NOTES ON ELLIPTIC CURVES

DINO FESTI

Contents

Date: August 11, 2018.

1. Introduction: Solving equations

Solving equations or, more precisely, finding the zeros of a given equation has been one of the first reasons to study mathematics, since the ancient times. The branch of mathematics devoted to solving equations is called *Algebra*. We are going to see how elliptic curves represent a very natural and important step in the study of solutions of equations.

Since 19^{th} century it has been proved that *Geometry* is a very powerful tool in order to study Algebra. Elliptic curves offer a beautiful example of how different areas of math join together.

1.1. **Equation of degree one in one variable.** Let R be any ring, and let $R[x_1, ..., x_n]$ denote the polynomial ring with n variables over R. Let $f(x_1, ..., x_n)$ be an element of $R[x_1, ..., x_n]$ and let K be a field containing R.

Solving $f = 0$ over K or, more precisely, finding the roots of f in K means finding the n-tuples $(a_1, ..., a_n) \in K^n$ such that

$$f(a_1, ..., a_n) = 0.$$

Remark 1.1. In this section we will only consider $R = \mathbb{Z}$ or $\mathbb{Q}$, and $K = \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$. For elliptic curves over finite fields see Section 6.

The easiest, and best known, case of an equation is given by

$$ax + b = 0, \tag{1}$$

with $a, b \in R$, $a \neq 0$ and x the variable; that is, an *equation of degree one in one variable*. We all know the following result.

Proposition 1.2. *Let K be a field containing R. The equation* (1) *has always exactly one solution in K, namely $x = -b/a$.*

1.2. **Equations of higher degree in one variable.** There are two natural ways to generalise (1): considering equations of higher degree, or considering equations with more coefficients.

Taking a more classically algebraic approach, the next step is to consider equations of degree 2 over $R = \mathbb{Q}$:

$$ax^2 + bx + c = 0, \tag{2}$$

with $a, b, c \in \mathbb{Q}$ and $a \neq 0$. We have seen that the quantities

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

are (the) two solutions, counted with multiplicity, of (2) over $\mathbb{C}$. Notice though that $x_{1,2}$ do not need to be defined over $\mathbb{Q}$ or even $\mathbb{R}$.

Proposition 1.3. *The following statements hold.*

(a) If $K = \mathbb{C}$, then the equation (2) *has two solutions, counted with multiplicity, in K.*

(b) If $K = \mathbb{R}$, then the equation (2) *has two solutions, counted with multiplicity, in K if and only if $b^2 - 4ac \geq 0$. Otherwise it has no solutions in K.*

(c) If $K = \mathbb{Q}$, then the equation (2) has two solutions, counted with multiplicity, in K if and only if $b^2 - 4ac \in \mathbb{Q}^2$. Otherwise it has no solutions in K.

Remark 1.4. Notice that when (2) has solutions over K, then they are x_1 and x_2.

For the case of equations of degree $d \geq 3$ over $\mathbb{Q}$ we have similar statements. For these notes it will be enough to explicitly state only the case $d = 3$:

$$ax^3 + bx^2 + cx + d = 0. \tag{3}$$

with $a, b, c, d \in \mathbb{Q}$ and $a \neq 0$.

Proposition 1.5. *The following statements hold.*

(a) If $K = \mathbb{C}$, then the equation (3) has three solutions, counted with multiplicity, in K.

(b) If $K = \mathbb{R}$, then the equation (3) has either one or three solutions, counted with multiplicity, in K.

(c) If $K = \mathbb{Q}$, then the equation (3) has either three, one, or no solutions, counted with multiplicity, in K.

Remark 1.6. Note that also in this case it would be possible to write explicit an condition on the coefficients of (3) in order to determine whether we have one, three or no solutions over K. This condition is called the *discriminant* of the polynomial. In Definition 2.11 we explicitly write it down for the case with $a = 1$ and $b = 0$.

An analogous quantity can be defined for $d = 4$.

For $d \geq 5$ we do not have explicit conditions on the coefficients to determine the number of solutions on $K = \mathbb{R}, \mathbb{Q}$ (recall that an equation of degree d has always d solutions in $\mathbb{C}$, if counted with multiplicity). What we can say is that if d is odd, then there is at least one real solution. There is an algorithm to find all the solutions over $\mathbb{Q}$.

So the situation for equations of degree d in one variable over $\mathbb{Q}$, namely equations of the form

$$\sum_{i=0}^{d} a_i x^i = 0, \tag{4}$$

with $a_i \in \mathbb{Q}$ and $a_d \neq 0$, is quite clear.

Theorem 1.7. *Let $K = \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$. The equation (4) has finitely many solutions in K. If $K = \mathbb{C}$ then it has exactly d solutions, if counted with multiplicity. If $K = \mathbb{Q}$, there is an algorithm to determine whether (4) has solutions in K and, in case it does, to find all of them.*

1.3. **Equations of degree one in more variables.** In the previous subsection we have seen what happen if consider equations over $\mathbb{Q}$ of higher degree but in only one variable. In this section we are going to study the solutions of equations of degree one but allowing more variables. We start with an example.

Example 1.8. Consider the equation

$$ax + by + c = 0, \tag{5}$$

with $a, b, c \in \mathbb{Q}$ and $a, b \neq 0$. Take $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ and let $x = x_0 \in K$ be fixed. Then the pair $(x_0, \frac{-c-ax_0}{b}) \in K \times K$ is a solution over K of (5). So for every fixed value of x we have a value of y that gives us a solution of the equation. We say that the solutions are parametrised by $K = \mathbb{A}^1_K$.

Example 1.8 can be easily extended to the general case:

$$a_0 + \sum_{i=1}^{n} a_i x_i = 0, \tag{6}$$

with $a_i \in \mathbb{Q}$ for $i = 0, 1, ..., n$ and $a_i \neq 0$ for $i = 1, ..., n$. In this case, if we fix the value of the first $n-1$ variables we always get exactly one value of the last variable satisfying the equation.

Theorem 1.9. *The solutions of* (6) *over* K *are parametrised by* $K^{\times n-1} = \mathbb{A}_K^{n-1}$.

Proof. All the solutions are of the form

$$\left(x_1, ..., x_{n-1}, \frac{-a_0 - a_1 x_1 - ... - a_{n-1} x_{n-1}}{a_n} \right) \in \mathbb{A}_K^n,$$

with $(x_1, ..., x_{n-1}) \in \mathbb{A}_K^{n-1}$. □

Remark 1.10. Notice that in this case the number of solutions does not depend on the field K.

1.4. **Equations of degree two in two variables: plane conics.** So far we have kept either the degree or the number of variables equal to one. What happens if we let both grow? The first case is then given by equations of degree two in two variables:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{7}$$

with $a, ..., f \in \mathbb{Q}$ and $(a, b, c) \neq (0, 0, 0)$. We will see in the next example how this problem, that looks purely algebraic, can be solved by using geometric tools. The theory of the conics it is very beautiful and rich. Here we will only give a quick survey about the rational points of conics.

Example 1.11. Consider the following equation over $\mathbb{Q}$:

$$f(x, y) := x^2 + y^2 - 1 = 0. \tag{8}$$

Our goal is to determine how many solutions does (8) have and, possibly, write them all.

Notice that equation $f(x, y) = 0$ define the unit circle C in $\mathbb{A}^2$, and that $P = (-1, 0)$ is a point on it, that is, $f(-1, 0) = 0$. Yet in other words, $(-1, 0)$ is a solution for (8). We call the solution of f *the* K*-rational points of* C; we denote the set of solutions of (8) in K by $C(K)$, *the set of* K*-rational points* of C.

Let ℓ be a curve *defined* over K passing through the point P, that is, ℓ is defined by the equation $y = m(x + 1)$, with $m \in K$. Finding the intersection $C \cap \ell$ implies solving an equation of degree two in one variable, by substituting y in the equation of C:

$$\begin{aligned} 0 &= x^2 + (m(x+1))^2 - 1 = \\ &= (1 + m^2)x^2 + 2m^2 x + x^2 - 1. \end{aligned}$$

The solutions to the above equations are -1 (which we already knew) and $x = \frac{1-m^2}{1+m^2}$. This implies $\ell \cap C = \{P, (\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2})\}$. Notice that as $m \in K$, then $(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}) \in K \times K$. Since this construction holds for any $m \in K$, we have

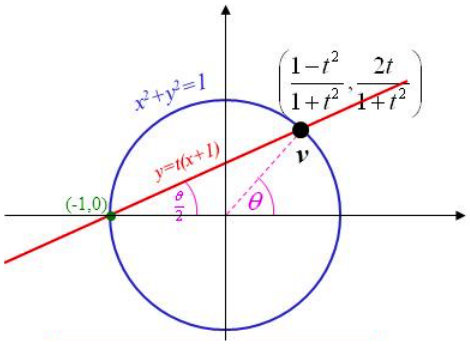
$$\{(-1, 0)\} \cup \{(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2}) \mid m \in K \} \subseteq C(K).$$

Does the equality hold? Assume $Q = (x_0, y_0) \in C(K)$ and consider the line ℓ passing through Q and P, that is,

$$\ell\colon y = m(x+1),$$

with $m = \frac{y_0}{x_0+1} \in K$. Hence it follows that $Q \in \{(-1,0)\} \cup \{(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}) \mid m \in K\}$, proving the equality.

So we have seen that (8) has infinitely many solutions over K, and that they are parametrised by $\mathbb{A}^1$ plus a point.



