JACOBIANS OF HYPERELLIPTIC CURVES

by Jeff Yelton

# 1 Algebraic Construction

## 1.1 Smooth, projective hyperelliptic curves

Let $k$ be any field of characteristic $\neq 2$. Abstractly, a (smooth, projective) hyperelliptic curve $C/k$ can be thought of as a 2-fold cover of the projective line $\mathbb{P}^1_k$. If $C$ has genus $g$, then Hurwitz's formula tells us this cover is ramified at $2g+2$ points of $\mathbb{P}^1_k$. If one of these points is $\infty$ and the other $2g+1$ are labled $\alpha_1, ..., \alpha_{2g+1} \in \mathbb{P}^1_k \backslash \{\infty\}$, then $C$ is isomorphic to the smooth compactification of the affine curve defined by $y^2 = \prod_{i=1}^{2g+1}(x-\alpha_i)$. If $\infty$ is not a ramification point and the $2g+2$ ramification points are labeled $\alpha_1, ..., \alpha_{2g+2} \in \mathbb{P}^1_k \backslash \{\infty\}$, then $C$ is isomorphic to the smooth compactification of the affine curve defined by $y^2 = \prod_{i=1}^{2g+2}(x-\alpha_i)$. Thus, a hyperelliptic curve $C$ of genus $g$ is the smooth projective model of an affine curve defined by $y^2 = f(x)$ where the degree of $f$ is $d = 2g+1$ or $d = 2g+2$.

These smooth projective models are constructed as follows. Let $C_1$ be the affine curve given by $y^2 = \prod_{i=1}^{d}(x-\alpha_i)$. Let $C_2$ be the affine curve given by $y'^2 = x\prod_{i=1}^{d}(1-\alpha_i x')$ if $d = 2g+1$ and $y'^2 = \prod_{i=1}^{d}(1-\alpha_i x')$ if $d = 2g+2$. To get $C$, glue $C_1$ and $C_2$ along the open subsets $C_1\backslash\{(0,0)\}$ and $C_2\backslash\{(0,0)\}$ via the identifications $x' = 1/x$ and $y' = y/x^{g+1}$. If $d = 2g+1$, then there is one "point at infinity" in $C\backslash C_1$ coming from $(0,0) \in C_2$, which we denote by $\infty$. (It is the point in the preimage of the ramified point $\infty \in \mathbb{P}^1_k$.) If $d = 2g+2$, then there are two "points at infinity" in $C\backslash C_1$ coming from $(0,1), (0,-1) \in C_2$, which we denote by $\infty_1$ and $\infty_2$. (They are the two points in the preimage of the non-ramified point $\infty \in \mathbb{P}^1_k$.)

There is an important involution $\iota : C to C$ given (in the affine part) by $(x,y) \mapsto (x,-y)$. (In fact, the 2-fold covering $C \to \mathbb{P}^1$ is the quotient map of $C$ by this involution.) Note that if $d = 2g+1$, $\iota$ fixes $\infty$, and if $d = 2g+2$, $\iota$ switches $\infty_1$ and $\infty_2$.

Write $\bar{k}[C] := \bar{k}[x,y]/(y^2 - f(x))$ for the ring of functions defined on the affine subset given by $y^2 = f(x)$. Write $\bar{k}(C)$ for its corresponding fraction field, which is the function field of $C$. We consider $x$ and $y$ as functions in

$\bar{k}[C]$, and thus, for any non-infinity point $P \in C(\bar{k})$, we write $x(P)$ for its $x$-coordinate and $y(P)$ for its $y$-coordinate.

Write $\mathrm{Div}(C)$ for the group of divisors on $C$ (which is the group of formal sums of points in $C(\bar{k})$). Let $\mathrm{Div}^0(C)$ denote the subgroup of $\mathrm{Div}(C)$ consisting of divisors of degree 0 on $C$. If $f \in \bar{k}(C)$, we will denote its corresponding divisor by $(f)$. Since $C$ is projective, the degree of $(f)$ is 0, so the set of principal divisors $(f)$ is a subgroup of $\mathrm{Div}^0(C)$. Let $\mathrm{Pic}(C)$ denote the *Picard group* of $C/\bar{k}$, which is the quotient of $\mathrm{Div}(C)$ by its subgroup of principal divisors. Finally, let $\mathrm{Pic}^0(C)$ denote the quotient of $\mathrm{Div}^0(C)$ by its subgroup of principal divisors. The following, which is easy to verify, will be useful in our study of representatives of divisor classes in $\mathrm{Pic}^0(C)$.

