A QUICK INTRODUCTION TO ELLIPTIC CURVES

This writeup sketches aspects of the theory of elliptic curves, first over fields of characteristic zero and then over arbitrary fields.

1. Elliptic curves in characteristic zero

Let $\mathbf{k}$ denote any field of characteristic 0.

Definition 1. *An element α of an extension field $\mathbf{K}$ of $\mathbf{k}$ is* algebraic over $\mathbf{k}$ *if it satisfies some monic polynomial with coefficients in $\mathbf{k}$. Otherwise α is* transcendental over $\mathbf{k}$. *A field extension $\mathbf{K}/\mathbf{k}$ is* algebraic *if every $\alpha \in \mathbf{K}$ is algebraic over $\mathbf{k}$. A field $\mathbf{k}$ is* algebraically closed *if there is no proper algebraic extension $\mathbf{K}/\mathbf{k}$; that is, in any extension field $\mathbf{K}$ of $\mathbf{k}$, any element α that is algebraic over $\mathbf{k}$ in fact lies in $\mathbf{k}$. An* algebraic closure $\overline{\mathbf{k}}$ *of $\mathbf{k}$ is a minimal algebraically closed extension field of $\mathbf{k}$.*

Every field has an algebraic closure. Any two algebraic closures $\overline{\mathbf{k}}$ and $\overline{\mathbf{k}}'$ of $\mathbf{k}$ are $\mathbf{k}$-isomorphic, meaning there exists an isomorphism $\overline{\mathbf{k}} \xrightarrow{\sim} \overline{\mathbf{k}}'$ fixing $\mathbf{k}$ pointwise, so we often refer imprecisely to "the" algebraic closure of $\mathbf{k}$.

A *Weierstrass equation over* $\mathbf{k}$ is any cubic equation of the form

$$E : y^2 = 4x^3 - g_2 x - g_3, \quad g_2, g_3 \in \mathbf{k}. \tag{1}$$

Define the *discriminant* of the equation to be

$$\Delta = g_2^3 - 27 g_3^2 \in \mathbf{k},$$

and if $\Delta \neq 0$ define the *invariant* of the equation to be

$$j = 1728 g_2^3 / \Delta \in \mathbf{k}.$$

Definition. *Let $\overline{\mathbf{k}}$ be an algebraic closure of the field $\mathbf{k}$. When a Weierstrass equation E has nonzero discriminant Δ it is called* nonsingular *and the set*

$$\mathcal{E} = \{(x, y) \in \overline{\mathbf{k}}^2 \text{ satisfying } E(x, y)\} \cup \{\infty\}$$

is called an elliptic curve over $\mathbf{k}$.

Thus an elliptic curve always contains the point ∞. As the solution set of a polynomial equation in two variables, an elliptic curve as defined here is a special case of a plane algebraic curve.

Strictly speaking we are interested in equivalence classes of elliptic curves under *admissible changes of variable*,

$$x = u^2 x', \quad y = u^3 y', \qquad u \in \mathbf{k}^*.$$

These transform Weierstrass equations to Weierstrass equations, taking g_2 to g_2/u^4, g_3 to g_3/u^6, the discriminant Δ to Δ/u^{12} (again nonzero) and preserving the invariant j (exercise). Admissible changes of variable are special cases of isomorphisms between algebraic curves.

For example, consider an elliptic curve $\mathcal{E}$ over $\mathbb{C}$ whose invariant is rational. Supposing g_2 and g_3 are nonzero, the condition $j \in \mathbb{Q}$ is $g_2^3 = r g_3^2$ for some nonzero

$r \in \mathbb{Q}$ (exercise). Let $u \in \mathbb{C}$ satisfy $g_2/u^4 = r$; then also $r^3u^{12} = g_2^3 = rg_3^2$ and thus $g_3/u^6 = \pm r$, and we may take $g_3/u^6 = r$ after replacing u by iu if necessary. Since the admissible change of variable $x = u^2x'$, $y = u^3y'$ produces new Weierstrass coefficients $g_2' = g_2/u^4$ and $g_3' = g_3/u^6$, this shows that up to isomorphism $\mathcal{E}$ is defined over $\mathbb{Q}$ by a Weierstrass equation

$$y^2 = 4x^3 - gx - g, \quad g \in \mathbb{Q}.$$

A separate argument when one of g_2, g_3 is zero (exercise) shows that in all cases an elliptic curve over $\mathbb{C}$ has rational invariant $j \in \mathbb{Q}$ if and only if it is isomorphic over $\mathbb{C}$ to an elliptic curve over $\mathbb{Q}$. This argument works with $\mathbb{C}$ replaced by any algebraically closed field $\mathbf{k}$ of characteristic 0 and with $\mathbb{Q}$ replaced by any subfield $\mathbf{f}$ of $\mathbf{k}$. It shows that any two elliptic curves over $\mathbf{k}$ with the same invariant j are isomorphic when $\mathbf{k}$ is algebraically closed.

Associated to each Weierstrass equation and also denoted E is a corresponding *Weierstrass polynomial*,

$$E(x, y) = y^2 - 4x^3 + g_2x + g_3 \in \mathbf{k}[x, y].$$

The Weierstrass equation (1) is nonsingular, meaning as in Definition 1 that its discriminant Δ is nonzero, if and only if the corresponding curve $\mathcal{E}$ is *geometrically nonsingular*, meaning that at each point $(x, y) \in \mathcal{E}$ at least one of the partial derivatives $D_1E(x, y)$, $D_2E(x, y)$ of the Weierstrass polynomial is nonzero. To see this, note that the Weierstrass polynomial takes the form

$$E(x, y) = y^2 - 4(x - x_1)(x - x_2)(x - x_3), \quad x_1, x_2, x_3 \in \overline{\mathbf{k}}.$$

The third condition of

$$E(x, y) = 0, \qquad D_1E(x, y) = 0, \qquad D_2E(x, y) = 0$$

is $y = 0$ since $\mathrm{char}(\mathbf{k}) = 0$. Now the first condition is $x \in \{x_1, x_2, x_3\}$, making the second condition impossible exactly when x_1, x_2, x_3 are distinct, i.e., when $\Delta \neq 0$. One can think of geometric nonsingularity as meaning that $\mathcal{E}$ has a tangent line at each point.

