Attribution Key

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

Use + Share + Adapt

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

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

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

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

ZERO **Creative Commons – Zero Waiver**

BY **Creative Commons – Attribution License**

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

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

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

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

Make Your Own Assessment

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

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

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

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

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

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

Lecture 11: Criterion for rank 0

In this lecture, we establish Theorem B from Lecture 1, which is a criterion for an abelian variety to have rank 0. The idea of the proof is similar to that of the weak Mordell–Weil theorem, but here we control the ramification of the cohomology classes much more carefully. Most of the work goes into understanding a certain class of group schemes (the admissible ones) very precisely.

1 Overview

1.1 Statement of criterion

The purpose of today's lecture is to establish the following criterion for an abelian variety to have rank 0 (Theorem B from Lecture 1):

Theorem 1. *Let $A/\mathbf{Q}$ be an abelian variety, and let N and p be distinct prime numbers, with N odd. Suppose the following conditions hold:*

- *A has good reduction away from N.*
- *A has completely toric reduction at N.*
- *The Jordan–Hölder constituents of $A[p](\overline{\mathbf{Q}})$ are 1-dimensional and either trivial or cyclotomic.*

Then $A(\mathbf{Q})$ has rank 0.

Remark 2. The proof uses many special properties of $\mathbf{Q}$, but can be generalized slightly, as follows. Let K be an imaginary quadratic number field, let p be a rational prime, and let $\mathfrak{N}$ be a prime of K. Assume that p does not divide the class number of K and if $p \le 3$ then p is unramified in K. Then the obvious generalization holds: if A/K be an abelian variety with good reduction away from $\mathfrak{N}$, completely toric reduction at $\mathfrak{N}$, and such that the Jordan–Hölder constituents of $A[p](\overline{K})$ are either trivial or cyclotomic then $A(K)$ has rank 0. □

Remark 3. This theorem, and the proof presented here, comes from III.3 of Mazur's paper "Modular curves and the Eisenstein ideal" (MR488287). It is not stated there explicitly, however. □

1.2 Idea of proof

Recall the proof of the weak Mordell–Weil theorem. Kummer theory gives an injection of $A(\mathbf{Q})/nA(\mathbf{Q})$ into $\mathrm{H}^1(G_{\mathbf{Q}}, A[n])$, so it suffices to prove the H^1 is finite. However, it's not, because we have not restricted ramificiation. One can show that there is a finite set of places S such that the image of $A(\mathbf{Q})/nA(\mathbf{Q})$ lands in $\mathrm{H}^1(G_{\mathbf{Q},S}, A[n])$. This H^1 is finite, and this proves the weak Mordell–Weil theorem.

As one shrinks S, the H^1 gets smaller and smaller, so it makes sense for us to take S as small as possible. In general, one can take S to be the set of places of bad reduction together with the divisors of n. So if work with p-power torsion, we can take $S = \{N, p\}$. However, this is still too big for us!

We can improve the situation using the following idea. Let $\mathcal{A}$ be the Néron model of A over $\mathbf{Z}$, and let $G_n = \mathcal{A}[p^n]$. Then $\mathrm{H}^1(G_{\mathbf{Q},S}, A[p^n])$ is the étale cohomology group $\mathrm{H}^1_{\mathrm{et}}(\mathrm{Spec}(\mathbf{Z}[1/Np]), G_n)$

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

— restricting ramification to S corresponds to taking étale cohomology over the ring of integers with the primes in S removed. It is not true that $A(\mathbf{Q})/p^n A(\mathbf{Q})$ injects into $\mathrm{H}^1_{\mathrm{et}}(\mathrm{Spec}(\mathbf{Z}), G_n)$: this group is often zero. However, $A(\mathbf{Q})/p^n A(\mathbf{Q})$ does inject into $\mathrm{H}^1_{\mathrm{fppf}}(\mathrm{Spec}(\mathbf{Z}), G_n)$, and this is the group we will use. (This is a slight lie that we will correct below.)

The idea is to show that this H^1 is bounded independent of n, which will establish that $A(\mathbf{Q})$ has rank 0. To do this, we need to understand the flat cohomology of G_n very well, so we begin by studying groups like G_n and their flat cohomology.

2 Admissible groups

2.1 Definition

Two initial definitions:

- A group scheme G over $\mathbf{Z}[1/N]$ is pre-admissible if it is finite, flat, commutative, and killed by a power of p.
- A group scheme G over $\mathbf{Z}$ is pre-admissible if it is commutative, separated, of finite presentation, quasi-finite, flat, killed by a power of p, and its restriction to $\mathbf{Z}[1/N]$ is finite (and thus pre-admissible).