The argument used in Example 1.11 can be generalised to any equation $f(x,y) = 0$ defining a *smooth conic* (cf. Definition 1.12).

Definition 1.12. Let C be the curve in $\mathbb{A}^2$ defined by the equation $f(x,y) = 0$. The curve C is called a *conic* if f has degree two. Let $P = (u,v)$ be a K-point of C, that is, $u, v \in K$ and $f(u,v) = 0$. We say that P is a *singular point* of C if

$$\frac{\partial f}{\partial x}(u,v) = \frac{\partial f}{\partial y}(u,v) = 0.$$

We say that C is *singular* if it admits singular points. We say that C is *smooth* if it is not singular.

Theorem 1.13. *Let $f(x,y) = 0$ be an equation of degree two in two variable defining a smooth conic C in $\mathbb{A}^2_K$. One of the two following statements holds:*

(a) f admits no solutions;
(b) the solutions of f are parametrised by $\mathbb{A}^1_K$ plus a point.

Proof. If f admits no solution then we are done. If it does admit one solution, it means that $C(K)$ contains at least one point, say P. Consider the lines defined over K passing through P. By Proposition 1.3 we know that each such line intersects in two points, one of them being P and as P is defined over K, so is also the other one. □

Corollary 1.14. *The points of any smooth conic over $\mathbb{C}$ are parametrised by $\mathbb{A}^1_{\mathbb{C}}$ plus a point.*

1.5. **Exercises.** The exercises marked with * are harder; those marked with ! are important.

1.1 A triple (A, B, C) of positive integer numbers is called *pythagorean* if $A^2+B^2 = C^2$. A pythagorean triple is called *primitive* if $\gcd(A, B, C) = 1$. Describe all the primitive pythagorean triples. [Hint: use Example 1.11.]

1.2 Describe all the $\mathbb{Q}$-rational points of the hyperbole $x^2 - y^2 = 1$.

1.3 Give an example of a smooth conic over $\mathbb{Q}$ and $\mathbb{R}$ not admitting rational points.

1.4 Give an example of a conic with only finitely many K-rational points, for $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. [Hint: for $K = \mathbb{C}$, it must necessarily be singular.]

1.5 ! Recall (or read) the definitions of $\mathbb{P}^1$ and $\mathbb{P}^2$.

2. Cubic curves and Weierstrass form

After giving a complete answer for the solution of quadratic equations in two variables, we proceed by studying equations of degree three in two variables. In this section, we will assume $K = \mathbb{Q}$, but all the statements holds (sometimes trivially) also for $\mathbb{R}$ and $\mathbb{C}$.

Definition 2.1. A cubic curve C over K is the curve defined by a polynomial

$$f(x, y) = \sum a_{ij} x^i y^j,$$

where the sum ranges over all the $0 \leq i, j \leq 3$ such that $i + j \leq 3$, $a_{ij} \in K$ for every i, j and the polynomial has actual degree 3.

Remark 2.2. The curve C is a curve inside the affine plane $\mathbb{A}^2_K$. Let $\mathbb{P}^2$ be the projective plane with coordinates X, Y, Z such that $X/Z = x$ and $Y/Z = y$. The projective closure of C inside $\mathbb{P}^2_K$ is the projective curve $\bar{C}$ defined by the equation

$$\sum a_{ijk} X^i Y^j Z^k,$$

where the sum ranges over all the non-negative integers i, j, k such that $i+j+k = 3$.

As in Definition 1.12, we define a singular point of C to be a point where both partial derivatives vanish; a smooth cubic is a conic with no singular points.

2.1. Weierstrass form.

Definition 2.3. We say that a cubic is in (short) *Weierstrass form* if it is defined by an equation of the form

$$y^2 = x^3 + ax + b.$$

Proposition 2.4. *Let C be a smooth projective cubic over K with a K-rational point. Then C can be put into Weierstrass form using K-rational maps.*

Proof. This proof follows [1, I.3]. Let $\bar{C}$ denote the projective closure of C inside $\mathbb{P}^2(X, Y, Z)$. Then $\bar{C}$ is defined by the homogeneous degree three polynomial

$$f_0 := a_0X^3+a_1X^2Y+a_2X^2Z+a_3XY^2+a_4XYZ+a_5XZ^2+a_6Y^3+a_7Y^2Z+a_8YZ^2+a_9Z^3.$$

By assumption $\bar{C}$ has a rational point, say $(x_0 : y_0 : z_0)$; without loss of generality we assume $x_0 \neq 1$. Applying the transformation

$$t_1 : \begin{cases} X' &= X \\ Y' &= x_0Y - y_0X \\ Z' &= x_0Z - z_0X \end{cases}$$

we move the point $(x_0 : y_0 : z_0)$ to $(1 : 0 : 0)$ and $\bar{C}$ transforms into the curve C_1 defined by

$$f_1 := b_1X^2Y + b_2X^2Z + b_3XY^2 + b_4XYZ + b_5XZ^2 + b_6Y^3 + b_7Y^2Z + b_8YZ^2 + b_9Z^3.$$

Notice that the coefficient of X^3 is zero as $(1 : 0 : 0)$ is on C_1.

Let $L_{\mathcal{O}}$ be the tangent curve of C_1 at $\mathcal{O}$: it is defined by the equation $b_2Z + b_1Y = 0$. By applying the transformation

$$t_2 : \begin{cases} X' &= X \\ Y' &= Y/b_2 \\ Z' &= Z/b_1 + b_1Y/b_2 \end{cases}$$

we fix the point $\mathcal{O}$, we move $L_{\mathcal{O}}$ to the line $Z = 0$ and C_1 gets mapped to the curve C_2 defined by

$$f_2 := c_2X^2Z + c_3XY^2 + c_4XYZ + c_5XZ^2 + c_6Y^3 + c_7Y^2Z + c_8YZ^2 + c_9Z^3.$$

Notice that the coefficient of X^2Y is zero since $Z = 0$ is the tangent line of C_2 at $(1 : 0 : 0)$.

Let P be the third point of intersection of $L_{\mathcal{O}} = \{Z = 0\}$ and C_2, that is, $P = (c_6 : c_3 : 0)$. Then the transformation

$$t_3 : \begin{cases} X' &= c_3X - c_6Y \\ Y' &= Y \\ Z' &= Z \end{cases}$$

moves P to the point $(0 : 1 : 0)$ and keeps the point $\mathcal{O} = (1 : 0 : 0)$ and the line $\{Z = 0\}$ fixed; it sends C_2 to the curve C_3 defined by

$$f_3 := d_2X^2Z + d_3XY^2 + d_4XYZ + d_5XZ^2 + d_7Y^2Z + d_8YZ^2 + d_9Z^3.$$

Notice that the coefficient of Y^3 is zero since $(0 : 1 : 0)$ is a point on the curve.

As before, we consider the tangent line L_P to C_3 at $(0 : 1 : 0)$: it is defined by the equation $d_3Z + d_7X = 0$. Then the transformation

$$t_4 : \begin{cases} X' &= d_7X + d_3Z \\ Y' &= Y \\ Z' &= Z \end{cases}$$

fixes $\mathcal{O} = (1 : 0 : 0), P = (0 : 1 : 0)$ and the line $\{Z = 0\}$; it sends the line L_P to $\{X = 0\}$ and the curve C_3 to the curve C_4 defined by

$$f_4 := e_2X^2Z + e_3XY^2 + e_4XYZ + e_5XZ^2 + e_8YZ^2 + e_9Z^3.$$

Notice that the coefficient of Y^2Z is zero since $X = 0$ is the tangent line to C_4 at $(0 : 1 : 0)$.

We consider the affine part of C_4 given by $C_4 \cap \{Z \neq 0\}$; for sake of simplicity we will denote it again by C_4. If we take $x = X/Z, y = Y/Z$ to be the affine coordinates of $\mathbb{A}^2 = \{Z \neq 0\}$, we can write C_4 as the curve defined by the equation

$$xy^2 + (\alpha_0x + \alpha_1)y = \alpha_2x^2 + \alpha_3x + \alpha_4.$$

We can multiply both sides by x obtaining the curve

$$C_5 \colon (xy)^2 + (\alpha_0x + \alpha_1)xy = \alpha_2x^3 + \alpha_3x^2 + \alpha_4x.$$

By applying the transformation

$$t_5 : \begin{cases} x' &= x \\ y' &= xy \end{cases}$$

we send C_5 to the curve

$$C_5 \colon y^2 + (\alpha_0 x + \alpha_1)y = \alpha_2 x^3 + \alpha_3 x^2 + \alpha_4 x.$$

Using the transformation

$$t_6 : \begin{cases} x' &= x \\ y' &= y + (\alpha_0 x + \alpha_1)/2 \end{cases}$$

we transform C_5 into the curve

$$C_6 \colon y^2 = \beta_0 x^3 + \beta_1 x^2 + \beta_2 x + \beta_3.$$

Finally, via the transformation

$$t_7 : \begin{cases} x' &= x + \beta_1/3 \\ y' &= y \end{cases}$$

we send C_6 to the curve

$$C_7 \colon y^2 = x^3 + ax + b.$$

□

Remark 2.5. When we say that the curve C 'can be put into Weierstrass form' we more precisely mean that there is a rational map over $\mathbb{Q}$ from C to a curve defined by an equation in Weierstrass form. One can easily see that all the transformation $t_i, i = 1, ..., 7$, are rational transformation of $\mathbb{P}^2$ defined over $\mathbb{Q}$. In fact all of them except t_5 are automorphisms of $\mathbb{P}^2$.