Many good texts on elliptic curves exist, so we state without proof the facts that we need. Most importantly,

> *every elliptic curve forms an Abelian group with the point ∞ as its additive identity.*

The point ∞ is therefore denoted $0_{\mathcal{E}}$ from now on. One can think of addition on $\mathcal{E}$ geometrically, algebraically, and analytically.

Geometrically the elliptic curve really sits in the *projective plane over* $\overline{\mathbf{k}}$, denoted $\mathbb{P}^2(\overline{\mathbf{k}})$, the usual plane $\overline{\mathbf{k}}^2$ (called the *affine* plane) along with some additional points conceptually out at infinity added to complete it. (The reader who is unfamiliar with this construction should work exercise 3 to follow for details of the following assertions.) The projective plane is the union of three overlapping affine planes and the elliptic curve is correspondingly the union of three affine pieces. The projective point ∞ of $\mathcal{E}$ is infinitely far in the y-direction, i.e., $0_{\mathcal{E}} = [0, 1, 0]$ in projective notation. The curve can be studied about $0_{\mathcal{E}}$ by working in a different affine piece of $\mathbb{P}^2(\overline{\mathbf{k}})$, and it is geometrically nonsingular at $0_{\mathcal{E}}$ as it is at its finite points. Projective space is a natural construct, e.g., the Riemann sphere $\mathbb{C} \cup \{\infty\}$ is $\mathbb{P}^1(\mathbb{C})$, and similarly the set $\{0, \ldots, p-1, \infty\}$ that often serves as an index set in the context of the Hecke operator T_p can be viewed as $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$.

Bézout's Theorem says that if $\mathcal{C}_1$ and $\mathcal{C}_2$ are plane curves over $\mathbf{k}$ whose defining polynomials have degrees d_1 and d_2 and are relatively prime in $\overline{\mathbf{k}}[x, y]$ (a unique factorization domain) then their intersection in $\mathbb{P}^2(\overline{\mathbf{k}})$ consists of $d_1 d_2$ points, suitably counting multiplicity. Thus cubic curves, and only cubic curves, naturally produce triples P, Q, R of collinear points, meaning projective points satisfying an equation $ax + by + cz = 0$ where $a, b, c \in \mathbf{k}$ are not all zero. If the line is tangent to the curve then two or three of P, Q, and R will coincide. The addition law on elliptic curves $\mathcal{E}$ is that *collinear triples sum to* $0_\mathcal{E}$. That is,

$$P + Q + R = 0_\mathcal{E} \iff P,\ Q,\ R \text{ are collinear.}$$

In particular, since $P - P + 0_\mathcal{E} = 0_\mathcal{E}$ it follows that P, $-P$, and $0_\mathcal{E}$ are collinear. So far this only requires $0_\mathcal{E}$ to be any point of $\mathcal{E}$, but the condition $0_\mathcal{E} = [0, 1, 0]$ gives the addition law a pleasing geometry. Since $0_\mathcal{E}$ is infinitely far in the vertical direction, P and $-P$ have the same x-coordinate. At most two points with the same x-coordinate satisfy the Weierstrass equation (1), so any two points with the same x-coordinate are equal or opposite, possibly both. Since the y-values satisfying (1) for a given x sum to 0 the additive inverse of $P = (x_P, y_P)$ is the natural companion point

$$-P = (x_P, -y_P).$$

As remarked, this could well be P again. More generally, given points P and Q of $\mathcal{E}$, let R be their third collinear point. The addition law $P + Q = -R$ says that the sum is the companion point of R, its reflection through the x-axis,

$$\text{(2)} \qquad \textit{if } P,\ Q,\ R \textit{ are collinear then } P + Q = (x_R, -y_R).$$

Figure 1 illustrates this for the elliptic curve $y^2 = 4x^3 - 4x$.

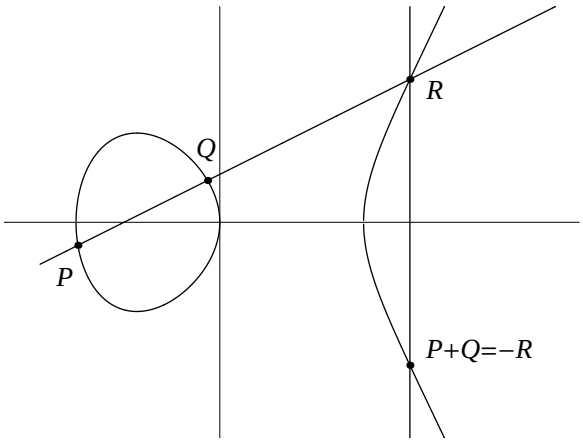

FIGURE 1. The addition law

Moving from geometry to algebra, the group law is defined by rational functions over the field $\mathbf{k}$. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be nonzero points of the curve, and suppose their sum $P + Q = (x_{P+Q}, y_{P+Q})$ is nonzero as well. Then

$$x_{P+Q} = r(x_P, y_P, x_Q, y_Q) \quad \text{and} \quad y_{P+Q} = s(x_P, y_P, x_Q, y_Q)$$

where r and s are rational functions with coefficients in $\mathbf{k}$. Even more specifically since $\text{char}(\mathbf{k}) = 0$, r and s are rational functions over the field $\mathbb{Q}(g_2, g_3)$. If $x_Q = x_P$

and $y_Q = -y_P$ then $Q = -P$ and so $P+Q = 0_{\mathcal{E}}$. Otherwise $P+Q$ lies in the affine part of $\mathcal{E}$. Let

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & x_P \neq x_Q, \\ \dfrac{12x_P^2 - g_2}{2y_P} & x_P = x_Q, \end{cases} \qquad \mu = \begin{cases} \dfrac{x_Q y_P - x_P y_Q}{x_Q - x_P} & x_P \neq x_Q, \\ \dfrac{-4x_P^3 - g_2 x_P - 2g_3}{2y_P} & x_P = x_Q. \end{cases}$$

The line $y = \lambda x + \mu$ passes through P and Q when $P \neq Q$ and is the tangent line to $\mathcal{E}$ at P when $P = Q$ (exercise). The casewise nature of λ and μ will be discussed further in the next section. In either case, the rational functions giving x_{P+Q} and y_{P+Q} are

$$\begin{aligned} r(x_P, y_P, x_Q, y_Q) &= \lambda^2/4 - x_P - x_Q, \\ s(x_P, y_P, x_Q, y_Q) &= -\lambda\, r(x_P, y_P, x_Q, y_Q) - \mu. \end{aligned} \tag{3}$$

This algebraic definition of addition corresponds to the geometric description (2) (exercise). For example, on the curve $y^2 = 4x^3 - 4x$ of Figure 1, $(0,0) + (2, 2\sqrt{6}) = (-1/2, \sqrt{6}/2)$.

