The Geometry of Elliptic Curves

1 Projective space

Definition 1.1. Let K be a field and E_k a vector space over K. We denote the *projective space* $P(E_K)$ by

$$P(E_K) = (E - \{0\})/K^\times.$$

Suppose E finite dimension $n < \infty$. Then we have $E \simeq K^n$, which implies

$$P(E_K) \simeq (K^n - \{0\})/K^n.$$

We observe that two nonzero vectors $u, v \in K^n$ are equivalent, i.e. $u \sim v$, if there exists some $\lambda \in K^\times$ such that $u = \lambda v$. In other words, the points in $P(E_k)$ are given by equivalence classes

$$[u] = Ku = \{\lambda u : \lambda \in K^\times\}.$$

which are one dimensional subspaces spanned by the respective vectors u. We note also that $\dim P(E) = \dim(E_K) - 1$.

Example 1. The space $P(\mathbb{R}^2)$ is given by all the lines in $\mathbb{R}^2$, which can be identified with S^1. Observe here that we have the freedom to choose the point at infinity. Given a chart, we can carry out computations there.

This idea of projectivization will play an important role in the next section when we obtain a projective variety from an affine variety.

2 Varieties

Let K be an algebraically closed field. We have $A_K^n = K^n$.

Definition 2.1. We say that $S \subset A_K^n$ is an algebraic set if $S = V(I)$, where I is an ideal in $K[x_1, \ldots, x_n]$ and

$$V(I) = \{P \in A^n = K^n : \text{ for all } f \in I, f(P) = 0\}.$$

Definition 2.2. Given a set $S \subset A^n$, we can ask for the ideal that vanish on S and take

$$I(S) := \{f \in K[x_1, \ldots, x_n] : \text{ for all } s \in S, f(s) = 0\}.$$

We now have functions between the sets

$$\{\text{algebraic sets}\} \text{ and } \{\text{ideal of } K[x_1, \ldots, x_n]\}.$$

Definition 2.3. An affine algebraic set V is an affine variety if $I(V)$ is a prime ideal in $K[x_1, \ldots, x_n]$. In particular, we observe that the quotient ring

$$K[V] = K[x_1, \ldots, x_n]/I(V)$$

is an integral domain.

Definition 2.4. Let V be a variety. Then the dimension of V or $\dim V$ is the transcendence degree of $K(V)$, the field of fractions of $K[V]$, over K. Note that every nonzero element in $K[V]$ has an inverse in $K(V)$ because $K[V]$ is an integral domain.

Definition 2.5. Let V be a variety, $P \in V$, and $f_1, \ldots, f_m \in \overline{K}[X]$ a set of generators for $I(V)$. Then V is *nonsingular* (or *smooth*) at P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial X_j}(P) \right)_{1 \leq i \leq m, 1 \leq j \leq n}$$

has rank $n - \dim(V)$. If V is nonsingular at every point, then we say that V is nonsingular (or smooth).

Let V be given by a single nonconstant polynomial equation

$$f(X_1, \ldots, X_n) = 0.$$

Then $\dim(V) = n - 1$, so $P \in V$ is a singular point if and only if

$$\frac{\partial f}{\partial X_1}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0.$$

Since P also satisfies $f(P) = 0$, this gives $n + 1$ equations for the n coordinates of any singular point.

3 Topology on A^n

Definition 3.1. In the Zariski topology, we take the closed sets to be

$$\tau_{\text{Zariski}}(A^n) = \{\text{algebraic sets}\}.$$

We check easily that τ_{Zariski} contains $\emptyset = V(1)$ and $A^n = V(0)$. Moreover, τ_{Zariski} is stable under arbitrary intersections and finite unions.

Proof. Suppose $Y_1 = V(T_1)$ and $Y_2 = V(T_2)$. Then $Y_1 \cap Y_2 = V(T_1 T_2)$. If $Y_\alpha = V(T_\alpha)$ is any family of algebraic sets, then $\bigcap Y_\alpha = V(\bigcup T_\alpha)$. $\square$

Example 2. To illustrate the peculiarities of the Zariski topology, we consider the space of complex numbers $\mathbb{C}$. Since $\mathbb{C}$ is algebraically closed and any ideal $I \subset \mathbb{C}[x]$ is principal, we have

$$V(I) = V(\langle f \rangle) = \{z \in \mathbb{C} \mid f(z) = 0\}, \text{ which means } |V(I)| = \deg f.$$

Then a set in $\mathbb{C}$ is finite if and only if it is closed. In particular, this topology is not Hausdorff because any open set is infinite so given any $x_1 \neq x_2$, we must have

$$u(x_1) \cap u(x_2) \neq \emptyset.$$

In more intuitive terms, the open sets here are "too big" to separate points.

