Abelian varieties and Jacobians

November 25, 2013

1 Abelian varieties and Jacobians

An *abelian variety* A over a field K is an irreducible smooth projective group variety. In other words, A is a smooth projective variety equipped with morphisms $\mu\colon A\times A\to A$ and $i\colon A\to A$ obeying the axioms of an abelian group. In fact, if A is a group variety which is proper over a field, then A is automatically projective, and thus an abelian variety.

The first examples are elliptic curves, which are smooth projective curves E/K of genus 1 equipped with an origin $O\in E(K)$. How is this a group variety? Let us just see why $E(K)$ has a group law. If $P,Q\in E(K)$, then the divisor $D=3[O]-P-Q$ has degree 1. A calculation using the Riemann-Roch formula shows that there exists a rational function f on E with divisor $\geq -D$. We must have $\operatorname{div} f = P+Q+R-3(O)$ for some uniquely determined $R\in E(K)$, and then $P+Q+R=0$ in $E(K)$. (If E is a plane cubic, then the role of f is played by the linear form which intersects E at P, Q, and R.) Similarly, if $P\in E(K)$ then the same argument applied to $D=2[O]-P$ shows that there exists P' such that $[P]+[P']-2(O)$ is principal, and then $P'=-P$ in $E(K)$.

More to the point, let $\operatorname{Pic} E$ be the group of divisors on E modulo principal divisors, and let $\operatorname{Pic}^0 E\subset \operatorname{Pic} E$ be the subgroup of divisors of degree 0. One finds a bijection $P\mapsto [P]-[0]$ between the set $E(K)$ and $\operatorname{Pic}^0 E$, which shows that $E(K)$ has the structure of an abelian group.

Generally, if C/K is a curve of genus g, then the Jacobian variety $J(C)$ is an abelian variety having the property that $\operatorname{Pic}^0 C_L = J(C)(L)$ for any field L containing K. (The precise definition of $J(C)$ is more subtle. One defines a certain functor on K-schemes, whose value on S is a certain group of classes of line bundles on $C\times_K S$. There are additional subtleties when

$C(K)$ is empty. See Milne's notes on abelian varieties for the full story.) The dimension of $J(C)$ is g.

2 Jacobians over $\mathbb{C}$

When $K = \mathbb{C}$, the construction of the Jacobian is due to Jacobi himself. Let X be a compact Riemann surface. We have the first homology group $H_1(X, \mathbb{Z}) \approx \mathbb{Z}^{2g}$ and the g-dimensional complex vector space $H^0(X, \Omega^1_{X/\mathbb{C}})$ of holomorphic 1-forms on X. Let $\omega_1, \ldots, \omega_g$ be a basis for $H^0(X, \Omega^1_{X/\mathbb{C}})$. There is an injective map

$$\begin{aligned} H_1(X, \mathbb{Z}) &\to H^0(X, \Omega^1_{X/\mathbb{C}})^* \\ \gamma &\mapsto \left(\omega \mapsto \int_\gamma \omega\right) \end{aligned}$$

Let $J(X)$ be the complex torus $\mathbb{C}^g / H_1(X, \mathbb{Z})$. Let $P_0 \in X$ be a base point. The Abel-Jacobi theorem states that there is an isomorphism of groups

$$\mathrm{Pic}^0(C) \to J(X)$$

which sends a divisor $[P] - [P_0]$ to

$$\omega \mapsto \int_{P_0}^P \omega.$$

One can find an embedding of $J(X)$ to projective space, whereby it must be (the complex variety associated to) a projective variety.

What we've just described is a functor $X \mapsto J(X)$ which is covariant in X. The Jacobian is usually considered to be contravariant, probably for the reason that is is simpler to pull back divisors/line bundles than it is to push them forward. There is a contravariant reformulation of the above, whereby $J(X)$ gets identified with $H^0(X, \Omega^1_{X/\mathbb{C}})$ modulo $H^1(X, \mathbb{Z})$. Then the Lie algebra of $J(X)$ is $H^0(X, \Omega^1 X/C)$.