**Fact 1.1.** *a) Let $P$ be a non-infinity point in $C(\bar{k})$. If $d = 2g + 1$, then*

$$(x - x(P)) = P + \iota(P) - 2(\infty).$$

*If $d = 2g + 2$, then*

$$(x - x(P)) = P + \iota(P) - \infty_1 - \infty_2.$$

*b) If $d = 2g + 1$, then*

$$(y) = \sum_{i=1}^{2g+1} (\alpha_i, 0) - (2g + 1)(\infty).$$

*If $d = 2g + 2$, then*

$$(y) = \sum_{i=1}^{2g+2} (\alpha_i, 0) - (g + 1)(\infty_1) - (g + 1)(\infty_2).$$

## 1.2 The abstract group $\mathrm{Pic}^0(C)$

As an abstract group, the Jacobian of $C$ is isomorphic to $\mathrm{Pic}^0(C)$. Therefore, in order to construct the Jacobian, we will show that $\mathrm{Pic}^0(C)$ can be given the structure of a variety over $k$. Our first step is to show that there is a bijection between $\mathrm{Div}^g(C)$ and "most" of $\mathrm{Pic}^0(C)$.

**Proposition 1.2.** *Any element of $\mathrm{Pic}^0(C)$ can be represented by a divisor of the form $\sum_{i=1}^{g} P_i - g(\infty)$. Moreover, any element of $\mathrm{Pic}^0(C)$ is represented by a unique divisor of the form $\sum_{i=1}^{m} P_i - m(\infty)$ such that $P_i \neq \infty$ and $P_i \neq \iota(P_j)$ for $i \neq j$.*

**Remark 1.3.** The first statement can be proven for any curve $C$ of genus $g$ (not necessarily hyperelliptic) using the Riemann-Roch theorem, but we give a more explicit proof here in the case that $C$ is a hyperelliptic curve defined by the equation $y^2 = f(x)$.

*Proof.* Choose a divisor $D$ representing any element of $\mathrm{Pic}^0(C)$. Then after adding principal divisors of the form $P + \iota(P) - 2 \cdot (\infty)$ to $D$ for suitable points $P$, we may assume that $D$ is of the form $\sum_{i=1}^{m} P_i - m(\infty)$ for some $m \geq 0$, with $P_i \neq \iota(P_j)$ for $i \neq j$. Clearly, to prove the first statement of the proposition, it suffices to show that if $m = g + 1$, there exist points $P_1', ..., P_g' \in C(\bar{k})$ such that $D \equiv \sum_{i=1}^{g} P_i' - g(\infty)$. It suffices to show that there is a function $h \in k(C)$ with a zero at $(\infty)$, a simple pole at each $P_i$, and no poles anywhere else. Using polynomial interpolation, one may construct $\phi \in k[x]$ such that $\phi(x(P_i)) = y(P_i)$ for $i = 1, ..., g + 1$, and such that $\phi$ has degree $\leq g$. Then let

$$h := \frac{y + \phi(x)}{\prod_{i=1}^{g+1}(x - x(P_i))}.$$

One checks that $h$ has the desired property, and the first statement is proved.

To prove the second statement, choose points $P_1, ..., P_m \in C(\bar{k})$ with $m \geq g$, $P_i \neq \infty$, and $P_i \neq \iota(P_j)$ for $i \neq j$, and let $h \in \mathcal{L}(\sum_{i=1}^{m} P_i)$. If we let $\tilde{h} := h \prod_{i=1}^{m}(x - x(P_i))$, then $\tilde{h} \in \mathcal{L}(2m(\infty) - \sum_{i=1}^{m} \iota(P_i))$. Since the only poles of $\tilde{h}$ are at $\infty$, $\tilde{h} \in k[C]$ and can be expressed as $s(x)y + t(x)$ where $s$ and $t$ are polynomial functions. Note that since $\mathrm{ord}_\infty(x) = -2$ and $\mathrm{ord}_\infty(y) = -2g - 1$, the order of the pole at $\infty$ of $s(x)y + t(x)$ is $\max\{2\deg(s) + 2g + 1, 2\deg(t)\}$. But we know the order of this pole is $2m \leq 2g$, which forces $s = 0$ and $\deg(t) = m$. So $\tilde{h}$ is a polynomial in $x$ of degree $m$ with zeros at each $\iota(P_i)$ (or equivalently, zeros at each $P_i$). Since $P_i \neq \iota(P_j)$ for $i \neq j$, the elements $x(P_i)$ are distinct, forcing $\tilde{h}$ to be a constant multiple of $\prod_{i=1}^{m}(x - x(P_i))$. This implies that $h$ is a constant function. Thus, the only functions with no poles other than possibly simple poles at the $P_i$'s are constant functions. This implies that if $\sum_{i=1}^{m} P_i - m(\infty) \equiv \sum_{i=1}^{m} P_i' - m(\infty)$ for points $P_i' \in C(\bar{k})$, then $P_i' = P_i$, and so there is only one representative of this form.

