THE WEIL PAIRING ON ELLIPTIC CURVES

Background

Non-Singular Curves. Let k be a number field, that is, a finite extension of $\mathbb{Q}$; denote $\overline{\mathbb{Q}}$ as its (separable) algebraic closure. The absolute Galois group $G_k = \mathrm{Gal}(\overline{\mathbb{Q}}/k) = \varprojlim_K \mathrm{Gal}(F/k)$ is the projective limit of Galois groups associated with finite, normal (separable) extensions F/k. Let $I \subseteq k[x_1, x_2, \ldots, x_n]$ be an ideal, and define the sets

$$X(\overline{\mathbb{Q}}) = \left\{ P \in \mathbb{A}^n(\overline{\mathbb{Q}}) \;\middle|\; f(P) = 0 \text{ for all } f \in I \right\}$$

$$I(X) = \left\{ f \in \overline{\mathbb{Q}}[x_1, x_2, \ldots, x_n] \;\middle|\; f(P) = 0 \text{ for all } P \in X(\overline{\mathbb{Q}}) \right\} \supseteq I \otimes_k \overline{\mathbb{Q}}.$$

Since $G_F \subseteq G_k$ acts on $\overline{\mathbb{Q}}$, we define $X(F) = X(\overline{\mathbb{Q}})^{G_F} = X(\overline{\mathbb{Q}}) \cup \mathbb{A}^n(F)$, namely the F-rational points, as the points fixed by this action. We think of X as a functor which takes fields F to (algebraic) sets $X(F)$, and say that X is an *affine variety over* k if $I(X) \subseteq \overline{\mathbb{Q}}[x_1, x_2, \ldots, x_n]$ is a prime ideal.

> **Proposition 1.** Let X be an affine variety over k, and define the integral domain $\mathscr{O}(X) = \overline{\mathbb{Q}}[x_1, x_2, \ldots, x_n]/I(X)$. Then the map $X(\overline{\mathbb{Q}}) \to \mathrm{mSpec}\, \mathscr{O}(X)$ which sends $P = (a_1, a_2, \ldots, a_n)$ to $\mathfrak{m}_P = \langle x_1 - a_1,\, x_2 - a_2,\, \ldots,\, x_n - a_n \rangle$ is an isomorphism.

Proof. The map is well-defined $\mathcal{O}/\mathfrak{m}_P \simeq \overline{\mathbb{Q}}$ is a field. Conversely, let $\mathfrak{m}$ be a maximal ideal of $\mathcal{O}$. Fix a surjection $\mathcal{O} \twoheadrightarrow \mathcal{O}/\mathfrak{m} \simeq \overline{\mathbb{Q}}$, and denote $a_i \in \overline{\mathbb{Q}}$ as the image of $x_i \in \mathcal{O}$. It is easy to check that $\mathfrak{m} = \mathfrak{m}_P$ for $P = (a_1, a_2, \ldots, a_n)$. □

We define $\mathcal{O} = \mathscr{O}(X)$ as the *global sections of* X or the *coordinate ring of* X. Often, we abuse notation and write $X = \mathrm{Spec}\, \mathcal{O}$. If we denote $K = \overline{\mathbb{Q}}(X)$ as its quotient field, we define the *dimension of* X as the transcendence degree of K over $\overline{\mathbb{Q}}$. We say that X is a *curve* if $\dim(X) = 1$.

> **Theorem 2.** Let X be a curve over k, and write the ideal $I = \langle f_1, f_2, \ldots, f_m \rangle \subseteq K[x_1, x_2, \ldots, x_n]$ so that $\dim(X) = n - m = 1$. The following are equivalent:
>
> i. For each $P \in X(\overline{\mathbb{Q}})$, the $m \times n$ matrix
>
> $$\mathrm{Jac}_P(X) = \begin{bmatrix} \dfrac{\partial f_1}{\partial x_1}(P) & \dfrac{\partial f_1}{\partial x_2}(P) & \cdots & \dfrac{\partial f_1}{\partial x_n}(P) \\ \dfrac{\partial f_2}{\partial x_1}(P) & \dfrac{\partial f_2}{\partial x_2}(P) & \cdots & \dfrac{\partial f_2}{\partial x_n}(P) \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{\partial f_m}{\partial x_1}(P) & \dfrac{\partial f_m}{\partial x_2}(P) & \cdots & \dfrac{\partial f_m}{\partial x_n}(P) \end{bmatrix}$$

yields an exact sequence:

$$\{0\} \longrightarrow T_P(X) \longrightarrow \mathbb{A}^n(\overline{\mathbb{Q}}) \xrightarrow{\mathrm{Jac}_P(X)} \mathbb{A}^m(\overline{\mathbb{Q}}) \longrightarrow \{0\}.$$

That is, the Jacobian matrix $\mathrm{Jac}_P(X)$ has rank m while the tangent space has dimension $\dim_{\overline{\mathbb{Q}}}\big(T_P(X)\big) = \dim(X)$.

ii. The Zariski cotangent space has dimension $\dim_{\overline{\mathbb{Q}}}\big(\mathfrak{m}/\mathfrak{m}^2\big) = \dim(X)$ for each maximal ideal $\mathfrak{m} \in \mathrm{mSpec}\,\mathcal{O}$.

iii. For each $P \in X(\overline{\mathbb{Q}})$, denote $\mathcal{O}_P$ as the localization of $\mathcal{O}$ at $\mathfrak{m}_P$. Then $\mathfrak{m}_P\,\mathcal{O}_P$ is a principal ideal.

iv. For each $P \in X(\overline{\mathbb{Q}})$, $\mathcal{O}_P$ is a discrete valuation ring.

v. For each $P \in X(\overline{\mathbb{Q}})$, $\mathcal{O}_P$ is integrally closed.

vi. $\mathcal{O}$ is a Dedekind Domain.

This is essentially a a restatement of Proposition 9.2 on pages 94-95 in Atiyah-Macdonald. If any of these equivalent statements holds true, we say that X is a *non-singular curve*.

Proof. (i) $\iff$ (ii). We have a perfect (i.e., bilinear and nondegenerate) pairing

$$\big(\mathfrak{m}_P/\mathfrak{m}_P^2\big) \times T_P(X) \to \overline{\mathbb{Q}} \qquad \text{defined by} \qquad \big(f,\,(b_1, b_2, \ldots, b_n)\big) \mapsto \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P)\, b_i.$$

Hence $\dim_{\overline{\mathbb{Q}}}\big(\mathfrak{m}_P/\mathfrak{m}_P^2\big) = \dim_{\overline{\mathbb{Q}}}\big(T_P(X)\big) = n - m = \dim(X)$.

(ii) $\iff$ (iii). As $\mathfrak{m} = \mathfrak{m}_P$ is a maximal ideal, Nakayama's Lemma states that we can find $\varpi \in \mathfrak{m}_P$ where $\varpi \notin {\mathfrak{m}_P}^2$. Consider the injective map $\mathcal{O}/\mathfrak{m}_P \to \mathfrak{m}_P/\mathfrak{m}_P^2$ defined by $x \mapsto \varpi\, x$. Clearly this is surjective if and only if $\mathfrak{m}_P\,\mathcal{O}_P = \varpi\,\mathcal{O}_P$ is principal. Recall now that $\dim_{\overline{\mathbb{Q}}}\big(\mathcal{O}/\mathfrak{m}_P\big) = 1$.

(iii) $\implies$ (iv). Say that $\mathfrak{m}_P\,\mathcal{O}_P = \varpi\,\mathcal{O}_P$ as a principal ideal. In order to show that $\mathcal{O}_P$ is a discrete valuation ring, it suffices to show that any nonzero $x \in \mathcal{O}_P$ is in the form $x = \varpi^m\, y$ for some $m \in \mathbb{Z}$ and $y \in \mathcal{O}_P^{\times}$. Consider the radical of the ideal generated by x:

$$\sqrt{\langle x \rangle} = \left\{ y \in \mathcal{O}_P \,\middle|\, y^n \in x\,\mathcal{O}_P \text{ for some nonnegative integer } n \right\}.$$

As $\mathcal{O}_P$ has a unique nonzero prime ideal, we must have $\sqrt{\langle x \rangle} = \mathfrak{m}_P\,\mathcal{O}_P$. But then there is largest nonnegative integer m such that $t^{m-1} \notin x\,\mathcal{O}_P$ yet $\varpi^m \in x\,\mathcal{O}_P$. Hence $y = x/\varpi^m \in \mathcal{O}_P$ but $y \notin \mathfrak{m}_P$.

(iv) $\implies$ (v). Say that $\mathcal{O}_P$ is a discrete valuation ring. Say that $x \in K$ is a root of a polynomial equation $x^n + a_1\, x^{n-1} + \cdots + a_n = 0$ for some $a_i \in \mathcal{O}_P$. Assume by way of contradiction that $x \notin \mathcal{O}_P$. Then $v_P(x) < 0$, so that $v_P(1/x) > 0$, hence $y = 1/x$ is an element of $\mathcal{O}_P$. Upon dividing by x^{n-1} we have the relation $x = -\big(a_1 + a_2\, y + \cdots + a_n\, y^{n-1}\big) \in \mathcal{O}_P$. This contradiction shows that $\mathcal{O}_P$ is indeed integrally closed.

(v) $\implies$ (iii). Say that $\mathcal{O}_P$ is integrally closed. We must construct an element $\varpi \in \mathcal{O}_P$ such that $\mathfrak{m}_P\,\mathcal{O}_P = \varpi\,\mathcal{O}_P$. Fix a nonzero $x \in \mathfrak{m}_P$. By considering the radical $\sqrt{\langle x \rangle}$ and noting that $\mathfrak{m}_P\,\mathcal{O}_P$ is a finitely generated $\mathcal{O}_P$-module, we see that there exists some $m \in \mathbb{Z}$ such that $\mathfrak{m}_P^m\,\mathcal{O}_P \subseteq x\,\mathcal{O}_P$ yet $\mathfrak{m}_P^{m-1}\,\mathcal{O}_P \not\subseteq x\,\mathcal{O}_P$. Choose $y \in \mathfrak{m}_P^{m-1}$ such that $y \notin x\,\mathcal{O}_P$, and let $\varpi = x/y$ be an element in K. Consider the module $(1/\varpi)\,\mathfrak{m}_P\,\mathcal{O}_P \subseteq \mathcal{O}_P$; we will show equality. As $y \notin \mathcal{O}_P$, we have $1/\varpi \notin \mathcal{O}_P$, so that $1/\varpi$ is not integral over $\mathcal{O}_P$. Then $(1/\varpi)\,\mathfrak{m}_P\,\mathcal{O}_P$ cannot be a finitely generated $\mathcal{O}_P$-module,

we have $(1/\varpi)\,\mathfrak{m}_P\,\mathcal{O}_P \not\subseteq \mathfrak{m}_P$. As there is an element of $(1/varpi)\,\mathfrak{m}_P\,\mathcal{O}_P$ which is not in $\mathfrak{m}_P$, we must have equality: $(1/\varpi)\,\mathfrak{m}_P\,\mathcal{O}_P = \mathcal{O}_P$. Hence $\mathfrak{m}_P\,\mathcal{O}_P = \varpi\,\mathcal{O}_P$ as desired.

