1.5 Jacobians of Curves

1. I will give a research talk in the modular curves seminar tomorrow (Thursday, October 16, 3-4pm in SC 507) about the arithmetic of the Jacobian $J_1(p)$ of $X_1(p)$. It will fit well with this part of the course.

2. New web page: `http://modular.fas.harvard.edu/calc/`. Type or paste in a MAGMA or PARI program, click a button, get the output. No need to install MAGMA or PARI or log in anywhere.

Today we're going to learn about Jacobians. First, some inspiring words by David Mumford:

> "The Jacobian has always been a corner-stone in the analysis of algebraic curves and compact Riemann surfaces. [...] Weil's construction [of the Jacobian] was the basis of his epoch-making proof of the Riemann Hypothesis for curves over finite fields, which really put characteristic p algebraic geometry on its feet." – Mumford, *Curves and Their Jacobians*, page 49.

1.5.1 Divisors on Curves and Linear Equivalence

Let X be a projective nonsingular algebraic curve over an algebraically field k. A *divisor* on X is a formal finite $\mathbf{Z}$-linear combination $\sum_{i=1}^m n_i P_i$ of closed points in X. Let $\mathrm{Div}(X)$ be the group of all divisors on X. The *degree* of a divisor $\sum_{i=1}^m n_i P_i$ is the integer $\sum_{i=1}^m n_i$. Let $\mathrm{Div}^0(X)$ denote the subgroup of divisors of degree 0.

Suppose k is a perfect field (for example, k has characteristic 0 or k is finite), but do not require that k be algebraically closed. Let the group of divisors on X over k be the subgroup

$$\mathrm{Div}(X) = \mathrm{Div}(X/k) = \mathrm{H}^0(\mathrm{Gal}(\overline{k}/k), \mathrm{Div}(X/\overline{k}))$$

of elements of $\mathrm{Div}(X/\overline{k})$ that are fixed by every automorphism of $\overline{k}/k$. Likewise, let $\mathrm{Div}^0(X/k)$ be the elements of $\mathrm{Div}(X/k)$ of degree 0.

A *rational function* on an algebraic curve X is a function $X \to \mathbf{P}^1$, defined by polynomials, which has only a finite number of poles. For example, if X is the elliptic curve over k defined by $y^2 = x^3 + ax + b$, then the field of rational functions on X is the fraction field of the integral domain $k[x, y]/(y^2 - (x^3 + ax + b))$. Let $K(X)$ denote the field of all rational functions on X defined over k.

There is a natural homomorphism $K(X)^* \to \mathrm{Div}(X)$ that associates to a rational function f its divisor

$$(f) = \sum \mathrm{ord}_P(f) \cdot P$$

where $\mathrm{ord}_P(f)$ is the order of vanishing of f at P. Since X is nonsingular, the local ring of X at a point P is isomorphic to $k[[t]]$. Thus we can write $f = t^r g(t)$ for some unit $g(t) \in k[[t]]$. Then $R = \mathrm{ord}_P(f)$.

Example 1.5.1. If $X = \mathbf{P}^1$, then the function $f = x$ has divisor $(0) - (\infty)$. If X is the elliptic curve defined by $y^2 = x^3 + ax + b$, then

$$(x) = (0, \sqrt{b}) + (0, -\sqrt{b}) - 2\infty,$$

and

$$(y) = (x_1, 0) + (x_2, 0) + (x_3, 0) - 3\infty,$$

where x_1, x_2, and x_3 are the roots of $x^3+ax+b=0$. A uniformizing parameter t at the point ∞ is x/y. An equation for the elliptic curve in an affine neighborhood of ∞ is $Z = X^3 + aXZ^2 + bZ^3$ (where $\infty = (0,0)$ with respect to these coordinates) and $x/y = X$ in these new coordinates. By repeatedly substituting Z into this equation we see that Z can be written in terms of X.

It is a standard fact in the theory of algebraic curves that if f is a nonzero rational function, then $(f) \in \mathrm{Div}^0(X)$, i.e., the number of poles of f equals the number of zeros of f. For example, if X is the Riemann sphere and f is a polynomial, then the number of zeros of f (counted with multiplicity) equals the degree of f, which equals the order of the pole of f at infinity.