Because the coordinates of $0_{\mathcal{E}} = [0,1,0]$ lie in $\mathbf{k}$ and because the group law is rational over $\mathbf{k}$, for any algebraic extension $\mathbf{K}/\mathbf{k}$ (i.e., $\mathbf{k} \subset \mathbf{K} \subset \overline{\mathbf{k}}$) the set of $\mathbf{K}$-*points of* $\mathcal{E}$ is a subgroup of $\mathcal{E}$,

$$\mathcal{E}(\mathbf{K}) = \{P \in \mathcal{E} - \{0_{\mathcal{E}}\} : (x_P, y_P) \in \mathbf{K}^2\} \cup \{0_{\mathcal{E}}\}.$$

In particular if $\mathcal{E}$ is an elliptic curve over $\mathbb{Q}$ then its affine rational points and $0_{\mathcal{E}}$ form a group under the addition law. A special case of the *Mordell–Weil Theorem* states that this group is finitely generated. The text by Silverman and Tate gives an excellent discussion of this subject.

We want to study the torsion structure of $\mathcal{E}$ algebraically. For any positive integer N let

$$[N] : \mathcal{E} \longrightarrow \mathcal{E}$$

denote N-fold addition, e.g., $[2]P = P + P$. This takes the form of a rational function,

$$[N](x,y) = \left(\frac{\phi_N(x,y)}{\psi_N(x,y)^2}, \frac{\omega_N(x,y)}{\psi_N(x,y)^3} \right).$$

Here the *Nth division polynomials* ϕ_N, ω_N, ψ_N lie in $\mathbb{Z}[g_2, g_3, x, y]$, and (∞, ∞) is understood to mean $0_{\mathcal{E}}$. Thus the condition $[N](x,y) = 0_{\mathcal{E}}$ is $\psi_N(x,y) = 0$. This works out to a polynomial condition on x alone,

$$[N](x,y) = 0_{\mathcal{E}} \iff \tilde{\psi}_N(x) = 0, \quad \tilde{\psi}_N \in \mathbb{Z}[g_2, g_3, x].$$

For instance, the condition $[2]P = 0$ for a nonzero point P is $y_P = 0$, or $4x_P^3 - g_2 x_P - g_3 = 0$. Similarly, the condition that $[3]P = 0$ for nonzero P is $[2]P = -P$, or $x([2]P) = x_P$, or $r(x_P, y_P, x_P, y_P) = x_P$, and this works out to $48x_P^4 - 24g_2x_P^2 - 48g_3x_P - g_2^2 = 0$ (exercise).

Let $\mathcal{E}[N]$ denote the group of N-*torsion points of* $\mathcal{E}$, the kernel of $[N]$,

$$\mathcal{E}[N] = \{P \in \mathcal{E} : [N]P = 0_{\mathcal{E}}\}.$$

We quote the structure theorem for $\mathcal{E}[N]$.

Theorem. *Let $\mathcal{E}$ be an elliptic curve over a field $\mathbf{k}$ of characteristic 0 and let N be a positive integer. Then $\mathcal{E}[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$.*

Let $\mathbf{K}$ be a Galois extension field of $\mathbf{k}$ containing the x- and y-coordinates of $\mathcal{E}[N] \setminus \{0_\mathcal{E}\}$. The relations $E(x^\sigma, y^\sigma) = E(x,y)^\sigma$ and $\tilde{\psi}_N(x^\sigma) = \tilde{\psi}_N(x)^\sigma$ for any $x, y \in \mathbf{K}$ and any automorphism $\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{k})$ show that the Galois group acts on $\mathcal{E}[N]$. The action is an automorphism since the coefficients of the rational functions r and s lie in $\mathbb{Q}(g_2, g_3)$ and hence in $\mathbf{k}$. That is, $r(x_P^\sigma, y_P^\sigma, x_Q^\sigma, y_Q^\sigma) = r(x_P, y_P, x_Q, y_Q)^\sigma$ for all $P, Q \in \mathcal{E}[N]$, and similarly for s, making $P^\sigma + Q^\sigma = (P+Q)^\sigma$. Since $\mathcal{E}[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$, once an ordered basis (P, Q) of $\mathcal{E}[N]$ over $\mathbb{Z}/N\mathbb{Z}$ is chosen this gives a representation

$$\rho : \mathrm{Gal}(\mathbf{K}/\mathbf{k}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}), \qquad \begin{bmatrix} P^\sigma \\ Q^\sigma \end{bmatrix} = \rho(\sigma) \begin{bmatrix} P \\ Q \end{bmatrix},$$

where as always $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is the group of invertible 2-by-2 matrices with entries in $\mathbb{Z}/N\mathbb{Z}$. (Here we are seeing the beginning of the idea of a Galois representation associated to the ellpitic curve.)

Analytically, when $\mathbf{k} \subset \mathbb{C}$ we may view the coefficients of the Weierstrass equation as complex numbers. We know that there exists a lattice $\Lambda \subset \mathbb{C}$ such that the Weierstrass equation (1) takes the form $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, and addition on the corresponding curve $\mathcal{E}$ is compatible with the natural addition on $\mathbb{C}/\Lambda$ via the Weierstrass function $\wp$. In particular, the torsion group structure theorem is clear and familiar when $\mathbf{k} = \mathbb{C}$. Also we know that holomorphic isomorphisms of complex tori correspond to admissible changes of variable in complex Weierstrass equations.