(v) $\iff$ (vi). A Dedekind domain is a Noetherian integral domain of dimension 1 that is integrally closed. But the localization $\mathcal{O}_P$ is integrally closed for each maximal ideal $\mathfrak{m}_P$ if and only if $\mathcal{O}$ is integrally closed. (Consult Theorem 5.13 on page 63 of Atiyah-Macdonald.) □

Examples.

- Choose $\{a_1,\, a_2,\, a_3,\, a_4,\, a_6\} \subseteq k$, and consider the polynomial
$$f(x,y) = \big(y^2 + a_1\,x\,y + a_3\,y\big) - \big(x^3 + a_2\,x^2 + a_4\,x + a_6\big).$$
Then $X : f(x,y) = 0$ is a curve over K. Define the K-rational numbers
$$b_2 = a_1^2 + 4\,a_2 \qquad\qquad c_4 = b_2^2 - 24\,b_4$$
$$b_4 = 2\,a_4 + a_1\,a_3 \qquad\qquad c_6 = -b_2^3 + 36\,b_2\,b_4 - 216\,b_6$$
$$b_6 = a_3^2 + 4\,a_6 \qquad\qquad \Delta = -b_2^2\,b_8 - 8\,b_4^3 - 27\,b_6^2 + 9\,b_2\,b_4\,b_6$$
$$b_8 = a_1^2\,a_6 + 4\,a_2\,a_6 - a_1\,a_3\,a_4 + a_2\,a_3^2 - a_4^2$$
Then X is non-singular if and only if $\Delta \neq 0$.

- Choose $\{a_0,\, a_1,\, a_2,\, a_3,\, a_4\} \subseteq k$, and consider the quartic polynomial
$$f(x) = a_4\,x^4 + a_3\,x^3 + a_2\,x^2 + a_1\,x + a_0.$$
Then $X : y^2 = f(x)$ is a curve over k. If X has a k-rational point $P_\infty = (x_0, y_0)$, then it is birationally equivalent over k to the cubic curve $v^2 = u^3 + A\,u + B$ in terms of
$$A = \frac{-a_2^2 + 3\,a_1\,a_3 - 12\,a_0\,a_4}{3}$$
$$B = \frac{2\,a_2^3 - 9\,a_1\,a_2\,a_3 + 27\,a_0\,a_3^2 + 27\,a_1^2\,a_4 - 72\,a_0\,a_2\,a_4}{27}.$$
Then X is nonsingular if and only if $16\,\mathrm{disc}(f) = -16\,\big(4\,A^3 + 27\,B^2\big) = \Delta \neq 0$.

The Riemann-Roch Theorem

Let X be a non-singular curve over $k = \mathbb{C}$. From now on, we will identity X with $X(k)$, and embed $X \hookrightarrow \mathbb{C}$. We'll explain how to choose such an embedding later.

Meromorphic Functions. Let $k = \mathbb{C}$ denote the complex numbers. Let $X \subseteq \mathbb{C}$ be a compact Riemann surface. We will denote $\mathcal{O}$ as the ring of holomorphic (i.e., analytic) functions on X, and K as the field of meromorphic functions on X. Let me explain.

Say that $f : U \to \mathbb{C}$ is a function defined on an open subset $U \subseteq X$. Using the embedding $X \hookrightarrow \mathbb{R} \times \mathbb{R}$ which sends $x + i\,y \mapsto (x,y)$, we say that f is *smooth* if $f(z) = u(x,y) + i\,v(x,y)$ in terms of smooth functions $u,\, v : U \to \mathbb{R}$, where $z = x + i\,y$. We may denote the set of all such by $\mathscr{C}^\infty(U)$. By considering the identities
$$\frac{\partial f}{\partial z} = \frac{1}{2}\left(\frac{\partial f}{\partial x} - i\,\frac{\partial f}{\partial y}\right) = \frac{1}{2}\left(\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y}\right) + i\,\frac{1}{2}\left(\frac{\partial v}{\partial x} - \frac{\partial u}{\partial y}\right)$$
$$\frac{\partial f}{\partial \bar{z}} = \frac{1}{2}\left(\frac{\partial f}{\partial x} + i\,\frac{\partial f}{\partial y}\right) = \frac{1}{2}\left(\frac{\partial u}{\partial x} - \frac{\partial v}{\partial y}\right) + i\,\frac{1}{2}\left(\frac{\partial v}{\partial x} + \frac{\partial u}{\partial y}\right)$$

we see that the *Cauchy-Riemann Equations* imply that $f(z)$ is *holomorphic* (or *antiholomorphic*, respectively) on U if and only if $\partial f/\partial \bar{z} = 0$ (or $\partial f/\partial z = 0$, respectively). Note that $f(z)$ is holomorphic if and only if $f(\bar{z})$ is antiholomorphic. Denote $\mathscr{O}(U)$ as the collection of such holomorphic functions on U. Since this is an integral domain, we may denote $\mathscr{K}(U)$ as its function field; this is the collection of *meromorphic* functions on U. The following diagram may be useful:

$$\{0\} \longrightarrow \mathscr{O}(U) \longrightarrow \mathscr{K}(U) \longrightarrow \mathscr{C}^\infty(U)$$

We will denote $\mathcal{O} = \mathscr{O}(X)$ and $K = \mathscr{K}(X)$.

Meromorphic Differentials. Continue to let $U \subseteq X$ be an open subset. Denote $\Omega^0\,\mathscr{C}^\infty(U)$, the collection of *differential 0-forms* on U, as the set of smooth functions f on U. Similarly, denote $\Omega^1\,C^\infty(U)$, the collection of *differential 1-forms* on U, as the set of sums

$$\omega = f\,dx + g\,dy = \frac{f - i\,g}{2}\,dz + \frac{f + i\,g}{2}\,d\bar{z}$$

where f and g are smooth functions on U. Hence we have a canonical decomposition $\Omega^1\,\mathscr{C}^\infty(U) = \Omega^{1,0}\,\mathscr{C}^\infty(U) \oplus \Omega^{0,1}\,\mathscr{C}^\infty(U)$ as the direct sum of 1-forms in the form $\omega = f\,dz$ (or $\omega = f\,d\bar{z}$, respectively) where f is a smooth function on U. In particular, $\omega \in \Omega^{1,0}\,\mathscr{C}^\infty(U)$ (or $\omega \in \Omega^{0,1}\,\mathscr{C}^\infty(U)$, respectively) if and only if $g = i\,f$ (or $g = -i\,f$), which happens if and only if $\omega(\bar{z}) = -i\,\omega(z)$. As complex conjugation acts on the set $\Omega^1\,\mathscr{C}^\infty(U)$ of differential 1-forms via $\omega(z) \mapsto \omega(\bar{z})$, we see that we may identify $\Omega^1\,\mathscr{C}^\infty(U)^- = \Omega^{1,0}\,\mathscr{C}^\infty(U)$ and $\Omega^1\,\mathscr{C}^\infty(U)^+ = \Omega^{0,1}\,\mathscr{C}^\infty(U)$ as the eigenspaces corresponding to the eigenvalues $\mp i$, respectively.

We have a differential map $d:\ \Omega^0\,\mathscr{C}^\infty(U) \to \Omega^1\,\mathscr{C}^\infty(U)$ defined by

$$f \qquad \mapsto \qquad df = \frac{\partial f}{\partial z}\,dz + \frac{\partial f}{\partial \bar{z}}\,d\bar{z}.$$

We say that a 1-form ω is a *holomorphic differential* (or *antiholomorphic differential*, respectively) if $\omega = f\,dz$ (or $\omega = f\,d\bar{z} \in$, respectively) for some holomorphic (or antiholomorphic, respectively) function f on U. Denote $\Omega(U)$ as the collection of holomorphic differentials on U. Similarly, we say that a 1-form ω is a *meromorphic differential* (or *antimeromorphic differential*, respectively) if $\omega = (f/g)\,dz$ (or $\omega = (f/g)\,d\bar{z} \in$, respectively) for some holomorphic (or antiholomorphic, respectively) functions f and g on U. Denote $\Omega\,\mathscr{K}(U)$ as the collection of meromorphic differentials on U. The following diagram may be useful:

$$\{0\} \longrightarrow \Omega(U) \longrightarrow \Omega\,\mathscr{K}(U) \longrightarrow \Omega^{1,0}\,\mathscr{C}^\infty(U)$$

Note that $\Omega(X)$ is the collection of holomorphic differentials on X.

Homology Groups. Let $H_1(X, \mathbb{Z})$ denote the free abelian group of closed loops γ in X. It is well-known that $H_1(X, \mathbb{Z}) \simeq \mathbb{Z}^{2g}$ for some nonnegative integer g; we call g the *genus* of X. Complex conjugation $\gamma \mapsto \overline{\gamma}$ acts on these closed loops, so we may consider eigenspaces corresponding to the eigenvalues ∓ 1 (either reversing or preserving direction) generated by this involution:

$$H_1(X, \mathbb{Z}) = H_1(X, \mathbb{Z})^- \oplus H_1(X, \mathbb{Z})^+ \qquad \text{where} \qquad H_1(X, \mathbb{Z})^\mp \simeq \mathbb{Z}^g.$$

Upon tensoring with $\mathbb{C}$, we have the homology group $H_1(X, \mathbb{C}) \simeq \mathbb{C}^{2g}$, with eigenspaces $H_1(X, \mathbb{C})^\mp \simeq \mathbb{C}^g$. We have a nondegenerate, bilinear pairing

$$H_1(X, \mathbb{C})^- \times \Omega(X) \to \mathbb{C}, \qquad \left(\sum_i n_i\,\gamma_i,\ \omega\right) \mapsto \sum_i n_i \oint_{\gamma_i} \omega.$$

Note here that ω must be a *holomorphic* differential on X, so that each loop $\gamma_i \in H_1(X, \mathbb{Z})^-$. This implies the following results:

Proposition 3. Let $\mathscr{O}(X)$ be the collection of such holomorphic functions on X, $\Omega(X)$ be the collection of holomorphic differentials on X, and $H_1(X,\mathbb{Z}) \simeq \mathbb{Z}^{2g}$ be the free abelian group of closed loops γ in X.

- $\Omega(X) \simeq \mathrm{Hom}_{\mathbb{C}}\big(H_1(X,\mathbb{C})^-,\, \mathbb{C}\big) \simeq \mathbb{C}^g$.
- As the map $\mathcal{O} \to \Omega(X)$ defined by $f \mapsto f\,dz$ is an isomorphism, we see that $\Omega(X)$ is an $\mathcal{O}$-module of rank 1, but a complex vector space of dimension g.

Examples.

