# Lecture 17: Abel-Jacobi Map, Elliptic Curves

Few more remarks on the analytics theory. Last time we let $X$ be a smooth compact $\mathbb{C}$-manifold of dimension 1, obtained from a normal, complete curve over $\mathbb{C}$. (In fact, any smooth compact $\mathbb{C}$-manifold of dimension 1 is obtained from an algebraic curve; note that this fails for dimension $\geq 2$). In this case, $\mathrm{Pic}^\circ(X) = \mathrm{Div}(X)/\mathrm{PDiv}(X)$. We remarked that we have a map from it to $\Gamma(\Omega^1(X))^*/H_1(X,\mathbb{Z}) = \mathbb{C}^g/\mathbb{Z}^{2g}$ (the Abel-Jacobi map).

**Theorem 1.1.** *$X$ can be reconstructed from the lattice $H_1(X,\mathbb{Z}) \subseteq \Gamma(\Omega^1)^*$.*

This can be generalized to smooth complete varieties in any dimension. Instead of degree, we consider a map $\mathrm{Div} \to H_{n-2}(X)$, and principal divisors are the preimages of 0. There is another $\mathrm{Pic}(X) \to H_{n-2}(X)$ with kernel $\mathrm{Pic}^\circ(X)$, and the theorem reads $\mathrm{Pic}^\circ(X) = \Gamma(\Omega^{n-1}(X))^*/H_1(X,\mathbb{Z})$.

**Proposition 1.** *$\mathrm{Pic}^\circ(X)$ is itself a complex variety as well as a compact abelian Lie group. In fact, one can define an algebraic group $\mathrm{Jac}(X)$ on it, such that for a curve $X$, the A-J map is algebraic.*

To formally define the Jacobian, one defines a functor it represents. More explicitly, for a variety $S$, one define a family of invertible sheaves of $X$ parametrized by $S$, which is essentially an invertible sheaf on $S \times X$, modulo the line bundles pulled back from $S$.

**Theorem 1.2.** *Let $g$ be the (geometric) genus of $X$ and assume it equals 1. Then $\mathbb{C}^g/\mathbb{Z}^{2g} = \mathbb{C}/\mathbb{Z}^2$ has dimension 1 and is therefore a curve. Fix $x_0 \in X$. The A-J map gives a map $X \to \mathrm{Pic}^\circ(X)$, where we send $x$ to $x - x_0$. Then this is an isomorphism.*

**Corollary 1.** *Every normal curve of genus 1 has a group structure (they are called the elliptic curves).*

As an example, consider $X \subseteq \mathbb{P}^2$ is the projective closure $y^2 = P(x) = x^3 + ax + b$ (char $k \neq 2,3$) (and assume no multiple roots). We'll check today that $X$ is a smooth curve by showing it's normal and irreducible.

Assume $k = \mathbb{C}$, we claim that $g = 1$, i.e. the topological Euler character is 0. Consider the map $(x,y) \mapsto x$, which extends to a morphism $X \to \mathbb{P}^1$. This is of degree 2 and has four ramification points: the roots of $P(x)$ as well as the infinity. Thinking in classical topology and choose your favorite argument, we know that $\mathrm{Eul}(X) = 2\mathrm{Eul}(\mathbb{CP}^1) - 4 = 0$.

Now let's consider how to write down the composition (group) law. To do so, we first fix the initial point $x_0 = (0:1:0)$, where we see that $\{x_0\} = X \cap \mathbb{P}^1_\infty$. The complex story suggests that we have a group law on $X$, such that for every $x, y \in X$, we have the divisor equivalence $(x +_E y) - x_0 \sim (x - x_0) + (y - x_0)$ (where $+_E$ denotes the addition using the group law), in other words, $(x +_E y) - x - y \sim -x_0$. We know that for every two lines $l, l' = \mathbb{P}^1 \subseteq \mathbb{P}^2$ we have $(l \cap X) \sim (l' \cap X)$ (we discussed this before). Now take $l' = \mathbb{P}^1_\infty$, then $(l' \cap X) = 3x_0$. Write $l \cap X = x_1 + x_2 + x_3$, then $(x_1 - x_0) + (x_2 - x_0) + (x_3 - x_0) \sim 0$ in $\mathrm{Pic}(X)$. So we should expect $x_1 +_E x_2 +_E x_3 = 0$. Now we construct the group law. For $x = (a,b) \subseteq X$, $x' = (a,-b)$, we have $x + x' + x_0 \sim 3x_0 \in \mathrm{Pic}$, so we define $x +_E x' = 0$. Now in general, define $x +_E y$ to be the 3rd point in $l \cap X$, where $l$ passes through $x'$ and $y'$. One can directly check that this is a group law that makes $X$ an abelian algebraic group.