This holds in the general setting: if C/K is a smooth projective curve, then the tangent space to $J(C)$ at the origin is $H^0(C, \Omega^1_{C/K})$.

3 Isogenies and duality

A *homomorphism* $f\colon A \to A'$ between abelian varieties is a morphism of varieties which preserves the group structure on A and A'. A homomorphism f is an *isogeny* if it is surjective with finite kernel. In that case, the *degree* of f is the order of its kernel. The multiplication-by-n map $n_A\colon A \to A$ has degree n^{2g}.

If A has dimension g over a field K, and ℓ is a prime number other than the characteristic of K, then the torsion subgroup $A[\ell^n]$ is isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^g$, for all $n \geq 1$. The ℓ-adic Tate module of A is

$$T_\ell A = \varprojlim A[\ell^n] \approx \mathbb{Z}_\ell^g.$$

This is the pro-ℓ part of the étale fundamental group of A, and therefore it is the $\mathbb{Z}_\ell$-linear dual of $H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Z}_\ell)$.

The *dual* abelian variety is $\hat{A} = \operatorname{Pic}^0 A$. The duality $A \mapsto \hat{A}$ is contravariant. Unlike the case for elliptic curves, A need not be isomorphic to its dual. If D is a divisor on A, then we get a homomorphism $\phi_D\colon A \to \hat{A}$ defined by $P \mapsto T_P(D) - D$, where $T_P\colon A \to A$ is the translation-by-P map. Then ϕ_D is an isogeny when D is ample. An isogeny $A \to \hat{A}$ arising this way is called a *polarization.* A polarization is *principal* if it is an isomorphism. Jacobian varieties always admit a principal polarization.

There is a nondegenerate pairing

$$T_\ell A \times T_\ell \hat{A} \to \mathbb{T}_\ell \mu$$

which generalizes the Weil pairing on elliptic curves.

4 Abelian varieties over finite fields

Let A be an abelian variety over a finite field $\mathbb{F}_q$. We have the Frobenius endomorphism $A \to A$, which is the identity on the underlying topological space but which is the qth power map on the structure sheaf. Let $\phi_q\colon A_{\overline{\mathbb{F}}_q} \to A_{\overline{\mathbb{F}}_q}$ be its base extension to $\overline{\mathbb{F}}_q$. In essence, the effect of ϕ_q on a closed point of $A_{\overline{\mathbb{F}}_q}$ is to raise each of its coordinates to the qth power.

Theorem 4.0.1. *(The Weil conjectures for abelian varieties over finite fields.) Let ℓ be a prime not dividing q, and let $T_\ell(\phi_q)$ be the endomorphism of $T_\ell(A)$ induced by ϕ_q. Let $P(X)$ be the characteristic polynomial of $T_\ell(\phi_q)$. Then:*

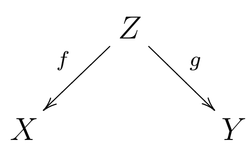
1. *$P(X)$ has integral coefficients and does not depend on ℓ.* (Independence of ℓ.)

2. *If α is a complex root of $P(T)$, then so is q/α.* (Functional equation.)

3. *If α is a complex root of $P(T)$ then $|\alpha| = \sqrt{q}$.* (Riemann hypothesis.)

5 Correspondences

If X and Y are two smooth projective curves, then a *correspondence* between X and Y is a diagram



where Z is a third projective curve and the arrows represent finite morphisms. (There is a more general definition for varieties X and Y of higher dimension.) If $h\colon X \to Y$ is a finite morphism, then h gives a correspondence as above by setting $Z = X$, but not all correspondences will arise this way. But a correspondence can act like a morphism, in that it induces maps between various vector spaces attached to X and Y. For example, if D is a divisor on X, we can get a divisor $g_* f^* D$ on Y by taking the preimage of D in Z (this will increase the degree by a factor of $\deg(f)$) and then pushing this into Y. This induces a morphism $J(X) \to J(Y)$ (exercise).