- The unit sphere is given by

$$S^2(\mathbb{R}) = \left\{ (u,v,w) \in \mathbb{R}^3 \,\middle|\, u^2+v^2+w^2 = 1 \right\}.$$

Stereographic Projection is the map $\pi : \mathbb{C} \to S^2(\mathbb{R})$ defined by

$$\pi(z) = \left(\frac{2\,\mathrm{Re}(z)}{|z|^2+1},\ \frac{2\,\mathrm{Im}(z)}{|z|^2+1},\ \frac{|z|^2-1}{|z|^2+1} \right) \qquad \text{with inverse} \qquad \pi^{-1}(u,v,w) = \frac{u+i\,v}{1-w}.$$

Of course, the inverse sends the "north pole" $(u,v,w) = (0,0,1)$ to $z = \infty$, so we actually find a birational equivalence between $X = \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ and $S^2(\mathbb{R})$. We consider X a compact Riemann surface – although it cannot really be imbedded in the complex plane.

Consider the differential 1-form $\omega = dz$. This is clearly a holomorphic differential on $\mathbb{A}^1(\mathbb{C}) = \mathbb{C}$, but upon making the substitution

$$w = \frac{1}{z} \qquad \Longrightarrow \qquad \omega = dz = -\frac{dw}{w^2}$$

we see that ω is *not* holomophic on $X = \mathbb{P}^1(\mathbb{C})$. In fact, X has no nonzero holomorphic differentials – only meromorphic ones! – so its genus must be $g = 0$.

- Fix complex numbers $g_2,\ g_3$ such that $g_2^3 \neq 27\,g_3^2$. We define a meromorphic map $\wp : \mathbb{C} \to \mathbb{C}$ implicitly via the relation

$$z = \int_\infty^{\wp(z)} \frac{dx}{\sqrt{4\,x^3 - g_2\,x - g_3}} \qquad \Longrightarrow \qquad \wp'(z)^2 = 4\,\wp(z)^3 - g_2\,\wp(z) - g_3.$$

(This is the *Weierstrass pae-function.*) Hence the map $z \mapsto \big(\wp(z),\, \wp'(z)\big)$ induces a short exact sequence

$$\{0\} \longrightarrow \Lambda \longrightarrow \mathbb{C} \longrightarrow E(\mathbb{C}) \longrightarrow \{0\}$$

in terms of a lattice $\Lambda = \mathbb{Z}[\omega_1,\, \omega_2]$, generated by integrating around the poles of the cubic polynomial, and the complex points on the elliptic curve $E:\ y^2 = 4\,x^3 - g_2\,x - g_3$. We have the compact Riemann surface

$$X = \left\{ z = m\,\omega_1 + n\,\omega_2 \in \mathbb{C} \,\middle|\, 0 \le m \le 1 \text{ and } 0 \le n \le 1 \right\} \simeq \frac{\mathbb{C}}{\Lambda} \simeq E(\mathbb{C}).$$

The collection of meromorphic functions on $X \subseteq \mathbb{C}$ is $K = \mathbb{C}\big(\wp(z),\, \wp'(z)\big)$. Note that the differential

$$\omega = dz = \frac{d\wp}{\wp'} = \frac{dx}{y} = \frac{2\,dy}{12\,x^2 - g_2}$$

is not only meromorphic on $\mathbb{C}$, it is actually *holomorphic*. As this is the only such differential, we see that $\Omega(X) \simeq \mathbb{C}$ consists of constant multiples of $\omega = dx/y$. In particular, $g = 1$.

Divisors. Denote $\mathrm{Div}(X)$ as the collection of divisors; these are formal sums $\mathfrak{a} = \sum_P n_P (P)$ over the points $P \in X$, where all but finitely many of the integers n_P are zero. The degree of a divisor is the integer $\deg(\mathfrak{a}) = \sum_P n_P$. There is a partial ordering on $\mathrm{Div}(X)$: given another divisor $\mathfrak{b} = \sum_P m_P (P)$, we say $\mathfrak{a} \leq \mathfrak{b}$ when $n_P \leq m_P$ for all points P. The map $K^\times/k^\times \to \mathrm{Div}(X)$ which sends $f \mapsto \sum_P \mathrm{ord}_P(f)(P)$ is injective. In fact, we have the following short exact sequence:

$$\{1\} \longrightarrow K^\times/k^\times \longrightarrow \mathrm{Div}(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow \{0\}.$$

Similarly, any nonzero memomorphic differential $\omega = f\,dz$ for some meromorphic function $f \in \mathcal{O}$, so define $\mathrm{div}(\omega) = \mathrm{div}(f) = \sum_P \mathrm{ord}_P(f)(P)$. As $\Omega(X) \simeq \mathcal{O}$, we say $\mathfrak{c} = \mathrm{div}(\omega_0)$ is a *canonical divisor* for *any* nonzero meromorphic differential ω_0. We have the following commutative diagram, where the rows and columns are exact:

$$\begin{array}{ccccccccc}
 & & \{1\} & & \{0\} & & \{0\} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & K^\times/k^\times & \xrightarrow{\mathrm{div}} & \mathrm{Div}^0(X) & \longrightarrow & \mathrm{Jac}(X) & \longrightarrow & \{0\} \\
 & & \downarrow{=} & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & K^\times/k^\times & \xrightarrow{\mathrm{div}} & \mathrm{Div}(X) & \longrightarrow & \mathrm{Pic}(X) & \longrightarrow & \{0\} \\
 & & \downarrow & & \downarrow{\deg} & & \downarrow{\deg} & & \\
\{1\} & \longrightarrow & \{1\} & \xrightarrow{\mathrm{div}} & \mathrm{Div}(X)/\mathrm{Div}^0(X) & \xrightarrow{=} & NS(X) & \longrightarrow & \{0\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \{1\} & & \{0\} & & \{0\} & &
\end{array}$$

The quotient group $\mathrm{Jac}(X) = \mathrm{Div}^0(X)/\mathrm{Div}(k)$ of degree 0 divisors modulo principal divisors is the *Jacobian* of X; the quotient group $\mathrm{Pic}(X) = \mathrm{Div}(X)/\mathrm{Div}(k)$ of divisors modulo principal divisors is the *Picard group* or the *(divisor) class group* of X; and the quotient group $NS(X) = \mathrm{Pic}(X)/\mathrm{Jac}(X)$ is the *Néron-Severi group* of X.

Riemann-Roch Theorem. For any divisor $\mathfrak{a} = \sum_P n_P (P)$, we wish to consider the following two complex vector spaces:

$$\left.\begin{aligned} H^0(\mathfrak{a}) &= \left\{ f \in k^\times \,\middle|\, \mathrm{div}(f) \geq -\mathfrak{a} \right\} \cup \{0\} \\ H^1(\mathfrak{a}) &= \left\{ \omega \in \Omega\,\mathscr{K}(X) - \{0\} \,\middle|\, \mathrm{div}(\omega) \geq \mathfrak{a} \right\} \cup \{0\} \end{aligned}\right\} \quad \Longrightarrow \quad \begin{cases} l(\mathfrak{a}) = \dim_{\mathbb{C}} H^0(\mathfrak{a}) \\ \deg(\mathfrak{a}) = \displaystyle\sum_{P \in X} n_P \\ \delta(\mathfrak{a}) = \dim_{\mathbb{C}} H^1(\mathfrak{a}) \end{cases}$$

(Note the change in the signs for the ordering!) The main question here concerns the relationship between $H^0(\mathfrak{a})$, $H^1(\mathfrak{a})$, and $H_1(X, \mathbb{Z})$. We have the following results:

Proposition 4.

- Any divisor $\mathfrak{a}$ can be written as a difference $\mathfrak{a} = \mathfrak{b} - \mathfrak{p}$ for divisors such that $\mathfrak{b}$, $\mathfrak{p} \geq 0$. Since $\mathfrak{a} \leq \mathfrak{a} + \mathfrak{p} = \mathfrak{b}$, we have $H^0(\mathfrak{a}) \subseteq H^0(\mathfrak{b})$. One shows by induction

that

$$l(\mathfrak{a}) \le l(\mathfrak{b}) \le \deg(\mathfrak{b}) + 1.$$

In particular, $H^0(\mathfrak{a})$ is a finite dimensional complex vector space.

- For each canonical divisor $\mathfrak{c} = \operatorname{div}(\omega_0)$, the map $\omega \mapsto \omega/\omega_0$ shows that

$$H^1(\mathfrak{a}) \simeq H^0\big(\mathfrak{c} - \mathfrak{a}\big) \qquad \Longrightarrow \qquad \delta(\mathfrak{a}) = l(\mathfrak{c} - \mathfrak{a}).$$

In particular $H^1(\mathfrak{a})$ is also a finite dimensional complex vector space.

- Say $\mathfrak{a} = 0$ is the zero divisor. Then $H^0(0) = \mathbb{C}$ consists of the constant functions, while $H^1(0) = \Omega(X)$ consists of the holomorphic differentials. In particular,

$$H^0(\mathfrak{c}) \simeq H^1(0) \simeq \mathbb{C}^g.$$

In the 1850's, Bernhard Riemann proved the inequality $l(\mathfrak{a}) \ge \deg(\mathfrak{a}) + 1 - g$. In 1864, his student, Gustav Roch, showed more precisely:

Theorem 5 (Riemann-Roch).

$$l(\mathfrak{a}) - \deg(\mathfrak{a}) - l(\mathfrak{c} - \mathfrak{a}) = l(\mathfrak{a}) - \deg(\mathfrak{a}) - \delta(\mathfrak{a}) = 1 - g.$$

for any canonical divisor $\mathfrak{c}$.

Remarks.

- The paper appears in Crelle's Journal as "Über die Anzahl der willkürlichen Constanten in algebraischen Functionen". This is usually called the *Riemann-Roch Theorem.* Sadly, both Riemann and Roch died two years later in Italy of tuberculosis: Riemann aged 39, and Roch aged 26.

- In 1874, Max Noether and Alexander von Brill gave a refinement of Roch's result, and were the first to call it the "Riemann-Roch" Theorem. In 1929, F. K. Schmidt generalized the Roch's result to algebraic curves. Subsequent generalizations were given by Friedrich Hirzebruch, Jean-Pierre Serre, and Alexander Grothendieck.

Classification via the Genus

Let me give some applications. Now we can let $k = \overline{\mathbb{Q}}$ be an algebraically closed field, $\mathcal{O}$ be a Dedekind domain, and K be its quotient field. We will let $X = \operatorname{Spec} \mathcal{O}$ be our nonsingular curve. Recall that for any divisor $\mathfrak{a} = \sum_P n_P (P)$ we have the identity

$$\dim_k H^0(\mathfrak{a}) - \deg(\mathfrak{a}) - \dim_k H^0(\mathfrak{c} - \mathfrak{a}) = 1 - g$$

where $H^0(\mathfrak{a}) = \big\{ f \in K \,\big|\, \operatorname{div}(f) + \mathfrak{a} \ge 0 \big\}$. We see two facts right away regarding a canonical divisor $\mathfrak{c} = \operatorname{div}(\omega_0)$:

- $g = \dim_k H^0(\mathfrak{c})$, which we see by choosing $\mathfrak{a} = 0$.

