The Jacobian Variety

Now we will give another, perhaps more natural, proof that the group law on the elliptic curve makes it a group variety. Our earlier proof used geometric properties of the embedding in $\mathbb{P}^2$. Now instead, we will show that the group $\mathrm{Pic}^\circ X$ has a structure of algebraic variety which is so natural that it is automatically a group variety. This approach makes sense for a curve of any genus, and leads to the Jacobian variety of a curve. The idea is to find a universal parameter space of divisor classes of degree 0.

Let X be a curve over k. For any scheme T over k, we define $\mathrm{Pic}^\circ(X \times T)$ to be the subgroup of $\mathrm{Pic}(X \times T)$ consisting of invertible sheaves whose restriction to each fiber X_t for $t \in T$ has degree 0. Let $p : X \times T \to T$ be the second projection. For any invertible sheaf $\mathcal{N}$ on T, $p^*\mathcal{N} \in \mathrm{Pic}^\circ(X \times T)$, because it is in fact trivial on each fibre. We define $\mathrm{Pic}^\circ(X/T) = \mathrm{Pic}^\circ(X \times T)/p^*\mathrm{Pic}T$, and we regard its elements as "families of invertible sheaves of degree0 on X, parametrized by T." Justification for this is the fact that if T is integral and of finite type over k, and if $\mathcal{L}, \mathcal{M} \in \mathrm{Pic}(X \times T)$, then $\mathcal{L}_t \cong \mathcal{M}_t$ on X_t for all $t \in T$ if and only if $\mathcal{L} \otimes \mathcal{M}^{-1} \in p^*\mathrm{Pic}T$ (III, Ex. 12.4).

Definition: Let X be a curve of any genus over k. The *Jacobian variety* of X is a scheme J of finite type over k, together with an element $\mathcal{L} \in \mathrm{Pic}^\circ(X/J)$, having the following universal property: for any scheme T of finite type over k, and for any $\mathcal{M} \in \mathrm{Pic}^\circ(X/T)$, there is a unique morphism $f : T \to J$ such that $f^*\mathcal{L} \cong \mathcal{M}$ in $\mathrm{Pic}^\circ(X/T)$.

Remark 4.10.2. In the language of representable functors, this definition says that J represents the functor $T \to \mathrm{Pic}^\circ(X/T)$.

Remark 4.10.3. Since J is defined by a universal property, it is unique if it exists. We will prove below that if X is an elliptic curve, then J exists, and in fact we can take $J = X$. For curves of genus ≥ 2, the existence is much more difficult. See, for example, Chow [3] or Mumford [2] or Grothendieck [5].

Remark 4.10.4. Assuming J exists, its closed points are in one-to-one correspondence with elements of the group $\mathrm{Pic}^\circ X$. Indeed, it give a closed points of J is the same as giving a morphism $\mathrm{Spec}k \to J$ (so morphisms of schemes can only send closed points to closed points? According to Stacks Project 26.13 Points of schemes: " A continuous map preserves the relation of specialization/generalization."), which by the universal property is the same thing as giving an element of $\mathrm{Pic}^\circ(X/k) = \mathrm{Pic}^\circ X$.

Definition: A scheme X with a morphism to another scheme S is a *group scheme over* S if there is a section $e : S \to X$ (the identity) and a morphism $\rho : X \to X$ over S (the inverse) and a morphism $\mu : X \times X \to X$ over S (the group operation) such that

(1) the composition $\mu \circ (\mathrm{id} \times \rho) : X \to X$ is equal to the projection $X \to S$ followed by e, and

(2) the two morphisms $\mu \circ (\mu \times \mathrm{id})$ and $\mu \circ (\mathrm{id} \times \mu)$ from $X \times X \times X \to X$ are the same.

Remark 4.10.5. This notion of group scheme generalizes the earlier notion of group variety (I, Ex. 3.21). Indeed, if $S = \mathrm{Spec} k$ and X is a variety over k, taking e to be the point 0, the properties (1) and (2) can be checked on the closed points of X. Then (1) says that ρ gives the inverse of each point, and (2) says that the group law is associative.

Remark 4.10.6. The Jacobian variety J of a curve X is automatically a group scheme over k. Indeed, using the universal property of J, define $e : \mathrm{Spec} k \to J$ by taking the element $0 \in \mathrm{Pic}^{\circ}(X/k)$. Define $\rho : J \to J$ by taking $\mathcal{L}^{-1} \in \mathrm{Pic}^{\circ}(X/J)$. Define $\mu : J \times J \to J$ by taking $p_1^*\mathcal{L} \otimes p_2^*\mathcal{L} \in \mathrm{Pic}(X/J \times J)$. The properties (1) and (2) are verified immediately by the universal property of J.