Example 4. Let A be an abelian variety with good reduction away from N and let $\mathcal{A}$ be its Néron model over $\mathbf{Z}$. Then $\mathcal{A}[p^n]$ is a pre-admissible group scheme over $\mathbf{Z}$. □

Let G be an pre-admissible group over $\mathbf{Z}[1/N]$. An admissible filtration on G is a filtration

$$0 = F^0 G \subset F^1 G \subset \cdots \subset F^n G = G$$

by closed subgroups such that $F^{n+1}G/F^n G$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ or μ_p for each n. We say that G is admissible if it has an admissible filtration. We say that a pre-admissible group over $\mathbf{Z}$ is admissible if its restriction to $\mathbf{Z}[1/N]$ is.

We make a similar definition for Galois representations. Precisely, let V be a $\Gamma_{\mathbf{Q}}$-module. We say that V is admissible if it possess a filtration $F^\bullet V$ by $\Gamma_{\mathbf{Q}}$-submodules such that $F^{n+1}V/F^n V$ is a one-dimensional $\mathbf{F}_p$ vector space on which $\Gamma_{\mathbf{Q}}$ acts either trivially or through the cyclotomic character.

2.2 Detecting admissible filtrations

Proposition 5. *Let G be a pre-admissible group over $\mathbf{Z}[1/N]$. Then G is admissible if and only if $G(\overline{\mathbf{Q}})$ is.*

Proof. Let $V \subset G(\overline{\mathbf{Q}})$ be the first piece of an admissible filtration, let $H_0 \subset G_{\mathbf{Q}}$ be the subgroup it corresponds to, and let H be the closure of H_0 in G. Over $\mathbf{Z}[1/Np]$, the group H is finite étale, and therefore isomorphic to either μ_p or $\mathbf{Z}/p\mathbf{Z}$, depending on the Galois action on $H(\overline{\mathbf{Q}})$. Over $\mathbf{Z}_p$, the group H is a finite flat commutative group which is generically isomorphic to μ_p or $\mathbf{Z}/p\mathbf{Z}$. If $p \neq 2$, Raynaud's theorem implies that the isomorphism extends over $\mathbf{Z}_p$; the same is true for $p = 2$ by a theorem of Fontaine. (Note: it is important here that we're over $\mathbf{Q}_p$, so that there is no ramification.) Thus H is isomorphic, over $\mathbf{Z}[1/N]$, to μ_p or $\mathbf{Z}/p\mathbf{Z}$. Applying the same reasoning to G/H, the result follows by induction. □

2.3 Invariants

Let G be an admissible group over $\mathbf{Z}$. Following Mazur, we define several invariants:

- Let $\ell(G) = \log_p(\#G_{\mathbf{Q}})$. This coincides with the length of an admissible filtration on G.
- Let $\delta(G) = \log_p(\#G_{\mathbf{Q}}) - \log_p(\#G_{\mathbf{F}_N})$.
- Define $\alpha(G)$ to be the number of $\mathbf{Z}/p\mathbf{Z}$'s appearing in an admissible filtration of G (over $\mathbf{Z}[1/N]$).
- Let $h^i(G)$ be $\log_p(\#\mathrm{H}^i_{\mathrm{fppf}}(\mathrm{Spec}(\mathbf{Z}), G))$, for $i = 0, 1$.

Note that everything we're applying $\log_p$ to is a pth power.

Remark 6. Let G be a group scheme over a base scheme S. The group $\mathrm{H}^1_{\mathrm{fppf}}(S, G)$ admits a fairly concrete description, as follows. A torsor for G is a scheme T/S equipped with an action of G that is simply transitive, in the following sense: for any scheme S'/S and any section $x \in T(S')$, the map $G(S') \to T(S')$ given by $g \mapsto gx$ is a bijection. An fppf (or étale) torsor is a torsor T/S for which there exists an fppf (or étale) cover $S' \to S$ such that $T(S')$ is non-empty. Then $\mathrm{H}^1_{\mathrm{fppf}}(S, G)$ is naturally in bijection with the set of isomorphism classes of fppf torsors; similarly, $\mathrm{H}^1_{\mathrm{et}}(S, G)$ is in bijection with the set of isomorphism classes of étale torsors. Of course, $\mathrm{H}^0_{\mathrm{fppf}}(S, G) = \mathrm{H}^0_{\mathrm{et}}(S, G) = G(S)$ is even easier to describe. □