- $\deg(\mathfrak{c}) = 2\,g - 2$, which we see by choosing $\mathfrak{a} = \mathfrak{c}$.

We will show that, in some cases, we can classify X depending on the genus g.

Genus 0. We show that $g = 0$ if and only if $X \simeq \mathbb{P}^1(k)$.

Proposition 6. If $X \simeq \mathbb{P}^1(k)$, then $\mathrm{Jac}(X) \simeq \{0\}$ whereas $\mathrm{Pic}(X) \simeq NS(X) \simeq \mathbb{Z}$.

Proof. Choose $\mathcal{O} = k[x]$ as the polynomial ring in one variable, so that its quotient field $K = k(x)$ consists of those rational functions in one variable. Each nonzero prime ideal $\mathfrak{m}_P \subseteq \mathcal{O}$ is in the form $\mathfrak{m}_P = \langle x - a \rangle$ for some $P = a \in k$, so we have a one-to-one correspondence $\mathrm{mSpec}\,\mathcal{O} \simeq k$. We define $\mathbb{A}^1(k) = \mathrm{Spec}\,\mathcal{O}$ as the *affine line* over k. In order to make this a *projective line*, we add in the point at infinity: $\mathbb{P}^1(k) = \mathbb{A}^1(k) \cup \{P_\infty\}$.

Fix a nonnegative integer d, and consider the divisor $\mathfrak{b} = d\,(P_\infty)$ of the point at infinity. We show that $H^0(\mathfrak{b}) = \big\{ f \in K \,\big|\, \mathrm{div}(f) + \mathfrak{b} \geq 0 \big\}$ consists of those polynomials of degree at most d. As the divisor of $x \in K$ is $(P_0) - (P_\infty)$ we see that $\mathrm{ord}_{P_\infty}(f) \geq -d$ for any polynomial $f = \sum_{i=0}^{d} a_i\, x^i$. Hence $f \in H^0(\mathfrak{b})$. Conversely, let $f \in H^0(\mathfrak{b})$. Write $f = g/h$ for some polynomials $g,\, h \in \mathcal{O}$. If h has degree greater than 0, then it contains a nontrivial zero in k, so that f has a pole at some point in k. Hence h must be a constant. If g has degree greater than d then $\mathrm{ord}_{P_\infty}(g) < -d$. Hence g has degree at most d. This shows in particular the equality $l(\mathfrak{b}) = \deg(\mathfrak{b}) + 1$.

We show that any divisor $\mathfrak{a} = \sum_P n_P\,(P)$ can be expressed as a sum $\mathfrak{a} = \mathfrak{b} + \mathrm{div}(f)$. Since *affine points* $P = (x - a)$ for some $a \in k$, we may choose $f(x) = \prod_{a \in k} (x - a)^{n_P}$, so that $\mathrm{div}(f) = \sum_P \mathrm{ord}_P(f)\,(P) = \sum_P n_P \big((P) - (P_\infty) \big) = \mathfrak{a} - d\,(P_\infty)$ for $d = \deg(\mathfrak{a})$. □

Proposition 7. $g = 0$ if and only if $X \simeq \mathbb{P}^1(k)$.

Proof. Let $\mathfrak{b} = 2\,g\,(P_\infty)$ be the divisor of degree $2\,g$ associated with the point at infinity. We have seen that $\dim_k H^0(\mathfrak{a}) = \deg(\mathfrak{b}) + 1$ in this case, so the Riemann-Roch Theorem states that $g = \dim_k H^0(\mathfrak{c} - \mathfrak{b})$. But $\deg(\mathfrak{c} - \mathfrak{b}) = -2$ so that $H^0(\mathfrak{c} - \mathfrak{b}) = \{0\}$, showing that $g = 0$.

Conversely assume that $g = 0$. We will construct a birational map $X \to \mathbb{P}^1(k)$. Let $\mathfrak{b} = (P_\infty)$ as the divisor of a point in X. Then $\deg(\mathfrak{c} - \mathfrak{b}) < 0$ so that $H^0(\mathfrak{c} - \mathfrak{b}) = \{0\}$. The Riemann-Roch Theorem states that $l(\mathfrak{b}) = 2$. Fix a nonconstant function $f \in H^0(\mathfrak{b})$. For each $a \in k$, we note that $\mathrm{ord}_P(f - a) \geq 0$ for $P \neq P_\infty$ and $\mathrm{ord}_{P_\infty}(f - a) \geq -1$, so $\mathrm{div}(f - a) = (P_a) - (P_\infty)$ for some point P_a in X. As $\mathcal{O}/P \simeq k$, define a map $f : X \to \mathbb{P}^1(k)$ which sends a prime ideal P to the projective point $f(P) = \big(f \mod P : 1 \big)$. Note that $f(P_a) = (a : 1)$ and $f(P_\infty) = (1 : 0)$. As this map is one-to-one and onto, we see that $X \simeq \mathbb{P}^1(k)$. □

Base Points. Given a divisor $\mathfrak{a} \in \mathrm{Div}(X)$, define a *complete linear system* as the set

$$\big|\mathfrak{a}\big| = \left\{ \mathfrak{b} \in \mathrm{Div}(X) \,\middle|\, \mathfrak{b} \geq 0 \text{ and } \mathfrak{a} = \mathfrak{b} + \mathrm{div}(f) \text{ for some } f \in k^\times \right\}.$$

Note that $\deg\big|\mathfrak{a}\big| = \deg(\mathfrak{b})$ is independent of the choice of $\mathfrak{b} \in \big|\mathfrak{a}\big|$. It is easy to see that this fits into the following exact sequence:

$$\begin{array}{ccccccccc}
\{1\} & \longrightarrow & k^\times & \longrightarrow & H^0(\mathfrak{a}) - \{0\} & \xrightarrow{\mathrm{div}} & \big|\mathfrak{a}\big| & \longrightarrow & \{0\} \\
 & & \big\downarrow = & & \big\downarrow \simeq & & \big\downarrow \simeq & & \\
\{1\} & \longrightarrow & k^\times & \longrightarrow & \mathbb{A}^n(k) - \{\mathbf{0}\} & \longrightarrow & \mathbb{P}^{n-1}(k) & \longrightarrow & \{\mathbf{0}\}
\end{array}$$

where $n = l(\mathfrak{a})$. This relates affine vector spaces with projective vector spaces.

In particular, the complete linear system $\big|\mathfrak{c}\big| \simeq \mathbb{P}^{g-1}(k)$ has $\deg\big|\mathfrak{c}\big| = 2\,(g - 1)$. We say that a point $P_\infty \in X$ is a *base point* if $\mathfrak{b} \geq (P_\infty)$ for all $\mathfrak{b} \in \big|\mathfrak{c}\big|$.

Proposition 8.
- $X \simeq \mathbb{P}^1(k)$ whenever X has a base point.
- If $g \geq 1$, then X is base point free.

Proof. Say that P_∞ is one such base point. If $f \in H^0(\mathfrak{c})$ is a nonzero function, then $\operatorname{div}(1/f) + \mathfrak{c} = \mathfrak{b} \geq (P_\infty)$ so that $\operatorname{div}(1/f) + \big(\mathfrak{c} - (P_\infty)\big) \geq 0$. Hence $H^0(\mathfrak{c}) \subseteq H^0\big(\mathfrak{c} - (P_\infty)\big)$, so the Riemann-Roch Theorem states that

$$\dim_k H^0\big((P_\infty)\big) = 1 - g + \deg\big((P_\infty)\big) + \dim_k H^0\big(\mathfrak{c} - (P_\infty)\big) \geq 2.$$

Let $f \in H^0\big((P_\infty)\big)$ be a nonconstant function. Following the same argument as above, $\operatorname{div}(f - a) = (P_a) - (P_\infty)$, so that the map $f : X \to \mathbb{P}^1(k)$ is the desired isomorphism. □

Genus 1. Assume that k has characteristic different from 2 or 3.

Proposition 9. *$g = 1$ if and only if $X \simeq E(k)$ for some $E : y^2 = x^3 + A\,x + B$ with $4\,A^3 + 27\,B^2 \neq 0$.*

Proof. Assume that $g = 1$. Fix a positive integer d, and consider the divisor $\mathfrak{b} = d\,(P_\infty)$. Then $\deg(\mathfrak{c} - \mathfrak{b}) = -d < 0$, so that $H^0(\mathfrak{c} - \mathfrak{b}) = \{0\}$. The Riemann-Roch Theorem states that

$$\dim_k H^0(\mathfrak{b}) = 1 - g + \deg(\mathfrak{b}) + \dim_k H^0(\mathfrak{c} - \mathfrak{b}) = d.$$

Let $\{1,\, u\}$ and $\{1,\, u,\, v\}$ be bases for $H^0\big(2\,(P_\infty)\big)$ and $H^0\big(3\,(P_\infty)\big)$, respectively. Since the set $\{1,\, u,\, v,\, u^2,\, u\,v,\, v^2,\, u^3\}$ of seven functions is contained in a vector space $H^0\big(6\,(P_\infty)\big)$ of dimension 6, we must have a linear combination in the form

$$a_1 + a_2\,u + a_3\,v + a_4\,u^2 + a_5\,u\,v + a_6\,v^2 + a_7\,u^3 = 0$$

for some $a_i \in k$. Note that $\{1,\, u,\, v,\, u^2,\, u\,v\}$ is a basis for $H^0\big(5\,(P_\infty)\big)$ so we must have $a_6,\, a_7 \neq 0$. Upon making the substitutions

$$\begin{aligned}
x &= 3\,\big(a_5^2 - 4a_4\,a_6 - 12\,a_6\,a_7\,u\big)\\
y &= 108\,a_6\,a_7\,\big(a_3 + a_5\,u + 2\,a_6\,v\big)\\
A &= 27\,\big(-a_5^4 + 8\,a_4\,a_5^2\,a_6 - 16\,a_4^2\,a_6^2 - 24\,a_3\,a_5\,a_6\,a_7 + 48\,a_2\,a_6^2\,a_7\big)\\
B &= 54\,\big(a_5^6 - 12\,a_4\,a_5^4\,a_6 + 48\,a_4^2\,a_5^2\,a_6^2 - 64\,a_4^3\,a_6^3 + 36\,a_3\,a_5^3\,a_6\,a_7\\
&\qquad - 144\,a_3\,a_4\,a_5\,a_6^2\,a_7 - 72\,a_2\,a_5^2\,a_6^2\,a_7 + 288\,a_2\,a_4\,a_6^3\,a_7 + 216\,a_3^2\,a_6^2\,a_7^2 - 864\,a_1\,a_6^3\,a_7^2\big)
\end{aligned}$$

we find the identity $y^2 = x^3 + A\,x + B$. Denote this curve by E.

