle in dual.

Inherits all properties but a priori may not be perfect. (In worst case λ trivial map.)

Theorem 16.6: E^L is skew-symmetric, i.e. $E^L(x, y) = -E^L(y, x)$.

Proof. Omitted. (See Mumford [4]; he has 2 proofs.) □

Lemma 16.7: lem:Ef*L For any $f \in \mathrm{End}(A)$,

$$E^{f^*L}(x, y) = E^L(fx, fy).$$

Proof. We have

$$E^{f^*L}(x, y) = e(x, \lambda_{f^*L} y).$$

Recall that $\lambda_{f^*L} = f^\vee \lambda_L f$. Plugging in the formula and applying Lemma 16.4 gives

$$E^{f^*L}(x, y) = e(x, \lambda_{f^*L} y) = e(x, f^\vee \lambda_L f y) = e(fx, \lambda_L f y) = E^L(fx, fy).$$

□

Letting $\mathcal{P}$ be the Poincaré line bundle on $A \times A^\vee$, we have

$$\lambda_{\mathcal{P}} : A \times A^\vee \to (A \times A^\vee)^\vee \cong A^\vee \times A.$$

Lemma 16.8: lem:Ef*L We have

$$E^{\mathcal{P}}((x, x^\vee), (y, y^\vee)) = e(x, y^\vee) - e(y, x^\vee).$$

We have a canonical isomorphism

$$T_\ell(A \times A^\vee) \cong T_\ell A \times T_\ell A^\vee.$$

Proof. It suffices to prove the following three items.

1. $E^{\mathcal{P}}((x, 0), (y, 0)) = 0$.
2. $E^{\mathcal{P}}((0, x^\vee), (0, y^\vee)) = 0$.
3. $E^{\mathcal{P}}((x, 0), (0, y^\vee)) = e(x, y^\vee)$.

Once we have this, we write

$$\begin{aligned}(x, x^\vee) &= (x, 0) + (0, x^\vee)\\ (y, y^\vee) &= (y, 0) + (0, y^\vee).\end{aligned}$$

Expand using bilinearity and use skew-symmetry to conclude the lemma:

$$E((x,0),(0,y^\vee)) + E((0,x^\vee),(y,0)) = e(x,y^\vee) - E((y,0),(0,x^\vee)) = e(x,y^\vee) - e(y,x^\vee).$$

We now check the three items.

1. Plug in
$$A \xrightarrow{f=(\mathrm{id}_A, e_{A^\vee})} A \times A^\vee$$
in Lemma 16.8.

   Since $(\mathrm{id}_A, e_{A^\vee})^*\mathcal{P}$ is trivial because by the definition of Pic it corresponds to the trivial line bundle. Hence by Lemma 16.8
$$E^{\mathcal{P}}((x,0),(y,0)) = E^{(\mathrm{id},e)^*\mathcal{P}}(x,y) = e(x, \lambda_{\mathscr{O}_A} y) = 0.$$
because $\lambda_{\mathscr{O}_A} = 0$ (the Mumford line bundle corrsponding to the trivial line bundle is trivial).

2. Similar to (1).

3. The point is to check that $\lambda_{\mathcal{P}}(x, x^\vee) = (x^\vee, x)$. See [4]. We have to do some computations with line bundles. We obtain

$$\begin{aligned} E^{\mathcal{P}}((x,0),(0,y^\vee)) &= E^{\mathcal{P}}((x,0),(y,y^\vee)) && \text{by part 1} \\ &= e((x,0),\lambda_{\mathcal{P}}((y,y^\vee))) \\ &= e(x,y^\vee)\underbrace{e(0,y)}_{\text{trivial}}. \end{aligned}$$

(Note the pairing on

$$(T_\ell A \times T_\ell A^\vee) \times (T_\ell A^\vee \times T_\ell A)$$

is just the product of the pairings $(T_\ell A \times T_\ell A^\vee) \times (T_\ell A^\vee \times T_\ell A)$.)

□

We are now ready to prove the following.

Theorem 16.9: 1. $E^\lambda : (x,y) \mapsto e(x, \lambda y)$ is skew-symmetric.

2. There exists $L \in \mathrm{Pic}(A)$ such that $2\lambda = \lambda_L$. (Over $\overline{k}$ we can find L' so that $\lambda = \lambda_{L'}$.)

Think of this as a converse of lemma 1. If the form is skew-symmetric then it almost comes from a line bundle.

Proof. We have that (2) implies (1) by Theorem 1.

We now show (1) $\Longrightarrow$ (2). We are going to exhibit a line bundle that works. We check that

$$2\lambda = \lambda_L$$

for $L = (1 \times \lambda)^* \mathcal{P}$. We compute

$$\begin{aligned} e(x, \lambda_L y) &= E^L(x,y) && \text{definition} \\ &= E^{\mathcal{P}}(\underbrace{(1\times\lambda)(x)}_{(x,\lambda x)}, \underbrace{(1\times\lambda)(y)}_{(y,\lambda y)}) && \text{Lemma 16.4 1} \\ &= e(x,\lambda y) - e(y,\lambda x) && \text{Lemma 2} \\ &= e(x, 2\lambda y) && \text{part 1.} \end{aligned}$$

Now $e(,)$ is perfect implies $\lambda_L = 2\lambda$ in $\mathrm{Hom}(T_\ell A, T_\ell A^\vee)$. Thus $\lambda_L = 2\lambda$ in $\mathrm{Hom}(A, A^\vee) \hookrightarrow \mathrm{Hom}(T_\ell A, T_\ell A^\vee)$. □

Next time we'll talk about the Rosati involution.

Lecture 17
Thu. 11/8/12

Today we'll talk about the Rosati involution.

Recall that if $A \in (\mathrm{Ab}/k)$ is an abelian variety, $(\ell, \operatorname{char} k)$, we defined a pairing

$$A[\ell^n] \times A[\ell^n]^\vee \to \mu_\ell^n.$$

Using $A[\ell^n]^\vee \cong A^\vee[\ell^n]$, and using the functorial nature of this isomorphism, we were able to patch these map together, taking the inverse limit over $\overline{k}$-points to get

$$T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell(1),$$

where $\mathbb{Z}_\ell(1)$ is a free $\mathbb{Z}_\ell$ module of rank 1 (without a canonical basis).

Given $\lambda \in \operatorname{Hom}(A, A^\vee)$, we defined E^λ using the following diagram.

$$\begin{array}{ccccc} T_\ell A & \times & T_\ell A^\vee & \xrightarrow{e} & \mathbb{Z}_\ell[1] \\ \| & & \uparrow{\scriptstyle \lambda} & & \| \\ T_\ell A & \times & T_\ell A & \xrightarrow[E^\lambda]{} & \mathbb{Z}_\ell(1). \end{array}$$

A line bundle L gives a pairing $E^L := E^{\lambda_L}$. e is perfect $\mathbb{Z}_\ell$-linear; E^L is $\mathbb{Z}_\ell$-linear but may not be perfect We showed that

- E^L is skew-symmetric.
- E^λ is skew-symmetric. This implies $\lambda = 2\lambda_L$ and $L = (1 \times \lambda)^* \mathcal{P}$.

A variant of this is that letting

$$V_\ell A := T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

ane $\lambda \in \operatorname{Hom}^0(A, A^\vee)$ we get a $\mathbb{Q}_\ell$-bilinear pairing:

$$E^\lambda : V_\ell \times V_\ell A \to \mathbb{Q}_\ell(1) := \mathbb{Z}_\ell(1) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

We have that E^λ is skew-symmetric iff $\lambda = c\lambda_L$ for some $c \in \mathbb{Q}$ and line bundle L. After killing denominator you know $\lambda = 2\lambda_L$ for some L.

§1 Rosati involution

Definition 17.1: Let B be a finite dimensional noncommutative semisimple $\mathbb{Q}$-algebra. A map $* : B \to B$ is an **involution** if $*$ is a $\mathbb{Q}$-algebra map $B \xrightarrow{\cong} B^{\mathrm{op}}$ with $*^2 = \mathrm{id}$.

The involution $*$ is **positive** $\operatorname{Tr}_{B/\mathbb{Q}}(bb^*) > 0$ for all $b \neq 0$.

By this we mean the following. For $B = \prod B_i$, $Z(B) = \prod Z(B_i)$ and

$$\mathrm{Tr}_{B/\mathbb{Q}}(b_i) = \prod_i \mathrm{Tr}_{Z(B_i)/\mathbb{Q}}(\mathrm{Tr}^0_{B_i/Z(B_i)}(b_i))$$

for all $b \neq 0$. It doesn't hurt to think of the case of division algebras.

If you're over p-adic field, Hasse invariant changes from λ to $1-\lambda$. But number field, can do at every place, classifying invariant for opposite algebra.

Example 17.2: ex:qi-inv Suppose $[E : \mathbb{Q}] = 2$. Let $1 \neq c \in G(E/\mathbb{Q})$. Then

- c is an involution.
- c is positive iff E is imaginary.

Example 17.3: Let $B = \mathcal{M}_n(\mathbb{Q})$. Define $* : g \mapsto g^T$. It is not an automorphism because it changes the order; it is an homomorphism to the opposite algebra. This is a positive involution because $g^T g$ is a sum of squares.

Now let $B = \mathcal{M}_n(\mathbb{Q}) \times \mathcal{M}_n(\mathbb{Q})$. Then let $* : (g, h) \mapsto (h^T, g^T)$. This is an involution, but is not positive. For instance $(0, 1)$ goes to $(1, 0)$, and the trace is 0.

Now let $B = \mathcal{M}_n(E)$ as in Example 17.2. Then $* : g \mapsto (g^c)^T$ is an involution; it is positive if R is imaginary.

This is still true if we replace $\mathbb{Q}$ by a totally real field and E by a purely imaginary quadratic extension.

Let's now define the Rosati involution.

Definition 17.4: Let L be a fixed ample line bundle. The **Rosati involution**

$$\ddagger_L : \mathrm{End}^0 \to \mathrm{End}^0$$

associated to L is defined by

$$\ddagger_L(\phi) = \lambda_L^{-1} \circ \phi^\vee \circ \lambda_L.$$

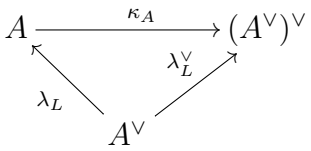
Proposition 17.5: pr:ri-inv We have the following.

1. $\ddagger_L$ is an involution.
2. ($\ddagger_L$ behaves nicely under Weil pairing) $E^L(\phi x, y) = E^L(x, \phi^{\ddagger_L} y)$.

Proof. We have

$$\begin{aligned} \ddagger_L^2 &= \lambda_L^{-1}(\lambda_L^{-1}\phi^\vee \lambda_L)^\vee \lambda_L \\ &= (\lambda_L^{-1}\lambda_L^\vee)\phi(\lambda_L^{-1}\lambda_L^\vee). \end{aligned}$$

We've shown before that $\lambda_L = \lambda_L^\vee$; this is from the commutative triangle



For part 2, note the RHS equals

$$\begin{aligned} E^L(x, \lambda_L^{-1}\phi^\vee\lambda_L y) &= e(x, \lambda_L(\lambda_L^{-1}\phi^\vee\lambda_L)y) \\ &= e(\phi x, \lambda_L y) \\ &= E^L(\phi x, y). \end{aligned}$$

This equals the LHS. □

Here's our first deep fact.

Theorem 17.6: $\ddagger_L$ is a positive involution.

Proof. See [4, §21] for $k = \overline{k}$ and [7] for $k \neq \overline{k}$. □

§2 Symmetric elements

Consider the group homomorphism

$$\begin{aligned} \Lambda : \operatorname{Pic} A &\to \operatorname{Hom}(A, A^\vee) \\ \mathscr{L} &\mapsto \lambda_{\mathscr{L}}. \end{aligned}$$

To see this is a group homomorphism, note that the correspondence below associates $\lambda_{\mathscr{L}}$ and $M(L)$ by definition:

$$\begin{aligned} A^\vee(A) &\cong \operatorname{Pic}^0(A \times A) \\ \lambda_{\mathscr{L}} &\leftrightarrow M(\mathscr{L}) = \mu^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1}. \end{aligned}$$

Under this correspondence,

$$\begin{aligned} \lambda_{\mathscr{L}_1} - \lambda_{\mathscr{L}_2} &\leftrightarrow M(\mathscr{L}_1) \otimes M(\mathscr{L}_2)^{-1} \\ \lambda_{\mathscr{L}_1 \otimes \mathscr{L}_2^{-1}} &\leftrightarrow M(\mathscr{L}_1 \otimes \mathscr{L}_2^{-1}). \end{aligned}$$

The RHS's are congruent, just by unraveling the definition of $M(\mathscr{L})$. Hence Λ is a group homomorphism.

Proposition 17.7: Let $\mathscr{L} \in \operatorname{Pic} A$. Then $\lambda_{\mathscr{L}} = 0$ iff $\mathscr{L} \in \operatorname{Pic}^0 A$.

Note our definition of Pic^0 is a bit different from Mumford's. From Mumford's definition this is trivial but from our definition it's not.

Proof. $\Leftarrow$: See [4, §8, Theorem 1].
$\Rightarrow$: Exercise. □

Choose an ample line bundle L. This gives an isogeny $\lambda_L \in \mathrm{Hom}^0(A^\vee, A)$. Now consider the following diagram.

$$\frac{\mathrm{Pic}\, A}{\mathrm{Pic}^0} \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}, \cong} \mathrm{Hom}^0(A, A^\vee) \xrightarrow{\lambda_L^{-1}} \mathrm{End}^0(A)$$
$$\psi \mapsto \lambda_L^{-1}\psi.$$

Definition 17.8: The **Neron-Severi** group of A is

$$\mathrm{NS}(A) := \frac{\mathrm{Pic}\, A}{\mathrm{Pic}^0 A}.$$

First map doesn't depend on ℓ but the second does.

Proposition 17.9: We have

$$\mathrm{im}(\lambda_L^{-1} \circ \Lambda_{\mathbb{Q}}) = (\mathrm{End}^0(A))^{\ddagger_L = 1} := \left\{\phi \in \mathrm{End}^0(A) : \phi^{\ddagger_L} = \phi\right\}.$$

We call the elements in the right set **symmetric elements**.

Proof. Let $\phi \in \mathrm{End}^0(A)$. We have the following chain of equivalences.

1. $\phi \in \mathrm{im}(\lambda_L^{-1})$
2. $\lambda_L \phi \in \mathrm{im}(\Lambda_{\mathbb{Q}})$
3. $\lambda_L \phi = c\lambda_{\mathscr{L}}$ for some $\mathscr{L}$ and $c \in \mathbb{Q}$.
4. $e(x, \lambda_L \phi y) = -e(y, \lambda_L \phi x)$ for all x, y.
5. $E^L(x, \phi y) = -E^L(y, \phi x) = E^L(\phi x, y)$.
6. $E^L(x, \phi y) = E^L(x, \phi^{\ddagger_L} y)$ for all x, y. (To get here, we used Proposition 17.5.)
7. $\phi y = \phi^{\ddagger y}$ for all $y \in V_\ell A$. (by perfectness)
8. $\phi = \phi^\ddagger$ in $\mathrm{End}^0(T_\ell A)$.
9. $\phi = \phi^\ddagger$ in $\mathrm{End}^0(A)$ (because it injects into $\mathrm{End}^0(T_\ell A)$).

□

Corollary 17.10: cor:Qsubalg—g Let $A \in (\mathrm{Ab}/k)$ of dimension g. For $K \subset (\mathrm{End}^0 Q)^{\ddagger_L = 1}$ be a $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(A)$ (a priori non-commutative). Then $[K : \mathbb{Q}] \mid g$.

This imposes a condition on what the center of the endomorphism algebra can be. Roughly speaking the center is preserved by the Rosati involution. If it's nontrivial it's an automorphism of order 2.

Index 1 or 2 subfield of the center is contained in here. For that field you can apply this corollary.

Example 17.11: Suppose A is simple. Then $K = (Z(\mathrm{End}^0(A)))^{\ddagger_L=1}$.

Proof of Corollary 17.10. Step 1: K is a field. Let $\phi, \psi \in K$. Because $K \subseteq (\mathrm{End}^0 A)^{\ddagger_L=1}$.

$$\phi\psi = (\phi\psi)^{\ddagger=1} = \psi^{\ddagger_L}\phi^{\ddagger_L} = \psi\phi.$$

Step 2: The function

$$\begin{aligned} \chi : \mathrm{Pic}\, A &\to \mathbb{Z} \\ M &\mapsto \chi(M) \end{aligned}$$

induces a map

$$\chi_{\mathbb{Q}} : \frac{\mathrm{Pic}\, A}{\mathrm{Pic}^0(A)} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}$$

We won't prove the first fact.

Fact 17.12: ([4, §16]) $\chi(M \otimes M') = \chi(M)$ for all $M' \in \mathrm{Pic}^0(A)$.

Here is an intuitive explanation. Discrete locally constant valued function. Moduli spce Pic^0. M' defines point in conn scheme. Line bund corresp ident. Alg family connecting them. Euler char doesn't change. Constant in whole conn component. You can make this rigorous.

