CHAPTER VII

Jacobian Varieties

J. S. Milne

This chapter contains a detailed treatment of Jacobian varieties. Sections 2, 5, and 6 prove the basic properties of Jacobian varieties starting from the definition in Section 1, while the construction of the Jacobian is carried out in Sections 3 and 4. The remaining sections are largely independent of one another.

The conventions are the same as those listed at the start of Chapter V, "Abelian Varieties" (see also those at the start of Section 5 of that chapter).

§1. Definitions

Recall that for a scheme S, $\mathrm{Pic}(S)$ denotes the group $H^1(S, \mathcal{O}_S^\times)$ of isomorphism classes of invertible sheaves on S, and that $S \mapsto \mathrm{Pic}(S)$ is a functor from the category of schemes over k to that of abelian groups.

Let C be a complete nonsingular curve over k. The degree of a divisor $D = \sum n_i P_i$ on C is $\sum n_i [k(P_i) : k]$. Since every invertible sheaf $\mathcal{L}$ on C is of the form $\mathcal{L}(D)$ for some divisor D, and D is uniquely determined up to linear equivalence, we can define $\deg(\mathcal{L}) = \deg(D)$. Then $\deg(\mathcal{L}^n) = \deg(nD) = n \cdot \deg(D)$, and the Riemann–Roch theorem says that

$$\chi(C, \mathcal{L}^n) = n \cdot \deg(\mathcal{L}) + 1 - g.$$

This gives a more canonical description of $\deg(\mathcal{L})$: when $\chi(C, \mathcal{L}^n)$ is written as a polynomial in n, $\deg(\mathcal{L})$ is the leading coefficient. We write $\mathrm{Pic}^0(C)$ for the group of isomorphism classes of invertible sheaves of degree 0 on C.

Let T be a connected scheme over k, and let $\mathcal{L}$ be an invertible sheaf on $C \times T$ (by which we mean $C \times_{\mathrm{spec}(k)} T$). Then [14, 4.2(b)] shows that

$\chi(C_t, \mathscr{L}_t^n)$, and therefore $\deg(\mathscr{L}_t)$, is independent of t; moreover, the constant degree of $\mathscr{L}_t$ is invariant under base change relative to maps $T' \to T$. Note that for a sheaf $\mathscr{M}$ on $C \times T$, $(q^*\mathscr{M})_t$ is isomorphic to $\mathcal{O}_{C_t}$ and, in particular, has degree 0. Let

$$P_C^0(T) = \{\mathscr{L} \in \operatorname{Pic}(C \times T) | \deg(\mathscr{L}_t) = 0 \text{ all } t\}/q^* \operatorname{Pic}(T).$$

We may think of $P_C^0(T)$ as being the group of families of invertible sheaves on C of degree 0 parametrized by T, modulo the trivial families. Note that P_C^0 is a functor from schemes over k to abelian groups. It is this functor that the Jacobian attempts to represent.

Theorem 1.1. *There is an abelian variety J over k and a morphism of functors $\iota: P_C^0 \to J$ such that $\iota: P_C^0(T) \to J(T)$ is an isomorphism whenever $C(T)$ is nonempty.*

Let k' be a finite Galois extension of k such that $C(k')$ is nonempty, and let G be the Galois group of k' over k. Then for every scheme T over k, $C(T_{k'})$ is nonempty, and so $\iota(T_{k'})$: $P_C^0(T_{k'}) \to J(T_{k'})$ is an isomorphism. As

$$J(T) \overset{\text{df}}{=} \operatorname{Mor}_k(T, J) = \operatorname{Mor}_{k'}(T_{k'}, J_{k'})^G = J(T_{k'})^G,$$

we see that J represents the functor $T \mapsto P_C^0(T_{k'})^G$, and this implies that the pair (J, ι) is uniquely determined up to a unique isomorphism by the condition in the theorem. The variety J is called the *Jacobian variety* of C. Note that for any field $k' \supset k$ in which C has a rational point, ι defines an isomorphism $\operatorname{Pic}^0(C) \overset{\approx}{\to} J(k')$.

When C has a k-rational point, the definition takes on a more attractive form. A *pointed k-scheme* is a connected k-scheme S together with an element $s \in S(k)$. Abelian varieties will always be regarded as being pointed by the zero element. A *divisorial correspondence* between two pointed schemes (S, s) and (T, t) over k is an invertible sheaf $\mathscr{L}$ on $S \times T$ such that $\mathscr{L}|S \times \{t\}$ and $\mathscr{L}|\{s\} \times T$ are both trivial.

Theorem 1.2. *Let P be a k-rational point on C. Then there is a divisorial correspondence $\mathscr{M}^P$ between (C, P) and J such that, for every divisorial correspondence $\mathscr{L}$ between (C, P) and a pointed k-scheme (T, t), there exists a unique morphism $\varphi: T \to J$ such that $\varphi(t) = 0$ and $(1 \times \varphi)^*\mathscr{M}^P \approx \mathscr{L}$.*

Regard $\mathscr{M}^P$ as an element of $\operatorname{Pic}(C \times J)$; then the pair $(J, \mathscr{M}^P)$ is uniquely determined up to a unique isomorphism by the condition in (1.2). Note that each element of $\operatorname{Pic}^0(C)$ is represented by exactly one sheaf $\mathscr{M}_a$, $a \in J(k)$, and the map $\varphi: T \to J$ sends $t \in T(k)$ to the unique a such that $\mathscr{M}_a \approx \mathscr{L}_t$.

Theorem 1.1 will be proved in Section 4. Here we merely show that it implies (1.2).

Lemma 1.3. *Theorem* 1.1 *implies Theorem* 1.2.

PROOF. Assume there is a k-rational point P on C. Then for any k-scheme T, the projection $q: C \times T \to T$ has a section $s = (t \mapsto (P, t))$, which induces a map $s^* = (\mathscr{L} \mapsto \mathscr{L}|\{P\} \times T)$: $\operatorname{Pic}(C \times T) \to \operatorname{Pic}(T)$ such that $s^* \circ q^* = \text{id}$. Consequently, $\operatorname{Pic}(C \times T) = \operatorname{Im}(q^*) \oplus \operatorname{Ker}(s^*)$, and so $P_C^0(T)$ can be identified with

$$P'(T) = \{\mathscr{L} \in \operatorname{Pic}(C \times T) | \deg(\mathscr{L}_t) = 0 \text{ all } t, \mathscr{L}|\{P\} \times T \text{ is trivial}\}.$$

Now assume (1.1). As $C(T)$ is nonempty for all k-schemes T, J represents the functor $P_C^0 = P'$. This means that there is an element $\mathscr{M}$ of $P'(J)$ (corresponding to id: $J \to J$ under ι) such that, for every k-scheme T and $\mathscr{L} \in P'(T)$, there is a unique morphism $\varphi: T \to J$ such that $(1 \times \varphi)^*\mathscr{M} \approx \mathscr{L}$. In particular, for each invertible sheaf $\mathscr{L}$ on C of degree 0, there is a unique $a \in J(k)$ such that $\mathscr{M}_a \approx \mathscr{L}$. After replacing $\mathscr{M}$ with $(1 \times t_a)^*\mathscr{M}$ for a suitable $a \in J(k)$, we can assume that $\mathscr{M}_0$ is trivial, and therefore that $\mathscr{M}$ is a divisorial correspondence between (C, P) and J. It is clear that $\mathscr{M}$ has the universal property required by (1.2). □

Exercise 1.4. Let $(J, \mathscr{M}^P)$ be a pair having the universal property in (1.2) relative to some point P on C. Show that J is the Jacobian of C.

We next make some remarks concerning the relation between P_C^0 and J in the case that C does not have a k-rational point.

Remark 1.5. For all k-schemes T, $\iota(T)$: $P_C^0(T) \to J(T)$ is injective. The proof of this is based on two observations. Firstly, because C is a complete variety $H^0(C, \mathcal{O}_C) = k$, and this holds universally: for any k-scheme T, the canonical map $\mathcal{O}_T \to q_*\mathcal{O}_{C \times T}$ is an isomorphism. Secondly, for any morphism $q: X \to T$ of schemes such that $\mathcal{O}_T \overset{\approx}{\to} q_*\mathcal{O}_X$, the functor $\mathscr{M} \mapsto q^*\mathscr{M}$ from the category of locally free $\mathcal{O}_T$-modules of finite-type to the category of locally free $\mathcal{O}_X$-modules of finite-type is fully faithful, and the essential image is formed of those modules $\mathscr{F}$ on X such that $q_*\mathscr{F}$ is locally free and the canonical map $q^*(q_*\mathscr{F}) \to \mathscr{F}$ is an isomorphism. (The proof is similar to that of [14, 5.1].)

Now let $\mathscr{L}$ be an invertible sheaf on $C \times T$ that has degree 0 on the fibres and which maps to zero in $J(T)$; we have to show that $\mathscr{L} \approx q^*\mathscr{M}$ for some invertible sheaf $\mathscr{M}$ on T. Let k' be a finite extension of k such that C has a k'-rational point, and let $\mathscr{L}'$ be the inverse image of $\mathscr{L}$ on $(C \times T)_{k'}$. Then $\mathscr{L}'$ maps to zero in $J(T_{k'})$, and so (by definition of J) we must have $\mathscr{L}' \approx q^*\mathscr{M}'$ for some invertible sheaf $\mathscr{M}'$ on $T_{k'}$. Therefore $q_*\mathscr{L}'$ is locally free of rank one on $T_{k'}$, and the canonical map $q^*(q_*\mathscr{L}') \to \mathscr{L}'$ is an isomorphism. But $q_*\mathscr{L}'$ is the inverse image of $q_*\mathscr{L}$ under $T' \to T$ (see [14, 4.2a]), and elementary descent theory (cf. (1.8) below) shows that the properties of $\mathscr{L}'$ in the last sentence descend to $\mathscr{L}$; therefore $\mathscr{L} \approx q^*\mathscr{M}$ with $\mathscr{M} = q_*\mathscr{L}$.

Remark 1.6. It is then sometimes possible to compute the cokernel to $\iota: P_C^0(k) \to J(k)$. There is always an exact sequence

$$0 \to P_C^0(k) \to J(k) \to \operatorname{Br}(k),$$

where Br(k) is the Brauer group of k. When k is a finite extension of $\mathbb{Q}_p$, $\mathrm{Br}(k) = \mathbb{Q}/\mathbb{Z}$, and it is known (see [11, p. 130]) that the image of $J(k)$ in $\mathrm{Br}(k)$ is $P^{-1}\mathbb{Z}/\mathbb{Z}$, where P (the *period* of C) is the greatest common divisor of the degrees of the k-rational divisor classes on C.

Remark 1.7. Regard P_C^0 as a presheaf on the large étale site over C; then the precise relation between J and P_C^0 is that J represents the sheaf associated with P_C^0 (see [6, §5]).

Finally, we show that it suffices to prove (1.1) after an extension of the base field. For the sake of reference, we first state a result from descent theory. Let k' be a finite Galois extension of a field k with Galois group G, and let V be a variety over k'. A *descent datum* for V relative to k'/k is a collection of isomorphisms $\varphi_\sigma: \sigma V \to V$, one for each $\sigma \in G$, such that $\varphi_{\tau\sigma} = \varphi_\tau \circ \tau\varphi_\sigma$ for all σ and τ. There is an obvious notion of a morphism of varieties preserving the descent data. Note that for a variety V over k, $V_{k'}$ has a canonical descent datum. If V is a variety over k and $V' = V_{k'}$, then a descent datum on an $\mathcal{O}_{V'}$-module $\mathcal{M}$ is a family of isomorphisms $\varphi_\sigma: \sigma\mathcal{M} \to \mathcal{M}$ such that $\varphi_{\tau\sigma} = \varphi_\tau \circ \tau\varphi_\sigma$ for all σ and τ.

Proposition 1.8. *Let k'/k be a finite Galois extension with Galois group G.*

(a) *The map sending a variety V over k to $V_{k'}$ endowed with its canonical descent datum defines an equivalence between the category of quasi-projective varieties over k and that of quasi-projective varieties over k' endowed with a descent datum.*

(b) *Let V be a variety over k, and let $V' = V_{k'}$. The map sending an $\mathcal{O}_V$-module $\mathcal{M}$ to $\mathcal{M}' = \mathcal{O}_{V'} \otimes \mathcal{M}$ endowed with its canonical descent datum defines an equivalence between the category of coherent $\mathcal{O}_V$-modules and that of coherent $\mathcal{O}_{V'}$-modules endowed with a descent datum. Moreover, if $\mathcal{M}'$ is locally free, then so also is $\mathcal{M}$.*

PROOF. See [17, V. 20] or [19, §17]. (For the final statement, note that being locally free is equivalent to being flat, and that V' is faithfully flat over V.) □

Proposition 1.9. *Let k' be a finite separable extension of k; if* (1.1) *is true for $C_{k'}$, then it is true for C.*

PROOF. After possibly enlarging k', we can assume that it is Galois over k (with Galois group G, say) and that $C(k')$ is nonempty. Let J' be the Jacobian of $C_{k'}$. Then J' represents $P_{C_{k'}}^0$, and so there is a universal $\mathcal{M}$ in $P_C^0(J')$. For any $\sigma \in G$, $\sigma\mathcal{M} \in P_C^0(\sigma J')$, and so there is a unique map $\varphi_\sigma: \sigma J' \to J'$ such that $(1 \times \varphi_\sigma)^*\mathcal{M} = \sigma\mathcal{M}$ (in $P_C^0(\sigma J')$). One checks directly that $\varphi_{\tau\sigma} = \varphi_\tau \circ \tau\varphi_\sigma$; in particular, $\varphi_\sigma \circ \sigma\varphi_{\sigma^{-1}} = \varphi_{\mathrm{id}}$, and so the φ_σ are isomorphisms and define a descent datum on J'. We conclude from (1.8) that J' has a model J over k such that the map $P_C^0(T_{k'}) \to J(T_{k'})$ is G-equivariant for all k-schemes T. In particular, for all T, there is a map $P_C^0(T) \to P_C^0(T_{k'})^G \xrightarrow{\approx} J(k')^G = J(k)$. To see that the map is an isomorphism when $C(T)$ is nonempty, we have to show that in this case $P_C^0(T) \to P_C^0(T_{k'})^G$ is an isomorphism. Let $s \in C(T)$; then (cf. the proof of (1.3)), we can identify $P_C^0(T_{k'})$ with the set of isomorphism classes of pairs $(\mathcal{L}, \alpha)$ where $\mathcal{L}$ is an invertible sheaf on $C \times T_{k'}$ whose fibres are of degree 0 and α is an isomorphism $\mathcal{O}_{T_{k'}} \xrightarrow{\approx} (1, s)^*\mathcal{L}$. Such pairs are rigid—they have no automorphisms—and so each such pair fixed under G has a canonical descent datum, and therefore arises from an invertible sheaf on $C \times T$. □

§2. The Canonical Maps from C to its Jacobian Variety

Throughout this section, C will be a complete nonsingular curve, and J will be its Jacobian variety (assumed to exist).

Proposition 2.1. *The tangent space to J at 0 is canonically isomorphic to $H^1(C, \mathcal{O}_C)$; consequently, the dimension of J is equal to the genus of C.*

PROOF. The tangent space $T_0(J)$ is equal to the kernel of $J(k[\varepsilon]) \to J(k)$, where $k[\varepsilon]$ is the ring in which $\varepsilon^2 = 0$ (see [8, II, Ex. 2.8]). Analogously, we define the tangent space $T_0(P_C^0)$ to P_C^0 at 0 to be the kernel of $P_C^0(k[\varepsilon]) \to P_C^0(k)$. From the definition of J, we obtain a map of k-linear vector spaces $T_0(P_C^0) \to T_0(J)$ which is an isomorphism if $C(k) \neq \Phi$. Since the vector spaces and the map commute with base change, it follows that the map is always an isomorphism.

Let $C_\varepsilon = C_{k[\varepsilon]}$; then, by definition, $P_C^0(k[\varepsilon])$ is equal to the group of invertible sheaves on C_ε whose restrictions to the closed subscheme C of C_ε have degree zero. It follows that $T_0(P_C^0)$ is equal to the kernel of $H^1(C_\varepsilon, \mathcal{O}_{C_\varepsilon}^\times) \to H^1(C, \mathcal{O}_C^\times)$. The scheme C_ε has the same underlying topological space as C, but $\mathcal{O}_{C_\varepsilon} = \mathcal{O}_C \otimes_k k[\varepsilon] = \mathcal{O}_C \oplus \mathcal{O}_C\varepsilon$. Therefore we can identify the sheaf $\mathcal{O}_{C_\varepsilon}^\times$ on C_ε with the sheaf $\mathcal{O}_C^\times \oplus \mathcal{O}_C\varepsilon$ on C, and so $H^1(C_\varepsilon, \mathcal{O}_{C_\varepsilon}^\times) = H^1(C, \mathcal{O}_C^\times) \oplus H^1(C, \mathcal{O}_C\varepsilon)$. It follows that the map $a \mapsto \exp(a\varepsilon) = 1 + a\varepsilon$, $\mathcal{O}_C \to \mathcal{O}_{C_\varepsilon}^\times$, induces an isomorphism $H^1(C, \mathcal{O}_C) \to T_0(P_C^0)$. This completes the proof. □

Let $P \in C(k)$, and let $\mathcal{L}^P$ be the invertible sheaf $\mathcal{L}(\Delta - C \times \{P\} - \{P\} \times C)$ on $C \times C$, where Δ denotes the diagonal. Note that $\mathcal{L}^P$ is symmetric and that $\mathcal{L}^P | C \times \{Q\} \approx \mathcal{L}(Q - P)$. In particular, $\mathcal{L}^P | \{P\} \times C$ and $\mathcal{L}^P | C \times \{P\}$ are both trivial, and so $\mathcal{L}^P$ is a divisorial correspondence between (C, P) and itself. Therefore, according to (1.2) there is a unique map $f^P: C \to J$ such that $f^P(P) = 0$ and $(1 \times f^P)^*\mathcal{M}^P \approx \mathcal{L}^P$. When $J(k)$ is identified with $\mathrm{Pic}^0(C)$,

$f^P\colon C(k)\to J(k)$ becomes identified with the map $Q\mapsto \mathscr{L}(Q)\otimes\mathscr{L}(P)^{-1}$ (or, in terms of divisors, the map sending Q to the linear equivalence class $[Q-P]$ of $Q-P$). Note that the map $\sum n_Q Q\mapsto \sum n_Q f^P(Q) = [\sum n_Q Q]$ from the group of divisors of degree zero on C to $J(k)$ induced by f^P is simply the map defined by ι. In particular, it is independent of P, is surjective, and its kernel consists of the principal divisors.

From its definition (or from the above descriptions of its action on the points) it is clear that if P' is a second point on C, then $f^{P'}$ is the composite of f^P with the translation map $t_{[P-P']}$, and that if P is defined over a Galois extension k' of k, then $\sigma f^P = f^{\sigma P}$ for all $\sigma\in \mathrm{Gal}(k'/k)$.

If C has genus zero, then (2.1) shows that $J=0$. From now on we assume that C has genus $g>0$.

Proposition 2.2. *The map $(f^P)^*\colon \Gamma(J,\Omega^1_J)\to\Gamma(C,\Omega^1_C)$ is an isomorphism.*

PROOF. As for any group variety, the canonical map $h_J\colon \Gamma(J,\Omega^1_J)\to T_0(J)^\vee$ is an isomorphism [18, III, 5.2]. Also there is a well-known duality between $\Gamma(C,\Omega^1_C)$ and $H^1(C,\mathcal{O}_C)$. We leave it as an exercise to the reader (unfortunately rather complicated) that the following diagram commutes:

$$\begin{array}{ccc} \Gamma(J,\Omega^1_J) & \xrightarrow{f^*} & \Gamma(C,\Omega^1_C)\\ h_J\downarrow\approx & & \downarrow\approx \\ T_0(J)^\vee & \xrightarrow{\approx} & H^1(C,\mathcal{O}_C)^\vee \end{array} \qquad \text{(dual of isomorphism in (2.1)).}$$

Proposition 2.3. *The map f^P is a closed immersion (that is, its image $f^P(C)$ is closed and f^P is an isomorphism from C onto $f^P(C)$); in particular, $f^P(C)$ is nonsingular.*

PROOF. It suffices to prove this in the case that k is algebraically closed.