Definition 3.2. A nonempty subset Y of a topological subset$Y$ of a topological space X is *irreducible* if it cannot be expressed as the union $Y = Y_1 \cap Y_2$ of two proper subsets, each one of which is closed in Y. The empty set is not considered to be irreducible.

Example 3. Any nonempty open subset of an irreducible space is irreducible and dense.

Proof. Let $U \subset Y$ be a non-empty open subset. We check first that $\overline{U} = Y$, otherwise $Y = U^c \cup \overline{U}$, which gives a contradiction. Now assume by way of contradiction that $U = A \cup B$. Then $Y = \overline{U} = \overline{A} \cup \overline{B}$. If we take $Y = \overline{A}$ without loss of generality, we get that the closure of A in U is A. Then

$$A = \overline{A} \cap U = Y \cap U = U,$$

so U is also irreducible. □

Example 4. If Y is an irreducible subset of X, then its closure $\overline{Y}$ in X is also irreducible.

Proof. Assume by way of contradiction that Y is irreducible but $\overline{Y}$ is not. Then we can write $\overline{Y} = A \cup B$ for A, B proper, closed subsets. We get

$$Y = (A \cap Y) \cup (B \cap Y),$$

which are respectively closed in Y. □

We now describe some of the properties of the function which maps ideals to algebraic sets and the function which maps algebraic sets to ideals.

Theorem 3.3. *(Hilbert's Nullstellensatz) Let k be an algebraically closed field, let $\mathfrak{a}$ be an ideal in $A = k[x_1, \ldots, x_n]$, and let $f \in A$ be a polynomial which vanishes at all points of $V(\mathfrak{a})$. Then $f^r \in \mathfrak{a}$ for some integer $r > 0$.*

Proposition 3.4. *(a) If $T_1 \subset T_2$ are subsets of A, then $V(T_1) \supset V(T_2)$.*
(b) If $Y_1 \subset Y_2$ are subsets of $\mathbb{A}^n$, then $I(Y_1) \supset I(Y_2)$.
(c) For any two subsets Y_1, Y_2 of $\mathbb{A}^n$, we have $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.
(d) For any ideal $\mathfrak{a} \subset A, I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$, the radical of $\mathfrak{a}$.
(e) For any subset $Y \subset \mathbb{A}^n, V(I(Y)) = \overline{Y}$, the closure of Y.

Proof. (d) is a consequence of Hilbert's Nullstellensatz. To prove (e), we note that $Y \subset V(I(Y))$, which is a closed set, which implies $\overline{Y} \subset V(I(Y))$. Conversely, let W be any closed set containing Y. Then $W = V(\mathfrak{a})$ for some ideal $\mathfrak{a}$. So $V(\mathfrak{a}) \supset Y$ and by (b), $IV(\mathfrak{a}) \subset I(Y)$. But we must have $\mathfrak{a} \subset IV(\mathfrak{a})$, so by (a), we have $W = V(\mathfrak{a}) \supset VI(Y)$. Hence we conclude that $VI(Y) = \overline{Y}$. □

Corollary 3.5. *There is a one-to-one inclusion-reversing correspondence between algebraic sets in $\mathbb{A}^n$ and radical ideals, given by $Y \mapsto I(Y)$ and $\mapsto Z(\mathfrak{a})$. Furthermore, an algebraic set is irreducible if and only if its ideal is a prime ideal.*

Proof. If Y is irreducible, we show that $I(Y)$ is prime. Suppose that $fg \in I(Y)$, then $Y \subset V(fg) = V(f) \cup V(g)$. Thus $Y = (Y \cap V(f)) \cup (Y \cap V(g))$, both being closed subsets of Y. Since Y is irreducible, we have either $Y = Y \cap V(f)$, in which case $Y \subset V(f)$ or $Y \subset V(g)$. Hence either $f \in I(Y)$ or $g \in I(Y)$.