We know that χ is a polynomial function on $\mathrm{Pic}\, A \otimes_{\mathbb{Z}} \mathbb{Q}$, homogeneous of degree g (§16, $\chi(L) = \frac{(D^g)}{g!}$. Then $\chi(L^{\otimes n}) = \frac{n^g(D^g)}{g!}$); we already used this in Section 19. (calculating $\chi(M^n)$).

Let's consider the diagram from a slightly different perspective. We have the following maps

$$\begin{array}{ccccc} (\mathrm{End}^0 A)^{\ddagger_L=1} & \xleftarrow[\cong]{} & \frac{\mathrm{Pic}\, A}{\mathrm{Pic}^0 A} \otimes \mathbb{Q} & \xrightarrow{\chi_{\mathbb{Q}}} & \mathbb{Q} \\ & \searrow^{\xi'} & & \searrow_{\chi'_{\mathbb{Q}}} & \\ & & & & \mathbb{Q} \end{array}$$

where teh top left map is $\lambda^{-1}\lambda_M \leftarrow\!\shortmid M$. We have $\chi' = \frac{1}{\chi(L)}\chi$ (L is fixed).

Step 3: $\xi'|_K$ is a norm function.

We have $\xi'(1) = \chi'_{\mathbb{Q}}(L) = \frac{\chi(L)}{\chi(L)} = 1$ (this is why we scaled it).

Lemma 17.13: Let B be a finite-dimensional vector space and $f : V \to \mathbb{Q}$ be polynomial with $f(1) = 1$. Then $f(xy) = f(x)f(y)$ iff $f(xy)^2 = f(x)^2 f(y)^2$.

Proof. Exercise. □

If suffices to prove that

$$\xi'((\lambda_L^{-1}\lambda_M)(\lambda_L^{-1}\lambda_{M'}))^2 = \xi'(\lambda_L^{-1}\lambda_M)^2\xi'(\lambda_L^{-1}\lambda_{M'})^2$$

Plugging in another result from §16, $\xi'(\lambda_L^{-1}\lambda_M) = \frac{\chi(M)^2}{\chi(L)^2}$.

Let K be closed under multiplication. We find $K \ni \lambda_L^{-1}\lambda_{M''} = \lambda_L^{-1}\lambda_M \circ \lambda_L^{-1}\lambda_{M'}$. Using another fact from §16, $\chi(L)^2 = \deg \lambda_L$, unraveling, we get the RHS is

$$\frac{\deg \lambda_M}{\deg \lambda_L} \cdot \frac{\deg \lambda_{M'}}{\deg \lambda_L}.$$

Using the fact that the degree is multiplicative (two isogenies, think of the extension degree of function field, or generic number of fibers), even when extended to Hom^0, we get the LHS is

$$\frac{\deg \lambda_{M''}}{\deg \lambda_L} = \frac{\deg(\lambda_M \circ \lambda_L^{-1} \circ \lambda_{M'})}{\deg \lambda_L} = \frac{\deg \lambda_M (\deg \lambda_L)^{-1} \deg \lambda_{M'}}{\deg \lambda_L}$$

which is the RHS.

Step 4: By Step 3, we conclude that

$$\xi'|_{\mathbb{Q}} = (N_{K/\mathbb{Q}}^{\min})^r, \qquad r \in \mathbb{Z}.$$

The LHS is a norm of degree g and $\mathbb{N}_{K/\mathbb{Q}}^{\min}$ has degree $[K : \mathbb{Q}]$. Thus $[K : \mathbb{Q}] \mid g$. □

Let's summarize what we have found out about the endomorphism algebra.

§3 Summary on $\mathrm{End}^0 A$

Let $A \in (\mathrm{Ab}/k)$, and let the center be $F = Z(\mathrm{End}^0 A)$; this is finite dimensional semisimple over $\mathbb{Q}$.

Then $\mathrm{End}^0 A$ is a finite-dimensional semisimple $\mathbb{Q}$-algebra. Suppose A is simple and F is a field. Then

- $\mathrm{End}^0(A)$ is a finite division algebra over $\mathbb{Q}$.
- $[\mathrm{End}^0 : F]^{\frac{1}{2}}[F : \mathbb{Q}] = 2g$. Using complex theory, we actually have $[\mathrm{End}^0 A : \mathbb{Q}] \mid 2g$ is $\mathrm{char}\, k = 0$.
- $\mathrm{End}^0(A)$ has a positive involution.

- $F^{\ddagger_L=1}$ is a totally real subfield, of index 1 or 2 in F. F is a "CM field" or a totally real field.
- If $K \subseteq (\mathrm{End}^0 A)^{\ddagger_L}$ then $[K:\mathbb{Q}] \mid g$.

Now we can go to the purely algebra side and try classify all division algebra with positive involution with all these properties, and make a list of candidates, [4, §21].

Converse statement: given algebra can we realize as endomorphism algebra of ab var?
finfield: Honda-Tate theory
Char 0: complex theory.
Complete info or not?
next time complex abelian var.

Lecture 18
Tue. 11/13/12

Last time we showed that for $A \in (\mathrm{Ab}/k)$, an ample line bundle L on A induces a Rosati involution

$$\ddagger_L : \phi \mapsto \lambda_L^{-1} \phi^\vee \lambda_L$$

on $\mathrm{End}^0(A)$. This is a positive involution. We will see that the Rosati involution leads to the Riemann Hypothesis for A.

First we prove a fact about the Frobenius.

Theorem 18.1: thm:frob-ri-frob Let $A \in (\mathrm{Ab}/\mathbb{F}_q)$. Then

$$\mathrm{Frob}_q^{\ddagger_L} \mathrm{Frob}_q = [q].$$

Proof. We have

$$\begin{aligned} &\lambda_L^{-1} \mathrm{Frob}_q^\vee \lambda_L \mathrm{Frob}_q = [q] \\ \iff\ &\mathrm{Frob}_q^\vee \lambda_L \mathrm{Frob}_q = [q]\lambda_L. \end{aligned}$$

Now the LHS is (using $f^\vee \lambda_L f = \lambda_{f^* L}$ and noting $\mathrm{Frob}_q^* L \cong L^{\otimes q}$) $\lambda_{\mathrm{Frob}_q^* L} = \lambda_{L^{\otimes q}} = q\lambda_L$. Construction of Mumford line bundle commutes with tensor.

$\Lambda : \mathrm{Pic}\, A \to \mathrm{Hom}(A, A^\vee)$, $L \mapsto \lambda_L$ is group homomorphism. □

While we won't prove it here, the Riemann hypothesis for abelian varieties relies on Theorem 18.1.

§1 Complex abelian varieties: An overview

We'll talk about complex abelian varieties. We start with elliptic curves over $\mathbb{C}$.

Let

$$\tau \in \mathcal{H} := \{z \in \mathbb{C} : \Im z > 0\}.$$

Define the lattice

$$\Lambda_\tau := \mathbb{Z} \otimes \mathbb{Z}\tau$$

and

$$E_\tau := \mathbb{C}/\Lambda_\tau$$

as a complex manifold of dimension 1 with group structure (call it an "abelian manifold," if you'd like).

Note although E_τ is defined as a complex manifold, it comes from an algebraic variety in the following sense. We have a map

$$\begin{aligned} E_Z \cong \mathbb{C}/\Lambda_\tau &\xrightarrow{\cong} \{y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)\} \overset{\text{closed}}{\subset} \mathbb{P}^2(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)) \end{aligned}$$

where $\wp$ is the Weierstrass $\wp$-function. We have that E_τ is a projective algebraic variety with group structure.

Higher dimensional complex torus, algebraic structure, better handle on abelian variety. Difficult construct. Lattice, magincally an abelian varity comes out. Doesn't work exactly that way.

In fact, we have bijections compile

$$\begin{gathered} \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \overset{1\text{–}1}{\longleftrightarrow} \left\{\begin{matrix}\mathbb{C}\text{-tori} \\ \text{of dimension } 1\end{matrix}\right\}/\cong \overset{1\text{–}1}{\longleftrightarrow} \left\{\begin{matrix}\text{elliptic} \\ \text{curves}/\mathbb{C}\end{matrix}\right\}/\cong \\ \tau \mapsto \mathbb{C}/\Lambda_\tau \mapsto \text{Projective curve } y^2 = 4x^3 + \cdots \end{gathered}$$

We have the middle is projective complex manifold, the RHS is a projective curve.

We have $x \mapsto (\omega \mapsto \int_0^x \omega)$, $x \in E_{\mathrm{an}}$. $E(\mathbb{C}) \cong H^0(E_{\mathrm{an}}, \Omega^1)^*/H_1(E_{\mathrm{an}}, \mathbb{Z})$, where the embedding is given by $\gamma \mapsto (\omega \mapsto \int_\gamma \omega)$, and $E \mapsto E(\mathbb{C})$.

nonvanish global diffl form tangent space cotangent to that guy, think of as exponential map.

We're seeking a generalization. Not all $\mathbb{C}$-tori of dimension g correspond to abelian varities. We need an extra condition, and then we get

$$\left\{\begin{matrix}\text{polarizable} \\ \mathbb{C}\text{-tori} \\ \text{of dimension } g\end{matrix}\right\}/\cong \overset{1\text{–}1}{\longleftrightarrow} \left\{\begin{matrix}\text{abelian variety}/\mathbb{C} \\ \text{of dimension } g\end{matrix}\right\}/\cong .$$

The generalization of the upper half plane is the Siegel upper half space $\mathcal{H}_g$ of dimension $\frac{g(g+1)}{2}$.

$$\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathcal{H}_g \overset{1\text{–}1}{\longleftrightarrow} \left\{\begin{matrix}\text{principally polarized} \\ \mathbb{C}\text{-torus of dimension } g\end{matrix}\right\}/\cong .$$

Polarizable vs. polarized. Admits one polarization, vs. actually a pair: complex torus and principal polarization.

Elliptic curve has only 1 possible polarization up to congruence.

For torus a polarization will be the same as a Riemann form. A polarization is $(A, \text{Riemann form})$.

§2 $\mathbb{C}$-tori

Definition 18.2: A $\mathbb{C}$-torus is a complex manifold isomorphic to V/Λ where

- V is a $\mathbb{C}$-vector space of dimension $g < \infty$
- Λ is a free $\mathbb{Z}$-module generated by some $\mathbb{R}$-basis of V (i.e., a lattice).

Note a $\mathbb{C}$-torus is a compact complex manifold with group structure, i.e. a compact Lie group.

We can show that

$$\mathrm{Hom}(V/\Lambda, V'/\Lambda') = \left\{ \begin{matrix} \phi \in \mathrm{Hom}_{\mathbb{C}-\mathrm{linear}}(V, V') \text{ such that} \\ \phi(\Lambda) \subseteq \Lambda' \end{matrix} \right\}.$$

A different perspective is given by the following.

Definition 18.3: A **Riemann pair** (Λ, J) where Λ a free $\mathbb{Z}$ module of finite rank and $J \in \mathrm{End}_{\mathbb{R}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{R})$ such that $J^2 = -1$. (Hence there is a "complex structure" on $\Lambda_{\mathbb{R}} := \Lambda \otimes \mathbb{R}$.)

The reason for introducing this is that given a complex torus we can associate it with a Riemann pair.

$$\begin{aligned} (\mathbb{C}\text{-torus}) &\to (\text{Riemann pairs}) \\ V/\Lambda &\mapsto (\Lambda, J = \text{multiplication by i} \circlearrowleft V = \Lambda_{\mathbb{Z}} \otimes \mathbb{R}) \\ (\Lambda \otimes_{\mathbb{Z}} \otimes \mathbb{R})/\Gamma &\leftarrow\!\shortmid (\Lambda, J). \end{aligned}$$

Here the complex structure on $\Lambda \otimes_{\mathbb{Z}} \otimes \mathbb{R}$ is given by the isomorphism $\mathbb{R}[J]/(J^2 + 1) \cong \mathbb{C}$, with $J \leftrightarrow i$.

The key questions are

- is the manifold projective?
- algebraic?

As we will see, these questions are related. In algebraic geometry, to study this question you study ample line bundles. It would be nice to have a classification of line bundles. That's what we'd like to do.

2.1 Line bundles on $X_{\mathbf{an}} = V/\Lambda$

We'll soon consider algebraic varieties over $\mathbb{C}$; we'd like to distinguish algebraic and analytic varieties.

We follow [4, §2]. We have a correspondence (Appell-Humbert Theorem)

$$\operatorname{Pic} X \xrightarrow{\cong} \left\{ \begin{array}{c} (E,\alpha),\ E : \Lambda \times \Lambda \to \mathbb{Z} \\ \text{bilinear alternating, } E(Jx,Jy) = E(x,y) \forall x,y \in \Lambda \\ \exists \alpha : \Lambda \to \mathbb{C}_1^* = \{|z| = 1\} \dots \end{array} \right\}.$$

We'll give the details. Correspondence $L(E,\alpha) \leftarrow\!\shortmid (E,\alpha)$.

Pull back from $V \times \Lambda$ to V. Line bundles correspond to certain Λ-action on V. Action on trivial line bundle over V.

We can make the above correspondence explicit.

The correspondence restricts to

$$\operatorname{Pic}^0(X_{\mathrm{an}}) \xrightarrow{\cong} \{(0,\alpha) : \alpha \in \operatorname{Hom}_{\mathrm{cont}}(\Lambda, \mathbb{C}_1^*)\}$$

Theorem 18.4 (Lefschetz, §3)**:** $L(E,\alpha)$ is ample iff

$$\text{for all } x \in \Lambda, x \neq 0, \qquad E(x,Jx) > 0.$$

(condition 3) (Different conventions. Here, follow Milne's notation.)

Definition 18.5: A form satisfying the following is a **Riemann form** (a polarization).

1. $\mathbb{Z}$-bilinear and alternating.
2. $E(Jx,Jy) = E(x,y)$ for all $x,y \in \Lambda$.
3. For all $x \in \Lambda, x \neq 0, \qquad E(x,Jx) > 0.$

Consequently, say $X_{\mathrm{an}} \leftrightarrow (\Lambda, J)$. If there exists a Riemann form E for (Λ, J), then there exists $X_{\mathrm{an}} \hookrightarrow \mathbb{P}^N(\mathbb{C})_{\mathrm{an}}$ a closed imbedding.

Analytic topology finer than Zariski, but the amazing thing here is that analytic closed subsets are projectively closed in Zariski topology.

We'll use Chow's Theorem as a black box, and get if X_{an} is Zariski closed so X_{an} is a projective variety over $\mathbb{C}$.

sat lin cond, then torus is alg variety, even proj variety.

For the converse, let's get some general facts, using Chow's Theorem and Serre's GAGA. We have a faithful map

$$(x, \mathscr{O}_X) \mapsto (X_{\mathrm{an}},$$
$$(\text{algebraic varieties}/\mathbb{C}) \mapsto (\mathbb{C}\text{-analytic spaces})$$

If we have alg variety, then we can cover it with open affine varieties, locally closed sets in affine spaces. Complex analytic structure on $S \subseteq \mathbb{C}^N$ locally closed. This correspondence restricts to the following.

$$\begin{gathered}(\text{algebraic varieties}/\mathbb{C}) \mapsto (\mathbb{C}\text{-analytic spaces}) \\ (\text{smooth algebraic varieties}/\mathbb{C}) \mapsto (\text{smooth } \mathbb{C}\text{-analytic spaces})\end{gathered}$$

where the bottom map is a bijection, actually Smooth projective, get equivalence of categories. Don't expect fully faithful because exponential map cannot be imitated by polynomial or rational map. But faithful because happening on level of points, if 2 maps same on points, then same algebraic maps.

In the bottom case,

$$\mathrm{Coh}(X) \xrightarrow{\cong} \mathrm{Coh}(X_{\mathrm{an}}).$$

Algebraic Picard group same as analytic Picard group.

In equiv of categories, proj manifold has unique alg structure. If two alg varieties is analy, then already is as alg varieties.

Theorem 18.6: Let X_{an} be a $\mathbb{C}$-torus, corresponding to (Λ, J). Then the following are equivalent.

1. (Λ, J) admits a Riemann form.
2. X_{an} is a projective manifold.
3. There exists Y algebraic variety over $\mathbb{C}$, such that $Y_{\mathrm{an}} \cong X_{\mathrm{an}}$.
4. There exist $f_1, \ldots, f_g$ algebraically independent meromorphic functions on X_{an}.

Proof. For (1) $\implies$ (2) use Lefschetz Theorem, for (2) $\implies$ (3) use Chow's Theorem, for (3) $\implies$ (4) use for smooth projective, set of meromorphic functions are set of rational function, $\mathbb{C}(X)$, transcendence degree g. For (4) $\implies$ (1) the idea is that if we have $f_1, \ldots, f_g$, then we can form a divisor $(D_i) = (\text{poles of } f_i)$. Take linear combination with coefficient order of poles. Then take $D = \sum D_i$ and find that $L(D) = L(E, \alpha)$ with E a Riemann form. □

The upshot of this is that the set of Riemann pairs (Λ, J) admitting a Riemann form ("polarizable") correspond to $\mathbb{C}$-tori which are algebraic, which corresponds to abelian varieties over $\mathbb{C}$.

$$\left\{\begin{array}{c}\text{Riemann pairs } (\Lambda, J) \\ \text{admitting a Riemann form}\end{array}\right\} \overset{1\text{–}1}{\longleftrightarrow} \left\{\begin{array}{c}\mathbb{C}\text{-tori which} \\ \text{are algebraic}\end{array}\right\} \overset{1\text{–}1}{\longleftrightarrow} (\mathrm{Ab}/\mathbb{C})\,.$$

Not just pos semidef, but pos def/ (Hermitian form). No isotropic subspace where trivial. Mod out by subspace, down to smaller dimension, make work.

