

We begin with letting F be algebraically closed with characteristic not 2 or 3. We saw for an elliptic curve E , $E(F) \longrightarrow \text{Jac } E$, where $P \mapsto P - \mathcal{O}$, is surjective (and the proof can be extended to show it is a homomorphism). We now show it is injective. So we need to show that if $P \neq \mathcal{O}$ then $P - \mathcal{O} \not\sim 0$; that is, there is no function h on E with $(h) = P - \mathcal{O}$. Note:

$$\begin{array}{c} F(E) = F(x, y) \quad (\text{degree 2 since } y = \sqrt{x^3 + ax + b}) \\ \Big|_2 \\ F(x) \end{array}$$

Thus $F(E) = \{r(x) + ys(x) : r(x), s(x) \in F(x)\}$ so we may write $h(x, y) = \frac{a(x) + yb(x)}{c(x)}$, with $\gcd(a, b, c) = 1$ (by getting a common denominator and cancelling common factors).

We claim that if h has no poles in the affine part of E then c is a constant. To see this, suppose $\deg(c) \geq 1$. Then $\exists \alpha \in F$ with $c(\alpha) = 0$. Let β satisfy $\beta^2 = f(\alpha)$ (where $f(x) = x^3 + ax + b$) so the points $(\alpha, \pm\beta) \in E$. If h has no pole at $(\alpha, \pm\beta)$, the numerator must vanish; so $a(\alpha) \pm b(\alpha)\beta = 0$. Since it must hold for both $(\alpha, +\beta)$ and $(\alpha, -\beta)$, we can add both equations to deduce $a(\alpha) = 0$, and so $b(\alpha)\beta = 0$.

If $\beta \neq 0$, then $b(\alpha) = 0$; implying that $(x - \alpha)$ is a common factor to a , b , and c , contradiction. If $\beta = 0$ then $f(\alpha) = 0$. So $y^2 = f(x) = (x - \alpha)g(x)$. We have $\text{ord}_{(\alpha,0)}(x - \alpha) = 2$ and $\text{ord}_{(\alpha,0)} y = 1$, so $a(x) = (x - \alpha)^r a_1(x)$ and $\text{ord}_{(\alpha,0)}(a(x)) = 2r \geq 2$ and similarly for b . In particular, their orders are even. If $\text{ord}_{(\alpha,0)}(h) \geq 0$ then $\text{ord}(a + by) \geq \text{ord}(c)$, so $\min\{\text{ord}(a), \text{ord}(b)\} \geq \text{ord}(c)$. But $\text{ord}(b) > 0$ implies $b(\alpha) = 0$, contradiction as above. So $\text{ord}(b(\alpha)y) = \text{ord}(b) + \text{ord}(y) = \text{ord}(y) = 1$. Thus we have $1 \geq 2$, contradiction.

Thus we have $h = a + yb$ for $a, b \in F[x]$. Now the $\text{ord}_{\mathcal{O}} a = -2 \deg a$ and $\text{ord}_{\mathcal{O}} by = -2 \deg b - 3$ (the latter follows since $y^2 = f(x)$ the $\text{ord}_{\mathcal{O}} x = -2$ and $\text{ord}_{\mathcal{O}} y = -3$). Now $-1 = \text{ord}_{\mathcal{O}} h = \min\{-2 \deg a, -2 \deg b - 3\}$ for $a, b \neq 0$. [If $a = 0$ or $b = 0$, we have a term not appearing in the minimum.] We get a contradiction, and this shows injectivity.

Example. Let $y^2 = f(x)$ with $\deg f(x) = 5$ and f has distinct roots. It is a fact that this gives a curve of genus 2. $f(x) - (ax^2 + bx + c)$ has 5 zeroes say $\alpha_1, \dots, \alpha_5$. Say $\beta_i = -(a\alpha_i^2 + b\alpha_i + c)$ and $P_i = (\alpha_i, \beta_i)$. Then $(h) = P_1 + P_2 + \dots + P_5 - 5P_{\infty}$, where $h(x, y) = y + (ax^2 + bx + c)$.

Now given P_1, P_2, P_3 , we can choose a, b, c so that $P_1 + P_2 + P_3 - 3P_\infty \sim 2P_\infty - (P_4 + P_5)$ is the relation given by h .

Using these kinds of relations, we can trade three points for two points and prove that every divisor D , $\deg D = 0$, is linear equivalent to a divisor of the form $P_1 + P_2 - 2P_\infty$.

Define $C^{(2)} = C \times C/S_2$ (i.e. mod out by switching coordinates); this is the set of unordered pairs. Hence we have a map $\Phi : C^{(2)} \longrightarrow \text{Jac}(C)$ given by $\{P_1, P_2\} \mapsto P_1 + P_2 - 2P_\infty$, which is surjective.