Conversely, let $\mathfrak{p}$ be a prime ideal, and suppose that $V(\mathfrak{p}) = Y_1 \cup Y_2$. Then $\mathfrak{p} = I(Y_1) \cap I(Y_2)$, so either $\mathfrak{p} = I(Y_1)$ or $\mathfrak{p} = I(Y_2)$. Thus $V(\mathfrak{p}) = Y_1$ or Y_2, which means it is irreducible. □

For any subset $V \subset A^n$, we can define a topology on V by taking the subspace topology, i.e. $U \subset V$ is open if and only if $U = K \cap V$ for some open K in A^n. We can thus extend the Zariski topology to the nth projective space

$$P^n_{K^n} = (K^{n+1} - \{0\})/K^\times.$$

However, we notice here that for an algebraic set

$$V(f) = \{P \in \mathbb{P}^n \mid f(P) = 0\},$$

to be well-defined, the function f must satisfy

$$f(x_0, x_1, \ldots, x_n) = 0 \iff f(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = 0.$$

Hence, we must impose the additional restriction that f is a homogeneous polynomial of degree n.

4 Weierstrass Equations

Definition 4.1. We define an elliptic curve in K by the following equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ where } a_i \in K. \tag{4.1}$$

This is a cubic equation, whose solutions lie in $\mathbb{A}^2 = K^2$.

Given a polynomial $f \in K[x, y]$, we can homogenize it by taking

$$z^3 f(\frac{x}{z}, \frac{y}{z}) = zy^2 + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

The solutions to this equation now lie in $\mathbb{P}^2$. Here $O = [0, 1, 0]$ is the base point.

If $\mathrm{char}(\overline{K}) \neq 2$, then we can simplify the equation by completing the square. The substitution

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6$. We also define the following quantities

$$\begin{aligned}
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\
c_4 &= b_2^2 - 24b_4, \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\
j &= c_4^3/\Delta, \\
\omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.
\end{aligned}$$

These satisfy the relations

$$4b_8 = b_2b_6 - b_4^2 \text{ and } 1728\Delta = c_4^3 - c_6^2.$$

If further $\mathrm{char}(\overline{K}) \neq 2, 3$, then the substitution

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right),$$

eliminates the x^2 term, yielding the simpler equation

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Definition 4.2. The quantity Δ is the *discriminant* of the Weierstrass equation, the quantity j is the j-invariant of the elliptic curve, and ω is the invariant differential associated to the Weierstrass equation.

Let $P = (x_0, y_0)$ be a singular point on the elliptic curve satisfying the Weierstrass equation. We have

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

It follows that there are $\alpha, \beta \in \overline{K}$ such that the Taylor series expansion of $f(x, y)$ at P has the form

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3.$$

Definition 4.3. The singular point P is a *node* if $\alpha \neq \beta$. In this case, the lines

$$y - y_0 = \alpha(x - x_0) \text{ and } y - y_0 = \beta(x - x_0)$$

are the *tangent lines* at P. Conversely, if $\alpha = \beta$, then we say that P is a *cusp*, in which case the *tangent line* at P is given by

$$y - y_0 = \alpha(x - x_0).$$

Here, we mention that the Weierstrass equation for an elliptic curve may not necessarily be unique. Assuming that the line at infinity, i.e. the line $Z = 0$ in $\mathbb{P}^2$ is required to intersect E only at the one point $[0, 1, 0]$. We will see that the only change of variables fixing $[0, 1, 0]$ and preserving the Weierstrass form of the equation

$$x = u^2x'r \text{ and } y = u^3y' + u^2sx' + t,$$

where $u, r, s, t \in \overline{K}$ and $u \neq 0$. The coefficients and associated quantities for the new equation are compiled in Table 3.1 of [3]. Here, we check that the j-invariant does not depend on the equation If the characteristic of K is not 2 or 3, our elliptic curve(s) have Weierstrass equation(s) of the form

$$E : y^2 = x^3 + Ax + B.$$

Associated to this equation are the quantities

$$\Delta = -16(4A^3 + 27B^2) \text{ and } j = -1728\frac{(4A)^3}{\Delta}.$$

The only change of variables preserving this form of the equation is

$$x = u^2x' \text{ and } y = u^3y' \text{ for some } u \in \overline{K}^*$$

with $u^4A' = A, u^6B' = B, u^{12}\Delta' = \Delta$.

Proposition 4.4. *(a) The curve given by a Weierstrass equation satisfies:*

(i) It is nonsingular if and only if $\Delta \neq 0$.

(ii) It has a node if and only if $\Delta = 0$ *and* $c_4 \neq 0$.

(iii) It has a cusp if and only if $\Delta = c_4 = 0$.

In cases (ii) and (iii), there is only the one singular point.

(b) Two elliptic curves are isomorphic over $\overline{K}$ *if and only if they both have the same* j*-invariant.*

(c) Let $j_0 \in \overline{K}$. *There exists an elliptic curve defined over* $K(j_0)$ *whose* j*-invariant is equal to* j_0.