§3 Duals

Let X be an abelian variety over $\mathbb{C}$, $X_{\text{an}} = V/\Lambda$. We have a dual abelian variety over $\mathbb{C}$, $X^\vee$. What is $(X^\vee)_{\text{an}} = V'/\Lambda'$? We want to describe V', Λ' in terms of V and Λ.

We know that as groups

$$\text{Pic}^0(X) \cong \text{Hom}(\Lambda, \mathbb{C}_1^*) \overset{?}{\cong} V'/\Lambda'.$$

How to put complex torus structure such that also abelian variety?

The answer is that the Poincaré line bundle $\mathcal{P} \to X \times X^\vee$ goes to $\mathcal{P}_{\text{an}} = L(\mathscr{E}, \alpha) \to X_{\text{an}} \times X_{\text{an}}$. Eventually we get a Hermitian pairing

$$V \times V' \to \mathbb{C}$$

and restricting,

$$\Lambda \times \Lambda' \to \mathbb{Z}.$$

So we let V' be the Hermitian dual,

$$V' = V^* = \text{Hom}_{\mathbb{C}\text{-antilinear}}(V, \mathbb{C}) \cong \{\phi : V \to \mathbb{C} : \phi(az) = \overline{a}\phi(z), a \in \mathbb{C}\}$$

and

$$\Lambda' = \{\phi \in V : \text{im}\phi(\lambda) \in \mathbb{Z} \text{ for all } \lambda \in \Lambda\}$$

we can check there exists a Riemann form V'/Λ'. We have as a group,

$$\begin{aligned} V'/\Lambda' &\xrightarrow{\cong} \text{Hom}(\Lambda, \mathbb{C}_1^*) \\ \phi &\mapsto (\lambda \mapsto e^{-2\pi i \text{im}\phi(\lambda)}). \end{aligned}$$

Given Pic^0 the structure of complex polarizable torus.

Why are Riemann forms polarizations?

§4 Polarization

Given X a complex abelian variety corresponding to (Λ, J), we have

$$\left\{\begin{matrix}\text{Riemann forms} \\ \text{for } (\Lambda, J)\end{matrix}\right\} \overset{1-1}{\longleftrightarrow} \left\{\begin{matrix}\text{polarization} \\ X \to X^\vee\end{matrix}\right\}$$
$$E \mapsto \lambda_L(E, \alpha).$$

A priori this construction is analytic. Can view as algebraic, associate...? Polarization is by definition a morphism $X \to X^\vee$ which have the form λ_L for some L. Since line bundles exhausted by $L(E, \alpha)$, surj.If two things are same, Riemann form same, well-defined (doesn't depend α).

Principal pol. are those inducing isomorphisms. Riemann forms give perfect pairing on λ, equivalently determinant 1. In the above, those E with $\det E = 1$ correspond to principal polarizations $X \xrightarrow{\cong} X^\vee$. This Riemann form really is compatible with the ℓ-adic Riemann form, formula relating them, just tensor this with $\mathbb{Z}_\ell$. Naturally, share very similar characteristics. All formulas here sim to formulas there.

Thursday, CM abelian varieties.

Lecture 19
Thu. 11/15/12

Today we'll talk about CM abelian varieties. Last time we talked about complex abelian varieties. This is especially relevant to abelian varieties with complex multiplication.

§1 CM Abelian Varieties

First, some definitions.

Definition 19.1: Suppose $A \in (\mathrm{Ab}/k)$ is k-simple of dimension g. Let $F := Z(\mathrm{End}^0(A))$ (this is a field because A is simple, so $\mathrm{End}^0(A)$ is a central division algebra over F). We say that A is of **CM type**, or A is a CM abelian variety, if

$$[\mathrm{End}^0(A) : F]^{\frac{1}{2}}[F : \mathbb{Q}] = 2g.$$

Note that $\leq$ is always true. We've even shown the LHS divides the RHS by using the norm function defined by the degree function.

Lemma 19.2: Let $k = \mathbb{C}$ (or any characteristic 0 field).[13]

For all simple $A \in (\mathrm{Ab}/\mathbb{C})$, we have

$$[\mathrm{End}^0(A) : \mathbb{Q}] \leq 2g.$$

Proof. We have that $\mathrm{End}^0(A)$, a finite-dimensional algebra over $\mathbb{Q}$, acts on the first homology group $H_1(A_{\mathrm{an}}, \mathbb{Q})$:

$$\mathrm{End}^0 A \circlearrowright H_1(A_{\mathrm{an}}, \mathbb{Q}).$$

The only finitely generated left D-module is congruent to $D^{\oplus r}$ so $2g = r[D : \mathbb{Q}]$, and $[D : \mathbb{Q}] \mid g$.

Note that if we extend to larger field, the endomorphism algebra can only increase: We have $\mathrm{End}^0_k(A) \hookrightarrow \mathrm{End}^0_{\overline{k}}(A)$ by $f \mapsto f_{\overline{k}}$. □

Remark: The lemma fails when the characteristic is nonzero. A division algebra over $\mathbb{Q}$ may not be a division algebra when tensored with $\overline{\mathbb{F}_p}$. A counterexample is a supersingular elliptic curve over $\overline{\mathbb{F}_p}$. We have $\mathrm{End}^0 A$ is the unique quaternionic algebra over $\mathbb{Q}$, and

$$[\mathrm{End}^0 A : \mathbb{Q}] = 4.$$

Corollary 19.3: Let $A \in (\mathrm{Ab}/k)$ be a simple CM abelian variety, and k be of characteristic 0. Then $\mathrm{End}^0(A)$ is a field of degree $2g$ over $\mathbb{Q}$.

[13] The Lefschetz principle says that if something true over $\mathbb{C}$, then the same is true over any algebraically closed characteristic 0 field; just embed the field in $\mathbb{C}$.

Proof. We have $[\mathrm{End}^0(A) : \mathbb{Q}] \leq 2g$ and $[\mathrm{End}^0(A) : F]^{\frac{1}{2}}[F : \mathbb{Q}] = 2g$. This gives that we must have equality. □

We know that $\mathrm{End}^0(A)$ carries a positive involution, and this restricts the possibilities of F. So let's classify number fields with positive involutions.

§2 CM fields

Definition 19.4: Let $F/\mathbb{Q}$ be a finite field extension. We say that F is **totally real** if every field embedding $F \hookrightarrow \mathbb{C}$ factors through $\mathbb{R} \subset \mathbb{C}$, i.e., has image in $\mathbb{R}$. We say that F is **CM** if it is a totally imaginary quadratic extension of a totally real field.

We relate these to number fields with positive involutions.

Lemma 19.5: F is CM if and only if there exists a nontrivial automorphism $c \in \mathrm{Aut}(F)$ such that for every embedding $F \hookrightarrow \mathbb{C}$, complex conjugation on $\mathbb{C}$ restricts to F.

$$\overline{\bullet}|_F = \mathbb{C}.$$

$$\begin{array}{ccc} F & \hookrightarrow & \mathbb{C} \\ \circlearrowleft & & \circlearrowleft \\ c & \longleftrightarrow & \overline{\bullet}. \end{array}$$

Then the fixed field F^c is totally real, and $[F : F^c] = 2$.

Example 19.6: If a quadratic extension of $\mathbb{Q}$ is...

- real, then it is totally real.
- imaginary, then it is CM.

We have that, for $n \geq 3$, $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is a totally real subfield of $\mathbb{Q}(\zeta_n)$ which is CM.

A lot of fields are neither CM nor totally real. Any field with both a complex embedding and a real embedding such as $\mathbb{Q}(\sqrt[3]{2})$ is neither CM nor totally real.

Lemma 19.7: If $(F, *)$ is a number field with a positive involution, then either

1. $* = 1$ and F is totally real, or
2. $* \neq 1$ and F is CM. ($* = \overline{\bullet}|_F$ for any $F \hookrightarrow \mathbb{C}$.)

Proof. Tensoring with $\mathbb{R}$, we get an action $*_{\mathbb{R}} = * \otimes 1$ action on $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R}$. We know that

$$F \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$$

where r is the number of real embeddings and s is the number of conjugate pairs of complex embeddings (so $r+2s=[F:\mathbb{Q}]$). Now we just check that the positive involution on $\mathbb{R}^r\times\mathbb{C}^s$ (as a $\mathbb{R}$-algebra) has to be

$$(x,\dots,x_r,y_1,\dots,y_s)\mapsto(x_1,\dots,x_r,\overline{y_1},\dots,\overline{y_s}).$$

(First show that a positive involution has to preserve each component. Then the theorem is almost immediate.)

(See notebook diag.)

Suppose $*\neq 1$. Then the trivial automorphism cannot restrict to a nontrivial automorphism. Hence $r=0$. Then $F^{*=1}$ is totally real (this is obvious in (2)), and $F^{*=1}\subset F$ of index 2.

Suppose $*=1$. Then (2) can't happen, so $s=0$. We've shown $\implies$. Conversely, if F is totally real or CM, then you can define a positive involution on F. □

Proposition 19.8: Let $A\in(\mathrm{Ab}/k)$ be a simple CM abelian variety over k with characteristic 0. Then $\mathrm{End}^0 A$ is a CM field of degree $2g$ over $\mathbb{Q}$.

Proof. We have seen that $[(\mathrm{End}^0 A)^{*=1}:\mathbb{Q}]\mid g$ where $*$ is the Rosati involution. In particular, if $\mathrm{End}^0(A)$ were totally real, then

$$(\mathrm{End}^0(A))^{*=1}=\mathrm{End}^0(A)$$

which has degree $2g$ over $\mathbb{Q}$; this is a contradiction.

Hence $\mathrm{End}^0(A)$ is a CM field. □

Note that the involution doesn't depend on the choice of polarization because there is only 1 involution, that induced by complex conjugation.

Is this a sufficient condition? Given such a CM field, is there an abelian variety with that field as $\mathrm{End}^0(A)$? The answer turns out to be yes.

§3 CM type

Definition 19.9: Let F be a CM field. A **CM-type** over F is

$$\Phi\subseteq\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(F,\mathbb{C})$$

where

$$\Phi\sqcup c(\Phi)=\mathrm{Hom}(F,\mathbb{C}).$$

We say that (F,Φ) is a **CM-pair**.

(Given a morphism Φ we can twist it by complex conjugation. There is no ambiguity because c on F is the restriction of c on $\mathbb{C}$.)

Given $A\in(\mathrm{Ab}/\mathbb{C})$ a simple CM abelian variety and an embedding $i:F\xrightarrow{\cong}\mathrm{End}^0(A)$ where F is a CM field, let's construct $(A,i)\mapsto(F,\Phi)$.

Theorem 19.10: Fix a CM field F of degree $2g$. Then we have a 1-1 correspondence

$$\left\{\begin{matrix}\text{dimension } g \text{ CM abelian variety} \\ (A,i)\end{matrix}\right\} / \cong \overset{1\text{–}1}{\longleftrightarrow} \left\{\begin{matrix}\text{CM-pairs} \\ (F,\Phi)\end{matrix}\right\}$$
$$(A,i) \mapsto (F,\Phi)$$

(Note a dimension g CM abelian variety over F is automatically simple.)

Proof. We have that

$$H_1(A_{\text{an}},\mathbb{C}) \cong \text{Lie}(A) \oplus \overline{\text{Lie}(A)};$$

this is the dual of the Hodge decomposition of $H^1(A_{\text{an}},\mathbb{C})$. We have that

$$\text{Lie}(A) \circlearrowleft F \otimes_{\mathbb{Q}} \mathbb{C} \cong \prod_{\sigma \in \text{Hom}(F,\mathbb{C})} F_\sigma$$

where each $F_\sigma \cong \mathbb{C}$.

A module over a product of fields is just a product of vector spaces over fields. We have that as $F \otimes \mathbb{C}$-modules,

$$\text{Lie}(A) \cong \prod_\sigma F_\sigma^{n_\sigma}$$

where $n_\sigma \in \mathbb{N}_0$. (Note that $\text{Lie}\, A \cong T_0 A$.) Then

$$\overline{\text{Lie}(A)} \cong \prod_\sigma F_\sigma^{n_{c\sigma}}.$$

We have $H_1(A,\mathbb{Q})$ is a free F-module of rank 1 because it is a F-vector space, and $\dim_{\mathbb{Q}} H_1(A,\mathbb{Q}) = 2g = [F:\mathbb{Q}]$. Hence $\text{Lie}(A) \oplus \overline{\text{Lie}(A)}$ is a free moidule over $F \otimes \mathbb{C} \cong \prod_\sigma F_\sigma$ of rank 1.

Thus $n_\sigma + n_{c\sigma} = 1$ for all σ. This means that

$$\Phi := \{\sigma \in \text{Hom}(F,\mathbb{C}) : n_\sigma = 1\}$$

is a CM-type on F.

We basically read off the Φ by looking at action on tangent space.

Next we have to show there exists an inverse map. We do this by constructing the abelian variety as a complex torus.

We define

$$(\Lambda = \mathcal{O}_F, J) \leftarrow\!\shortmid (F,\Phi)$$

as follows. We have $F \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\cong} \prod_{\sigma\in\Phi} \underbrace{F_\sigma}_{\mathbb{C}}$ via $(a \otimes b) \mapsto (\sigma(a)b)$; let J be multiplication by $i \in \mathbb{C}$. $\mathscr{O}_F$ by left multiplication?

We have a categorical equivalence

$$A \leftarrow\!\shortmid (\Lambda, J),$$

and $\mathscr{O}_F$ acting on Λ and on A. This gives : $F \hookrightarrow \text{End}^0 A$. □

Actually we can define everything over a number field. Thus this is deeply arithmetic.

§4 From $\mathbb{C}$ to $\overline{Q}$

Our goal is to show that each CM abelian variety over $\mathbb{C}$ can be defined over $\overline{\mathbb{Q}}$, or in fact a number field.

Lemma 19.11: Let $A \in (\mathrm{Ab}/k)$ where $k = \overline{k}$ is such that $(\ell, \operatorname{char} k) = 1$. Then

$$A[\ell^\infty](k) := \bigcup_n A[\ell^n](k) \subset A$$

is Zariski dense.

Proof. Let $Z := A[\ell^\infty](k) \subseteq A$. Let $\overline{Z}^\circ \subseteq Z$, the reduced closed subscheme of A, is stable undergroup operations, and $\overline{Z}^\circ$ is a abelian subvariety of A over k.

Now $\overline{Z}^\circ[\ell^m] \subset A[\ell^m]$ because $\overline{Z}^\circ \subset A$ and by construction $A[\ell^m] \subseteq \overline{Z}^\circ[\ell^m]$ using $A[\ell^m] \subset Z[\ell^m]$.

Then $\dim \overline{Z}^\circ = \dim A$ so $\overline{Z}^\circ = A$. (We have $(\mathbb{Z}/\ell^m\mathbb{Z})^{2 \dim \overline{Z}^\circ}$.) □

Proposition 19.12: The basechange functor $A \mapsto A \times_{\mathbb{Q}} \mathbb{C}$ restricts to a functor on simple CM abelian varieties over $\overline{\mathbb{Q}}$.

$$\begin{array}{ccc} (\mathrm{Ab}/\mathbb{Q}) & \longrightarrow & (\mathrm{Ab}/\mathbb{C}) \\ \uparrow & & \uparrow \\ \left(\text{CM simple AV}/\overline{Q}\right) & \xrightarrow{\cong} & (\text{CM simple AV}/\mathbb{C}) \end{array}$$

The top functor is fully faithful and the restricted functor is an equivalence of categories.

The content is in essential surjectivity: Every CM abelian variety over $\mathbb{C}$ is isomorphic to something defined over $\overline{Q}$.

Proof. By the lemma on Zariski density of torsion, we get the functor is fully faithful. ($+A/\overline{Q}$, we have $A[\ell^m](\overline{Q}) = A[\ell^m](\mathbb{C})$.)

I'll give a reference for essential surjectivity. □

§5 Good reduction

Let $\mathcal{O}_K$ be a complete DVR, for instance, a finite extension of $\overline{Q}_p$. Let $\mathfrak{m} \subset \mathcal{O}_K$ be the maximal idea.

Definition 19.13: A has **good reduction** modulo $\mathfrak{m}$ if there exists an abelian scheme $\mathscr{A}/\mathcal{O}_K$ such that

$$\mathscr{A} \times_{\mathcal{O}_K} K \cong A.$$

If so, then the special fiber is $\mathscr{A} \times_{\mathcal{O}_K} \mathcal{O}_K/\mathfrak{m}$.

Remark: If so, then $\mathscr{A}$ is the Neron model of A over $\mathcal{O}_K$ and is unique up to canonical isomorphism.

smooth proper group scheme over K. Remove smooth or proper. In general, bad reduction, Neron model is smooth group scheme, not necessarily proper, which approximates.

Next time we'll talk about the Neron-Ogg-Shafarevich criterion: for $(\ell, \operatorname{char} k) = 1$, then A has good reduction iff $I_K \subset G(\overline{K}/K)$ acts trivially on $T_\ell A$. A has CM implies A has potential good reduction, i.e., there exists K'/K finite such that $A \times_K K'$ has good reduction.

