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 3: Abelian varieties (analytic theory)

This lecture covers two disjoint topics. First, I go over the theory of elliptic curves over finite fields (point counting and the notions of ordinary and supersingular). Then I talk about the abelian varieties over the complex numbers from the analytic point of view.

1 Elliptic curves over finite fields

A good reference for this section is Chapter V of Silverman's "The arithmetic of elliptic curves" (MR0817210).

1.1 Point counting

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_q$. Then $E^{(q)} = E$, and so the Frobenius map $F_q$ maps $E$ to itself. A point $x$ of $E(\mathbb{F}_q)$ belongs to $E(\mathbb{F}_q)$ if and only if it is fixed by $F_q$ (since this is equivalent to it being Galois invariant). Thus $E(\mathbb{F}_q)$ is the set of $\mathbb{F}_q$-points of the kernel of the endomorphism $1 - F_q$. This endomorphism is separable: indeed, if $\omega$ is a differential on $E$ then $F_q^*(\omega) = 0$, and so $(1 - F_q)^* \omega = \omega$ is non-zero. We have thus proved the following proposition:

**Proposition 1.** $\# E(\mathbb{F}_q) = \deg(1 - F_q)$.

Recall that we have defined a positive definite bilinear pairing $\langle , \rangle$ on $\text{End}(E)$, and that $\langle f, f \rangle = \deg(f)$. Appealing to the Cauchy–Schwartz inequality, we find $\langle 1, -F_q \rangle^2 \leq \deg(q) \deg(F_q) = q$, and so $\langle 1, -F_q \rangle \leq \sqrt{q}$. But, by definition,

$$2\langle 1, -F_q \rangle = \deg(1 - F_q) - \deg(1) - \deg(F_q),$$

and so we have the following theorem

**Theorem 2** (Hasse bound). $|\# E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.

In other words, we can write $\# E(\mathbb{F}_q)$ as $q + 1 - a$, where $a$ is an error term of size at most $2\sqrt{q}$. We have $a = \langle 1, F_q \rangle$ by the above. We also have the following interpretation of $a$:

**Proposition 3.** We have $a = \text{tr}(F_q | T_1E)$.

**Proof.** This is formal: if $A$ is any $2 \times 2$ matrix, then

$$\text{tr}(A) = 1 + \det(A) - \det(1 - A).$$

Applying this to the matrix of $F_q$ on $T_1E$, the result follows. \qed

A Weil number (with respect to $q$) of weight $w$ is an algebraic number with the property that any complex embedding of it has absolute value $q^{w/2}$.

**Theorem 4** (Riemann hypothesis). The eigenvalues of $F_q$ on $T_1E$ are Weil numbers of weight 1.

**Proof.** The characteristic polynomial of $F_q$ on $T_1E$ is $T^2 - aT + q$. The eigenvalues are the roots of this polynomial, i.e., $(a \pm \sqrt{a^2 - 4q})/2$. The Hasse bound shows that $a^2 - 4q \leq 0$, and so the absolute value of this algebraic number (or its complex conjugate) is $\sqrt{q}$. This completes the proof. \qed

These are notes for Math 679, taught in the Fall 2013 semester at the University of Michigan by Andrew Snowden.
The zeta function of a variety $X/F_q$ is defined by

$$Z_X(T) = \exp \left( \sum_{r=1}^{\infty} \#X(F_q) \frac{T^r}{r} \right).$$

**Theorem 5** (Rationality of the zeta function). We have

$$Z_E(T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}.$$

**Proof.** The above results show that

$$\#E(F_q) = q + 1 - \text{tr}(F_q | T_1 E).$$

Let $\alpha$ and $\beta$ be the eigenvalues of $F_q$ on $T_1 E$. Since $F_q$ is just $F_q^r$, the eigenvalues of $F_q^r$ on $T_1(E)$ are $\alpha^r$ and $\beta^r$. We thus see that

$$\#E(F_q^r) = q^r + 1 - \alpha^r - \beta^r.$$ We now have

$$\sum_{r=1}^{\infty} \#E(F_q^r) \frac{T^r}{r} = -\log(1 - T) - \log(1 - qT) + \log(1 - \alpha T) + \log(1 - \beta T),$$

and so

$$Z_E(T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}.$$

from which the result easily follows. \qed

**Corollary 6.** $\#E(F_q^r)$ is determined, for any $r$, from $\#E(F_q)$.

Suppose that $f: E_1 \to E_2$ is an isogeny. Then $f$ induces a map $T_1(E_1) \to T_1(E_2)$ which commutes with Frobenius. Since the kernel of $f$ is finite, the map it induces on Tate modules has finite index image; in particular, it induces an isomorphism after tensoring with $\mathbb{Q}_l$. It follows that the eigenvalues of Frobenius on the two Tate modules agree, and so:

**Theorem 7.** If $E_1$ and $E_2$ are isogenous then $\#E_1(F_q) = \#E_2(F_q)$.

In fact, the converse to this theorem is also true, as shown by Tate.