□

Proposition 1.2 says that there is a bijection between $\mathrm{Pic}^0(C)$ and the set of divisors of the form $\sum_{i=1}^{m} P_i - m(\infty)$, with $m \leq g$, $P_i \neq \infty$, and $P_i \neq \iota(P_j)$ for $i \neq j$. Let $Z$ denote the subset of divisors of the above form with $m = g$.

We will be able to view $Z$ as an open affine subvariety of the Jacobian we are constructing.

## 1.3 $Z \subset \mathrm{Pic}^0(C)$ as an affine variety

The goal of this subsection is to show that $\mathrm{Pic}^0(C)$ can be given the structure of a smooth affine variety over $\bar{k}$ of dimension $g$ (and that $G_k$-invariant elements of $\mathrm{Pic}^0(C)$ correspond to $k$-points of $Z$). Choose any divisor $D \in Z$, and write $D = \sum_{i=1}^{g} P_i - g(\infty)$, with $P_i \neq \infty$, $P_i \neq \iota(P_j)$ for $i \neq j$. Let $u(x) := \prod_{i=1}^{g}(x - x(P_i)) \in \bar{k}[x]$. By the theory of polynomial interpolation, there is a unique polynomial $v(x) \in \bar{k}[x]$ of degree $\leq g-1$ such that for all $i$, $v(x(P_i)) = y(P_i)$ (note that this condition makes sense because $x(P_i) = x(P_j)$ implies $y(P_i) = y(P_j)$ for $i \neq j$). Write

$$u(x) = x^g + u_{g-1}x^{g-1} + ... + u_1 x + u_0,\ v(x) = v_{g-1}x^{g-1} + ... + v_1 x + v_0,$$

with $u_i, v_i \in \bar{k}$.

Note that in $\bar{k}[x]$, $u$ divides $f - v^2$ because $u(x) = 0$ implies that $f(x) - v(x)^2 = 0$. Conversely, given $(u, v)$ with $u$ a monic polynomial of degree $g$ and $v$ a polynomial of degree $g-1$, such that $u|f - v^2$, one can determine points $P_1, ..., P_g \in \mathbb{P}^2_{\bar{k}}$ satisfying the desired conditions (their $x$-coordinates are the roots of $u$, and plugging those roots into $v$ gives you their $y$-coordinates; the "$u|f - v^2$" condition implies that these points lie on $C\backslash\{\infty\}$). So there is a bijection between $Z$ and the set of such $(u, v)$.

Now the set of $(u, v)$ with the above properties can be described in the following way. In general, for any monic, degree-$g$ polynomial $u(x) = x^g + u_{g-1}x^{g-1} + ... + u_1 x + u_0$ and any polynomial (of degree $\leq g-1$) $v(x) = v_{g-1}x^{g-1} + ... + v_1 x + v_0$, by the Euclidean algorithm, $f(x) - v(x)^2 \equiv u(x)q(x) + r(x)$, where $q(x)$ is monic of degree $g+1$ and the "remainder polynomial" $r(x)$ has degree $g-1$. Here $r = r_{g-1}x^{g-1} + ... + r_1 x + r_0$ is uniquely determined by $(u, v)$, and each coefficient $r_i$ is a polynomial function of the coefficients $u_j, v_k$. The condition that $u|f - v^2$ is equivalent to the condition that $r \equiv 0$, so the set of such $(u, v)$ satisfying this condition can be viewed as a variety over $\bar{k}$ in the $2g$ variables $u_0, ..., u_{g-1}, v_0, ..., v_{g-1}$ defined by the $g$ equations $r_0 = ... = r_{g-1} = 0$. In this way, $Z$ is given the structure of an affine variety.