The map t_5 is a *rational* map, i.e., it is not defined on the whole $\mathbb{P}^2$, but on an open subset of it. In fact, it is defined everywhere except at $(1 : 0 : 0)$ and $(0 : 1 : 0)$. This is not too much of a problem as the point $(0 : 1 : 0)$ is on the curve C_6 but not in the image of t_5. This means that passing from the original cubic to the one in Weierstrass form we only lose one solution, the one we already knew from the beginning and started with.

Remark 2.6. The argument in the proof works in every characteristic until t_5. To apply t_6 one has to assume that the characteristic of K is not 2; in addition, to apply t_7 one has to assume that the characteristic of K is not 3 either. This means that for a generic field K, of arbitrary characteristic we can only say that every elliptic curve can be put in the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

This form is also called Weierstrass form, as opposed to the short Weierstrass form defined in 2.3

Remark 2.7. In the proof we tacitly assumed some coefficients to be nonzero. This can be done as if this were the case, putting the cubic in the desired form would actually be easier, even though the transformations used would be slightly different. Analogously, we assumed $\mathcal{O}$ not to be a flex point. If it were, we could

have assumed that $\mathcal{O} = (0 : 1 : 0)$ with tangent line $Z = 0$. This implies that we can write the equation of C as

$$\alpha_0 y^2 + (\alpha_1 x + \alpha_2)y = \alpha_3 x^3 + \alpha_4 x^2 + \alpha_5 x + \alpha_6.$$

From here one can use transformations t_6 and t_7 as in the proof of Proposition 2.4 to obtain the short Weierstrass form.

2.2. **First definition of elliptic curves.**

Definition 2.8. An elliptic curve is a pair (C, P) where C is a smooth projective cubic and P is a point on it.

Corollary 2.9. *Every elliptic curve can be put in Weierstrass form.*

Proof. Immediate from Proposition 2.4. □

Remark 2.10. The (short) Weierstrass form is not the only useful and classical form to write the equation of an elliptic curves. Other classical forms to write an elliptic curve E are the following:

$$E\colon y^2 = x(x-1)(x-\lambda) \quad \text{(Legendre form)}, \tag{9}$$

for some $\lambda \in \mathbb{R} - \{0, 1\}$;

$$E\colon y^2 = (1-x^2)(1-k^2x^2) \quad \text{(Jacobi form)}, \tag{10}$$

for some $k \in \mathbb{C} - \{0, \pm 1\}$;

Definition 2.11. Let C be the curve defined by the equation

$$y^2 = x^3 + ax + b.$$

We define the *discriminant* of C to be

$$\Delta = \Delta(C) = -16(4a^3 + 27b^2).$$

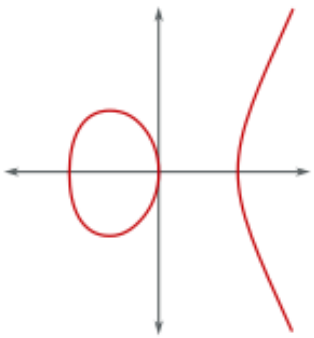


Figure 1. An elliptic curve with $\Delta > 0$.

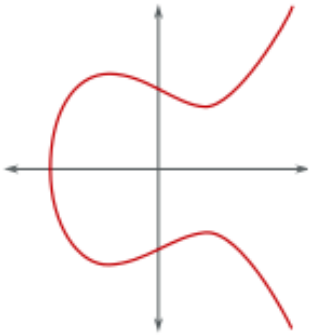


Figure 2. An elliptic curve with $\Delta < 0$

Lemma 2.12. *Let C be the curve the curve defined by the equation*

$$y^2 = x^3 + ax + b.$$

Then $(\bar{C}, (0 : 1 : 0))$ is an elliptic curve if and only if $\Delta(C) \neq 0$.

Proof. Notice that if C is defined as in the hypothesis, then $\bar{C}$ always has at least one point, namely $(0:1:0)$. So to prove the statement it is enough to prove that C is smooth if and only if $\Delta \neq 0$.

Let $f(x)$ be the polynomial $x^3 + ax + b$, and notice that the discriminant of f is exactly Δ.

By studying the partial derivatives of the equation defining C, one can see that C has a singular point if and only if f admits a double root, that is, if and only $\Delta = 0$. □

Remark 2.13. Notice that if the cubic C is singular, then its rational points can be studied by projecting from a (the) singular point, using the same argument as in the case for conics. (cf. Exercises 2.4).

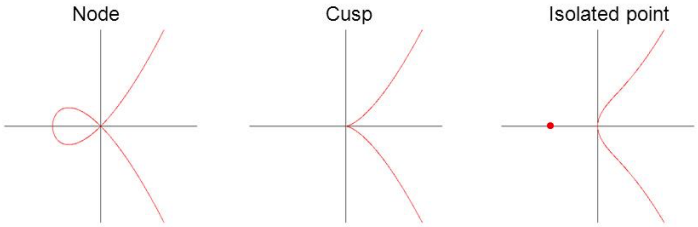


Figure 3. The three possible types of singular cubics.

2.3. **The j-invariant.** In Subsection 2.2 we have seen that every elliptic curve can be put into Weierstrass form. Is this form unique?
This question can be phrased in a different way: what are the isomorphism of affine curves that preserve the Weierstrass form?

Lemma 2.14. *The only change of variables preserving the short Weierstrass form is*

$$t_u : \begin{cases} x &= u^2 x' \\ y &= u^3 y' \end{cases}$$

for some $u \in K^*$.

Proof. The generic change of variables can be written as

$$t : \begin{cases} x &= \alpha_1 x' + \alpha_2 y' + \alpha_3 \\ y &= \beta_1 x' + \beta_2 y' + \beta_3 \end{cases}$$

Substituting these expression x and y into the short Weierstrass form and imposing the conditions on the coefficient in order to obtain again a short Weierstrass form, we get that t must be of the form

$$t : \begin{cases} x &= \alpha_1 x' \\ y &= \beta_2 y' \end{cases}$$

with $\alpha_1^3 = \beta_2^2$. From this it follows that $(\alpha_1, \beta_2) = (u^2, u^3)$ for some $u \in K^*$. □

Definition 2.15. In what follows, we say that two elliptic curves E and E' given in short Weierstrass form are *form* if there is a change of variables (as in Lemma 2.14) sending one to the other.

Remark 2.16. Consider $u \in K^*$ and apply the transformation t_u to the curve C with equation $y^2 = x^3 + ax + b$. We get the curve C' with equation $y^2 = x^3 + a'x + b'$ with $a' = a/u^4$ and $b' = b/u^6$. From this it also follows that $\Delta(C') = \Delta(C)/u^{12}$. Can we define a quantity associated to C that is invariant under this kind of transformation?

Definition 2.17. Let E be the elliptic curve defined by $y^2 = x^3 + ax + b$. We define the j-invariant of E to the quantity

$$j(E) := -1728\frac{(4a)^3}{\Delta(E)} = 1728\frac{4a^3}{4a^3 + 27b^2}. \tag{11}$$

Proposition 2.18. *Let K be any field and fix an algebraic closure $\bar{K}$ of K. The following statements hold.*

(a) Two elliptic curves over K are isomorphic (over $\bar{K}$) if and only if they have the same j-invariant.
(b) Let $j_0 \in \bar{K}^*$. Then there exists an elliptic curve E, defined over $K(j_0)$, such that $j(E) = j_0$.

Proof. (a) By Lemma 2.14, Remark 2.16 and the definition of the j-invariant one can immediately see that if two elliptic curves are isomorphic then they have the same j-invariant.

Conversely, assume that $C\colon y^2 = x^3 + ax + b$ and $C'\colon y'^2 = x'^3 + ax' + b$ are two elliptic with the same j-invariant, that is

$$1728\frac{4a^3}{4a^3 + 27b^2} = 1728\frac{4a'^3}{4a'^3 + 27b'^2}.$$

The equality above yields $a^3b'^2 = a'^3b^2$. Recall that our goal is to find a $u \in \bar{K}$ such that t_u sends C to C'. We have three cases.

I. $a = 0$. It follows that: $a' = 0$, as C and C' have the same j-invariant; $b \neq 0$, as C is an elliptic curve and so $\Delta(C) \neq 0$; $b' \neq 0$, for the same reason. Then consider $u = (b/b')^{1/6} \in \bar{K}^*$.
II. $b = 0$. It follows that: $j(C') = j(C) = 1728$; $b' = 0$; $a \neq 0$ and $a' \neq 0$. Then consider $u = (a/a')^{1/4}$.
III. $ab \neq 0$. It follows that $a'b' \neq 0$. Then consider $u = (b/b')^{1/6} = (a/a')^{1/4}$.

(b) Exercise.

□

2.4. **Exercises.** The exercises marked with * are harder; those marked with ! are important.

2.1 ! Find all the $\mathbb{Q}$-rational points of the singular cubic $y^2 = x^3$.
2.2 ! Prove Proposition 2.18.ii) . [Extra*: For every fixed j_0, how many different, yet isomorphic, elliptic curves in Weierstrass form with j invariant equal to j_0 are there?]
2.3 Put the Fermat cubic $u^3 + v^3 = 1$ in Weierstrass form.
2.4 * Find a rational solution of the following equation:

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4.$$

2.5 Write an explicit example for each type of singular curve in Figure 3.

3. Rational points of an elliptic curve

In Section 2 we have seen that every elliptic curve can be put into Weierstrass form. Having an elliptic curve written in Weierstrass form helps considerably the study of rational points.

