Abelian Varieties

Abelian Variety: A projective group variety (the group law is automatically commutative).

Examples:
1. Elliptic curves \( y^2 + y = x^3 - x \)
2. Jacobians of curves
3. Modular abelian varieties
4. Weil restriction of scalars

The Modular Jacobian \( J_1(N) \)

\( J_1(N) = \text{Jacobian of } X_1(N) \)

• The Hecke Algebra:
  \( T = \mathbb{Z}[T_1, T_2, \ldots] \hookrightarrow \text{End}(J_1(N)) \)

• Cuspidal Modular Forms:
  \( S_2(\Gamma_1(N)) = H^0(X_1(N), \Omega^{1}_{X_1(N)}) \)

Jacobians of Curves

If \( X \) is an algebraic curve then
\( \text{Jac}(X) = \{ \text{divisor classes of degree 0 on } X \} \),
has structure of abelian variety of dimension = genus(\( X \)).

Example: Elliptic curves are their own Jacobians.

Example: Let \( X_1(N) \) be the modular curve that (tries to) parametrize isomorphism classes of pairs \((E, \text{embedding of } \mathbb{Z}/N\mathbb{Z} \text{ into } E)\).
The Jacobian of \( X_1(N) \) is \( J_1(N) \).

Introduction to Modular Abelian Varieties and Shafarevich-Tate Groups

William Stein
Harvard University
September 15, 2003 for Math 252

Overview

0. Syllabus
1. Modular Abelian Varieties
2. Shafarevich-Tate Group
3. A Story about Orders of Shafarevich-Tate Groups

Modular Abelian Varieties

A modular abelian variety is any quotient of \( J_1(N) \).

Goro Shimura associated an abelian variety \( A_f \) to any newform \( f \) (much of Math 252 will culminate in this construction):
\[ A_f := J_1(N)/I_f J_1(N) \]
where
\[ f = q + \sum_{n \geq 2} a_n q^n \in S_2(\Gamma_1(N)) \]
\[ I_f = \text{Ker}(T \mapsto \mathbb{Z}[a_1, a_2, a_3, \ldots]), \quad T_n \mapsto a_n \]
A=Af Has Lots of Structure

• A is an abelian variety defined over \( \mathbb{Q} \)
• The ring \( \mathbb{Z}[a_1,a_2,\ldots] \) is a subring of \( \text{End}(A) \)
• The dimension of \( A \) equals the degree of the field \( \mathbb{Q}[a_1,a_2,\ldots] \) generated by the \( a_n \)

Modular Abelian Varieties \( A_f \) Are Interesting!!!

• Wiles et al.: Every elliptic curve over \( \mathbb{Q} \) is modular, i.e., isogenous to an \( A_f \)
  Consequence (Ribet): Fermat’s Last Theorem
  (I will not sketch a proof of either of these statements in 252.)
• Serre’s Conjecture: Every odd irreducible Galois representation
  \( \rho : \text{Gal}(\mathbb{Q}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F}_p) \)
  occurs up to twist in the torsion points of some \( A_f \).
  (I will discuss Serre’s conjecture further in 252.)

Birch and Swinnerton-Dyer

The Birch and Swinnerton-Dyer Conjecture

\[
L(1, A_f) = \frac{\Pi_{\text{irred}} \cdot \Omega_{A_f} \cdot \text{Reg}_{A_f}}{\# A_f(\mathbb{Q}) \cdot \# A_f(\mathbb{Q})_{\text{tor}}} \cdot \# \text{III}(A_f/\mathbb{Q})
\]

\[
L(A_f, s) = \prod_{\text{galois orbit}} \left( \sum_{n=1}^{\infty} a(n)^s \right)
\]

\( r = \text{ord}_{s=1} L(A_f, s) \)
\( c_p = \text{order of component group at } p \)
\( \Omega_{A_f} = \text{canonical measure of } A_f(\mathbb{R}) \)

(We will spend at least 2 weeks on this conjecture in Math 252.)

The Shafarevich-Tate Group of \( A_f \)

“Sha” is a subgroup of the first Galois cohomology of \( A_f \); it measures failure of local to global:

\[
\text{III}(A_f/\mathbb{Q}) = \ker \left( H^1(\mathbb{Q}, A_f) \to \bigoplus \text{H}^1(\mathbb{Q}, A_f) \right)
\]

Example:

\[
[3x^3 + 4y^3 + 5z^3 = 0] \in \text{III}(\mathbb{Q})
\]

Conjecture (Shafarevich-Tate):

\[
\text{III}(A_f/\mathbb{Q}) \text{ is finite.}
\]

From Birch’s paper Conjectures Concerning Elliptic Curves

The so-called Tate-Shafarevich conjecture (adopted by Lang, Cassels and Tate, but apparently disowned by Shafarevich) asserts that TS is always a finite group: this is a very natural strengthening of the Selmer conjecture. Unfortunately, the evidence is very weak; in fact, TS has not yet been fully computed for a single curve. It is very difficult to compute more than TS; for a general elliptic curve over \( \mathbb{Q} \), and (TS), for a curve of shape \( x^2 = y^3 + B \), Cassels’ theorem implies that if TS is finite then its order must be a square.