Recall that the map $(\wp_\tau, \wp'_\tau)$ takes the complex torus $\mathbb{C}/\Lambda_\tau$ to the algebraic curve $E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$. (From now on the symbol E interchangeably denotes an elliptic curve, its equation, or its polynomial, and the symbol $\mathcal{E}$ will no longer be used.) The field of meromorphic functions on the modular curve $X(N)$ is generated by the modular invariant j and by functions of τ closely related to the x-coordinates of the nonzero N-torsion points on the curve E_τ. We now scale the curve E_τ to a new curve so that indeed $\mathbb{C}(X(N))$ is generated by j and the N-torsion x-coordinates.

Fix any $\tau \in \mathcal{H}$ such that $j(\tau) \notin \{0, 1728\}$. This means that $g_2(\tau)$ and $g_3(\tau)$ are nonzero since $j = 1728 g_2^3/(g_2^3 - 27g_3^2)$. Choose either complex square root $(g_2(\tau)/g_3(\tau))^{1/2}$ and consider the map

$$\left(\frac{g_2(\tau)}{g_3(\tau)} \wp_\tau \, , \, \left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{3/2} \wp'_\tau \right) : \mathbb{C}/\Lambda_\tau \longrightarrow \mathbb{C}^2 \cup \{\infty\}.$$

This differs from $(\wp_\tau, \wp'_\tau)$ by the admissible change of variable $(x, y) = (u^2 x', u^3 y')$ where $u = (g_3(\tau)/g_2(\tau))^{1/2}$. Thus $u^{-4} = (g_2(\tau)/g_3(\tau))^2$ and $u^{-6} = (g_2(\tau)/g_3(\tau))^3$, and nonzero points $z + \Lambda_\tau$ map to points (x, y) satisfying the suitable modification of the cubic equation of E_τ according to an exercise.

$$E_{j(\tau)} : y^2 = 4x^3 - \frac{g_2(\tau)^3}{g_3(\tau)^2} x - \frac{g_2(\tau)^3}{g_3(\tau)^2}.$$

Since $g_3^2 = (g_2^3 - \Delta)/27$, so that $g_2^3/g_3^2 = 27g_2^3/(g_2^3 - \Delta) = 27j/(j - 1728)$, the equation is defined in terms of $j(\tau)$, justifying the name of the curve,

$$E_{j(\tau)} : y^2 = 4x^3 - \left(\frac{27j(\tau)}{j(\tau) - 1728}\right) x - \left(\frac{27j(\tau)}{j(\tau) - 1728}\right).$$

(Cf. the method of reducing the general $y^2 = 4x^3 - g_2x - g_3$ to the form $y^2 = 4x^3 - gx - g$.) The equation is independent of which square root $(g_2(\tau)/g_3(\tau))^{1/2}$ was chosen. The map $\mathbb{C}/\Lambda_\tau \xrightarrow{\sim} E_{j(\tau)}$ restricts to an isomorphism of N-torsion subgroups. In particular it takes the canonical generators $\tau/N + \Lambda_\tau$ and $1/N + \Lambda_\tau$ of $(\mathbb{C}/\Lambda_\tau)[N]$ to the points

$$\begin{aligned} P_\tau &= \left(\frac{g_2(\tau)}{g_3(\tau)}\,\wp_\tau(\tau/N)\,,\,\left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{3/2}\wp'_\tau(\tau/N)\right), \\ Q_\tau &= \left(\frac{g_2(\tau)}{g_3(\tau)}\,\wp_\tau(1/N)\,,\,\left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{3/2}\wp'_\tau(1/N)\right). \end{aligned} \tag{4}$$

Negating the square root $(g_2(\tau)/g_3(\tau))^{1/2}$ negates these points, but modulo this (P_τ, Q_τ) is a canonical ordered basis of $E_{j(\tau)}[N]$ over $\mathbb{Z}/N\mathbb{Z}$. The x-coordinates of $\pm P_\tau$ and $\pm Q_\tau$ are $f_{1,0}(\tau)$ and $f_{0,1}(\tau) = f_1(\tau)$ respectively, and more generally the nonzero points of $E_{j(\tau)}[N]$ have x-coordinates $\{f_0^{\pm\overline{v}}(\tau)\}$ as desired. The information $j(\tau)$, $f_{1,0}(\tau)$, $f_{0,1}(\tau)$ thus describes an enhanced elliptic curve for $\Gamma(N)$ modulo negation,

$$(E_{j(\tau)}, \pm(P_\tau, Q_\tau)).$$

This is the sort of element that represents a point $[\mathbb{C}/\Lambda_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)]$ of the moduli space $\mathrm{S}(N)$, excluding the finitely many such points with $j(\tau) \in \{0, 1728\}$. Similarly, the information $j(\tau)$, $f_1(\tau)$ describes $(E_{j(\tau)}, \pm Q_\tau)$, representing a point of $\mathrm{S}_1(N)$, and $j(\tau)$, $f_0(\tau)$ describes $(E_{j(\tau)}, \langle Q_\tau\rangle)$, representing a point of $\mathrm{S}_0(N)$. The moduli space description of modular curves is emerging from the function field description.

Change τ to a variable so that $j = j(\tau)$ varies as well. This gathers the family of elliptic curves $E_{j(\tau)}$ into a single *universal elliptic curve*,

$$E_j : y^2 = 4x^3 - \left(\frac{27j}{j-1728}\right)x - \left(\frac{27j}{j-1728}\right), \tag{5}$$

whose j-invariant is indeed the variable j (exercise). The universal elliptic curve specializes to a complex elliptic curve for every complex j except 0 and 1728.