We construct a birational map $X \to E(k)$. Choose $a,\, b \in k$ satisfying $b^2 = a^3 + A\,a + B$. Since $\{1,\, x\}$ and $\{1,\, x,\, y\}$ are bases for $H^0\big(2\,(P_\infty)\big)$ and $H^0\big(3\,(P_\infty)\big)$, respectively, we have $\operatorname{div}(x - a) = (P_{a,b}) + (P_{a,-b}) - 2\,(P_\infty)$ and $\operatorname{div}(y - b) = (P_{a,b}) + (P'_{a,b}) + (P''_{a,b}) - 3\,(P_\infty)$. As $\mathcal{O}/P \simeq k$, consider that map $f : X \to \mathbb{P}^2(k)$ which sends a prime ideal P to the projective point $f(P) = \big(x \mod P : y \mod P : 1\big)$. Note that $f(P_{a,b}) = (a : b : 1)$ and $f(P_\infty) = (0 : 1 : 0)$. As this map is one-to-one and onto, we see that $X \simeq E(k)$. □

Elliptic Curves. As before, assume that k has characteristic different from 2 or 3. Fix $A,\, B \in k$ such that $4\,A^3 + 27\,B^2 \neq 0$. Let $X \subseteq \mathbb{P}^2(k)$ denote the collection of k-rational points on $y^2 = x^3 + A\,x + B$. We say that X is an *elliptic curve*. We will show that X is an abelian group with respect to some operation $\oplus$.

Theorem 10. Assume that $g = 1$. Then $X \simeq \mathrm{Jac}(X)$. In particular, X is an abelian group.

Proof. This is the content of Proposition 3.4 in Chapter III.3.5 in Silverman's "The Arithmetic of Elliptic Curves": we will construct a birational map $\kappa : X \to \mathrm{Jac}(X)$. Fix a point $P_\infty \in X$ and send $\kappa : X \to \mathrm{Jac}(X)$ by $P \mapsto (P) - (P_\infty)$. To see why this map is surjective, choose $\mathfrak{a} \in \mathrm{Div}^0(X)$ and set $\mathfrak{b} = \mathfrak{a} + (P_\infty)$. Since $\deg(\mathfrak{c} - \mathfrak{b}) < 0$, the Riemann-Roch Theorem states that

$$\dim_k H^0(\mathfrak{b}) = 1 - g + \deg(\mathfrak{b}) + \dim_k H^0(\mathfrak{c} - \mathfrak{b}) = 1.$$

Let $f \in H^0(\mathfrak{b})$ be nonzero; as this space is 1-dimensional we must have $\mathrm{div}(f) = (P) - \mathfrak{b}$ for some unique point P. Hence $\mathfrak{a} = \big((P) - (P_\infty)\big) - \mathrm{div}(f)$ for some unique $P \in X$. □

We explain how the *group law* on elliptic curves can be derived from the Riemann Roch Theorem. Fix a point $P_\infty \in X$ and denote $O = (0 : 1 : 0)$. Given two points $P, Q \in X$ draw a line in $\mathbb{P}^2(k)$ going through them. Rather explicitly, if $P = (p_1 : p_2 : p_0)$ and $Q = (q_1 : q_2 : q_0)$, then the line is in the form $f(x_1, x_2, x_0) = 0$ in terms of the linear polynomial

$$f(x_1, x_2, x_0) = \begin{vmatrix} p_1 & p_2 & p_0 \\ q_1 & q_2 & q_0 \\ x_1 & x_2 & x_0 \end{vmatrix}.$$

It is easy to see that $\mathrm{div}(f) = (P) + (Q) + (P * Q) - 3\,(O)$ for some point $P * Q$. Now consider the line going through $P * Q$ and P_∞; this is in the form $g(x_1, x_2, x_0) = 0$ for some linear polynomial. Again, it is easy to see that $\mathrm{div}(g) = (P * Q) + (P \oplus Q) + (P_\infty) - 3\,(O)$ for some point $P \oplus Q$. Hence we find that

$$\big((P \oplus Q) - (P_\infty)\big) = \big((P) - (P_\infty)\big) + \big((Q) - (P_\infty)\big) - \mathrm{div}(f/g).$$

Hence the map $X \to \mathrm{Jac}(X)$ defined by $P \mapsto (P) - (P_\infty)$ yields an associative group law $\oplus$. Note that P_∞ is the identity, which we often choose as $P_\infty = O$.

Theorem 11. Let X be an elliptic curve, and let $D = \sum_{i=1}^m n_i\,(P_i)$ be a divisor on E. Then $D = \mathrm{div}(f)$ for some rational function $f : X \to \mathbb{P}^1$ if and only if both $\sum_{i=1}^m n_i = 0$ in $\mathbb{Z}$ and $\bigoplus_{i=1}^m [n_i]\,P_i = O$ in X.

The notation "$[n]P = P \oplus P \oplus \cdots \oplus P$" is the sum of P a repeated n times in X.

Proof. This is the content of Corollary 3.5 in Chapter III.3.5 in Silverman's "The Arithmetic of Elliptic Curves": We have seen that the map $\kappa : X \mapsto \mathrm{Jac}(X)$ which sends $P \mapsto (P) - (O)$ is an isomorphism. Assume that $D = \mathrm{div}(f)$. Then $\sum_i n_i = \deg D = \deg \mathrm{div}(f) = 0$, and $\bigoplus_i [n_i] P_i = \bigoplus_i [n_i]\big(P - O\big) = \kappa^{-1}(D) = \kappa^{-1}\,\mathrm{div}(f)$. □

Tate Pairing and Weil Pairing

Group Law. Now let k be any number field, and choose $\{a_1, a_2, a_3, a_4, a_6\} \subseteq k$. The set E : $f(x, y) = 0$ in terms of the polynomial

$$f(x, y) = \big(y^2 + a_1\,x\,y + a_3\,y\big) - \big(x^3 + a_2\,x^2 + a_4\,x + a_6\big)$$

is a curve over k. Define the k-rational numbers

$$b_2 = a_1^2 + 4\,a_2 \qquad\qquad c_4 = b_2^2 - 24\,b_4$$
$$b_4 = 2\,a_4 + a_1\,a_3 \qquad\qquad c_6 = -b_2^3 + 36\,b_2\,b_4 - 216\,b_6$$
$$b_6 = a_3^2 + 4\,a_6 \qquad\qquad \Delta = -b_2^2\,b_8 - 8\,b_4^3 - 27\,b_6^2 + 9\,b_2\,b_4\,b_6$$
$$b_8 = a_1^2\,a_6 + 4\,a_2\,a_6 - a_1\,a_3\,a_4 + a_2\,a_3^2 - a_4^2$$

Then E is non-singular if and only if $\Delta \neq 0$. In this case, E is an elliptic curve.

We review the group law $\oplus : E(k) \times E(k) \to E(k)$ defined above: Given two points $P = (p_1 : p_2 : p_0)$ and $Q = (q_1 : q_2 : q_0)$ in $E(k)$ draw a line $f(x_1, x_2, x_0) = 0$ in $\mathbb{P}^2(k)$ going through them in terms of the linear polynomial

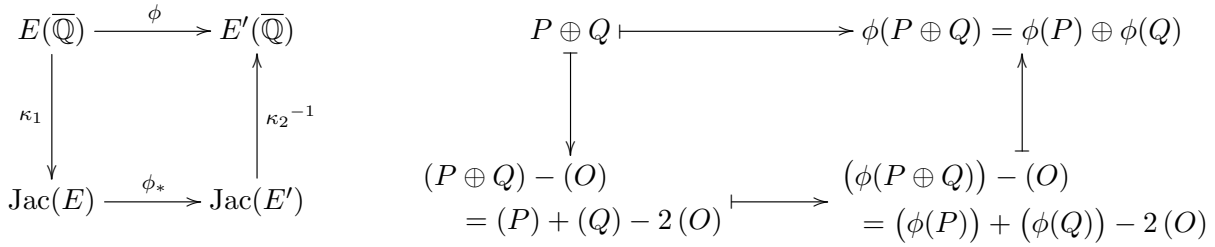
$$f(x_1, x_2, x_0) = \begin{vmatrix} p_1 & p_2 & p_0 \\ q_1 & q_2 & q_0 \\ x_1 & x_2 & x_0 \end{vmatrix} \qquad \Longrightarrow \qquad \operatorname{div}(f) = (P) + (Q) + (P * Q) - 3\,(O).$$

Now consider the line going through $P * Q$ and O; this is in the form $g(x_1, x_2, x_0) = 0$ for some linear polynomial, where $\operatorname{div}(g) = (P * Q) + (P \oplus Q) - 2\,(O)$ for some point $P \oplus Q \in E(k)$.

Isogenies. Let E and E' be two elliptic curves defined over k. An *isogeny* is a rational map $\phi : E(\overline{\mathbb{Q}}) \to E'(\overline{\mathbb{Q}})$ defined over k such that $\phi(O) = O$. Since $\phi : E \to E'$ induces a map $\phi^* : \overline{\mathbb{Q}}(E') \to \overline{\mathbb{Q}}(E)$ which sends $f \mapsto f \circ \phi$, we define the *degree* of ϕ as the degree of the extension $\overline{\mathbb{Q}}(E)/\phi^*\,\overline{\mathbb{Q}}(E')$.

> **Theorem 12.** Let $\phi : E \to E'$ be an nonconstant isogeny of degree m between elliptic curves over k.
>
> - ϕ is a group homomorphism, that is, $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$ as a sum in $E'(\overline{\mathbb{Q}})$ for any P, $Q \in E(\overline{\mathbb{Q}})$.
> - The map $\ker(\phi) \to \operatorname{Gal}\big(\overline{\mathbb{Q}}(E)/\phi^*\,\overline{\mathbb{Q}}(E')\big)$ which sends T to the function $\tau_T^*\,g : P \mapsto g(P \oplus T)$ is an isomorphism. In particular, $\big|\ker(\phi)\big| = m$.
> - There exists a unique dual isogeny $\widehat{\phi} : E' \to E$ such that the composition $\widehat{\phi} \circ \phi = [m] : E \to E' \to E$ sends $P \mapsto [m]\,P$ on E.

Proof. This first statement the content of Theorem 4.8 in Chapter III.4 of Silverman's "The Arithmetic of Elliptic Curves": It follows from a diagram chase.



For the second statement, we begin by showing the map is well-defined. Each $T \in \ker(\phi)$ maps to that automorphism τ_T^* which sends a function $g \in \overline{\mathbb{Q}}(E)$ to that function $\tau_T^*\,g : P \mapsto g(P \oplus T)$.