3.1. **The group law.** In Definition 2.8 we have defined an elliptic curve to be a smooth cubic C together with a point $P \in C$. From now on, if the curve C is a smooth curve defined by an equation in the Weierstrass form, then we will assume that the rational point is always the point $\mathcal{O} = (0 : 1 : 0)$.

Definition 3.1. Recall that $\bar{C}(K)$ is the set of K-rational points of $\bar{C}$. It is possible to define an operation on this set. Let $P, Q \in \bar{C}(K)$, and let L the line passing through P, Q. Let $P * Q$ be the third point of intersection of L and $\bar{C}$. Let L' be the line passing through $P * Q$ and $\mathcal{O}$. We define $P + Q$ to be the the third point of intersection of L' and $\bar{C}$.

Remark 3.2. Notice that Definition 3.1 makes sense also if C is not given in Weierstrass form.

Remark 3.3. Given the genuinely geometric nature of Definition 3.1, we naturally have that the sum $P + P =: 2P$ is obtained by considering the tangent line to C at P.

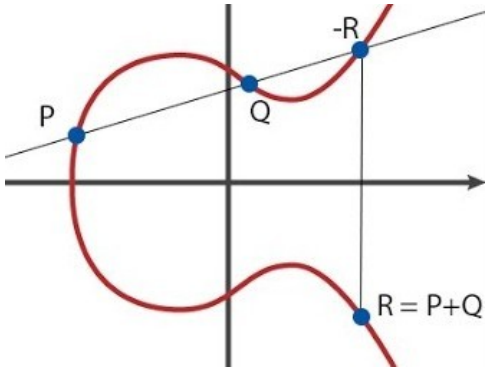


Figure 4. Geometric construction of the sum of two points.

Proposition 3.4. *The following statements hold:*

(a) the addition $+$ on $\bar{C}(K)$ is well defined;
(b) the addition $+$ is associative and commutative;
(c) $\mathcal{O}$ is the neutral element for $+$;
(d) for every P the element $-P$ exists.
(e) $P + Q + R = \mathcal{O}$ if and only if P, Q, R lie on a line.

Proof. (a) In order to prove that the operation is well defined, it is enough to show that $P + Q \in \bar{C}(K)$. By Proposition 1.5 we have that as P and Q are defined over K, so is $P * Q$. The same argument shows that also $P + R$ is defined over K.

(b) Exercise. Note that commutativity is almost trivial; associativity is the hard part.

(c) Let L the line passing through P and $\mathcal{O}$. Then $L \cap \bar{C} = \{P, \mathcal{O}, Q\}$, from which it follows that $P + \mathcal{O} = P$.

(d) Exercise.
(e) Exercise.

□

Corollary 3.5. $(\bar{C}, +)$ *is an abelian group.*

Proof. Immediate from Proposition 3.4.ii)–iv). □

Remark 3.2 tells us that the sum of two points can be defined on any elliptic curve, independently of the Weierstrass form. Nevertheless, if the elliptic curve is given in Weierstrass form, then it is much easier to explicitly write the coordinates of $P+Q$ in terms of the coordinates of P and Q.

Proposition 3.6. *Let C be the elliptic curve in Weierstrass form $y^2 = x^3 + ax + b$; let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two elements of $C(K)$. Then*

$$P + Q := (x_3, y_3) = (\lambda^2 - x_1 - x_2, -\lambda(x_2 - x_1) - y_1), \tag{12}$$

where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$;

$$-P = (x_1, -y_1). \tag{13}$$

Proof. The line$L$ passing through P and Q has equation $y - y_1 = \lambda(x - x_1)$. We can then substitute y in the equation of C, getting a cubic monic polynomial $f(x)$. Doing the computations, one can check that the coefficient of x^2 is $-\lambda^2$. Since the coefficient of x^2 equals minus the sum of the roots of a cubic monic polynomial, and we already know that x_1 and x_2 are roots of f, we have that the third root, x_3 is $\lambda^2 - x_1 - x_2$. The value of y_3 follows by simply plugging the value x_3 in the equation of L. □

Remark 3.7. One can use Proposition 3.6 to prove 3.4.

Remark 3.8. One can also find explicit formula to express the coordinates of $2P$ (cf. Remark 3.3).

We have seen that if E is an elliptic curve over $K = \mathbb{Q}$, the set of rational points $E(\mathbb{Q})$ can be endowed with a group structure. The natural question is then: how does this group look like?

3.2. **Group structures theorems over $\mathbb{Q}$.** Let C be an elliptic curve over a field K, and let $+$ the addition on $C(K)$ be defined as in 3.1 From Corollary 3.5 we know that $(\bar{C}(K), +)$ is an abelian group. This extra structure can help us in the study of the rational points of C.
A first difference among elements of a group comes from the distinction between elements of finite order and elements of infinite order. In an abelian group, the set of elements of finite order form a subgroup.

Definition 3.9. We denote by $E(\mathbb{Q})_{tors}$ the subgroup $E(\mathbb{Q})$ formed by torsion elements:

$$E(\mathbb{Q})_{tors} := \{P \in E(\mathbb{Q}) \mid \exists m \in \mathbb{Z} : mP = \mathcal{O}\}.$$

An element of $E(\mathbb{Q})_{tors}$ is called a *(rational) torsion* point of E.

We have several tools to study the torsion points of an elliptic curve. Below we state some very useful ones.

Theorem 3.10 (Nagell–Lutz)**.** *Let $E/\mathbb{Q}$ be the elliptic curve with equation*

$$y^2 = x^3 + ax + b,$$

with $a, b \in \mathbb{Z}$. Suppose $P = (x(P), y(P))$ is a torsion point. Then:
(a) $x(P), y(P) \in \mathbb{Z}$;
(b) either $2P = \mathcal{O}$ or $y(P)^2$ divides $4a^3 + 27b^2$.

Proof. See [2, Corollary VIII.7.2]. □

Theorem 3.11 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ is one of the following fifteen groups:*

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} \quad & 1 \leq N \leq 10 \text{ or } N = 12; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \quad & 1 \leq N \leq 4. \end{aligned}$$

Further, each of these groups does occur as an $E(\mathbb{Q})_{tors}$.

Studying the points of infinite order is definitely more complicated, and here we will only state the Mordell–Weil theorem. The proof of this theorem is not very complicated, but pretty long and requiring some background.

Theorem 3.12 (Mordell–Weil)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated.*

Proof. See [2, VIII.4]. □

We will not focus on the proof of this theorem, but on an immediate consequence. From Theorem 3.2 it immediately follows that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors},$$

for some integer $r \geq 0$.

Definition 3.13. We define r to be the *rank* of $E/\mathbb{Q}$.

Remark 3.14. To our knowledge, there is no known algorithm to compute the rank of a given elliptic curve.

3.3. **Exercises.** The exercises marked with * are harder; those marked with ! are important.

3.1 ! Prove 3.4.ii), iv), and v). [Extra: do not use Proposition 3.6.]

3.2 ! *(Duplication formula)* Let C be an elliptic curve given in Weierstrass form and let P be a point of C. Write down the formula for the coordinates of $2P = P + P$ (cf. Remark 3.3). Give a characterisation of the two torsion points.

3.3 Consider the cubic curve C over $\mathbb{Q}$ given by

$$y^2 = x^3 + 17.$$

The points $P_1 = (-2, 3)$ and $P_2 = (-1, 4)$ are on the curve. Compute $P_1 + P_2$. Find all the $\mathbb{Q}$-torsion points of C.

3.4 Find all the $\mathbb{Q}$-torsion points of the elliptic curve $C\colon y^2 = x^3 - x$.

3.5 * Find more $\mathbb{Q}$-rational solutions of the following equation:

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4.$$

4. Divisors on a curve

In this section we define the notion of divisors, divisors group and Picard group for a curve C (cf. [2, Section II.3]).

4.1. The divisor group.

Definition 4.1. Let C be a curve, we define the *divisor group of* C, denoted by $\operatorname{Div} C$ to be the free abelian group generated by the points of C.

From the definition it follows that an element D of $\operatorname{Div} C$ has the form

$$D = \sum_{P \in C} n_P P,$$

where n_P is an integer and it is equal to zero for almost all P.

Definition 4.2. Let $D = \sum n_P P$ be a divisor of C. We define the *degree* of D as

$$\sum_{P \in C} n_P \in \mathbb{Z}.$$

This defines a map (in fact a group homomorphism)

$$\deg\colon \operatorname{Div} C \to \mathbb{Z}\,.$$

We define $\operatorname{Div}^0 C$ to be the kernel of deg.

If C is defined over a field k, then $\operatorname{Gal}(\overline{k}/k)$ acts on $\operatorname{Div} C$ (and $\operatorname{Div}^0 X$) in the obvious way: if $\sigma \in \operatorname{Gal}(\overline{k}/k)$ and $D = \sum n_P P$, then

$$D^\sigma = \sum n_P P^\sigma.$$

Definition 4.3. Let $D \in \operatorname{Div} C$ a divisor on C. We say that D *can be defined over* k if $D^\sigma = D$ for any $\sigma \in \operatorname{Gal}(\overline{k}/k)$.