Exercises

1. *Show that every admissible change of variable $x = u^2x'$, $y = u^3y'$ where $u \in \mathbf{k}^*$ transforms a Weierstrass equation E into another Weierstrass equation E' with*

$$u^4g'_2 = g_2, \qquad u^6g'_3 = g_3, \qquad u^{12}\Delta' = \Delta, \qquad j' = j.$$

2. (a) *Confirm that for a Weierstrass equation* (1) *with g_2 and g_3 nonzero the condition $j \in \mathbb{Q}$ is equivalent to the condition $g_2^3 = rg_3^2$ for some nonzero $r \in \mathbb{Q}$.*
(b) *Show that an elliptic curve over $\mathbb{C}$ with either of g_2, g_3 zero is isomorphic to an elliptic curve over $\mathbb{Q}$.*

3. *For any positive integer n and any field $\mathbf{K}$,* n-dimensional projective space over $\mathbf{K}$ *is the set of equivalence classes of nonzero $(n+1)$-tuples modulo scalar multiplication,*

$$\mathbb{P}^n(\mathbf{K}) = (\mathbf{K}^{n+1} - \{\mathbf{0}\})/\sim$$

where $v \sim v'$ if $v' = cv$ for some nonzero $c \in \mathbf{K}$. Let $[v] \in \mathbb{P}^n(\mathbf{K})$ denote the equivalence class of the vector v.

(a) *When $n = 1$ this construction gives the* projective line. *Show that*

$$\mathbb{P}^1(\mathbf{K}) = \{[x, 1] : x \in \mathbf{K}\} \cup \{[1, y] : y \in \mathbf{K}\},$$

so the projective line is an overlapping union of two affine lines. Show also that

$$\mathbb{P}^1(\mathbf{K}) = \{[x, 1] : x \in \mathbf{K}\} \cup \{[1, 0]\},$$

so the projective line is a disjoint union of the line and a point at infinity. In particular, $\mathbb{P}^1(\mathbb{C})$ is the Riemann sphere $\widehat{\mathbb{C}}$.
(b) *When $n = 2$ the construction gives the projective plane mentioned in the section. Show that*

$$\mathbb{P}^2(\mathbf{K}) = \{[x, y, 1] : x, y \in \mathbf{K}\} \cup \{[x, 1, z] : x, z \in \mathbf{K}\} \cup \{[1, y, z] : y, z \in \mathbf{K}\},$$

so the projective plane is a union of three affine planes. Show also that

$$\begin{aligned}\mathbb{P}^2(\mathbf{K}) &= \{[x, y, 1] : x, y \in \mathbf{K}\} \cup \{[x, 1, 0] : x \in \mathbf{K}\} \cup \{[1, 0, 0]\} \\ &= \{[x, y, 1] : x, y \in \mathbf{K}\} \cup (\mathbb{P}^1(\mathbf{K}) \times \{0\}),\end{aligned}$$

so the projective plane is a disjoint union of the plane and a projective line at infinity.
(c) Homogenize *the Weierstrass polynomial by adding in powers of z to make each term cubic,*

$$E_{\text{hom}}(x, y, z) = y^2 z - 4x^3 + g_2 x z^2 + g_3 z^3.$$

Show that either all points or no points in each equivalence class $[x, y, z] \in \mathbb{P}^2(\overline{\mathbf{k}})$ satisfy E_{hom}. Show that $[0, 1, 0]$ satisfies E_{hom} and no other $[x, y, 0]$ does.
(d) *Dehomogenize E_{hom} by setting $y = 1$ to obtain a second affine version of E,*

$$E'(x, z) = z - 4x^3 + g_2 x z^2 + g_3 z^3.$$

In the (x, z) coordinate system, the infinite point $0_{\mathcal{E}}$ is $(0, 0)$. Working in this affine coordinate system, show that $\mathcal{E}$ is geometrically nonsingular at $0_{\mathcal{E}}$. Is the set of points $(x, z) \in \overline{\mathbf{k}}^2$ satisfying $E'(x, z)$ all of $\mathcal{E}$?
(e) *Let $P = (x_P, y_P)$ be any (x, y)-point of $\mathcal{E}$, and homogenize it to $P = [x_P, y_P, 1]$. Show that the homogeneous equation $x - x_P z = 0$ is satisfied by P and by $0_{\mathcal{E}}$, thus defining the projective line containing them. Dehomogenize back to an (x, y)-equation to obtain a vertical line. Thus $0_{\mathcal{E}}$ is infinitely far in the vertical direction.*

4. (a) *Show that the casewise definitions of λ and μ make the line $y = \lambda x + \mu$ the secant line through P and Q when $P \neq Q$ and the tangent line to $\mathcal{E}$ through P when $P = Q$.*
(b) *Show that the algebraic definition* (3) *of elliptic curve addition corresponds to the geometric description* (2)*.*
(c) *The points $(2, \pm 5)$ satisfy the equation $y^2 = 4x^3 - 7$. Find another point $(x, y) \in \mathbb{Q}^2$ that does so as well.*

5. (a) *Confirm that the condition $x([2]P) = x_P$ works out to the polynomial condition given in the section.*
(b) *Compute $\mathcal{E}[2]$ and $\mathcal{E}[3]$ for the elliptic curve with Weierstrass equation $y^2 = 4x^3 - 4x$.*

2. Elliptic curves in arbitrary characteristic

Much of the material in section 1 on elliptic curves in characteristic 0 is also valid in characteristic p. Let $\mathbf{k}$ be an arbitrary field. A *Weierstrass equation over* $\mathbf{k}$ is any cubic equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, \dots, a_6 \in \mathbf{k}. \tag{6}$$

To study this, define

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2,$$

and define the *discriminant* of the equation to be

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Further define

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

and if $\Delta \neq 0$ define the *invariant* of the equation to be

$$j = c_4^3/\Delta.$$

Then all $b_i \in \mathbf{k}$, $\Delta \in \mathbf{k}$, all $c_i \in \mathbf{k}$, and $j \in \mathbf{k}$ when it is defined. Also, $4b_8 = b_2b_6 - b_4^2$ and $1728\Delta = c_4^3 - c_6^2$. (Confirming the calculations in this paragraph is an exercise.) If $\mathbf{k}$ does not have characteristic 2 then replacing y by $y - (a_1x + a_3)/2$ in (6) eliminates the xy and y terms from the left side, reducing the Weierstrass equation to

$$E : y^2 = x^3 + (b_2x^2 + 2b_4x + b_6)/4, \quad b_2, b_4, b_6 \in \mathbf{k}, \text{ char}(\mathbf{k}) \neq 2. \tag{7}$$

If $\mathbf{k}$ does not have characteristic 2 or 3 then replacing x by $(x - 3b_2)/36$ and y by $y/216$ in (7) eliminates the x^2 term from the right side, further reducing the Weierstrass equation to the form

$$E : y^2 = x^3 - 27c_4x - 54c_6, \quad c_4, c_6 \in \mathbf{k}, \text{ char}(\mathbf{k}) \notin \{2, 3\}. \tag{8}$$

Since (7) and (8) are special cases of (6), the coefficients of a Weierstrass equation will be referred to as the a_i in all cases.