If $g \in \phi^* \overline{\mathbb{Q}}(E')$, then $g = f \circ \phi$ for some $f \in \overline{\mathbb{Q}}(E')$, so that $\tau_T^* g$ is that function which sends $P \in E(\overline{\mathbb{Q}})$ to $\big(\tau_T^* g\big)(P) = f\big(\phi(P) \oplus \phi(T)\big) = f\big(\phi(P) \oplus O\big) = g(P)$. Hence τ_T^* acts trivially on $\phi^* \overline{\mathbb{Q}}(E')$. Clearly the map $T \mapsto \tau_T^*$ is a well-defined injection. Conversely, $\deg(\phi) = \big|\phi^{-1}(Q)\big|$ for some $Q \in E'(\overline{\mathbb{Q}})$. Fix $P \in \phi^{-1}(Q)$. Then the map $\tau_P : \phi^{-1}(O) \to \phi^{-1}(Q)$ which sends $T \mapsto P \oplus T$ is a one-to-one correspondence, so that

$$\big|\mathrm{Gal}\big(\overline{\mathbb{Q}}(E)/\phi^* \overline{\mathbb{Q}}(E')\big)\big| = \deg(\phi) = \big|\phi^{-1}(Q)\big| = \big|\phi^{-1}(O)\big| = \big|\ker(\phi)\big|.$$

For the third statement, consider the extension $\overline{\mathbb{Q}}(E)/[m]^* \overline{\mathbb{Q}}(E)$ with Galois group $\ker[m]$. Since $[m]\, T = O$ for any $T \in \ker(\phi)$ by Lagrange's Theorem, we see that $\ker(\phi) \subseteq \ker[m]$. In particular, we have the following tower of fields:

$$[m]^* \overline{\mathbb{Q}}(E) \text{ ——— } \phi^* \overline{\mathbb{Q}}(E') \text{ ——— } \overline{\mathbb{Q}}(E)$$

This shows that the map $[m] : E \to E$ is in the form $[m] = \widehat{\phi} \circ \phi$ for some rational map $\widehat{\phi} : E' \to E$. Note that we have the following diagram:

$$\begin{array}{ccc} E'(\overline{\mathbb{Q}}) & \xrightarrow{\widehat{\phi}} & E(\overline{\mathbb{Q}}) \\ \downarrow{\scriptstyle \kappa_2} & & \uparrow{\scriptstyle \kappa_1{}^{-1}} \\ \mathrm{Jac}(E') & \xrightarrow{\phi^*} & \mathrm{Jac}(E) \end{array} \qquad \begin{array}{ccc} Q & \longmapsto & [m]\, P \\ \downarrow & & \uparrow \\ (Q) - (O) & \longmapsto & \sum_{T \in \ker(\phi)} \big((P \oplus T) - (T)\big) \end{array}$$

for any $P \in E(\overline{\mathbb{Q}})$ such that $\phi(P) = Q$. In particular, $\big(\widehat{\phi} \circ \phi\big)(P) = \widehat{\phi}(Q) = [m]\, P$ so that $\widehat{\phi}(O) = \widehat{\phi}\big(\phi(O)\big) = [m]\, O = O$. If $\widehat{\phi}'$ is any other dual isogeny, then $\big(\widehat{\phi}' - \widehat{\phi}\big) \circ \phi = [m] - [m] = [0]$ on E, so that $\widehat{\phi}' - \widehat{\phi} = [0]$ must be constant. This shows that $\widehat{\phi}$ is the unique rational map with $\widehat{\phi} \circ \phi = [m]$ and $\widehat{\phi}(O) = O$, so $\widehat{\phi}$ must be an isogeny. □

Examples.

- Consider an elliptic curve $E : \; y^2 + a_1\, x\, y + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6$ where $a_i \in k$. Given a point $P = (x : y : 1)$ in $E(k)$, we have $[m]\, P = O$ if and only of $\psi_m(P) = 0$ in terms of the division polynomials

$$\psi_m(P) = \begin{cases} 1 & \text{for } m = 1, \\ 2\, y + a_1\, x + a_3 = \sqrt{4\, x^3 + b_2\, x^2 + 2\, b_4\, x + b_6} & \text{for } m = 2, \\ 3\, x^4 + b_2\, x^3 + 3\, b_4 + 3\, b_6\, x + b_8 & \text{for } m = 3, \\ \psi_2(P) \big[2\, x^6 + b_2\, x^5 + 5\, b_4\, x^4 & \\ \qquad +10\, b_6\, x^3 + 10\, b_8\, x^2 + (b_2\, b_8 - b_4\, b_6)\, x + (b_4\, b_8 - b_6^2)\big] & \text{for } m = 4. \end{cases}$$

  Other division polynomials can be generated by the recursive relation

$$\psi_{m+n}(P)\, \psi_{m-n}(P)\, \psi_1(P)^2 = \psi_{m+1}(P)\, \psi_{m-1}(P)\, \psi_n(P)^2 - \psi_{n+1}(P)\, \psi_{n-1}(P)\, \psi_m(P)^2$$

for any integers m and n. In fact, the "multiplication-by-m" map $[m] : E(k) \to E(k)$ sends P to $[m]P = \big(\phi_m(P)/\psi_m(P)^2 \,:\, \omega_m(P)/\psi_m(P)^3 \,:\, 1\big)$ in terms of the polynomials

$$\phi_m(P) = \begin{cases} x & \text{for } m = 1, \\ x^4 - b_4\,x^2 - 2\,b_6\,x - b_8 & \text{for } m = 2, \\ \phi_1(P)\,\psi_m(P)^2 - \psi_{m+1}(P)\,\psi_{m-1}(P) & \text{for } m \ge 2. \end{cases}$$

$$\omega_m(P) = \begin{cases} y & \text{for } m = 1, \\ \dfrac{-a_1\,\phi_2(P)\,\psi_2(P)^2 - a_3\,\psi_2(P)^4 + \psi_4(P)}{2\,\psi_2(P)} & \text{for } m = 2, \\ -\dfrac{a_1\,\phi_m(P)\,\psi_m(P)^2 + a_3\,\psi_m(P)^3}{2} & \\ \qquad + \dfrac{\psi_{m-1}(P)^2\,\psi_{m+2}(P) + \psi_{m-2}(P)\,\psi_{m+1}(P)^2}{2\,\psi_2(P)} & \text{for } m \ge 2. \end{cases}$$

In particular, $\deg\big(\psi_m(P)^2\big) = m^2 - 1$, so that the "multiplication-by-m" map is an isogeny of degree m^2. In fact, $\ker[m] \simeq Z_m \times Z_m$ and $\widehat{[m]} = [m]$.

- Consider the elliptic curves

$$\begin{array}{lcl} E:\ y^2 = x^3 + a\,x^2 + b\,x & & A = -2\,a \\ & \text{where} & \\ E':\ Y^2 = X^3 + A\,X^2 + B\,X & & B = a^2 - 4\,b \end{array}$$

where a, b, A, $B \in k$ satisfy $b\,B \neq 0$. It is easy to check that $T = (0:0:1)$ is a k-rational point of order 2, that is, $[2]T = O$. Then we have a maps $\phi : E \to E'$ and $\widehat{\phi} : E' \to E$ which send

$$\begin{array}{rccl} \phi: & (x_1 : x_2 : x_0) & \mapsto & \big(x_2^2\,x_0 \ :\ x_2\,(b\,x_0^2 - x_1^2) \ :\ x_1^2\,x_0\big) \\ \widehat{\phi}: & (X_1 : X_2 : X_0) & \mapsto & \big(2\,X_2^2\,X_0 \ :\ X_2\,(B\,X_0^2 - X_1^2) \ :\ 8\,X_1^2\,X_0\big) \end{array}$$

It is easy to check that $\ker(\phi) = \big\{(0:0:1),\,(0:1:0)\big\} \simeq Z_2$ and that $\widehat{\phi} \circ \phi = [2]$ is the "multiplication-by-2" map. Hence both ϕ and $\widehat{\phi}$ are 2-isogenies.

- Let $A \subseteq E(\overline{\mathbb{Q}}) \hookrightarrow \mathbb{C}/\Lambda$ be any finite subgroup such that G_k acts trivially. Then we can find an isogeny $\phi : E \to E'$ such that $\ker(\phi) \simeq A$. One can construct E' explicitly using the cohomology group $H^1\big(G_k,\,A\big)$. Usually, one focuses on subgroups in the form $A \simeq Z_m \times Z_m$ or $A \simeq Z_n$, but we can certainly consider others such as $A \simeq Z_m \times Z_n$.

Weil Pairing. For any isogeny $\phi : E \to E'$ and its dual $\widehat{\phi} : E' \to E$, the kernels $E[\phi] = \ker(\phi)$ and $E'[\widehat{\phi}] = \ker(\widehat{\phi})$ are intimately related.

Theorem 13. Let $\phi : E \to E'$ be a nonconstant isogeny of degree m between elliptic curves over k. Denote $E[\phi] = \ker(\phi) \subseteq E(k)$ and $E'[\widehat{\phi}] = \ker(\widehat{\phi}) \subseteq E'(k)$ as the kernels of the isogeny and its dual. Then there exists a pairing

$$e_\phi : \ker(\phi) \times \ker(\widehat{\phi}) \to \boldsymbol{\mu}_m$$

satisfying the following properties:

- *Bilinearity:* For all $S \in \ker(\phi)$ and $T \in \ker(\widehat{\phi})$, we have
$$e_\phi(S_1 \oplus S_2,\, T) = e_\phi(S_1, T) \cdot e_\phi(S_2, T)$$
$$e_\phi(S,\, T_1 \oplus T_2) = e_\phi(S, T_1) \cdot e_\phi(S, T_2)$$

- *Non-Degenerate:* $e_\phi(S,T) = 1$ for all $S \in \ker(\phi)$, then $T = O$.

- *Galois Invariant:* $\sigma\big(e_\phi(S,T)\big) = e_\phi\big(\sigma(S), \sigma(T)\big)$ for all $\sigma \in G_k$.

- *Compatibility:* If $\psi : E' \to E''$ is another isogeny, then $e_{\psi\circ\phi}(P,Q) = e_\psi\big(\phi(P), Q\big)$ for all $P \in \ker(\psi \circ \phi)$ and $Q \in \ker(\widehat{\psi})$.

Proof. We follow Section III.8 on pages 92–99 and Exercise 3.15 on page 108 of Joseph Silverman's "The Arithmetic of Elliptic Curves". Let $T \in \ker(\widehat{\phi}) \subseteq E'[m]$. According to Theorem 11, there are functions $f_T \in \overline{\mathbb{Q}}(E')$ and $g_T \in \overline{\mathbb{Q}}(E)$ satisfying

$$\operatorname{div}(f_T) = m\,(T) - m\,(O)$$
$$\operatorname{div}(g_T) = \phi^*\big((T) - (O)\big) = \sum_{T' \in \ker(\phi)} \big((P \oplus T') - (T')\big) \qquad \text{where} \qquad P \in \phi^{-1}(T) \subseteq E[m].$$

Since $\operatorname{div}(g_T^m) = \operatorname{div}(f_T \circ \phi)$, we may assume without loss of generality that $f_T \circ \phi = g_T^m$. For any $S \in \ker(\phi)$, consider the map $E(\overline{\mathbb{Q}}) \to \mathbb{P}^1(\overline{\mathbb{Q}})$ which sends $X \mapsto g_T(X \oplus S)/g_T(X)$. Since $g_T(X \oplus S)^m = f_T\big(\phi(X) \oplus \phi(S)\big) = f_T\big(\phi(X)\big) = g_T(X)^m$, we see that this map takes on only finitely may values – and hence must be constant. We define the Weil pairing $e_\phi : \ker(\phi) \times \ker(\widehat{\phi}) \to \boldsymbol{\mu}_m$ as the mth root of unity $e_\phi(S,T) = g_T(X \oplus S)/g_T(X)$.