Definition 4.4. Let $C \subset \mathbb{A}^n$ be an affine curve. A *regular function* of C is a function that can be expressed as

$$P = (x_1, ..., x_n) \mapsto \frac{f_1(x_1, ..., x_n)}{f_2(x_1, ..., x_n)},$$

where f_1, f_2 are polynomials in n variables. Notice that a regular function of C does not need to be defined on the whole C.
If C is a *projective* curve, that is, $C \subset \mathbb{P}^n$, then a *regular function* of C is a function that can be expressed as

$$P = (x_0 : ... : x_n) \mapsto \frac{f_1(x_0, ..., x_n)}{f_2(x_0, ..., x_n)},$$

where f_1, f_2 are polynomials of the same degree in $n+1$ variables. Also in this case, a regular function of C does not need to be defined on the whole C.

Example 4.5. Let C be the affine line $\mathbb{A}^1_K$ with coordinate x. Then a function of C is given by a ratio f_1/f_2, with f_1, f_2 polynomials in x. For example,

$$f\colon x \mapsto \frac{x-2}{x^2-1}.$$

Notice that f is not defined at 1 and -1, that is, it has poles (of multiplicity one) at 1 and -1; it has a zero at 2

If we embed $\mathbb{A}^1$ into $\mathbb{P}^1$ via

$$x \mapsto (X : Y) = (x : 1),$$

then f extends to the regular map of $\mathbb{P}^1$ given by

$$(X : Y) \mapsto \frac{(X - 2Y)Y}{X^2 - Y^2}.$$

Then notice that it has poles at $(1 : 1), (-1 : 1)$ and zeros at $(2 : 1), (1 : 0)$.

Definition 4.6. Let f be a function of C defined over $\overline{k}$, that is an element of $\overline{k}(C)$, then we defined the divisor associated to f to be the divisor

$$(f) = \operatorname{div} f = \sum \operatorname{ord}(P)P.$$

Divisors of the form $D = \operatorname{div} f$ for $f \in \overline{k}(C)$ are called *principal*.
Two divisors D_1, D_2 are called *linearly equivalent* if their difference is principal.

Example 4.7. Continuing Example 4.5, the divisor associated to the map of $\mathbb{P}^1$ defined by

$$(X : Y) \mapsto \frac{(X - 2Y)Y}{X^2 - Y^2}.$$

is

$$(2 : 1) + (1 : 0) - (1 : 1) - (-1 : 1).$$

Example 4.8. Let E be the elliptic curve over $\mathbb{Q}$ given by the equation

$$E\colon y^2 = x^3 - x\ .$$

Consider the points $P_1 = (-1, 0), P_2 = (0, 0), P_3 = (0, 0) \in E(\mathbb{Q})$, and the points $Q_1 = (2, \sqrt{6}), Q_2 - (2, -\sqrt{6})$.
Then $D = 2(-1, 0) - 3(0, 0) + (2, \sqrt{6})$ is a divisor of E. The degree of D is 0, and hence $D \in \operatorname{Div}^0 E$.
Let $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the map defined by

$$\sigma\colon \sqrt{6} \to -\sqrt{6}.$$

Then $D^\sigma = 2(-1, 0) - 3(0, 0) + (2, -\sqrt{6}) \neq D$, hence D cannot be defined over $\mathbb{Q}$.
Consider instead the divisor $D_1 = (2, -\sqrt{6}) + (2, \sqrt{6})$. Notice that $D_1^\sigma = (2, \sqrt{6}) + (2, -\sqrt{6}) = D_1$ and hence D_1 can be defined over $\mathbb{Q}$, even though Q_1 and Q_2 cannot, if taken singularly!
Consider the function of E defined by

$$f := y = \frac{Y}{Z}.$$

Then f has three zeros of multiplicity one at P_1, P_2, P_3 and one pole of multiplicity three at $\mathcal{O} = (0 : 1 : 0)$. It follows that $P_1 + P_2 + P_3 \sim_{\text{lin}} 3\mathcal{O}$.

Facts 4.9. *Let C be a smooth curve and $f \in \overline{k}(C)$. let $\phi\colon C_1 \to C_2$ be a noncostant map of curves. Then the following statements hold.*

(a) $\operatorname{div} f = 0$ *if and only if* $f \in \overline{k}^*$.
(b) $\deg \operatorname{div} f = 0$.

4.2. **The Picard group.**

Definition 4.10. The *Picard group* of C, denoted by $\operatorname{Pic} C := \operatorname{Div} C/\sim_{\text{lin}}$, is the quotient of $\operatorname{Div} C$ by linear equivalence.
We define $\operatorname{Pic}^0 C$ to be $\operatorname{Div}^0 / \sim_{\text{lin}}$.

Example 4.11 (Picard group of $\mathbb{P}^1$)**.** It is easy to see, that if $C = \mathbb{P}^1$, then a divisor $D \in \operatorname{Div} \mathbb{P}^1$ is principal if and only if $\deg D = 0$. It follows that the map deg induces an isomorphism between $\operatorname{Pic} \mathbb{P}^1$ and $\mathbb{Z}$

Example 4.12. As in Example 4.8, consider the function of E defined by

$$f := y = \frac{Y}{Z}.$$

Then f has three zeros of multiplicity one at P_1, P_2, P_3 and one pole of multiplicity three at $\mathcal{O} = (0:1:0)$. It follows that $P_1 + P_2 + P_3 \sim_{\text{lin}} 3\mathcal{O}$ or, equivalently, that $P_1 + P_2 + P_3 = 3\mathcal{O}$ in $\operatorname{Pic} E$.

Definition 4.13. Let $D = \sum n_P P$ be a divisor of C. We say that D is *effective*, denoted by

$$D \geq 0,$$

if $n_P \geq 0$ for every P.
We say that $D_1 \geq D_2$ if $D_1 - D_2$ is effective.

Definition 4.14. Let D be a divisor of C. We associate to D the set of function

$$\mathcal{L}(D) := \{f \in \overline{k}(C)^* \colon \operatorname{div} f \geq -D\} \cup \{0\}.$$

We denote the dimension of $\mathcal{L}(D)$ by $\ell(D) := \dim_{\overline{k}} \mathcal{L}(D)$.

Example 4.15. We continue with Example 4.8. The divisor $D_2 = P_1 + P_2 + P_3$ is effective, and $f \in \mathcal{L}(D_2)$.

Facts 4.16. *Let $D \in \operatorname{Div} C$. Then the following statements hold.*

(a) If $\deg D < 0$, then $\mathcal{L}(D) = \{0\}$.
(b) $\mathcal{L}(D)$ is a finitely dimensional $\overline{k}$-vector space.
(c) If D' is linearly equivalent to D, then $\mathcal{L}(D) \cong \mathcal{L}(D')$.

Theorem 4.17 (Riemann–Roch for elliptic curves)**.** *Let E be an elliptic curve and D any divisor on E. Then*

$$\ell(D) - \ell(-D) = \deg D\ .$$

Example 4.18. We again use Example 4.8 and 4.15. As $D_2 \sim_{\text{lim}} 3\mathcal{O}$, we have that $\mathcal{L}(D_2) \cong \mathcal{L}(3\mathcal{O})$. As $\deg -3\mathcal{O} = -3 < 0$, from Facts 4.16a it follows that $\ell(-3\mathcal{O}) = 0$ and hence, by Theorem 4.17, it follows that $\ell(D_2) = \ell(3\mathcal{O}) = 3$.

Theorem 4.19. *Let E be an elliptic curve. Then the map*

$$\begin{aligned} \kappa \colon E &\to \operatorname{Pic}^0 E \\ P &\mapsto [P - \mathcal{O}] \end{aligned}$$

is a group isomorphism.

Proof. In this proof we will use $\oplus$ to denote the sum of points on E, while $+$ to use the sum of divisors.
First we show that the map is injective. Take $P, Q \in E$ such that $[P-\mathcal{O}] = [Q-\mathcal{O}]$, that is, $P-Q$ is a principal divisor. Let f be a function of E such that $\operatorname{div} f = P-Q$. Then $f \in \mathcal{L}(Q)$. At the same time notice that $1 \in \mathcal{L}(Q)$ and that, by Theorem 4.17, $\dim \mathcal{L}(Q) = 1$. It follows that $\mathcal{L}(Q) = k$ and hence f is constant. Therefore $\operatorname{div} f = 0$ and hence $P = Q$.
Now we prove that κ is a group homomorphism, that is, $\kappa(P \oplus Q) = \kappa(P) + \kappa(Q)$. Let f be the equation of the line passing through P and Q and let R be its third point of intersection with E. Let f' be the equation of the line passing through $\mathcal{O}$ and R and notice that its third point of intersection with E is exactly $P \oplus Q$ (by definition of the sum on E). Consider the functions f/Z and f'/Z on E. As Z intersects E in $\mathcal{O}$ with multiplicity 3, we have

$$\operatorname{div} f/Z = P + Q + R - 3\mathcal{O},$$
$$\operatorname{div} f'/Z = R + (P \oplus Q) - 2\mathcal{O}.$$

It follows that

$$\operatorname{div} f/f' = P + Q - \mathcal{O} - (P \oplus Q) = (P - \mathcal{O}) + (Q - \mathcal{O}) - (P \oplus Q - \mathcal{O}),$$

that is,

$$\kappa(P) + \kappa(Q) - \kappa(P \oplus Q) = 0,$$

proving that κ is a group homomorphism.
Finally, notice that the surjectivity of κ directly follows from the property of being a group homomorphism. □

Corollary 4.20. *Let E be an elliptic curve and $D = \sum n_P P$ a divisor on E. Then D is principal if and only if* $\deg D = 0$ *and* $\sum [n_P]P = 0$.

