Abelian Varieties - The Basics

Travis Scholl

June 17, 2015

Abstract

These are my summary notes from the first two sections from Milne's notes [Mil08] on Abelian varieties.

1 Definition

The goal of this section is to motivate the definition of an abelian variety. The main example of a variety with the structure of an abelian group is an elliptic curve. This is the kind of object we want to generalize. First, we recall some of the various definitions of elliptic curves.

Definition 1.1 (From [DS07, Ch. 1.3-1.4])**.** An *elliptic curve* over $\mathbb{C}$ is the complex tori $\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}$ where Λ a lattice (a rank 2 $\mathbb{Z}$-submodule such that $\mathbb{R}\Lambda = \mathbb{C}$).

Definition 1.2 (From [Sil09, Ch. III.3])**.** An *elliptic curve* over a field k is a nonsingular projective curve E of genus 1 with a specified point $\mathcal{O} \in E(k)$.

Definition 1.3 (From [LE06, Defn. 6.1.25])**.** An *elliptic curve* is a smooth projective curve E over k isomorphic to a closed subvariety of $\mathbb{P}^2_k$ defined by a polynomial (homogenized) of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

together with the specified point $\mathcal{O} = (0 : 1 : 0)$.

Definition 1.4 (From [Mil08, Pg. 1])**.** An *elliptic curve* is a nonsingular projective curve together with a group structure defined by regular maps.

The first three definitions are very standard and you probably have seen. However, the fourth one may be slightly new.

Proposition 1.5. *The previous definitions of an elliptic curve are all the same.*

Proof. A sketch of this proof is in [Mil08, Pg. 1], [Mil06, Ch. II], and for the complex case [**?**, Ch. 1.3] is very readable. We will focus on the less standard directions.

(4) $\Rightarrow$ (2) Let E be a nonsingular projective curve over a field k with a group structure defined by regular maps. We need to show the genus g of E is 1.

Consider the sheaf of differentials $\Omega_E = \Omega_{E/k}$. This is locally free of rank one by [Har77, Thm. II.8.15] (here we are using[1] non-singular and projective).

[1]Here we are using the assumption that E is nonsingular, and projective to get irreducible, separated, and finite type. We may assume $k = \overline{k}$ for this because it's enough to show something is invertible after a faithfully flat base change.

By Lemma 1.6 $\Omega_E \cong \pi^* e^* \Omega_E$ where $\pi : E \to k$ is the structure map and $e : k \to E$ is the identity element in the group structure. But $e^*\Omega_E$ is free since is a locally free sheaf on k, so it follows that it's pull back $\pi^*(e^*\Omega_E)$ is free and hence Ω_E is free of rank 1. Hence

$$g := \dim \Gamma(\Omega_E, E) = \dim \Gamma(\mathcal{O}_E, E) = 1$$

The last equality follows since E is projective.

(2) $\Rightarrow$ (4) (See also [Sil09, Ch. III.3]) Let E be a non-singular projective curve of genus 1 with a specified point $\mathcal{O} \in E(k)$. We need to define a group structure on E defined by regular maps. Let $\mathrm{Pic}^0(E)$ be the quotient of degree zero divisors by principle divisors. Consider the map

$$\kappa : E(k) \to \mathrm{Pic}^0(E) \quad \text{defined by} \quad P \mapsto [P] - [\mathcal{O}]$$

Recall that the Riemann-Roch theorem says $l(D) - l(K_E - D) = \deg D - g + 1 = \deg D$ where K_E is a canonical divisor on E. By hypothesis on E, we have $g = 1$ and it follows that $\deg K_E = 0$ and $l(K_E) = 1$ (in fact, it turns out on an elliptic curve that $K_E \sim 0$).

If $P \neq \mathcal{O}$ and $P \mapsto 0$ then $[P] \sim [\mathcal{O}]$. But this implies $E \approx \mathbb{P}^1$ by a Hartshorne exercise or Silverman (specifically [Sil09, Ex. II.2.5]) which contradicts the genus of E being 1. Therefore the map κ is injective.