We show (Bilinearity). For the first factor we have

$$\begin{aligned} e_\phi(S_1 \oplus S_2,\, T) &= \frac{g_T(X \oplus S_1 \oplus S_2)}{g_T(X)} \\ &= \frac{g_T(X \oplus S_1 \oplus S_2)}{g_T(X \oplus S_2)} \cdot \frac{g_T(X \oplus S_2)}{g_T(X)} = \frac{g_T(X \oplus S_1)}{g_T(X)} \cdot \frac{g_T(X \oplus S_2)}{g_T(X)} \\ &= e_\phi(S_1, T) \cdot e_\phi(S_2, T). \end{aligned}$$

For the second factor, fix $T_1,\, T_2 \in \ker(\widehat{\phi})$. Using Theorem 11 again, we can find functions $f_1, f_2, f_3 \in \overline{\mathbb{Q}}(E')$ and $g_1, g_2, g_3 \in \overline{\mathbb{Q}}(E)$ satisfying

$$\begin{array}{lll} \operatorname{div}(f_1) = m\,(T_1) - m\,(O) & \operatorname{div}(g_1) = \phi^*\big((T_1) - (O)\big) & f_1 \circ \phi = g_1^m \\ \operatorname{div}(f_2) = m\,(T_2) - m\,(O) & \operatorname{div}(g_2) = \phi^*\big((T_2) - (O)\big) \quad \Longrightarrow & f_2 \circ \phi = g_2^m \\ \operatorname{div}(f_3) = m\,(T_1 \oplus T_2) - m\,(O) & \operatorname{div}(g_3) = \phi^*\big((T_1 \oplus T_2) - (O)\big) & f_3 \circ \phi = g_3^m \end{array}$$

Similarly, we can find a function $h \in \overline{\mathbb{Q}}(E')$ such that $\operatorname{div}(h) = (T_1 \oplus T_2) - (T_1) - (T_2) + (O)$, and so

$$\operatorname{div}\left(\frac{f_3}{f_1\, f_2}\right) = m \operatorname{div}(h) \qquad \Longrightarrow \qquad \frac{f_3}{f_1\, f_2} = h^m \qquad \Longrightarrow \qquad \left(\frac{g_3}{g_1\, g_2}\right)^m = \big(h \circ \phi\big)^m.$$

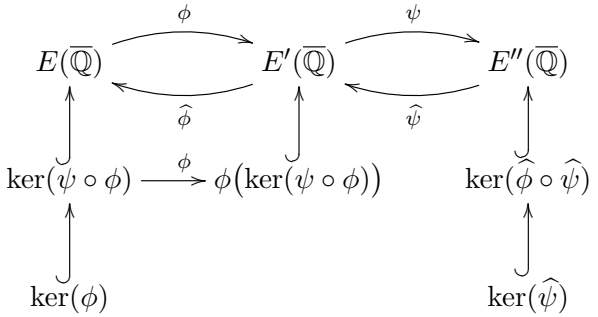
Hence $g_3 = c \cdot g_1\, g_2\, \big(h \circ \phi\big)$ for some constant $c \in \overline{\mathbb{Q}}$. This gives

$$\begin{aligned} e_\phi(S,\, T_1 \oplus T_2) &= \frac{g_3(X \oplus S)}{g_3(X)} = \frac{g_1(X \oplus S)}{g_1(X)} \cdot \frac{g_2(X \oplus S)}{g_2(X)} \cdot \frac{h\big(\phi(X) \oplus \phi(S)\big)}{h\big(\phi(X)\big)} \\ &= \frac{g_1(X \oplus S)}{g_1(X)} \cdot \frac{g_2(X \oplus S)}{g_2(X)} \cdot \frac{h\big(\phi(X) \oplus O\big)}{h\big(\phi(X)\big)} \\ &= e_\phi(S, T_1) \cdot e_\phi(S, T_2). \end{aligned}$$

We show (Non-Degeneracy). Say that $e_\phi(S,T) = 1$ for all $S \in \ker(\phi)$. Then $g_T(X \oplus S) = g_T(X)$ for all $X \in E(\overline{\mathbb{Q}})$. Following the ideas in Theorem 12, we see that $g_T \in \phi^*\, \overline{\mathbb{Q}}(E')$, so that $g_T = h_T \circ \phi$ for some $h_T \in \overline{\mathbb{Q}}(E')$. Since $\big(h_T \circ \phi\big)^m = g_T^m = f_T \circ \phi$, we find that $f_T = h_T^m$, and so $\operatorname{div}(h_T) = (T) - (O)$. According to Theorem 10, we must have $T = O$.

(Galois Invariance) is clear.

We show (Compability) using the following diagram:



Say that $\psi : E' \to E''$ is an isogeny of degree n. For each $Q \in \ker(\widehat{\psi}) \subseteq \ker(\widehat{\psi \circ \phi})$, there are functions d_Q, $f_Q \in \overline{\mathbb{Q}}(E'')$, $g_Q \in \overline{\mathbb{Q}}(E')$, and $h_Q \in \overline{\mathbb{Q}}(E)$ satisfying

$$\begin{aligned} &\operatorname{div}(d_Q) = n\,(Q) - n\,(O) && && d_Q \circ \psi = g_Q^n \\ &\operatorname{div}(f_Q) = m\,n\,(Q) - m\,n\,(O) && && f_Q \circ \psi \circ \phi = h_Q^{mn} \\ &\operatorname{div}(g_Q) = \psi^*\big((Q) - (O)\big) && \Longrightarrow && f_Q = d_Q^m \\ &\operatorname{div}(h_Q) = (\psi \circ \phi)^*\big((Q) - (O)\big) && && g_Q \circ \phi = h_Q \end{aligned}$$

We define the pairings $e_\psi : \ker(\psi) \times \ker(\widehat{\psi}) \to \boldsymbol{\mu}_{mn}$ and $e_{\psi\circ\phi} : \ker(\psi \circ \phi) \times \ker(\widehat{\psi}) \to \boldsymbol{\mu}_{mn}$ via $e_\psi(S,Q) = g_Q(X \oplus S)/g_Q(X)$ and $e_{\psi\circ\phi}(P,Q) = h_Q(Y \oplus P)/h_Q(Y)$, respectively. If we write $X = \phi(Y)$, then

$$e_\psi\big(\phi(P), Q\big) = \frac{g_Q\big(X \oplus \phi(P)\big)}{g_Q(X)} = \frac{g_Q\big(\phi(Y) \oplus \phi(P)\big)}{g_Q\big(\phi(Y)\big)} = \frac{h_Q(Y \oplus P)}{h_Q(Y)} = e_{\psi\circ\phi}(P,Q).$$

This completes the proof. □

Examples.

- Consider the elliptic curve

$$E: \quad y^2 + a_1\, x\, y + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6$$

Say $\phi = [2]$ is the "multiplication-by-2" map. Recall that the 2-division polynomial is $\psi_2(x) = 2\, y + a_1\, x + a_3 = \sqrt{4\, x^3 + b_2\, x^2 + 2\, b_4\, x + b_6}$. If we denote e as one of the roots of

this polynomial, then $T = (e : -a_1\,e - a_3 : 1)$ as a point of order $m = 2$. We denote the functions

$$\left.\begin{aligned} f_T(P) &= x - e \\ g_T(P) &= \frac{4\,e^2 + b_2\,e + b_4 + 4\,e\,x - 2\,x^2}{2\,(2\,y + a_1\,x + a_3)} \end{aligned}\right\} \qquad \Longrightarrow \qquad \big(f_T \circ [2]\big)(P) = g_T(P)^2.$$

- Consider the elliptic curves

$$\begin{aligned} E:&\ y^2 = x^3 + a\,x^2 + b\,x & & A = -2\,a \\ &\qquad\qquad\qquad\qquad \text{where} \\ E':&\ Y^2 = X^3 + A\,X^2 + B\,X & & B = a^2 - 4\,b \end{aligned}$$

where a, b, A, $B \in k$ satisfy $b\,B \neq 0$. Then we have a maps $\phi : E \to E'$ and $\widehat{\phi} : E' \to E$ which send

$$\begin{aligned} \phi :&\quad (x_1 : x_2 : x_0) &\mapsto& \quad \big(x_2^2\,x_0 \ :\ x_2\,(b\,x_0^2 - x_1^2) \ :\ x_1^2\,x_0\big) \\ \widehat{\phi} :&\quad (X_1 : X_2 : X_0) &\mapsto& \quad \big(2\,X_2^2\,X_0 \ :\ X_2\,(B\,X_0^2 - X_1^2) \ :\ 8\,X_1^2\,X_0\big) \end{aligned}$$

where $\widehat{\phi} \circ \phi = [2]$ is the "multiplication-by-2" map. Note that $\ker(\phi) = \big\{T,\, O\big\}$ is the kernel, there $T = (0 : 0 : 1)$ is a k-rational point of order 2, that is, $[2]T = O$. We denote the functions

$$\left.\begin{aligned} f_T(Q) &= X \\ g_T(P) &= \frac{y}{x} \end{aligned}\right\} \qquad \Longrightarrow \qquad \big(f_T \circ \phi\big)(P) = g_T(P)^2.$$

- There is an easy way to interpret the Weil pairing. Consider the "multiplication-by-m" map $[m] : E \to E$. Since $E[m] \simeq Z_m \times Z_m$ over $\overline{\mathbb{Q}}$, we can choose a basis $\{T_1, T_2\}$. Then define $e_m : E[m] \times E[m] \to \mu_m$ via $S = [a]T_1 \oplus [b]T_2$, and $T = [c]T_1 \oplus [d]T_2$ to ζ_m^{ad-bc}. The only downside to making this definition is one would have to prove that $E[m] \simeq Z_m \times Z_m$!

Tate Pairing. We discuss how a specific example of an isogeny gives information about the elliptic curve.

Theorem 14. Say that E is an elliptic curve over k as above.