As before,

Definition. *Let* $\overline{\mathbf{k}}$ *be an algebraic closure of the field* $\mathbf{k}$*. When a Weierstrass equation* E *has nonzero discriminant* Δ *it is called* nonsingular *and the set*

$$E = \{(x, y) \in \overline{\mathbf{k}}^2 \text{ satisfying } E(x, y)\} \cup \{\infty\}$$

is called an elliptic curve over $\mathbf{k}$.

Note that an elliptic curve over $\mathbf{k}$ has infinitely many points even when $\mathbf{k}$ is a finite field.

The *general admissible change of variable* is

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t, \qquad u, r, s, t \in \mathbf{k}, \ u \neq 0.$$

These form a group, and they transform Weierstrass equations to Weierstrass equations, taking the discriminant Δ to Δ/u^{12} and preserving the invariant j (exercise). In particular the changes of variable between Weierstrass equations (6), (7), and (8) are admissible, and thus we may work with (8) if $\text{char}(\mathbf{k}) \notin \{2, 3\}$ and with (7) if $\text{char}(\mathbf{k}) \neq 2$, needing the general (6) only when $\text{char}(\mathbf{k}) = 2$ or when there is no assumption about the characteristic—for example, one can reduce a Weierstrass

equation (6) over $\mathbb{Q}$ modulo an arbitrary prime p. Since the changes of variable from (6) to (7) to (8) have $u = 1$ and $u = 1/6$ respectively, the discriminant of (8) is 6^{12} times the discriminant of (6) and (7), i.e., $\Delta_{(8)} = 2^6 3^9 (c_4^3 - c_6^2)$.

Somewhat awkwardly, the cubic equation $y^2 = 4x^3 - g_2 x - g_3$ from section 1 is no longer a Weierstrass equation by our new definition since the coefficients of y^2 and x^3 are unequal, and replacing y by $2y$ to put it in the form (8) is an inadmissible change of variable. Both sorts of cubic equation can be encompassed in more general definitions of Weierstrass equation and admissible change of variable, but since normalizing the coefficients of y^2 and x^3 to 1 simplifies the formulas of this chapter we accept the small inconsistency in terminology instead. Modulo the inadmissible substitution, the earlier definitions of the discriminant and the invariant for equations $y^2 = 4x^3 - g_2 x - g_3$ are the same as their definitions for (8) (exercise).

In particular, replacing y by $2y$ in the universal elliptic curve (5) leads to the Weierstrass equation

$$y^2 = x^3 - \frac{1}{4}\left(\frac{27j}{j-1728}\right)x - \frac{1}{4}\left(\frac{27j}{j-1728}\right), \tag{9}$$

with discriminant $2^6 3^{12} j^2/(j-1728)^3$ and invariant j. An admissible change of variable then gives a more general universal curve (exercise)

$$y^2 + xy = x^3 - \left(\frac{36}{j-1728}\right)x - \left(\frac{1}{j-1728}\right), \tag{10}$$

with discriminant $j^2/(j-1728)^3$ and invariant j. The curve (10) is well suited for fields of arbitrary characteristic since its discriminant is nonzero even in characteristic 2 or 3. It is used to define modular curves in prime characteristic as the universal elliptic curve is used to define modular curves over $\mathbb{Q}$.

Most of the results from Section 1 hold in arbitrary characteristic. The Weierstrass polynomial associated to (6) is

$$E(x,y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 \in \mathbf{k}[x,y], \tag{11}$$

and similarly for (7) and (8). In all cases the Weierstrass equation is nonsingular if and only if the corresponding curve E is geometrically nonsingular, i.e., the gradient of the Weierstrass polynomial never vanishes. Verifying this in characteristic 2 requires a different argument from the one given before (exercise). Again an elliptic curve E lies in $\mathbb{P}^2(\overline{\mathbf{k}})$, it forms an Abelian group with the infinite point $[0,1,0]$ (see exercise 3(a)) as its additive identity 0_E, and the addition law is that collinear triples sum to 0_E. Opposite pairs of points P and $-P$ have the same x-coordinate, at most two points with the same x-coordinate satisfy (6), and so any two points with the same x-coordinate are equal or opposite, possibly both. Since the y-values satisfying (6) for a given x sum to $-a_1 x - a_3$ the additive inverse of $P = (x_P, y_P)$ is the natural companion point

$$-P = (x_P, -y_P - a_1 x_P - a_3).$$

Given points P and Q of E, let R be their third collinear point. The addition law $P + Q = -R$ says that the sum is the companion point of R,

$$\textit{if } P, Q, R \textit{ are collinear then } P + Q = (x_R, -y_R - a_1 x_R - a_3). \tag{12}$$

Let $\mathbf{k}_{\text{prime}}$ denote the *prime subfield* of $\mathbf{k}$, meaning the smallest subfield inside $\mathbf{k}$, either the rational numbers $\mathbb{Q}$ if $\text{char}(\mathbf{k}) = 0$ or the finite field $\mathbb{F}_p$ of order p if

$\mathrm{char}(\mathbf{k}) = p$. Then the group law is defined by rational functions r and s over the field $\mathbf{k}_{\mathrm{prime}}(\{a_i\})$ where the a_i are the Weierstrass coefficients. If $x_Q = x_P$ and $y_Q = -y_P - a_1x_P - a_3$ then $Q = -P$ and so $P + Q = 0_E$. Otherwise $P + Q$ lies in the affine part of E. Let

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & x_P \neq x_Q, \\ \dfrac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{a_1x_P + a_3 + 2y_P} & x_P = x_Q, \end{cases}$$

and

$$\mu = \begin{cases} \dfrac{y_Px_Q - y_Qx_P}{x_Q - x_P} & x_P \neq x_Q, \\ \dfrac{-x_P^3 + a_4x_P + 2a_6 - a_3y_P}{a_1x_P + a_3 + 2y_P} & x_P = x_Q. \end{cases}$$

