Abelian Varieties.
Lecture 5.

Elisa Lorenzo García

29th February 2016

Contents

1 Basic definitions **1**
- 1.1 Isogenies . . . 2
- 1.2 The Tate-module . . . 3
- 1.3 Tate-Honda Theorem . . . 3
- 1.4 Albert's classification . . . 4
- 1.5 The dual abelian variety . . . 4

2 Abelian Varieties over the complex numbers **4**

3 Jacobians **5**

4 Exercises **6**

The main reference for today's lecture is paper [3].

1 Basic definitions

Let us fix $k = \mathbb{F}_q$ a finite field. An abelian variety over k is a subset of some projective n-space which

1. is defined by polynomials equations on the coordinates with coefficients in k.
2. is connected, and
3. has a group law which is algebraic (in the sense that the coordinates f the product of two points are rational functions of the coordinates of the factors).

In other words, an abelian variety A/k is an algebraic projective smooth and irreducible variety endow with a group law, that is, rational maps $\times : A \times A \to A : (P, Q) \to P + Q$ and $A \to A : P \to -P$. We usually denote the trivial element by O, that moreover, can be proved to be defined over the base field k.

The first Theorem one proves is that abelian varieties are commutative, and this justifies why we denote the group law with the addition symbol.

Example 1.1. *Elliptic curves with the group law explained in last lectures, are abelian varieties of dimension* 1*. In particular, all dimension* 1 *abelian varieties are elliptic curves. The product of* n *elliptic curves* $E_1 \times ... \times E_n$ *is an abelian variety of dimension* n*.*

1.1 Isogenies

We define a homomorphism of abelian varieties as a homomorphism of varieties that preserves the group law, that is, $\phi : A \to B$ such that $\phi(P + Q) = \phi(P) + \phi(Q)$ for all $P, Q \in A$. In particular, $\phi(0_A) = 0_B$.

Definition 1.2. *A homomorphism of abelian varieties is called and isogeny if it is surjective and with finite kernel. The degree of an isogeny is the cardinality of the kernel. A degree* 1 *isogeny is an isomorphism.*

Example 1.3. *The multiplication by* n *map* $[n] : A \to A : P \to n \cdot P$ *is a degre* n^{2g} *isogeny when* $p \nmid n$*. We denote its kernel by* $A[n]$*, the* n*-torsion of the abelian variety.*

Example 1.4. *The (geometric) Frobenius endomorphism* $\pi : A \to A : (x_1, ..., x_n) \to (x_1^p, ..., x_n^p)$ *is an isogeny. The set of rational points of* A *can be written as* $A(\mathbb{F}_q) = Ker(1 - \pi)$*.*

We say that A and B are isogenous is there exists an isogeny $\phi : A \to B$; this is reasonable terminology because there is then also an isogeny from B to A. If $\deg(\phi) = n$, then $\overline{\phi} : B = A/\mathrm{Ker}(\phi) \to^{[n]} A$ is an isogeny and $\phi\overline{\phi} = \overline{\phi}\phi = [n]$.

Theorem 1.5. *Let* A *be an abelian variety. Then* $End(A)$ *is finitely generated and torsion-free, and* $End(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is a semisimple* $\mathbb{Q}$*-algebra*[1]

Note that if $\phi : A \to B$ is an isogeny, the map $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{End}(B) \otimes_{\mathbb{Z}} \mathbb{Q} : \alpha \to \phi\alpha\overline{\phi}$ is an isomorphism.

Definition 1.6. *An abelian variety is simple if it has no nontrivial abelian subvarieties.*

Theorem 1.7 (Poincaré-Weil)**.** *Every abelian variety is isogenous to the product of powers of non-isogenous simple abelian varieties.*

[1] A $\mathbb{Q}$-algebra is a $\mathbb{Q}$-vector space with a multiplication rule, and in the finite dimensional case, it is semisimple if it is a sum of simple algebras, that is, without no non-trivial two size ideals.

1.2 The Tate-module

Let l be a prime different from p. We know that $A[l^n] = \mathrm{Ker}([l^n] : A \to A)$ is isomorphic to $(\mathbb{Z}/l^n\mathbb{Z})^{2g}$[2]. The $A[l^n]$ form an inverse limit under the maps $l^m : A[l^n] \to A[l^{n-m}]$, and we fit them together to form the Tate module:

$$T_l A = \lim_{\leftarrow} A[l^n] \simeq (\mathbb{Z}_l)^{2g}.$$

Let G be the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$[3]. It acts on natural way in $V_l A = T_l A \otimes \mathbb{Q}$, and it defines the l-torsion representation

$$\rho_l : G \to \mathrm{GL}(V_l A) \simeq \mathrm{GL}_{2g}(\mathbb{Q}_l).$$

Theorem 1.8 (Weil-Tate)**.** *The map $Hom(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_l \simeq Hom_G(T_l A, T_l B)$ is an isomorphism.*