2.4 Elementary admissible groups

We say that an admissible group G is elementary if $\ell(G) = 1$. Over $\mathbf{Z}[1/N]$, there are two elementary admissible groups: $\mathbf{Z}/p\mathbf{Z}$ and μ_p. Recall the following result:

Proposition 7. *Let H be a pre-admissible group over $\mathbf{Q}_N$. Then extensions of H to a pre-admissible group over $\mathbf{Z}_N$ correspond to unramified Galois submodules of $H(\overline{\mathbf{Q}}_N)$. In particular, if $H(\overline{\mathbf{Q}}_N)$ is unramified and one-dimensional, it admits exactly two such extensions: a finite one (corresponding to the full module) and the extension by zero $H^\flat$ (correspond to the zero submodule).*

This applies to both $\mathbf{Z}/p\mathbf{Z}$ and μ_p over $\mathbf{Z}[1/N]$ (even though we only stated the above result locally). We thus see that there are four elementary admissible groups over $\mathbf{Z}$, namely: $\mathbf{Z}/p\mathbf{Z}$, $(\mathbf{Z}/p\mathbf{Z})^\flat$, μ_p, and $\mu_p^\flat$.

Proposition 8. *The invariants of the elementary admissible groups are given as follows:*

	$\mathbf{Z}/p\mathbf{Z}$	$(\mathbf{Z}/p\mathbf{Z})^\flat$	μ_p	$\mu_p^\flat$
δ	0	1	0	1
α	1	1	0	0
h^0	1	0	*0 if p odd* *1 if $p = 2$*	0
h^1	0	0	*0 if p odd* *1 if $p = 2$*	ϵ

Here ϵ is 0 if p is odd and $N \not\equiv 1 \bmod p$, or if p is even and $N = 3 \pmod 4$, and 1 otherwise.

Proof. The first three lines are obvious. We explain the fourth. For this proof, let $S = \mathrm{Spec}(Z)$. Since $\mathbf{Z}/p\mathbf{Z}$ is étale, $\mathrm{H}^1_{\mathrm{fppf}}(S, \mathbf{Z}/p\mathbf{Z}) = \mathrm{H}^1_{\mathrm{et}}(S, \mathbf{Z}/p\mathbf{Z})$: if T is an fppf torsor for $\mathbf{Z}/p\mathbf{Z}$ over S then there is an fppf cover $S' \to S$ such that $T_{S'}$ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})_{S'}$, and thus étale; this implies that T is étale since this is an fppf local property. Since $\mathbf{Z}/p\mathbf{Z}$ is a constant scheme, we have $\mathrm{H}^1_{\mathrm{et}}(S, \mathbf{Z}/p\mathbf{Z}) = \mathrm{Hom}(\pi_1^{\mathrm{et}}(S), \mathbf{Z}/p\mathbf{Z})$. However, $\pi_1^{\mathrm{et}}(S)$ is trivial: it is the Galois group of the maximal everywhere unramified extension of $\mathbf{Q}$, which is just $\mathbf{Q}$. Thus $h^1(\mathbf{Z}/p\mathbf{Z}) = 0$.

Let G be the quotient of $\mathbf{Z}/p\mathbf{Z}$ by $(\mathbf{Z}/p\mathbf{Z})^\flat$; this is the push-forward of $\mathbf{Z}/p\mathbf{Z}$ along the inclusion $\mathrm{Spec}(\mathbf{F}_N) \to \mathrm{Spec}(\mathbf{Z})$. By what we already have shown, there is a short exact sequence

$$0 \to \mathrm{H}^0_{\mathrm{fppf}}(S, \mathbf{Z}/p\mathbf{Z}) \to \mathrm{H}^0_{\mathrm{fppf}}(S, G) \to \mathrm{H}^1_{\mathrm{fppf}}(S, (\mathbf{Z}/p\mathbf{Z})^\flat) \to 0$$

Both the H^0's are $\mathbf{Z}/p\mathbf{Z}$, which shows $h^1((\mathbf{Z}/p\mathbf{Z})^\flat) = 0$.