Proof. First assume that D is principal. Then by Facts 4.9b it follows that $\deg D = 0$. By Theorem 4.19 we have that the sums in $\operatorname{Pic}^0 E$ and E coincide, and hence $\sum [n_P]P = 0$.
Conversely, assume that $\deg D = 0$ and $\sum [n_P]P = 0$. Then $D = 0 \in \operatorname{Pic}^0 E$ and hence it is a principal divisor. □

Example 4.21. Consider again Example 4.8. From Proposition 3.4e and Corollary 4.20 it immediately follows that the divisor $P_1 + P_2 + P_3 - 3\mathcal{O}$ is a principal divisor, without the need of exhibiting the function f.

5. Isogenies

After giving to an elliptic curve a group structure, it is very natural to look for morphisms that preserve this structure. We will start with some general theory about morphisms of curves.

5.1. **Maps between curves.** The results in this subsection are stated without proofs. For the proofs (and much more!) you can consult [3, Chapters I and IV] and/or [2, Chapter II].

Definition 5.1. Let $C \subset \mathbb{P}^m$ be a projective curve and let V be a subvariety of $\mathbb{P}^n$. We define a *rational map* from C to V a map $C \to V$ defined by

$$P \mapsto (f_0(P) : \ldots : f_n(P))$$

such that $f_0, ..., f_n$ are homogeneous polynomials in $m+1$ variables of the same degree, and $(f_0(P) : ... : f_n(P)) \in V$ for every point P such that $(f_0(P), ..., f_n(P)) \neq (0, ..., 0)$.
Let P be a point of C; we say that f is defined at P if $(f_0(P), ..., f_n(P)) \neq (0, ..., 0)$. If a rational map is defined everywhere (some authors say *everywhere regular*), then we say that the map is a *morphism*.

Example 5.2. Consider the curve $C = \mathbb{P}^1$, the variety $V = \mathbb{P}^2$ and the map $\mathbb{P}^1 \to \mathbb{P}^2$ defined by

$$(X : Y) \to \left(X^2(X^2 - Y^2) : Y^2(X - Y)^2 : (X^2 - Y^2)(X - Y)^2\right).$$

Notice that the map is not defined at $(1 : 1)$.

We give a list of results about morphism of curves.

Facts 5.3. *Let C be a curve, $V \subset \mathbb{P}^n$ a variety, $\phi\colon C \to V$ a rational map. The following statements hold.*

(a) If $P \in C$ is a smooth point for C, then ϕ is defined at P. In particular, if C is smooth, ϕ is a morphism.
(b) If ϕ is a morphism and V is also a curve, then ϕ is either surjective or constant.

Definition 5.4. Let $\phi\colon C_1 \to C_2$ be a rational map of curves, and let $Q \in C_2$ a point of C_2. We define the *degree* of ϕ to the be the number of points in the pre-image $\phi^{-1}(Q)$ of Q, *counted with multiplicity*. If ϕ is constant, the degree is defined to be zero.

Example 5.5. Let $E\colon Y^2Z = X^3 + aXZ^2 + bZ^3$ and let $\pi\colon E \to \mathbb{P}^1$ be the projection on the X-axis, i.e.,

$$\pi\colon (X : Y : Z) \to (X : Z).$$

Notice that π is not defined at $(0 : 1 : 0)$, it is not surjective as $(1 : 0)$ is not in the image, and it has degree 2. Indeed, if $Q = (x : 1)$, then $\pi^{-1}(Q) = \{\pm\sqrt{x^3 + ax + b}\}$. The rational map π can be extended to a morphism defining $\pi((0 : 1 : 0)) = (1 : 0)$.

Facts 5.6. *The degree of ϕ is independent of the choice of Q.*

Remark 5.7. By multiplicity here we mean what in [2] is called ramification index. See [2, Section II.2] for more details about this notion.

Definition 5.8. Let $f\colon C_1 \to C_2$ be a map of curves. Then f induces *two* maps at the level of divisors:

$$\begin{aligned} \phi^*\colon \operatorname{Div} C_2 &\to \operatorname{Div} C_1 \\ Q &\mapsto \sum_{P \in f^{-1}(Q)} e_\phi(P)P \end{aligned}$$

where $e_\phi(P)$ is the multiplicity of P inside $f^{-1}(Q)$;

$$\begin{aligned} \phi_*\colon \operatorname{Div} C_1 &\to \operatorname{Div} C_2 \\ P &\mapsto \phi(P)\,. \end{aligned}$$

Remark 5.9. One can rephrase Definition 5.8 for $\operatorname{Div}^0 C$, $\operatorname{Pic} C$, and/or $\operatorname{Pic}^0 C$.

Facts 5.10. *Let $\phi\colon C_1 \to C_2$ be a noncostant map of curves. Then the following statements hold.*

(a) For all $D \in \operatorname{Div} C_2$, $\deg \phi^* D = \deg \phi \cdot \deg D$.
(b) For all $f \in \overline{k}(C_1)$, $\phi^*(\operatorname{div} f) = \operatorname{div}(\phi^* f)$.
(c) For all $D \in \operatorname{Div} C_1$, $\deg(\phi_* D) = \deg D$.
(d) For all $f \in \overline{k}(C_1)$, $\phi_*(\operatorname{div} f) = \operatorname{div}(\phi_* f)$.
(e) $\phi_* \circ \phi^*$ acts as multiplication by $\deg \phi$ on $\operatorname{Div} C_2$.
(f) If $\psi\colon C_2 \to C_3$ is another nonconstant morphism of curves, then

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \text{ and}$$
$$(\psi \circ \phi)_* = \psi_* \circ \phi_* .$$

5.2. **Isogenies of elliptic curves.**

Definition 5.11. Let C_1 and C_2 be two elliptic curves over a field K. We define an *isogeny* from C_1 to C_2 over K to be a morphism ϕ of curves from C_1 to C_2 defined over K and such that $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in \bar{C}(K)$.

Remark 5.12. Let $(E_1, \mathcal{O}_1)$ and $(E_2, \mathcal{O}_2)$ be two elliptic curves, and $\phi\colon E_1 \to E_2$ an isogeny. From the definition, it immediately follows that $\phi(\mathcal{O}_1) = \mathcal{O}_2$. It turns out that this condition is equivalent to our definition (cf. [2, Theorem III.4.8]).

Definition 5.13. Given two elliptic curves E_1, E_2, we denote the set of isogenies from E_1 to E_2 defined over K by

$$\operatorname{Hom}_K(E_1, E_2) := \{\phi\colon E_1 \to E_2 \mid \phi \text{ isogeny over } K\ \}.$$

Given an elliptic curve E, we define the set of *endomorphisms* of E as

$$\operatorname{End}_K(E) := \operatorname{Hom}_K(E, E).$$

The set of invertible elements of $\operatorname{End}_K(E)$ is denoted by $\operatorname{Aut}_K(E)$.

Remark 5.14. The set $\operatorname{Hom}_K(E_1, E_2)$ can be endowed with an abelian group structure (and hence of $\mathbb{Z}$-module) by defining the sum $\phi + \psi\colon P \mapsto \phi(P) + \psi(P)$. This structure is inherited by $\operatorname{End}_K(E)$, that can also be endowed with the composition: $(\operatorname{End}_K(E), +, \circ)$ is called *the endormorphism ring of E*.
As $\operatorname{Aut}_K(E)$ is set of invertible elements of $\operatorname{End}_K(E)$ and so $(\operatorname{Aut}_K(E), \circ)$ has the structure of group; it is called the *automorphism group* of E.

Example 5.15. The first and easiest example of an isogeny comes from the multiplication by an integer. Let E be an elliptic curve and let $m \in \mathbb{Z}$ be an integer. We define the map $[m]\colon E \to E$ by sending a point P to

$$[m](P) := \begin{cases} \underbrace{P + \ldots + P}_{m \text{ times}} & \text{if } m > 0 \\ \underbrace{(-P) + \ldots + (-P)}_{-m \text{ times}} & \text{if } m < 0\ . \\ \mathcal{O} & \text{if } m = 0 \end{cases}$$

One can immediately check that $[m]$ is indeed an isogeny.

Proposition 5.16. *Let E be an elliptic curve over a field K of characteristic 0. The map $[\ ]\colon \mathbb{Z} \to \operatorname{End}(E)$ is an injective ring homomorphism.*

Proof. Checking that [ ] is a ring homomorphism is immediate: in fact, $[m+n] = [m] + [n]$ and $[mn] = [m] \circ [n]$.
First notice that the duplication formula (cf. 3.3) shows that $[2] \neq 0$. Then over $\bar{K}$ there are three non-trivial 2-torsion points (use the duplication formula). Let P_0 be one of them. Then $[m](P_0) = P_0 \neq 0$ for every odd m, in particular for every odd prime. This shows that the kernel of [ ] is trivial. □

Remark 5.17. When K has characteristic zero, the map [ ] is usually also surjective, that is, $\mathrm{End}_K(E) \cong \mathbb{Z}$.
When this is not the case, we say that E has *complex multiplication.*

Example 5.18. Let E be the elliptic curve $y^2 = x^3 - x$ over $K = \mathbb{C}$ (but any field containing $\mathbb{Q}(i)$ is also fine). Beside $\mathbb{Z}$, in $\mathrm{End}_K(E)$ there is also the element

$$[i] \colon (x, y) \to (-x, iy).$$

Definition 5.19. Let E be an elliptic curve over K and m an integer. We define the m-torsion points of E over K, denoted by $E(K)[m]$, as the elements in the kernel of $[m]$, that is:

$$E(K)[m] := \{P \in E(K) \mid [m]P = \mathcal{O}\}.$$

Remark 5.20. Trivially

$$E(K)_{tors} = \bigcup_{m=1}^{\infty} E(K)[m].$$

Later we will see that the size of $E[m]$ is bounded by m^2. If K is algebraically closed the bound is reached (see Proposition 8.5).