**Proposition 1.4.** *With the structure of variety described above, $Z$ is smooth of dimension $g$.*

*Proof.* First, we study the set of all triples $(u, v, w)$, where $u \in \bar{k}[x]$ is monic of degree $g$, $v \in \bar{k}[x]$ is of degree $\leq g-1$, $w \in \bar{k}[x]$ is monic of degree $g+1$, and $f - v^2 = uw$. Denote the coefficients of $u$ and $v$ as before, and denote the non-leading coefficients of $w$ by $w_0, ..., w_g$. Then this set can be viewed as a variety in the $3g+1$ variables $\{u_i, v_j, w_k\}$ defined by the $2g+1$ equations obtained by equating the coefficients of $f - v^2$ and $uw$. Moreover, this variety can easily be seen to be isomorphic to $Z$. Thus, to prove that $Z$ is smooth of dimension $g$, it suffices to show that this variety whose points are of the form $(u, v, w)$ with the above properties has tangent space of dimension $g$ at each point.

Fix $(u, v, w)$ in $Z$. The tangent space at this point $(u, v, w)$ can be viewed as the vector space of all $(\tilde{u}, \tilde{v}, \tilde{w})$ with $\tilde{u}$ and $\tilde{v}$ of degree $g-1$ and $\tilde{w}$ of degree $g$, such that

$$f - (v + \epsilon\tilde{v})^2 \equiv (u + \epsilon\tilde{u})(w + \epsilon\tilde{w}) \pmod{\epsilon^2}.$$

Expanding both sides and using the relation $f - v^2 = uw$, we get the condition

$$2v\tilde{v} + u\tilde{w} + \tilde{u}w = 0.$$

Let $V$ denote the vector space consisting of the polynomials $2v\tilde{v} + u\tilde{w} + \tilde{u}w$ for all $\tilde{u}$, $\tilde{v}$ of degree $g-1$ and $\tilde{w}$ of degree $g$. Note that for any $x$, we cannot have $u(x) = v(x) = w(x) = 0$, or else $f = v^2 + uw$ would have a multiple zero. Thus, if $a_1, ..., a_g$ are the roots of $u$, given any choice of $b_1, ..., b_g \in \bar{k}$, we may choose $\tilde{v}$ and $\tilde{w}$ such that $p := 2v\tilde{v} + u\tilde{w} + \tilde{u}w$ evaluated at each $a_i$ is $b_i$. By the Euclidean algorithm, we may write $p(x) = qu + r$ for unique $q$ of degree $\leq g$ and $r$ of degree $\leq g-1$. But clearly $qu \in V$, and it follows that $r$ is in $V$. In other words, given any choice of $b_1, ..., b_g \in \bar{k}$, there is a polynomial $r \in V$ of degree $\leq g-1$ such that $r(a_i) = b_i$ for $1 \leq i \leq g$. Thus, $V$ contains all polynomials of degree $\leq g-1$.

Now let $p$ be an arbitrary polynomial of degree $\leq 2g$. Then, again using the Euclidean algorithm, write $p = qu + r$ for $q$ of degree $\leq g$ and $r$ of degree $\leq g-1$. Since $r \in V$ and $qu \in V$, we get $p \in V$. Since certainly all polynomials in $V$ are of degree $\geq 2g$, it follows that $V$ coincides with the vector space of all polynomials of degree $2g$.

Thus, the condition that $2v\tilde{v}+u\tilde{w}+\tilde{u}w = 0$ imposes $2g+1$ linear equations on the $3g+1$ coefficients of $\tilde{u}$, $\tilde{v}$, and $\tilde{w}$, and so this tangent space is of dimension $(3g+1) - (2g+1) = g$, as desired.

□

## 1.4 Gluing translates of $Z$

We now want to show that $\mathrm{Pic}^0(C)$ is the union of translations of $Z$ by certain elements, and that when we glue these translates of $Z$ together, we get a variety which we will denote by $J$. Letting $B$ as before be the set of branch points, for any subset $T \subset B$, let $D_T := \sum_{P \in T} P - \#T(\infty)$. Note that $D_T \equiv \sum_{P \in B \setminus T} P - (2g + 1 - \#T)(\infty)$ in $\mathrm{Pic}^0(C)$, and that $2D_T$ is a principal divisor. For any $T \subset B$, let $Z + D_T$ denote the subset of $\mathrm{Pic}^0(C)$ obtained by translating the translating the elements of $Z$ by the divisor class of $D_T$ in $\mathrm{Pic}^0(C)$.