Remark 4.10.7. We can determine the Zariski tangent space to J at 0 as follows. To give an element of the Zariski tangent space is equivalent to giving a morphism of $T = \mathrm{Spec} k[\varepsilon]/(\varepsilon^2)$ to J sending $\mathrm{Spec} k$ to 0 (II, Ex. 2.8). By the definition of J, this is equivalent to giving $\mathcal{M} \in \mathrm{Pic}^{\circ}(X/T)$ whose restriction to $\mathrm{Pic}^{\circ}(X/k)$ is 0. But according to (III, Ex. 4.6) there is an exact sequence $0 \to H^1(X, \mathcal{O}_X) \to \mathrm{Pic} X[\varepsilon] \to \mathrm{Pic} X \to 0$. So we see that the Zariski tangent space to J at 0 is just $H^1(X, \mathcal{O}_X)$.

Remark 4.10.8. J is proper over k. We apply the valuative criterion of properness (II, 4.7). It is enough to show (II, Ex. 4.11) that if R is any discrete valuation ring containing k, with quotient field K, then a morphism of $\mathrm{Spec} K$ to J extends uniquely to a morphism of $\mathrm{Spec} R$ to J. In other words, we must show that an invertible sheaf $\mathcal{M}$ on $X \times \mathrm{Spec} K$ extends uniquely to an invertible sheaf on $X \times \mathrm{Spec} R$. Since $X \times \mathrm{Spec} R$ is a regular scheme, this follows from (II, 6.5) (note that the closed fibre of $X \times \mathrm{Spec} R$ over $\mathrm{Spec} R$, as a divisor on $X \times \mathrm{Spec} R$, is linearly equivalent to 0).

Remark 4.10.9. If we fix a base point P_0, then for any $n \geq 1$ there is a morphism $\varphi_n : X^n \to J$ defined by "$\langle P_1, \ldots, P_n \rangle \to \mathcal{L}(P_1 + \cdots + P_n - nP_0)$" (which means cook up the appropriate sheaf on $X \times X^n$ to define φ_n). If g is the genus of X, then φ_n will be surjective for $n \geq g$, because by Riemann-Roch, every divisor class of degree $\geq g$ contains an effective divisor. The fibre of φ_n over a point of J consists of all n-tuples $\langle P_1, \ldots, P_n \rangle$ such that the divisors $P_1 + \cdots + P_n$ form a complete linear system.

If $n = g$, then for most choices of $P_1, \ldots, P_g$, we have $\ell(P_1 + \cdots + P_g) = 1$. Indeed, by Riemann-Roch,

$$\ell(P_1 + \cdots + P_g) = g + 1 - g + \ell(K - P_1 - \cdots - P_g).$$

But $\ell(K) = g$. Taking P_1 not a base point of K (are base points of K the same as Weierstrass points?), $\ell(K - P_1) = g - 1$. At each step, taking P_i not a base point of $K - P_1 - \cdots - P_{i-1}$, we get $\ell(K - P_1 - \cdots - P_g) = 0$. Therefore, most fibres of φ_g are finite sets of points. We conclude that J is irreducible and $\dim J = g$. On the other hand, by (4.10.7), the Zariski tangent space to J at 0 is $H^1(X, \mathcal{O}_X)$, which has dimension g, so J is nonsingular at 0. Since it is a group scheme, it is a homogeneous space, hence nonsingular everywhere, Hence J is a nonsingular variety.

Theorem 4.11. Let X be an elliptic curve, and fix a point $P_0 \in X$. Take $J = X$, and take $\mathcal{L}$ on $X \times J$ to be $\mathcal{L}(\Delta) \otimes p_1^*\mathcal{L}(-P_0)$. Then $J, \mathcal{L}$ is a Jacobian variety for X. Furthermore, the resulting structure of group variety on J (4.10.6) induces the same group structure on X, P_0, defined earlier.

Proof. The last statement follows from the definitions. So we have only to show that if T is any scheme of finite type over k, and if $\mathcal{M} \in \mathrm{Pic}^\circ(X/T)$, then there is a unique morphism $f : T \to J$ such that $f^*\mathcal{L} \cong \mathcal{M}$.