We denote by f_A the characteristic polynomial of the image of the Forbenius endomorphism by ρ_l (it does not depend on the prime l). Note that

$$\#A(\mathbb{F}_q) = \deg(\pi_A - 1) = f_A(1) = \prod(1 - \alpha_i).$$

Theorem 1.9. *Let A and B be abelian varieties over a finite field k. The following are equivalent:*

1. *A and B are isogenous.*
2. *$V_l A$ and $V_l B$ are G-isomorphic for some l.*
3. *$f_A = f_B$.*
4. *The zeta function of A and B are the same.*
5. *For each extension k' of k, A and B have the number of points over k'.*

1.3 Tate-Honda Theorem

We call an integer π a Weil-number if it satisfies that it is algebraic integer whose conjugates have all norm $q^{1/2}$.

Theorem 1.10 (Tate-Honda)**.** *Let k be a finite field. Then there is a one-to-one correspondence between*

$$\{\textit{Isogeny classes of simple abelian varieties over } k\}$$

and

$$\{\textit{Conjugacy classes of Weil numbers for } q = \#k\}.$$

We will not prove this Theorem, but we will just mention that the idea behind the proof is constructing abelian varieties with complex multiplication over the p-adic fields and reduce them modulo p.

[2] If $l = p$, then $A[p] \simeq (\mathbb{Z}_p)^r$ for some $0 \le r \le g$, but we will not discuss this today.

[3] which is topologically generated by the (arithmetic) Frobenius endomorphism.

1.4 Albert's classification

Theorem 1.11. *Let A be a simple abelian variety over the field k with q elements. Then*

1. *$f_A = m_A^e$ for some integer e and some irreducible monic polynomial m_A with integer coefficients.*
2. *$E = End(A) \otimes \mathbb{Q}$ is a division algebra whose center if $\Phi = \mathbb{Q}(\pi_A)$.*
3. *$| E : \mathbb{Q} | = e^2 | \Phi : \mathbb{Q} |$, and $2dim(A) = e | \Phi : \mathbb{Q} |$.*
4. *All roots of f_A has absolute value $q^{1/2}$.*

Definition 1.12. *We say that A has complex multiplication if there exist a complex multiplication field (degree 2 extension of a totally real field) K of degree $2g$ such that $K \hookrightarrow End(A) \otimes \mathbb{Q}$.*

Example 1.13. *The elliptic curve $E : y^2 = x^3 - x$ has complex multiplication by $\mathbb{Q}(i)$, the extra endomorphism is given by $(x, y) \to (-x, iy)$.*

1.5 The dual abelian variety

Given an abelian variety A, we define its dual $A^\vee$ by $\mathrm{Pic}_0(A) := \mathrm{Div}_0(A)/Princ(A)$ (quotient of degree 0 divisors by the principal ones), it is again an abelian variety and $(A^\vee)^\vee \simeq A$.

A polarization is an isogeny $\lambda : A \to A^\vee$. We say that a polarization is principal if it has degree 1, that is, if it is an isomorphism.

All the elliptic curves are naturally endowed with a principal polarization since $E \simeq E^\vee$. Such natural polarization is $E \to E^\vee \simeq \mathrm{Div}_0(E)/\sim : P \to P - 0$. In general, divisors of degree zero of genus g hyperelliptic[4] curves can be written as $(P_1 + ... + P_g - g \cdot 0)$.

2 Abelian Varieties over the complex numbers

The main reference for this subsection is [1]. In the classical sense $k = \mathbb{C}$ the structure of abelian varieties is fairly well understood: they are all of the form $\mathbb{C}^g/\Lambda$ where Λ is a certain kind of lattice in $\mathbb{C}^g$. These lattice are basic to the classical treatment of the subject. They unfortunately disappear in characteristic $p > 0$. The Tate-module will play this role.

A complex torus $T = \mathbb{C}^g/\Lambda$ is not always an abelian variety, since it is an analytical variety, to make it a projective algebraic variety, we need an embedding $\iota : \mathbb{C}^g/\Lambda \hookrightarrow \mathbb{P}^d$ for some d. It is well-known that such an embedding exists if and only if there exists a polarization $\lambda : T \to T^\vee$.

Theorem 2.1 (Lefschezt)**.** *A polarization in a complex torus $\mathbb{C}^g/\Lambda$ is given by positive definite form $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ such that $H(\Lambda \times \Lambda) \subseteq \mathbb{Z}$. Or equivalently, by an alternate $\mathbb{Z}$-bilinear form $Im(H) = E : \Lambda \times \Lambda \to \mathbb{Z}$ such that the extension $E \otimes \mathbb{R} : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ satisfies $E(ix, iy) = E(x, y)$ for all $x, y \in \mathbb{C}^g$.*

[4] A curve is non-hyperelliptic if the canonical divisor is an embedding, otherwise it is a $2 : 1$ map, the curve is called hyperelliptic and has a (maybe singular) model $y^2 = f(x)$. The genus $g = \lfloor \frac{d-1}{2} \rfloor$, where $\deg(f) = d$.