Later we'll classify av up to isog over finite fields. At some point we'll have to construct our abelian varieties. Starting from CM field, integer ring, write down Riemann pairing, lattice, given lots interesting abelian var.

Can be Riemann form on pairs so actual ab var. If want over finite fields, start from CM field, bc good reduction, take special fiber. Cm can always def over number field, reduction, over finite field. Construct lots ab var def over finite field, get all possible av over finite field.

Two things impt: define over number field, potential good reduction so can always get over ff. Tate's thm next time.

Lecture 20
Tue. 11/20/12

Last time we talked about CM abelian varieties, first over $\mathbb{C}$ and then over $\overline{\mathbb{Q}}$. We explicitly constructed CM abelian types using *CM-types*, that is, pairs (F, Φ) where

- F is a CM-field, and
- $\Phi \subseteq \operatorname{Hom}(F, \mathbb{C})$ is a subset such that $\Phi \sqcup c\Phi = \operatorname{Hom}(F, \mathbb{C})$

We found that CM-types are in 1-to-1 correspondence with CM abelian varieties over $\mathbb{C}$ up to isogeny. Then we defined the following correspondences:

$$\left\{\begin{matrix}\text{CM-pairs} \\ (F, \Phi)\end{matrix}\right\} \overset{1-1}{\longleftrightarrow} (\text{CM abelian variety}/\mathbb{C})\,/\text{isogeny} \overset{1-1}{\longleftrightarrow} \left(\text{CM abelian variety}/\overline{\mathbb{Q}}\right)/\text{isogeny}.$$

To go from a CM abelian variety to a CM-pair, we look at the action of the field on the tangent space of A. To go from a CM abelian variety over $\overline{\mathbb{Q}}$ to $\mathbb{C}$, we just base change from $\overline{\mathbb{Q}}$ to $\mathbb{C}$; we proved that we can go from $\mathbb{C}$ to $\overline{\mathbb{Q}}$ as well. Once A is defined over $\overline{Q}$ it is defined over a number field because of finiteness. A natural inclination is to study the reduction of A modulo primes in the number field.

A starting point for studying abelian varieties over a finite field k is Tate's Theorem 20.2, which tells us that to understand homomorphisms between two abelian varieties, it suffices to look at homomorphisms on their ℓ-power torsion points. Tate's theorem is fundamental to helping us understand abelian varieties over finite fields.

§1 Tate's Theorem

We will prove Tate's Theorem in this lecture and the next.

First, we remind the reader of some preliminaries. Recall that the ℓ-adic Tate module is defined by $T_\ell A := \varprojlim A[\ell^n](\overline{k})$ and the rational Tate module is $V_\ell A := T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. If A has dimension g, then $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank $2g$ and $V_\ell A$ is a $\mathbb{Q}_\ell$-vector space of dimension $2g$ (Theorem 9.9).

Let $\Gamma = \Gamma_k := G(\overline{k}/k)$.

We've seen that the following map is injective:

$$\mathcal{T}_\ell : \mathrm{Hom}_{(\mathrm{Ab}/k)}(A, B) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell\text{-module}}(T_\ell A, T_\ell B).$$

The natural Galois action of Γ_k on $T_\ell A$ is compatible with multiplication-by-ℓ map because the multiplication-by-ℓ map is defined over k.

Because the maps in $\mathrm{Hom}_{(\mathrm{Ab}/k)}(A, B)$ are defined over k, they commute with the Galois action of the Tate module. Thus the map $\mathcal{T}_\ell$ above actually lands in $\mathrm{Hom}_{\mathbb{Z}_\ell\Gamma\text{-module}}(T_\ell A, T_\ell B)$. Optimistically we predict that this inclusion is an isomorphism.

$$\begin{array}{ccc} \mathrm{Hom}_{(\mathrm{Ab}/k)}(A, B) & \xhookrightarrow{\mathcal{T}_\ell} & \mathrm{Hom}_{\mathbb{Z}_\ell\text{-module}}(T_\ell A, T_\ell B) \\ & \searrow^{\mathcal{T}_\ell} & \uparrow \\ & & \mathrm{Hom}_{\mathbb{Z}_\ell\Gamma\text{-module}}(T_\ell A, T_\ell B) \end{array}$$

Because $\bullet \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is exact, we can tensor with $\mathbb{Q}_\ell$ to get the injection

$$\mathcal{V}_\ell : \mathrm{Hom}_{(\mathrm{Ab}/k)}(A, B) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{Hom}_{\mathbb{Q}_\ell\Gamma\text{-module}}(V_\ell A, V_\ell B).$$

Conjecture 20.1 (Tate)**:** If k is finitely generated over $\mathbb{F}_p$ or $\mathbb{Q}$, then

$$\mathcal{T}_\ell : \mathrm{Hom}_{(\mathrm{Ab}/k)}(A, B) \to \mathrm{Hom}_{\mathbb{Z}_\ell\Gamma\text{-module}}(A, B)$$

is an isomorphism.

In other words, the image is as large as it can by while still commuting with with the Galois action.

This conjecture is known to be true in two important cases.

Theorem 20.2: thm:tateLet k is a field and ℓ be a prime with $\mathrm{char}(k) \neq \ell$. Let $A, B \in (\mathrm{Ab}/k)$.

In either of the following cases $\mathcal{T}_\ell$ is an isomorphism:

1. (Tate's Theorem, Inventiones, 1966, [6]) k is finite.
2. (Faltings, 1983) k is a number field.

Tate's Theorem is a relatively short and beautiful argument. Faltings's result is more difficult.

Remark: Note that by contrast, when $k = \overline{k}$.

$$\mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell\Gamma}(V_\ell A, V_\ell B)$$

is never an isomorphism. The LHS is $\bigcup_{k'/k \text{ finite}} \mathrm{Hom}_{\mathbb{Z}_\ell\Gamma_{k'}}(V_\ell A, V_\ell B)$, so the homomorphism have to be invariant under some small open Galois subgroup near the identity, while the $\mathbb{Z}_\ell\Gamma$-condition on the right is trivial.

§2 Reduction Steps

These reduction steps work for any field. Later, we'll use specific results which are true for finite fields.

First we would like to consider V_ℓ instead of T_ℓ because V_ℓ is a vector space (Step 1); next we would like to only have to work with one prime ℓ because then we can choose ℓ with nice splitting properties (Step 2); third, we would like to only have to consider $A = B$ so we can consider End rather than Hom (Step 3); finally we rephrase in terms of centralizers using some noncommutative algebra (Step 4). Note that Step n here is Lemma n in [6, §1].

Step 1: We show that $\mathcal{T}_\ell$ is bijective iff $\mathcal{V}_\ell$ is bijective.

Hence it suffices to prove that $\mathcal{V}_\ell$ is a bijection.

The forward direction is obvious.

For the reverse direction, it suffices to show $\operatorname{coker} \mathcal{T}_\ell$ is torsion-free. Then it will follow $\operatorname{coker} \mathcal{T}_\ell = 0$ iff

$$\operatorname{coker} \mathcal{V}_\ell \otimes \mathbb{Q}_\ell = 0,$$

i.e., $\mathcal{T}_\ell$ is bijective iff $\mathcal{V}_\ell$ is bijective.

Suppose $f : T_\ell A \to T_\ell B$ is a $\mathbb{Z}_\ell\Gamma$-module homomorphism, and $\ell^n f = \mathcal{T}_\ell(\phi) \in \mathrm{im}\mathcal{T}_\ell$ for some n and some $\phi : A \to B$. Then $\mathcal{T}_\ell(\phi) \bmod \ell^n = 0$, so $\phi|_{A[\ell^n](\overline{k})} = 0$; thus $\phi|_{A[\ell^n]} = 0$.

This means that $\phi = \ell^n\phi'$ for some $\phi' \in \mathrm{Hom}(A, B)$. Then $\ell^n\mathcal{T}_\ell(\phi') = \ell^n f$, giving $f = \mathcal{T}_\ell(\phi') \in \mathrm{im}\mathcal{T}_\ell$.

Step 2: To show that $\mathcal{V}_\ell$ is a bijection for all $\ell \neq \operatorname{char} k$, it suffices to prove

(A) $\mathcal{V}_\ell$ is a bijection for one ℓ, and

(B) $\dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell\Gamma}(V_\ell A, V_\ell B)$ is independent of ℓ.

Proof. Let ℓ be as in (A), and $\ell' \neq \operatorname{char} k$ be another prime. We have that

$$\dim_{\mathbb{Q}_\ell} \mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell \overset{(A)}{=} \dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell\Gamma}(V_\ell A, V_\ell B) \overset{(B)}{=} \dim_{\mathbb{Q}_{\ell'}} \mathrm{Hom}_{\mathbb{Q}_{\ell'}}(V_{\ell'} A, V_{\ell'} B).$$

Because the dimensions are equal and $\mathrm{Hom}(A, B)\otimes\mathbb{Q}_\ell \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell\Gamma}(V_{\ell'} A, V_{\ell'} B)$ is an injection, it is a bijection. □

Later we'll choose a favorite prime ℓ which has a nice property.

Step 3: We claim that to show $\mathcal{V}_\ell$ is a bijection, we can just take A and B to be equal, i.e., it suffices to show that

(A'_ℓ) for all $A \in (\mathrm{Ab}/k)$,

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \xrightarrow{\mathcal{V}_\ell} \mathrm{End}_{\mathbb{Q}_\ell\Gamma}(V_\ell A)$$

is a bijection.

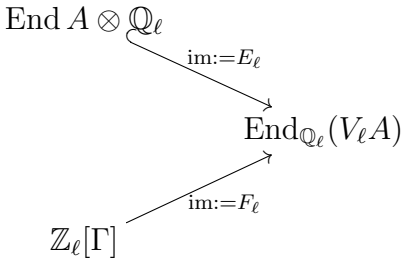
The clear advantage to working with End is that we have an algebra structure rather than just a module structure.

Proof. Plug in $A \times_k B$ in place of A in (A'_ℓ). We have the decomposition

$$\begin{array}{ccccccccc}
\mathrm{End}(A\times B)_{\mathbb{Q}_\ell} & = & \mathrm{End}(A)_{\mathbb{Q}_\ell} & \times & \mathrm{End}(B)_{\mathbb{Q}_\ell} & \times & \mathrm{Hom}(A,B)_{\mathbb{Q}_\ell} & \times & \mathrm{Hom}(B,A)_{\mathbb{Q}_\ell} \\
\downarrow{\scriptstyle \alpha\otimes\beta\otimes\alpha'\otimes\beta'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \beta'} \\
\mathrm{End}_{\mathbb{Q}_\ell\Gamma}(V_\ell A \times V_\ell B) & = & \mathrm{End}_{\mathbb{Q}_\ell\Gamma}(V_\ell A) & \times & \mathrm{End}_{\mathbb{Q}_\ell\Gamma}(V_\ell B) & \times & \mathrm{Hom}_{\mathbb{Q}_\ell\Gamma}(V_\ell A, V_\ell B) & \times & \mathrm{Hom}_{\mathbb{Q}_\ell\Gamma}(V_\ell B, V_\ell A)
\end{array}$$

Because (A'_ℓ) is a bijection, we get $\alpha\otimes\beta\otimes\alpha'\otimes\beta'$ is a bijection, hence α', β' are bijections. □

Now we have maps $\mathcal{V}_\ell : \mathrm{End}(A)\otimes\mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell Q)$ and $\mathbb{Z}_\ell[\Gamma] \to \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)$. Let their images be E_ℓ and F_ℓ.



Note that an equivalent way to write $E_\ell = \mathrm{End}_{\mathbb{Q}_\ell\Gamma}(V_\ell A)$ (what we want to prove) is that E_ℓ is the centralizer of F_ℓ:

$$E_\ell = Z_{\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)}(F_\ell).$$

Step 4: Showing (A'_ℓ) is equivalent to the following two statements.

$(A''_\ell - 1)$ F_ℓ is a semisimple $\mathbb{Q}_\ell$-algebra.

$(A''_\ell - 2)$ $F_\ell = Z_{\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)}(E_\ell)$ (the centralizer/commutant of E_ℓ).

Proof. We have

- by Poincaré reducibility, E_ℓ is a semisimple $\mathbb{Q}_\ell$-algebra.

- The Double Centralizer (bicommutant) Theorem says that if $A, B \subseteq E = \mathrm{End}_K(V)$ with A K-semisimple, then $C(A)$ is semisimple and

$$A = Z_E(B) \iff B = Z_E(A).$$

Apply the Double Centralizer Theorem to $E_\ell, F_\ell \subseteq \mathcal{E}_\ell$ where $\mathcal{E}_\ell = \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)$. Because we know E_ℓ is semisimple, we get

$$E_\ell = Z_{\mathcal{E}_\ell}(F_\ell) \iff F_\ell = Z_{\mathcal{E}_\ell}(E_\ell) \text{ and } F_\ell \text{ semisimple.}$$

□

§3 Proof of (A)

We will show the following.

(a1) Start from the finiteness hypothesis $\mathrm{Hyp}(k, A, d, \ell)$. Here $d \in \mathbb{N}$. The hypothesis says

$\mathrm{Hyp}(k, A, d, \ell)$: We have that the set of isomorphism classes of abelian varieties satisfying several hypotheses is finite: the set

$$\left\{ \begin{array}{c} B \in (\mathrm{Ab}/k) \text{ such that} \\ \exists \text{ polarization } \lambda : B \to B^\vee \text{ of degree } d^2 \\ \exists B \to A \, k\text{-isogeny of } \ell\text{-power degree} \end{array} \right\} / \cong$$

is finite.

There are 2 proofs. We give the proof with moduli spaces because it is quick (though it requires more machinery).

Proof. There exists a quasi-projective scheme of finite type $\mathscr{A} / \operatorname{Spec} \mathbb{Z}$ that parametrizes abelian varieties and polarizations of degree d^2 with level structure, up to isomorphism. Because $\mathscr{A}$ is of finite type, the number of points over a finite field is finite: $|\mathscr{A}(k)| < \infty$. □

Note that this method doesn't apply over other fields; there are infinitely many points.

(a2) Fix a polarization $\lambda : A \to A^\vee$ over k. Note $\lambda_{\overline{k}} = \lambda_L$ for some line bundle L on $A_{\overline{k}}$. Let $W \subseteq V_\ell A$ be the maximal isotropic subspace (i.e. the largest subspace W such that the symplectic pairing E^λ is trivial on $W \times W$). Note that beecause E^λ is symplectic, $\dim_{\mathbb{Q}_\ell} W = g$.

Then there exists a projection $u \in E_\ell$ such that $u(V_\ell A) = W$.

(a3) If $F_\ell \cong \mathbb{Q}_\ell \times \cdots \times \mathbb{Q}_\ell$ then $(A''_\ell - 2)$ is true (and $(A''_\ell - 1)$ holds).

(a4) $F := \mathbb{Q}(\mathrm{Frob}_q) \subseteq \mathrm{End}^0(A)$ is a semisimple $\mathbb{Q}$-algebra, and $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong F_\ell$.

The plan is to show (a1) $\Longrightarrow$ (a2) $\Longrightarrow$ (a3) and (a3)+(a4) $\Longrightarrow$ (A).

Note that to satisfy the condition of (a3), we can just take ℓ splitting completely in F. By the Chebotarev density theorem, there are infinitely many such primes. We have to justify (a1) $\Longrightarrow$ (a2), (a2) $\Longrightarrow$ (a3), and (a4). We'll prove (a1) $\Longrightarrow$ (a2) today.

3.1 Proof of (a1) $\Longrightarrow$ (a2)

We follow page 137 of [6].

Step 1: We introduce lattices X_n in $T_\ell A$ defined by

$$X_n := (T_\ell A \cap W) + \ell^n T_\ell A.$$

Note X_n is a lattice as

$$\ell^n T_\ell A \subset \underbrace{(T_\ell A \cap W) + \ell^n T_\ell A}_{=X_n} \subset T_\ell A;$$

moreover both inclusions are with index ℓ^{ng}. To see this, let $\{v_i\}$ be a basis of W and extend it to a basis $\{v_i\} \cup \{w_j\}$ of $T_\ell A$. Then explicit bases are given by $\ell^n T_\ell A = \{\ell^n v_i\} \cup \{\ell^n w_j\}$ and $X_n = \{\ell^n v_i\} \cup \{w_j\}$.

We can construct $B_n \in (\mathrm{Ab}/k)$ and a k-isogeny $f_n : B_n \to A$ with image X_n, i.e.,

$$f_n(T_\ell B_n) = X_n \subset T_\ell A.$$

The construction is not too difficult; we omit it.

Step 2: We will show that

$$\lambda_n := \ell^{-n} f_n^\vee \lambda f_n = \ell^{-n} f_n^* \lambda$$

is a polarization of B_n over k. The map $f_n^*\lambda$ is defined over k because f_n and λ are defined over k. But multiplying by ℓ^{-n} might be a problem. (We need to multiply by ℓ^{-n} to make the degree equal d^2.)

To show that multiplication by ℓ^{-n} is valid, we show that $E^{f_n^*\lambda}(x, y) = E^\lambda(f_n x, f_n y)$ has values in $\ell^n \mathbb{Z}_\ell(1)$. Then $f_n^*\lambda = \ell^n \lambda'$ for some polarization λ'.