### 1.2 Ordinary and supersingular curves

Let $E$ be an elliptic curve over a field $k$ of characteristic $p$. Then the map $[p]: E \to E$ is not separable and has degree $p^2$. It follows that the separable degree of $[p]$ is either $p$ or 1. In the first case, $E$ is called ordinary, and in the second case, supersingular. The following result follows immediately from the definitions, and earlier results:

**Proposition 8.** If $E$ is ordinary then $E[p](\overline{k}) \cong \mathbb{Z}/p\mathbb{Z}$. If $E$ is supersingular then $E[p](\overline{k}) = 0$.

We will revisit the ordinary/supersingular dichotomy after discussing group schemes. For now, we prove just one more result.

**Proposition 9.** If $E$ is supersingular then $j(E) \in \mathbb{F}_{p^2}$. 

2
Proof. Suppose $E$ is supersingular. Then $[p]$ is completely inseparable, and thus factors as $E \to E^{(p^2)} \to E$, where the first map is the Frobenius $F_{p^2}$ and the second map is an isomorphism (since it has degree 1). Since $j(E^{(p^2)})$ is equal to $F_{p^2}(j(E))$ and $j$ is an isomorphism invariant, we see that $j(E) = F_{p^2}(j(E))$, from which the result follows.

Corollary 10. Assume $k$ algebraically closed. Then there are only finitely many supersingular elliptic curves over $k$, and they can all be defined over $\mathbf{F}_{p^2}$.

Proof. An elliptic curve over an algebraically closed field descends to the field of its $j$-invariant, which gives the final statement. The finiteness statement follows immediately from this.

2 Abelian varieties

A good reference for this section is the first chapter of Mumford’s “Abelian varieties” (MR0282985).

2.1 Definition and relation to elliptic curves

Definition 11. An abelian variety is a complete connected group variety (over some field).

Example 12. An elliptic curve is a one-dimensional abelian variety.

Proposition 13. Every one-dimensional abelian variety is an elliptic curve.

Proof. Let $A$ be a one-dimensional abelian variety. We must show that $A$ has genus 1. Pick a non-zero cotangent vector to $A$ at the identity. The group law on $A$ allows us to translate this vector uniquely to any other point, and so we can find a nowhere vanishing holomorphic 1-form on $A$. This provides an isomorphism $\Omega^1_A \cong \mathcal{O}_A$, and so $H^0(A, \Omega^1_A)$ is one-dimensional.

For the rest of this lecture we work over the complex numbers.

2.2 Compact complex Lie groups

Let $A$ be an abelian variety. Then $A(\mathbb{C})$ is a connected compact complex Lie group. We begin by investigating such groups. Thus let $X$ be such a group. Define $V$ to be the tangent space to $X$ at the identity (the Lie algebra). Let $g = \dim(X)$. Recall that there is a holomorphic map $\exp: V \to X$. We have the following results:

- $X$ is commutative. Reason: the map $\text{Ad}: X \to \text{End}(V)$ is holomorphic, and therefore constant, since $X$ is compact and $\text{End}(V)$ is a vector space. Since $\text{Ad}$ assumes the value 1, this is the only value it assumes. It follows that $X$ acts trivially on $\text{End}(V)$, and so $V$ is a commutative Lie algebra. The result follows.

- $\exp$ is a homomorphism. Reason: this follows from commutativity.

- $\exp$ is surjective. Reason: the image of $\exp$ contains an open subset of $X$, since $\exp$ is a local homeomorphism. The image of $\exp$ is also a subgroup of $X$. Thus the image is an open subgroup $U$. The quotient $X/U$ is discrete, since $U$ is open, and connected, since $X$ is, and is therefore a point. Thus $X = U$.

- $M = \ker(\exp)$ is a lattice in $V$, and thus isomorphic to $\mathbb{Z}^g$. Reason: since $\exp$ is a local homeomorphism, $M$ is discrete. Since $X = V/M$ is compact, $M$ is cocompact.
• $X$ is a torus, i.e., isomorphic to a product of circles. Reason: clear from $X = V/M$.

• The $n$-torsion $X[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2g$. Reason: $X[n]$ is isomorphic to $\frac{1}{n}M/M$ by the exponential map.