Example 2.2. *As a complex torus, the natural polarization for the elliptic curve* $\mathbb{C}/\mathbb{Z}+\tau\mathbb{Z}$ *is given by* $H : \mathbb{C}\times\mathbb{C} \to \mathbb{C} : (1,1) \to 1/Im(\tau)$.

Example 2.3. *Let* C/k *be a smooth genus* g *curve. Fix a basis* $\omega_1, ..., \omega_g$ *of* $\Omega^1(C)$ *and a symplectic basis of paths* $\alpha_1, ..., \alpha_g, \beta_1, ..., \beta_g$ *in* $H_1(C, \mathbb{Z})$. *The lattice* Λ *generated by* $a_i = (\int_{\alpha_i}\omega_1, ..., \int_{\alpha_i}\omega_g)$ *and* $b_i = (\int_{\beta_i}\omega_1, ..., \int_{\beta_i}\omega_g)$ *in* $\mathbb{C}^g$ *together with the (principal) polarization given by the symplectic basis define an abelian variety.*

CONSTRUCTION OF ABELIAN VARIETIES WITH CM BY AN ORDER

3 Jacobians

For this section, we use reference [2].

We will see how to attach an abelian variety to a curve $C/\mathbb{F}_q$. We will assume that there exist a rational point $P_0 \in C(\mathbb{F}_q)$[5], then the jacobian $\mathrm{Jac}(C) := \mathrm{Div}_0(C)$ and there is a rational inclusion $C \hookrightarrow \mathrm{Jac}(C) : P \to (P - P_0)$. Moreover, there is a natural polarization $\lambda : \mathrm{Jac}(C) \to \mathrm{Jac}(C)^\vee$ given by the curve C and the previous inclusion.

Remark 3.1. *In the case* $k = \mathbb{C}$, *the abelian variety defined in example 2.3 coincides with the definition given here of jacobian of a curve.*

Remark 3.2. *The polynomial* f_A *has degree* $2g$ *and corresponds to the numerator of the zeta function of the curve* C.

Theorem 3.3 (Torelli)**.** *Let* C_i *be smooth curves with jacobian* (J_i, λ_i) *for* $i \in \{1, 2\}$. *Given* $\phi : J_2 \to J_1$ *an isomorphism of polarized abelian varieties (that is,* $\lambda_2 = \phi^\vee\lambda_1\phi$*), there exist an unique isomorphism* $\alpha : C_1 \to C_2$ *such that*

1. $\alpha^* = \phi$ *if* C_i *are hyperelliptic,*
2. $\alpha^* = \pm\phi$ *if* C_i *are non-hyperelliptic.*

A Jacobian is always a principal polarized abelian variety. The Schottky problem ask for the reciprocal question. Given a (irreducible) principal polarized dimension g abelian variety, when it is the jacobian of a genus g curve? For genus 1, 2 and 3, the answer is always. For higher genus, this is not true anymore.

A usefull construction that will be used in the sequel is the following: given a morphism of curves $\phi : C_1 \to C_2$, we obtain an induced morphism between the jacobian varieties $\phi* : J(C_2) \to J(C_1)$.

[5]If there is not such rational point the construction is slightly more complicated, so we skip this case and we refer the interested reader to [2]

4 Exercises

Exercise 4.1. *List all the possibilities for End(A) using Albert's classification (Theorem 1.11) for an abelian variety of dimension $g = 1$ and $g = 2$. Check in which cases the abelian variety has complex multiplication.*

Exercise 4.2. *Classify the Weil-numbers defined by polynomials of degree 2 and 4.*

Exercise 4.3. *As a reminder of the things learned in Lecture 1, prove the statement about the genus of a hyperelliptic curve in the footnote in subsection 1.5.*

Exercise 4.4. *Check explicitly example 2.2.*

Exercise 4.5. *Use the construction at the end of section 3 to compute the isogeny class of the jacobian of the genus 2 curve $y^2 = x^6 + 1$.*

References

[1] C. Birkenhake, H. Lange, *Complex abelian varieties*. Second edition. Grundlehren der Mathematischen Wissenschaften, Fundamental Principles of Mathematical Sciences, 302. Springer-Verlag, Berlin, 2004.

[2] J. S. Milne, *Abelian Varieties*, notes available at http://www.jmilne.org/math/CourseNotes/AV.pdf

[3] W. C. Waterhouse, J. S. Milne, *Abelian varieties over finite fields*, Proc. Sympos. pure math. Vol. XX, 1969 Number Theory Institute (Stony Brook), AMS 1971, pp. 53-64.