We'd like to show an element $u \in E_\ell = \mathrm{End}_\ell A \otimes \mathbb{Q}_\ell$ as an ℓ-adic limit of elements in $\mathrm{End}\, A$.

Step 3: Construct a sequence $\{u_j\}$ in $\mathrm{End}^0(A)$. By hypothesis of (a1), there are finitely many isomorphism classes of B_i's. By the Pigeonhole Principle, there exists an infinite subsequence $i_1 < i_2 < \cdots$ such that the B_{i_j} are all isomorphic over k. *This is where we use finiteness (a1) in an essential way.*

For all j, fix an isomorphism $B_{i_1} \xrightarrow{\cong} B_{i_j}$ over k. Define

$$u_j := f_{i_j} \circ v_j \circ f_{i_1}^{-1} \in \mathrm{End}^0(A),$$

(this is well defined in End^0) i.e., as the map making the following picture commute:

$$\begin{array}{ccc} B_{i_1} & \xrightarrow{\cong} & B_{i_j} \\ {\scriptstyle f_{i_1}}\downarrow & & \downarrow{\scriptstyle f_{i_j}} \\ A & \xrightarrow[u_j \in \mathrm{End}^0 A]{} & A. \end{array}$$

On Tate modules this gives the map

$$\begin{array}{ccc} T_\ell B_{i_1} & \xrightarrow{\cong} & T_\ell B_{i_j} \\ \downarrow & & \downarrow \\ X_{i_1} & \xrightarrow{u_j} & X_{i_j}. \end{array}$$

We have $u_j \in \mathrm{End}^0(A)$ and $u_j(X_{i_1}) = X_{i_j} \subset X_{i_1}$.

Step 4: Take the limit. We have $\{u_j\} \subset \mathrm{End}_{\mathbb{Z}_\ell}(X_{i_1})$. The RHS is compact so the sequence has a convergent subsequence $u_{j_1}, u_{j_2}, \ldots$ with limit $u \in \mathrm{End}(X_{i_1})$. But then $u(X_{i_1}) = \bigcap_{m \geq 1} \underbrace{u_{j_m}(X_{i_1})}_{X_{j_m}}$. We have $X_n = (T_\ell A \cap W) + \ell^n T_\ell A$ so

$$u(X_{i_1}) = \bigcap_{m \geq 1} \underbrace{u_{j_m}(X_{i_1})}_{X_{j_m}} = T_\ell A \cap W.$$

Finally, we get $u(V_\ell A) = W$ because for every $v \in V_\ell A$, by the fact that X_{i_1} is a $\mathbb{Z}_\ell$-lattice, $\ell^N v \in X_{i_1}$ for large enough N. This shows that $u(\ell^N v) \in T_\ell A \cap W$. Hence $u(v) \in W$. By scaling we can generate everything in W in this manner.

Lecture 21
Tue. 11/27/12

We finish the proof of Tate's Theorem and give some applications.

First, recall our conditions. We fix a polarization λ on A; then we have the Weil pairing E^λ, which is skew-symmetric.

(a1) $\mathrm{Hyp}(k, A, d, \ell)$:

$$\left\{ \begin{array}{c} B \in (\mathrm{Ab}/k) \\ \exists \text{ polarization of degree } d^2 \\ \exists \text{ isogeny } B \to A \text{ of degree } \ell\text{-power} \end{array} \right\} / \cong \text{ is finite.}$$

(a2) If $W \subseteq V_\ell A$ is a maximal E^λ-isotropic $\mathbb{Q}_\ell$-subspace, which is Γ-stable. Then there exists $u \in E_\ell$ such that $u(V_\ell A) = W$.

(a3) If $\ell \neq \operatorname{char} k$ and $F_\ell \cong \mathbb{Q}_\ell \times \cdots \times \mathbb{Q}_\ell$, then $(A''_\ell - 2)$.

(a4) $F := \mathbb{Q}(\mathrm{Frob}_q) \subset E = \mathrm{End}^0(A)$ is a semisimple $\mathbb{Q}$-algebra and as $\mathbb{Q}_\ell$-algebras, $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong F_\ell$.

Last time we we in the middle of proving the following.

Theorem (Theorem 20.2)**:** Let $A, B \in (\mathrm{Ab}/k)$, let $k = \mathbb{F}_q$, and let $\Gamma = G(\overline{k}/k)$. Let $\ell \neq p$ be prime, where $p = \operatorname{char} k$. Then the natural map

$$\mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\cong} \mathrm{Hom}_{\mathbb{Z}_\ell\Gamma}(T_\ell A, T_\ell B)$$

is an isomorphism.

Last time we reduced to showing that

(A'_ℓ) For one ℓ,

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \xrightarrow{\cong} \mathrm{End}_{\mathbb{Q}_\ell\Gamma}(V_\ell A).$$

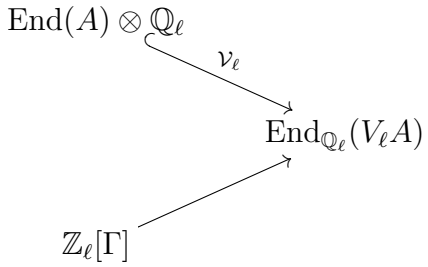
(B) $\dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell\Gamma}(V_\ell A, V_\ell B)$ is independent of ℓ, for $\ell \neq p$.

We further reduced (A'_ℓ) to the following two conditions.

$(A''_\ell - 1)$ F_ℓ is a semisimple $\mathbb{Q}_\ell$-algebra.

$(A''_\ell - 2)$ $F_\ell = Z_{\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)}(E_\ell)$.

Here E_ℓ, F_ℓ are the images in the following diagram.



Recall that our plan is to show (a1) $\Longrightarrow$ (a2) $\Longrightarrow$ (a3) and (a3)+(a4) $\Longrightarrow$ (A). We then choose ℓ splitting completely in F using Chebotarev to get that the conditions of (a3) hold.

We've seen that (a1) holds, and that (a1) $\Longrightarrow$ (a2).

First, we'll review (a1) $\Longrightarrow$ (a2). (a2) is very technical; its use is apparent in the proof of (a3).

§1 Proof of (A)

1.1 Review: Proof of (a1) $\Longrightarrow$ (a2)

We defined an intermediate lattice

$$\ell^n T_\ell A \subset X_n := (T_\ell A \cap W) + \ell^n T_\ell A \subset T_\ell A.$$

We constructed $f_n : B_n \to A$ as an isogeny of ℓ-power degree with $f(T_\ell B_n) = X_n$. We exhibited a polarization $\lambda_n := \ell^{-n} f_n^\vee \lambda f_n$ on B_n of degree d^2 (degree independent of n). Then we applied (a1) to show there are finitely many isomorphism classes of B_n. Thus we can find a subsequence $\{B_{i_j}\}$ all isomorphic over k. Then we obtained maps u_j making the following commute:

$$\begin{array}{ccc} B_{i_1} & \xrightarrow{\cong} & B_{i_j} \\ {\scriptstyle f_{i_1}}\downarrow & & \downarrow{\scriptstyle f_{i_j}} \\ A & \xrightarrow[u_j \in \mathrm{End}^0 A]{} & A. \end{array}$$

We found an infinite subsequence $\{u_{j_k}\}$ converging to $u \in E_\ell$ and we checked $u(V_\ell A) = W$.

1.2 Proof of (a2) $\Longrightarrow$ (a3)

Let $D_\ell := Z_{\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)}(E_\ell)$. We claim that $F_\ell \subseteq D_\ell$. Indeed, by definition F_ℓ is the image of $\mathbb{Q}_\ell\Gamma$, and all endomorphisms in E_ℓ are defined over k and hence commute with the Galois action.

We want to show $D_\ell \subseteq F_\ell$. The key claim is the following.

Claim 21.1: clm:787-21 Let $W \subset V_\ell A$ be an isotropic subspace with respect to E^λ. If W is F_ℓ-stable, then W is D_ℓ-stable.

Let's assume this for now.

We know that V_ℓ is a module over $F_\ell \cong \mathbb{Q}_\ell \times \cdots \times \mathbb{Q}_\ell$. Then we can decompose

$$V_\ell A = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

where the ith $\mathbb{Q}_\ell$ in F_ℓ operates on V_i. The decomposition is obtained from multiplying by idempotents: $V_1 = (1, 0, \ldots, 0)V_\ell A$, and so forth.

For all i, for all nonzero $v \in V_i$, consider $W = \mathbb{Q}_\ell v_i$, the line generated by v. Because the action of each $\mathbb{Q}_\ell$ is just scalar multiplication, W is F_ℓ-stable. because E^λ is skew-symmetric and the line is 1-dimensional, W is isotropic.

Because W is skew-symmetric and isotropic, applying Claim 21.1 gives that W is D_ℓ-stable. Because every vector in V_i is an eigenvector, $D_\ell|_{V_i}$ is a scalar operator. But F_ℓ contains all possible combinations of scalar operators for each V_i, so $D_\ell \subseteq F_\ell$. This shows that (a2) $\Longrightarrow$ (a3).

We now prove the key claim.

Proof of Claim 21.1. We use a decreasing induction on $\dim W$. Recall that if A has dimension g, $V_\ell A$ has dimension $2g$. Because E is skew-symmetric, the maximal isotropic subspace is of dimension g.

1. Base case: Suppose W is maximal isotropic: $\dim W = g = \dim A$. This is where we use (a2). By (a2), there exists $u \in E_\ell$ with $u(V_\ell A) = W$. Then
$$D_\ell(W) = D_\ell[u(V_\ell A)] = u[D_\ell(V_\ell A)] \subseteq u(V_\ell A) = W.$$

2. Let $d \leq g$ be given. We give the induction step from dimension d to dimension $d-1$. Suppose W is F_ℓ-stable and isotropic as in the claim, and $\dim W = d-1$. We create an isotropic subspace which is F_ℓ-stable and has dimension one larger. Consider the orthogonal space
$$W^\perp := \left\{ v \in V_\ell A : E^\lambda(v, w) = 0 \right\}.$$
We can check
   - $W \subseteq W^\perp$: This follows since W is isotropic.
   - $W^\perp$ is F_ℓ-stable: We have a canonical pairing $e_\ell : T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell(1)$. It suffices to show $e_\ell(\gamma x, \gamma, y) = 0$ iff $e_\ell(x, y) = 0$ for all $\gamma \in \Gamma$. But this is clear: because the pairing comes from Cartier duality, $e_\ell(\gamma x, \gamma y) = \gamma e_\ell(x, y)$.

   The idea in the following is that since $W^\perp$ is strictly larger, we can attach one more dimension to W to use the induction hypothesis.

   Since $F_\ell \cong \mathbb{Q}_\ell \times \cdots \times \mathbb{Q}_\ell$, the F_ℓ-module injection $W \hookrightarrow W^\perp$ splits,. As the irreducible $\mathbb{Q}_\ell$-modules are 1-dimensional, we can write
$$W^\perp = W \oplus \left(\bigoplus_{i=1}^{2(g - \dim W)} L_i \right)$$
   where $\dim_{\mathbb{Q}_\ell} L_i = 1$ and L_i is F_ℓ-stable.

Note that $2(g - \dim W) \geq 2$. Consider $W \oplus L_i$, $i = 1, 2$. They are

- F_ℓ-stable (clear), and
- isotropic. Indeed, we have $E^\lambda(W, W) = 0$, and and $L_i \subset W^\perp$ implies $E^\lambda(L_i, W) = 0$. Finally, $E^\lambda(L_i, L_i) = 0$ by skew-symmetry.

By the induction hypothesis, $W \oplus L_i$ are D_ℓ-stable. Hence $W = (W \oplus L_1) \cap (W \oplus L_2)$ is D_ℓ-stable. □

1.3 Proof of (a4)

It remains to prove (a4). The key claim is a comparison between the geometric action Frob_q and arithmetic (Galois) action F_q. Here F_q sends X to X^q; it is a topological generator on Γ. This induces some action on $V_\ell A$ which we'll denote by F_q'.

By definition of the Frobenius maps, we have

$$\begin{array}{ccc} \operatorname{Spec}\overline{\mathbb{F}_q} & \xrightarrow{F_q} & \operatorname{Spec}\overline{\mathbb{F}_q} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ A & \xrightarrow{\mathrm{Frob}_q} & A. \end{array}$$

Now we have an injection

$$\mathcal{V}_\ell : E := \mathrm{End}^0(A) \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A).$$

This shows that $V_\ell(\mathrm{Frob}_q) = F_q' \in F_\ell$. Then $\mathcal{V}_\ell|_F$ factors through F_ℓ:

$$\begin{array}{ccc} E = \mathrm{End}^0 A & \xrightarrow{\mathcal{V}_\ell} & \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A) \\ \uparrow & & \uparrow \\ F = \mathbb{Q}(\mathrm{Frob}_q) & \xrightarrow{\exists!} & F_\ell \end{array}$$

$F \subseteq Z(E)$. (Because Γ centralizes E, so does F_ℓ and hence F.) Hence F is a semisimple $\mathbb{Q}$-algebra.

Next we show that in the diagram above, $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong F_\ell$. Injectivity is clear because $\mathcal{V}_\ell$ is injective. Surjectivity follows from the fact that $F_q^{\mathbb{Z}} \subset \Gamma$ is dense, hence $\mathcal{V}_\ell(F \otimes \mathbb{Q}_\ell) \subseteq F_\ell$ is dense.

A finite-dimensional vector space over $\mathbb{Q}_\ell$ is complete. Thus $\mathcal{V}_\ell(F \otimes \mathbb{Q}_\ell) = F_\ell$. This proves (a4).

Note that also F_ℓ is semisimple (and $(A_\ell'' - 1)$), because it is in the center of $\mathrm{End}_{\mathbb{Q}_\ell}(A)$.

To see (A), note by the Chebotarev density theorem we can take ℓ splitting completely in F. Then $F \otimes_{\mathbb{Q}} \cong \mathbb{Q}_\ell \times \cdots \times \mathbb{Q}_\ell$, so by (a4), $F_\ell \cong \mathbb{Q}_\ell \times \cdots \times \mathbb{Q}_\ell$. By (a3), $(A_\ell'' - 2)$ holds. Hence (A) holds.

We used the fact that k is a finite field in (a4). The other place we used it was in the finiteness hypothesis in (a1).

It remains to justify part (B).

§2 Proof of (B)

We need the following lemma from linear algebra.

Lemma 21.2 (Rational canonical form)**:** thm:rcf Let V be a finite-dimensional k-vector space, where k is any field. Let $\phi \in \mathrm{End}_k(V)$ be semisimple (i.e., diagonalizable over $\overline{k}$). Let

$$P_\phi := \prod_{f \in k[x]} f^{a(f)}.$$

be the characteristic polynomial of ϕ. Then $V \cong \bigoplus_{f \text{ irreducible}} (k[x]/f)^{a(f)}$ as $k[x]$-modules, where x acts on V as ϕ.

Definition 21.3: Let $A, B \in (\mathrm{Ab}/k)$. Let $P_{\mathrm{Frob},A}, P_{\mathrm{Frob},B} \in \mathbb{Q}[X]$ be the characteristic polynomials of Frob_q on $V_\ell A$, $V_\ell B$. For any extension $K/\mathbb{Q}$, write

$$P_{\mathrm{Frob}_q,A} = \prod_{f \in K[X] \text{ irreducible}} f^{a_K(f)}, \qquad P_{\mathrm{Frob}_q,B} = \prod_{f \in K[X] \text{ irreducible}} f^{b_K(f)}.$$

Define

$$r_k(A,B) = \sum_f a_k(f) b_k(f) \deg f \in \mathbb{Z}.$$

By Lemma 21.2 it suffices to prove the following claim.

Claim 21.4: Keep the setup. For $\ell \neq p$, we have

1. $\dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell \Gamma}(V_\ell A, V_\ell B) = r_{\mathbb{Q}_\ell}(A,B)$.
2. $r_{\mathbb{Q}_\ell}(A,B) = r_{\mathbb{Q}}(A,B)$.

Proof. (1) Using the fact that $\mathrm{Frob}_q^{\mathbb{Z}} \subset \Gamma$ is dense, the LHS is $\dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell(\mathrm{Frob}_q)}(V_\ell A, V_\ell B)$. By the lemma, this equals

$$\dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell(\mathrm{Frob}_q)} \left(\bigoplus_f (\mathbb{Q}_\ell[X]/f)^{a_{\mathbb{Q}_\ell}(f)}, \bigoplus_g (\mathbb{Q}_\ell[X]/g)^{b_{\mathbb{Q}_\ell}(g)}. \right)$$

(From (a4), Frob_q is semisimple.) Why need semisimple? The only nontrivial homomorphisms between simple modules are endomorphisms, so this equals

$$\dim \left(\bigoplus_f \mathcal{M}_{a_{\mathbb{Q}_\ell}(f) \times b_{\mathbb{Q}_\ell}(f)} \left(\mathrm{End}_{\mathbb{Q}_\ell\text{-module}} \left(\mathbb{Q}_\ell[X]/f \right) \right) \right)$$

Note that the End has dimension equal to the degree of f. Thus the total dimension is

$$\sum_f a_{\mathbb{Q}_\ell}(f) b_{\mathbb{Q}_\ell}(f) \deg f = r_{\mathbb{Q}_\ell}(A,B).$$

(2) Write $P_{\mathrm{Frob}_q,A} = \prod_{f \in \mathbb{Q}[X] \text{ irreducible}} f^{a_{\mathbb{Q}}(f)}$. Decompose $f = \prod_{f_i \in \mathbb{Q}_\ell[X] \text{ irreducible}} f_i$. Note because f is separable there is no repeated factor. This shows $a_{\mathbb{Q}}(f) = a_{\mathbb{Q}_\ell}(f_i)$, and $\deg(f) = \sum_i \deg(f_i)$. We also have $b_{\mathbb{Q}}(f) = b_{\mathbb{Q}_\ell}(f_i)$. This shows $r_{\mathbb{Q}}(A,B) = r_{\mathbb{Q}_\ell}(A,B)$. □

This completes the proof of Tate's Theorem.