**Proposition 1.5.** *We have*

$$\mathrm{Pic}^0(C) = \bigcup (Z + D_T),$$

*where the union is taken over all subsets $T \subset B$ of even cardinality.*

*Proof.* Choose any element of $\mathrm{Pic}^0(C)$, and let $D = \sum_{i=1}^{m} P_i - m(\infty)$ be a divisor representing it, with $m \leq g$, $P_i \neq \infty$, and $P_i \neq \iota(P_j)$ for $i \neq j$ (a representative of this form exists by Proposition 1.2). Choose $g - m$ branch points $Q_1, ..., Q_{g-m} \in B$ not equal to any of the $P_i$'s, and let $T := \{Q_i\}$ if $g - m$ is even, and let $T := B \setminus \{Q_i\}$ if $g - m$ is odd. Then it is clear that

$$D + \sum_{i=1}^{g-m} Q_i - (g-m)(\infty) \equiv \sum_{i=1}^{m} P_i + \sum_{j=1}^{g-m} Q_j - g(\infty) \equiv D + D_T \equiv D - D_T.$$

Moreover, since the $Q_j$'s are distinct, equal to their own images under $\iota$, and different from the $P_i$'s, it is clear by letting $P_{m+i} := Q_i$ for $1 \leq i \leq g - m$ that $D - D_T \equiv \sum_{i=1}^{g} P_i - g(\infty) \in Z$. Therefore, the element of $\mathrm{Pic}^0(C)$ represented by $D$ lies in $Z + D_T$.

□

We now want to show that $\bigcup (Z + D_T)$ can be given the structure of a variety, arising from the structure of $Z$ as a variety. The following lemma is well known.

**Lemma 1.6.** *Let $X$ and $Y$ be varieties, $U \subset X$ and $V \subset Y$ be open subsets, and $\phi : U \xrightarrow{\sim} V$ be an isomorphism. Then the scheme obtained by gluing $X$ and $Y$ along $U \cong V$ is a variety if and only if*

$$\{(a, b) \in U \times V \mid b = \phi(a)\} \subset X \times Y$$

*is Zariski closed.*

In light of the above lemma, to show that gluing together the $(Z + D_T)$'s gives us a variety, it will suffice to prove the following:

**Proposition 1.7.** *For subsets $T_1, T_2 \subset B$ of even cardinality, let*

$$\Gamma_{T_1,T_2} := \{(D_1, D_2) \in Z \times Z \mid D_1 + D_{T_1} \equiv D_2 + D_{T_2}\}.$$

*Then $\Gamma_{T_1,T_2}$ is Zariski closed in $Z \times Z$, and the images in $Z$ of each of its projections are Zariski open in $Z$.*

*Proof.* Write $D_1 = \sum_{i=1}^{g} P_{1,i} - g(\infty)$ and $D_2 = \sum_{i=1}^{g} P_{2,i} - g(\infty)$ with the usual conditions on the $P_{1,i}$'s and the $P_{2,i}$'s. Let $n := 2g + \#T_1 + \#T_2$. Then $(D_1, D_2) \in \Gamma_{T_1,T_2}$ if and only if $\sum_{i=1}^{g} P_{1,i} + \sum_{j=1}^{g} \iota(P_{2,j}) + \sum_{P \in T_1} P + \sum_{P \in T_2} P - n(\infty)$ is a principal divisor $(h)$ for some function $h \in k(C)$.

Now associate $D_1$ with $(u_{D_1}, v_{D_1})$ and $D_2$ with $(u_{D_2}, v_{D_2})$ as in the above construction of the affine variety structure of $Z$. The ideal in $\bar{k}[Z \times Z][x, y]/(y^2 - f(x))$ of functions which at each $(D_1, D_2) \in Z \times Z$ specialize to functions in $\bar{k}[x, y]/(y^2 - f(x))$ with zeros at the $P_{1,i}$'s and $P_{2,i}$'s is

$$I := (u^{(1)}(x), y - v^{(1)}(x)) \cdot (u^{(2)}(x), y - v^{(2)}(x)) \cdot \prod_{P \in T_1} (x - x(P)) \cdot \prod_{P \in T_2} (x - x(P)).$$

