Abelian Varieties - The Basics

Travis Scholl

June 23, 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 a group structure is an elliptic curve. 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 $\mathbb{C}/\Lambda = \{z + \Lambda\colon z \in \mathbb{C}\}$ 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 smooth 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 [DS07, Ch. 1.3] is very readable. We will focus on one equivalence.

(4) $\Rightarrow$ (2) Let E be a smooth 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 [LE06, Prop. 6.2.2].

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 on E. But $e^*\Omega_E$ is free since is a locally free sheaf on k, so the pull back $\pi^*(e^*\Omega_E)$ is free and hence Ω_E is free of rank 1.

This implies that the canonical divisor has degree 0, which by Riemann-Roch shows $g = 1$. Alternatively,

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

The last equality follows since E is projective, see [Har77, Thm. I.3.4].

(2) $\Rightarrow$ (4) (See also [Sil09, Ch. III.3]) Let E be a nonsingular 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 $l(K_E) = 1$ (actually 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 [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 regular functions. One way to see this is to identify the operation with the usual chord and tangent formulas.

□

Lemma 1.6. [1] *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

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

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 $(a, b) \mapsto (ab, b)$.

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

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. They will be for sure finite type and separated. They should probably be geometrically reduced.

Warning 1.8. We need varieties to be *geometrically reduced* if we want abelian varieties to be smooth. For example consider the group scheme μ_p given by $\mathbb{F}_p[x]/(x^p - 1)$ which picks out pth roots. This is finite type, irreducible (the only prime ideal of $\mathbb{F}_p[x]$ containing $(x-1)^p$ is $(x-1)$) and separated (stacks project Lemma 38.7.3 or exercise in AWS notes). However, it is not smooth since $\frac{d}{dx}(x^p - 1) = 0$. This is because it is not a separable extension of fields. Separable extension of fields is equivalent to geometrically reduced, see Stacks project, specifically see:

Lemma 32.20.7 `http://stacks.math.columbia.edu/tag/056V`]

Let X be a scheme over a field k. If X is locally of finite type and geometrically reduced over k then X contains a dense open which is smooth over k.

Remark 1.9. 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 should be smooth.*

Sketch. First base change to $\overline{k}$. As a variety (see Warning 1.8), it should have a non-empty open smooth locus. It can be translated around via the group operation. □

Warning 2.2. Be careful with definitions. Some authors use "*nonsingular*" to mean "*smooth*". A definition of abelian variety should include smooth. The previous proposition fails if variety's can have an empty nonsingular locus. For example, a purely inseparable field extension has empty nonsingular locus. Also see Warning 1.8. Smooth and nonsingular are different notions. Smooth (flat and geometrically regular fibers) is relative and nonsingular (locally noetherian and regular) is intrinsic.

Proposition 2.3. *Abelian varieties are irreducible.*

Sketch. Connected and smooth implies irreducible, though this is not necessarily obvious or trivial. To show this, first show smooth implies regular (see [LE06, 4.3.32]) and then show regular local rings are domains. Finally, recall a point in two distinct irreducible components has non-trivial zero divisors in its local ring. □

Proposition 2.4. *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 the identity point, so (by the orbit stabilizer theorem) there is only one connected component. □

Proposition 2.5. *Abelian varieties are rigid.*

What we mean is that abelian varieties satisfy the hypothesis of the following.

Lemma 2.6 (Rigidity Lemma)**.** *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. It's enough to prove in the case $k = \overline{k}$.

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. Note that $W = \pi \circ \alpha^{-1}(Z \backslash U)$ 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 2.7. *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 2.8. *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 2.9. *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. Moreover we have the following.

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. One can show this implies ker is a lattice (using the pigeonhole principle), 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 $r = 2g$.

$\square$

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. For examples see [SBIfASP08, Pg. 104] or [Sha12, Ch. VIII.1.4-5].

Theorem 3.3 (Poincare complete irreducibility theorem)**.** *Let X, Y be abelian varieties and a map $\varphi : X \to Y$ a surjective homomorphism. Then there exists an abelian subvariety $Z \subseteq X$ such that $\dim Z = \dim Y$ and $\varphi|_Z : Z \to Y$ is surjective.*

Example 3.4 (See [Sha12, Ch. VIII.1.5, Pg. 162])**.** Consider the complex tori given by $A = \mathbb{C}^2/L$ where L has as a basis

$$L = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} i \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right\rangle.$$

Let $B = \mathbb{C}/L'$ where L' has as a basis $\langle 1, i \rangle$. Note $\varphi : X \to Y$ induced by $p_2 : (z_1, z_2) \mapsto z_2$ is a surjective holomorphic group homomorphism $A \to B$. Suppose A is algebraic (i.e. the analytification of some abelian variety). We will derive a contradiction from Theorem 3.3 (note B is already algebraic as it is an elliptic curve).