In our computations leading to the formula

\[
\alpha(x_0^2 + y_0^2) \cdot (TS) \cdot \text{TS}^2
\]

we actually verified that \( f^2 \cdot (TS) \) was an integer square, usually 1, and was divisible by the order of (TS), when this could be calculated.
The Shafarevich-Tate Group \(\Sha(A_f/\mathbb{Q})\)


These are partial results towards the Birch and Swinnerton-Dyer conjecture, which we will discuss at the end of the course.

Now for a motivating story that involves lots of things you shouldn’t understand yet, but will when this course is over:

**QUESTION:** What can we say about the possible sizes of Shafarevich-Tate Groups?

The Dual Abelian Variety

The dual of \(A\) is an abelian variety isogenous to \(A\) that parametrizes classes of invertible sheaves on \(A\) that are algebraically equivalent to zero.

\[A^\vee = \text{Pic}^0(A)\]

The dual is functorial:

If \(A \to B\) then \(B^\vee \to A^\vee\).

Polarized Abelian Varieties

A polarization of \(A\) is an isogeny (homomorphism) from \(A\) to its dual that is induced by a divisor on \(A\). A polarization of degree 1 is called a principal polarization.

**Theorem.** If \(A\) is the Jacobian of a curve, then \(A\) is canonically principally polarized. For example, elliptic curves are principally polarized.

Cassels-Tate Pairing

**Theorem.** If \(A\) is principally polarized by a polarization arising from an \(F\)-rational divisor, then there is a nondegenerate alternating pairing on \(\Sha(A_f/F)\) so for all \(\pi\):

\[\#\Sha(A_f/F)_{br} \cap \Sha(F)_{br} \approx \square\]

(Same statement away from minimal degree of polarizations.)

**Corollary.** If \(\dim A = 1\) and \(\Sha(A_f/F)\) finite, then

\[\#\Sha(A_f/F) = \square\]
What if the abelian variety $A$ is not an elliptic curve?

Assume $\# \Sha(A/F)$ is finite. Overly optimistic literature:

- Page 306 of [Tate, 1963]: If $A$ is a Jacobian then $\# \Sha(A/F) = 0$.
- Page 149 of [Swinnerton-Dyer, 1967]: Tate proved that $\# \Sha(A/F) = 0$.

Michael Stoll's Computation

During a grey winter day in 1996, Michael Stoll sat puzzling over a computation in his study on a majestic embassy-peppered hill near Bonn overlooking the Rhine. He had implemented an algorithm for computing 2-torsion in Shafarevich-Tate groups of Jacobians of hyperelliptic curves. He stared at a curve $X$ for which his computations were in direct contradiction to the previous slide!

$\# \Sha(Jac(X)/Q)[2] = 2$.

What was wrong????

---

Poonen-Stoll

From: Michael Stoll (9 Dec 1996)

Dear Bjorn, Dear Ed:

[...]

I think I may have resolved the problem. There is nothing wrong with the computations. The thing that is wrong is the claim that Sha must have square order!

Poonen-Stoll Theorem

Theorem (Annals, 1999): Suppose $J$ is the Jacobian of a curve and $J$ has finite Shafarevich-Tate group. Then

$\# \Sha(J/F) = 0$ or $2 \cdot 0$.

Example: The Jacobian of this curve has Sha of order 2

$y^2 = -3(x^2 + 1)(x^2 - 6x + 1)(x^2 + 6x + 1)$

---

Is Sha Always Square or Twice a Square?

Poonen asked at the Arizona Winter School in 2000, “Is there an abelian variety $A$ with Shafarevich-Tate group of order three?”

---

In 2002 I finally found Sha of order 3 (times a square):
Plenty of Non-square Sha!

- **Theorem (Stein):** For every prime \( p < 25000 \) there is an abelian variety \( A \) over \( \mathbb{Q} \) such that
  \[
  \#\Sha(A/Q) = p \cdot \square
  \]

- **Conjecture (Stein):** Same statement for all \( p \).

How to Construct Non-square Sha

While attempting to connect groups of points on elliptic curves of high rank to Shafarevich-Tate groups of abelian varieties of rank 0, I found a construction of non-square Shafarevich-Tate groups.