Unfortunately, it is not injective. The divisor of $(x - \alpha)$ is $(\alpha, \beta) + (\alpha, -\beta) - 2P_\infty$ (where $\beta^2 = f(\alpha)$). Hence all the pairs of the form $\{(\alpha, \beta), (\alpha, -\beta)\}$ gives \mathcal{O} under Φ . It turns out that this is the only source of non-injectivity. The other points in $C^{(2)}$ uniquely represent a point in $\text{Jac}(C)$. [In algebraic geometry terms, Φ is a birational map and $\text{Jac}(C)$ is the blow-down of $C^{(2)}$ along a curve.]

For curves of genus 2, the Jacobian is a surface. In general the Jacobian of a curve of genus g is an algebraic variety of dimension g . In fact, $\text{Jac}(C)$ is projective and, since it has a group law, it is an abelian variety. Moreover, $\text{Jac}(C)$ is birational to $C^{(g)} := C^g/S_g$, where $\{P_1, \dots, P_g\} \mapsto P_1 + \dots + P_g - gP_0$ for some fixed P_0 . The sources of non-injectivity are more complicated, but it is a collection of blow-downs.

Example. If $F = \mathbb{C}$ and C/\mathbb{C} you can choose $\omega_1, \dots, \omega_g$ linear independent holomorphic differential forms on C with $\text{Jac}(C) \longrightarrow \mathbb{C}^g/L$, where L is a lattice, given by $P_1 + \dots + P_g - gP_0 \mapsto \sum_{i=1}^g \left(\int_{P_0}^{P_i} \omega_1, \dots, \int_{P_0}^{P_i} \omega_g \right)$; the lattice is $\left\{ \left(\int_\gamma \omega_1, \dots, \int_\gamma \omega_g \right) : \gamma \in \pi_1(C(\mathbb{C})) \right\}$.

Back to a global field

Suppose K is a global field and C/K is a smooth curve of genus g . Write $F = \overline{K}$. We can view C as a curve over F and get $\text{Jac}(C)$ which is an abelian variety. It turns out that $\text{Jac}(C)$ is defined over K .

We have $\text{Jac}(C)(K)$ is a subgroup of $\text{Jac}(C)(F)$. Suppose $D = \sum n_i P_i$ is a divisor and K is perfect. Take $\sigma \in \text{Gal}(F/K)$ and $P_i \in C(F)$. Note σ acts on points by acting on coordinates and gives another point in C , since C is defined over K . Thus σ can act on D by $\sigma(D) = \sum n_i \sigma(P_i)$.

Definition. We say D is *defined over* K if $\sigma(D) \sim D$ for all $\sigma \in \text{Gal}(F/K)$

It can be shown that $\text{Jac}(C)(K)$ is exactly the set of equivalence classes of divisors of degree zero defined over K .

Example. For $g = 1$, $\text{Jac}(E) = E$ over F . It turns out $\text{Jac}(E)(K) = E(K)$, since $\sigma(P) - \mathcal{O} = \sigma(P - \mathcal{O}) \sim P - \mathcal{O}$ (that is using the fact that \mathcal{O} is rational) implies $\sigma P \sim P$. Which can be shown to imply $\sigma(P) = P$. If this happens for all $\sigma \in \text{Gal}(F/K)$, we have $P \in E(K)$.

If C is curve of genus 1 with no rational points, we get $\text{Jac}(C) = E$ is an elliptic curve E/K with E and C isomorphic over F .

Example. Consider $g = 2$. Let $y^2 = f(x)$, where $\deg f = 5$. Assume P_0 is a rational point at ∞ . Now $\text{Jac}(C) = \{[P_1 + P_2 - 2P_0] : P_1, P_2 \in C(F)\}$; note $\sigma(P_1) + \sigma(P_2) - 2P_0 = \sigma(P_1 + P_2 - 2P_0) \sim P_1 + P_2 - 2P_0$ “usually” implies $\sigma(P_1) + \sigma(P_2) = P_1 + P_2$. If $\sigma(P_i) = P_2$ for $i = 1, 2$ for all σ then $P_i \in C(K)$. Unfortunately this need not always happen. For example, we could have $\sigma(P_1) = P_2$ and $\sigma(P_2) = P_1$, which would occur if $P_1 \in C(L)$ where $[L : K] = 2$ and P_2 is the galois conjugate of P_1 ; we have

$$\text{Jac}(C)(K) = \{[P_1 + P_2 - 2P_0] : P_1, P_2 \in C(K)\} \cup \bigcup_{[L:K]=2} \{[P + \bar{P} - 2P_0] : P \in C(L)\}$$

where \bar{P} denotes the conjugate of P . We have a case of this example: If $y^2 = (x^2 + 1)(x^3 + 2)$ and $P = (i, 0) \in C(\mathbb{Q}(i))$; so $(i, 0) + (-i, 0) - 2P_0 \in \text{Jac}(C)(\mathbb{Q})$.