Let C be any 1-dimensional sub-abelian variety of A. Write $M \subseteq \mathbb{C}^2$ for the inverse image of C under the map $\mathbb{C}^2 \to \mathbb{C}^2/L$. Note M is a closed subgroup of $\mathbb{C}^2$. One can show that M must be of the form $\mathbb{R}^s \oplus \mathbb{Z}^t$ (similar to the proof of Theorem 3.1). Since M descends to a complex 1 dimensional manifold we must have $M = \mathbb{R}e_1 + \mathbb{R}e_2 + \mathbb{Z}e_3 + \mathbb{Z}e_4$ for some $\mathbb{R}$-independent vectors $e_1, \ldots, e_4$.

Because $M \supset L$ and L has rank 4, we can assume (with some argument) that $e_1, e_2 \in L$.

As C has codimension 1 in A, C is locally cut out by a single function f. Let M^0 be the connected component of M containing 0 so in particular $M^0 = \mathbb{R}e_1 + \mathbb{R}e_2$. Because C is nonsingular and M^0 is an $\mathbb{R}$-vector subspace, one can show that f is linear and therefore $\mathbb{R}e_1 + \mathbb{R}e_2$ is a complex line, i.e. $e_2 = \lambda e_1$ for some $\lambda \in \mathbb{C}\backslash\{0\}$.

So we have $e, \lambda e \in L$ with $\lambda \in \mathbb{C}\backslash\mathbb{R}$ with $p_2(e) \neq 0$. Write

$$\begin{aligned} e &= a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} i \\ 0 \end{pmatrix} + c \begin{pmatrix} 0 \\ 1 \end{pmatrix} + d \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ \lambda e &= \lambda a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda b \begin{pmatrix} i \\ 0 \end{pmatrix} + \lambda c \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \lambda d \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= a' \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b' \begin{pmatrix} i \\ 0 \end{pmatrix} + c' \begin{pmatrix} 0 \\ 1 \end{pmatrix} + d' \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \end{aligned}$$

where all coefficients are in $\mathbb{Z}$.

Note that $p_2(\lambda e) = \lambda(c + d\beta) \in p_2(L) = \mathbb{Z}[\beta]$ and by hypothesis $c + d\beta \neq 0$ so $\lambda \in \mathbb{Q}(\beta)$.

Suppose $p_1(e) = 0$. We may assume $1, i, \alpha$ are $\mathbb{Z}$-independent by choosing α appropriately so $a = b = d = 0$. But $p_1(\lambda e) = 0$ which implies $a' = b' = d' = 0$. But then $p_1(\lambda e) = 0$ and hence $a' = b' = d' = 0$. This means we must have $\lambda c = c'$ but λ is not rational so this is a contradiction. Therefore $p_1(e) \neq 0$. So now we can do exactly the same argument, $\lambda p_1(e) = p_1(\lambda e) \in p_1(L) = \mathbb{Z}[i, \alpha]$ so $\lambda \in \mathbb{Q}(i, \alpha)$.

Now we only need to set α to be $\mathbb{Z}$-independent from i and 1. So take $\alpha = \sqrt{2}$ and $\beta = \sqrt{-3}$. Then $\lambda \in \mathbb{Q}(i, \sqrt{2}) \cap \mathbb{Q}(\sqrt{-3})$. As $\mathbb{Q}(\sqrt{-3})$ is a quadratic extension this intersection is either $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}$. But we know the subfields of $\mathbb{Q}(i, \sqrt{2})$. The only that is clearly not $\mathbb{Q}(\sqrt{-3})$ is $\mathbb{Q}(\sqrt{-2})$. But these are not the same as $\sqrt{2}$ and $\sqrt{3}$ are $\mathbb{Q}$-linearly independent.

4 Riemann Forms

Even though not every complex tori is an abelian variety, there is a necessary and sufficient condition using mostly linear algebra to test whether it is.

Lemma 4.1. *Let V be a complex vector space. There is a bijection between real-valued (i.e. view V as a real vector space) alternating*[2] *bilinear forms $E : V \times V \to \mathbb{R}$ such that $E(iv, iw) = E(w, v)$ and Hermitian forms $H : V \times \overline{V} \to \mathbb{R}$. The correspondence is given by*

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

Proof.

$(\Rightarrow)$: Suppose E is a real-valued alternating bilinear form on V such that $E(iu, iv) = E(u, v)$.

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 so that $H(iv, w) = iH(v, w)$ and $H(v, iw) = -iH(v, w)$. By equating real and imaginary parts, we see this is exactly the hypothesis on E.

$(\Leftarrow)$: 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.

Here $E_{\mathbb{R}}$ means E viewed as an $\mathbb{R}$-bilinear form on $L \otimes \mathbb{R}$.

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 positive definite.

[2] Note that alternating and skew-symmetric are equivalent in characteristic 0.

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/.

[Mil12] James S. Milne. Algebraic geometry (v5.22), 2012. 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.

[Sha12] I.R. Shafarevich. *Basic Algebraic Geometry 2: Schemes and Complex Manifolds.* Springer Berlin Heidelberg, 2012.

[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`