§3 Application

We highlight one application which we'll use in Honda-Tate Theory.

Theorem 21.5 (Tate, §3)**:** Let A be abelian varieties over a finite field k.

(a) We have
$$\operatorname{rank}_{\mathbb{Z}} \operatorname{Hom}(A, B) = r_{\mathbb{Q}}(A, B).$$

(b) Omitted.

(c) The following are equivalent.

(c1) $B \sim A$, i.e., B, A are $\mathbb{F}_q$-isogenous.

(c2) $P_{\mathrm{Frob}_q, A} = P_{\mathrm{Frob}_q, B}$.

(c3) $\zeta(s, A) = \zeta(s, B)$.

(c4) $\#A(\mathbb{F}_{q^r}) = \#B(\mathbb{F}_{q^r})$ for all $r \geq 1$.

Proof. Use the main theorem and the proof of (B).

Note $(c2) \iff (c3) \iff (c4)$ is standard. In fact, these equivalences hold for smooth proper varieties over a finite field, if we require (c2) to be true for all cohomological degrees. (c1) is specific to abelian varieties.

(c1) $\iff$ (c2): (c1) implies $V_\ell A \cong V_\ell B$ as $\mathbb{Q}_\ell\Gamma$-modules. This gives (c2). To go backwards use Tate's Theorem 20.2. If $\varphi_\ell : V_\ell A \to V_\ell B$ is an injection, then there is $\varphi : A \to B$ in $\operatorname{Hom}(A, B) \otimes \mathbb{Q}$ approximating φ_ℓ that is injective. Since it is an injective homomorphism between abelian varieties of the same dimension, it has to be an isogeny. □

Lecture 22
Thu. 11/29/12

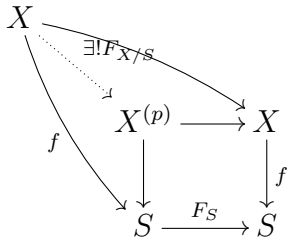
Today we'll talk about finite commutative group schemes over a field. Next time we'll talk about Dieudonné theory, and our final topic will be Honda-Tate theory.

§1 Frobenius and Verschiebung

1.1 Frobenius

The key to studying finite group schemes over a field (or an arbitrary base scheme) is the Frobenius map. Recall that for a $\mathbb{F}_p$-scheme X, we defined the absolute Frobenius map $F_X : X \to X$ by acting on topological spaces as the identity $X^{\mathrm{top}} \xrightarrow{\mathrm{id}} X^{\mathrm{top}}$ and acting on the underlying ring as the pth power map, $a^p \leftarrow\!\shortmid a$.

For an scheme $X \xrightarrow{f} S$ in $(\mathrm{Sch}/\mathbb{F}_p)$, we define the relative Frobenius map $F_{X/S}$ using the fiber diagram



We're interested in group schemes.

1.2 Verschiebung

Let S be a $\mathbb{F}_p$-scheme, and let $G \in (\mathrm{Gp}/S)$. We have a map $F_{G/S} : G \to G^{(p)}$ a morphism of S group schemes. There is a useful map going the opposite direction.

Fact 22.1: Suppose G is commutative. Then there exists a canonical map

$$V_G : G^{(p)} \to G$$

in (Gp/S) called the **Verschiebung** such that

$$F_{G/S} \circ V_G = [p], \qquad V_G \circ F_{G/S} = [p].$$

We only care about the case where k is a field. Suppose $G \in (\mathrm{FCGp}/k)$ where FCGp stands for "finite locally free commutative group scheme." (We could work over a general scheme S, but we won't need this generality.)

It turns out we can express V_G in terms of the Frobenius map.

Proposition 22.2: We have

$$V_G = (F_{G^\vee})^\vee$$

where $^\vee$ denotes Cartier dual.

By this we mean the following. Dualizing the map

$$G^\vee \xrightarrow{F_{G^\vee}} G^{\vee(p)}$$

gives

$$\begin{array}{ccc} G^{\vee\vee} & \xleftarrow{F^\vee_{G^\vee}} & G^{\vee(p)\vee} \\ \| & & \| \\ G & \xleftarrow[V_G]{} & G^{(p)} \end{array}$$

One can check that $G^{(p)}$, F_G, V_G are all functorial in G.

§2 On (FCGp/k).

Let k be any field.

2.1 Approach using fppf sheaves

Definition 22.3: A **fppf scheme** is a map

$$(\mathrm{Sch}/k) \xrightarrow{\mathcal{F}} (\mathrm{Grp})$$

satisfying the fppf sheaf axioms (finitely presented, faithfully flat).

We can embed the category of schemes into the category of fppf sheaves:

$$(\mathrm{FCGp}/k) \hookrightarrow (\mathrm{fppf}/k)\,.$$

This is a fully faithful functor (over abstract groups).

The different notions of quotients in these categories are the same: an exact sequence in (FCGp/k) is an exact sequence as fppf sheaves. If we have $H \hookrightarrow G$, we can define G/H as a geometric quotient. Or we can look at them as fppf sheaves, take the presheaf quotient, sheafify, and then see it's represented by an object in (FCGp/k). We hence have two ways to view the quotient.

2.2 Decomposition into ℓ-primary parts

Let $G \in (\mathrm{FCGp}/k)$. Then there is a (finite) product decomposition

$$\prod_{\ell \text{ prime}} \underbrace{G[\ell^\infty]}_{\varinjlim G[\ell^n]}\,.$$

The proof uses the fact that if $r = |G|$, then $[r] = 0$ on G. (The analogue for groups is that raising an element to the order of a group gives the identity element. However the proof for schemes is nontrivial.)

Thus it's enough to study the ℓ-primary part for each ℓ.

2.3 ℓ-groups

Fact 22.4: Suppose $\ell \neq \operatorname{char} k$. Let $G \in (\mathrm{FCGp}/k)$. Let $r = \operatorname{rank} G$. If $r^{-1} \in k$ (i.e., $\ell \nmid r$), the G is étale over $\operatorname{Spec} k$.

There are several definitions of "étale." One of them is "smooth of relative dimension 0."

It suffices to check G is étale after base change.

2.4 $(\textbf{Étale FCGp}/k)$

Let $G = \operatorname{Spec} R \to \operatorname{Spec} k$.

Write $R = \prod_{i=1}^{r} R_i$, where R_i are finite local k-algebras. Then G is étale iff R_i are finite separable extensions of k_i for each i.

Proposition 22.5: There is an equivalence

$$\left(\text{ÉtFCGp}/k\right) \xrightarrow{\cong} \left\{ \begin{matrix} \text{discrete finite} \\ G(k^{\text{sep}}/k)\text{-modules} \end{matrix} \right\}.$$

(Here discrete means that the stabilizer of a point in the Galois group is open.) The map sends

$$\mathcal{F} \mapsto \mathcal{F}(k^{\text{sep}}).$$

In other words, we can understand an étale finite commutative group scheme over k just by understanding its k^{sep} points and the Galois action on them. We generally believe that the guy on the RHS is easier than the guy on the LHS.

But there are still lots of non-étale schemes, and they remain mysterious.

2.5 Conclusion

We can focus on p-groups over k where $\operatorname{char} k = p$. Dieudonné theory classifies these objects.

§3 Types of group schemes

We'll take a step back to give some strategies and overview. First we need some basic definitions.

Definition 22.6: Let k be any field. Let $G \in (\text{FCGp}/k)$.

1. G is **infinitesimal** if G is connected. (This is true iff $G_{\overline{k}}$ is connected, iff $G_{\text{top}} = \{\cdot\}$ (as G has a finite number of points), iff $G_{\overline{k},\,\text{top}} = \{\cdot\}$.)
2. G is **unipotent** iff $G^\vee$ is infinitesimal.

   G is **multiplicative** (diagonalizable) iff $G^\vee$ is étale.

   G is **bi-infinitesimal** iff G and $G^\vee$ are infinitesimal.

We can restrict to studying these types of schemes, because everything is an extension of an étale by an infinitesimal group scheme; they account for everything if you allow extensions.

Proposition 22.7: Let $\operatorname{char}(k) = p > 0$, and let G be a p-group scheme. If G is étale, then $G^\vee$ is infinitesimal.

Proof. First reduce to $k = \overline{k}$ by using the fact that étale group schemes are preserved by basechange.

Now $\Gamma := G(k)$ is finite abstract p-group. We have $G^\vee = \operatorname{Spec} k[\Gamma]$. Let

$$\mathfrak{m} = \left\{ \sum_{\gamma \in \Gamma} a_\gamma \gamma : \sum_{\gamma \in \Gamma} a_\gamma = 0 \right\}.$$

We can check

- $\mathfrak{m}$ is nilpotent: For large N we have
$$\left(\sum a_\gamma \gamma\right)^{p^N} = \left(\sum a_\gamma\right)^{p^N} \cdot 1 = 0.$$
- $\mathfrak{m}$ is maximal: We see that $k[\Gamma]/\mathfrak{m} = k$ from the exact sequence
$$0 \to \mathfrak{m} \to k[\Gamma] \xrightarrow{\text{Tr}} k \to 0$$
where the trace sends $\sum a_\gamma \gamma \mapsto \sum a_\gamma$.

Every prime ideal contain nilpotents, so it contains $\mathfrak{m}$ and nothing else. Thus $G^\vee_{\text{top}} = \{\cdot\}$. □

Lemma 22.8: If G is étale and infinitesimal, then G is trivial.

Proof. Write $G = \operatorname{Spec}\left(\prod_{i=1}^r R_i\right)$. Because G is infinitesimal, $r = 1$. Because G is étale, R_1 is finite separable over k. Because there exists an identity section, $R_1 = k$. □

Say that G is a finite commutative p-group. We have the following summary.[14]

$G \setminus G^\vee$	étale	infinitesimal
étale	$\operatorname{char} k \neq p$	unipotent
infinitesimal	multiplicative	bi-infinitesimal

Mumford calls bi-infinitesimal group schemes "local-local." The definitions coincide when k is perfect.

Example 22.9: We have the following examples.

	$\underline{\mathbb{Z}/p\mathbb{Z}}$
μ_p	α_p

[14]Note that unipotent group schemes contain bi-infinitesimal group schemes, and multiplicative group schemes contain bi-infinitesimal group schemes as well. For ease of classification we will sometimes write "unipotent"/"multiplicative" to exclude bi-infinitesimal schemes; hopefully this is clear from context.

Here

$$\mu_p = \ker([p] : \mathbb{G}_m \to \mathbb{G}_m)$$

and

$$\alpha_p := \ker(F_{\mathbb{G}_a} : \mathbb{G}_a \to \mathbb{G}_a).$$

(Recall addition on $\mathbb{G}_a$ was given by the map $x \mapsto x \otimes 1 + 1 \otimes x$.) We have $\alpha_p = \operatorname{Spec} k[x]/(x^p)$ with the same comultiplication as $\mathbb{G}_a$ (?). Note $\alpha_p^\vee \cong \alpha_p$ which can be seen by the existence of a perfect pairing

$$\alpha_p \times \alpha_p \to \mu_p$$

given by

$$(x, y) \mapsto \exp(xy) = 1 + xy + \cdots + \frac{(xy)^{p-1}}{(p-1)!}.$$

Fact 22.10: When $k = \overline{k}$, $\underline{\mathbb{Z}/p\mathbb{Z}}$, μ_p, and α_p are the only groups of order p in (FCGp$/k$).

All other p-groups are extensions of them, we can find a filtration such that each quotient is one of these groups:

$$G = G_0 \supset \cdots \supset G_r = \{0\}.$$

Example 22.11: look into this example more. For instance, consider elliptic curves over $\overline{\mathbb{F}_p}$. Ordinary curves are extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p. Supersingular curves are extensions of α_p by another α_p.

Proposition 22.12: pr:787-FV The following hold.

1. G is étale iff $F_{G/k}$ is an isomorphism.

   G is infinitesimal iff $F_{G/k}$ is nilpotent.

2. G is multiplicative iff V_G is an isomorphism.

   G is unipotent iff V_G is nilpotent.

   G is bi-invariant iff both $F_{G/k}$ and V_G are nilpotent.

Proof. Going from (1) to (2), just use the fact that the dual of Frobenius is Verschiebung.

Think of $F_{G/k}$ as a twist. We have that $F_{G/k}$ is nilpotent iff for some $r > 0$, the following composition is 0:

$$G \xrightarrow{F_{G/k}} G^{(p)} \xrightarrow{F_{G^{(p)}/k}} \cdots \longrightarrow G^{(p^r)}, \qquad F^{(r)}_{G/k} : G \to G^{(p^r)}.$$

Consider G over $\operatorname{Spec} k$:

$$\begin{array}{c} G = \operatorname{Spec} R \\ \downarrow \uparrow e \\ \operatorname{Spec} k. \end{array}$$

We can write where $R = k \oplus J$ where J is the augmentation ideal. Then we have the commutative diagram

$$\begin{array}{ccccc} \operatorname{Spec} R = G & \longrightarrow & G^{(p^r)} & = & \operatorname{Spec}(R \otimes_k k) \\ \uparrow & & \uparrow & & \\ \ker F^{(r)}_{G/k} & \longrightarrow & \operatorname{Spec} k & = & \operatorname{Spec} R/J \otimes_k k. \end{array}$$

??? Here the inclusion $k \to R \otimes_k k$ is given by $F : k \to k$. Here $\ker F^{(r)}_{G/k} = \operatorname{Spec} R/J_r$, where J_r is the ideal generated by $F^r(J)$. $F : R \to R$, $x \mapsto x^p$. We have $J_r \subseteq J^{p^r}$ because $F^r(J) \subseteq J^{p^r}$.

On the other hand, we have an inclusion in the other direction: J has p^N generators, for $N \gg 0$, and then $J^{p^{r+N}} \subseteq J_r$ by purely algebra considerations (Pigeonhole Principle).

Once we have this, we can conclude that F_G is nilpotent iff $J_r = 0$ for $r \gg 0$. This is true iff $J^{p^s} = 0$ for $s \gg 0$, iff G is infinitesimal. (J is maximal and nilpotent, so G can only be infinitesimal.) □

§4 Connected-étale sequence

This is very important.

For simplicity, we assume $\operatorname{char} k = p$ and let $G \in (p\text{-FCGp}/k)$.

Proposition 22.13: There exists a canonical exact sequence

$$0 \to G^0 \to G \to G_{\text{ét}} := G/G^0 \to 0$$

where G^0 is the connected component of the identity element e, G^0 is infinitesimal, and $G_{\text{ét}}$ is étale.

Note G^0 is infinitesimal because the connected component is just a point.

Proof. We may assume $k = \overline{k}$ because if the scheme is connected it is still connected over $\overline{k}$. Because the inclusion $G^\circ \hookrightarrow G$ is open and closed, the inclusion

$$\operatorname{Spec} k \cong G^\circ/G^\circ \hookrightarrow G/G^\circ$$

is open. This says $\mathscr{O}_{G_{\text{ét}},e} \cong k$. Why? By group translation, $\mathscr{O}_{G/G_{\text{ét}},p}$ is the same for every point p, and G_{et} is étale. (A scheme is étale if it is étale at every point.) □

4.1 Refining G^0

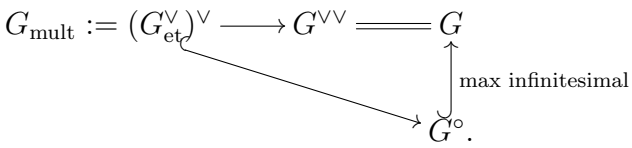
Now we refine G^0. Apply the proposition to $G^\vee$ to obtain

$$0 \to (G^\vee)^0 \to G^\vee \to (G^\vee)_{\text{ét}} \to 0.$$

By Cartier duality, ?

$$G_{\text{mult}} := (G_{\text{ét}}^\vee)^\vee \to G^{\vee\vee} \cong G.$$

Because G_{mult} is multiplicative, i.e., its dual is étale, it must be infinitesimal. The map hence factors through G°, the maximal infinitesimal subgroup scheme of G:



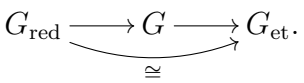
We get an exact sequence

$$0 \to G_{\text{mult}} \to G^0 \to G^0/G_{\text{mult}} \to 0.$$

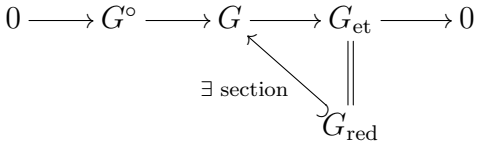
Here $G^0/G_{\text{mult}} =: G_{\text{bi}}$. We can check this is bi-infinitesimal.