• $H^1(X, \mathbb{Z})$ is naturally isomorphic to Hom$(\wedge^1(M), \mathbb{Z})$. Reason: a simple application of the K"unneth formula shows that if $T$ is any torus then cup product induces an isomorphism $\wedge^1(H^1(T, \mathbb{Z})) \to H^1(T, \mathbb{Z})$. For our torus $X$, we have $H_1(X, \mathbb{Z}) = M$, and the result follows.

### 2.3 Line bundles on complex tori

Let $X = V/M$, as above. Define Pic$(X)$ (the Picard group of $X$) to be the set of isomorphism classes of line bundles on $X$. This is a group under tensor product. Define Pic$^0(X)$ to be the subgroup consisting of those bundles which are topologically trivial, and define NS$(X)$ (the Néron–Severi group) to be the quotient $\text{Pic}(X)/\text{Pic}^0(X)$. We are now going to describe how to compute these groups in terms of $V$ and $M$.

A Riemann form on $V$ (with respect to $M$) is a Hermitian form $H$ such that $E = \text{Im}H$ takes integer values when restricted to $M$. (Note: some people include positive definite in their definition of Riemann form; we do not.) Let $\mathcal{R}$ be the set of Riemann forms, which forms a group under addition. Let $\mathcal{P}$ be the set of pairs $(H, \alpha)$, where $H \in \mathcal{R}$ and $\alpha: M \to U(1)$ is a function satisfying $\alpha(x + y) = e^{i\pi E(x,y)}\alpha(x)\alpha(y)$. (Here $U(1)$ is the set of complex numbers of absolute value 1.) We give $\mathcal{P}$ the structure of a group by $(H_1, \alpha_1)(H_2, \alpha_2) = (H_1 + H_2, \alpha_1\alpha_2)$. Let $\mathcal{P}^0$ be the group of homomorphisms $M \to U(1)$, regarded as the subgroup of $\mathcal{P}$ with $H = 0$.

**Theorem 14** (Appell–Humbert). We have an isomorphism $\text{Pic}(X) \cong \mathcal{P}$, which induces isomorphisms $\text{Pic}^0(X) \cong \mathcal{P}^0$ and $\text{NS}(X) \cong \mathcal{R}$.

Some remarks on the theorem:

• Let $\pi: V \to X$ be the quotient map. If $L$ is a line bundle on $X$ then $\pi^*(L)$ is the trivial line bundle on $V$, since all line bundles on $V$ are trivial. Furthermore, $\pi^*(L)$ is $M$-equivariant, and $L$ can be recovered as the quotient of $\pi^*(L)$ by $M$. Thus to prove the theorem, it suffices to understand the $M$-equivariant structures on the trivial line bundle over $V$.

• Let $(H, \alpha) \in \mathcal{P}$. Define an action of $M$ on $V \times \mathbb{C}$ by

$$
\lambda \cdot (v, z) = (v + \lambda, \alpha(\lambda)e^{\pi H(v, \lambda) + \pi H(\lambda, \lambda)/2}z).
$$

This gives the trivial bundle on $V$ an $M$-equivariance. We let $L(H, \alpha)$ be the quotient, a line bundle on $X$. The isomorphism $\mathcal{P} \to \text{Pic}(X)$ is $(H, \alpha) \mapsto L(H, \alpha)$. The main content of the theorem is to show that the equivariances we just constructed are all of them.

• Remark. There is a bijection between Hermitian forms $H$ on $V$ and alternating real forms $E$ satisfying $E(ix, iy) = E(x, y)$. The correspondence takes $H$ to $E = \text{Im}H$, and $E$ to $H(x, y) = E(ix, y) + iE(x, y)$. Thus a Riemann form $H$ is determined by the associated alternating pairing on $M$.

• Let $(H, \alpha) \in \mathcal{P}$, and let $E = \text{Im}H$. Then $E$ defines an element of Hom$(\wedge^2(M), \mathbb{Z})$. But we have previously identified this group with $H^2(X, \mathbb{Z})$. In fact, $E$, regarded as an element of $H^2$, is the Chern class $c_1(L(H, \alpha))$. We thus see that $L(H, \alpha)$ is topologically trivial if and only if $E = 0$, which is the same as $H = 0$. This gives the isomorphic $\text{Pic}^0(X) \cong \mathcal{P}^0$. 