Let $p : X \times T \to T$ be the projection, and let $q : X \times T \to X$ be the other projection. Define $\mathcal{M}' = \mathcal{M} \otimes q^*\mathcal{L}(P_0)$. Then $\mathcal{M}'$ has degree 1 along the fibres. Hence, for any closed point $t \in T$, we can apply Riemann-Roch to $\mathcal{M}'_t$ on $X_t = X$, and we find

$$\dim H^0(X, \mathcal{M}'_t) = 1$$

$$\dim H^1(X, \mathcal{M}'_t) = 0.$$

Since p is a projective morphism, and $\mathcal{M}'$ is flat over T, we can apply the theorem of cohomology and base change (III, 12.11). Looking first at $R^1p_*(\mathcal{M}')$, since the cohomology along the fibres is 0, the map $\varphi^1(t)$ of (III, 12.11) is automatically surjective, hence an isomorphism, so we conclude that $R^1p_*(\mathcal{M}')$ is identically 0. In particular, it is locally free, so we deduce from part (b) of the theorem that $\varphi^0(t)$ is also surjective. Therefore, it is an isomorphism, and since $\varphi^{-1}(t)$ is always surjective, we see that $p_*(\mathcal{M}')$ is locally free of rank 1.

Now replacing $\mathcal{M}$ by $\mathcal{M} \otimes p^*p_*(\mathcal{M}')^{-1}$ in $\mathrm{Pic}^\circ(X/T)$, we may then assume that $p_*(\mathcal{M}') \cong \mathcal{O}_T$. The section $1 \in \Gamma(T, \mathcal{O}_T)$ gives a section $s \in \Gamma(X \times T, \mathcal{M}')$, which defines an effective Cartier divisor $Z \subseteq X \times T$. By construction, Z intersects each fibre of p in just one point, and in fact one sees easily that the restricted morphism $p : Z \to T$ is an isomorphism. Thus we get a section $s : T \to Z \subseteq X \times T$. Composing with q gives the required morphism $f : T \to X$.

Indeed, since Z is the graph of f, we see that $Z = f^*\Delta$, where $\Delta \subseteq X \times X$ is the diagonal. Hence the corresponding invertible sheaves correspond: $\mathcal{M}' \cong f^*\mathcal{L}(\Delta)$. Now twisting by $-P_0$ shows that $\mathcal{M} \cong f^*\mathcal{L}$, as required. The uniqueness of f is clear for the same reasons. $\square$

Elliptic Functions

It is hard to discuss elliptic curves without bringing in the theory of elliptic functions of a complex variable. This classical topic from complex analysis gives an insight into the theory of elliptic curves over $\mathbb{C}$ which cannot be matched by purely algebraic techniques. So we will recall some of the definitions and results of that without proof (signalling those statements with a **B** in their number), and give some applications to elliptic curves. We refer to the book Hurwitz-Courant [1] for proofs.

Fix a complex number $\tau \in \mathbb{C} \setminus \mathbb{R}$. Let Λ be the lattice in the complex plant $\mathbb{C}$ consisting of all $n + m\tau$ with $n, m \in \mathbb{Z}$.

Definition: An *elliptic function* (with respect to the lattice Λ) is a meromorphic function $f(z)$ of the complex variable z such that $f(z + \omega) = f(z)$ for all $\omega \in \Lambda$. (Sometimes these are called *doubly periodic functions*, since they are periodic with respect to the periods $1, \tau$.)

Because of the periodicity, an elliptic function is determined if one knows its values on a single *period parallelogram*, such as the one bounded by $0, 1, \tau, 1+\tau$.

An example of an elliptic function is the *Weierstrass $\mathscr{P}$-function* defined by

$$\mathscr{P}(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

where $\Lambda' = \Lambda \setminus \{0\}$. One shows (Hurwitz-Courant [1, II, 1, §6]) that this series converges at all $z \notin \Lambda$, thus giving a meromorphic function gaving a double pole at the points of Λ, and which is elliptic. Its derivative

$$\mathscr{P}'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3}$$

is another elliptic function.

If one adds, subtracts, multiplies, or divides two elliptic functions with periods Λ, one gets another such. Hence the elliptic functions for a given Λ form a field.