Lemma 2.4. *Let $f\colon V\to W$ be a map of varieties over an algebraically closed field k, and assume that V is complete. If the map $V(k)\to W(k)$ defined by f is injective and, for all closed points Q of V, the map on tangent spaces $T_Q(V)\to T_{fQ}(W)$ is injective, then f is a closed immersion.*

PROOF. The proof is the same as that of the "if" part of [8, II, 7.3]. (Briefly, the image of f is closed because V is complete, and the condition on the tangent spaces (together with Nakayama's lemma) shows that the maps $\mathcal{O}_{fQ}\to\mathcal{O}_Q$ on the local rings are surjective.) □

We apply the lemma to $f=f^P$. If $f(Q)=f(Q')$ for some Q and Q' in $C(k)$, then the divisors $Q-P$ and $Q'-P$ are linearly equivalent. This implies that $Q-Q'$ is linearly equivalent to zero, which is impossible if $Q\neq Q'$ because C has genus >0. Consequently, f is injective, and it remains to show that

the maps on tangent spaces $(df^P)_Q\colon T_Q(C)\to T_{fQ}(J)$ are injective. Because f^Q differs from f^P by a translation, it suffices to do this in the case that $Q=P$. The dual of $(df^P)_P\colon T_P(C)\to T_0(J)$ is clearly $\Gamma(J,\Omega^1)\xrightarrow{f^*}\Gamma(C,\Omega^1)\xrightarrow{h_C}T_P(C)^\vee$, where h_C is the canonical map, and it remains to show that h_C is surjective. The kernel of h_C is $\{\omega\in\Gamma(C,\Omega^1)\mid \omega(P)=0\} = \Gamma(C,\Omega^1(-P))$, which is dual to $H^1(C,\mathscr{L}(P))$. The Riemann–Roch theorem shows that this last group has dimension $g-1$, and so $\mathrm{Ker}(h_C)\neq\Gamma(C,\Omega^1)$: h_C is surjective, and the proof is complete. □

We now assume that $k=\mathbb{C}$ and sketch the relation between the abstract and classical definitions of the Jacobian. In this case, $\Gamma(C(\mathbb{C}),\Omega^1)$ (where Ω^1 denotes the sheaf of holomorphic differentials in the sense of complex analysis) is a complex vector space of dimension g, and one shows in the theory of abelian integrals that the map $\sigma\mapsto(\omega\mapsto\int_\sigma\omega)$ embeds $H_1(C(\mathbb{C}),\mathbb{Z})$ as a lattice into the dual space $\Gamma(C(\mathbb{C}),\Omega^1)^\vee$. Therefore $J^{an}\overset{\mathrm{df}}{=}\Gamma(C(\mathbb{C}),\Omega^1)^\vee/H_1(C(\mathbb{C}),\mathbb{Z})$ is a complex torus, and the pairing

$$H_1(C(\mathbb{C}),\mathbb{Z})\times H_1(C(\mathbb{C}),\mathbb{Z})\to\mathbb{Z}$$

defined by Poincaré duality gives a nondegenerate Riemann form on J^{an}. Therefore J^{an} is an abelian variety over $\mathbb{C}$. For each P there is a canonical map $g^P\colon C\to J^{an}$ sending a point Q to the element represented by $(\omega\mapsto\int_\gamma\omega)$, where γ is any path from P to Q. Define $e\colon\Gamma(C(\mathbb{C}),\Omega^1)^\vee\to J(\mathbb{C})$ to be the surjection in the diagram:

$$\begin{array}{ccc} \Gamma(C(\mathbb{C}),\Omega^1)^\vee & \twoheadrightarrow & J(\mathbb{C})\\ f^{*\vee}\downarrow\approx & & \uparrow\exp \\ \Gamma(J,\Omega^1)^\vee & \xrightarrow{\approx} & T_0(J). \end{array}$$

Note that if $\Gamma(C(\mathbb{C}),\Omega^1)^\vee$ is identified with $T_P(C)$, then $(de)_0=(df^P)_P$. It follows that if γ is a path from P to Q and $l=(\omega\mapsto\int_\gamma\omega)$, then $e(l)=f^P(Q)$.

Theorem 2.5. *The canonical surjection $e\colon\Gamma(C(\mathbb{C}),\Omega^1)^\vee\twoheadrightarrow J(\mathbb{C})$ induces an isomorphism $J^{an}\to J$ carrying g^P into f^P.*

PROOF. We have to show that the kernel of e is $H_1(C(\mathbb{C}),\mathbb{Z})$, but this follows from Abel's theorem and the Jacobi inversion theorem.

(Abel) Let $P_1,\dots,P_r$ and $Q_1,\dots,Q_r$ be elements of $C(\mathbb{C})$; then there is a meromorphic function on $C(\mathbb{C})$ with its poles at the P_i and its zeros at the Q_i if and only if for any paths γ_i from P to P_i and γ_i' from P to Q_i there exists a γ in $H_1(C(\mathbb{C}),\mathbb{Z})$ such that

$$\sum\int_{\gamma_i}\omega-\sum\int_{\gamma_i'}\omega=\int_\gamma\omega\quad\text{all }\omega.$$

(Jacobi) Let l be a linear mapping $\Gamma(C(\mathbb{C}),\Omega^1)\to\mathbb{C}$. Then there exist g

points $P_1, \ldots, P_g$ on $C(\mathbb{C})$ and paths $\gamma_1, \ldots, \gamma_g$ from P to P_i such that $l(\omega) = \sum \int_{\gamma_i} \omega$ for all $\omega \in \Gamma(C(\mathbb{C}), \Omega^1)$.

Let $l \in \Gamma(C(\mathbb{C}), \Omega^1)^\vee$; we may assume it is defined by g points $P_1, \ldots, P_g$. Then l maps to zero in $J(\mathbb{C})$ if and only if the divisor $\sum P_i - gP$ is linearly equivalent to zero, and Abel's theorem shows that this is equivalent to l lying in $H_1(C(\mathbb{C}), \mathbb{Z})$. □

§3. The Symmetric Powers of a Curve

Both in order to understand the structure of the Jacobian, and as an aid in its construction, we shall need to study the symmetric powers of C.

For any variety V, the symmetric group S_r on r letters acts on the product of r copies V^r of V by permuting the factors, and we want to define the rth symmetric power $V^{(r)}$ of V to be the quotient $S_r \backslash V^r$. The next proposition demonstrates the existence of $V^{(r)}$ and lists its main properties.

A morphism $\varphi\colon V^r \to T$ is said to be *symmetric* if $\varphi \circ \sigma = \varphi$ for all σ in S_r.

Proposition 3.1. *Let V be a variety over k. Then there is a variety $V^{(r)}$ and a symmetric morphism $\pi\colon V^r \to V^{(r)}$ having the following properties:*

(a) *as a topological space, $(V^{(r)}, \pi)$ is the quotient of V^r by S_r;*
(b) *for any open affine subset U of V, $U^{(r)}$ is an open affine subset of $V^{(r)}$ and $\Gamma(U^{(r)}, \mathcal{O}_{V^{(r)}}) = \Gamma(U^r, \mathcal{O}_{V^r})^{S_r}$ (set of elements fixed by the action of S_r).*

The pair $(V^{(r)}, \pi)$ has the following universal property: every symmetric k-morphism $\varphi\colon V^r \to T$ factors uniquely through π.

The map π is finite, surjective, and separable.

This doesn't work. Must write V^r as a union of open affines.

PROOF. If V is affine, say $V = \operatorname{spec} A$, define $V^{(r)}$ to be $\operatorname{spec}((A \otimes_k \cdots \otimes_k A)^{S_r})$. In the general case, write V as a union $\bigcup U_i$ of open affines, and construct $V^{(r)}$ by patching together the $U_i^{(r)}$. See [16, II, §7, p. 66 and III, §11, p. 112] for the details. □

The pair $(V^{(r)}, \pi)$ is uniquely determined up to a unique isomorphism by the conditions of the proposition. It is called the rth *symmetric power* of V.

Proposition 3.2. *The symmetric power $C^{(r)}$ of a nonsingular curve is nonsingular.*

PROOF. We may assume that k is algebraically closed. The most likely candidate for a singular point on $C^{(r)}$ is the image of Q of a fixed point $(P, \ldots, P)$ of S_r on C^r, where P is a closed point of C. The completion $\hat{\mathcal{O}}_P$ of the local ring at P is isomorphic to $k[[X]]$, and so

$$\hat{\mathcal{O}}_{(P,\ldots,P)} \approx k[[X]] \hat{\otimes} \ldots \hat{\otimes} k[[X]] \approx k[[X_1, \ldots, X_r]].$$

It follows that $\hat{\mathcal{O}}_Q \approx k[[X_1, \ldots, X_r]]^{S_r}$ where S_r acts by permuting the variables. The fundamental theorem on symmetric functions says that, over any ring, a symmetric polynomial can be expressed as a polynomial in the elementary symmetric functions $\sigma_1, \ldots, \sigma_r$. This implies that

$$k[[X_1, \ldots, X_r]]^{S_r} = k[[\sigma_1, \ldots, \sigma_r]],$$

which is regular, and so Q is nonsingular.

For a general point $Q = \pi(P, P, \ldots, P', \ldots)$ with P occuring r' times, P' occuring r'' times, and so on,

$$\hat{\mathcal{O}}_Q \approx k[[X_1, \ldots, X_{r'}]]^{S_{r'}} \hat{\otimes} k[[X_1, \ldots, X_{r''}]]^{S_{r''}} \hat{\otimes} \ldots,$$

which the same argument shows to be regular. □

Remark 3.3. The reader may find it surprising that the fixed points of the action of S_r on C^r do not force singularities on $C^{(r)}$. The following remarks may help clarify the situation. Let G be a finite group acting effectively on a nonsingular variety V, and suppose that the quotient variety $W = G \backslash V$ exists. Then $V \to W$ is ramified exactly at the fixed points of the action. A purity theorem [5, X, 3.1] says W can be nonsingular only if the ramification locus is empty or has pure codimension 1 in V. As the ramification locus of V^r over $V^{(r)}$ has pure codimension $\dim(V)$, this implies that $V^{(r)}$ can be nonsingular only if V is a curve.

Let K be field containing k. If K is algebraically closed, then (3.1a) shows that $C^{(r)}(K) = S_r \backslash C(K)^r$, and so a point of $C^{(r)}$ with coordinates in K is an unordered r-tuple of K-rational points. This is the same thing as an effective divisor of degree r on C_K. When K is perfect, the divisors on C_K can be identified with those on $C_{\bar{K}}$ fixed under the action of $\mathrm{Gal}(\bar{K}/K)$. Since the same is true of the points on $C^{(r)}$, we see again that $C^{(r)}(K)$ can be identified with the set of effective divisors of degree r on C. In the remainder of this section we shall show that $C^{(r)}(T)$ has a similar interpretation for any k-scheme. (Since this is mainly needed for the construction of J, the reader more interested in the properties of J can pass to the Section 5.)

Let X be a scheme over k. Recall [8, II, 6, p. 145] that a Cartier divisor D is *effective* if it can be represented by a family $(U_i, g_i)_i$ with the g_i in $\Gamma(U_i, \mathcal{O}_X)$. Let $\mathcal{I}(D)$ be the subsheaf of $\mathcal{O}_X$ such that $\mathcal{I}(D)|U_i$ is generated by g_i. Then $\mathcal{I}(D) = \mathcal{L}(-D)$, and there is an exact sequence

$$0 \to \mathcal{I}(D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0,$$

where $\mathcal{O}_D$ is the structure sheaf of the closed subscheme of X associated with D. The closed subschemes arising from effective Cartier divisors are precisely those whose sheaf of ideals can be locally generated by a single element that is not a zero-divisor. We shall often identify D with its associated closed subscheme.

For example, let $T = \mathbb{A}^1 = \operatorname{Spec} k[Y]$, and let D be the Cartier divisor associated with the Weil divisor nP, where P is the origin. Then D is represented by $(Y^n, \mathbb{A}^1)$, and the associated subscheme is $\operatorname{Spec}(k[Y]/(Y^n))$.

Definition 3.4. Let $\pi: X \to T$ be a morphism of k-schemes. A *relative effective Cartier divisor* on X/T is a Cartier divisor on X that is flat over T when regarded as a subscheme of X.

Loosely speaking, the flatness condition means that the divisor has no vertical components, that is, no components contained in a fibre. When T is affine, say $T = \operatorname{spec}(R)$, then a subscheme D of X is a relative effective Cartier divisor if and only if there exists an open affine covering $X = \bigcup U_i$ and $g_i \in \Gamma(U_i, \mathcal{O}_X) = R_i$ such that:

(a) $D \cap U_i = \operatorname{spec}(R_i/g_iR_i)$;
(b) g_i is not a zero-divisor; and
(c) R_i/g_iR_i is flat over R, for all i.

Henceforth all divisors will be Cartier divisors.

Lemma 3.5. *If D_1 and D_2 are relative effective divisors on X/T, then so also is their sum $D_1 + D_2$.*

PROOF. It suffices to prove this in the case that T is affine, say $T = \operatorname{spec}(R)$. We have to check that if conditions (b) and (c) above hold for g_i and g_i', then they also hold for g_ig_i'. Condition (b) is obvious, and the flatness of $R_i/g_ig_i'R_i$ over R follows from the exact sequence

$$0 \to R_i/g_iR_i \xrightarrow{g_i'} R_i/g_ig_i'R_i \to R_i/g_i'R_i \to 0,$$

which exhibits it as an extension of flat modules. □

Remark 3.6. Let D be a relative effective divisor on X/T. On tensoring the inclusion $\mathcal{I}(D) \subset \mathcal{O}_X$ with $\mathcal{L}(D)$ we obtain an inclusion $\mathcal{O}_X \subset \mathcal{L}(D)$ and hence a canonical global section s_D of $\mathcal{L}(D)$. For example, in the case that T is affine and D is represented as in the above example, $\mathcal{L}(D)|U_i$ is $g_i^{-1}R_i$ and $s_D|U_i$ is the identity element in R_i.

The map $D \mapsto (\mathcal{L}(D), s_D)$ defines a one-to-one correspondence between relative effective divisors on X/T and isomorphism classes of pairs $(\mathcal{L}, s)$ where $\mathcal{L}$ is an invertible sheaf on X and $s \in \Gamma(X, \mathcal{L})$ is such that

$$0 \to \mathcal{O}_X \xrightarrow{s} \mathcal{L} \to \mathcal{L}/s\mathcal{O}_X \to 0$$

is exact and $\mathcal{L}/s\mathcal{O}_X$ is flat over T.

Observe that, in the case that X is flat over T, $\mathcal{L}/s\mathcal{O}_X$ is flat over T if and only if, for all t in T, s does not become a zero-divisor in $\mathcal{L} \otimes \mathcal{O}_{X_t}$. (Use that an R-module M is flat if $\operatorname{Tor}_1^R(M, N) = 0$ for all finitely generated modules N, and that any such module N has a composition series whose quotients are the quotient of R by a prime ideal; therefore the criterion has only to be checked with N equal to such a module.)

Proposition 3.7. *Consider the Cartesian square*

$$\begin{array}{ccc} X & \leftarrow & X' \\ \downarrow & & \downarrow \\ T & \leftarrow & T' \end{array}$$

If D is a relative effective divisor on X/T, then its pull-back to a closed subscheme D' of X' is a relative effective divisor on X'/T'.

PROOF. We may assume both T and T' are affine, say $T = \operatorname{spec} R$ and $T' = \operatorname{spec} R'$, and then have to check that the conditions (a), (b), and (c) above are stable under the base change $R \to R'$. Write $U_i' = U_i \times_T T'$; clearly $D' \cap U_i' = \operatorname{spec}(R_i'/g_iR_i')$. The conditions (b) and (c) state that

$$0 \to R_i \xrightarrow{g_i} R_i \to R_i/g_iR_i \to 0$$

is exact and that R_i/g_iR_i is flat over R. Both assertions continue to hold after the sequence has been tensored with R'. □

Proposition 3.8. *Let D be a closed subscheme of X, and assume that D and X are both flat over T. If $D_t \stackrel{\text{df}}{=} D \times_T \{t\}$ is an effective divisor on X_t/t for all points t of T, then D is a relative effective divisor on X.*

PROOF. From the exact sequence

$$0 \to \mathcal{I}(D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0$$

and the flatness of X and D over T, we see that $\mathcal{I}(D)$ is flat over T. The flatness of $\mathcal{O}_D$ implies that, for any $t \in T$, the sequence

$$0 \to \mathcal{I}(D) \otimes_{\mathcal{O}_T} k(t) \to \mathcal{O}_{X_t} \to \mathcal{O}_{D_t} \to 0$$

is exact. In particular, $\mathcal{I}(D) \otimes k(t) \xrightarrow{\approx} \mathcal{I}(D_t)$. As D_t is a Cartier divisor, $\mathcal{I}(D_t)$ (and therefore also $\mathcal{I}(D) \otimes k(t)$) is an invertible $\mathcal{O}_{X_t}$-module. We now apply the fibre-by-fibre criterion of flatness: if X is flat over T and $\mathcal{F}$ is a coherent $\mathcal{O}_X$-module that is flat over T and such that $\mathcal{F}_t$ is a flat $\mathcal{O}_{X_t}$-module for all t in T, then $\mathcal{F}$ is flat over X [2, III, 5.4]. This implies that $\mathcal{I}(D)$ is a flat $\mathcal{O}_X$-module, and since it is also coherent, it is locally free over $\mathcal{O}_X$. Now the isomorphism $\mathcal{I}(D) \otimes k(t) \xrightarrow{\approx} \mathcal{I}(D_t)$ shows that it is of rank one. It is therefore locally generated by a single element, and the element is not a zero-divisor; this shows that D is a relative effective divisor. □

Let $\pi: \mathcal{C} \to T$ be a proper smooth morphism with fibres of dimension one. If D is a relative effective divisor on $\mathcal{C}/T$, then D_t is an effective divisor on $\mathcal{C}_t$, and if T is connected, then the degree of D_t is constant; it is called the *degree* of D. Note that $\deg(D) = r$ if and only if $\mathcal{O}_D$ is a locally free $\mathcal{O}_T$-module of rank r.

Corollary 3.9. *A closed subscheme D of $\mathscr{C}$ is a relative effective divisor on $\mathscr{C}/T$ if and only if it is finite and flat over T; in particular, if $s\colon T \to \mathscr{C}$ is a section to π, then $s(T)$ is a relative effective divisor of degree 1 on $\mathscr{C}/T$.*

PROOF. A closed subscheme of a curve over a field is an effective divisor if and only if it is finite. Therefore (3.8) shows that a closed subscheme D of $\mathscr{C}$ is a relative effective divisor on $\mathscr{C}/T$ if and only if it is flat over T and has finite fibres, but such a subscheme D is proper over T and therefore has finite fibres if and only if it is finite over T (see [13, I, 1.10] or [8, III, Ex. 11.3]). □

If D and D' are relative effective divisors on $\mathscr{C}/T$, then we write $D \geq D'$ if $D \supset D'$ as subschemes of $\mathscr{C}$ (that is, $\mathscr{I}(D) \subset \mathscr{I}(D')$).

Proposition 3.10. *If $D_t \geq D'_t$ (as divisors on C_t) for all t in T, then $D \geq D'$.*

PROOF. Represent D as a pair $(s, \mathscr{L})$ (see 3.6). Then $D \geq D'$ if and only if s becomes zero in $\mathscr{L} \otimes \mathscr{O}_{D'} = \mathscr{L}|D'$. But $\mathscr{L} \otimes \mathscr{O}_{D'}$ is a locally free $\mathscr{O}_T$-module of finite rank, and so the support of s is a closed subscheme of T. The hypothesis implies that this subscheme is the whole of T. □

Let D be a relative effective divisor of degree r on $\mathscr{C}/T$. We shall say that D is *split* if $\mathrm{Supp}(D) = \bigcup s_i(T)$ for some sections s_i to π. For example, a divisor $D = \sum n_i P_i$ on a curve over a field is split if and only if $k(P_i) = k$ for all i.