We have the following short exact sequence on the fppf site of S:

$$0 \to \mu_p \to \mathbf{G}_m \xrightarrow{p} \mathbf{G}_m \to 0.$$

Taking cohomology, we obtain an exact sequence

$$0 \to \mathbf{Z}^\times/(\mathbf{Z}^\times)^p \to \mathrm{H}^1_{\mathrm{fppf}}(S, \mu_p) \to \mathrm{H}^1_{\mathrm{fppf}}(S, \mathbf{G}_m)[p] \to 0.$$

The group on the left is 0 if p is odd, and $\mathbf{Z}/p\mathbf{Z}$ if $p = 2$. By the theory of fppf descent, $\mathrm{H}^1_{\mathrm{fppf}}(S, \mathbf{G}_m) = \mathrm{H}^1_{\mathrm{Zar}}(S, \mathbf{G}_m) = \mathrm{Pic}(S)$, which is just the ideal class group of $\mathbf{Q}$, which is trivial. Thus $h^1(\mu_p)$ is 1 if $p = 2$ and 0 otherwise.

Let G be the quotient of μ_p by $\mu_p^\flat$: this is the push-forward of μ_p along the inclusion $\mathrm{Spec}(\mathbf{F}_N) \to \mathrm{Spec}(\mathbf{Z})$. We have an exact sequence

$$0 \to \mathrm{H}^0_{\mathrm{fppf}}(S, \mu_p) \to \mathrm{H}^0_{\mathrm{fppf}}(S, G) \to \mathrm{H}^1_{\mathrm{fppf}}(S, \mu_p^\flat) \to \mathrm{H}^1_{\mathrm{fppf}}(S, \mu_p) \to \mathrm{H}^1_{\mathrm{fppf}}(S, G)$$

If $p \neq 2$, then $\mathrm{H}^i_{\mathrm{fppf}}(S, \mu_p) = 0$ for $i = 0, 1$, and so the map $\mathrm{H}^0_{\mathrm{fppf}}(S, G) \to \mathrm{H}^1_{\mathrm{fppf}}(S, \mu_p^\flat)$ is an isomorphism. The source is just $\mu_p(\mathbf{F}_N)$, which has order p if $p \mid N - 1$, and vanishes otherwise. Now suppose that p is even. Then the map $\mathrm{H}^0_{\mathrm{fppf}}(S, \mu_p) \to \mathrm{H}^0_{\mathrm{fppf}}(S, G)$ is an isomorphism. Kummer theory shows that the unique non-trivial element of $\mathrm{H}^1_{\mathrm{fppf}}(S, \mu_2)$ is represented by the μ_2 torsor $\mathrm{Spec}(\mathbf{Z}[\sqrt{-1}])$. This torsor splits over $\mathbf{F}_N$ if and only if -1 is a square mod N. Thus the kernel of $\mathrm{H}^1_{\mathrm{fppf}}(S, \mu_p) \to \mathrm{H}^1_{\mathrm{fppf}}(S, G)$ is $\mathbf{Z}/2\mathbf{Z}$ if N is 1 mod 4, and 0 if N is 3 mod 4. This completes the proof. □

Proposition 9. *Let G be an admissible group over $\mathbf{Z}$. Then $h^1(G) - h^0(G) \le \delta(G) - \alpha(G)$.*

Proof. Let

$$0 \to G_1 \to G_2 \to G_3 \to 0$$

be a short exact sequence of admissible groups. From the first few terms of the long exact sequence in cohomology, we find

$$h^1(G_2) - h^0(G_2) \le (h^1(G_1) - h^0(G_1)) + (h^1(G_3) - h^0(G_3)),$$

that is, $h^1 - h^0$ is sub-additive. It is clear that

$$\delta(G_2) - \alpha(G_2) = (\delta(G_1) - \alpha(G_1)) + (\delta(G_3) - \alpha(G_3)),$$

i.e., $\delta - \alpha$ is additive (in fact, both δ and α are additive separately). Thus if the result is true for G_1 and G_3 then it is true for G_2. It thus suffices to prove the result for elementary admissible groups, which follows easily from the computation of the invariants. □

3 Proof of criterion

We now prove the main theorem. Let $\mathcal{A}$ be the Néron model of A over $\mathbf{Z}$ and let $\mathcal{A}^\circ$ be its identity component (i.e., throw out the non-identity components in each fiber). Let $G_n = \mathcal{A}^\circ[p^n]$. Since A has good reduction away from N, it is clear that G_n is pre-admissible. The condition on $A[p](\overline{\mathbf{Q}})$ exactly says that it is admissible, and so $A[p^n](\overline{\mathbf{Q}})$ is as well, since it is an iterated self-extension of $A[p](\overline{\mathbf{Q}})$. It follows that G_n is admissible.