Theorem 4.12B. The field of elliptic functions for given Λ is generated over $\mathbb{C}$ by the Weierstrass $\mathscr{P}$-function and its derivative $\mathscr{P}'$. They satisfy the algebraic relation

$$(\mathscr{P}')^2 = 4\mathscr{P}^3 - g_2\mathscr{P} - g_3,$$

where

$$g_2 = 60 \sum_{\omega \in \Lambda'} \frac{1}{\omega^4} \text{ and } g_3 = 140 \sum_{\omega \in \Lambda'} \frac{1}{\omega^6}.$$

Proof. Hurwitz-Courant [1, II, 1, §8, 9]. □

Thus if we define a mapping $\varphi : \mathbb{C} \to \mathbb{P}^2_{\mathbb{C}}$ by sending $z \mapsto (\mathscr{P}(z), \mathscr{P}'(z))$ in affine coordinates, we obtain a holomorphic mapping whose image lies inside the curve X with equation

$$y^2 = 4x^3 - g_2x - g_3.$$

In fact, φ induces a bijective mapping of $\mathbb{C}/\Lambda$ to X (Hurwitz-Courant [1, II, 5, §1]), and X is nonsingular, hence an elliptic curve. Under this mapping the field of elliptic functions is identified with the function field of the curve X. Thus for any elliptic function, we can speak of its *divisor* $\sum n_i(a_i)$, with $a_i \in \mathbb{C}/\Lambda$.

Theorem 4.13B. Given distinct points $a_1, \dots, a_q \in \mathbb{C}/\Lambda$, and given integers $n_1, \dots, n_q$, a necessary and sufficient condition that there exist an elliptic function with divisor $\sum n_i(a_i)$ is that $\sum n_i = 0$ and $\sum n_i a_i = 0$ in the group $\mathbb{C}/\Lambda$.

Proof. Hurwitz-Courant [1, II, 1, §5, 14]. □

In particular, this says that $a_1 + a_2 \equiv b \mod \Lambda$ if and only if there is an elliptic function with zeros at a_1 and a_2, and poles at b and 0. Since this function is a rational function of the curve X, this says that $\varphi(a_1) + \varphi(a_2) \sim \varphi(b) = \varphi(0)$ as divisors on X. If we let $P_0 = \varphi(0)$, which is the points at infinity on the y-axis $(0,1,0)$, and give X the group structure with origin P_0, this says that $\varphi(a_1) + \varphi(a_2) = \varphi(b)$ in the group structure on X. In other words, φ gives a group isomorphism between $\mathbb{C}/\Lambda$ under addiction, and X with its group law.

Theorem 4.14B. Given $c_2, c_3 \in \mathbb{C}$, with $\Delta = c_2^3 - 27c_3^2 \neq 0$, there exists a $\tau \in \mathbb{C} \setminus \mathbb{R}$, and an $\alpha \in \mathbb{C}^\times$, such that the lattice $\Lambda = (1, \tau)$ gives $g_2 = \alpha^4 c_2$ and $g_3 = \alpha^6 c_3$ by the formulas above.

Proof. Hurwitz-Courant [1, II, 4, §4]. □

This shows that every elliptic curve over $\mathbb{C}$ arises this way. Indeed, if X is any elliptic curve, we can embed X in $\mathbb{P}^2$ to have an equation of the form $y^2 = x(x-1)(x-\lambda)$, with $\lambda \neq 0, 1$ (4.6). By a linear change of variable in x, one can bring this into the form $y^2 = 4x^3 - c_2 x - c_3$, with $c_2 = (\sqrt[3]{4}/3)(\lambda^2 - \lambda + 1)$ and $c_3 = (1/27)(\lambda + 1)(2\lambda^2 - 5\lambda + 2)$. Then $\Delta = \lambda^2(\lambda - 1)^2$, which is different from 0 since $\lambda \neq 0, 1$. Now the curve determined by the lattice Λ is equivalent to this one by a change of variables $y' = \alpha^3 y$, $x' = \alpha^2 x$.

Next we define $J(\tau) = g_2^3/\Delta$. Then the j-invariant of X which we defined earlier is just $j = 1728 \cdot J(\tau)$. Thus $J(\tau)$ classifies the curve X up to isomorphism.

Theorem 4.15B. Let τ, τ' be two complex numbers. Then $J(\tau) = J(\tau')$ if and only if there are integers $a, b, c, d \in \mathbb{Z}$ with $ad - bc = \pm 1$ and

$$\tau' = \frac{a\tau + b}{c\tau + d}.$$

Furthermore, given any τ', there is a unique τ with $J(\tau) = J(\tau')$ such that τ lies in the region G defined by

$$-\frac{1}{2} \leq \text{Re } \tau < \frac{1}{2}$$

and

$$|\tau| \geq 1 \text{ if Re } \tau \leq 0$$

$$|\tau| > 1 \text{ if Re } \tau > 0.$$

Proof. Hurwitz-Courant [1, II, 4, §3]. □

Now we will start drawing consequences from this theory.