4.2 Splittings

Assume k is perfect and $\operatorname{char} k = p$. We get $G_{\text{red}} \subseteq G$ is a subgroup scheme. (The condition that k be perfect is essential. See [7, Exercise 3.2].) We get



We can check that $G_{\text{red}}(\overline{k}) \xrightarrow{\cong} G(\overline{k}) \xrightarrow{\cong} G_{\text{et}}(\overline{k})$. So? We obtain a splitting



Hence $G \cong G^0 \times G_{\text{et}}$ canonically. We can similarly split the sequence for G°. The upshot is that we have the following.

Theorem 22.14: thm:decomp-fcgp Suppose $G \in (\text{FCGp}/k)$ is a p-group, and $\operatorname{char} k = 0$. Then there is a unique decomposition

$$G \cong G_{\text{mult}} \times G_{\text{bi}} \times G_{\text{ét}}$$

where G_{mult} is multiplicative (with étale dual), G_{bi} is bi-infinitesimal, and $G_{\text{ét}}$ is étale.

Lecture 23
Tue. 12/4/12

Let k be a field and let $G \in (\text{FCGp}/k)$ be a p-group. Recall we had four possibilities. We are mainly interested in the characteristic p case; then we have 3 possibilities.

$G \setminus G^\vee$	étale	infinitesimal
étale	$\operatorname{char} k \neq p$	unipotent
infinitesimal	multiplicative	bi-infinitesimal

Recall that G is étale iff $F_G : G \to G^{(p)}$ is an isomorphism, and G is infinitesimal iff $F_G : G \to G^{(p)}$ is nilpotent. For k perfect, we saw that we could decompose

$$G \cong G_{\text{ét}} \times G_{\text{mult}} \times G_{\text{bi}}.$$

The goal of Dieudonné Theory is to classify p-groups and p-divisible groups in terms of linear algebraic data.

§1 Witt vectors

Definition 23.1: Let $n \geq 1$. Let R be a ring and let $\mathbb{W}_n(R) := R^n$ equipped with the ring structure such that the map

$$\phi = (\phi_1, \dots, \phi_n) : \mathbb{W}_n(R) \xrightarrow{R}{}^n$$

given by

$$\phi_i(X_1, \dots, X_n) = X_1^{p^{i-1}} + pX_2^{p^{i-2}} + \cdots + p^{i-1}X_i$$

is a homomorphism.

In other words, we define the ring structure on $\mathbb{W}_n(R)$ as the transport of the ring structure on R^n via ϕ.

We can define Witt vectors of infinite length by taking an inverse limit.

Definition 23.2: Define

$$\mathbb{W}(R) := \varprojlim \mathbb{W}_n(R)$$

where the maps are the obvious projection maps

$$\begin{aligned} \mathbb{W}_{n+1}(R) &\to \mathbb{W}_n(R) \\ (x_1, \dots, x_{n+1}) &\mapsto (x_1, \dots, x_n). \end{aligned}$$

Remark: By taking Spec, $\mathbb{W}_n$ and $\mathbb{W}$ can be though of as ring schemes over $\operatorname{Spec} \mathbb{Z}$.

What's nice about this construction is that it comes with nice operators F, T, and V.

Definition 23.3: Define the **Verschiebung**, **translation**, and **Frobenius maps**

$$\begin{aligned} V &: \mathbb{W}_n \to \mathbb{W}_n \\ T &: \mathbb{W}_n \to \mathbb{W}_{n+1} \\ F &: \mathbb{W}_n \to \mathbb{W}_n \end{aligned}$$

by

$$V(x_1, \ldots, x_n) = (0, x_1, \ldots, x_{n-1})$$
$$T(x_1, \ldots, x_n) = (0, x_1, \ldots, x_n)$$
$$F(x_1, \ldots, x_n) = (x_1^p, \ldots, x_n^p).$$

Taking the inverse limit, F and V operate on $\mathbb{W}$. For an extension $k/\mathbb{F}_p$, define $\mathbb{W}_k := \mathbb{W} \times_{\mathbb{Z}} k$, and extend the action of F and V to $\mathbb{W}_k$.

Note that if W is over k and k has characteristic p, then F is a ring homomorphism and V is an additive homomorphism.

Lemma 23.4: $FV = VF = p$.

Here p is the map $x \mapsto \underbrace{x + \cdots + x}_{p}$.

Proof. Computation. □

We are interested in the case where k is a perfect field of characteristic p. Let

$$W := W_k = \mathbb{W}(k) = \varprojlim \mathbb{W}_n(k)$$

In this case we also denote F by σ; it's an automorphism.

Example 23.5: If $k = \mathbb{F}_p$, then $W = \mathbb{Z}_p$. Ring integers in max unram extension of $\mathbb{Q}_p$. Integer ring of unram ext of $\mathbb{Q}_p$ of degree r.

We've completed the first step in introducing our linear algebraic category.

§2 Dieudonné theory I

Definition 23.6: Fix a perfect field k with characteristic p. Define the **Dieudonné ring** $W[F, V] = W(k)[F, V]$ as the non-commutative ring generated by F, V over W with relations

$$F\lambda = \sigma(\lambda)F, \qquad \lambda V = V\sigma(\lambda), \qquad FV = VF = p$$

for all $\lambda \in W$.

The key definition is the following. This category classifies finite commutative group schemes over k of p-power order.

Definition 23.7: Define the category of **left Dieudonné modules** by

$$\mathrm{Mod}^{\mathrm{fl}}_{W[F,V]} := \left\{ \begin{array}{c} \text{left } W[F,V]\text{-modules} \\ \text{of finite length as } W\text{-modules} \end{array} \right\}$$

Note that any object is killed by a power of p. This is true of a module M of length 1 because in this case pM is a submodule and hence must be 0; now use an induction argument.

Rephrasing the definition, $M \in \mathrm{Mod}^{\mathrm{fl}}_{W[F,V]}$ is a Dieudonné module iff M is a W-module of finite length with maps

- $F : M \to M$ that is σ-linear $F(\lambda m) = \sigma(\lambda)F(m)$,
- $V : M \to M$ that is σ^{-1}-linear,

such that $FV = VF = p$. Equivalently, M has maps

- $F_M : M^{(p)} \to M$ and
- $V_M : M \to M^{(p)}$

where $M^{(p)} := M \otimes_W \to W$ with the map in the tensor product given by $\sigma : W \to W$. Note $M^{(p)}$ is also written M^σ (Grothendieck).

We will see in a moment that these maps correspond to the Frobenius and Verschiebung maps on group schemes. Our main theorem is the following.

Theorem 23.8: Let k be a perfect field of characteristic p.

There exists a canonical anti-equivalence of categories

$$(p\text{-FCGp}/k) \xrightarrow{\mathbb{D}} \mathrm{Mod}^{\mathrm{fl}}_{W[F,V]}$$

with a canonical isomorphism $\mathbb{D}(G^{(p)}) \cong \mathbb{D}(G)^\sigma$, such that the maps

$$G \xrightarrow{F_G} G^{(p)}$$
$$G \leftrightarrow V_G G^{(p)}$$

corresponds under $\mathbb{D}$ to the maps

$$M \xleftarrow{F_M} M^\sigma$$
$$M \xrightarrow{V_M} M^\sigma$$

where $M = \mathbb{D}(G)$. In other words,

$$\mathbb{D}(F_G) = F_{\mathbb{D}(G)}$$
$$\mathbb{D}(V_G) = V_{\mathbb{D}(G)}.$$

One natural thing to check is how the Diedonné functor is affect by base change. We have the following.

Proposition 23.9: Let K/k be perfect. Then

$$\mathbb{D}(G \times_k K) \cong \mathbb{D}(G) \otimes_{W_k} W_K$$

functorially.

This will fall out as a corollary of our main theorem.

Another natural question is how the order of the group is related to the length of the Dieudonné module.

Proposition 23.10: We have

$$\log_p(|G|) = \text{length}_W \mathbb{D}(G)$$

Example 23.11: Let's revisit our three prototypical examples $\underline{\mathbb{Z}/p\mathbb{Z}}, \mu_p, \alpha_p$. We can write down the corresponding Dieudonné modules corresponding to them. The Diedonné module is

$$\mathbb{D}(G) = W/pW = k$$

with structure depending on G: (we'll justify these choices below.)

1. If $G = \underline{\mathbb{Z}/p\mathbb{Z}}$, then $F = \sigma$ and $V = 0$. (F is a bijection.)
2. If $G = \mu_p$, then $F = 0$ and $V = \sigma^{-1}$. (V is a bijection.) σ is really the identity?
3. If $G = \alpha_p$, then $F = V = 0$.

How do we actually match them up? To check, we first reduce to the case where $k = \overline{k}$. Because $\mathbb{D}$ is an equivalence, we try to find simple objects in each category. If a Dieudonné module has length 1, must be one of these three modules; these are the only F and V actions we can define. On the finite commutative group scheme side, $\underline{\mathbb{Z}/p\mathbb{Z}}, \mu_p, \alpha_p$ are exactly all the simple objects, in the sense that cannot be decomposed further as smaller p-group schemes.

By considering simple objects on both sides, there are 6 possibilities for matching them! How should they be matched?

We use Proposition 22.12.

1. Since $\underline{\mathbb{Z}/p\mathbb{Z}}$ is étale, the Frobenius should be bijective, so we must have $F = \sigma$.
2. Since μ_p multiplicative, the Verschiebung should be bijective.
3. Since α_p is bi-infinitesimal, V, F are nilpotent.

This gives a starting point for understanding $\mathbb{D}$. Using this example, we get a relationship between length of Dieudonné modules and the order of the group schemes. To see this, we use the fact that given an arbitrary finite commutative p-group scheme ext of group scheme, we can find a filtration

$$0 = G_0 \subset \cdots \subset G.$$

Each quotient will correspond to one of $\mathbb{Z}/p\mathbb{Z}$, μ_p, and α_p.

§3 Construction of $\mathbb{D}$

Definition 23.12: Consider an inductive system of group schemes

$$\underrightarrow{\mathbb{W}}_k = \varinjlim \mathbb{W}_{n,k}$$

via the translation maps $T : \mathbb{W}_{n,k} \to \mathbb{W}_{n+1,k}$ defined by

$$T(x_1, \ldots, x_n) = (0, x_1, \ldots, x_n).$$

We can define a $W[F,V]$-action on $\underrightarrow{\mathbb{W}}_k$ because F, V commute with T; this gives F, V acting on $\underrightarrow{\mathbb{W}}_k$.

The idea of the construction is as follows. We carry it out in 3 steps.

Recall that for p-groups in characteristic p, group schemes are organized as follows: we have unipotent groups, multiplicative groups, and the intersection consists of the bi-infinitesimal group schemes. Because there is a product decomposition into these 3 parts, it is enough to define the Dieudonné functor $\mathbb{D}$ on unipotent and on multiplicative groups, and then show we can put these definitions of $\mathbb{D}$ together.

1. G is unipotent (i.e., $G^\vee$ is infinitesimal). Then define the functor

$$\mathbb{D}(G) := \mathrm{Hom}_{k\text{-group}}(G, \underrightarrow{\mathbb{W}}_k).$$

Note $\underrightarrow{\mathbb{W}}_k$ carries a $W[F,V]$-action. So this is actually a $W[F,V]$-module; we show it is of finite length. We still have $FV = VF = p$ because it is true at every finite level. Pass from G to G^σ, keep track of what Frobenius does on Dieudonné module. Corresp to Frob on Dieudonné module. (?)

We have the following.

Proposition 23.13: pr:787-23-unip There is an anti-equivalence of categories

$$\left\{\begin{matrix}\text{unipotent} \\ \text{FCGp}/k\end{matrix}\right\} \xrightarrow{\mathbb{D}} \mathrm{Mod}^{\text{fl, } V\text{-nilp}}_{W[F,V]}.$$

such that $\mathbb{D}(G^{(p)}) \cong \mathbb{D}(G)^\sigma$, $\mathbb{D}(F_G) = F_{\mathbb{D}(G)}$, and $V_G = V_{\mathbb{D}(G)}$.

Decomposing into the étale and bi-infinitesimal part, this functor is the same as the product functor

$$\left\{\begin{matrix}\text{étale} \\ \text{FCGp}/k\end{matrix}\right\} \times \left\{\begin{matrix}\text{bi-infinitesimal} \\ \text{FCGp}/k\end{matrix}\right\} \xrightarrow{\mathbb{D}} \mathrm{Mod}^{\text{fl, } F\text{-bij}}_{W[F,V]} \times \mathrm{Mod}^{\text{fl, } F,V\text{-nilp}}_{W[F,V]}.$$

2. We do the same for multiplicative groups.

Proposition 23.14: pr:787-23-mult There is an anti-equivalence of categories

$$\left\{\begin{matrix}\text{multiplicative} \\ \text{FCGp}/k\end{matrix}\right\} \xrightarrow{\mathbb{D}} \mathrm{Mod}^{\text{fl, } V\text{-bij}}_{W[F,V]}.$$

Proof. The idea is to dualize twice and use the equivalence of categories from Proposition 23.13. We have

$$\left\{\begin{matrix}\text{étale}\\ \text{FCGp}/k\end{matrix}\right\} \cong \text{Mod}_{W[F,V]}^{\text{fl, } F\text{-bij}}.$$

First take the Cartier dual. Then take the Pontryagin dual on category of finite abelian group schemes ($\text{Hom}(\bullet, \mathbb{Q}_p/\mathbb{Z}_p)$). □

3. Decompose the linear category. Given an arbitrary Dieudonné module, we claim there is a functorial decomposition into a V-nilpotent and V-bijective part. This is basically a linear algebra problem.

   Lemma 23.15: lem:787-23-decomp

$$\text{Mod}_{W[F,V]}^{\text{fl}} \cong \text{Mod}_{W[F,V]}^{\text{fl, } V\text{-nilp}} \times \text{Mod}_{W[F,V]}^{\text{fl, } V\text{-bij}}$$

Propositions 23.13 and 23.14 and Lemma 23.15 give the main theorem. A good exercise is to think about the Dieudonné modules for $\mathbb{Z}/p^n\mathbb{Z}$ and μ_{p^n}.

This is the Dieudonné theory for finite commutative group schemes.

§4 p-divisible groups

These are also called p-Barsotti-Tate groups. We define p-divisible groups and then explain what Dieudonné theory tells us about p-divisible groups.

Definition 23.16: A **p-divisible group** $\underrightarrow{G}/S$ of height $h \in \mathbb{N}_0$ is an inductive group schemes over S,

$$\underrightarrow{G} = \varinjlim(G_n, i_n)$$

such that $\text{rank}\, G_n = p^{nh}$, the sequence

$$0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{[p^n]} G_{n+1}$$

is exact.

We have

$$\begin{aligned}\underrightarrow{G} : (\text{Sch}/S) &\to (\text{Gp}/S)\\ T &\mapsto \varinjlim G_n(T).\end{aligned}$$

This is represented by a fppf sheaf. The sheaf is p-divisible in that $[p] : \underrightarrow{G} \to \underrightarrow{G}$ is a fppf surjection.

The example to keep in mind (and the primary motivation for defining p-divisible groups) is the following.

Example 23.17: Let $A \in (\mathrm{Ab}/S)$. Then $A[p^\infty] = \varinjlim A[p^n]$ is a p-divisible group.

For instance, $\underline{\mathbb{Q}_p/\mathbb{Z}_p} = \varinjlim \left(\frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p\right)$ and $\mu_{p^\infty} = \varinjlim \mu_{p^n}$ are both p-divisible groups.

Theorem 23.18: Let k be perfect. There exists a canonical equivalence of categories

$$(p\text{-divisible group}/k) \xrightarrow{\mathbb{D}} \left\{ \begin{array}{c} \text{free finite rank} \\ W[F,V]\text{-modules} \end{array} \right\}$$

with a canonical isomorphism $\mathbb{D}(\underrightarrow{G}^{(p)}) \cong \mathbb{D}(\underrightarrow{G})^\sigma$. The equivalence is given by

$$\mathbb{D}(\underrightarrow{G}) := \varprojlim \mathbb{D}(G_n).$$

Lecture 24
Tue. 12/11/12

Today we'll discuss Honda-Tate Theory. which does... We'll start by recalling some facts about Brauer groups.

§1 Brauer groups

Let F be any field. We're particularly interested in the p-adic case.

Definition 24.1: Define the **Brauer group** as the group of similarity classes of central simple algebras over F,

$$\mathrm{Br}(F) = (\mathrm{CSA}/F)/\sim$$

with multiplication given by tensor product. We impose that $A \sim \mathcal{M}_n(A)$ for any algebra A.

The Brauer group is generated by division algebras D.
For F a number field, we have

1. for v non-archimedean,[15]
$$\mathrm{inv}_v : \mathrm{Br}(F_v) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}$$
2. for v real,
$$\mathrm{inv}_v : \mathrm{Br}(F_v) \xrightarrow{\cong} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$
3. for v complex,
$$\mathrm{Br}(F_v) = 0.$$

[15]This is one of the ingredients that goes into saying we have a *class formation* in local class field theory. Note $\mathrm{Br}(F_v) = H^2(\overline{F_v}/F_v)$.