The *Picard group* $\mathrm{Pic}(X)$ of X is the group of divisors on X modulo linear equivalence. Since divisors of functions have degree 0, the subgroup $\mathrm{Pic}^0(X)$ of divisors on X of degree 0, modulo linear equivalence, is well defined. Moreover, we have an exact sequence of abelian groups

$$0 \to K(X)^* \to \mathrm{Div}^0(X) \to \mathrm{Pic}^0(X) \to 0.$$

Thus for any algebraic curve X we have associated to it an abelian group $\mathrm{Pic}^0(X)$. Suppose $\pi : X \to Y$ is a morphism of algebraic curves. If D is a divisor on Y, the pullback $\pi^*(D)$ is a divisor on X, which is defined as follows. If $P \in \mathrm{Div}(Y/\overline{k})$ is a point, let $\pi^*(P)$ be the sum $\sum e_{Q/P}Q$ where $\pi(Q) = P$ and $e_{Q/P}$ is the ramification degree of Q/P. (Remark: If t is a uniformizer at P then $e_{Q/P} = \mathrm{ord}_Q(\phi^* t_P)$.) One can show that $\pi^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$ induces a homomorphism $\mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X)$. Furthermore, we obtain the contravariant *Picard functor* from the category of algebraic curves over a fixed base field to the category of abelian groups, which sends X to $\mathrm{Pic}^0(X)$ and $\pi : X \to Y$ to $\pi^* : \mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X)$.

Alternatively, instead of defining morphisms by pullback of divisors, we could consider the push forward. Suppose $\pi : X \to Y$ is a morphism of algebraic curves and D is a divisor on X. If $P \in \mathrm{Div}(X/\overline{k})$ is a point, let $\pi_*(P) = \pi(P)$. Then π_* induces a morphism $\mathrm{Pic}^0(X) \to \mathrm{Pic}^0(Y)$. We again obtain a functor, called the covariant *Albanese functor* from the category of algebraic curves to the category of abelian groups, which sends X to $\mathrm{Pic}^0(X)$ and $\pi : X \to Y$ to $\pi_* : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(Y)$.

1.5.2 Algebraic Definition of the Jacobian

First we describe some universal properties of the Jacobian under the hypothesis that $X(k) \neq \emptyset$. Thus suppose X is an algebraic curve over a field k and that $X(k) \neq \emptyset$. The Jacobian variety of X is an abelian variety J such that for an extension k'/k, there is a (functorial) isomorphism $J(k') \to \mathrm{Pic}^0(X/k')$. (I don't know whether this condition uniquely characterizes the Jacobian.)

Fix a point $P \in X(k)$. Then we obtain a map $f : X(k) \to \mathrm{Pic}^0(X/k)$ by sending $Q \in X(k)$ to the divisor class of $Q-P$. One can show that this map is induced by an injective morphism of algebraic varieties $X \hookrightarrow J$. This morphism has the following universal property: if A is an abelian variety and $g : X \to A$ is a morphism that sends P to $0 \in A$, then there is a unique homomorphism $\psi : J \to A$ of abelian varieties such that $g = \psi \circ f$:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "g"'] & J \arrow[d, "\psi"] \\ & A \end{tikzcd}$$

This condition uniquely characterizes J, since if $f' : X \to J'$ and J' has the universal property, then there are unique maps $J \to J'$ and $J' \to J$ whose composition in both directions must be the identity (use the universal property with $A = J$ and $f = g$).

If X is an arbitrary curve over an arbitrary field, the Jacobian is an abelian variety that represents the "sheafification" of the "relative Picard functor". Look in Milne's article or Bosch-Lüktebohmert-Raynaud *Neron Models* for more details. Knowing this totally general definition won't be important for this course, since we will only consider Jacobians of modular curves, and these curves always have a rational point, so the above properties will be sufficient.

A useful property of Jacobians is that they are canonically principally polarized, by a polarization that arises from the "θ divisor" on J. In particular, there is always an isomorphism $J \to J^\vee = \mathrm{Pic}^0(J)$.

1.5.3 The Abel-Jacobi Theorem

Over the complex numbers, the construction of the Jacobian is classical. It was first considered in the 19th century in order to obtain relations between integrals of rational functions over algebraic curves (see Mumford's book, *Curves and Their Jacobians*, Ch. III, for a nice discussion).