Theorem 4.16. Let X be an elliptic curve over $\mathbb{C}$. Then as an abstract group, X is isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. In particular, for any n, the subgroup of points of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof. We have seen that X is isomorphic as a group to $\mathbb{C}/\Lambda$, which in turn is isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. The points of order n are represented by $(a/n) + (b/n)\tau$, with $a, b = 0, 1, \ldots, n-1$. The points whose coordinates are not rational combinations of $1, \tau$ are of infinite order. □

Corollary 4.17. The morphism multiplication by n, $n_X : X \to X$ is a finite morphism of degree n^2.

Proof. Since it is separable, and a group homomorphism, its degree is the order of the kernel, which is n^2. □

Next we will investigate the ring of endomorphisms $R = \text{End}(X, P_0)$ of the elliptic curve X determined by the elliptic functions with periods $1, \tau$.

Proposition 4.18. There is a one-to-one correspondence between endomorphisms $f \in R$ and complex numbers $\alpha \in \mathbb{C}$ such that $\alpha \cdot \Lambda \subseteq \Lambda$. This correspondence gives an injective ring homomorphism of R to $\mathbb{C}$.

Proof. Given $f \in R$, we have seen (4.9) that f is a group homomorphism of X to X. Hence under the identification of X with $\mathbb{C}/\Lambda$ it gives a group homomorphism $\overline{f}$ of $\mathbb{C}$ to $\mathbb{C}$ such that $\overline{f}(\Lambda) \subseteq \Lambda$. On the other hand, since f is a morphism, the induced map $\overline{f} : \mathbb{C} \to \mathbb{C}$ is holomorphic. Now expanding $\overline{f}$ as a power series in a neighborhood of the origin, and expressing the fact that $\overline{f}(z+w) = \overline{f}(z) + \overline{f}(w)$ for any z, w there, we see that $\overline{f}$ must be just multiplication by a complex number α.

Conversely, given $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subseteq \Lambda$, clearly multiplication by α induces a group homomorphism f of $\mathbb{C}/\Lambda$ to itself, hence of X to itself. But f is also holomorphic, so in fact it is a morphism of X to itself by GAGA (=Serre [4]): see (App. B, Ex. 6.6).

It is clear under this correspondence that the ring operations of R corrspond to addition and multiplication of the corresponding complex numbers α. $\square$

Remark 4.18.1. Note in particular that the morphism $n_X \in R$, which is multiplication by n in the group structure (4.8.1) corresponds to multiplication by n in $\mathbb{C}$. This gives another proof of (4.10) for elliptic curves over $\mathbb{C}$.

Definition: If X is an elliptic curve over $\mathbb{C}$, we say that it has *complex multiplication* if the ring of endomorphisms R is bigger than $\mathbb{Z}$. This terminology is explained by (4.18).

Theorem 4.19. If X has complex multiplication, then $\tau \in \mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{Z}_+$, and in that case, R is a subring ($\neq \mathbb{Z}$) of the ring of integers of the field $\mathbb{Q}(\sqrt{-d})$. Conversely, if $\tau = r + s\sqrt{-d}$ with $r, s \in \mathbb{Q}$, then Xhas complex multiplication, and in fact

$$R = \{a + b\tau : a, b \in \mathbb{Z}, \text{ and } 2br, b(r^2 + ds^2) \in \mathbb{Z}\}.$$

Proof. Given τ, we can determine R as the set of all $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subseteq \Lambda$. A necessary and sufficient condition for $\alpha\Lambda \subseteq \Lambda$ is that there exist integers a, b, c, e such that

$$\alpha = a + b\tau$$

$$\alpha\tau = c + e\tau$$

(aka $\alpha \in \Lambda$ and for any $\lambda \in \Lambda$, $\alpha\lambda \in \Lambda$). If $\alpha \in \mathbb{R}$, then $\alpha \in \mathbb{Z}$ so we see that $R \cap \mathbb{R} = \mathbb{Z}$. On the other hand, if X has complex multiplication, then there is an $\alpha \notin \mathbb{R}$, and in this case $b \neq 0$.

Eliminating α from these equations, we see that

$$b\tau^2 + (a - e)\tau - c = 0,$$

which shows that τ is in a quadratic extension of $\mathbb{Q}$. Since $\tau \notin \mathbb{R}$, it must be an imaginary quadratic extension, so $\tau \in \mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{Z}_+$.

Eliminating τ from the same equations, we find that

$$\alpha^2 - (a - e)\alpha + (ae - bc) = 0,$$

which shows that α is integral over $\mathbb{Z}$. Therefore R must be a subring of the ring of integers of the field $\mathbb{Q}\left(\sqrt{-d}\right)$.