- Denote the 2-division polynomial as $\psi_2(x) = 2\,y + a_1\,x + a_3 = \sqrt{4\,x^3 + b_2\,x^2 + 2\,b_4\,x + b_6}$. This has distinct roots $e_1,\ e_2,\ e_3 \in \overline{\mathbb{Q}}$, and so $E : Y^2 = (X - e_1)\,(X - e_2)\,(X - e_3)$. Moreover,

$$\begin{aligned} E[2] &= \big\{T \in E(\overline{\mathbb{Q}}) \,\big|\, [2]\,T = 0\big\} \\ &= \Big\{(e_1 : 0 : 1),\ (e_2 : 0 : 1),\ (e_3 : 0 : 1),\ (0 : 1 : 0)\Big\} \simeq Z_2 \times Z_2. \end{aligned}$$

- Assume that $E[2] \subseteq E(k)$. Consider the map defined by

$$\mathsf{e}_2 :\ \frac{E(k)}{2\,E(k)} \times E[2] \to \frac{k^\times}{(k^\times)^2}, \qquad (P, T) \mapsto \begin{cases} 1 & \text{if } T = O, \\ X - e & \text{otherwise;} \end{cases}$$

where $P = (X : Y : 1)$ and $T = (e : 0 : 1)$. This is a "perfect" pairing i.e.,

– *Non-Degeneracy:* If $\mathsf{e}_2(P,T) = 1$ for all $T \in E[2]$ then $P \in 2\,E(k)$.

– *Bilinearity:* For all $P, Q \in E(k)$ and $T \in E[2]$ we have

$$\mathsf{e}_2(P \oplus Q,\, T) = \mathsf{e}_2(P,T) \cdot \mathsf{e}_2(Q,T),$$
$$\mathsf{e}_2(P,\, T_1 \oplus T_2) = \mathsf{e}_2(P,T_1) \cdot \mathsf{e}_2(P,T_2).$$

Proof. Choose $P = (p_1 : p_2 : p_0) \in E(k)$, and say that $\mathsf{e}_2(P,T) = 1$ for all $T \in E[2]$. To show $P \in 2\,E(k)$ it suffices to exhibit $P' \in E(k)$ such that $P = [2]P'$. If $P = O$ we may choose $P' = O$ as well, so assume $p_0 \neq 0$. Upon considering $T = (e : 0 : 1)$, we see that $f_i = \sqrt{\frac{p_1}{p_0} - e_i} \in k$ for $i = 1, 2, 3$; we choose the signs so that $\frac{p_2}{p_0} = f_1\, f_2\, f_3$. It is easy to check that the desired k-rational point is

$$P' = \left(\frac{(e_1 - e_3)\,(e_2 - e_3)}{(f_1 - f_3)\,(f_2 - f_3)} + e_3 \;:\; \frac{(e_1 - e_2)\,(e_1 - e_3)\,(e_2 - e_3)}{(f_1 - f_2)\,(f_1 - f_3)\,(f_2 - f_3)} \;:\; 1 \right).$$

We show $\mathsf{e}_2(P \oplus Q, T) = \mathsf{e}_2(P,T) \cdot \mathsf{e}_2(Q,T)$. If $T = O$ there is nothing to show since $\mathsf{e}_2(P,T) = \mathsf{e}_2(Q,T) = \mathsf{e}_2(P \oplus Q, T) = 1$ so assume that $T = (e : 0 : 1)$. Choose two points $P = (p_1 : p_2 : p_0)$ and $Q = (q_1 : q_2 : q_0)$ in $E(k)$. Draw a line through them, say $a\,x_1 + b\,x_2 + c\,x_0 = 0$, and assume that it intersects E at a third point $R = (r_1 : r_2 : r_0)$. The projective curve E is defined by the homogeneous polynomial $F(x_1, x_2, x_0) = x_2^2\,x_0 - (x_1 - e_1\,x_0)\,(x_1 - e_2\,x_0)\,(x_1 - e_3\,x_0)$ so the intersection with the line $a\,x_1 + b\,x_2 + c\,x_0 = 0$ admits the factorization

$$p_0\,q_0\,r_0 \cdot F(x_1, x_2, x_0) = (p_1\,x_0 - p_0\,x_1)\,(q_1\,x_0 - q_0\,x_1)\,(r_1\,x_0 - r_0\,x_1)\,.$$

When $(x_1 : x_2 : x_0) = (b\,e : -a\,e - c : b)$ is the point where the lines $a\,x_0 + b\,x_1 + c\,x_0 = 0$ and $x_1 - e\,x_0 = 0$ intersect, we have the equality

$$b^3 \left(\frac{p_1}{p_0} - e\right)\left(\frac{q_1}{q_0} - e\right)\left(\frac{r_1}{r_0} - e\right) = F\,(b\,e,\; -a\,e - c,\, b) = (a\,e + c)^2\,b.$$

This implies the congruence $\mathsf{e}_2(P,T) \cdot \mathsf{e}_2(Q,T) \cdot \mathsf{e}_2(R,T) \equiv 1 \mod (k^\times)^2$. We conclude that $\mathsf{e}_2(P \oplus Q, T) = \mathsf{e}_2(P,T) \cdot \mathsf{e}_2(Q,T)$.

We show $\mathsf{e}_2(P, T_1 \oplus T_2) = \mathsf{e}_2(P,T_1) \cdot \mathsf{e}_2(P,T_2)$. If $T_1 = T_2$ then

$$\mathsf{e}_2(P, T_1 \oplus T_2) = \mathsf{e}_2(P, \mathcal{O}) = 1 \equiv \mathsf{e}_2(P,T_1)^2 = \mathsf{e}_2(P,T_1) \cdot \mathsf{e}_2(P,T_2).$$

If $T_1 \neq T_2$, we may assume $T_1 = (e_1 : 0 : 1)$ and $T_2 = (e_2 : 0 : 1)$. (If either T_1 or T_2 is $\mathcal{O}$ there is nothing to show.) Then $T_1 \oplus T_2 = (e_3 : 0 : 1)$. The identity

$$\left(\frac{p_1}{p_0} - e_1\right)\left(\frac{p_1}{p_0} - e_2\right)\left(\frac{p_1}{p_0} - e_3\right) = \left(\frac{p_2}{p_0}\right)^2$$

implies the congruence $\mathsf{e}_2(P,T_1) \cdot \mathsf{e}_2(P,T_2) \cdot \mathsf{e}_2(P, T_1 \oplus T_2) \equiv 1 \mod (k^\times)^2$. We conclude that $\mathsf{e}_2(P, T_1 \oplus T_2) = \mathsf{e}_2(P,T_1) \cdot \mathsf{e}_2(P,T_2)$. □

Remarks.

- This sometimes called the *Tate pairing*. This is not quite a perfect pairing: non-degeneracy holds on the right, but not on the left.

- Since $\mathsf{e}_2(P,T)$ is bilinear, it is easy to compute its value when $P \in E[2]$. For example, write $T_i = (e_i : 0 : 1)$ so that we find:

$$\begin{aligned} &\mathsf{e}_2(T_i, T_{i-1}) = e_i - e_{i-1}, \\ &\mathsf{e}_2(T_i, T_{i+1}) = e_i - e_{i+1} \end{aligned} \qquad \Longrightarrow \qquad \begin{aligned} \mathsf{e}_2(T_i, T_i) &= \mathsf{e}_2(T_i, T_{i-1}) \cdot \mathsf{e}_2(T_i, T_{i+1}) \\ &= (e_i - e_{i-1})\,(e_i - e_{i+1}). \end{aligned}$$

- If k is a number field, the image in $k^\times / \big(k^\times\big)^2$ is actually finite. One uses this to conclude that $E(k)/2\,E(k)$ is finite as well. This was first shown for $k = \mathbb{Q}$ by Mordell. Say that we can write $E(k) \simeq E(k)_{\text{tors}} \times \mathbb{Z}^r$ for some finite group $E(k)_{\text{tors}} \simeq Z_m \times Z_n$ and some nonnegative integer r; this nonnegative integer is called the *rank* of E over k. Then we can write

$$\frac{E(k)}{2\,E(k)} \simeq \frac{E(k)_{\text{tors}}}{2\,E(k)_{\text{tors}}} \times Z_2^r, \qquad \frac{E(k)_{\text{tors}}}{2\,E(k)_{\text{tors}}} = \begin{cases} \{1\} & \text{if } m \text{ and } n \text{ are odd,} \\ Z_2 & \text{if } m \text{ is even but } n \text{ is odd,} \\ Z_2 \times Z_2 & \text{if both } m \text{ and } n \text{ are even.} \end{cases}$$

  The Theorem above concerns the case where m and n are both even. Hence we can determine the rank r if we can determine the image of this pairing.

- There is a more general construction for each positive integer m:

$$\mathsf{e}_m : \ \frac{E(k)}{m\,E(k)} \times E[m] \to \frac{k^\times}{(k^\times)^m} \qquad \text{assuming} \qquad E[m] \subseteq E(k).$$

  This pairing is used quite often in cryptography, especially when $k = \mathbb{F}_p$ is a finite field of order $p \equiv 1 \pmod{m\,\mathbb{Z}}$ so that $E[m] \simeq Z_m \times Z_m$.

- It is not a coincidence that the Tate pairing is defined via $f_T(Q) = X - e$. In general, say that $\phi : E \to E'$ is a nonconstant isogeny of degree m. We have seen that for each $T \in E'[\widehat{\phi}]$, there are functions $f_T \in \overline{\mathbb{Q}}(E')$ and $g_T \in \overline{\mathbb{Q}}(E)$ such that

$$\begin{aligned} &\operatorname{div}(f_T) = m\,(T) - m\,(O) \\ &\operatorname{div}(g_T) = \phi^*\big((T) - (O)\big) \end{aligned} \qquad \Longrightarrow \qquad f_T \circ \phi = g_T^m.$$

  You can actually choose f_T and g_T to have coefficients in k. This yields a perfect pairing

$$\frac{E'(k)}{\phi\big(E(k)\big)} \times \ker(\widehat{\phi}) \longrightarrow \frac{k^\times}{(k^\times)^m}, \qquad \big(P,\, T\big) \mapsto f_T(P) \bmod (k^\times)^m.$$

- One can derive this pairing from the Weil pairing. We will see in general that the Weil pairing $e_\phi : \ker(\phi) \times \ker(\widehat{\phi}) \to \boldsymbol{\mu}_m$ yields a cup product on Galois cohomology:

$$H^i\big(G_k,\, E[\phi]\big) \times H^j\big(G_k,\, E'[\widehat{\phi}]\big) \longrightarrow H^{i+j}\big(G_k,\, \boldsymbol{\mu}_m\big).$$

  Indeed, there is a short exact sequence

$$\{O\} \longrightarrow E[\phi] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{\ \phi\ } E'(\overline{\mathbb{Q}}) \longrightarrow \{O\}$$

so Galois cohomology gives the diagram

$$\begin{array}{ccccc}
\dfrac{E'(k)}{\phi\big(E(k)\big)} & \times & \ker(\widehat{\phi}) & \longrightarrow & \dfrac{k^\times}{(k^\times)^m} \\
\big\downarrow{\scriptstyle \delta} & & \| & & \| \\
H^1\big(G_k,\, E[\phi]\big) & \times & H^0\big(G_k,\, E'[\widehat{\phi}]\big) & \longrightarrow & H^1\big(G_k,\, \boldsymbol{\mu}_m\big)
\end{array}$$