Let X be a Riemann surface, so X is a one-dimensional complex manifold. Thus there is a system of coordinate charts (U_α, t_α), where $t_\alpha : U_\alpha \to \mathbf{C}$ is a homeomorphism of U_α onto an open subset of $\mathbf{C}$, such that the change of coordinate maps are analytic isomorphisms. A *differential* 1*-form* on X is a choice of two continuous functions f and g to each local coordinate $z = x + iy$ on $U_\alpha \subset X$ such that $f\,dx + g\,dy$ is invariant under change of coordinates (i.e., if another local coordinate patch U'_α intersects U_α, then the differential is unchanged by the change of coordinate map on the overlap). If $\gamma : [0,1] \to X$ is a path and $\omega = f\,dx + g\,dy$ is a 1-form, then

$$\int_\gamma \omega := \int_0^1 \left(f(x(t), y(t))\frac{dx}{dt} + g(x(t), y(t))\frac{dy}{dt} \right) dt \in \mathbf{C}.$$

From complex analysis one sees that if γ is homologous to γ', then $\int_\gamma \omega = \int_{\gamma'} \omega$. In fact, there is a nondegenerate pairing

$$\mathrm{H}^0(X, \Omega^1_X) \times \mathrm{H}_1(X, \mathbf{Z}) \to \mathbf{C}$$

If X has genus g, then it is a standard fact that the complex vector space $\mathrm{H}^0(X, \Omega^1_X)$ of holomorphic differentials on X is of dimension g. The integration pairing defined above induces a homomorphism from integral homology to the dual V of the differentials:

$$\Phi : \mathrm{H}_1(X, \mathbf{Z}) \to V = \mathrm{Hom}(H^0(X, \Omega^1_X), \mathbf{C}).$$

This homomorphism is called the *period mapping.*

Theorem 1.5.2 (Abel-Jacobi). *The image of* Φ *is a lattice in* V.

The proof involves repeated clever application of the residue theorem.

The intersection pairing

$$\mathrm{H}_1(X,\mathbf{Z}) \times \mathrm{H}_1(X,\mathbf{Z}) \to \mathbf{Z}$$

defines a nondegenerate alternating pairing on $L = \Phi(\mathrm{H}_1(X,\mathbf{Z}))$. This pairing satisfies the conditions to induce a nondegenerate Riemann form on V, which gives $J = V/L$ to structure of abelian variety. The abelian variety J is the Jacobian of X, and if $P \in X$, then the functional $\omega \mapsto \int_P^Q \omega$ defines an embedding of X into J. Also, since the intersection pairing is perfect, it induces an isomorphism from J to $J^\vee$.

Example 1.5.3. For example, suppose $X = X_0(23)$ is the modular curve attached to the subgroup $\Gamma_0(23)$ of matrices in $\mathrm{SL}_2(\mathbf{Z})$ that are upper triangular modulo 24. Then $g = 2$, and a basis for $\mathrm{H}_1(X_0(23),\mathbf{Z})$ in terms of modular symbols is

$$\{-1/19, 0\}, \quad \{-1/17, 0\}, \quad \{-1/15, 0\}, \quad \{-1/11, 0\}.$$

The matrix for the intersection pairing on this basis is

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

With respect to a reduced integral basis for

$$\mathrm{H}^0(X,\Omega_X^1) \cong S_2(\Gamma_0(23)),$$

the lattice $\Phi(\mathrm{H}_1(X,\mathbf{Z}))$ of periods is (approximately) spanned by

```
[
    (0.59153223605591049412844857432 - 1.68745927346801253993135357636*i
        0.762806324458047168681080323846571478727 - 0.60368764497868211035115379488*i),
    (-0.59153223605591049412844857432 - 1.68745927346801253993135357636*i
        -0.762806324458047168681080323846571478727 - 0.60368764497868211035115379488*i),
    (-1.354338560513957662809528899804 - 1.083771628489330429580199780856874871 4097*i
        -0.59153223605591049412844857401 + 0.48008398351064831922904598 7467*i),
    (-1.52561264891609433736216065099 0.342548176804273349105263499648)
]
```