We now compute the invariants α and δ for G_n. We begin with δ. We have $\ell(G_n) = 2gn$, where $g = \dim(A)$. Now, $(G_n)_{\mathbf{F}_N} = \mathcal{A}^\circ_{\mathbf{F}_N}[p^n]$. By hypothesis, $\mathcal{A}^\circ_{\mathbf{F}_N}$ is a torus of dimension g, and so its p^n torsion has cardinality p^{ng}. Thus $(G_n)_{\mathbf{F}_N}$ has cardinality p^{gn}. We thus find $\delta(G_n) = gn$.

We now compute α. Since α is additive and only depends on the group over $\mathbf{Z}[1/N]$, we see that $\alpha(G_n) = n\alpha(G_1)$, so it suffices to treat the $n = 1$ case. Note that $\alpha(G_1)$ is the number of $\mathbf{Z}/p\mathbf{Z}$'s appearing in $(G_1)_{\mathbf{F}_p}$; thus it is $\log_p$ of the order of the étale part of $\mathcal{A}_{\mathbf{F}_p}[p]$. Since G_1 is admissible, $\mathcal{A}_{\mathbf{F}_p}[p]$ has only $\mathbf{Z}/p\mathbf{Z}$'s and μ_p's in it, and so $\mathcal{A}_{\mathbf{F}_p}$ is ordinary. This implies that its étale part has order p^g, and so $\alpha(G_1) = g$. Thus $\alpha(G_n) = gn$.

We thus have $\delta(G_n) = gn$ and $\alpha(G_n) = gn$. It follows that $h^1(G_n) - h^0(G_n) \le 0$. However, $h^0(G_n)$ is the p^n torsion in $\mathcal{A}^\circ(\mathbf{Z}) \subset \mathcal{A}(\mathbf{Z}) = A(\mathbf{Q})$, which is bounded independent of n by the Mordell–Weil theorem. It follows that $h^1(G_n)$ is bounded independent of n.

Consider now the short exact sequence of sheaves on the fppf site of Spec($\mathbf{Z}$):

$$0 \to G_n \to \mathcal{A}^\circ \xrightarrow{p^n} \mathcal{A}^\circ \to 0.$$

A few remarks:

- The map $[p^n]\colon \mathcal{A} \to \mathcal{A}$ is not a surjection of fppf sheaves in general since the component group of $\mathcal{A}_{\mathbf{F}_N}$ might have p-torsion. This is why we use $\mathcal{A}^\circ$ instead of $\mathcal{A}$.
- The map $[p^n]\colon \mathcal{A}^\circ \to \mathcal{A}^\circ$ is not a surjection of étale sheaves in general, since give a section $x \in \mathcal{A}^\circ(S)$, one cannot in general find an étale extension S'/S a section $y \in \mathcal{A}^\circ(S')$ such that $p^n y = x$. This is why we must use fppf cohomology.
- The map $[p^n]\colon \mathcal{A}^\circ \to \mathcal{A}^\circ$ is faithfully flat: the key point is that $\mathcal{A}^\circ$ is p-divisible, and so $[p^n]$ is surjective on points. This implies that $[p^n]\colon \mathcal{A}^\circ \to \mathcal{A}^\circ$ is a surjection of fppf sheaves.

Taking cohomology, we obtain an injection

$$\mathrm{H}^0_{\mathrm{fppf}}(\mathrm{Spec}(\mathbf{Z}), \mathcal{A}^\circ) \otimes \mathbf{Z}/p^n\mathbf{Z} \to \mathrm{H}^1_{\mathrm{fppf}}(\mathrm{Spec}(\mathbf{Z}), G_n).$$

It follows that the cardinality of $\mathcal{A}^\circ(\mathbf{Z}) \otimes \mathbf{Z}/p^n\mathbf{Z}$ is bounded as $n \to \infty$.

Let C be the $\mathbf{F}_N$-points of the component group of $\mathcal{A}_{\mathbf{F}_N}$. Then there is an exact sequence

$$0 \to \mathcal{A}^\circ(\mathbf{Z}) \to \mathcal{A}(\mathbf{Z}) \to C$$

It follows that $\mathcal{A}^\circ(\mathbf{Z})$ is a finite index subgroup of $\mathcal{A}(\mathbf{Z}) = A(\mathbf{Q})$. In particular, $\mathcal{A}^\circ(\mathbf{Z})$ is finitely generated. Since the cardinality of $\mathcal{A}^\circ(\mathbf{Z}) \otimes \mathbf{Z}/p^n\mathbf{Z}$ is bounded, it follows that $\mathcal{A}^\circ(\mathbf{Z})$ has rank 0. Thus $A(\mathbf{Q})$ has rank zero, as it contains $\mathcal{A}^\circ(\mathbf{Z})$ with finite index.