4
Let \( x \in X \) and let \( t_x : X \to X \) be the translation-by-\( x \) map, i.e., \( t_x(y) = x + y \). Given a line bundle \( L \) on \( X \), we get a new line bundle \( t_x^*(L) \) on \( X \). We thus get an action of \( X \) on \( \text{Pic}(X) \), with \( x \) acting by \( t_x^* \). The following proposition describes this action in terms of the Appell–Humbert theorem.

**Proposition 15.** We have an isomorphism \( t_x^* L(H, \alpha) \cong L(H, \alpha \cdot e^{2\pi i E(x, -)}) \).

A few remarks:

- First, we note that \( \lambda \mapsto e^{2\pi i E(x, \lambda)} \) makes sense as a function on \( M \), since \( E \) takes integral values on \( M \).

- The line bundle \( L(H, \alpha) \) is translation invariant (i.e., isomorphic to its pullbacks by \( t_x^* \)) if and only if \( H = 0 \). Indeed, it is clear that if \( H = 0 \) then \( L(H, \alpha) \) is translation invariant. Conversely, if \( L(H, \alpha) \) is translation invariant then \( e^{2\pi i E(x, \lambda)} = 1 \) for all \( x \in V \) and all \( \lambda \in M \), from which it easily follows that \( E = 0 \), and so \( H = 0 \) as well. We can therefore characterize \( \text{Pic}^0(X) \) as the group of translation invariant line bundles on \( X \).

- Let \( L \) be a line bundle on \( X \). Then \( x \mapsto t_x^*(L) \otimes L^* \) defines a group homomorphism \( \phi_L : X \to \text{Pic}^0(X) \). Indeed, taking \( L = L(H, \alpha) \), we see that \( t_x^*(L) \otimes L^* \) is equal to \( L(0, e^{2\pi i E(x, -)}) \). It follows that, in fact, \( \phi_L \) depends only on \( c_1(L) \).

### 2.4 Sections of line bundles

A \( \theta \)-function on \( V \) with respect to \((H, \alpha) \in \mathcal{P} \) is a holomorphic function \( \theta : V \to \mathbb{C} \) satisfying the functional equation

\[
\theta(v + \lambda) = \alpha(\lambda)e^{\pi H(v, \lambda) + \pi H(\lambda, \lambda)/2}.
\]

Given a section \( s \) of \( L(H, \alpha) \) over \( X \), we obtain a section \( \pi^*(s) \) of \( \pi^*(L(H, \alpha)) \) over \( V \). Identifying \( \pi^*(L(H, \alpha)) \) with the trivial bundle, \( \pi^*(s) \) becomes a function on \( V \), and the equivariance condition is exactly the above functional equation. We therefore find:

**Proposition 16.** The space \( \Gamma(X, L(H, \alpha)) \) is canonically identified with the space of \( \theta \)-functions for \((H, \alpha) \).

Suppose that \( H \) is degenerate, and let \( V_0 \) be its kernel (i.e., \( x \in V_0 \) if \( H(x, -) = 0 \)). Then \( V_0 \) is also the kernel of \( E \), and since \( E \) takes integral values on \( M \), it follows that \( M_0 = V_0 \cap M \) is a lattice in \( V_0 \). Let \( \theta \) be a \( \theta \)-function, and \( u \) a large element of \( V_0 \). Write \( u = \lambda + \epsilon \) with \( \lambda \in M_0 \) and \( \epsilon \) in some fundamental domain. Then for any \( v \in V \) we have

\[
|\theta(v + u)| = |\theta(v + \epsilon)|
\]

since \( H(\lambda, -) = 0 \). It follows that \( u \mapsto \theta(v + u) \) is a bounded holomorphic function on \( V_0 \), and therefore constant. Thus \( \theta \) factors through \( V/V_0 \). In particular, \( L(H, \alpha) \) is not ample.

Now suppose that \( H(w, w) < 0 \) for some \( w \in V \). Let \( t \) be a large complex number and write \( tw = \lambda + \epsilon \), similar to the above. Then

\[
|\theta(v + tw)| = |\theta(v + \epsilon)|e^{\pi \text{Re}(H(v + \epsilon, \lambda)) + \pi H(\lambda, \lambda)/2}.
\]

The quantity \( H(\lambda, \lambda) \) is dominant, and very negative. We thus see that \( |\theta(v + tw)| \to 0 \) as \( |t| \to \infty \), which implies \( \theta(v + tw) \) is 0 as a function of \( t \). Thus \( \theta(v) = 0 \) for all \( v \), and so 0 is the only \( \theta \)-function.

We have thus shown that if \( H \) is not positive definite then \( L(H, \alpha) \) is not ample. The converse holds as well:
Theorem 17 (Lefschetz). The bundle $L(H, \alpha)$ is ample if and only if $H$ is positive definite.