(In the above expression, $u^{(1)}$ is the function $x^g + u_{g-1}x^{g-1} + ... + u_0$ where the $u_i$'s are coordinate functions of the first copy of $Z$, and similarly with $v^{(1)}$, $u^{(2)}$, and $v^{(2)}$.) Then the quotient ring $R_I := (\bar{k}[Z \times Z][x, y]/(y^2 - f(x)))/I$ is a finite $\bar{k}[Z \times Z]$-algebra which, when specialized to any $(D_1, D_2) \in Z \times Z$, is a vector space over $\mathbb{C}$ of dimension $n$. It follows that $R_I$ is locally free of rank $n$ over $\bar{k}[Z \times Z]$, and thus is locally generated over $\bar{k}[Z \times Z]$ by $n$ basis elements – we choose some suitable open subset $U \subset Z \times Z$ and denote these basis elements by $e_1, ..., e_n$.

Let $\mathcal{L}(n(\infty))$ denote the $\bar{k}[Z \times Z]$-module of functions in $\bar{k}[Z \times Z][x, y]/(y^2 - f(x))$ with poles bounded by $n(\infty)$. Now I claim that $(D_1, D_2) \in \Gamma_{T_1,T_2}$ if and only if there is an element in the specialization of $\mathcal{L}(n(\infty))$ at $(D_1, D_2)$ which is also contained in the specialization of $I$ at $(D_1, D_2)$. Indeed, such an element would be a function $h \in k(C)$ whose poles are bounded by $n(\infty)$ and with zeros at the $P_{1,i}$'s and the $P_{2,i}$'s. This forces $(h) = \sum_{i=1}^{g} P_{1,i} + \sum_{j=1}^{g} \iota(P_{2,j}) + \sum_{P \in T_1} P + \sum_{P \in T_2} P - n(\infty)$, as desired. Now, let $\psi : \mathcal{L}(n(\infty)) \to R_I$ be the restriction of the usual quotient map $\bar{k}[Z \times Z] \to R_I$; it is a homomorphism of $\bar{k}[Z \times Z]$ modules. By viewing $\mathcal{L}(n(\infty))$ as a set of polynomials

of certain bounded degrees in $x$ and $y$ (or by using the Riemann-Roch theorem), it is clear that $\mathcal{L}(n(\infty))$ is free of rank $n-g+1$ as a $\bar{k}[Z\times Z]$-module. Let $f_1,...,f_{n-g+1}$ be a basis. Then for $1\leq i\leq n-g+1$, $\psi(f_i)=\sum_{j=1}^{n}c_{i,j}e_j$ for elements $c_{i,j}\in\bar{k}[Z\times Z]$. So $\Gamma_{T_1,T_2}$ is the subset of points $(D_1,D_2)$ such that the specialization of $\psi$ at those points has nontrivial kernel, or equivalently, the matrix $(c_{i,j})$ has rank $\leq n-g$. (Observe that the kernel can have dimension at most 1 since functions in the kernel have the same zeros and poles, and thus, the matrix $(c_{i,j})$ has rank exactly $(n-g)$.) Thus, $\Gamma_{T_1,T_2}\cap U$ can be defined by polynomial functions and is Zariski closed in $U\subset Z\times Z$. Since this can be done for any open $U$ in an open cover of $Z\times Z$, we have shown that $\Gamma_{T_1,T_2}$ is Zariski closed in $Z\times Z$.

The fact that for $(D_1,D_2)\in\Gamma_{T_1,T_2}$, $(c_{i,j})$ has rank exactly $n-g$ can be used to show that $\Gamma_{T_1,T_2}$ is cut out by $g$ polynomials in $Z\times Z$ and is therefore of dimension $2g-g=g$. Since projection to each copy of $Z$ is injective on $\Gamma_{T_1,T_2}$, the images of these projections are $g$-dimensional subsets of $Z$ and therefore (using Zariski's Main Theorem) open subsets of $Z$.

□

We have now constructed a variety $J$ whose $\bar{k}$-points are in bijection with $\mathrm{Pic}^0(C)$.