Proof. (a) Let E be given by the Weierstrass equation

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Our first goal is to show that the point at infinity is never singular. When we look at the homogeneous equation

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$$

and at the point $O = [0, 1, 0]$. Since

$$\frac{\partial F}{\partial Z}(O) = 1 \neq 0,$$

we see that O is a nonsingular point of E.

Next suppose that E is singular, say at $P_0 = (x_0, y_0)$. The substitution

$$x = x' + x_0 \text{ and } y = y' + y_0$$

leave Δ and c_4 invariant, so we assume without loss of generality that E is singular at $(0, 0)$. Then

$$a_6 = f(0, 0) = 0, \quad a_4 = \frac{\partial f}{\partial x}(0, 0) = 0, \quad a_3 = \frac{\partial f}{\partial y}(0, 0) = 0,$$

so the equation for E takes the form

$$E : f(x, y) = y^2 + a_1xy - a_2x^2 - x^3 = 0.$$

This equation has the associated quantities

$$c_4 = (a_1^2 + 4a_2)^2 \text{ and } \Delta = 0.$$

By definition, E has a node (respectively cusp) at $(0, 0)$ if the quadratic form $y^2+a_1xy-a_2x^2$ has distinct (respectively equal) factors, which occurs if and only if the discriminant satisfies

$$a_1^2 + 4a_2 \neq \text{(respectively =) } 0.$$

To complete the proof of (i)-(iii), it remains to show that if E is nonsingular, then $\Delta \neq 0$. To simplify the computation, we assume that $\text{char}(K) \neq 2$ and consider a Weierstrass equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4 + b_6.$$

The curve E is singular if and only if there is a point $(x_0, y_0) \in E$ satisfying

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0.$$

In other words, the singular points are exactly the points of the form $(x_0, 0)$ such that x_0 is a double root of the cubic polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$. This polynomial has a double root if and only if its discriminant, which equals 16Δ, vanishes. This completes the proof of (i)-(iii). Further, since a cubic polynomial cannot have two double roots, E has at most one singular point.

(b) If two elliptic curves are isomorphic, then the transformation formulas show that they have the same j-invariant. For the converse, we will assume that $\mathrm{char}(K) \geq 5$. Let E and E' be elliptic curves with the same j-invariant, say with Weierstrass equations

$$E : y^2 = x^3 + Ax + B,$$
$$E' : y'^2 = x'^3 + A'x' + B'.$$

Then the assumption that $j(E) = j(E')$ means that

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2},$$

which yields $A^3B'^2 = A'^3B^2$. We look for an isomorphism of the form $(x, y) = (u^2x', u^3y')$ and consider three cases:

1. $A = 0 (j = 0)$. Then $B \neq 0$, since $\Delta \neq 0$ so $A' = 0$, and we obtain an isomorphism using $u = (B/B')^{1/6}$.
2. $B = 0 (j = 1728)$. Then $A \neq 0$, so $B' = 0$ and we take $u = (A/A')^{1/4}$.
3. $AB \neq 0 (j \neq 0, 1728)$. Then $A'B' \neq 0$, since if one of them were 0, then both of them would be 0, contradicting $\Delta' \neq 0$. Taking $u = (A/A')^{1/4} = (B/B')^{1/6}$ gives the desired isomorphism.

(c) Assume that $j_0 \neq 0, 1728$ and consider the curve

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

We then get

$$\Delta = \frac{j_0^3}{(j_0 - 1728)^3} \text{ and } j = j_0.$$

For the cases $j = 0, 1728$, we take

$$E : y^2 + y = x^3, \Delta = -27, \text{ and } E : y^2 = x^3 + x, \Delta = -64$$

respectively. $\square$

5 The Group Law

Let E be an elliptic curve given by a Weierstrass equation. Thus $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the Weierstrass equation, together with the point $O = [0, 1, 0]$ at infinity. Let $L \subset \mathbb{P}^2$ be a line. Then, since the equation has degree three, the line L intersects E at exactly three points, say P, Q, R. Bezout's theorem tells us that $L \cap E$ consists of exactly three points (taken with multiplicities).

We define a composition law $\oplus$ on E by the following rule:

Definition 5.1. (Composition Law) Let $P, Q \in E$, let L be a line through P and Q (if $P = Q$, let L be the tangent line to E at P) and let R be the third point of intersection of L with E. Let L' be the line through R and O. Then L' intersects E at $R, 0$, and a third point. We denote that third point by $P \oplus Q$.