Proposition 3.11. *Every split relative effective divisor D on $\mathscr{C}/T$ can be written uniquely in the form $D = \sum n_i s_i(T)$ for some sections s_i.*

PROOF. Let $\mathrm{Supp}(D) = \bigcup s_i(T)$, and suppose that the component of D with support on $s_i(T)$ has degree n_i. Then $D_t = (\sum n_i s_i(T))_t$ for all t, and so (3.10) shows that $D = \sum n_i s_i(T)$. □

Example 3.12. Consider a complete nonsingular curve C over a field k. For each i there is a canonical section s_i to $q\colon C \times C^r \to C^r$, namely, $(P_1, \ldots, P_r) \mapsto (P_i, P_1, \ldots, P_r)$. Let D_i to be $s_i(C^r)$ regarded as a relative effective divisor on $C \times C^r/C^r$, and let $D = \sum D_i$. Then D is the unique relative effective divisor $C \times C^r/C^r$ whose fibre over $(P_1, \ldots, P_r)$ is $\sum P_i$. Clearly D is stable under the action of the symmetric group S_r, and $D_{\mathrm{can}} = S_r \backslash D$ (quotient as a subscheme of $C \times C^r$) is a relative effective divisor on $C \times C^{(r)}/C^{(r)}$ whose fibre over $D \in C^{(r)}(k)$ is D.

For C a complete smooth curve over k and T a k-scheme, define $\mathrm{Div}^r_C(T)$ to be the set of relative effective Cartier divisors on $C \times T/T$ of degree r. Proposition 3.7 shows that Div^r_C is a functor on the category of k-schemes.

Theorem 3.13. *For any relative effective divisor D on $C \times T/T$ of degree r, there is a unique morphism $\varphi\colon T \to C^{(r)}$ such that $D = (1 \times \varphi)^{-1}(D_{\mathrm{can}})$. Therefore $C^{(r)}$ represents Div^r_C.*

PROOF. Let us first assume that D is split, so that $D = \sum n_i s_i(T)$ for some sections $s_i\colon T \to C \times T$. In this case, we define $T \to C^r$ to be the map $(p \circ s_1, \ldots, p \circ s_1, p \circ s_2, \ldots)$, where s_i occurs n_i times, and we take φ to be the composite $T \to C^r \to C^{(r)}$. In general, we can choose a finite flat covering $\psi\colon T' \to T$ such that the inverse image D' of D on $C \times T'$ is split, and let $\varphi'\colon T' \to C^{(r)}$ be the map defined by D'. Then the two maps $\varphi' \circ p$ and $\varphi' \circ q$ from $T' \times_T T'$ to $C^{(r)}$ are equal because they both correspond to the same relative effective divisor

$$p^{-1}(D') = (\psi \circ p)^{-1}(D) = (\psi \circ q)^{-1}(D) = q^{-1}(D')$$

on $T' \times_T T'$. Now descent theory [13, I, 2.17] shows that φ' factors through T. □

Exercise 3.14. Let E be an effective Cartier divisor of degree r on C, and define a subfunctor Div^E_C of Div^r_C by

$$\mathrm{Div}^E_C(T) = \{D \in \mathrm{Div}^r_C(T) \mid D_t \sim E \text{ all } t \in T\}.$$

Show that Div^E_C is representable by $\mathbb{P}(V)$ where V is the vector space $\Gamma(C, \mathscr{L}(E))$ (use [8, II, 7.12]) and that the inclusion $\mathrm{Div}^E_C \subset \mathrm{Div}^r_C$ defines a closed immersion $\mathbb{P}(V) \subset C^{(r)}$.

Remark 3.15. Theorem 3.13 says that $C^{(r)}$ is the Hilbert scheme $\mathrm{Hilb}^P_{C/k}$ where P is the constant polynomial r.

§4. The Construction of the Jacobian Variety

In this section, C will be a complete nonsingular curve of genus $g > 0$, and P will be a k-rational point on C. Recall (1.9), that in constructing J, we are allowed to make a finite separable extension of k.

For a k-scheme T, let

$$P^r_C(T) = \{\mathscr{L} \in \mathrm{Pic}(C \times T) \mid \deg(\mathscr{L}_t) = r \text{ all } t\}/\sim,$$

where $\mathscr{L} \sim \mathscr{L}'$ means $\mathscr{L} \approx \mathscr{L}' \otimes q^*\mathscr{M}$ for some invertible sheaf $\mathscr{M}$ on T. Let $\mathscr{L}_r = \mathscr{L}(rP)$; then $\mathscr{L} \mapsto \mathscr{L} \otimes p^*\mathscr{L}_r$ is an isomorphism $P^0_C(T) \to P^r_C(T)$, and so, to prove (1.1), it suffices to show that P^r_C is representable for some r. We shall do this for a fixed $r > 2g$.

Note that there is a natural transformation of functors $f\colon \mathrm{Div}^r_C \to P^r_C$ sending a relative effective divisor D on $C \times T/T$ to the class of $\mathscr{L}(D)$ (or, in other terms, $(s, \mathscr{L})$ to the class of $\mathscr{L}$).

Lemma 4.1. *Suppose there exists a section s to $f\colon \mathrm{Div}^r_C \to P^r_C$. Then P^r_C is representable by a closed subscheme of $C^{(r)}$.*

PROOF. The composite $\varphi = s \circ f$ is a natural transformation of functors $\mathrm{Div}^r_C \to \mathrm{Div}^r_C$ and Div^r_C is representable by $C^{(r)}$, and so φ is represented by a morphism of varieties. Define J' to be the fibre product,

$$\begin{array}{ccc} C^{(r)} & \leftarrow & J' \\ {\scriptstyle (1,\varphi)}\downarrow & & \downarrow \\ C^{(r)} \times C^{(r)} & \xleftarrow{\Delta} & C^{(r)}. \end{array}$$

Then

$$\begin{aligned} J'(T) &= \{(a, b) \in C^{(r)}(T) \times C^{(r)}(T) \mid a = b,\ a = \varphi b\} \\ &= \{a \in C^{(r)}(T) \mid a = \varphi(a)\} \\ &= \{a \in C^{(r)}(T) \mid a = sc, \text{ some } c \in P^r_C(T)\} \\ &\approx P^r_C(T), \end{aligned}$$

because s is injective. This shows that P^r_C is represented by J', which is a closed subscheme of $C^{(r)}$ because Δ is a closed immersion. □

The problem is therefore to define a section s or, in other words, to find a natural way of associating with a family of invertible sheaves $\mathscr{L}$ of degree r a relative effective divisor. For $\mathscr{L}$ an invertible sheaf of degree r on C, the dimension $h^0(\mathscr{L})$ of $H^0(C, \mathscr{L})$ is $r + 1 - g$, and so there is an $(r-g)$-dimensional system of effective divisors D such that $\mathscr{L}(D) \approx \mathscr{L}$. One way to cut down the size of this system is to fix a family $\gamma = (P_1, \ldots, P_{r-g})$ of k-rational points on C and consider only divisors D in the system such that $D \geq D_\gamma$, where $D_\gamma = \sum P_i$. As we shall see, this provides a partial solution to the problem.

Proposition 4.2. *Let γ be an $(r-g)$-tuple of k-rational points on C, and let $\mathscr{L}_\gamma = \mathscr{L}(\sum_{P \in \gamma} P)$.*

(a) *There is an open subvariety C^γ of $C^{(r)}$ such that, for all k-schemes T,*

$$C^\gamma(T) = \{D \in \mathrm{Div}^r_C(T) \mid h^0(D_t - D_\gamma) = 1, \text{ all } t \in T\}.$$

If k is separably closed, then $C^{(r)}$ is the union of the subvarieties C^γ.

(b) *For all k-schemes T, define*

$$P^\gamma(T) = \{\mathscr{L} \in P^r_C(T) \mid h^0(\mathscr{L}_t \otimes \mathscr{L}_\gamma^{-1}) = 1, \textit{ all } t \in T\}.$$

Then P^γ is a subfunctor of P^r_C and the obvious natural transformation $f\colon C^\gamma \to P^\gamma$ has a section.

PROOF. (a) Note that for any effective divisor D of degree r on C, $h^0(D - D_\gamma) \geq 1$, and that equality holds for at least one D (for example,

$D = D_\gamma + Q_1 + \cdots + Q_g$ for a suitable choice of points $Q_1, \ldots, Q_g$; see the elementary result (5.2b) below). Let D_{can} be the canonical relative effective divisor of degree r on $C \times C^{(r)}/C^{(r)}$. Then [14, 4.2c] applied to $\mathscr{L}(D_{\mathrm{can}} - p^{-1}D_\gamma)$ shows that there is an open subscheme C^γ of $C^{(r)}$ such that $h^0((D_{\mathrm{can}})_t - D_\gamma) = 1$ for t in C^γ and $h^0((D_{\mathrm{can}})_t - D_\gamma) > 1$ otherwise. Let T be a k-scheme, and let D be a relative effective divisor of degree r on $C \times T/T$ such that $h^0(D_t - D_\gamma) = 1$. Then (3.13) shows that there is a unique morphism $\varphi\colon T \to C^{(r)}$ such that $(1 \times \varphi)^{-1}(D_{\mathrm{can}}) = D$, and it is clear that φ maps T into C^γ. This proves the first assertion.

Assume that k is separably closed. To show that $C = \bigcup C^\gamma$, it suffices to show that $C(k) = \bigcup C^\gamma(k)$, or that for every divisor D of degree r on C, there exists a γ such that $h^0(D - D_\gamma) = 1$. Choose a basis $e_0, \ldots, e_{r-g}$ for $H^0(C, \mathscr{L}(D))$, and consider the corresponding embedding $\iota\colon C \subset \mathbb{P}^{r-g}$. Then $\iota(C)$ is not contained in any hyperplane (if it were contained in $\sum a_i X_i = 0$, then $\sum a_i e_i$ would be zero on C), and so there exist $r - g$ points $P_1, \ldots, P_{r-g}$ on C disjoint from D whose images are not contained in any linear subspace of codimension 2 (choose $P_1, P_2, \ldots$ inductively so that $P_1, \ldots, P_i$ are not contained in a linear subspace of dimension $i - 2$). The $(r-g)$-tuple $\gamma = (P_1, \ldots, P_{r-g})$ satisfies the condition because

$$H^0(C, \mathscr{L}(D - \textstyle\sum P_j)) = \{\sum a_i e_i \mid \sum a_i e_i(P_j) = 0, j = 1, \ldots, r - g\},$$

which has dimension < 2.

(b). Let $\mathscr{L}$ be an invertible sheaf on $C \times T$ representing an element of $P^\gamma(T)$. Then $h^0(D_t - D_\gamma) = 1$ for all t, and the Riemann–Roch theorem shows that $h^1(D_t - D_\gamma) = 0$ for all t. Now [14, 4.2e] shows that $\mathscr{M} \overset{\mathrm{df}}{=} q_*(\mathscr{L} \otimes p^*\mathscr{L}_\gamma^{-1})$ is an invertible sheaf on T and that its formation commutes with base change. This proves that P^γ_C is a subfunctor of P^r_C. On tensoring the canonical map $q^*\mathscr{M} \to \mathscr{L} \otimes p^*\mathscr{L}_\gamma^{-1}$ with $q^*\mathscr{M}^{-1}$, we obtain a canonical map $\mathscr{O}_{C \times T} \to \mathscr{L} \otimes p^*\mathscr{L}_\gamma^{-1} \otimes q^*\mathscr{M}^{-1}$. The natural map $\mathscr{L}_\gamma \to \mathscr{O}_C$ induces a map $p^*\mathscr{L}_\gamma^{-1} \to \mathscr{O}_{C \times T}$, and on combining this with the preceding map, we obtain a canonical map $s_\gamma\colon \mathscr{O}_{C \times T} \to \mathscr{L} \otimes q^*\mathscr{M}^{-1}$. The pair $(s_\gamma, \mathscr{L} \otimes q^*\mathscr{M}^{-1})$ is a relative effective divisor on $C \times T/T$ whose image under f in $P^\gamma(T)$ is represented by $\mathscr{L} \otimes q^*\mathscr{M}^{-1} \sim \mathscr{L}$ (see 3.6). We have defined a section to $C^\gamma(T) \to P^\gamma(T)$, and our construction is obviously functorial. □

Corollary 4.3. *The functor P^γ is representable by a closed subvariety J^γ of C^γ.* □

PROOF. The proof is the same as that of (4.1).

Now consider two $(g-r)$-tuples γ and γ', and define $P^{\gamma,\gamma'}$ to be the functor such that $P^{\gamma,\gamma'}(T) = P^\gamma(T) \cap P^{\gamma'}(T)$ for all k-schemes T. It easy to see that $P^{\gamma,\gamma'}$ is representable by a variety $J^{\gamma,\gamma'}$ such that the maps $J^{\gamma,\gamma'} \subset J^\gamma$ and $J^{\gamma,\gamma'} \subset J^{\gamma'}$ defined by the inclusions $P^{\gamma,\gamma'} \subset P^\gamma$ and $P^{\gamma,\gamma'} \subset P^{\gamma'}$ are open immersions.

We are now ready to construct the Jacobian of C. Choose tuples $\gamma_1, \ldots, \gamma_m$ of points in $C(k_s)$ such that $C^{(r)} = \bigcup C^{\gamma_i}$. After extending k, we can assume that the γ_i are tuples of k-rational points. Define J by patching together the varieties J^{γ_i} using the open immersions $J^{\gamma_i,\gamma_j} \subset J^{\gamma_i}, J^{\gamma_j}$. It is easy to see that J represents the functor P_C^r, and therefore also the functor P_C^0. Since the latter is a group functor, J is a group variety. The natural transformations $\mathrm{Div}_C^r \to P_C^r \to P_C^0$ induce a morphism $C^{(r)} \to J$, which shows that J is complete and is therefore an abelian variety. The proof of (1.1) is complete. □

§5. The Canonical Maps from the Symmetric Powers of C to its Jacobian Variety

Throughout this section C will be a complete nonsingular curve of genus $g > 0$. Assume there is a k-rational point P on C, and write f for the map f^P defined in Section 2.

Let f^r be the map $C^r \to J$ sending $(P_1, \ldots, P_r)$ to $f(P_1) + \cdots + f(P_r)$. On points, f^r is the map $(P_1, \ldots, P_r) \mapsto [P_1 + \ldots + P_r - rP]$. Clearly it is symmetric, and so induces a map $f^{(r)}: C^{(r)} \to J$. We can regard $f^{(r)}$ as the map sending an effective divisor D of degree r on C to the linear equivalence class of $D - rP$. The fibre of the map $f^{(r)}: C^{(r)}(k) \to J(k)$ containing D can be identified with the space of effective divisors linearly equivalent to D, that is, with the linear system $|D|$. The image of $C^{(r)}$ in J is a closed subvariety W^r of J, which can also be written $W^r = f(C) + \ldots + f(C)$ (r summands).

Theorem 5.1. (a) *For all $r \leq g$, the morphism $f^{(r)}: C^{(r)} \to W^r$ is birational; in particular, $f^{(g)}$ is a birational map from $C^{(g)}$ onto J.*

(b) *Let D be an effective divisor of degree r on C, and let F be the fibre of $f^{(r)}$ containing D. Then no tangent vector to $C^{(r)}$ at D maps to zero under $(df^{(r)})_D$ unless it lies in the direction of F; in other words, the sequence*

$$0 \to T_D(F) \to T_D(C^{(r)}) \to T_a(J), \qquad a = f^{(r)}(D),$$

is exact. In particular, $(df^{(r)})_D: T_D(C^{(r)}) \to T_a(J)$ is injective if $|D|$ has dimension zero.

PROOF. For D a divisor on C, we write $h^0(D)$ for the dimension of

$$H^0(C, \mathscr{L}(D)) = \{f \in k(C) | (f) + D \geq 0\}$$

and $h^1(D)$ for the dimension of $H^1(C, \mathscr{L}(D))$. Recall that

$$h^0(D) - h^1(D) = \deg(D) + 1 - g,$$

and that $H^1(C, \mathscr{L}(D))^\vee = H^0(C, \Omega^1(-D))$, which can be identified with the set of $\omega \in \Omega^1_{k(C)/k}$ whose divisor $(\omega) \geq D$.

Lemma 5.2. (a) *Let D be a divisor on C such that $h^1(D) > 0$; then there is a nonempty open subset U of C such that $h^1(D + Q) = h^1(D) - 1$ for all closed points Q in U, and $h^1(D + Q) = h^1(D)$ for $Q \notin U$.*

(b) *For any $r \leq g$, there is an open subset U of C^r such that $h^0(\sum P_i) = 1$ for all $(P_1, \ldots, P_r)$ in U.*

PROOF. (a) If Q is not in the support of D, then $H^1(C, \mathscr{L}(D + Q))^\vee = \Gamma(C, \Omega^1(-D - Q))$ can be identified with the subspace of $\Gamma(C, \Omega^1(-D))$ of differentials with a zero at Q. Clearly therefore we can take U to be the complement of the zero set of a basis of $H^1(C, \mathscr{L}(D))$ together with a subset of the support of D.

(b) Let D_0 be the divisor zero on C. Then $h^1(D_0) = g$, and on applying (a) repeatedly, we find that there is an open subset U of C^r such that $h^1(\sum P_i) = g - r$ for all $(P_1, \ldots, P_r)$ in U. The Riemann–Roch theorem now shows that $h^0(\sum P_i) = r + (1 - g) + (g - r) = 1$ for all $(P_1, \ldots, P_r)$ in U. □

In proving (5.1), we can assume that k is algebraically closed. If U' is the image in $C^{(r)}$ of the set U in (5.2b), then $f^{(r)}: C^{(r)}(k) \to J(k)$ is injective on $U'(k)$, and so $f^{(r)}: C^{(r)} \to W^r$ must either be birational or else purely inseparable of degree > 1. The second possibility is excluded by part (b) of the theorem, but before we can prove that we need another proposition.

Proposition 5.3. (a) *For all $r \geq 1$, there are canonical isomorphisms*

$$\Gamma(C, \Omega^1) \overset{\approx}{\to} \Gamma(C^r, \Omega^1)^{S_r} \overset{\approx}{\leftarrow} \Gamma(C^{(r)}, \Omega^1).$$

Let $\omega \in \Gamma(C, \Omega^1)$ correspond to $\omega' \in \Gamma(C^{(r)}, \Omega^1)$; then for any effective divisor D of degree r on C, $(\omega) \geq D$ if and only if ω' has a zero at D.

(b) *For all $r \geq 1$, the map $f^{(r)*}: \Gamma(J, \Omega^1) \to \Gamma(C^{(r)}, \Omega^1)$ is an isomorphism.*

PROOF. A global 1-form on a product of projective varieties is a sum of global 1-forms on the factors. Therefore $\Gamma(C^r, \Omega^1) = \oplus\, p_i^* \Gamma(C, \Omega^1)$, where the p_i are the projection maps onto the factors, and so it is clear that the map $\omega \mapsto \sum p_i^* \omega$ identifies $\Gamma(C, \Omega^1)$ with $\Gamma(C^r, \Omega^1)^{S_r}$. Because $\pi: C^r \to C^{(r)}$ is separable, $\pi^*: \Gamma(C^{(r)}, \Omega^1) \to \Gamma(C^r, \Omega^1)$ is injective, and its image is obviously fixed by the action of S_r. The composite map

$$\Gamma(J, \Omega^1) \to \Gamma(C^{(r)}, \Omega^1) \subset \Gamma(C^r, \Omega^1)^{S_r} = \Gamma(C, \Omega^1)$$

sends ω to the element ω' of $\Gamma(C, \Omega^1)$ such that $f^{r*}\omega = \sum p_i^* \omega'$. As $f^r = \sum f \circ p_i$, clearly $\omega' = f^*\omega$, and so the composite map is f^* which we know to be an isomorphism (2.2). This proves that both maps in the above sequence are isomorphisms. It also completes the proof of the proposition except for the second part of (a), and for this we need a combinatorial lemma.