**Remark 1.** *Over $\mathbb{C}$, $X = \mathbb{C}/\mathbb{Z}^2$ makes it clear that for all $N > 0$ we have $\{x \in X \mid Nx = 0\} \cong (\mathbb{Z}/N\mathbb{Z})^2$. This can be checked algebraically to hold for $k$ of characteristic $p \nmid N$. If $N = p$, then this group is $\mathbb{Z}/p$, or trivial if $X$ is respectively ordinary or supersingular.*

Consider $X_0 \subseteq \mathbb{A}^2$ given by $\{(x,y) \mid y^2 = P(x)\}$. If $X_0 - \{z\}$ is affine, then it corresponds to $k[X_0]_{(f)}$ where $f$ is a function in $k[X_0]$ such that $f(x) = 0 \Leftrightarrow x = z$, which is iff $(f) = Nz - Nx_0$ for some $N$ (where $x_0$ is the group law identity, which is the infinite point). For a given $N$ there are $N^2 - 1$ such $z$.

Last time we proved that if $X$ is normal irreducible complete curve, $f \in K(X)$, then it defines some $f : X \to \mathbb{P}^1$, then the divisor $(f)$ is $(f_0) - (f_\infty)$ where $\deg(f_0) = \deg(f_\infty) = \deg(f)$. We proved this modulo the following proposition, which we shall prove today:

**Proposition 2.** *A non-constant map between irreducible compact curves is finite.*

**Normalization** Let $X$ be an irreducible variety, $F = K(X)$ be the field of rational functions on $X$. Let $E/F$ be a (finite) field extension. Then build a new variety as follows:

**Proposition 3.** *There exists a variety $Y$ along with a finite map $f : Y \to X$ such that for every affine open $U \subseteq X$, $k[f^{-1}(U)] = \overline{k[U]}_E$ (the integral closure).*

If $E = F$, then $Y$ is called a renormalization of $X$. In fact, $Y$ is the unique normal variety with a finite onto map to $X$ with the fractional field being $E$. $\overline{k[U]}_E$ is finitely generated as a $k[U]$-module, or equivalently, as a ring. In other words $k[U]$ is a Nagata ring. Sketch of proof to this: using Noether normalization reduce to $X = \mathbb{A}^n$. Consider separately the case of purely inseparable and the separable extensions. For separable extension case, the bilinear form $(x, y) \mapsto \mathrm{Tr}(xy)$ on $E$ as an $F$-vector space is not degenerate, so if we pick a basis $(y_i)$ for $E/F$ which lies in $\overline{k[x_1, \ldots, x_n]}_E$, then $\overline{k[x_1, \ldots, x_n]}_E \subseteq \{e \in E \mid \mathrm{Tr}(ex_i) \in A\}$ is a finitely generated algebra for $A = k[x_1, \ldots, x_n]$. Now the assignment $U \mapsto \overline{k[U]}_E$ extends to a coherent sheaf $A$ of rings on $X$, and let $Y = \mathrm{Spec}_X(A)$.

**Corollary 2.** *Given $f : X \to Y$ where $X, Y$ are irreducible, if $X$ is normal, $f$ is finite, onto, then $X$ can be reconstructed from $Y$ and $f^{-1}(U)$ for some open $U \neq \emptyset \subseteq Y$.*

**Example 1.** *Let $X = V(x^3 - y^2)$, then the normalization of $X$ is $\mathbb{A}^1$, and the map is $t \mapsto (t^2, t^3)$.*

**Lemma 1.** *If $f : X \to Y$ is a map of irreducible curves, suppose $f$ is onto, birational, $Y$ is normal, then $f$ is an isomorphism.*

*Proof.* Let $\varphi \in K(Y)$, $\varphi$ on $f^{-1}(U) \Leftrightarrow \varphi$ is regular on $U$. If $\varphi$ is not, $\varphi^{-1}$ is regular and is 0 at some $x \in U$. Suppose $y \mapsto x$, then $\varphi$ is not regular at $y$. $\square$

**Lemma 2.** *Suppose $X \to Y$ is birational map, $X$ is complete, $Y$ is normal, then $X \cong Y$ iso.*

*Proof.* Since $f(X)$ is closed and not finite, we know $f$ must be onto. $\square$

*Proof of Proposition 2.* $X \to Y$ is a map of complete curves. We can assume $X$ is normal. Then it factors through normalization $X \to \mathrm{Nor}(Y) \to Y$. The first is isomorphism by assumption, and the second map is finite by construction. $\square$

**Tangent Space** Now let $X$ be an algebraic variety, $x \in X$. Let us define the Zariski tangent space $T_x X$. We first we note the tangent space to a smooth manifold is the fiber of the bundle of vector fields $\mathrm{Vect}(M) = \mathrm{Der}(\mathcal{C}^\infty(M))$. Each vector field $v$ gives a linear map $\delta_v : \mathrm{Fun}(M) \to \mathbb{C}$ that maps $f$ to $v \cdot f|_x$, so we see that $\delta_v(fg) = f(x)\delta_v(g) + g(x)\delta_v(f)$. This suggests the definition $T_x X \subseteq \mathrm{Hom}_k(\mathcal{O}_{X,x}, k)$ given by $\{\xi \mid \xi(fg) = f(x)\xi(g) + g(x)\xi(f)\}$. The cotangent space $T_x^* X$ is the dual $(T_x X)^*$, and we can describe it as $\mathfrak{m}_x/\mathfrak{m}_x^2$. In particular, for $X = \mathrm{Spec}(A)$, $\mathrm{Vect}(X) = \mathrm{Der}(A) = \{\delta : A \to A\ k\text{-linear} \mid \delta(fg) = \delta(f)(g) + f\delta(g)\}$.