The line $y = \lambda x + \mu$ passes through P and Q when $P \neq Q$ and is the tangent line to E at P when $P = Q$ (exercise). The rational functions giving x_{P+Q} and y_{P+Q} are

$$\begin{aligned} r(x_P, x_Q, y_P, y_Q) &= \lambda^2 + a_1\lambda - a_2 - x_P - x_Q, \\ s(x_P, x_Q, y_P, y_Q) &= -(\lambda + a_1)r(x_P, x_Q, y_P, y_Q) - \mu - a_3. \end{aligned} \tag{13}$$

This algebraic definition of addition corresponds to the geometric description (12) (exercise). As before, the casewise expressions for λ and μ arise from a single rational function (exercise). For any algebraic extension $\mathbf{K}/\mathbf{k}$ the set of $\mathbf{K}$-points of E is a subgroup of E,

$$E(\mathbf{K}) = \{P \in E - \{0_E\} : (x_P, y_P) \in \mathbf{K}^2\} \cup \{0_E\}.$$

Let N be a positive integer. The structure theorem for the N-torsion subgroup $E[N] = \ker([N])$ of an elliptic curve is

Theorem. *Let E be an elliptic curve over $\mathbf{k}$ and let N be a positive integer. Then*

$$E[N] \cong \prod E[p^{e_p}] \quad \textit{where } N = \prod p^{e_p}.$$

Also,

$$E[p^e] \cong (\mathbb{Z}/p^e\mathbb{Z})^2 \quad \textit{if } p \neq \mathrm{char}(\mathbf{k}).$$

Thus $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$ if $\mathrm{char}(\mathbf{k}) \nmid N$. On the other hand,

$$\left.\begin{array}{c} E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \textit{ for all } e \geq 1 \\ \textit{or} \\ E[p^e] = \{0\} \textit{ for all } e \geq 1 \end{array}\right\} \quad \textit{if } p = \mathrm{char}(\mathbf{k}).$$

In particular, if $\mathrm{char}(\mathbf{k}) = p$ then either $E[p] \cong \mathbb{Z}/p\mathbb{Z}$, in which case E is called *ordinary*, or $E[p] = \{0\}$ and E is *supersingular*.

In this chapter we will also need to know a bit about singular Weierstrass equations. As already mentioned, the condition $\Delta = 0$ is equivalent to the condition that for some point P satisfying the Weierstrass polynomial (11), both partial derivatives vanish at P. The projective point $[0, 1, 0]$ is always nonsingular (this was an exercise), so any such P is affine. The coordinates of P lie in $\mathbf{k}$ (exercise),

so an admissible change of variable over $\mathbf{k}$ takes P to $(0,0)$. Then the conditions $E(0,0) = D_1E(0,0) = D_2E(0,0) = 0$ force the Weierstrass polynomial to be

$$E(x,y) = y^2 + a_1xy - x^3 - a_2x^2. \tag{14}$$

If $\mathrm{char}(\mathbf{k}) \neq 2$ then letting $\tilde{y} = y + a_1x/2$ in (14) simplifies this to

$$E(x,y) = \tilde{y}^2 - x^3 - a_2'x^2. \tag{15}$$

The point $P = (0,0)$ is the only singular point satisfying E. If $\mathrm{char}(\mathbf{k}) = 2$ then this is easy to verify from (14), while if $\mathrm{char}(\mathbf{k}) \neq 2$ then it follows from (15) (exercise).

Rewrite (14) as

$$E(x,y) = (y - m_1x)(y - m_2x) - x^3, \tag{16}$$

where m_1 and m_2 satisfy the quadratic polynomial $f(t) = t^2 + a_1t - a_2$ over $\mathbb{F}_p$ but need not lie in $\mathbb{F}_p$ themselves. The singular point P is called a *node* if $m_1 \neq m_2$, meaning that two distinct tangent lines pass through the curve at P, and it is called a *cusp* if $m_1 = m_2$, when there is only one tangent line. (See Figure 2.) Working from (14) and (16), it is easy to compute that $c_4 = (m_1 - m_2)^4$ (exercise), so that the curve has a node if $c_4 \neq 0$ and a cusp if $c_4 = 0$. These conditions apply to the Weierstrass equation in its original form since the admissible change of variable translating the singular point P to $(0,0)$ multiplies c_4 by a nonzero scalar, as in an exercise. In sum,

Proposition. *Let E be a Weierstrass equation over $\mathbf{k}$. Then*

- *E describes an elliptic curve $\iff$ $\Delta \neq 0$,*
- *E describes a curve with a node $\iff$ $\Delta = 0$ and $c_4 \neq 0$,*
- *E describes a curve with a cusp $\iff$ $\Delta = 0$ and $c_4 = 0$.*

In the case of a node the set of projective solutions of E other than the singular point forms a multiplicative group isomorphic to $\overline{\mathbf{k}}^*$, and in the case of a cusp the set forms an additive group isomorphic to $\overline{\mathbf{k}}$. (See Silverman's book for the proof of this.)