Conversely, suppose $\tau = r + s\sqrt{-d}$, with $r, s \in \mathbb{Q}$. Then we can determine R as the set of all $\alpha = a + b\tau$ with $a, b \in \mathbb{Z}$, such that $\alpha\tau \in \Lambda$. Since $\alpha\tau = a\tau + b\tau^2$, we must have $b\tau^2 \in \Lambda$. Now

$$\tau^2 = r^2 - ds^2 + 2rs\sqrt{-d},$$

which can be written

$$\tau^2 = -(r^2 + ds^2) + 2r\tau.$$

So in order to have $b\tau^2 \in \Lambda$ we must have $2br \in \mathbb{Z}$ and $b(r^2 + ds^2) \in \mathbb{Z}$. These conditions are necessary and sufficient so we get the required expression for R. In particular, $R > \mathbb{Z}$, so X has complex multiplication. □

Corollary 4.20. There are only countably many values of $j \in \mathbb{C}$ for which the corresponding elliptic curve X has complex multiplication.

Proof. Indeed, there are only countably many elements of all quadratic extensions of $\mathbb{Q}$. □

Example 4.20.1. If $\tau = i$, then R is the ring of Gaussian integers $\mathbb{Z}[i]$. In this case the group of units $R^\times$ of R consists of $\pm 1, \pm i$, so $\mathbb{R}^\times \cong \mathbb{Z}/4\mathbb{Z}$. This means that the group of automorphisms of X has order 4, so by (4.7) we must have $j = 1728$. So we see in a roundabout way that $\tau = i$ gives $J(\tau) = 1$. Another way to see this is as follows. Since $\Lambda = \mathbb{Z} \oplus i\mathbb{Z}$, the lattice Λ is stable under multiplication by i. Therefore

$$g_3 = 140 \sum_{\omega \in \Lambda'} \omega^{-6} = 140 \sum_{\omega \in \Lambda'} i^{-6}\omega^{-6} = -g_3.$$

So $g_3 = 0$, which implies $J(\tau) = 1$. The equation of X can be written $y^2 = x^3 - Ax$.

Example 4.20.2. If $\tau = \zeta_3$, then $R = \mathbb{Z}[\zeta_3]$, which is the ring of integers of $\mathbb{Q}(\sqrt{-3})$. In this case $R^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$, which is isomorphic to $\mathbb{Z}/6$. So again from (4.7) we conclude that $j = 0$. One can also see this directly as in (4.20.1) by showing that $g_2 = 0$. The equation of X can be written $y^2 = x^3 - B$.

Example 4.20.3. If $\tau = 2i$, then $R = \mathbb{Z}[2i]$. In this case R is a proper subring of the ring of integers in the quadratic field $\mathbb{Q}(i)$, with conductor 2 (Ex. 4.21).

Example 4.20.4. Even though we have a good criterion for complex multiplication in terms of τ, the connection between τ and j is not easy to compute. Thus if we are given a curve by its equation in $\mathbb{P}^2$, or by its j-invariant, it is not easy to tell whether it has complex multiplication or not. See (Ex. 4.5) and (Ex. 4.12). There is an extensive classical literature relating complex multiplication to class field theory − see, e.g. Deuring [2] or Serre's article in Cassels and Frölich [1, Ch. XIII]. Here are some of the principal results: let X be an elliptic curve with complex multiplication, let $R = \operatorname{End}(X, P_0)$, let $K = \mathbb{Q}(\sqrt{-d})$ be the quotient field of R (4.19), and let j be the j-invariant. Then (1) j is an algebraic integer; (2) the field $K(j)$ is an abelian extension of K of degree $h_R = \#\mathrm{Pic}R$; (3) $j \in \mathbb{Z} \Leftrightarrow h_R = 1$, and there are exactly 13 such values of j.

The Hasse Invariant

If X is an elliptic curve over a field k of characteristic $p > 0$, we define an important invariant of X as follows. Let $F : X \to X$ be the Frobenius morphism (2.4.1). Then F induces a map

$$F^* : H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X)$$

on cohomology. This map is not linear, but it is *p-linear*, namely $F^*(\lambda a) = \lambda^p F^*(a)$ for all $\lambda \in k$, $a \in H^1(X, \mathcal{O}_X)$. Since X is elliptic, $H^1(X, \mathcal{O}_X)$ is a one-dimensional vector space. Thus, since k is perfect, the map F^* is either 0 or bijective.

Definition: If $F^* = 0$, we say that X has *Hasse invariant* 0 or that X is *supersingular*; otherwise we say that X has *Hasse invariant* 1.

For other interpretations of the Hasse invariant, see (Ex. 4.15), (Ex. 4.16).