Lemma 5.4. *Let $\sigma_1, \ldots, \sigma_r$ be the elementary symmetric polynomials in $X_1, \ldots, X_r$, and let $\tau_j = \sum X_i^j\, dX_i$. Then*

$$\sigma_m \tau_0 - \sigma_{m-1} \tau_1 + \cdots + (-1)^m \tau_m = d\sigma_{m+1}, \qquad \text{all } m \leq r - 1.$$

PROOF. Let $\sigma_m(i)$ be the mth elementary symmetric polynomial in the variables

$X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_r$. Then

$$\sigma_{m-n} = \sigma_{m-n}(i) + X_i \sigma_{m-n-1}(i),$$

and on multiplying this by $(-1)^n X_i^n$ and summing over n (so that the successive terms cancel out) we obtain the identity

$$\sigma_m - \sigma_{m-1} X_i + \cdots + (-1)^m X_i^m = \sigma_m(i).$$

On multiplying this with dX_i and summing, we get the required identity. □

We now complete the proof of (5.3). First let $D = rQ$. Then $\hat{\mathcal{O}}_Q = k[[X]]$ and $\hat{\mathcal{O}}_D = k[[\sigma_1, \ldots, \sigma_r]]$ (see the proof of (3.2); by $\mathcal{O}_D$ we mean the local ring at the point D on $C^{(r)}$). If $\omega = (a_0 + a_1 X + a_2 X^2 + \cdots)\, dX$, $a_i \in k$, when regarded as an element of $\Omega^1_{\hat{\mathcal{O}}_Q/k}$, then $\omega' = a_0 \tau_0 + a_1 \tau_1 + \cdots$. We know that $\{d\sigma_1, \ldots, d\sigma_r\}$ is a basis for $\Omega^1_{\hat{\mathcal{O}}_D/k}$ as an $\hat{\mathcal{O}}_D$-module, but the lemma shows that $\tau_0, \ldots, \tau_{r-1}$ is also a basis. Now $(\omega) \geq D$ and $\omega'(D) = 0$ are both obviously equivalent to $a_0 = a_1 = \cdots = a_{r-1} = 0$. The proof for other divisors is similar. □

We finally prove the exactness of the sequence in (5.1). The injectivity of $(di)_D$ follows from the fact that $i\colon F \subset C^{(r)}$ is a closed immersion. Moreover the sequence is a complex because $f \circ i$ is the constant map $x \mapsto a$. It remains to show that

$$\dim \operatorname{Im}(di)_D = \dim \operatorname{Ker}(df^{(r)})_D.$$

Identify $T_a(J)^\vee$ with $\Gamma(C, \Omega^1)$ using the isomorphisms arising from (2.1). Then (5.3) shows that ω is zero on the image of $T_D(C^{(r)})$ if and only if $(\omega) \geq D$, that is, $\omega \in \Gamma(C, \Omega^1(-D))$. Therefore the image of $(df^{(r)})_D$ has dimension $g - h^0(\Omega^1(-D)) = g - h^1(D)$, and so its kernel has dimension $r - g + h^1(D)$. On the other hand, the image of $(di)_D$ has dimension $|D|$. The Riemann–Roch theorem says precisely that these two numbers are equal, and so completes the proof. □

Corollary 5.5. *For all $r \leq g$, $f^r\colon C^r \to W^r$ is of degree $r!$.*

PROOF. It is the composite of $\pi\colon C^r \to C^{(r)}$ and $f^{(r)}$. □

Remark 5.6. (a) The theorem shows that J is the unique abelian variety birationally equivalent to $C^{(g)}$. This observation is the basis of Weil's construction of the Jacobian. (See Section 7.)

(b) The exact sequence in (5.1b) can be regarded as a geometric statement of the Riemann–Roch theorem (see especially the end of the proof). In fact it is possible to prove the Riemann–Roch theorem this way (see [12]).

(c) As we observed above, the fibre of $f^{(r)}\colon C^{(r)}(k) \to J(k)$ containing D can be identified with the linear system $|D|$. More precisely, the fibre of the map of functors $C^{(r)} \to J$ is the functor Div_C^D of (3.14); therefore the scheme-theoretic fibre of $f^{(r)}$ containing D is a copy of projective space of dimension $h^0(D) - 1$. Corollary 3.9 of [14] shows that conversely every copy of projective space in

$C^{(r)}$ is contained in some fibre of $f^{(r)}$. Consequently, the closed points of the Jacobian can be identified with the set of maximal subvarieties of $C^{(r)}$ isomorphic to projective space.

Note that for $r > 2g - 2$, $|D|$ has dimension $r - g$, and so $(df^{(r)})_D$ is surjective, for all D. Therefore $f^{(r)}$ is smooth (see [8, III, 10.4]), and the fibres of $f^{(r)}$ are precisely the copies of $\mathbb{P}^{r-g}$ contained in $C^{(r)}$. This last observation is the starting point of Chow's construction of the Jacobian [3].

§6. The Jacobian Variety as Albanese Variety; Autoduality

Throughout this section C will again be a complete nonsingular curve of genus $g > 0$ over a field k, and J will be its Jacobian variety.

Proposition 6.1. *Let P be a k-rational point on C. The map $f^P\colon C \to J$ has the following universal property: for any map $\varphi\colon C \to A$ from C into an abelian variety sending P to 0, there is a unique homomorphism $\psi\colon J \to A$ such that $\varphi = \psi \circ f^P$.*

PROOF. Consider the map $C^g \to A$, $(P_1, \ldots, P_g) \mapsto \sum \psi(P_i)$. Clearly this is symmetric, and so it factors through $C^{(g)}$. It therefore defines a rational map $\psi\colon J \to A$, which [14, 3.1] shows to be a morphism. It is clear from the construction that $\psi \circ f^P = \varphi$ (note that f^P is the composite of $Q \mapsto Q + (g-1)P\colon C \to C^{(g)}$ with $f^{(g)}\colon C^{(g)} \to J$). In particular, ψ maps 0 to 0, and [14, 2.2] shows that it is therefore a homomorphism. If ψ' is a second homomorphism such that $\psi' \circ f^P = \varphi$, then ψ and ψ' agree on $f^P(C) + \cdots + f^P(C)$ (g copies), which is the whole of J. □

Corollary 6.2. *Let $\mathcal{N}$ be a divisorial correspondence between (C, P) and J such that $(1 \times f^P)^* \mathcal{N} \approx \mathcal{L}^P$; then $\mathcal{N} \approx \mathcal{M}^P$ (notations as in Section 2 and (1.2)).*

PROOF. Because of [14, 6.2], we can assume k to be algebraically closed. According to (1.2) there is a unique map $\varphi\colon J \to J$ such that $\mathcal{N} \approx (1 \times \varphi)^* \mathcal{M}^P$. On points φ is the map sending $a \in J(k)$ to the unique b such that

$$\mathcal{M}^P | C \times \{b\} \approx \mathcal{N} | C \times \{a\}.$$

By assumption,

$$\mathcal{N} | C \times \{f^P Q\} \approx \mathcal{L}^P | C \times \{Q\} \approx \mathcal{M}^P | C \times \{f^P Q\},$$

and so $(\varphi \circ f^P)(Q) = f^P(Q)$ for all Q. Now (6.1) shows that f is the identity map. □

Corollary 6.3. *Let C_1 and C_2 be curves over k with k-rational points P_1 and P_2, and let J_1 and J_2 be their Jacobians. There is a one-to-one correspondence between $\mathrm{Hom}_k(J_1, J_2)$ and the set of isomorphism classes of divisorial correspondences between (C_1, P_1) and (C_2, P_2).*

PROOF. A divisorial correspondence between (C_2, P_2) and (C_1, P_1) gives rise to a morphism $(C_1, P_1) \to J_2$ (by 1.2), and this morphism gives rise to homomorphism $J_1 \to J_2$ (by 6.1). Conversely, a homomorphism $\psi: J_1 \to J_2$ defines a divisorial correspondence $(1 \times (f^{P_1} \circ \psi))^* \mathscr{M}^{P_2}$ between (C_2, P_2) and (C_1, P_1). □

In the case that C has a point P rational over k, define $F: C \times C \to J$ to be the map $(P_1, P_2) \mapsto f^P(P_1) - f^P(P_2)$. One checks immediately that this is independent of the choice of P. Thus, if $P \in C(k')$ for some Galois extension k' of k, and $F: C_{k'} \times C_{k'} \to J_{k'}$ is the corresponding map, then $\sigma F = F$ for all $\sigma \in \mathrm{Gal}(k'/k)$; therefore F is defined over k whether or not C has a k-rational point. Note that it is zero on the diagonal Δ of $C \times C$.

Proposition 6.4. *Let A be an abelian variety over k. For any map $\varphi: C \times C \to A$ such that $\varphi(\Delta) = 0$, there is a unique homomorphism $\psi: J \to A$ such that $\psi \circ F = \varphi$.*

PROOF. Let k' be a finite Galois extension of k, and suppose that there exists a unique homomorphism $\psi: C_{k'} \to J_{k'}$ such that $\psi \circ F_{k'} = \varphi_{k'}$. Then the uniqueness implies that $\sigma\psi = \psi$ for all σ in $\mathrm{Gal}(k'/k)$, and so ψ is defined over k. It suffices therefore to prove the proposition after extending k, and so we can assume that C has a k-rational point P. Now [14, 2.5] shows that there exist unique maps φ_1 and φ_2 from C to A such that $\varphi_1(P) = 0 = \varphi_2(P)$ and $\varphi(a, b) = \varphi_1(a) + \varphi_2(b)$ for all $(a, b) \in C \times C$. Because φ is zero on the diagonal, $\varphi_1 = -\varphi_2$. From (6.1) we know that there exists a unique homomorphism ψ from J to A such that $\varphi_1 = \psi \circ f$, and clearly ψ is also the unique homomorphism such that $\varphi = \psi \circ F$. □

Remark 6.5. The proposition says that (A, F) is the Albanese variety of C in the sense of [9, II.3, p. 45]. Clearly the pairs (J, f^P) and (J, F) are characterized by the universal properties in (6.1) and (6.4).

Assume again that C has a k-rational point P, and let $\Theta = W^{g-1}$. It is a divisor on J, and if P is replaced by a second k-rational point, Θ is replaced by a translate. For any effective divisor D on J, write

$$\begin{aligned}\mathscr{L}'(D) &= m^*\mathscr{L}(D) \otimes p^*\mathscr{L}(D)^{-1} \otimes q^*\mathscr{L}(D)^{-1} \\ &= \mathscr{L}(m^{-1}(D) - D \times J - J \times D).\end{aligned}$$

Recall [14, 9.1 and §10], that D is ample if and only if $\varphi_{\mathscr{L}(D)}: J \to J^\vee$ is an isogeny, and then $(1 \times \varphi_{\mathscr{L}(D)})^*(\mathscr{P}) = \mathscr{L}'(D)$, where $\mathscr{P}$ is the Poincaré sheaf on $J \times J^\vee$. Write Θ^- for the image of Θ under the map $(-1)_J: J \to J$, and Θ_a for $t_a\Theta = \Theta + a$, $a \in J(k)$. Abbreviate $(\Theta^-)_a$ by Θ_a^-.

Theorem 6.6. *The map $\varphi_{\mathscr{L}(\Theta)}: J \to J^\vee$ is an isomorphism; therefore, $1 \times \varphi_{\mathscr{L}(\Theta)}$ is an isomorphism $(J \times J, \mathscr{L}'(\Theta)) \xrightarrow{\approx} (J \times J^\vee, \mathscr{P})$.*

PROOF. As usual, we can assume k to be algebraically closed. Recall [14, 12.13] that $\varphi_{\mathscr{L}(\Theta^-)} = (-1)^2 \varphi_{\mathscr{L}(\Theta)} = \varphi_{\mathscr{L}(\Theta)}$, and that $\varphi_{\mathscr{L}(\Theta_a)} = \varphi_{\mathscr{L}(\Theta)}$ for all $a \in J(k)$.

Lemma 6.7. *Let U be the largest open subset of J such that:*

(i) the fibre of $f^{(g)}: C^{(g)} \to J$ at any point of U has dimension zero; and
(ii) if $a \in U(k)$ and $D(a)$ is the unique element of $C^{(r)}(k)$ mapping to a, then $D(a)$ is a sum of g distinct points of $C(k)$.

Then $f^{-1}(\Theta_a^-) = D(a)$ (as a Cartier divisor) for all $a \in U(k)$, where $f = f^P: C \to J$.

PROOF. Note first that U can be obtained by removing the subset over which the fibres have dimension > 0, which is closed (see [18, I.6, Theorem 7]), together with the images of certain closed subsets of the form $\Delta \times C^{g-2}$. These last sets are also closed because $C^g \to J$ is proper ([18, II, 4.8]), and it follows that U is a dense open subset of J.

Let $a \in U(k)$, and let $D(a) = \sum P_i$, $P_i \neq P_j$ for $i \neq j$. A point Q_1 of C maps to a point of Θ_a^- if and only if there exists a divisor $\sum_{i=2}^{g} Q_i$ on C such that $f^P(Q_1) = -\sum f^P(Q_i) + a$. The equality implies $\sum_{i=1}^{g} Q_i \sim D$, and the fact that $|D|$ has dimension 0 implies that $\sum Q_i = D$. It follows that the support of $f^{-1}(\Theta_a^-)$ is $\{P_1, \ldots, P_g\}$, and it remains to show that $f^{-1}(\Theta_a^-)$ has degree $\leq g$ for all a.

Consider the map $\psi: C \times \Theta \to J$ sending (Q, b) to $f(Q) + b$. As the composite of ψ with $1 \times f^{g-1}: C \times C^{g-1} \to C \times \Theta$ is $f^g: C^g \to J$, and these maps have degrees $(g-1)!$ and $g!$ respectively (5.5), ψ has degree g. Also ψ is projective because $C \times \Theta$ is a projective variety (see [8, II, Ex. 4.9]). Consider $a \in U$; the fibre of ψ over a is $f^{-1}(\Theta_a^-)$ (more accurately, it is the subscheme of C associated with the Cartier divisor $f^{-1}(\Theta_a^-)$). Therefore the restriction of ψ to $\psi^{-1}(U)$ is quasi-finite and projective, and so is finite (see [8, III, Ex. 11.2]). As U is normal, this means that all the fibres of ψ over points of U are finite schemes of rank $\leq g$ (cf. [18, II.5, Theorem 6]). This completes the proof of the lemma. □

Lemma 6.8. (a) *Let $a \in J(k)$, and let $f^{(g)}(D) = a$; then $f^*\mathscr{L}(\Theta_a^-) \approx \mathscr{L}(D)$.*
(b) *The sheaves $(f \times (-1)_J)^*\mathscr{L}'(\theta^-)$ and $\mathscr{M}^P$ on $C \times J$ are isomorphic.*

PROOF. Note that (6.7) shows that the isomorphism in (a) holds for all a in a dense open subset of J. Note also that the map $C \to C \times \{a\} \to J \times J \to J$,

$$m \circ (f \times (-1)) \circ (Q \mapsto (Q, a)) = t_{-a} \circ f,$$

and so

$$\begin{aligned}(f \times (-1))^* m^* \mathscr{L}(\Theta^-) | C \times \{a\} &\approx \mathscr{L}(t_{-a}^{-1}\Theta^-) | f(C) = \mathscr{L}(\Theta_a^-) | f(C) \\ &\approx f^*\mathscr{L}(\Theta_a^-).\end{aligned}$$

Similarly

$$(f \times (-1))^*p^*\mathcal{L}(\Theta^-)|C \times \{a\} \approx f^*\mathcal{L}(\Theta^-), \quad \text{and}$$

$$(f \times (-1))^*q^*\mathcal{L}(\Theta^-)|C \times \{a\} \text{ is trivial.}$$

On the other hand, $\mathcal{M}^P$ is an invertible sheaf on $C \times J$ such that:

(i) $\mathcal{M}^P|C \times \{a\} \approx \mathcal{L}(D - gP)$ if D is an effective divisor of degree g on C such that $f^{(g)}(D) = a$;

(ii) $\mathcal{M}^P|\{P\} \times J$ is trivial.

Therefore (a) is equivalent to $(f \times (-1))^*m^*\mathcal{L}(\Theta^-)|C \times \{a\}$ being isomorphic to $\mathcal{M}^P \otimes p^*\mathcal{L}(gP)|C \times \{a\}$ for all a. As we know this is true for all a in a dense subset of J, [14, 5.3] applied to

$$\mathcal{M}^P \otimes p^*\mathcal{L}(gP) \otimes (f \times (-1))^*m^*\mathcal{L}(\Theta^-)^{-1}$$

proves (a). In particular, on taking $a = 0$, we find that $f^*\mathcal{L}(\Theta^-) \approx \mathcal{L}(gP)$, and so $(f \times (-1))^*p^*\mathcal{L}(\Theta^-) \approx p^*\mathcal{L}(gP)$. Now [14, 5.1] shows that $(f \times (-1))^*(m^*\mathcal{L}(\Theta^-) \otimes p^*\mathcal{L}(\Theta^-)^{-1}) \approx \mathcal{M}^P \otimes q^*\mathcal{N}$ for some invertible sheaf $\mathcal{N}$ on J. On computing the restrictions of the sheaves to $\{P\} \times J$, we find that $\mathcal{N} \approx (-1)^*\mathcal{L}(\Theta^-)$, which completes the proof. □

Consider the invertible sheaf $(f \times 1)^*\mathcal{P}$ on $C \times J^\vee$. Clearly it is a divisorial correspondence, and so there is a unique homomorphism $f^\vee\colon J^\vee \to J$ such that $(1 \times f^\vee)^*\mathcal{M}^P \approx (f \times 1)^*\mathcal{P}$. The next lemma completes the proof of the theorem.

Lemma 6.9. *The maps* $-f^\vee\colon J^\vee \to J$ *and* $\varphi_{\mathcal{L}(\Theta)}\colon J \to J^\vee$ *are inverse.*

PROOF. Write $\psi = -\varphi_{\mathcal{L}(\Theta)} = -\varphi_{\mathcal{L}(\Theta^-)}$. We have

$$(1 \times \psi)^*(1 \times f^\vee)^*\mathcal{M}^P \approx (1 \times \psi)^*(f \times 1)^*\mathcal{P}$$
$$\approx (f \times \psi)^*\mathcal{P} \approx (f \times (-1))^*(1 \times \varphi_{\mathcal{L}(\Theta)})^*\mathcal{P}$$
$$\approx (f \times (-1))^*\mathcal{L}'(\Theta^-) \approx \mathcal{M}^P.$$

Therefore, $f^\vee \circ \psi$ is a map $\alpha\colon J \to J$ such that $(1 \times \alpha)^*\mathcal{M}^P \approx \mathcal{M}^P$; but the only map with this property is the identity. □

Remark 6.10. (a) Lemma 6.7 shows that $f(C)$ and Θ cross transversely at any point of U. This can be proved more directly by using the descriptions of the tangent spaces implicitly given near the end of the proof of (5.1).

(b) In (6.8) we showed that $\mathcal{M}^P \approx (f \times (-1))^*\mathcal{L}'(\Theta^-)$. This implies

$$\mathcal{M}^P \approx (f \times (-1))^*(1 \times \varphi_{\mathcal{L}(\Theta^-)})^*\mathcal{P} \approx (f \times (-1))^*(1 \times \varphi_{\mathcal{L}(\Theta)})^*\mathcal{P}$$
$$\approx (f \times (-1))^*\mathcal{L}'(\Theta).$$

Also, because $D \mapsto \varphi_{\mathcal{L}(D)}$ is a homomorphism, $\varphi_{\mathcal{L}(-\Theta)} = -\varphi_{\mathcal{L}(\Theta)}$, and so

$$\mathcal{M}^P \approx (f \times (-1))^*(1 \times \varphi_{\mathcal{L}(\Theta)})^*\mathcal{P} \approx (f \times 1)^*(1 \times \varphi_{\mathcal{L}(-\Theta)})^*\mathcal{P}$$
$$\approx (f \times 1)^*\mathcal{L}'(-\Theta).$$

(c) The map on points $J^\vee(k) \to J(k)$ defined by $f^\vee$ is induced by $f^*\colon \mathrm{Pic}(J) \to \mathrm{Pic}(C)$.