Proposition 5.2. *The composition law has the following properties:*

(a) If a line L intersects E at the (not necessarily distinct) points P, Q, R, then

$$(P \oplus Q) \oplus R = O.$$

(b) $P \oplus O = P$ for all $P \in E$.

(c) $P \oplus Q = Q \oplus P$ for all $P, Q \in E$.

(d) Let $P \in E$. There is a point of E, denoted by $\ominus P$, satisfying

$$P \oplus (\ominus P) = O.$$

(e) Let $P, Q, R \in E$. Then

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

In other words, the composition law makes E into an abelian group with identity element O.

(f) Suppose that E is defined over K. Then

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \cup \{O\}$$

is a subgroup of E.

Proof. (a) follows from the Composition Law. (b) Taking $Q = O$, we see that the lines L and L' coincide. The former intersects E at P, O, R and the latter at $R, O, P \oplus O$ so $P \oplus O = P$. (c) The construction of $P \oplus Q$ is symmetric. (d) Let the line through P and Q also intersect E at R. Then using (a) and (b), we find that

$$O = (P \oplus O) \oplus R = P \oplus R.$$

(f) The third point of intersection has coordinates given by a rational combination of the coordinates of the coefficients of the line and of E. $\square$

To conclude, we derive the explicit formulas for the group operations on E. Let E be an elliptic curve given by a Weierstrass equation

$$F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

and let $P_0 = (x_0, y_0) \in E$. In order to calculate $\ominus P_0$, we take the line L through P_0 and O and find its third point of intersection with E. The line L is given by

$$L : x - x_0 = 0.$$

Substituting this into the equation for E, we see that the quadratic polynomial $F(x_0, y_0)$ has roots y_0 and y_0' where $-P = (x_0, y_0')$. Writing out

$$F(x_0, y) = c(y - y_0)(y - y_0')$$

and equating the coefficients of y^2 gives $c = 1$, and similarly equating the coefficients of y gives $y_0' = -y_0 - a_1x_0 - a_3$. This yields

$$-P_0 = -(x_0, y_0) = (x_0, -y_0, a_1x_0 - a_3).$$

Now let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points of E. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then we have already shown that $P_1 + P_2 = O$. Otherwise the line L through P_1 and P_2 has an equation of the form

$$L : y = \lambda x + \nu;$$

formulas for λ and ν are given below. Substituting the equation of L into the equation of E, we see that $F(x, \lambda x + \nu)$ has roots x_1, x_2, x_3, where $P_3 = (x_3, y_3)$ is the third point of $L \cap E$. We get $P_1 + P_2 + P_3 = O$. We write out

$$F(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3)$$

and equate coefficients. The coefficient of x^3 gives $c = -1$, and then the coefficient of x^2 yields

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2.$$

This gives a formula for x_3, and substituting into the equation of L gives the value of $y_3 = \lambda x_3 + \nu$. Finally, to find $P_1 + P_2 = -P_3$, we apply the negation formula to P_3. We summarize these steps with the following algorithm.

Theorem 5.3. *(Group Law Algorithm) Let E be an elliptic curve given by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

(a) Let $P_0 = (x_0, y_0)$. Then

$$-P_0 = (x_0, -y_0, -a_1x_0 - a_3).$$

(b) *Next let* $P_1 + P_2 = P_3$*. If* $x_1 = x_2$ *and* $y_1 + y_2 + a_1x_2 + a_3 = 0$*, then* $P_1 + P_2 = O$*. Otherwise, if* $x_1 = x_2$*, take*

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

Then $y = \lambda x + \nu$ *is the line through* P_1 *and* P_2*, or tangent to* E *if* $P_1 = P_2$*.*

(c) *With notation as in (b),* $P_3 = P_1 + P_2$ *has coordinates*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

(d) *As special cases of (c), we have for* $P_1 \neq \pm P_2$*,*

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2,$$

and the duplication formula for $P = (x, y) \in E$

$$x(P + P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

where b_2, b_4, b_6, b_8 *are the polynomials in the* a_i*'s.*

References

[1] Robin Hartshorne (1977) *Algebraic Geometry*, Springer Science+Business Media, Inc.

[2] Joseph H. Silverman, John T.Tate (2015) *Rational Points on Elliptic Curves*, Springer International Publishing Switzerland.

[3] Joseph H. Silverman (2009) *The Arithmetic of Elliptic Curves*, Springer Science+Business Media, Inc.