Let $D \in \mathrm{Div}^0(E)$. We need to show there is some P such that $[P] - [\mathcal{O}] \sim [D]$. Note $\deg(D+\mathcal{O}) = 1$ so by Riemann-Roch $l(D+\mathcal{O}) - l(K_E - (D+\mathcal{O})) = 1$. But $\deg(K_E - (D+\mathcal{O})) = -1$ so $l(K_E - (D+\mathcal{O})) = 0$ and therefore $l(D+\mathcal{O}) = 1$. Hence there is some non-zero $f \in K(E)$ such that $\mathrm{Div}\, f \geqslant -D - \mathcal{O}$. But $\deg(\mathrm{Div}\, f) = 0$ and $\deg(-D - \mathcal{O}) = -1$. It follows that $\mathrm{Div}\, f = -D - \mathcal{O} + P$ for some $P \in E(k)$. This is because $\mathrm{Div}\, f + D + \mathcal{O}$ is effective and degree 1. Therefore the map κ is surjective.

Now we can define the group structure on E via κ. It turns out the group operations are rational functions. One way to see this is to identify the operation with the usual chord and tangent formulas.

$\square$

Lemma 1.6. [2] *Let G be a group scheme over S with structure map $\pi : G \to S$ and identity $e : S \to G$. Then there is an isomorphism*

$$\Omega_G \cong \pi^* e^* \Omega_G$$

Proof. Let $G \times G/G$ represent $G \times G$ as a G scheme with structure map p_2. Define $\tau : G \times G \to G \times G$ by (m, p_2). That is, we define τ by the diagram

$$\begin{tikzcd}
G \times G \arrow[dr, dotted, "\tau"] \arrow[drr, bend left, "p_2"] \arrow[ddr, bend right, "m"'] & & \\
& G \times G \arrow[r, "p_2"] \arrow[d, "p_1"] & G \arrow[d] \\
& G \arrow[r] & S
\end{tikzcd}$$

[2]See http://www.math.ru.nl/~bmoonen/BookAV/BasGrSch.pdf

Note that τ is an automorphism of $G \times G$ as a G-scheme. This is easy to see since on the functor of points τ is the map $(a, b) \mapsto (ab, b)$.

Now the sheaf of differentials plays well with base change (see [LE06, Prop. 6.1.24a]). It follows that $\tau^*\Omega_{G\times G/G} \cong \Omega_{G\times G/G}$ (by writing a base changing $G \times G/G$ to itself along the identity and replacing the top map with τ, this will still be cartesian). It also follows that $\Omega_{G\times G/G} \cong p_1^*\Omega_G$ since this is a base change of G/S to $G \times G/G$. Putting these facts together gives

$$\Omega_{G\times G/G} \cong \tau^*\Omega_{G\times G/G} \cong \tau^* p_1^*\Omega_G = (p_1 \circ \tau)^*\Omega_G = m^*\Omega_G.$$

Next define $\phi : G \to G \times G$ given by $(e \circ \pi, id)$. That is, we define ϕ by the diagram

$$\begin{tikzcd}
G \arrow[d, "\pi"'] \arrow[dr, dotted, "\phi"] \arrow[drr, bend left, "id"] & & \\
S \arrow[dr, "e"'] & G \times G \arrow[r, "p_2"] \arrow[d, "p_1"] & G \arrow[d] \\
& G \arrow[r] & S
\end{tikzcd}$$

Now on one hand since $m \circ \phi = id$ we have

$$\phi^*\Omega_{G\times G/G} \cong \phi^* m^*\Omega_G \cong \Omega_G$$

while on the other hand

$$\phi^*\Omega_{G\times G/G} \cong \phi^* p_1^*\Omega_G \cong \pi^* e^*\Omega_G.$$

□

So which definition do we want to use? The one which generalizes the easiest is Definition 1.4. So we will use this.

Definition 1.7. An *abelian variety* is a connected complete group variety.

Here a "group variety" is a group object in the category of varieties. All our varieties will be over a field k.

Remark 1.8. Here *complete* means universally closed, i.e. V is complete if for any other variety W the map $V \times_k W \to W$ is closed. In this setting you can interchange "complete" with "proper" since varieties by our definition will be separated and finite type over k.

2 Properties

Using this simple definition we get some easy consequences for free.

Proposition 2.1. *Abelian varieties are non-singular.*

Sketch. As a variety, it has an open non-singular locus. This can be translated around via the group operation. □

Proposition 2.2. *Abelian varieties are irreducible.*

Sketch. Milne's definition of non-singular means it lies in a single irreducible component. □

Proposition 2.3. *Abelian varieties are geometrically connected.*

Sketch. See [LE06, Ex. 3.2.11a] which says if X/k is connected and finite type, then X is geometrically connected. The sketch is that a connected component $C_{\overline{k}}$ of $X_{\overline{k}}$. Because everything is finite type it will be defined over a finite Galois extension k'. Note $\overline{k}/k'$ is faithfully flat so $C_{k'}$ is a connected component of $X_{k'}$.