5.3. **Automorphisms of elliptic curves.** Let E be an elliptic curve over a field k. Recall we ha defined the automorphisms of E as those isogenies from E to itself (endomorphisms) which hare invertible. In this subsection, we are going to see that the j-invariant completely determines the structure of the Automorphism group $\mathrm{Aut}(E)$. We state the result considering only fields with characteristic greater than 3, but analogous statements are known also in the remaining cases of characteristic 2 and 3.

Theorem 5.21. *Let E be an elliptic curve over a field K with of characteristic different from* 2 *and* 3*. The the following holds.*

$$\mathrm{Aut}\, E \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \text{ if } j(E) \neq 0, 1728; \\ \mathbb{Z}/4\mathbb{Z} \text{ if } j(E) = 1728; \\ \mathbb{Z}/6\mathbb{Z} \text{ if } j(E) = 0. \end{cases}$$

Proof. Lemma 2.14 tells us that the only isomorphisms of elliptic curves preserving the Weierstrass form are of the form

$$x' = u^2 x\ , \quad y' = u^3 y$$

for some invertible element $u \in \overline{K}^{\times}$, sending the elliptic curve with coefficients a, b to the elliptic curve with coefficients $u^4 a, u^6 b$. Let ψ be such an isomorphism. In order for ψ to be an automorphism of E, we must have that $u^4 a = a$ and $u^6 b = b$. If $j(E) \neq 0, 1728$, then $a, b \neq 0$ and therefore u must be at the same time a fourth and a sixth root of unity, hence $u = \pm 1$.

If $j(E) = 1728$, then $b = 0$ and u must be a fourth root of unity. Hence we have four possible automorphism. It is easy to see that the set of these four automorphisms with composition forms a group isomorphic to $\mathbb{Z}/4\mathbb{Z}$.
If $j(E) = 0$, then $a = 0$ and u must be a sixth root of unity. Hence we have six possible automorphism. It is easy to see that the set of these six automorphisms with composition forms a group isomorphic to $\mathbb{Z}/6\mathbb{Z}$. □

Remark 5.22. Theorem 5.21 can be proven also with lattice theoretic tools, using the correspondence between elliptic curves and complex lattices. See Corollary 8.3.

6. Elliptic curves over finite fields

In this section we focus on elliptic curves over finite fields. We will briefly recall the basic theory of finite fields. The main goal of the section is to state and prove the Weil conjectures for elliptic curves.

6.1. **Finite fields.** For an account on this subject you might read [4, Section V.5] or [5, Chapter 12].
A *finite field* is simply a field with finitely many elements.

Example 6.1. Let p be a prime number, and define $\mathbb{F}_p$ as the ring obtained by taking $\mathbb{Z}/p\mathbb{Z}$ with the usual sum and multiplication. One can easily verify that $\mathbb{F}_p$ is a field.

Example 6.2. Let p be a prime number, and let $q = p^n$ be a power of p. Define $\mathbb{F}_q$ as the ring obtained by taking $\mathbb{Z}/q\mathbb{Z}$ with the usual sum and multiplication. One can verify that $\mathbb{F}_q$ is a field.

Let K be a field (not necessarily finite). We define the characteristic of K, denoted by $\operatorname{char} K$, to be smallest non-negative integer n such that $n \cdot 1 = 0$ in K.

Example 6.3. The fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all contain the ring $\mathbb{Z}$ and therefore they all have characteristic 0.

Example 6.4. The fields $\mathbb{F}_p$ and $\mathbb{F}_q$ (cf. 6.1 and 6.2), have characteristic p.

The following result completely classifies the finite fields.

Theorem 6.5 (Moore, 1893)**.** *Let K be a finite field. Then K is of the form $\mathbb{F}_q$ for some prime p and some integer n such that $q = p^n$.*
For every prime power q there are finite fields of order q, and they are all isomorphic.
In $\mathbb{F}_q$ every element satisfies the equation

$$X^q = X. \tag{14}$$

Proof. For a proof, see [5, Theorem 12.1] or [4, Theorem V.5.2]. □

Corollary 6.6. *The field $\mathbb{F}_q$ contains the field $\mathbb{F}_{q'}$ if and only if $q = p^n$, $q' = p^m$, and $m \leq n$.*

Let K be a finite field of characteristic p. We define the *Frobenius automorphism* of K as the automorphism given by

$$\Phi \colon x \mapsto x^p.$$

Theorem 6.7. *Let K be a finite field of characteristic p Let $\overline{K}$ be an algebraic closure of K. Then the Frobenius map Φ of K defines an automorphism of $\overline{K}$. Furthermore, Φ topologically generates the Galois group $\mathrm{Gal}(\overline{K}/K)$. For every integer n, the set of elements of $\overline{K}$ fixed by Φ^n is a subfield isomorphic to $\mathbb{F}_{p^n}$.*

Proof. See [5, Section 12.5]. □

Remark 6.8. Let K be a finite field of characteristic p, and let $\overline{K}$ be an algebraic closure of K. Then $\overline{K}$ is an *infinite* field of characteristic p.

6.2. **The Hasse bound.** Let K be a finite field with $q = p^n$ elements, and let E be an elliptic curve over K. As K is finite, we know that the set $E(K)$ of rational points is also finite. Then the next question is: can we estimate the size of $E(K)$, that is, the number of K-rational points of E.

Lemma 6.9. *Let A be an abelian group and $d\colon A \to \mathbb{Z}$ a positive definite quadratic form. Then for all $a, b \in A$,*

$$|d(a-b) - d(a) - d(b)| \leq 2\sqrt{d(a)d(b)}.$$

Proof. For $a, b \in A$, let

$$L(a,b) := d(a-b) - d(a) - d(b).$$

As d is quadratic, L is bilinear. As d is positive definite, then for $m, n \in \mathbb{Z}$

$$0 \leq d(ma - nb) = m^2 d(a) + mnL(a,b) + n^2 d(b).$$

Then for $m = -L(a,b)$ and $n = 2d(a)$ we have

$$0 \leq d(a)[4d(a)d(b) - L(a,b)^2]$$

If $a \neq 0$, as d is positive definite, $d(a) > 0$ and so $0 \leq 4d(a)d(b) - L(a,b)^2$, leading to the statement.
If $a = 0$, then $d(a) = 0$ and the statement is trivially true. □

Theorem 6.10. *Let E and K defined as above. Then*

$$|\#E(K) - q - 1| \leq 2\sqrt{q}$$

Proof. Choose a Weierstrass equation for E with coefficients in K and consider the map $\phi\colon E(\overline{K}) \to E(\overline{K})$ defined by

$$(x, y) \mapsto (x^q, y^q).$$

Notice that the map above is the n-th power of the Frobenius morphism. Then, using Theorem 6.7, P is in $E(K)$ if and only if $\phi(P) = P$. Therefore $E(K) = \ker(1 - \phi)$ and so $\#E(K) = \#\ker(1-\phi) = \deg(1-\phi)$.
The degree is a quadratic form on $\mathrm{End}(E)$ and the degree of ϕ is q, then the result follows from Lemma 6.9. □

6.3. **Exercises.** The exercises marked with * are harder; those marked with ! are important.

4.1 ! Let n be a non-prime integer. Prove that the ring $\mathbb{Z}/n\mathbb{Z}$ is not a field.

7. Elliptic curves over $\mathbb{C}$

In this section we focus on elliptic curves defined over $\mathbb{C}$. We will see how they relate to classical problems in calculus and to the modern theory of complex manifolds.

7.1. **Ellipses and elliptic curves.** If one draws an elliptic curve, he will find that it does not look at all like an ellipse. Then why are they called *elliptic curves*? The reason is that they are related to the computation of the arclength of the ellipses. This theory is classical and vast; we will only briefly sketch it outlining the basic links and leaving some more details as exercises. More can be found in [2, Chapter VI] and [6, Section 1].

Let C be the ellipse defined by the equation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, then one can show that the perimeter of C is given by the integral

$$4aT(\sqrt{1-(b/a)^2}),$$

with

$$T(k) := \int_0^{\frac{\pi}{2}} (1 - k^2 \sin^2 \theta)^{-1/2} \mathrm{d}\theta. \tag{15}$$

The integral $T(k)$ can also be written as

$$T(k) = \int_0^1 \left(\frac{1-k^2x^2}{1-x^2} \right)^{1/2} \mathrm{d}x. \tag{16}$$

The problem is that this integral is not path-independent, because the square-root is not single valued. In order to make it well-defined we have to make branch cuts between the zeros and the poles of the integrating function, that is, between the points $z = \pm 1, \pm 1/k$. Then the integral will be path independent in the complement of the branch cuts. As the square-root is double-valued, we have to take two copies of $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ and glue them identifying the branch cuts. What we get is a torus, that is, as we will see later (cf. Proposition 7.17), an elliptic curve. So studying the arclength of an ellipse leads to the study of integrals on an elliptic curve.