Some remarks:

- This theorem shows that $X$ is a projective variety is and only if there exists a positive definite Riemann form on $V$.
- In fact, one can show that if $X$ is algebraic then it is necessarily projective, and so $X$ is algebraic if and only if it has a positive definite Riemann form. One can show that if $H$ is positive definite then $L(H, \alpha)^{\otimes n}$ is very ample for all $n \geq 3$.
- Suppose $E$ is the elliptic curve given by $C/(1, \tau)$. Then $H(x, y) = \frac{xy}{|\text{Im}(y)|}$ is a positive definite Riemann form on $C$. This recovers the fact that all one-dimensional complex tori are algebraic.
- Most complex tori of higher dimension do not possess even a non-zero Riemann form, and so most are not algebraic.

2.5 Maps of tori

A map of complex tori $X \to Y$ is a holomorphic group homomorphism. In fact, any holomorphic map taking 0 to 0 is a group homomorphism. We write $\text{Hom}(X, Y)$ for the group of maps. An isogeny is a map of tori which is surjective and has finite kernel. The degree of the isogeny is the cardinality of the kernel.

Example 18. Multiplication-by-$n$, denoted $[n]$, is an isogeny of degree $n^{2g}$. \qed

2.6 The dual torus

Let $X = V/M$ be a complex torus. Let $\mathcal{V}^*$ be the vector space of conjugate-linear functions $V \to \mathbb{C}$, and let $M^\vee \subset \mathcal{V}^*$ be the set of such functions $f$ for which $\text{Im} f(M) \subset \mathbb{Z}$. Then $M^\vee$ is a lattice in $\mathcal{V}^*$, and we define $X^\vee = \mathcal{V}^*/M^\vee$. We call $X^\vee$ the dual torus of $X$. Note that we have a natural isomorphism $(X^\vee)^\vee = X$.

Formation of the dual torus is clearly a functor: if $f: X \to Y$ is a map of tori then there is a natural map $f^\vee: Y^\vee \to X^\vee$. If $f$ is an isogeny, then so is $f^\vee$, and they have the same degree. Even better:

Proposition 19. If $f$ is an isogeny then $\ker(f)$ and $\ker(f^\vee)$ are canonically dual (in the sense of finite abelian groups).

Proof. Write $X = V_1/M_1$ and $Y = V_2/M_2$, and let $g: V_1 \to V_2$ be the linear map inducing. Then $\ker(f) = g^{-1}(M_2)/M_1$, while $\ker(f^\vee) = (g^*)^{-1}(M_1^\vee)/M_2^\vee$. If $x \in \ker(f)$ and $y \in \ker(f^\vee)$ then $\langle g(x), y \rangle$ is a rational number (since $g(x) \in M_2$ and $y$ is in a lattice containing $M_2^\vee$ with finite index), and is well-defined up to integers. We thus have a pairing $\ker(f) \times \ker(f^\vee) \to \mathbb{Q}/\mathbb{Z}$ with $n = \deg(f)$, which puts the two groups in duality. \qed

Applying this in the case where $X = Y$ and $f = [n]$, we see that $X[n]$ and $X^\vee[n]$ are in duality. This gives us a canonical pairing $X[n] \times X^\vee[n] \to \mathbb{Z}/n\mathbb{Z} \cong \mu_n$, which is called the Weil pairing.

Proposition 20. We have a natural isomorphism of groups $X^\vee = \text{Pic}^0(X)$.

Proof. The map $\mathcal{V}^* \to \mathcal{P}^0$ which takes $f \in \mathcal{V}^*$ to the map $\lambda \mapsto e^{2\pi i \text{Im}(f(\lambda))}$ is easily seen to be a surjective homomorphism with kernel $M^\vee$. It thus descends to an isomorphism $X^\vee \to \text{Pic}^0(X)$. \qed
Let $H$ be a Riemann form on $V$. Then $v \mapsto H(V, -)$ defines an isomorphism of complex vector spaces $V \to V^*$, and carries $M$ into $M^\vee$. It thus defines a map $\phi_H : X \to X^\vee$ of complex tori. This map is an isogeny if and only if $H$ is non-degenerate. Identifying $X^\vee$ with Pic$^0(X)$, $\phi_H$ coincides with $\phi_L$, where $L = L(H, \alpha)$ for any $\alpha$. A polarization of $X$ is a map of the form $\phi_H$ (or $\phi_L$) with $H$ positive-definite (or $L$ ample). A principal polarization is a polarization of degree 1. We thus see that $X$ admits a polarization if and only if it is algebraic.