Proposition 4.21. Let the elliptic curve X be embedded as a cubic curve in $\mathbb{P}^2$ with homogeneous equation $f(x, y, z) = 0$. Then the Hasse invariant of X is 0 if and only if the coefficient of $(xyz)^{p-1}$ in f^{p-1} is 0.

Corollary 4.22. Assume $p \neq 2$ and let X be given by the equation $y^2 = x(x-1)(x-\lambda)$ with $\lambda \neq 0, 1$. Then the Hasse invariant of X is 0 if and only if $h_p(\lambda) = 0$, where

$$h_p(\lambda) = \sum_{i=0}^{k} \binom{k}{i}^2 \lambda^i, \quad k = \frac{1}{2}(p-1).$$

Corollary 4.23. For a given p, there are only finitely many elliptic curves (up to isomorphism) over k having Hasse invariant 0. In fact, there are at most $[p/12] + 2$ of them.

Example 4.23.1. Let $p = 3$. Then $h_p(\lambda) = \lambda + 1$. The only solution is $\lambda = -1$, which corresponds to $j = 0 = 1728$.

Example 4.23.2. If $p = 5$, $h_p(\lambda) = \lambda^2 + 4\lambda + 1 \equiv \lambda^2 - \lambda + 1 \mod 5$. This has roots $-\zeta_3, -\zeta_3^2$ in a quadratic extension of $\mathbb{F}_p$. So $j = 0$.

Example 4.23.3. If $p = 7$, then

$$h_p(\lambda) = \lambda^3 + 9\lambda^2 + 9\lambda + 1.$$

This has roots $-1, 2, 4$ which correspond to $j = 1728$.

Remark 4.23.4. A very interesting problem arises if we "fix the curve and vary p." To make sense of this, let $X \subseteq \mathbb{P}^2_{\mathbb{Z}}$ be a cubic curve defined by an equation $f(x, y, z) = 0$ with integer coefficients, and assume that X is nonsingular as a curve over $\mathbb{C}$. Then for almost all primes p, the curve $X_{(p)} \subseteq \mathbb{P}^2_{\mathbb{F}_p}$ obtained by reducing the coefficients of $f \mod p$ will be nonsingular over $k_{(p)} = \overline{\mathbb{F}_p}$. So it makes sense to consider the set

$$\mathfrak{P} = \{p \text{ prime} : X_{(p)} \text{ is nonsingular over } k_{(p)}, \text{ and } X_{(p)} \text{ has Hasse invariant } 0\}.$$

What can we say about this set? The facts (which we will not prove) are that if X, as a curve over $\mathbb{C}$, has complex multiplication, then $\mathfrak{P}$ has density $\frac{1}{2}$. Here we define the *density* of a set of primes $\mathfrak{P}$ to be

$$\lim_{x\to\infty} \#\{p \in \mathfrak{P} : p \le x\}/\#\{p \text{ prime} : p \le x\}.$$

In fact, assuming $X_{(p)}$ is nonsingular, then $X_{(p)}$ has Hasse invariant 0 if and only if either p is ramified or p remains prime in the imaginary quadratic field containing the ring of complex multiplication of X (Deuring [1]). If X does not have complex multiplication, then $\mathfrak{P}$ has density 0, but Elkies has shown that $\mathfrak{P}$ is infinite (N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, Invent. Math. 89 (1987) 561-567). There is also ample numerical evidence for the conjecture of Land and Trotter [1], that more precisely

$$\#\{p \in \mathfrak{P} : p \le x\} \sim c\sqrt{x}/\log x$$

as $x \to \infty$, for some constant $c > 0$.

Example 4.23.5. Let X be the curve $y^2 = x^3 - x$. Then $j = 1728$, and as we have seen (4.20.1), X has complex multiplication by i. For any $p \neq 2$, $X_{(p)}$ is nonsingular, and we compute its Hasse invariant by the criterion of (4.21). With $k = \frac{1}{2}(p-1)$, we need the coefficient of x^k in $(x^2-1)^k$. If k is odd, the coefficient is 0. If k is even, say $k = 2m$, it is $(-1)^m\binom{k}{m}$ which is nonzero. We conclude that

$$\begin{cases} \text{if } p \equiv 1 \mod 4, \text{ then Hasse} = 1 \\ \text{if } p \equiv 3 \mod 4, \text{ then Hasse} = 0 \end{cases}.$$

Thus $\mathfrak{P} = \{p \text{ prime} : p \equiv 3 \mod 4\}$. According to Dirichlet's theorem on primes in arithmetic progressions (see, e.g., Serre [14, Ch VI, §4]), this is a set of primes of density $\frac{1}{2}$. In particular, there are infinitely many such primes. Note that $p \equiv 3 \mod 4$ if and only if p is prime in the ring of Gaussian integers $\mathbb{Z}[i]$.