Now the Galois group $\mathrm{Gal}(k'/k)$ acts transitively on the connected components of $X_{k'}$ but it also fixes $X_{k'}(k)$. Since this is non-empty, there is only one connected component. □

There is another very important property of abelian varieties.

Lemma 2.4 (Rigidity Theorem)**.** *Suppose X is complete and $X \times Y$ is geometrically irreducible. Let $\alpha : X \times Y \to Z$ be a morphism and suppose*

$$\alpha(\{x_0\} \times Y) = \{z_0\} = \alpha(X \times \{y_0\})$$

Then $\alpha(X \times Y) = \{z_0\}$.

Sketch. By the hypothesis on X, $\pi : X \times Y \to Y$ is closed. Recall that the image of a complete (or proper over k) and connected variety into an affine variety is a point.

Let U be an affine neighborhood of z_0. From the first fact, it follows $W = \pi \circ \alpha^{-1}(Z \backslash U)$ is closed in Y. This set is non-empty because $y_0 \notin W$ (as every tuple with y_0 is contained in U). Now for any $y \in Y \backslash W$ we have $X \approx X \times \{y\} \to Z$ maps to a point by the second fact. Since (x_0, y) is in this set, this point is z_0. Hence α is constant on $X \times (Y \backslash W)$. This is open, and hence dense in $X \times Y$. Since Z is separated, α agrees with this constant map on all of $X \times Y$. □

Proposition 2.5. *Every morphism between abelian varieties can be factored into a group homomorphism and a translation.*

Proof. Let $\varphi : X \to Y$ be a morphism of abelian varieties. Up to a translation we may assume it sends $0 \mapsto 0$.

Let $m_X : X \times X \to X$ and $m_Y : Y \times Y \to Y$ be the respective multiplication maps. Consider the difference $\varphi \circ m_X - m_Y \circ \varphi \times \varphi$. It's easy to see this takes $\{0\} \times X \to \{0\}$ and $X \times \{0\} \to \{0\}$. So by the Rigidity lemma, this difference is the constant map which means exactly that this map is a homomorphism. □

Proposition 2.6. *Abelian varieties are abelian.*

Proof. The inverse map is a morphism which sends $0 \mapsto 0$ so by the previous proposition, it's a group homomorphism. □

The last fact is somewhat remarkable, and the proof will be sketched next week.

Proposition 2.7. *Abelian varieties are projective.*

Proof. Wait for Bharath's talk. □

3 Analytic Abelian Varieties

Let A be an abelian variety over $\mathbb{C}$. If you are unfamiliar with the analytification functor, note that A is projective so it admits a closed embedding into $\mathbb{P}^n_{\mathbb{C}}$. After identifying $\mathbb{P}^n(\mathbb{C})$ as a complex manifold in the usual way we can give $A(\mathbb{C})$ a complex manifold structure via this embedding. It turns out A is a compact connected complex manifold. In fact, $A(\mathbb{C})$ has a rather simple complex structure.

Theorem 3.1. *$A(\mathbb{C})$ is a complex torus.*

Proof.

Exponential Map: Let G be any real Lie group. Recall the exponential map which sends the tangent space $\exp : T_eG \to G$ via one-parameter subgroups. That is, v maps to the point given by the end point of a path through e with direction v and flows for $|v|$ time. The main fact that we will use is that this map is smooth and the derivative at 0 is basically the identity map $T_eG \to T_eG$, so in particular it is a local diffeomorphism.

Surjective: All the theory extends to the complex case. So there exists a group homomorphism

$$\exp T_0A(\mathbb{C}) \to A(\mathbb{C})$$

To prove the theorem note that this map is a local homeomorphism near 0. Because exp is also a group homomorphism, the image H is a connected subgroup of $A(\mathbb{C})$ containing a neighborhood of the identity. Translating this neighborhood around via elements of H show that H is open in $A(\mathbb{C})$. Because H is open, so are it's cosets. Which implies H is closed. By hypothesis $A(\mathbb{C})$ is connected so exp is surjective.

Kernel: Since exp is a local isomorphism, 0 is a isolated point in ker. Therefore the ker is a discrete subgroup of a $2r$-dimensional real vector space. An argument from number theory shows this implies ker is a lattice, that is $\ker \approx \mathbb{Z}e_1 + \cdots \mathbb{Z}e_r$ for some vectors e_i. Moreover, the compactness of $A(\mathbb{C})$ implies ker is a full lattice so that $r = 2g$.