**Proposition 1.8.** *$J$ is an abelian variety (that is, $J$ is a group variety which is complete).*

*Proof.* Let $m:J\times J\to J$ be the addition map on elements of the abelian group $\mathrm{Pic}^0(C)$. In order to show that $m$ is a morphism, it suffices to show that the graph of $m$ in $J\times J\times J$ is Zariski closed. For any subsets $T_1,T_2,T_3\subset B$ of even cardinality, the intersection of this graph with $(Z+D_{T_1})\times(Z+D_{T_2})\times(Z+D_{T_3})$ is isomorphic to

$$\Gamma_{T_1,T_2,T_3}:=\{(D_1,D_2,D_3)\in Z\times Z\times Z\mid D_1+D_{T_1}+D_2+D_{T_2}\equiv D_3+D_{T_3}\}.$$

It therefore suffices to show that each $\Gamma_{T_1,T_2,T_3}$ is Zariski closed in $Z\times Z\times Z$. But this can be proven in the same way that the first statement of Proposition 1.7 is proven. Thus, $J$ is a group variety.

Finally, since Proposition 1.2 implies that $J$ is the surjective image of $C^g$, and $C^g$ is complete, $J$ is complete.

□

So far we have done everything over $\bar{k}$; we now want to descend to $k$. Let $G_k$ denote the absolute Galois group of $k$; note $G_k$ acts on $\mathrm{Div}_k(C)$ by acting in the obvious way on each point in $C(\bar{k})$. Let $\mathrm{Div}_k(C)$ (resp. $\mathrm{Div}_k^0(C)$ be the subgroup of $\mathrm{Div}(C)$ (resp. $\mathrm{Div}^0(C)$ of divisors which are fixed by all elements of $G_k$. Now note that if $h \in \bar{k}(C)$, the principal divisor $(h)$ lies in $\mathrm{Div}_k^0(C)$ if and only if $h \in k(C)$. Therefore, we may define $\mathrm{Pic}_k^0(C)$ to be the quotient of $\mathrm{Div}_k^0(C)$ by the subgroup of principal divisors $(h)$ for all $h \in k(C)$.

**Proposition 1.9.** *In the bijection between* $\mathrm{Pic}^0(C)$ *and* $J(\bar{k})$ *established in the above discussion, the elements of* $\mathrm{Pic}_k^0(C)$ *correspond to the points in* $J(k)$.

*Proof.* It is enough to show this for $Z$, the translates of which cover $J$. In other words, we must show that the elements of $\mathrm{Pic}_k^0$ which can be written as $\sum_{i=1}^g P_i - g(\infty)$ with $P_i \neq \infty$ and $P_i \neq \iota(P_j)$ for $i \neq j$ are in bijection with the points in $Z(k)$ when $Z$ is given the structure of affine variety as above. But since $G_k$ permutes the points $\{P_i\}$, clearly $G_k$ fixes the coefficients of the polynomial $u$. Now choose any $\sigma \in G_k$; clearly the polynomial $v$ sends each $x(\sigma(P_i))$ to $y(\sigma(P_i))$. Since there is a unique such polynomial of degree $\leq g-1$, it follows that $\sigma$ fixes $v$ as well. Thus, all elements of $G_k$ fix the coordinates of the point corresponding to $\sum_{i=1}^g P_i - g(\infty)$ in $Z(\bar{k})$, and so this point lies in $Z(k)$.

□

So $J$ is the desired abelian variety associated to $C$, the *Jacobian* of $C$.

## 1.5 2-torsion of the Jacobian

As in the above discussion, for each subset $T \subset B$ of even cardinality, $2D_T$ is a principal divisor, and hence, the divisor class of $D_T$ is a 2-torsion point in $\mathrm{Pic}^0(C)$ (so the corresponding point in $J$ is a 2-torsion point of $J$). Of course, it is natural to ask whether all 2-torsion points of $J$ can be described this way.

**Proposition 1.10.** *Each 2-torsion element of* $\mathrm{Pic}^0(C)$ *can be represented by a divisor of the form* $D_T$ *for a unique subset* $T \subset B$ *of even cardinality. Thus, the 2-torsion subgroup* $J[2]$ *of* $J(\bar{k})$ *is in bijection with the set of subsets* $T \in B$ *of even cardinality.*