Example 4.23.6. Let X be the curve $y^2 = x(x-1)(x+2)$, so $\lambda = -2$, and $j = 2^6 \cdot 3^{-2} \cdot 7^3$. Then $X_{(p)}$ is nonsingular for $p \neq 2, 3$, but one checks by the criterion of (4.22), using a calculator, that the only value of $p \le 73$ giving Hasse=0 is $p = 23$. So we can guess that $\mathfrak{P}$ has density 0. Indeed, j is not an integer, so by (4.20.4), X does not have complex multiplication. See Lang and Trotter [1] for more extensive computations.

Rational Points on an Elliptic Curve

Let X be an elliptic curve over an algebraically closed field k, let P_0 be a fixed point, and let X be embedded in $\mathbb{P}^2_k$ by the linear system $|3P_0|$. Suppose that X can be defined by an equation $f(x, y, z) = 0$ with coefficients in a smaller field $k_0 \subseteq k$, and that the point P_0 has coordinates in k_0. If this happens, then it is clear from the geometric nature of the group law on X, that the set $X(k_0)$ of points of X with coordinates in k_0 forms a subgroup of the group of all points in X. It is an interesting arithmetic problem to determine the nature of this subgroup.

In particular, if $k = \mathbb{C}$ and $k_0 = \mathbb{Q}$, then because x, y, z are homogeneous coordinates in $\mathbb{P}^2$, we may assume that the equation $f(x, y, z) = 0$ has integer coefficients, and we are looking for integer solutions x, y, z. So we have a cubic Diophantine equation in three variables.

A theorem of Mordell states that the group $X(\mathbb{Q})$ is a finitely generated abelian group. We will not prove this, but just give some examples. See Cassels [1] and Tate [3] for two excellent surveys of the subject.

Example 4.23.7. The Fermat curve $x^3 + y^3 = z^3$ is defined over $\mathbb{Q}$. Because Fermat's theorem is true for exponent 3, the only points of $X(\mathbb{Q})$ are $(-1, 1, 0)$, $(1, 0, 1)$, and $(0, 1, 1)$. These are three inflection points of X. Taking any one as base point, the group $X(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

Example 4.23.8. The curve $y^2 + y = x^3 - x$ is defined over $\mathbb{Q}$. Take $P_0 = (0, 1, 0)$ to be the 0 element in the group law, as usual. Then (according to Tate [3]), the group $X(\mathbb{Q})$ is infinite cyclic, generated by the point P with affine coordinates $(0, 0)$.

Exercise 4.1. Let X be an elliptic curve over k with $\operatorname{char} k \neq 2$, let $P \in X$ be a point, and let R be a graded ring $R = \bigoplus_{n \geq 0} H^0(X, \mathcal{O}_X(nP))$. Show that for suitable choice of t, x, y,

$$R \cong k[t, x, y]/(y^2 - x(x - t^2)(x - \lambda t^2)),$$

as a graded ring, where $k[t, x, y]$ is graded by setting $\deg t = 1$, $\deg x = 2$, and $\deg y = 3$.

Proof. Recall that $H^0(X, \mathcal{F}) = \Gamma(X, \mathcal{F}) = \mathcal{F}(X)$ and $\mathcal{O}(nP)(X) = \mathcal{L}(nP)(X)$. Recall the proof of Proposition 4.6: We embed X in $\mathbb{P}^2$ by the linear system $|3P_0|$, which gives a closed immersion (3.3.3). We choose our coordinates as follows. Think of the vector spaces $H^0(\mathcal{O}(nP_0))$ as contained in each other,

$$k = H^0(\mathcal{O}) \subseteq H^0(\mathcal{O}(P_0)) \subseteq H^0(\mathcal{O}(2P_0)) \subseteq \cdots.$$

By Riemann-Roch, we have

$$\dim H^0(\mathcal{O}(nP_0)) = n$$

for $n > 0$. Choose $x \in H^0(\mathcal{O}(2P_0))$ so that t, x form a basis of that space, and choose $y \in H^0(\mathcal{O}(3P_0))$ so that t, x, y form a basis for that space. Then the seven quantities

$$t^2, x, y, x^2, xy, x^3, y^2$$

are in $H^0(\mathcal{O}(6P_0))$, which has dimension 6, so there is a linear relation among them. $\square$