□

Warning 3.2. The converse to Theorem 3.1 is *not* true in general. That is, not every $\mathbb{C}^g/L$ is isomorphic to the analytification of an abelian variety. However, when $g = 1$ it is true as these are elliptic curves.

Example 3.3 (See [SBIfASP08, Pg. 104])**.** Suppose $X = \mathbb{C}^2/L$ came from some abelian variety $A(\mathbb{C})$. Note the function field of A has transcendence degree 2 over $\mathbb{C}$, so this implies $\mathbb{C}(X)$ contains non-constant meromorphic functions (these are meromorphic in two variables).

We will give an example of a lattice L such that there are no non-constant L-invariant meromorphic functions on $\mathbb{C}^2$ which by above shows that X does not come from an abelian variety.

Let L be the lattice spanned by the columns of the period matrix

$$C = \begin{pmatrix} 1 & 0 & \sqrt{-2} & \sqrt{-5} \\ 0 & 1 & \sqrt{-3} & \sqrt{-7} \end{pmatrix}.$$

Note these vectors are $\mathbb{R}$-linearly independent so they do in fact generate a full lattice in $\mathbb{C}^2$.

We will prove by contradiction that the transcendence degree s of $\mathbb{C}(X)/\mathbb{C}$ must be 0.

$(s = 2):$ Suppose that $\mathbb{C}(X)$ has transcendence degree 2. A consequence of the hypothesis is that there exists a matrix A made up of integral multiples of πi such that 1) A is non-singular, 2) $CA^{-1}C^T = 0$, and 3) $\overline{C}A^{-1}C^T < 0$ (i.e. negative definite).

Let $B = \pi i A^{-1}$ so that B has rational values. From the second condition, looking at the value of CBC^T in the first row and second column we find

$$\begin{pmatrix} 1 & 0 & \sqrt{-2} & \sqrt{-5} \end{pmatrix} B \begin{pmatrix} 1 \\ 0 \\ \sqrt{-3} \\ \sqrt{-7} \end{pmatrix} = b_{12} + b_{13}\sqrt{-3} + b_{14}\sqrt{-7} - b_{23}\sqrt{-2} - b_{24}\sqrt{-5} + b_{34}(\sqrt{14} - \sqrt{15}) = 0$$

But $b_{ij} \in \mathbb{Q}$ so this implies that $B = 0$ and hence contradicts (1).

$(s = 1):$ Suppose that $\mathbb{C}(X)$ has transcendence degree 1. One can show that this implies up to a linear transformation all functions are dependent on z_1 only. This linear transformation basically replaces $z = (z_1, z_2)$ with $Q^{-1}z$ where

$$Q = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

After making this substitution, the new period lattice is given by projecting QC onto the first copy of $\mathbb{C}$. This gives us

$$C_1 = \left(\alpha, \beta, \alpha\sqrt{-2} + \beta\sqrt{-3}, \alpha\sqrt{-5} + \beta\sqrt{-7}\right)$$

If this is a period matrix, it must generate a two dimensional lattice. Let ω_1, ω_2 be a basis for this lattice so that all the above points are integer combinations of the ω_i. In particular

$$\begin{aligned} \alpha &= p_1\omega_1 + p_2\omega_2 \\ \beta &= q_1\omega_1 + q_2\omega_2 \\ \alpha\sqrt{-2} + \beta\sqrt{-3} &= r_1\omega_1 + r_2\omega_2 \\ \alpha\sqrt{-5} + \beta\sqrt{-7} &= s_1\omega_1 + s_2\omega_2 \end{aligned}$$

Some slick linear algebra using that $1, \sqrt{-2}, \sqrt{-3}, \sqrt{-5}, \sqrt{-7}$ are all $\mathbb{Q}$-independent shows that every 2-row minor of

$$\begin{pmatrix} p_1 & p_2 \\ q_1 & q_2 \\ r_1 & r_2 \\ s_1 & s_2 \end{pmatrix}$$

has determinate 0 which contracts that two of the complex numbers from C_1 must be independent over $\mathbb{R}$.

4 Riemann Forms

Even though not every complex tori is an abelian variety, there is a necessary and sufficient condition to test whether it is. First some linear algebra. Let V be a complex vector space.