(d) Lemma 6.7 can be generalized as follows. An effective canonical divisor K defines a point on $C^{(2g-2)}$ whose image in J will be denoted κ. Let a be a point of J such that $a - \kappa$ is not in $(W^{g-2})^-$, and write $a = \sum f(P_i)$ with $P_1, \ldots, P_g$ points on C. Then W^r and $(W^{g-r})^-_a$ intersect properly, and $W^r(W^{g-r})^-_a = \sum (w_{i_1 \ldots i_r})$ where

$$w_{i_1 \ldots i_r} = f(P_{i_1}) + \cdots + f(P_{i_r})$$

and the sum runs over the $\binom{g}{r}$ combinations obtained by taking r elements from $\{1, 2, \ldots, g\}$. See [20, §39, Prop. 17].

Summary 6.11. Between (C, P) and itself, there is a divisorial correspondence $\mathcal{L}^P = \mathcal{L}(\Delta - \{P\} \times C - C \times \{P\})$.

Between (C, P) and J there is the divisorial correspondence $\mathcal{M}^P$; for any divisorial correspondence $\mathcal{L}$ between (C, P) and a pointed k-scheme (T, t), there is a unique morphism of pointed k-schemes $\varphi\colon T \to J$ such that $(1 \times \varphi)^*\mathcal{M}^P \approx \mathcal{L}$. In particular, there is a unique map $f^P\colon C \to J$ such that $(1 \times f^P)^*\mathcal{M}^P \approx \mathcal{L}^P$ and $f(P) = 0$.

Between J and $J^\vee$ there is a canonical divisorial correspondence $\mathcal{P}$ (the Poincaré sheaf); for any divisorial correspondence $\mathcal{L}$ between J and a pointed k-schemes (T, t) there is a unique morphism of pointed k-schemes $\psi\colon T \to J$ such that $(1 \times \psi)^*\mathcal{P} \approx \mathcal{L}$.

Between J and J there is the divisorial correspondence $\mathcal{L}'(\Theta)$. The unique morphism $J \to J^\vee$ such that $(1 \times \psi)^*\mathcal{P} \approx \mathcal{L}'(\Theta)$ is $\varphi_{\mathcal{L}(\Theta)}$, which is an isomorphism. Thus $\varphi_{\mathcal{L}(\Theta)}$ is a principal polarization of J, called the *canonical* polarization. There are the following formulas:

$$\mathcal{M}^P \approx (f \times (-1))^*\mathcal{L}'(\Theta) \approx (f \times 1)^*\mathcal{L}'(\Theta)^{-1}.$$

Consequently,

$$\mathcal{L}^P \approx (f \times f)^*\mathcal{L}'(\Theta)^{-1}.$$

If $f^\vee\colon J^\vee \to J$ is the morphism such that $(f \times 1)^*\mathcal{P} \approx (1 \times f^\vee)^*\mathcal{M}^P$, then $f^\vee = -\varphi^{-1}_{\mathcal{L}(\Theta)}$.

Exercise 6.12. It follows from (6.6) and the Riemann–Roch theorem [14, 13.3] that $(\Theta^g) = g!$. Prove this directly by studying the inverse image of Θ (and its translates) by the map $C^g \to J$. (Cf. [14, 8.3], but note that the map is not finite.) Hence deduce another proof of (6.6).

§7. Weil's Construction of the Jacobian Variety

As we saw in (5.6a), the Jacobian J of a curve C is the unique abelian variety that is birationally equivalent to $C^{(g)}$. To construct J, Weil used the Riemann–Roch theorem to define a rational law of composition on $C^{(g)}$ and then proved a general theorem that allowed him to construct an algebraic group out of $C^{(g)}$ and the rational law. Finally, he verified that the algebraic group so obtained had the requisite properties to be called the Jacobian of C. We give a sketch of this approach.

A *birational group* over k (or a nonsingular variety with a normal law of composition in the terminology of Weil [20, V]) is a nonsingular variety V together with a rational map $m: V \times V \dashrightarrow V$ such that

(a) m is associative (that is, $(ab)c = a(bc)$ whenever both terms are defined);
(b) the rational maps $(a, b) \mapsto (a, ab)$ and $(a, b) \mapsto (b, ab)$ from $V \times V$ to $V \times V$ are both birational.

Assume that C has a k-rational point P.

Lemma 7.1. (a) *There exists an open subvariety U of $C^{(g)} \times C^{(g)}$ such that for all fields K containing k and all (D, D') in $U(K)$, $h^0(D + D' - gP) = 1$.*
(b) *There exists an open subset V of $C^{(g)} \times C^{(g)}$ such that for all fields K containing k and all (D, D') in $V(K)$, $h^0(D' - D + gP) = 1$.*

PROOF. (a) Let D_{can} be the canonical relative effective divisor on $C \times C^{(2g)}/C^{(2g)}$ constructed in Section 3. According to the Riemann–Roch theorem, $h^0(D - gP) \geq 1$ for all divisors of degree $2g$ on C, and so [14, 4.2c] shows that the subset U of $C^{(2g)}$ of points t such that $h^0((D_{\text{can}})_t - gP) = 1$ is open. On the other hand, (5.2b) shows that there exist positive divisors D of degree g such that $h^0((D + gP) - gP) = 1$, and so U is nonempty. Its inverse image in $C^{(g)} \times C^{(g)}$ is the required set.

(b) The proof is similar to that of (a): the Riemann–Roch theorem shows that $h^0(D' - D + gP) \geq 1$ for all D and D', we know there exists a D' such that $h^0(D' - gP + gP) = h^0(D') = 1$, and [14, 4.2] applied to the appropriate invertible sheaf on $C \times C^{(g)} \times C^{(g)}$ gives the result. □

Proposition 7.2. *There exists a unique rational map $m: C^{(g)} \times C^{(g)} \dashrightarrow C^{(g)}$ whose domain of definition contains the subset U of* (7.1a) *and which is such that for all fields K containing k and all (D, D') in $U(K)$, $m(D, D') \sim D + D' - gP$; moreover m makes $C^{(g)}$ into a birational group.*

PROOF. Let T be an integral k-scheme. If we identify $C^{(g)}$ with the functor it represents (see (3.13)), then an element of $U(T)$ is a pair of relative effective divisors (D, D') on $C \times T/T$ such that, for all $t \in T$, $h^0(D_t + D'_t - gP) = 1$. Let $\mathscr{L} = \mathscr{L}(D + D' - g \cdot P \times T)$. Then [14, 4.2d] shows that $q_*(\mathscr{L})$ is an invertible sheaf on T. The canonical map $q^*q_*\mathscr{L} \to \mathscr{L}$ when tensored with $(q^*q_*\mathscr{L})^{-1}$ gives a canonical global section $s: \mathcal{O}_T \to \mathscr{L} \otimes (q^*q_*\mathscr{L})^{-1}$, which determines a relative effective divisor $m(D, D')$ of degree g on $C \times T/T$ (see (3.6)). The construction is clearly functorial. Therefore we have constructed a map $m: U \to C^{(g)}$ as functors of integral schemes over k, and this is represented by a map of varieties. On making the map explicit in the case that K is the spectrum of a field, one sees easily that $m(D, D') \sim D + D' - gP$ in this case.

The uniqueness of the map is obvious. Also associativity is obvious since it holds on an open subset of $U(K)$: $m((D, D'), D'') = m(D, (D', D''))$ because each is an effective divisor on C linearly equivalent to $D + D' + D'' - 2gP$, and in general $h^0(D + D' + D'' - 2gP) = 1$.

A similar argument using (7.1b) shows that there is a map $r: V \to C^{(g)}$ such that (p, r) is a birational inverse to

$$(a, b) \mapsto (a, ab): C^{(g)} \times C^{(g)} \dashrightarrow C^{(g)} \times C^{(g)}.$$

Because the law of composition is commutative, this shows that $(a, b) \mapsto (b, ab)$ is also birational. The proof is complete. □

Theorem 7.3. *For any birational group V over k, there is a group variety G over k and a birational map $f: V \dashrightarrow G$ such that $f(ab) = f(a)f(b)$ whenever ab is defined; moreover, G is unique up to a unique isomorphism.*

PROOF. In the case that $V(k)$ is dense in V (for example, k is separably closed), this is proved in [1, §2]. (Briefly, one replaces V by an open subset where m has better properties, and obtains G by patching together copies of translates of U by elements of $V(k)$.) From this it follows that, in the general case, the theorem holds over a finite Galois extension k' of k. Let $\sigma \in \mathrm{Gal}(k'/k)$. Then $\sigma f: \sigma V_{k'} \dashrightarrow \sigma G$ is a birational map, and as $\sigma V_{k'} = V_{k'}$, the uniqueness of G shows that there is a unique isomorphism $\varphi_\sigma: \sigma G \to G$ such that $\varphi_\sigma \circ \sigma f = f$. For any $\sigma, \tau \in \mathrm{Gal}(k'/k)$,

$$(\varphi_\tau \circ \tau\varphi_\sigma) \circ (\tau\sigma f) = \varphi_\tau \circ \tau(\varphi_\sigma \circ \sigma f) = f = \varphi_{\tau\sigma} \circ \tau\sigma f,$$

and so $\varphi_\tau \circ \tau\varphi_\sigma = \varphi_{\sigma\tau}$. Descent theory (see (1.8)) now shows that G is defined over k. □

Let J be the algebraic group associated by (7.3) to the rational group defined in (7.2).

Proposition 7.4. *The variety J is complete.*

PROOF. This can be proved using the valuative criterion of properness. (For Weil's original account, see [20, Théorème 16, et seq.].) □

Corollary 7.5. *The rational map $f: C^{(g)} \dashrightarrow J$ is a morphism. If D and D' are linearly equivalent divisors on C_K for some field K containing k, then $f(D) = f(D')$.*

PROOF. The first statement follows from [14, 3.1]. For the second, recall that if D and D' are linearly equivalent then they lie in a copy of projective space contained in $C^{(g)}$ (see (3.14)). Consequently [14, 3.9] shows that they map to the same point in J. □

We now prove that J has the correct universal property.

Theorem 7.6. *There is a canonical isomorphism of functors* $\iota: P^0_C \to J$.

PROOF. As in Section 4, it suffices to show that P^r_C is representable by J for some r. In this case we take $r = g$. Let $\mathscr{L}$ be an invertible sheaf with fibres of degree g on $C \times T$. If $\dim_k \Gamma(C_t, \mathscr{L}_t) = 1$ for some t, then this holds for all points in an open neighborhood U_t of t. As in the proof of (7.2), we get a relative effective divisor $s: \mathscr{O}_S \to \mathscr{L} \otimes (q^* q_* \mathscr{L})^{-1}$ of degree g on U_t. This family of Cartier divisors defines a map $U_t \to C^{(g)}$ which when composed with f gives a map $\psi_{\mathscr{L}}: U_t \to J$. On the other hand, if $\dim_k \Gamma(C_t, \mathscr{L}_t) > 1$, then we choose an invertible sheaf $\mathscr{L}'$ of degree zero on C such that $\dim(\Gamma(C_t, \mathscr{L}_t \otimes \mathscr{L}')) = 1$, and define $\psi_{\mathscr{L}}: U_t \to C^{(g)}$ on a neighborhood of t to be the composite of $\psi_{\mathscr{L} \otimes p^* \mathscr{L}'}$ with t_{-a}, where $a = f(D)$ for D an effective divisor of degree g such that $\mathscr{L}(D - gP) \approx \mathscr{L}'$. One checks that this map depends only on $\mathscr{L}$, and that the maps for different t agree on the overlaps of the neighborhoods. They therefore define a map $T \to J$. □

Remark 7.7. Weil of course did not show that the Jacobian variety represented a functor on k-schemes. Rather, in the days before schemes, the Jacobian variety was characterized by the universal property in (6.1) or (6.4), and shown to have the property that $\mathrm{Pic}^0(C) \xrightarrow{\approx} J(k)$. See [20] or [9].

§8. Generalizations

It is possible to construct Jacobians for families of curves. Let $\pi: \mathscr{C} \to S$ be a projective flat morphism whose fibres are integral curves. For any S-scheme T of finite-type, define

$$P^r_{\mathscr{C}}(T) = \{\mathscr{L} \in \mathrm{Pic}(\mathscr{C} \times_S T) | \deg(\mathscr{L}_t) = r \text{ all } t\}/\sim,$$

where $\mathscr{L} \sim \mathscr{L}'$ if and only if $\mathscr{L} \approx \mathscr{L}' \otimes q^* \mathscr{M}$ for some invertible sheaf $\mathscr{M}$ on T. (The degree of an invertible sheaf on a singular curve is defined as in the nonsingular case: it is the leading coefficient of $\chi(C, \mathscr{L}^n)$ as a polynomial in n.) Note that $P^r_{\mathscr{C}}$ is a functor on the category of S-schemes of finite-type.

Theorem 8.1. *Let $\pi: \mathscr{C} \to S$ be as above; then there is a group scheme $\mathscr{J}$ over S with connected fibres and a morphism of functors $P^0_{\mathscr{C}} \to \mathscr{J}$ such that $P^0_{\mathscr{C}}(T) \to \mathscr{J}(T)$ is always injective and is an isomorphism whenever $\mathscr{C} \times_S T \to T$ has a section.*

In the case that S is the spectrum of a field (but $\mathscr{C}$ may be singular), the existence of $\mathscr{J}$ can be proved by Weil's method (see [17, V]). When $\mathscr{C}$ is smooth over S, one can show as in Section 3 that $\mathscr{C}^{(r)}$ (quotient of $\mathscr{C} \times_S \dots \times_S \mathscr{C}$ by S_r) represents the functor $\mathrm{Div}^r_{\mathscr{C}/S}$ sending an S-scheme T to the set of relative effective Cartier divisors of degree r on $\mathscr{C} \times_S T/T$. In general one can only show more abstractly that $\mathrm{Div}^r_{\mathscr{C}/S}$ is represented by a Hilbert scheme. There is a canonical map $\mathrm{Div}^r_{\mathscr{C}/S} \to P^r_{\mathscr{C}/S}$ and the second part of the proof deduces the representability of $P^r_{\mathscr{C}/S}$ from that of $\mathrm{Div}^r_{\mathscr{C}/S}$. (The only reference for the proof in the general case seems to be Grothendieck's original rather succinct account [4, Exposé 232]; we sketch some of its ideas below.)

As in the case that the base scheme is the spectrum of a field, the conditions of the theorem determine $\mathscr{J}$ uniquely; it is called the *Jacobian scheme* of $\mathscr{C}/S$. Clearly $\mathscr{J}$ commutes with base change: the Jacobian of $\mathscr{C} \times_S T$ over T is $\mathscr{J} \times_S T$. In particular, if $\mathscr{C}_t$ is a smooth curve over $k(t)$, then $\mathscr{J}_t$ is the Jacobian of $\mathscr{C}_t$ in the sense of Section 1. Therefore if $\mathscr{C}$ is smooth over S, then $\mathscr{J}$ is an abelian scheme, and we may think of it as a family of Jacobian varieties. If $\mathscr{C}$ is not smooth over S, then $\mathscr{J}$ need not be proper, even in the case that S is the spectrum of a field.

Example 8.2. Let C be complete smooth curve over an algebraically closed field k. By a *modulus* for C one means simply an effective divisor $\mathfrak{m} = \sum n_P P$ on C. Let $\mathfrak{m}$ be such a modulus, and assume that $\deg(\mathfrak{m}) \geq 2$. We shall associate with C and $\mathfrak{m}$ a new curve $C_{\mathfrak{m}}$ having a single singularity at a point to be denoted by Q. The underlying topological space of $C_{\mathfrak{m}}$ is $(C - S) \cup \{Q\}$, where S is the support of $\mathfrak{m}$. Let $\mathscr{O}_Q = k + \mathfrak{c}_Q$, where

$$\mathfrak{c}_Q = \{f \in k(C) | \mathrm{ord}(f) \geq n_P \text{ all } P \text{ in } S\},$$

and define $\mathscr{O}_{C_{\mathfrak{m}}}$ to be the sheaf such that $\Gamma(U, \mathscr{O}_{C_{\mathfrak{m}}}) = \bigcap \mathscr{O}_P$, where the intersection is over the P in U. The Jacobian scheme $J_{\mathfrak{m}}$ of $C_{\mathfrak{m}}$ is an algebraic group over k called the *generalized Jacobian of C relative to $\mathfrak{m}$*. By definition, $J_{\mathfrak{m}}(k)$ is the group of isomorphism classes of invertible sheaves on $C_{\mathfrak{m}}$ of degree 0. It can also be described as the group of divisors of degree 0 on C relatively prime to $\mathfrak{m}$, modulo the principal divisors defined by elements congruent to 1 modulo $\mathfrak{m}$ (an element of $k(C)$ is congruent to 1 modulo $\mathfrak{m}$ if $\mathrm{ord}_P(f - 1) \geq n_P$ for all P in S). For each modulus $\mathfrak{m}$ with support on S there is a canonical map $f_{\mathfrak{m}}: C - S \to J_{\mathfrak{m}}$, and these maps are universal in the following sense: for any morphism $f: C - S \to G$ from $C - S$ into an algebraic group, there is a modulus $\mathfrak{m}$ and a homomorphism $\varphi: J_{\mathfrak{m}} \to G$ such that f is the composite of $f_{\mathfrak{m}} \circ \varphi$ with a translation. (For a detailed account of this theory, see [17].)

We now give a brief sketch of part of Grothendieck's proof of (8.1). First we need the notion of the Grassmann scheme.

Let $\mathscr{E}$ be a locally free sheaf of $\mathscr{O}_S$-modules of finite rank, and, for an S-scheme T of finite-type, define $\mathrm{Grass}^{\mathscr{E}}_n(T)$ to be the set of isomorphism classes of pairs $(\mathscr{V}, h)$, where $\mathscr{V}$ is a locally free $\mathscr{O}_T$-module of rank n and h is an epimorphism $\mathscr{O}_T \otimes_k \mathscr{E} \twoheadrightarrow \mathscr{V}$. For example, if $\mathscr{E} = \mathscr{O}^m_S$, then $\mathrm{Grass}^{\mathscr{E}}_n(T)$ can be identified with the set of isomorphism classes of pairs $(\mathscr{V}, (e_1, \dots, e_m))$ where $\mathscr{V}$ is a locally free sheaf of rank n on T and the e_i are sections of $\mathscr{V}$ over T that generate $\mathscr{V}$; two such pairs $(\mathscr{V}, (e_1, \dots, e_m))$ and $(\mathscr{V}', (e'_1, \dots, e'_m))$

are isomorphic if there is an isomorphism $\mathscr{V} \xrightarrow{\approx} \mathscr{V}'$ carrying each e_i to e'_i. In particular, $\mathrm{Grass}_1^{\mathcal{O}^{N+1}}(T) = \mathbb{P}_S^N(T)$ (cf. [8, II, 7.1]).

Proposition 8.3. *The functor $T \mapsto \mathrm{Grass}_n^{\mathscr{E}}(T)$ is representable by a projective variety $G_n^{\mathscr{E}}$ over S.*

PROOF. The construction of $G_n^{\mathscr{E}}$ is scarcely more difficult than that of $\mathbb{P}_S^N$ (see [7, 9.7]). □

Choose an $r > 2g - 2$ and an $m > 2g - 2 + r$. As in the case that S is the spectrum of a field, we first need to construct the Jacobian under the assumption that there is a section $s: S \to \mathscr{C}$. Let E be the relative effective divisor on $\mathscr{C}/S$ defined by s (see (3.9)), and for any invertible sheaf $\mathscr{L}$ on $\mathscr{C} \times_S T$, write $\mathscr{L}(m)$ for $\mathscr{L} \otimes \mathscr{L}(mE)$. The first step is to define an embedding of $\mathrm{Div}^r_{\mathscr{C}/S}$ into a suitable Grassmann scheme.