In the number field case we have the exact sequence (See Theorem 27.3.5 and §27.4 in my number theory text.)

$$eq:787-brauer-seq \quad 0 \longrightarrow \mathrm{Br}(F) \longrightarrow \bigoplus_v \mathrm{Br}(F_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{17}$$

$$D \longmapsto \{D \otimes_F F_v\}$$

In other words, given $\left\{\frac{r_v}{s_v} \in \mathbb{Q}/\mathbb{Z}\right\}_v$ that is zero for almost all v and $\sum_v \frac{r_v}{s_v} \equiv 0 \pmod 1$, there exists, up to equivalence, a unique central division algebra D/F such that $\mathrm{inv}_v(D_v) = \frac{r_v}{s_v}$. We have $[D:F]^{\frac{1}{2}} = \mathrm{lcm}_v\, s_v$.

§2 More on p-divisible groups

Let k be perfect of characteristic $p > 0$. Recall that there is an anti-equivalence of categories

$$\mathbb{D} : (\mathrm{BT}/k) := (p\text{-divisible group}/k) \xrightarrow{\cong} \left\{\begin{array}{c} W[F,V]\text{-modules} \\ \text{free of finite rank} \\ \text{as } W\text{-modules}\end{array}\right\}.$$

(We can get a covariant version by dualizing.) In particular, this sends

$$\mu_{p^n} = \lim \mu_{p^n} \mapsto (W, F = p, V = 1)$$
$$\mathbb{Q}_p/\mathbb{Z}_p = \lim \frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p \mapsto (W, F = 1, V = p).$$

These are W-modules rather than vector spaces over the fraction field of W. We introduce a rational version, which is more convenient to work with. Let

$$L := \mathrm{Frac}(W) = W\left[\frac{1}{p}\right].$$

Let (BT^0/k) be the category with the same objects but with

$$\mathrm{Hom}^0(\underrightarrow{G}, \underrightarrow{H}) := \mathrm{Hom}(\underrightarrow{G}, \underrightarrow{H}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Then we get the following anti-equivalence of categories, induced by $\mathbb{D}$:

$$\mathbb{V} : \left(\mathrm{BT}^0/k\right) \xrightarrow{\cong} \left\{\begin{array}{c}\text{finite-dimensional } L\text{-vector space } \mathcal{V} \\ F : \mathcal{V} \xrightarrow{\cong} \mathcal{V} \quad \sigma\text{-linear}\end{array}\right\} =: (\mathrm{Isoc}/k).$$

(The RHS is called **isocrystals** over k, "iso" standing for "isogeny.") By σ-linear we mean $F(\lambda v) = \sigma(\lambda)F(v)$. Note we only need data on F because $V = p \circ F^{-1} = F^{-1} \circ p$. When we rationalize, F and V has to be bijections, because multiplication by p is bijection (it wasn't a bijection on the $W[F,V]$-module).

Hom^0 is useful in classifying abelian varieties up to isogeny. By Poincaré reducibility, abelian varieties decompose into simple varieties. We want to identify and classify the simple objects. The way to do this is look at the linear algebraic category (Isoc/k) and do linear algebra.

If $k = \overline{k}$, there are no interesting extension classes between objects; every object in (Isoc/k) can be decomposed as a finite direct sum of simple objects:

$$\bigoplus_i L[F]/(F^{s_i} - p^{r_i})^{\oplus e_i}$$

where $\frac{r_i}{s_i} \in \mathbb{Q}$ is called the **slope**.[16] On the simple objects, F can act like p to some rational power.

When $k = \overline{k}$, these are all the objects.

Theorem 24.2: $\mathbb{V}$ induces an equivalence of categories

$$(\mathrm{BT}^0/k) \xrightarrow{\cong} (\mathrm{Isoc}\,/k)$$

where the RHS is generated by $\frac{r_i}{s_i} \in \mathbb{Q} \cap [0,1]$.

An application is the following. If we have a decomposition on the RHS, this corresponds to a decomposition on the LHS.

Let $\Sigma \in (\mathrm{BT}/k)$. We have an isogeny

$$\Sigma \to \prod_i (\Sigma_{\frac{r_i}{s_i}})^{e_i}$$

where $\Sigma_{r_i/s_i} = \mathbb{V}^{-1}(L[F]/(F^{s_i} - p^{r_i}))$. We can now compute the endomorphisms of Σ:

$$\begin{aligned}\mathrm{End}^0(\Sigma) &= \prod_i \mathcal{M}_{e_i}(\mathrm{End}^0(\Sigma_{r_i/s_i})) \\ &= \prod_i \mathcal{M}_{e_i}(D_{r_i/s_i}).\end{aligned}$$

Here $D_{\frac{r_i}{s_i}}$ is a central division algebra with $\mathrm{inv}_v D = \frac{r_i}{s_i}$. To see this, we can compute this in linear algebraic category (Isoc/k).

Example 24.3: For instance, if we have an elliptic curve E over $\mathbb{F}_p$, $E[p^\infty]$, ordinary elliptic curves correspond to $\mathbb{Q}_p \times \mathbb{Q}_p$, with slope 0 or 1. By semisimplicity, D is a CDA with inv 1 (?).

§3 Tate's Theorem for $\ell = p$

We give an analogue of Tate's Theorem 20.2 for when $\ell = p$.

[16] In fact it is the slope of a side of the Newton polygon of the characteristic polynomial of F.

Theorem 24.4 (Tate)**:** Let $A \in (\mathrm{Ab}/\mathbb{F}_q)$. Then

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{End}_{W[F,V]}(\mathbb{D}(A[p^\infty]))^{\mathrm{op}}$$

Proof. This follows directly from the equivalence of categories. □

We take the opposite because $\mathbb{D}$ is contravariant.

The theory seems analogous to that for Tate modules. Is there some big theory bringing them together? We expect some grand theory of unification. $\mathbb{D}$ generalizes to the p-adic crystalline cohomology theory and for $\ell \neq p$ we have the étale cohomology theory. Hopefully, there is some motivic cohomology theory that feeds both crystalline and étale cohomology theory depending on whether $\ell = p$.

§4 Honda-Tate Theory

4.1 Weil numbers

Definition 24.5: Let $q = p^a$, $a \in \mathbb{N}$. A **Weil q-integer (q-number)** of weight a is $\alpha \in \overline{\mathbb{Z}}$ (or $\overline{\mathbb{Q}}$) such that

$$\iota(\alpha)\overline{\iota(\alpha)} = q$$

for all $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$.

In the weight 0 case, the Weil q-integers (numbers) are exactly the roots of unity.

Remark: If α is a Weil q-integer, then for all $\gamma \in \Gamma_{\mathbb{Q}} := G(\overline{\mathbb{Q}}/\mathbb{Q})$, $\gamma\alpha$ is also a Weil q-integer.

We can rephrase the Riemann hypothesis succintly using abelian varieties.

Theorem 24.6 (Riemann hypothesis for abelian varieties)**:** The roots of $P_{\mathrm{Frob}_q,A} \in \mathbb{Z}[X]$ are Weil q-integers.

We didn't prove this, but basically the fact that $\mathrm{Frob}_q^{\ddagger_L} \mathrm{Frob}_q = [q]$ (Theorem 18.1) underlies the proof of the theorem.

4.2 Honda-Tate Theory

Write $\pi_A = \mathrm{Frob}_{q,A} \in \mathrm{End}(A)$. Suppose A is $\mathbb{F}_q$-simple. Then $\pi_A \in \mathbb{Q}(\pi_A) \subseteq \mathrm{End}(A)$, $\mathrm{End}(A)$ is a division algebra, and its center $\mathbb{Q}(\pi_A)$ is a field. We can choose an embedding $\mathbb{Q}(\pi_A) \hookrightarrow \overline{\mathbb{Q}}$, well defined up to the Galois action $\Gamma_{\mathbb{Q}}$ of $\overline{\mathbb{Q}}$. This assigns a well-defined element $\pi_A \in \overline{\mathbb{Q}}$ for any abelian variety, which is a Weil q-integer by the theorem.

Summarizing, we have a map

$$\left\{\begin{matrix}\mathbb{F}_q\text{-simple} \\ \text{abelian variety}/\mathbb{F}_q\end{matrix}\right\}/\mathbb{F}_q\text{-isogeny} \to (\text{Weil } q\text{-integer})\,/\Gamma_{\mathbb{Q}}\text{-action}$$

$$A \mapsto \pi_A.$$

Note that $P_{\mathrm{Frob},A}$ is a power of an irreducible polynomial.

Theorem 24.7 (Honda-Tate, 1967)**:** thm:honda-tate The map above is a bijection.

Tate showed this map is injective, and Honda showed it is surjective in his Ph.D. thesis in 1968.

By Honda-Tate, we can define an inverse map $\pi \mapsto A_\pi$.

Theorem 24.8: thm:honda-tate2 We have the following.

1. $E_\pi := \mathrm{End}^0(A_\pi)$ is the unique CDA over $F_\pi := \mathbb{Q}(\pi)$ such that for v a place of F_π,
$$\mathrm{inv}_v(E_\pi) = \begin{cases} 0, & v = \mathbb{C} \\ \frac{1}{2}, & v = \mathbb{R} \\ 0, & v \nmid p,\ v \nmid \infty \\ \frac{v(\pi)}{v(q)}[F_{\pi,v} : \mathbb{Q}_p], & v \mid p,\ v \nmid \infty. \end{cases}$$
2. Moreover,
$$2\dim(A_\pi) = [E_\pi : F_\pi]^{\frac{1}{2}}[F_\pi : \mathbb{Q}].$$

As a sanity check, we can check that the sum of the invariants claimed above is equal to 0 in $\mathbb{Q}/\mathbb{Z}$ (exercise). Note $v = \mathbb{R}$ occurs rarely, so you can argue that case by case. Use $\pi\overline{\pi} = q$, i.e., $v(\pi) + v(\overline{\pi}) = v(q)$.

Note $F_\pi = \mathbb{Q}(\pi)$ has a well-defined complex conjugation. We have $\mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$, and regardless of the embedding, conjugation in $\mathbb{C}$ induces the same automorphism in $\mathbb{Q}(\pi)$. This is simply because complex conjugation sends $\pi \mapsto \frac{q}{\pi}$, and $\frac{q}{\pi}$ is well-defined before embedding.

This implies π is totally real or CM. The totally real case occurs rarely; in fact we can give a complete list of cases where it occurs. We'll sketch one case of this in the following example.

Example 24.9: First note that $F_\pi = \mathbb{Q}(\pi)$ is totally real iff complex conjugation is trivial on $\mathbb{Q}(\pi)$, i.e., $\pi^2 = q$. Let $q = p^a$.

First suppose a is even. Then $F_\pi = \mathbb{Q}$. Then E_π is a CDA over $\mathbb{Q}$ ramified at exactly p, ∞. This is quaternionic, and it corresponds to a supersingular elliptic curve, unique up to isogeny over $\overline{\mathbb{F}_p}$ (in fact, isogeny over a quadratic extension). The dimension is 1 by part 2 of the theorem:
$$2\underbrace{\dim(A_\pi)}_{1} = \underbrace{[E_\pi : F_\pi]}_{4}^{\frac{1}{2}} \underbrace{[F_\pi : \mathbb{Q}]}_{1}.$$

Now suppose a is odd. Then $F_\pi = \mathbb{Q}(\sqrt{p})$, and E_π is a CDA over $\mathbb{Q}(\sqrt{p})$ ramified at two real places. The dimension is 2.
$$2\underbrace{\dim(A_\pi)}_{2} = \underbrace{[E_\pi : F_\pi]}_{4}^{\frac{1}{2}} \underbrace{[F_\pi : \mathbb{Q}]}_{2}.$$

For instance, when $a = 1$, there is no supersingular elliptic curve over $\mathbb{F}_p$, but there is a supersingular elliptic curve E over $\mathbb{F}_{p^2}$. Take the product of E and its Galois twist; it will be defined over $\mathbb{F}_p$ and be an abelian variety of dimension 2. By construction, when we basechange to a quadratic extension it splits into two supersingular elliptic curves.

Now we understand the totally real case, so we understand half of the theory.

Problem 24.1: Let $0 \leq \frac{r}{s} < \frac{1}{2}$. Suppose

$$x^2 - p^r x + p^s = 0$$

has roots $\{\pi, \pi'\}$. Show the following.

- π and π' are Weil q-integers where $q = p^s$.
- The corresponding places v, v' in $\mathbb{Q}(\pi)$ extend v_p.
- $v(\pi) = \frac{r}{s}$, $v(\pi') = v'(\pi) = 1 - \frac{r}{s}$.

In this case $\frac{v(\pi)}{v(p)} =$? We get a division algebra split outside p, and at p, the invariants can be $\frac{r}{s}$ or $1 - \frac{r}{s}$. It's not quaternionic but it can be arbitrarily large. The reason that Tate mentions this example is because this construction gives an answer to a question posed by Yuri Manin: Under what conditions does a p-divisble group arise as the p-divisible group of some abelian variety? We can construct any p-divisible group as the p-divisible group of an abelian variety, given it is symmetric, which roughly means isogenous to its dual.

We sketch a proof of Theorem 24.8.

Proof of Theorem 24.8. The proof for the totally real case comes from basic facts about supersingular elliptic curves and the above example.

We focus on when F_π is a CM field. We know $\mathrm{Br}(\mathbb{C}) = \{0\}$, so there is nothing to prove about invariants at archimedean places. Now suppose $v \nmid \infty$, $v \nmid p$. By Tate's Theorem 20.2 for $\ell \neq p$ we have

$$E_\pi \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \mathrm{End}_{\mathbb{Q}_\ell(\pi)}(V_\ell A_\pi).$$

The RHS is semisimple by Tate's Theorem and hence the product of matrix algebras over finite extensions of $\mathbb{Q}_\ell$. The LHS is

$$\prod_{v|\ell} E_\pi \otimes_F F_{\pi,v}.$$

By matching, we get

$$\mathrm{inv}_v(E_{\pi,v}) = 0.$$

For $v \mid p$ we do something similar except we use Dieudonné Theory and Tate's Theorem for $\ell = p$. □

(The key fact at play here is that by (17), to understand the endomorphism algebra it's sufficient to understand it over every $\mathbb{Q}_\ell$ and $\mathbb{Q}_p$, and Tate's Theorem tells us we can just understand the associated ℓ-adic Tate module or p-divisible group.)

We've converted proving facts about abelian varieties over finite fields to proving facts about rational Dieudonné modules. To do so, we had to go through p-divisible groups as an intermediate step. By looking at the endomorphism algebra of Dieudonné modules associated to p-divisible groups, we compute everything explicitly using linear algebra. There, the Frobenius (given by π) acts on simple objects like p to a rational number. We can compute the endomorphism algebra from that rational number.

The theorem is not easy, but we have the right way think about, it is "elementary" (a linear algebra problem).

Proof of Theorem 24.7. To show injectivity, suppose $\pi_A \sim \pi_B$ are $\Gamma_{\mathbb{Q}}$-conjugate.

We want to show $\mathrm{Hom}(A,B) \neq 0$. It suffices to prove that $\mathrm{Hom}^0(A,B) \neq 0$ (because $\mathrm{Hom}(A,B)$ is torsion-free). Since $\ell \neq p$, it is enough to show $\mathrm{Hom}^0(A,B) \otimes \mathbb{Q}_\ell$ is nonzero. But by Tate's Theorem,

$$\mathrm{Hom}^0(A,B) \otimes \mathbb{Q}_\ell \cong \mathrm{Hom}_{\mathbb{Q}_\ell(\mathrm{Frob})}(V_\ell A, V_\ell B).$$

Given that π_A and π_B are conjugate, can we find $\mathbb{Q}_\ell$-linear map from $V_\ell A$ to $V_\ell B$ intertwining Frob? Here $\pi_A \in V_\ell A$ and $\pi_B \in V_\ell B$ are the embeddings of Frob. We can use linear algebraic information to produce an actual map of algebraic varieties.

For surjectivity, we say that given a CM-pair (L,Φ), we can define a CM abelian variety (A,i) over a number field. We need some control of the data in order to realize the given Weil number. Taking A modulo w, $w \mid p$, we get A defined over a finite field with Frobenius π_A.

But how do we relate π_A and π? We keep track of our data: how L and Φ can be used to describe π_A. The key is to relate (L,Φ) to π_A. Additionally we have to choose L carefully to start with. We compute the reduction of the CM abelian variety in terms of the CM pair explicitly. We can compute the p-adic valuations $v(\pi_A)$ in terms of L,Φ. This is the key point.

These are other relatively minor issues: We have to choose ℓ carefully. We aer not in the $\mathbb{F}_q$ we started with, and have to adjust there. Even if we control the data, cannot arrange π_A to be exactly π.

We skip the proof of part 2. □

Lecture 24
References

[1] Gortz and Wedhorn. *Algebraic Geometry I.*

[2] R. Hartshorne. *Algebraic Geometry.* Springer, 1977.

[3] J. Milne and W. Waterhouse. Abelian varieties over finite fields, 1971.

[4] D. Mumford. *Abelian Varieties*. Tata Institute of Fundamental Research Studies in Mathematics, 1970.

[5] D. Mumford, J. Fogarty, and Kirwan. *Geometric Invariant Theory*. Springer, 2012.

[6] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones math.*, 2:134–144, 1966.

[7] G. van der Greer and B. Moonen. Abelian varieties.