*Proof.* Let $D \in \mathrm{Div}^0(C)$ represent a 2-torsion element of $\mathrm{Pic}^0(C)$; we will first show that $D \equiv D_T$ for some subset $T \subset B$ of even cardinality. By Proposition 1.2, we may assume $D = \sum_{i=1}^{m} P_i - m(\infty)$ with $P_i \neq \infty$, $P_i \neq \iota(P_j)$ for $i \neq j$. Since $2D \equiv 0$, $\sum_{i=1}^{m} 2P_i - 2m(\infty)$ is the divisor of a function $h$. The poles of $h$ are bounded by $2m(\infty)$, and $2m \leq 2g$, so by a similar argument as in the proof of Proposition 1.2, $h$ must be a polynomial in $x$. Note that a polynomial in $x$ has a zero at a point $P$ if and only if it has a zero at $\iota(P)$. So since the zeros of $h$ are all of even multiplicity and no zero is the image under $\iota$ of another zero, $h$ has zeros only at points $P \neq \infty$, $P = \iota(P)$, that is, at branch points. It follows that $P_1, ..., P_m$ are distinct branch points. If $m$ is even, then let $T = \{P_i\}$ and we are done. If $m$ is odd, then let $T = B \backslash \{P_i\}$ and note that $D_T = (y) - D \equiv -D \equiv D$, and we are done.

Now let $T_1, T_2 \subset B$ be subsets of even cardinality, and assume that $D_{T_1} \equiv D_{T_2}$. Note that $D_{T_1} - D_{T_2} \equiv D_{T_3}$, where $T_3 = (T_1 \cup T_2) \backslash (T_1 \cap T_2)$. Clearly, $T_3$ is also a subset of even cardinality. If $\#T_3 > g$, one may replace $T_3$ with $B \backslash T_3$ (note as above that this does not change the divisor class). So without loss of generality, assume that $\#T_3 \leq g$. We have $D_{T_3} \equiv 0$, so $D_{T_3} = \sum_{P \in T_3} P - \#T_3(\infty)$ is the divisor of a function $h$. Since the poles of $h$ are bounded by $\#T_3(\infty)$ and $\#T_3 \leq g$, again $h$ must be a polynomial of in $x$. Since $h$ has a zero at each point $P \in T_3$, $h$ must be divisible by $\prod_{P \in T_3}(x - x(P))$, which has double zeros at each $P \in T_3$, which produces a contradiction if $T_3$ is nonempty. Thus, $T_3 = (T_1 \cup T_2) \backslash (T_1 \cap T_2)$ is empty, so $T_1 = T_2$, implying that each divisor class in the 2-torsion of $\mathrm{Pic}^0(C)$ is represented uniquely by $D_T$.

□

**Corollary 1.11.** *The extension $k(J[2])/k$ over which the points in $J[2]$ are defined is $k(\alpha_1, ..., \alpha_{2g+1})$. Thus, $\mathrm{Gal}(k(J[2])/k)$ is the Galois group of the polynomial $f$.*

*Proof.* This follows immediately from the fact that the subgroup of the absolute Galois group $G_k$ stabilizing all elements of the form $D_T$ is the subgroup which fixes every element in the set of branch points $B = \{(\alpha_i, 0)\}$.

□

**Remark 1.12.** In the case that $f$ has even degree $2g+2$, one can show using a similar argument that all elements of $J[2]$ correspond to divisor classes represented by divisors of the form $\sum_{P \in T} P - \frac{\#T}{2}\infty_1 - \frac{\#T}{2}\infty_2$, where $T \subset B$ is a subset of even cardinality, and $\infty_1, \infty_2$ are the two points at infinity. Note

that $T$ can be replaced by $T \backslash B$ (also of even cardinality) without changing the divisor class, and in fact, there is a bijection between the elements of $J[2]$ and partitions of $B$ into two subsets of even cardinality. As is similar to the odd-degree case, for $g \neq 1$, it can be shown as a corollary that $k(J[2]) = k(\alpha_1, ..., \alpha_{2g+2})$ and $\mathrm{Gal}(k(J[2])/k)$ is the Galois group of the polynomial $f$. For $g = 1$, however, $k(J[2])$ is the fixed subfield of $k(\alpha_1, ..., \alpha_4)$ corresponding to the subgroup of the Galois group of $f$ of permutations whose cycle type is $(2, 2)$, and $\mathrm{Gal}(k(J[2])/k)$ is isomorphic the corresponding quotient group. This results from the fact that a nontrivial subgroup of permutations on 4 objects fixes all of its partitions into two subsets of 2 objects. Note that for a "general" choice of degree-4 polynomial $f$, $\mathrm{Gal}(f) \cong S_4$, and the subgroup fixing $k(J[2])$ is $\{(12)(34), (13)(24), (14)(23), 1\} \lhd S_4$, so $\mathrm{Gal}(k(J[2])/k) \cong S_4/\{(12)(34), (13)(24), (14)(23), 1\} \cong S_3$.