The Main Theorem

**Theorem (Stein).** Suppose \( E \) is an elliptic curve and \( p \) an odd prime that satisfies various technical hypothesis. Suppose \( E \) is a prime congruent to 1 mod \( p \) (and not dividing \( N_E \)) such that

\[
L(E, \chi_{E^2}) \neq 0 \quad \text{and} \quad \rho(E) \not\equiv \chi \pmod{p}
\]

Here \( \chi \) is a Dirichlet character of order \( p \) and conductor \( l \) corresponding to an abelian extension \( K \). Then there is a twist \( A \) of a product of copies of \( E \) and an exact sequence

\[
0 \to (\mathbb{Q}/p^\infty) \to \Sha(A/Q) \to \Sha(E/K)[p^\infty] \to \Sha(E/Q)[p^\infty] \to 0.
\]

If \( E \) has odd rank and \( \Sha(E/Q)[p^\infty] \) is finite then \( \Sha(A/Q)[p^\infty] \) has order that is **not** a perfect square.

**Proof Uses the Weil Restriction of Scalars**

\[
F/K: \text{finite extension of number fields}
\]
\[
A/F: \text{abelian variety over } F
\]
\[
R = \text{Res}_{F/K}(A) \text{ abelian variety over } K
\]
\[
\begin{align*}
\dim(R) &= \dim(A) \cdot [F : K] \\
R(S) &= A(S \times_K F)
\end{align*}
\]

Functorial characterization:

For any \( K \)-scheme \( S \),

\[
R(S) = A(S \times_K F)
\]

Proof Sketch (I): Exact Sequence of Neron Models

The exact sequence

\[
0 \to A \to R \to E \to 0
\]

extends to an exact sequence of Néron models (and hence sheaves for the étale topology) over \( \mathbb{Z} \):

\[
0 \to A \to R \to E \to 0.
\]

To check this, we use that formation of Néron models commutes with unramified base change and Prop. 7.5.3(a) of [Néron Models, 1995].

What is the Abelian Variety \( A \)?

Let \( R \) be the Weil restriction of scalars of \( E \) from \( K \) down to \( \mathbb{Q} \), so \( R \) is an abelian variety over \( \mathbb{Q} \) of dimension \( p \) (i.e., the degree of \( K \)). Then \( A \) is the kernel of the map induced by trace:

\[
0 \to A \to R \to E \to 0
\]

Note that

- \( A \) has dimension \( p - 1 \)
- \( A \) is isomorphic over \( K \) to a product of copies of \( E \)
- Our hypothesis on \( E \) and Kato’s finiteness theorems imply that \( A/Q \) and \( \#\Sha(A/Q) \) are both finite.
- Is isogenous to \( A_f \) where \( f \) is a twist of newform attached to \( E \).
Proof (2): Mazur’s Etale Cohomology Sha Theorem

Mazur’s Rational Points of Abelian Varieties with Values in Towers of Number Fields:

For \( F = A, R, E \) let \( \mathcal{F} = \text{Néron}(F) \). Then

\[
H^1_{\text{ét}}(\mathbb{Z}, \mathcal{F})[p^n] = \text{Sha}(F/\mathbb{Q})[p^n]
\]

In general this is not true, but our hypothesis on \( p \) and \( \ell \) are exactly strong enough to kill the relevant error terms.

Proof (3): Long Exact Sequence

The long exact sequence of étale cohomology begins

\[
\cdots \rightarrow H^1_{\text{ét}}(\mathbb{Z}, A) \rightarrow H^1_{\text{ét}}(\mathbb{Z}, \mathcal{E}) \rightarrow \delta \rightarrow H^2_{\text{ét}}(\mathbb{Z}, \mathcal{E}) \rightarrow H^2_{\text{ét}}(\mathbb{Z}, A)
\]

Take the \( p \)-power torsion in this exact sequence then use Mazur’s theorem. Next analyze the cokernel of \( \delta \).

Proof (4): Apply Kato’s Finiteness Theorems

We have \( \text{Coker}(\delta) = E(\mathbb{Q})/pE(\mathbb{Q}) \) since

\[
L(E, \chi_{p^n}, 1) \neq 0 \quad \text{and} \quad a_{\ell} \neq \ell + 1 \pmod{p}.
\]

(To see this requires chasing some diagrams.)

Also \( H^2_{\text{ét}}(\mathbb{Z}, A)[p^n] = 0 \) (proof uses Artin-Mazur duality).

Both of these steps use Kato’s finiteness theorem in an essential way. Putting everything together yields the claimed exact sequence

\[
0 \rightarrow E(\mathbb{Q})/pE(\mathbb{Q}) \rightarrow \text{Sha}(A/Q)[p^n] \rightarrow \text{Sha}(E/K)[p^n] \rightarrow \text{Sha}(E/Q)[p^n] \rightarrow 0.
\]

Thank you for coming and… Come Back!!