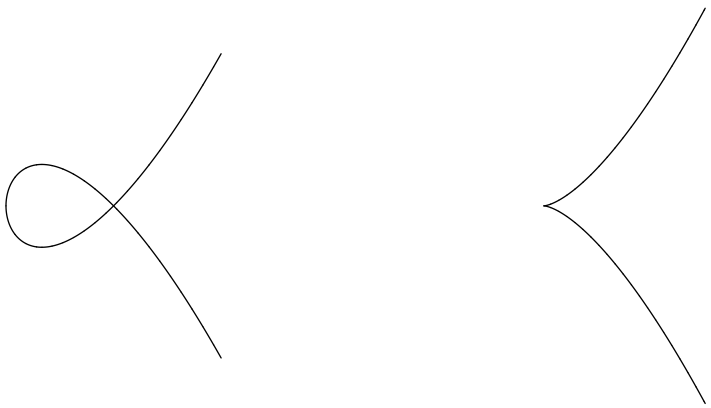

FIGURE 2. Node and cusp

Exercises

1. *(Suggestion: Don't do this problem by hand.)*
(a) *Confirm that* $4b_8 = b_2b_6 - b_4^2$ *and that* $1728\Delta = c_4^3 - c_6^2$. *Confirm that if* $\mathrm{char}(\mathbf{k}) \neq 2$ *then replacing* y *by* $y - (a_1x + a_3)/2$ *in* (6) *gives* (7). *Confirm that if* $\mathrm{char}(\mathbf{k}) \notin \{2, 3\}$ *then replacing* (x, y) *by* $((x - 3b_2)/36, y/216)$ *in* (7) *gives* (8).
(b) *Show that the admissible changes of variable* $x = u^2x' + r$, $y = u^3y' + su^2x' + t$ *where* $u, r, s, t \in \mathbf{k}$ *and* $u \neq 0$ *form a group. Show that every admissible change of variable transforms a Weierstrass equation* E *of the form* (6) *into another such equation* E' *with*

$$\begin{aligned}
ua_1' &= a_1 + 2s,\\
u^2a_2' &= a_2 - sa_1 + 3r - s^2,\\
u^3a_3' &= a_3 + ra_1 + 2t,\\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (rs + t)a_1 + 3r^2 - 2st,\\
u^6a_6' &= a_6 + ra_4 - ta_3 + r^2a_2 - rta_1 + r^3 - t^2,
\end{aligned}$$

and

$$\begin{aligned}
u^2b_2' &= b_2 + 12r,\\
u^4b_4' &= b_4 + rb_2 + 6r^2,\\
u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3,\\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4,
\end{aligned}$$

and

$$u^4c_4' = c_4, \qquad u^6c_6' = c_6,$$

and

$$u^{12}\Delta' = \Delta, \qquad j' = j.$$

(c) *Suppose the seemingly more general change of variable* $x = vx' + r$, $y = wy' + vsx' + t$, *where* $v, w, r, s, t \in \mathbf{k}$ *and* v, w *are nonzero, takes Weierstrass equations to Weierstrass equations. Show that* $v = u^2$ *and* $w = u^3$ *for some* $u \in \mathbf{k}$.
(d) *Replace* y *by* $y/2$ *in the third Weierstrass equation* (8) *to get*

$$y^2 = 4x^3 - g_2x - g_3, \quad g_2 = 108c_4,\ g_3 = 216c_6.$$

Show that the previously defined discriminant $\Delta_{\mathrm{old}} = g_2^3 - 27g_3^2$ *of this equation is equal to the discriminant* $\Delta_{(8)} = 2^63^9(c_4^3 - c_6^2)$ *of* (8) *in this section. Show that the previously defined invariant* $j = 1728g_2^3/\Delta_{\mathrm{old}}$ *is equal to the invariant* $j = c_4^3/\Delta$ *in this section.*
(e) *Find an admissible change of variable taking the modified universal elliptic curve* (9) *to the more general universal elliptic curve* (10). *Confirm that the discriminants and invariants of the two universal curves are as stated.*

2. *Show that algebraic and geometric nonsingularity are equivalent in characteristic 2.*

3. (a) *Homogenize the general Weierstrass polynomial by adding in powers of* z *to make each term cubic,*

$$E_{\mathrm{hom}}(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

Show that $[0,1,0]$ *satisfies* E_{hom} *and no other* $[x,y,0]$ *does.*
(b) *Dehomogenize* E_{hom} *by setting* $y=1$ *to obtain*

$$\tilde{E}(x,z) = z + a_1xz + a_3z^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

In the (x,z) *coordinate system, the infinite point* 0_E *is* $(0,0)$*. Working in this affine coordinate system, show that* E *is geometrically nonsingular at* 0_E*.*

4. (a) *Show that the casewise definitions of* λ *and* μ *make the line* $y=\lambda x+\mu$ *the secant line through* P *and* Q *when* $P\neq Q$ *and the tangent line to* E *through* P *when* $P=Q$*.*
(b) *Show that the geometric and algebraic descriptions* (12) *and* (13) *of the group law agree.*
(c) *Multiply the numerator and the denominator of the secant case* λ *by* $y_Q+y_P+a_1x_P+a_3$ *and use the Weierstrass equation* (6) *to obtain a new expression for* λ *when* $y_Q+y_P+a_1x_P+a_3\neq 0$*. Show that this also agrees with the old* λ *when* $x_P=x_Q$*, suitably giving* ∞ *when* $P=-Q$*. Similarly derive a new expression for* μ*.*

5. (a) *Let* P *be a singular point of a Weierstrass equation* E *over* $\mathbf{k}$*. Show that the coordinates of* P *lie in* $\mathbf{k}$*. For* $\mathrm{char}(\mathbf{k})=2$*, assume that every element of* $\mathbf{k}$ *is a square.*
(b) *Show that if* $\mathrm{char}(\mathbf{k})=2$ *then* $(0,0)$ *is the only singular point satisfying the Weierstrass polynomial* (14)*, and if* $\mathrm{char}(\mathbf{k})\neq 2$ *then* $(0,0)$ *is the only singular point satisfying the Weierstrass polynomial* (15)*.*
(c) *Show that* $c_4=(m_1-m_2)^4$ *in the context of equations* (14) *and* (16)*.*

6. (a) *For what values* $a,b\in\mathbb{Q}$ *do the Weierstrass equations*

$$y^2=x^3+ax^2+bx, \qquad y^2=x^3-2ax^2+(a^2-4b)x$$

both define elliptic curves E *and* E' *over* $\mathbb{Q}$*?*
(b) *For such values* a *and* b *show that the map*

$$(x,y)\mapsto (y^2/x^2, y(b-x^2)/x^2)$$

defines a map $\varphi: E\longrightarrow E'$ *taking* 0_E *to* $0_{E'}$*.*
(c) *Compute* $\ker(\varphi)$ *and compute* $\varphi^{-1}(0,0)$*.*
(d) *Find the dual isogeny* $\psi: E'\longrightarrow E$*, verifying the compositions* $\psi\circ\varphi=[2]_E$ *and* $\varphi\circ\psi=[2]_{E'}$*.*