Let $D \in \mathrm{Div}^r_{\mathscr{C}/S}(T)$, and consider the exact sequence

$$0 \to \mathscr{L}(-D) \to \mathcal{O}_{\mathscr{C}\times T} \to \mathcal{O}_D \to 0$$

on $\mathscr{C} \times_S T$ (we often drop the S from $\mathscr{C} \times_S T$). This gives rise to an exact sequence

$$0 \to \mathscr{L}(-D)(m) \to \mathcal{O}_{\mathscr{C}\times T}(m) \to \mathcal{O}_D(m) \to 0,$$

and on applying q_* we get an exact sequence

$$0 \to q_*\mathscr{L}(-D)(m) \to q_*\mathcal{O}_{\mathscr{C}\times T}(m) \to q_*\mathcal{O}_D(m) \to R^1q_*\mathscr{L}(-D)(m) \to \cdots.$$

Note that, for all t in T, $H^1(\mathscr{C}_t, \mathscr{L}(-D)(m))$ is dual to $H^0(C_t, \mathscr{L}(K + D - mE_t))$, where E_t is the divisor $s(t)$ of degree one on $\mathscr{C}_t$. Because of our assumptions, this last group is zero, and so (see [14, 4.2e]) $R^1q_*\mathscr{L}(-D)(m)$ is zero and we have an exact sequence

$$0 \to q_*\mathscr{L}(-D)(m) \to q_*\mathcal{O}_{\mathscr{C}\times T}(m) \to q_*\mathcal{O}_D(m) \to 0.$$

Moreover $q_*\mathcal{O}_D(m)$ is locally free of rank r, and $q_*(\mathcal{O}_{\mathscr{C}\times T}(m)) = q_*\mathcal{O}_{\mathscr{C}}(m) \otimes \mathcal{O}_T$ (loc. cit.), and so we have constructed an element $\Phi(D)$ of $\mathrm{Grass}_r^{q_*\mathcal{O}_{\mathscr{C}}(m)}(T)$.

On the other hand, suppose $a = (q_*\mathcal{O}_{\mathscr{C}\times T}(m) \twoheadrightarrow \mathscr{V})$ is an element of $\mathrm{Grass}_r^{q_*\mathcal{O}_{\mathscr{C}}(m)}(T)$. If $\mathscr{K}$ is the kernel of $q^*q_*\mathcal{O}_{\mathscr{C}\times T}(m) \twoheadrightarrow q^*\mathscr{V}$, then $\mathscr{K}(-m)$ is a subsheaf of $q^*q_*\mathcal{O}_{\mathscr{C}\times T}$, and its image under $q^*q_*\mathcal{O}_{\mathscr{C}\times T} \to \mathcal{O}_{\mathscr{C}\times T}$ is an ideal in $\mathcal{O}_{\mathscr{C}\times T}$. Let $\Psi(a)$ be the subscheme associated to this ideal. It is clear from the constructions that $\Psi\Phi(D) = D$ for any relative divisor of degree r. We have a diagram of natural transformations

$$\mathrm{Div}^r_{\mathscr{C}}(T) \,\Phi\, \mathrm{Grass}_r^{q_*\mathcal{O}_{\mathscr{C}}(m)}(T) \,\Psi\, \mathscr{S}(T) \supset \mathrm{Div}^r_{\mathscr{C}}(T), \qquad \Psi\Phi = \mathrm{id},$$

where $\mathscr{S}(T)$ denotes the set of all closed subschemes of $\mathscr{C} \times_S T$. In particular, we see that Φ is injective.

Proposition 8.4. *The functor Φ identifies $\mathrm{Div}^r_{\mathscr{C}}$ with a closed subscheme of $\mathrm{Grass}_r^{q_*\mathcal{O}_{\mathscr{C}}(m)}$.*

PROOF. See [4, Exposé 221, p. 12] (or, under different hypotheses, [15, Lecture 15]). □

Finally, one shows that the fibres of the map $\mathrm{Div}^r_{\mathscr{C}/S} \to P^r_{\mathscr{C}/S}$ are represented by the projective space bundles associated with certain sheaves of $\mathcal{O}_S$-modules ([4, Exposé 232, p. 11]; cf. (5.6c)) and deduces the representability of $P^r_{\mathscr{C}/S}$ (loc. cit.).

§9. Obtaining Coverings of a Curve from its Jacobian; Application to Mordell's Conjecture

Let V be a variety over field k, and let $\pi: W \to V$ be a finite étale map. If there is a finite group G acting freely on W by V-morphisms in such a way that $V = G\backslash W$, then (W, π) is said to be Galois covering of V with Galois group G. When G is abelian, then (W, π) is said to be an abelian covering of V. Fix a point P on V. Then the Galois coverings of V are classified by the (étale) fundamental group $\pi_1(V, P)$ and the abelian coverings by the maximal abelian quotient $\pi_1(V, P)^{\mathrm{ab}}$ of $\pi_1(V, P)$. For any finite abelian group M, $\mathrm{Hom}(\pi_1(V, P), M)$ (set of continuous homomorphisms) is equal to the set of isomorphism classes of Galois coverings of V with Galois group M. If, for example, V is nonsingular and we take P to be the generic point of V, then every finite connected étale covering of V is isomorphic to the normalization of V in some finite extension of K' of $k(P)$ contained in a fixed algebraic closure $\bar{K}$ of K; moreover, $\pi_1(V, P) = \mathrm{Gal}(K^{\mathrm{un}}/K)$ where K^{un} is the union of all finite extensions K' of $k(P)$ in $\bar{K}$ such that the normalization of V in K' is étale over V. The covering corresponding to a continuous homomorphism $\alpha: \mathrm{Gal}(K^{\mathrm{un}}/K) \to M$ is the normalization of V in $\bar{K}^{\mathrm{Ker}(\alpha)}$. (See [13, I, 5] for a more detailed discussion of étale fundamental groups.)

Now let C be a complete nonsingular curve over a field k, and let $f = f^P$ for some P in $C(k)$. From a finite étale covering $J' \to J$ of J, we obtain an étale covering of C by pulling back relative to f:

$$\begin{array}{ccc} J' & \leftarrow & C' = C \times_J J' \\ \downarrow & & \downarrow \\ J & \xleftarrow{f} & C. \end{array}$$

Because all finite étale coverings of J are abelian (cf. [14, 15.3]), we only obtain abelian coverings of C in this way. The next proposition shows that we obtain all such coverings.

Henceforth, k will be separably closed.

Proposition 9.1. *If $J' \to J$ is a connected étale covering of J, then $C' = C \times_J J' \to C$ is a connected étale covering of C, and every connected abelian covering of C is obtained in this way. Equivalently, the map $\pi_1(C, P)^{\mathrm{ab}} \to \pi_1(J, 0)$ induced by f^P is an isomorphism.*

PROOF. The equivalence of the two assertions follows from the interpretation of $\mathrm{Hom}(\pi_1(V, P), M)$ recalled above and the fact that $\pi_1(J, 0)$ is abelian. We shall prove the second assertion. For this it suffices to show that for all integers n, the map $\mathrm{Hom}(\pi_1(J, 0), \mathbb{Z}/n\mathbb{Z}) \to \mathrm{Hom}(\pi_1(C, P), \mathbb{Z}/n\mathbb{Z})$ induced by f^P is an isomorphism. The next two lemmas take care of the case that n is prime to the characteristic of k.

Lemma 9.2. *Let V be complete nonsingular variety and let P be a point of V; then for all integers n prime to the characteristic of k, $\mathrm{Hom}(\pi_1(V, P), \mathbb{Z}/n\mathbb{Z}) \approx \mathrm{Pic}(V)_n$.*

PROOF. Let D be a (Weil) divisor on V such that $nD = (g)$ for some $g \in k(V)$, and let V' be the normalization of V in the Kummer extension $k(V)(g^{1/n})$ of $k(V)$. A purity theorem [5, X.3.1] shows that $V' \to V$ is étale if, for all prime divisors Z on V, the discrete valuation ring $\mathcal{O}_Z$ (local ring at the generic point of Z) is unramified in $k(V')$. But the extension $k(V')/k(V)$ was constructed by extracting the nth root of an element g such that $\mathrm{ord}_Z(g) = 0$ if Z is not in the support of D and is divisible by n otherwise, and it follows from this that $\mathcal{O}_Z$ is unramified. Conversely, let $V' \to V$ be a Galois covering with Galois group $\mathbb{Z}/n\mathbb{Z}$. Kummer theory shows that the $k(V')/k(V)$ is obtained by extracting the nth root of an element g of $k(V)$. Let Z be a prime divisor on V. Because $\mathcal{O}_Z$ is unramified in $k(V')$, $\mathrm{ord}_Z(g)$ must be divisible by n (or is zero), and so $(g) = nD$ for some divisor D. Obviously D represents an element of $\mathrm{Pic}(V)_n$. It is easy to see now that the correspondence we have defined between coverings of V and elements of $\mathrm{Pic}(V)_n$ is one-to-one. (For a proof using étale cohomology, see [14, III, 4.11].) □

Lemma 9.3. *The map $\mathrm{Pic}(J) \to \mathrm{Pic}(C)$ defined by f induces an isomorphism $\mathrm{Pic}^0(J) \to \mathrm{Pic}^0(C)$.*

PROOF. This was noted in (6.10c). □

In the case that $n = p = \mathrm{characteristic}(k)$, (9.2) and (9.3) must be replaced by the following analogues.

Lemma 9.4. *For any complete nonsingular variety V and point P, $\mathrm{Hom}(\pi_1(V, P), \mathbb{Z}/p\mathbb{Z}) \approx \mathrm{Ker}(1 - F\colon H^1(V, \mathcal{O}_V) \to H^1(V, \mathcal{O}_V))$, where F is the map induced by $a \mapsto a^p\colon \mathcal{O}_V \to \mathcal{O}_V$.*

PROOF. See [14, p. 127] for a proof using étale cohomology as well as for hints for an elementary proof. □

Lemma 9.5. *The map $f^P\colon C \to J$ induces an isomorphism $H^1(J, \mathcal{O}_J) \to H^1(C, \mathcal{O}_C)$.*

PROOF. See [17, VII, Théorème 9]. (Alternatively, note that the same argument as in the proof of (2.1) gives an isomorphism $H^1(J, \mathcal{O}_J) \xrightarrow{\approx} T_0(J^\vee)$, and we know that $J \approx J^\vee$.) □

To prove the case $n = p^m$, one only has to replace $\mathcal{O}_C$ and $\mathcal{O}_J$ by the sheaves of Witt vectors of length m, $W_m\mathcal{O}_C$ and $W_m\mathcal{O}_J$. (It is also possible to use a five-lemma argument starting from the case $m = 1$.)

Corollary 9.6. *For all primes l, the map of étale cohomology groups $H^1(J, \mathbb{Z}_l) \to H^1(C, \mathbb{Z}_l)$ induced by f is an isomorphism.*

PROOF. For any variety V, $H^1(V_{et}, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\pi_1(V, P), \mathbb{Z}/n\mathbb{Z})$ [13, III, 4]. Therefore, there are isomorphisms

$$H^1(J, \mathbb{Z}/l^m\mathbb{Z}) \xrightarrow{\approx} \mathrm{Hom}(\pi_1(J, P), \mathbb{Z}/l^m\mathbb{Z}) \xrightarrow{\approx} \mathrm{Hom}(\pi_1(C, P), \mathbb{Z}/l^m\mathbb{Z}) \xrightarrow{\approx} H^1(C, \mathbb{Z}/l^m\mathbb{Z}),$$

and we obtained the required isomorphism by passing to the limit. □

To obtain ramified coverings of C, one can use the generalized Jacobians.

Proposition 9.7. *Let $C' \to C$ be a finite abelian covering of C that is unramified outside a finite set Σ. Then there is a modulus $\mathfrak{m}$ with support on Σ and an étale isogeny $J' \to J_{\mathfrak{m}}$ whose pull-back by $f_{\mathfrak{m}}$ is $C' - f^{-1}(\Sigma)$.*

PROOF. See [17]. □

Example 9.8. In the case that the curve is $\mathbb{P}^1$ and $\mathfrak{m} = 0 + \infty$, we have $J_{\mathfrak{m}} = \mathbb{P}^1 - \{0, \infty\}$, which is just the multiplicative group GL_1, and $f_{\mathfrak{m}}$ is an isomorphism. For any n prime to the characteristic, there is a unique unramified covering of $\mathbb{P}^1 - \{0, \infty\}$ of degree n, namely multiplication by n on $\mathbb{P}^1 - \{0, \infty\}$. When $k = \mathbb{C}$, this covering is the usual unramified covering $z \mapsto z^n\colon \mathbb{C} - \{0\} \to \mathbb{C} - \{0\}$.

Proposition 9.9. *Let C be a curve of genus g over a number field k, and let P be a k-rational point of C. Let S be a finite set of primes of k containing all primes dividing 2 and such that C has good reduction outside S. Then there exists a field k' of degree $\le 2^{2g}$ over k and unramified outside S, and a finite map $f_P\colon C_P \to C_{k'}$ of degree $\le 2^{2^{2g}(g-1)+2g+1}$, ramified exactly over P, and such that C_P has good reduction outside S.*

PROOF. *Sketch.* Let C' be the pull-back of $2\colon J \to J$; it is an abelian étale covering of C of degree 2^{2g}, and the Hurwitz genus formula [8, IV, 2.4] shows that the genus g' of C' satisfies

$$2g' - 2 = 2^{2g}(2g - 2),$$

so that $g' = 2^{2g}(g - 1) + 1$. Let D be the inverse image of P on C'. It is a divisor of degree 2^{2g} on C', and after an extension k' of k of degree $\leq 2^{2g}$ unramified over S, some point P of D will be rational. Let $\mathfrak{m} = D - P'$, and let C'' be the pull-back of the covering $2\colon J_{\mathfrak{m}} \to J_{\mathfrak{m}}$ (of degree $\leq 2^{2g'}$) by $C - \Sigma \to J_{\mathfrak{m}}$, where $\Sigma = \operatorname{Supp}(D) - \{P\}$. Then C'' is a curve over k', and we take C_P to the associated complete nonsingular curve. □

This result has a very striking consequence. Recall that a conjecture of Shafarevich states the following:

(9.10) *For any number field k, integer g, and finite set S of primes of k, there are only finitely many isomorphism classes of curves C of genus g over k having good reduction at all primes outside S.*

Theorem 9.11. *Shafarevich's conjecture (9.10) implies Mordell's conjecture.*

PROOF. Let C be curve of genus $g \geq 2$ over k with good reduction outside a set S containing all primes of k lying over 2. There is a finite field extension K of k containing all extensions k' of k of degree $\leq 2^{2g}$ that are unramified outside S. For each k-rational point P on C, Proposition 9.9 provides a map $f_P\colon C_P \to C_K$ of degree $\leq$ a fixed bound $B(g)$ which is ramified exactly over P; moreover, C_P has good reduction outside S. The Hurwitz genus formula shows that

$$2g(C_P) - 2 \leq B(g)(2g - 2) + B(g) - 1.$$

Therefore Shafarevich's conjecture implies that there can be only finitely many curves C_P. A classical result of de Franchis [10, p. 223] states that for each C_P, there are only finitely many maps $C_P \to C$ (this is where it is used that $g \geq 2$). Therefore there can be only finitely many k-rational points on C, as predicted by Mordell. □

§10. Abelian Varieties Are Quotients of Jacobian Varieties

The main result in this section sometimes allows questions concerning abelian varieties to be reduced to the special case of Jacobian varieties.

Theorem 10.1. *For any abelian variety A over an infinite field k, there is a Jacobian variety J and a surjective homomorphism $J \twoheadrightarrow A$.*

Lemma 10.2. *Let $\pi\colon W \to V$ be a finite morphism of complete varieties, and let $\mathscr{L}$ be an invertible sheaf on V. If $\mathscr{L}$ is ample, then so also is $\pi^*\mathscr{L}$.*

PROOF. We shall use the following criterion ([8, III, 5.3]): an invertible sheaf

$\mathscr{L}$ on a complete variety is ample if and only if, for all coherent $\mathscr{O}_V$-modules $\mathscr{F}$, $H^i(V, \mathscr{F} \otimes \mathscr{L}^n) = 0$ for all $i > 0$ and sufficiently large n. Also we shall need an elementary projection formula: if $\mathscr{N}$ and $\mathscr{M}$ are coherent sheaves of modules on W and V respectively, then

$$\pi_*(\mathscr{N} \otimes \pi^*\mathscr{M}) \approx \pi_*\mathscr{N} \otimes \mathscr{M}.$$

(Locally, this says that if B is an A-algebra and N and M are modules over B and A respectively, then $N \otimes_B (B \otimes_A M) \approx N \otimes_A M$ as A-modules.)

Let $\mathscr{F}$ be a coherent $\mathscr{O}_W$-module. Because π is finite (hence affine), we have by [8, II, Ex. 4.1 or Ex. 8.2] that

$$H^i(W, \mathscr{F} \otimes \pi^*\mathscr{L}^n) \approx H^i(V, \pi_*(\mathscr{F} \otimes \pi^*\mathscr{L}^n)).$$

The projection formula shows that the second group equals $H^i(V, \pi_*\mathscr{F} \otimes \mathscr{L}^n)$, which is zero for all $i > 0$ and sufficiently large n because $\mathscr{L}$ is ample and $\pi_*\mathscr{F}$ is coherent ([8, 4.1]). The criterion now shows that $\pi^*\mathscr{L}$ is ample. □

Lemma 10.3. *Let V be a nonsingular projective variety of dimension ≥ 2 over a field k, and let Z be a hyperplane section of V relative to some fixed embedding $V \subset \mathbb{P}^n$. Then, for any finite map π from a nonsingular variety W to V, $\pi^{-1}(Z)$ is geometrically connected (that is, $\pi^{-1}(Z)_{\bar{k}}$ is connected).*

PROOF. The hypotheses are stable under a change of the base field, and so we can assume that k is algebraically closed. It then suffices to show that $\pi^{-1}(Z)$ is connected. Because Z is an ample divisor on V, the preceding lemma shows that $\pi^{-1}(Z)$ is the support of an ample divisor on W, which implies that it is connected ([8, III, 7.9]). □

We now prove the theorem. Since all elliptic curves are their own Jacobians, we can assume that $\dim(A) > 1$. Fix an embedding $A \subset \mathbb{P}^n$ of A into projective space. Then Bertini's theorem [8, II, 8.18] shows that there exists an open dense subset U of the dual projective space $\mathbb{P}_k^{n\vee}$ of $\mathbb{P}_k^n$ such that, for all hyperplanes H in U, $A_{\bar{k}} \cap H$ is nonsingular and connected. Because k is infinite, $U(k)$ is nonempty (consider a line L in $\mathbb{P}_k^{n\vee}$), and so there exists such an H with coordinates in k. Then $A \cap H$ is a (geometrically connected) nonsingular variety in $\mathbb{P}^n$. On repeating the argument $\dim(A) - 1$ times, we arrive at a nonsingular curve C on A that is the intersection of A with a linear subspace of $\mathbb{P}^n$. Now (10.3) applied several times shows that for any nonsingular variety W and finite map $\pi\colon W \to A$, $\pi^{-1}(C)$ is geometrically connected.

Consider the map $J \to A$ arising from the inclusion of C into A, and let A_1 be the image of the map. It is an abelian subvariety of A, and if it is not the whole of A, then there is an abelian subvariety A_2 of A such that $A_1 \times A_2 \to A$ is an isogeny (see [14, 12.1]); in particular, $A_1 \cap A_2$ is finite. As $C \subset A_1$, this implies that $C \cap A_2$ is finite. Let $W = A_1 \times A_2$ and take π to be the composite of $1 \times n_{A_2}\colon A_1 \times A_2 \to A_1 \times A_2$ with $A_1 \times A_2 \to A$, where

$n > 1$ is an integer prime to the characteristic of k. Then $\pi^{-1}(C)$ is not geometrically connected. This is a contradiction, and so A_1 must equal A.

Remark 10.4. (a) Lemma 10.2 has the following useful restatement: let V be a variety over a field k and let D be divisor on V such that the linear system $|D|$ is without base points; if the map $V \to \mathbb{P}^n$ defined by $|D|$ is finite, then D is ample.