Lemma 4.1. *There is a bijection between real-valued (i.e. view V as a real vector space) alternating bilinear forms $E : V \times V \to \mathbb{R}$ and Hermitian forms $H : V \times \overline{V} \to \mathbb{R}$. The correspondence is given by*

$$\begin{aligned} H(v,w) &= E(iv,w) + iE(v,w) \\ E(v,w) &= \operatorname{Im} H(v,w) \end{aligned}$$

Proof. Note that alternating and skew-symmetric are equivalent in characteristic 0.

($\Rightarrow$) : Suppose E is a real-valued alternating bilinear form on V. Let J be the $\mathbb{R}$-linear map on V given by multiplication by i. Note that J is skew-symmetric. If we choose a basis $z_1, \dots, z_n$ for V over $\mathbb{C}$ then $x_1, y_1, \dots, x_n, y_n$ is a basis for V over $\mathbb{R}$. In this basis multiplication by i is a block matrix with blocks of the form

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Note that $(JE)^T = E^T J^T = (-E)(-J) = EJ$. Define H as above. It' clear H is $\mathbb{R}$-linear so it's enough to show what happens when we scale by i in each slot. Plugging into the formula and equating real and imaginary parts, it's enough to show

$$E(iv, iw) = -E(v,w) \quad \text{and} \quad E(v, iw) = -E(iv, w)$$

These follow from a quick basis calculation

$$E(iv,iw) = (Jv)^T EJw = v^T J^T EJw = v^T JJ^T Ew = v^T(-1)Ew = -E(v,w)$$

and

$$E(v,iw) = v^T EJw = v^T JEw = v^T(-J)^T Ew = -(Jv)^T Ew = -E(iv,w).$$

($\Leftarrow$) : Suppose H is a Hermitian form. Then it's imaginary component is clearly a skew-symmetric as $H(v,w) = \overline{H(w,v)}$.

□

Definition 4.2. Let L be a lattice in $\mathbb{C}^g$, a *Riemann form* is an alternating bilinear form $E : L \times L \to \mathbb{Z}$ such that

(a) $E_{\mathbb{R}}(iv, iw) = E_{\mathbb{R}}(v,w)$

(b) The associated Hermitian form is positive definite.

Definition 4.3. Let $X = \mathbb{C}^g/L$ be a complex torus. Then X is *polarizable* if it admits a Riemann form.

Theorem 4.4. *A complex torus X is of the form $A(\mathbb{C})$ if and only if it is polarizable.*

The proof is sketched in [Mil08, Thm. 2.8].

Example 4.5. Let X be the complex torus $\mathbb{C}/\mathbb{Z} + i\mathbb{Z}$, or better known as $y^2 = x^3 - x$. This has a Riemann form given by

$$E(x + iy, x' + iy') = x'y - xy'$$

It's easy to check this is an alternating bilinear form which takes $L \times L \to \mathbb{Z}$.

Now notice

$$E_{\mathbb{R}}(i(x+iy), i(x'+iy')) = (-y')x - (-y)x' = x'y - xy' = E(x+iy, x'+iy')$$

so it satisfies the first property of being a Rieman form.

Moreover, the associated Hermitian form is

$$H(z, z') = z\overline{z}'$$

which is clearly positive definite.

Remark 4.6. Let L be a lattice. Then an integer-valued alternating bilinear form on L is the same as a linear map $\bigwedge^2 L \to \mathbb{Z}$. If L has rank 2, i.e. the abelian variety has genus 1, then $\bigwedge^2 L$ has rank 1 which means $\bigwedge^2 L \approx \mathbb{Z}$. So in particular, all integer-valued alternating bilinear forms on L are multiples of a generating form defined up to a sign.

References

[DS07] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms (Graduate Texts in Mathematics, Vol. 228)*. Springer, 1st edition, 4 2007.

[Har77] R. Hartshorne. *Algebraic Geometry*. Encyclopaedia of mathematical sciences. Springer, 1977.

[LE06] Q. Liu and R.Q. Erne. *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics. OUP Oxford, 2006.

[Mil06] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[SBIfASP08] C.L. Siegel, P.T. Bateman, and N.J.) Institute for Advanced Study (Princeton. *Analytic Functions of Several Complex Variables: Lectures Delivered at the Institute for Advanced Study, 1948-1949*. Kendrick Press, 2008.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2009.

Travis Scholl
Department of Mathematics, University of Washington, Seattle WA 98195
email: `tscholl2@uw.edu`