(b) If some of the major theorems from étale cohomology are assumed, then it is possible to give a very short proof of the theorem. They show that, for any curve C on A constructed as in the above proof, the map $H^1(A, \mathbb{Z}_l) \to H^1(C, \mathbb{Z}_l)$ induced by the inclusion of C into A is injective (see [13, VI.5.6]). But $H^1(A, \mathbb{Z}_l)$ is dual to $T_l A$ and $H^1(C, \mathbb{Z}_l)$ is dual to $T_l J$, and so this says that the map $T_l J \to T_l A$ induced by $J \to A$ is surjective. Clearly this implies that J maps onto A.

Open Question 10.5. Let A be an abelian variety over an algebraically closed field k. We have shown that there is a surjection $J \twoheadrightarrow A$ with J a Jacobian variety. Let A_1 be the subvariety of J with support the identity component of the kernel of this map. Then A_1 is an abelian variety, and so there is a surjection $J_1 \twoheadrightarrow A_1$. Continuing in this way, we obtain a sequence of abelian varieties $A, A_1, A_2, \ldots$ and a complex

$$\cdots \to J_2 \to J_1 \to A \to 0.$$

Is it possible to make the constructions in such a way that the sequence terminates with 0? That is, does there exist a resolution (up to isogeny) of an arbitrary abelian variety by Jacobian varieties?

§11. The Zeta Function of a Curve

[Joe W. said [illegible] contains [illegible]]

Let C be a complete nonsingular curve over a finite field $k = \mathbb{F}_q$. The best way to prove the Riemann hypothesis for C is to use intersection theory on $C \times C$ (see [8, V, Ex. 1.10]), but in this section we show how it can be derived from the corresponding result for the Jacobian of C. Recall [14, §19] that the characteristic polynomial of the Frobenius endomorphism π_J of J acting on $T_l J$ is a polynomial $P(X)$ of degree $2g$ with integral coefficients whose roots a_i have absolute value $q^{1/2}$.

Theorem 11.1. *The number N of points on C with coordinates in k is equal to $1 - \sum a_i + q$. Therefore, $|N - q - 1| \le 2gq^{1/2}$.*

The proof will be based on the following analogue of the Lefschetz trace formula. A map $\alpha\colon C \to C$ induces a unique endomorphism α' of J such that $f^P \circ \alpha = \alpha' \circ f^P$ for any point P in $C(\bar{k})$ (cf. (6.1)).

Proposition 11.2. *For any endomorphism α of C,*

$$(\Gamma_\alpha \cdot \Delta) = 1 - \operatorname{Tr}(\alpha') + \deg(\alpha).$$

Recall [14, §12] that if $P_{\alpha'}(X) = \prod (X - a_i)$, then $\operatorname{Tr}(\alpha) = \sum a_i$, and that $\operatorname{Tr}(\alpha') = \operatorname{Tr}(\alpha' | T_l J)$. We now show that the proposition implies the theorem. Let $\pi_C\colon C_{\bar{k}} \to C_{\bar{k}}$ be the Frobenius endomorphism of C (see [14, §19]). Before proving (11.2) we need a lemma.

Lemma 11.3. *Let A be an abelian variety of dimension g over a field k, and let H be the class of an ample divisor in $\mathrm{NS}(A)$. For any endomorphism α of A, write $D_H(\alpha) = (\alpha + 1)^*(H) - \alpha^*(H) - H$. Then*

$$\operatorname{Tr}(\alpha) = g\frac{(H^{g-1} \cdot D_H(\alpha))}{(H^g)}.$$

PROOF. The calculation in [14, 12.4] shows that

$$(\alpha + n)^*(H) = n(n-1)H + n(\alpha + 1)^*H - (n-1)\alpha^*(H)$$

(because $(2_A)^*H = 4H$ in $\mathrm{NS}(A)$), and so

$$(\alpha + n)^*H = n^2 H + nD_H(\alpha) + \alpha^*(H).$$

Now the required identity can be read off from the equation

$$P_\alpha(-n) = \deg(\alpha + n) = (((\alpha + n)^*H)^g)/(H^g) \qquad \text{(see [14, 8.3])}$$

because $P_\alpha(-n) = n^{2g} + \operatorname{Tr}(\alpha)n^{2g-1} + \cdots$. □

We now prove (11.2). Consider the commutative diagram

$$\begin{array}{ccccc} C \times C & \xrightarrow{f \times f} & J \times J & \xrightarrow{1 \times \alpha'} & J \times J \\ \Delta\uparrow & & \Delta\uparrow & & \\ C & \xrightarrow{f} & J & & \end{array}$$

where $f = f^P$ for some rational point P of C. Consider the sheaf $\mathscr{L}'(\Theta) \overset{\text{df}}{=} \mathscr{L}(m^*\Theta - \Theta \times J - J \times \Theta)$ on $J \times J$ (see Section 6). Then

$$((1 \times \alpha')(f \times f))^*\mathscr{L}'(\Theta) = ((f \times f)(1 \times \alpha))^*\mathscr{L}'(\Theta)$$
$$\approx (1 \times \alpha)^*(f \times f)^*\mathscr{L}'(\Theta) \approx (1 \times \alpha)^*(\mathscr{L}^P)^{-1}$$

by a formula in (6.11). Now

$$\Delta^*(1 \times \alpha)^*\mathscr{L}^P = \mathscr{L}(\Gamma_\alpha \cdot (\Delta - P \times C - C \times P)),$$

which has degree $(\Gamma_\alpha \cdot \Delta) - 1 - \deg(\alpha)$. We next compute the sheaf by going round the diagram the other way. As $(1 \times \alpha) \circ \Delta = (1, \alpha)$, we have

$$((1 \times \alpha) \circ \Delta)^*\mathscr{L}(m^*\Theta) \approx (1 + \alpha)^*\mathscr{L}(\Theta) \quad \text{and}$$
$$\deg f^*\mathscr{L}((1 + \alpha)^*(\Theta)) = \deg f^*(1 + \alpha)^*\Theta.$$

Similarly $\deg f^*((1 \times \alpha)\circ\Delta)^*\mathscr{L}(\Theta \times J) \approx \deg f^*\Theta$ and

$$\deg f^*((1 \times \alpha)\circ\Delta)^*\mathscr{L}(J \times \Theta) = \deg f^*(\alpha^*\theta),$$

and so we find that

$$1 - (\Gamma_\alpha \cdot \Delta) + \deg(\alpha) = \deg f^*(D_\Theta(\alpha)).$$

We know (6.12) that $(\Theta^g) = g!$, and it is possible to show that $f^*(D_\Theta(\alpha)) = (f(C) \cdot D_\Theta(\alpha))$ is equal to $(g-1)!(\Theta^{g-1} \cdot D_\Theta(\alpha))$ (see [9, IV, §3]). Therefore (11.3) completes the proof. □

Corollary 11.4. *The zeta function of C is equal to*

$$Z(C, t) = \frac{P(t)}{(1-t)(1-qt)}.$$

Remark 11.5. As we saw in (9.6), $H^1(C_{et}, \mathbb{Z}_l) = H^1(J_{et}, \mathbb{Z}_l) = (T_l J)^\vee$, and so (11.2) can be rewritten as

$$(\Gamma_\alpha \cdot \Delta) = \sum (-1)^i \operatorname{Tr}(\alpha | H^i(C_{et}, \mathbb{Z}_l)).$$

§12. Torelli's Theorem: Statement and Applications

Torelli's theorem says that a curve C is uniquely determined by its canonically polarized Jacobian (J, λ).

Theorem 12.1. *Let C and C' be complete smooth curves over an algebraically closed field k, and let $f: C \to J$ and $f': C' \to J'$ be the maps of C and C' into their Jacobians defined by points P and P' on C and C'. Let $\beta: (J, \lambda) \to (J', \lambda')$ be an isomorphism from the canonically polarized Jacobian of C to that of C'.*

(a) *There exists an isomorphism $\alpha: C \to C'$ such that $f' \circ \alpha = \pm\beta \circ f + c$, for some c in $J'(k)$.*

(b) *Assume that C has genus ≥ 2. If C is not hyperelliptic, then the map α, the sign $\pm$, and c are uniquely determined by β, P, P'. If C is hyperelliptic, the sign can be chosen arbitrarily, and then α and c are uniquely determined.*

PROOF. (a) The proof involves complicated combinatorial arguments in the W^r—we defer it to the next section.

(b) Recall [8, IV, 5] that a curve C is hyperelliptic if there is a finite map $\pi: C \to \mathbb{P}^1$ of degree 2; the fibres of such a map form a linear system on C of degree 2 and dimension 1, and this is the unique such linear system on C. Conversely if C has a linear system of degree 2 and dimension 1, then the linear system defines a finite map $\pi: C \to \mathbb{P}^1$ of degree 2, and so C is hyperelliptic; the fibres of π are the members of the linear system, and so the nontrivial automorphism ι of C such that $\pi \circ \iota = \pi$ preserves these individual members.

Now suppose that there exist α, α', c, and c' such that

$$\begin{aligned} f' \circ \alpha &= +\beta \circ f + c \\ f' \circ \alpha' &= +\beta \circ f + c' \end{aligned} \qquad (12.1.1)$$

Then $f'(\alpha(Q)) - f'(\alpha'(Q)) = c - c'$ for all $Q \in C(k)$, which is a constant. Since the fibres of the map $\operatorname{Div}^0_C(k) \to J(k)$ defined by f' are the linear equivalence classes (see Section 2), this implies that for all Q and Q' in $C(k)$,

$$\alpha(Q) - \alpha'(Q) \sim \alpha(Q') - \alpha'(Q'), \quad \text{or}$$
$$\alpha(Q) + \alpha'(Q') \sim \alpha'(Q) + \alpha(Q').$$

Suppose $\alpha \neq \alpha'$. Then $\alpha(Q_0) \neq \alpha'(Q_0)$ for some $Q_0 \in C(k)$ and, for a suitable Q'_0, $\alpha(Q_0) \neq \alpha(Q'_0)$. Therefore $|\alpha(Q_0) + \alpha'(Q'_0)|$ is a linear system of dimension ≥ 1 (and degree 2) on C'. If C (hence C') is nonhyperelliptic, there is no such system, and we have a contradiction. If C is hyperelliptic, then there is a map $\pi: C \to \mathbb{P}^r$ of degree 2 such that $\pi(\alpha(Q)) = \pi(\alpha'(Q'))$ for all Q, Q'. Again we have a contradiction. We conclude that $\alpha = \alpha'$, and this implies that $c = c'$.

On the other hand, suppose that the equations (12.1.1) hold with different signs, say with a plus and a minus respectively. Then the same argument shows that

$$\alpha(Q) + \alpha'(Q) \sim \alpha(Q') + \alpha'(Q'), \quad \text{all } Q, Q' \text{ in } C(k).$$

Therefore $\{\alpha(Q) + \alpha'(Q) | Q \in C(k)\}$ is a linear system on C' of dimension ≥ 1, which is impossible if C is nonhyperelliptic. (In the case C is hyperelliptic, there is an involution ι of C' such that $\iota \circ \alpha = \alpha'$.)

The case that the equations (12.1.1) hold with minus signs can be treated the same way as the first case.

Finally let C' be hyperelliptic with an involution ι such that $|Q' + \iota Q'|$ is a linear system and $f'(Q') + f'(\iota Q') = $ constant. Then if $f' \circ \alpha = \beta \circ f + c$, we have $f' \circ \iota\alpha = -\beta \circ f + c'$. □

Corollary 12.2. *Let C and C' be curves of genus ≥ 2 over a perfect field k. If the canonically polarized Jacobian varieties of C and C' are isomorphic over k, then so also are C and C'.*

PROOF. Choose an isomorphism $\beta: (J, \lambda) \to (J', \lambda')$ defined over k. For each choice of a pair of points P and P' in $C(\bar{k})$ and $C'(\bar{k})$, there is a unique isomorphism $\alpha: C \to C'$ such that

$$f^{P'} \circ \alpha = \pm\beta \circ f^P + c$$

for some c in $J'(k)$ (in the case that C is hyperelliptic, we choose the sign to be +). Note that if (P, P') are replaced by the pair (Q, Q'), then $f^Q = f^P + d$ and $f^{Q'} = f^{P'} + e$ for some $d \in J(\bar{k})$ and $e \in J'(\bar{k})$, and so

$$f^{Q'} \circ \alpha = f^{P'} \circ \alpha + e = \pm\beta \circ f^P + c + e = \pm\beta \circ f^Q \mp \beta(d) + c + e.$$

In particular, we see that α does not depend on the choice of the pair (P, P'). On applying $\sigma \in \mathrm{Gal}(\bar{k}/k)$ to the above equation, we obtain an equation

$$\sigma f^{P'} \circ \sigma\alpha = \pm\beta \circ \sigma f^{P} + \sigma c.$$

As $\sigma f^{P'} = f^{\sigma P'}$ and $\sigma f^{P} = f^{\sigma P}$, we see that $\sigma\alpha = \alpha$, and so α is defined over k. □

Corollary 12.3. *Let k be an algebraic number field, and let S be a finite set of primes in k. The map $C \mapsto (J_C, \lambda)$ sending a curve to its canonically polarized Jacobian variety defines an injection from the set of isomorphism classes of curves of genus ≥ 2 with good reduction outside S into the set of isomorphism classes of principally polarized abelian varieties over k with good reduction outside S.*

PROOF. Let R be the discrete valuation ring in k corresponding to a prime of k not in S. Then C extends to a smooth proper curve $\mathscr{C}$ over $\mathrm{spec}(R)$, and (see Section 8) the Jacobian $\mathscr{J}$ of $\mathscr{C}$ has generic fibre the Jacobian of C and special fibre the Jacobian of the reduction of C. Therefore J_C has good reduction at the prime in question. The corollary is now obvious. □

Corollary 12.4. *Suppose that for any number field k, any finite set S primes of k, and any integer g, there are only finitely many principally polarized abelian varieties of dimension g over k having good reduction outside S. Then Mordell's conjecture is true.*

PROOF. Combine the last corollary with (9.11). □

Remark 12.5. Corollary 12.2 is false as stated without the condition that the genus of C is greater than 1. It would say that all curves of genus zero over k are isomorphic to $\mathbb{P}^1$ (but in general there exist conics defined over k having no rational point in k), and it would say that all curves of genus 1 are isomorphic to their Jacobians (and, in particular, have a rational point). However, it is obviously true (without restriction on the genus) that two curves over k having k-rational points are isomorphic over k if their canonically polarized Jacobians are isomorphic over k.

§13. Torelli's Theorem: The Proof

Throughout this section, C will be a complete nonsingular curve of genus $g \geq 2$ over an algebraically closed field k, and P will be a closed point of C. The maps $f^P\colon C \to J$ and $f^{(r)}\colon C^{(r)} \to J$ corresponding to P will all be denoted by f. Therefore $f(D + D') = f(D) + f(D')$, and if $f(D) = f(D')$, then

$$D \sim D' + rP \quad \text{where} \quad r = \deg(D) - \deg(D').$$

As usual, the image of $C^{(r)}$ in J is denoted by W^r. A canonical divisor K on C

defines a point on $C^{(2g-2)}$ whose image in J will be denoted by κ. For any subvariety Z of J, Z^* will denote the image of Z under the map $x \mapsto \kappa - x$

Lemma 13.1. *For all a in $J(k)$, $(W_a^{g-1})^* = W_{-a}^{g-1}$.*

PROOF. For any effective divisor D of degree $g-1$ on C,

$$h^0(K - D) = h^1(K - D) = h^0(D) \geq 1,$$

and so there exists an effective divisor D' such that $K - D \sim D'$. Then $\kappa - f(D) - a = f(D') - a$, which shows that $(W_a^{g-1})^* \subset W_{-a}^{g-1}$. On replacing a by $-a$, we get that $(W_{-a}^{g-1})^* \subset W_a^{g-1}$, and so $W_{-a}^{g-1} = (W_{-a}^{g-1})^{**} \subset (W_{-a}^{g-1})^*$. □

Lemma 13.2. *For any r such that $0 \leq r \leq g-1$,*

$$W_a^r \subset W_b^{g-1} \Leftrightarrow a \in W_b^{g-1-r}.$$

PROOF. $\Leftarrow$: If $c = f(D) + a$ with D an effective divisor of degree r, and $a = f(D') + b$ with D' an effective divisor of degree $g-1-r$, then $c = f(D + D') + b$ with $D + D'$ an effective divisor of degree $g-1$.

$\Rightarrow$: As $a \in W_b^{g-1}$, there is an effective divisor A of degree $g-1$ such that $a = f(A) + b$. Let D be effective of degree r. The hypothesis states that $f(D) + a = f(\bar{D}) + b$ for some $\bar{D}$ effective of degree $g-1$, and so $f(D) + f(A) = f(\bar{D})$ and

$$D + A \sim \bar{D} + rP.$$

Choose effective divisors A' and $\bar{D}'$ of degree $g-1$ such that $A + A'$ and $\bar{D} + \bar{D}'$ are linearly equivalent to K (cf. the proof of (13.1)). Then

$$D + K - A' \sim K - \bar{D}' + rP, \quad \text{and so}$$

$$D + \bar{D}' \sim A' + rP.$$

As the D's form a family of dimension r, this shows that $h^0(A' + rP) \geq r + 1$. (In more detail, $|A' + rP|$ can be regarded as a closed subvariety of $C^{(r+g-1)}$, and we have shown that it projects onto the whole of $C^{(r)}$.) It follows from the Riemann–Roch theorem that $h^0(K - A' - rP) \geq 1$, and so there is an effective divisor $\bar{A}$ of degree $g - 1 + r$ such that

$$A' + \bar{A} + rP \sim K.$$

Therefore $\bar{A} + rP \sim K - A' \sim A$, and so $f(\bar{A}) = f(A')$ and $a = f(\bar{A}) + b \in W_b^{g-1-r}$. □

Lemma 13.3. *For any r such that $0 \leq r \leq g-1$,*

$$W^{g-1-r} = \bigcap \{W_{-a}^{g-1} \mid a \in W^r\} \quad \textit{and} \quad (W^{g-1-r})^* = \bigcap \{W_a^{g-1} \mid a \in W^r\}.$$

PROOF. Clearly, for a fixed a in $J(k)$,

$$W^{g-1-r} \subset W_{-a}^{g-1} \Leftrightarrow W_a^{g-1-r} \subset W^{g-1},$$

and (13.2) shows that both hold if $a \in W^r$. Therefore

$$W^{g-1-r} \subset \bigcap \{W^{g-1}_{-a} \mid a \in W^r\}.$$

Conversely, $c \in W^{g-1}_{-a} \Leftrightarrow a \in W^{g-1}_{-c}$, and so if $c \in W^{g-1}_{-a}$ for all $a \in W^r$, then $W^r \subset W^{g-1}_{-c}$ and $W^r_c \subset W^{g-1}$. According to (13.2), this implies that $c \in W^{g-1-r}$, which completes the proof of the first equality. The second follows from the first and the equation

$$\bigcap\{W^{g-1}_a \mid a\in W^r\} = \bigcap\{(W^{g-1}_{-a})^* \mid a \in W^r\} = \left(\bigcap\{W^{g-1}_{-a}\mid a\in W^r\}\right)^*. \quad \square$$

Lemma 13.4. *Let r be such that $0 \le r \le g-2$, and let a and b be points of $J(k)$ related by an equation $a + x = b + y$ with $x \in W^1$ and $y \in W^{g-1-r}$. If $W^{r+1}_a \not\subset W^{g-1}_b$, then $W^{r+1}_a \cap W^{g-1}_b = W^r_{a+x} \cup S$ with $S = W^{r+1}_a \cap (W^{g-2}_{y-a})^*$.*

PROOF. Write $x = f(X)$ and $y = f(Y)$ with X and Y effective divisors of degree 1 and $g-1-r$. If $Y \ge X$, then, because $f(X)+a = f(Y)+b$, we will have $a = f(Y-X)+b$ with $Y-X$ an effective divisor of degree $g-2-r$. Therefore $a \in W^{g-2-r}_b$, and so $W^{r+1}_a \subset W^{g-1}_b$ (by (13.2)). Consequently, we may assume that X is not a point of Y.

Let $c \in W^{r+1}_a \cap W^{g-1}_b$. Then $c = f(D)+a = f(D')+b$ for some effective divisors D and D' of degree $r+1$ and $g-1$. Note that

$$f(D)+y = f(D)+a+x-b = f(D')+x,$$

and so $D+Y \sim D'+X$.

If $D+Y = D'+X$, then $D \ge X$, and so $c = f(D)+a = f(D-X)+x+a$; in this case $c \in W^r_{a+x}$.

If $D+Y \ne D'+X$, then $h^0(D+Y)\ge 2$, and so for any point Q of $C(k)$, $h^0(D+Y-Q)\ge 1$, and there is an effective divisor $\bar{Q}$ of degree $g-1$ such that $D+Y \sim Q+\bar{Q}$. Then

$$c = f(D)+a = f(\bar{Q})+a-y+f(Q),$$

and so $c \in \bigcap\{W^{g-1}_{a-y+d} \mid d\in W^1\} = (W^{g-2})^*_{a-y}$ (by (13.3)). As $(W^{g-2})^*_{a-y} = (W^{g-2}_{y-a})^*$ and c is in W^{r+1}_a by assumption, this completes the proof that $W^{r+1}_a \cap W^{g-1}_b \subset W^r_{a+x}\cup S$.

The reverse inclusion follows from the obvious inclusions:

$$W^r_{a+x}\subset W^{r+1}_a;\quad W^r_{a+x} = W^r_{b+y}\subset W^{g-1}_b;\quad (W^{g-2}_{y-a})^* \subset (W^{g-1}_{y-a-x})^* = W^{g-1}_b. \quad\square$$

Lemma 13.5. *Let $a\in J(k)$ be such that $W^1 \not\subset W^{g-1}_a$; then there is a unique effective divisor $D(a)$ of degree g on C such that*

$$f(D(a)) = a+\kappa \qquad (13.5.1)$$

and $W^1\cdot W^{g-1}_a$, when regarded as a divisor on C, equals $D(a)$.

PROOF. We use the notations of Section 6; in particular, $\Theta = W^{g-1}$. For

$a=0$, (13.1) says that $(\Theta^-)_\kappa = \Theta$. Therefore, on applying (6.8), we find that $W^1\cdot W^{g-1}_a = f(C)\cdot(\Theta^-)_{a+\kappa} \stackrel{\text{df}}{=} f^{-1}((\Theta^-)_{a+\kappa}) = D$, where D is a divisor of degree g on C such that $f^{(g)}(D) = a+\kappa$. This is the required result. $\square$

We are now ready to prove (12.1a). We use β to identify J with J', and write V^r for the image of $C'^{(r)}$ in J. As W^{g-1} and V^{g-1} define the same polarization of J, they give the same element of $NS(J)$ (see [14, §12]), and therefore one is a translate of the other, say $W^{g-1} = V^{g-1}_c$, $c\in J(k)$. To prove (12.1a), we shall show that V^1 is a translate of W^1 or of $(W^1)^*$.

Let r be the smallest integer such that V^1 is contained in a translate of W^{r+1} or $(W^{r+1})^*$. The theorem will be proved if we can show that $r = 0$. (Clearly, $r < g-1$.) Assume on the contrary that $r > 0$. We may suppose (after possibly replacing β by $-\beta$) that $V^1\subset W^{r+1}_a$. Choose an x in W^1 and a y in W^{g-1-r}, and set $b = a+x-y$. Then, unless $W^{r+1}_a \subset W^{g-1}_b$, we have (with the notations of (13.4))

$$V^1\cap W^{g-1}_b = V^1\cap W^{r+1}_a\cap W^{g-1}_b = (V^1\cap W^r_{a+x})\cup(V^1\cap S).$$

Note that, for a fixed a, W^r_{a+x} depends only on x and S depends only on y.

Fix an x; we shall show that for almost all y, $V^1 \not\subset W^{g-1}_b$, which implies that $W^{r+1}_a \not\subset W^{g-1}_b$ for the same y. As y runs over W^{g-1-r}, $-b$ runs over $W^{g-1-r}_{-(a+x)}$. Now, if $V^1\subset W^{g-1}_b$ for all $-b$ in $W^{g-1-r}_{-(a+x)}$, then $V^1 \subset W^r_{a+x}$ (by (13.3)). This contradicts the definition of r, and so there exist b for which $V^1\not\subset W^{g-1}_b$. Note that $V^1 \subset W^{g-1}_b$ $(= V^{g-1}_{b+c}) \Leftrightarrow -b\in V^{g-2}_c$ (by (13.2)). Therefore $V^{g-2}_c \not\subset W^{g-1-r}_{-(a+x)}$, and so the intersection of these sets is a lower dimensional subset of $W^{g-1-r}_{-(a+x)}$ whose points are the $-b$ for which $V^1\subset W^{g-1}_b$.

We now return to the consideration of the intersection $V^1\cap W^{g-1}_b$, which equals $(V^1\cap W^r_{a+x})\cup(V^1\cap S)$ for almost all y. We first show that $V^1\cap W^r_{a+x}$ contains at most one point. If not, then as $-b$ runs over almost all points of $W^{g-1-r}_{-(a+x)}$ (for a fixed x), the element $D'(b) \stackrel{\text{df}}{=} f'^{-1}(V'\cdot W^{g-1}_b)$ (cf. (13.5)) will contain at least two fixed points (because $W^r_{a+x}\subset W^{g-1}_{a+x-y} = W^{g-1}_b$), and hence $f(D'(b))$ will lie in a translate of V^{g-2}. As $f'(D'(b)) = b+\kappa'$, we would then have $(W^{g-1-r})^*$ contained in a translate of V^{g-2}, say V^{g-2}_d, and so

$$\bigcap\{V^{g-1}_{c-u}\mid u\in V^{g-2}_d\}\subset\bigcap\{W^{g-1}_{-u}\mid u\in(W^{g-1-r})^*\}.$$

On applying (13.3) to each side, we then get an inclusion of V in a translate of $(W^r)^*$, contradicting the definition of r.

Keeping y fixed and varying x, we see from (13.5.1) that $V^1\cap W^r_{a+x}$ must contain at least one point, and hence it contains exactly one point; according to the preceding argument, the point occurs in $D'(b)$ with multiplicity one for almost all choices of y.

It is now easily seen that we can find x, x' in W^1 and y in W^{g-1-r} such that $(D'(b) =)\ D'(a+x-y) = Q+\bar{D}$ and $(D'(b') =)\ D'(a+x'-y) = Q'+\bar{D}$ where Q, Q' are in C' and $\bar{D}$ is an effective divisor of degree $g-1$ on C' not containing Q or Q'. By equation (13.5.1), $f(Q)-f(Q') = x-x'$, and hence W^1 has two distinct points in common with some translate of V^1. Now, if x,

x' are in W^1, then $W^{g-1}_{-x} \cap W^{g-1}_{-x'} = W^{g-2} \cup (W^{g-2}_{x+x'})^*$ (by 13.4)). According to (13.3), we now get an inclusion of some translate of V^{g-2} in W^{g-2} or $(W^{g-2})^*$. Finally (13.3) shows that

$$V^1 = \bigcap \{V_{-e} | e \in V^{g-2}\}$$

which is contained in a translate of W^1 or W^{1*} according as V^{g-2} is contained in a translate of W^{g-2} or $(W^{g-2})^*$. This completes the proof. □

Bibliographic Notes for Abelian Varieties and Jacobian Varieties

The theory of abelian varieties over ℂ has a long history. On the other hand, the "abstract" theory over arbitrary fields, can be said to have begun with Weil's famous announcement of the proof of the Riemann hypothesis for function fields [Sur les fonctions algébriques à corps de constantes fini, *Comp. Rendu.* **210** (1940), 592–594]. Parts of the projected proof (for example, the key "lemme important") can best be understood in terms of intersection theory on the Jacobian variety of the curve, and Weil was to spend the next six years developing the foundational material necessary for making his proof rigorous. Unable in 1941 to construct the Jacobian as a projective variety, Weil was led to introduce the notion of an abstract variety (that is, a variety that is not quasi-projective). He then had to develop the theory of such varieties, and he was forced to develop his intersection theory by local methods (rather than the projective methods used by van der Waerden [*Einführing in die algebraische Geometrie*, Springer-Verlag, 1939]). In 1944 Weil completed his book [*Foundations of Algebraic Geometry*, AMS Coll., XXIX, 1946], which laid the necessary foundations in algebraic geometry, and in 1946 he completed his two books [*Sur les Courbes algébriques et les Variétés qui s'en déduisent*, Hermann, 1948] and [20], which developed the basic theory of abelian varieties and Jacobian varieties and gave a detailed account of his proof of the Riemann hypothesis. In the last work, abelian varieties are defined much as we defined them and Jacobian varieties are constructed, but it was not shown that the Jacobian could be defined over the same field as the curve.

Chow ([Algebraic systems of positive cycles in an algebraic variety, *Amer. J. Math.*, **72** (1950), 247–283] and [3]) gave a construction of the Jacobian variety which realized it as a projective variety defined over the same ground field as the original curve. Matsusaka [On the algebraic construction of the Picard variety, *Japan J. Math.*, **21** (1951), 217–235 and **22** (1952), 51–62] gave the first algebraic construction of the Picard and Albanese varieties and demonstrated also that they were projective and had the same field of definition as the original varieties. Weil showed that his construction of a group variety starting from a birational group could also be carried out without making an extension of the ground field [On algebraic groups of

transformations, *Amer. J. Math.*, **77** (1955), 355–391], and in [The field of definition of a variety, *Amer. J. Math.*, **78** (1956), 509–524] he further developed his methods of descending the field of definition of a variety. Finally Barsotti [A note on abelian varieties, *Rend. Circ. Mat. di Palermo*, **2** (1953), 236–257], Matsusaka [Some theorems on abelian varieties, *Nat. Sci. Report Ochanomizu Univ.*, **4** (1953), 22–35], and Weil [On the projective embedding of abelian varieties, in *Algebraic geometry and topology, A symposium in Honor of S. Lefschetz*, Princeton, 1957, pp. 177–181] showed that all abelian varieties are projective. In a course at the University of Chicago, 1954–55, Weil made substantial improvements to the theory of abelian varieties (the seesaw principle and the theorem of the cube, for example), and these and the results mentioned above together with Chow's theory of the "k-image" and "k-trace" [Abelian varieties over function fields, *Trans. Amer. Math. Soc.*, **78** (1955), 253–275] were incorporated by Lang in his book [9]. The main lacuna at this time (1958–59) was a satisfactory theory of isogenies of degree p and their kernels in characteristic p; for example, it was not known that the canonical map from an abelian variety to the dual of its dual was an isomorphism (its degree might have been divisible by p). Cartier [Isogenies and duality of abelian varieties, *Ann of Math.*, **71** (1960), 315–351] and Nishi [The Frobenius theorem and the duality theorem on an abelian variety, *Mem. Coll. Sc. Kyoto (A)*, **32** (1959), 333–350] settled this particular point, but the full understanding of the p-structure of abelian varieties required the development of the theories of finite group schemes and Barsotti–Tate groups. The book of Mumford [16] represents a substantial contribution to the subject of abelian varieties: it uses modern methods to give an comprehensive account of abelian varieties including the p-theory in characteristic p, and avoids the crutch of using Jacobians to prove results about general abelian varieties. (It has been a significant loss to the mathematical community that Mumford did not go on to write a second volume on the topics suggested in the introduction: Jacobians; Abelian schemes: deformation theory and moduli; the ring of modular forms and the global structure of the moduli space; the Dieudonné theory of the "fine" characteristic p structure; arithmetic theory: abelian schemes over local, global fields. We still lack satisfactory accounts of some of these topics.)

Much of the present two articles has been based on these sources. We now give some other sources and references. "Abelian Varieties" will be abbreviated by AV and "Jacobian Varieties" by JV.

The proof that abelian varieties are projective in AV, Section 7 is Weil's 1957 proof. The term "isogeny" was invented by Weil: previously, "isomorphism" had frequently been used in the same situation. The fact that the kernel of m_A has m^{2g} elements when m is prime to the characteristic was one of the main results that Weil had to check in order to give substance to his proof of the Riemann hypothesis. Proposition 11.3 of AV is mentioned briefly by Weil in [*Variétés Abéliennes. Colloque d'Algèbre et Théorie des Nombres*, 1949, pp. 125–128], and is treated in detail by Barsotti [Structure theorems for group varieties, *Annali di Mat.*, **38** (1955), 77–119]. Theorem 14.1 is folklore: it was used by Tate in [Endomorphisms of abelian varieties over finite fields, *Invent. math.*, **2** (1966), 134–144], which was one of the starting points for the work that led to Faltings's recent proof of Mordell's conjecture. The étale cohomology of an abelian variety is known to everyone who knows étale cohomology, but I was surprised not to be able to find an adequate reference for its calculation: in Kleiman [Algebraic cycles and the Weil conjectures, in *Dix Exposés sur la Cohomologie des Schémas*, North-Holland, 1968, pp. 359–386] Jacobians are used, and it was unaccountably omitted from [13]. In his 1940 announcement, Weil gives a definition of the e_m-pairing (in our terminology, $\bar{e}_m$-pairing) for divisor classes of degree zero and order m on a curve which is analogous to the explicit description at the start of Section 16 of AV. The results of that section mainly go back to Weil's 1948 monograph [20], but they were reworked and extended to the p-part in Mumford's book. The observation (see (16.12) of AV) that $(A \times A^\vee)^4$ is always principally polarized is due to Zarhin [A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction, *Invent. math.*, **79** (1985), 309–321]. Theorem 18.1 of AV was proved by Narasimhan and Nori [Polarizations on an abelian variety, in *Geometry and Analysis*, Springer-Verlag (1981), pp. 125–128]. Proposition 20.1 of AV is due to Grothendieck (cf. Mumford [*Geometric Invariant Theory*, Springer-Verlag, 1965, 6.1]), and (20.5) of AV (defining the K/k-trace) is due to Chow (reference above). The Mordell–Weil theorem was proved by Mordell [On the rational solutions of the indeterminate equations of the third and fourth degrees, *Proc. Cambridge Phil. Soc.*, **21** (1922), 179–192] (the same paper in which he stated his famous conjecture) for an elliptic curve over the rational numbers and by Weil [L'arithmétique sur les courbes algébriques, *Acta Math.*, **52** (1928), 281–315] for the Jacobian variety of a curve over a number field. (Weil, of course, stated the result in terms of divisors on a curve.)

The first seven sections of JV were pieced together from two disparate sources, Lang's book [9] and Grothendieck's Bourbaki talks [4], with some help from Serre [17], Mumford [15], and the first section of Katz and Mazur [*Arithmetic Moduli of Elliptic Curves*, Princeton, 1985].

Rosenlicht [Generalized Jacobian varieties, *Ann. of Math.*, **59** (1954), 505–530, and A universal mapping property of generalized Jacobians, *ibid.* (1957), 80–88], was the first to construct the generalized Jacobian of a curve relative to a modulus. The proof that all abelian coverings of a curve can be obtained from isogenies of its generalized Jacobians (Theorem 9.7 of JV) is due to Lang [Sur les séries L d'une variété algébrique, *Bull. SMF*, **84** (1956), 555–563]. Results close to Theorem 8.1 of JV were obtained by Igusa [Fibre systems of Jacobian varieties I, II, III, *Amer. J. Math.*, **78** (1956), 171–199, 745–760, and **81** (1959), 453–476]. Theorem 9.11 is due to Parshin [Algebraic curves over function fields, I, *Math. USSR—Izvestija*, **2** (1968), 1145–1169]. Matsusaka [On a generating curve of an abelian variety, *Nat. Sc. Rep. Ochanomizu Univ.*, **3** (1952), 1–4] showed that every abelian variety over an algebraically closed

field is generated by a curve (cf. (10.1) of JV). Regarding (11.2) of JV, Hurwitz [*Math. Ann.*, **28** (1886)] was the first to show the relation between the number of fixed points of a correspondence on a Rieman surface C and the trace of a matrix describing its action on the homology of the surface (equivalently that of its Jacobian). This result of Hurwitz inspired both Lefschetz in his proof of his trace formula and Weil in his proof of the Riemann hypothesis for curves.

Proofs of Torelli's theorem can be found in Andreotti [On a theorem of Torelli, *Amer. J. Math.*, **80** (1958), 801–821], Matsusaka [On a theorem of Torelli, *Amer. J. Math.*, **80** (1958), 784–800], Weil [Zum Beweis des Torellischen Satzes, *Gott. Nachr.*, **2** (1957), 33–53], and Ciliberto [On a proof of Torelli's theorem, in *Algebraic Geometry—Open problems*, Lecture Notes in Math., 997, Springer-Verlag, 1983, pp. 113–223]. The proof in Section 13 of JV is taken from Martens [A new proof of Torelli's theorem, *Ann. Math.*, **78** (1963), 107–111]. Torelli's original paper is [Sulle varieta di Jacobi, *Rend. R. Acad. Sci. Torino*, **50** (1914–15), 439–455]. Torelli's theorem shows that the map from the moduli space of curves into that of principally polarized abelian varieties is injective on geometric points; a finer discussion of the map can be found in the paper by Oort and Steenbrink [The local Torelli problem for algebraic curves, in *Algebraic Geometry Angers 1979*, Sijthoff & Noordhoff, 1980, pp. 157–204].

Finally, we mention that Mumford [*Curves and Their Jacobians*, University of Mich] provides a useful survey of the topics in its title, and that the commentaries in Weil [*Collected Papers*, Springer-Verlag, 1979] give a fascinating insight into the origins of parts of the subject of arithmetic geometry.

REFERENCES

[1] Artin, M. Néron models, this volume, pp. 213–230.

[2] Bourbaki, N. *Algèbre Commutative*. Hermann: Paris, 1961, 1964, 1965.

[3] Chow, W.-L. The Jacobian variety of an algebraic curve. *Amer. J. Math.*, **76** (1954), 453–476.

[4] Grothendieck, A. Technique de descente et théorèmes d'existence en géométrie algébrique, I–VI. *Séminaire Bourbaki*, Exposés 190, 195, 212, 221, 232, 236, 1959–62.

[5] Grothendieck, A. *Revêtements Étales et Groupe Fondamental* (SGA1, 1960–61). Lecture Notes in Mathematics, 224, Springer-Verlag: Heidelberg, 1971.

[6] Grothendieck, A. Le groupe de Brauer, III, in *Dix Exposés sur la Cohomologie des Schémas*. North-Holland: Amsterdam, 1968, pp. 88–188.

[7] Grothendieck, A. and Dieudonné, J. *Eléments de Géométrie Algébrique*, I. Springer-Verlag: Heidelberg, 1971.

[8] Hartshorne, R. *Algebraic Geometry*. Springer-Verlag: Heidelberg, 1977.

[9] Lang, S. *Abelian Varieties*. Interscience: New York, 1959.

[10] Lang, S. *Fundamentals of Diophantine Geometry*. Springer-Verlag: Heidelberg, 1983.

[11] Lichtenbaum, S. Duality theorems for curves over p-adic fields. *Invent. Math.*, **7** (1969), 120–136.

[12] Mattuck, A and Mayer, A. The Riemann–Roch theorem for algebraic curves. *Ann. Sci. Norm. Pisa*, **17**, (1963), 223–237.

[13] Milne, J. *Etale Cohomology*. Princeton University Press: Princeton, NJ, 1980.
[14] Milne, J. Abelian varieties, this volume, pp. 103–150.
[15] Mumford, D. *Lectures on Curves on an Algebraic Surface*. Princeton University Press: Princeton, NJ, 1966.
[16] Mumford, D. *Abelian Varieties*. Oxford University Press: Oxford, 1970.
[17] Serre, J.-P. *Groupes Algébriques et Corps de Classes*. Hermann, Paris, 1959.
[18] Shafarevich, I. *Basic Algebraic Geometry*. Springer-Verlag: Heidelberg, 1974.
[19] Waterhouse, W. *Introduction to Affine Group Schemes*. Springer-Verlag: Heidelberg, 1979.
[20] Weil, A. *Variétes Abéliennes et Courbes Algébriques*. Hermann: Paris, 1948.