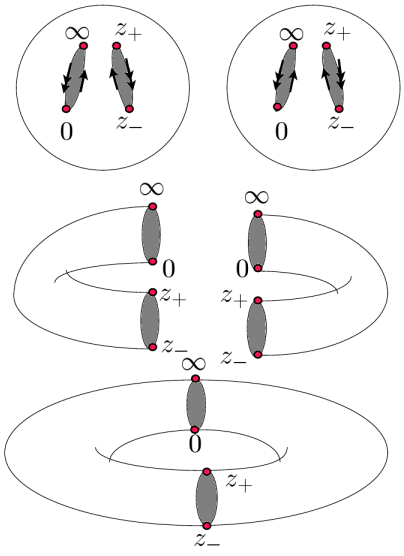


Figure 5. Construction of a torus by glueing together two copies of $\mathbb{P}^1_{\mathbb{C}}$ identifying the branch cuts. In the picture the branch cuts are between the points $0, \infty$ and z_+, z_-.

7.2. **Lattices and elliptic functions.**

Definition 7.1. We define a *lattice* Λ inside $\mathbb{C}$ to be a discrete subgroup of C containing an $\mathbb{R}$-basis of $\mathbb{C}$, that is, $\Lambda = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}$ with $\omega_1, \omega_2 \in \mathbb{C}$ such that $\omega_1\mathbb{R} + \omega_2\mathbb{R} = \mathbb{C}$. If $\{\omega_1, \omega_2\}$ is the basis contained inside Λ, we say that Λ is generated by $\{\omega_1, \omega_2\}$, and we write $\Lambda = \langle \omega_1, \omega_2 \rangle$.

Example 7.2. The ring $\mathbb{Z}[i] \subset \mathbb{C}$ is a lattice.

Definition 7.3. A *fundamental parallelogram* for a lattice $\Lambda = \langle \omega_1, \omega_2 \rangle$ is a set of the form

$$D = \{a + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 < 1\}$$

with $a \in \mathbb{C}$. It follows that the projection $D \to \mathbb{C}/\Lambda$ is bijective. We denote by $\bar{D}$ the closure of D inside $\mathbb{C}$.

Figure 6. A fundamental domain of the lattice generated by ω_1, ω_2. In the picture are also shown the 4-torsion points (cf. Proposition 8.5).

Definition 7.4. We define an *elliptic function (relative to the lattice Λ)* f to be a meromorphic function of $\mathbb{C}$ such that

$$f(z + \omega) = f(z)$$

for every $z \in \mathbb{C}$ and $\omega \in \Lambda$.

Example 7.5. Any constant function trivially is an elliptic function.

Definition 7.6. The *order* of an elliptic function is its number of poles and zeros (counted with multiplicity) in a fundamental parallelogram.

Definition 7.7. Let $\Lambda \subset \mathbb{C}$ be a lattice. We define $\mathbb{C}(\Lambda)$ to be the set of all the elliptic functions for Λ.
The pointwise sum and multiplication give $\mathbb{C}(\Lambda)$ the structure of field.

Proposition 7.8. *Let $\Lambda \subset \mathbb{C}$ be a lattice and f an elliptic function relative to Λ. The following statements hold:*
(a) if f has no poles (or no zeros) then it is constant;
(b) $\sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w(f) = 0$;
(c) $\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f) = 0$;
(d) $\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)w \in \Lambda$;
(e) A non-constant elliptic function has order at least 2.

Proof. See [2, Proposition VI.2.1, Theorem VI.2.2, Corollary VI.2.3]. □

7.3. **The Weierstrass $\wp$ function.** In this section we give some examples of (non-constant) elliptic functions.

Definition 7.9. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass $\wp$-function (relative to Λ)* is defined by the series

$$\wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{(z-w)^2} - \frac{1}{w^2}.$$

The *Eisenstein series of weight $2k$ (for Λ)* is the series

$$G_{2k}(\Lambda) := \sum_{\substack{w\in\Lambda \\ w\neq 0}} w^{-2k}.$$

We might write $\wp(z)$ and G_{2k} is the lattice is fixed or clear from the context.

Lemma 7.10. *Let $\Lambda \subset \mathbb{C}$ be a lattice. Then the function $\wp(z;\Lambda)$ is an elliptic even function.*

Proof. To show that it is even elliptic just notice that we can write

$$\wp(z) = \sum_{w\in\Lambda} \frac{1}{(z-w)^2} - \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{w^2}.$$

As the first sum, the only one where z appears, ranges over all the elements of Λ, the shifting by $\lambda \in \Lambda$ does not affect the sum.
The result about the parity is elementary □

Remark 7.11. Notice that we can explicitly write the first derivative of $\wp$, in fact

$$\wp'(z) = -2 \sum_{w\in\Delta} \frac{1}{(z-w)^3}.$$

From this expression or, more directly, from Lemma 7.10, it follows that $\wp'$ is an odd elliptic function.

Proposition 7.12. *Let $\Delta \subset \mathbb{C}$ be a lattice. The following statements hold:*
(a) $G_{2k}(\Lambda)$ is absolutely convergent for $k > 1$;
(b) $\wp(z,\Lambda)$ converges uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$.
(c) $\wp$ is an even elliptic function having a double pole with residue 0 at $z = 0$ (and so at every lattice point) and no other poles.
(d) $\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$.

Proof. See [2, Theorem VI.3.1, Theorem VI.3.2]. □

Theorem 7.13. *The following statements hold:*

(a) the Laurent series for $\wp(z)$ at $z = 0$ is given by

$$\wp(z) = z^{-2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n};$$

(b) for all $z \in \mathbb{C}$ with $z \notin \Delta$, we have that

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Proof. (a) Recall that the Laurent expansion of $\frac{1}{1-z}$ at 1 for $|z| < 1$ is $\sum_{k=0}^{\infty} z^n$. By derivation, it follows that

$$\frac{1}{(1-z)^2} = \sum_{k=1}^{\infty} kz^{k-1}$$

and hence

$$\frac{1}{(1-z)^2} - 1 = \sum_{k=1}^{\infty}(k+1)z^k.$$

Write $\wp(z)$ as

$$z^{-2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} \frac{1}{(z-w)^2} - \frac{1}{w^2} = z^{-2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} w^{-2}[(1-z/w)^{-2} - 1].$$

As we are computing the Laurent series of $\wp$ at $z = 0$ we may assume that $|z| < |w|$ for every $w \in \Lambda$, and hence we can apply the Laurent expansion computed before, getting

$$\begin{aligned}\wp(z) = z^{-2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}}\sum_{k=1}^{\infty}(k+1)\frac{z^k}{w^{k+2}} = \\ = z^{-2} + \sum_{k=1}^{\infty}(k+1)z^k \sum_{\substack{w\in\Lambda\\ w\neq 0}} w^{-(k+2)} = \\ = z^{-2} + \sum_{n=1}^{\infty}(2n+1)z^{2n}G_{2n+2},\end{aligned}$$

where $k = 2n$; notice that $\sum_{\substack{w\in\Lambda\\ w\neq 0}} w^{-(k+2)} = 0$ for k odd. This proves the statement.

(b) Consider the first terms of the following Laurent expansions:

$$\begin{aligned}\wp(z) &= z^{-2} + 3G_4z^2 + \cdots \\ \wp(z)^3 &= z^{-6} + 9G_4z^{-2} + 15G_6 + \cdots \\ \wp'(z)^2 &= 4z^{-6} - 24G_4z^{-2} - 80G_6 + \cdots .\end{aligned}$$

It follows that the function

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6$$

is holomorphic around $z = 0$ and it vanishes at $z = 0$. As f is a combination of functions that are elliptic for Λ, it is also elliptic for Λ. Then, by Proposition 7.12.i), it follows that $f(z)$ is the constantly 0, proving the statement.

□

Remark 7.14. It is customary to set

$$g_2 = g_2(\Lambda) := 60G_4,$$
$$g_3 = g_3(\Lambda) := 140G_6.$$

Then the relation in Theorem 7.13 reads

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Definition 7.15. Let $\Lambda \subset \mathbb{C}$ be a lattice and g_2, g_3 the quantities associated to it defined in Remark 7.14. We define the curve $E = E(\Lambda)$ as

$$E(\Lambda)\colon y^2 = x^3 - \frac{g_2}{4}x - \frac{g_3}{4}.$$

Lemma 7.16. *The curve $E(\Lambda)$ is an elliptic curve.*

Proof. To show that E is an elliptic curve it is enough to show that $\Delta(E) \neq 0$ or, equivalently, that the equation

$$x^3 + \frac{g_2}{4}x + \frac{g_3}{4} = 0 \tag{17}$$

has no repeated roots. Notice that the equation (17) has the same roots of the equation

$$f(x) := 4x^3 - g_2x - g_3 = 0.$$

So we have to show that $f(x)$ has no repeated roots.
In order to do so, let $\{w_1, w_2\}$ a basis for Λ, and define $w_3 := w_1 + w_2 \in \Lambda$ As $\wp'(z)$ is an odd elliptic function,

$$-\wp'(-w_i/2) = \wp'(w_i/2) = \wp'(w_i/2 - w_i) = \wp'(-w_i/2),$$

from which it follows that $\wp'(w_i/2) = 0$ for $i = 1, 2, 3$. By Theorem 7.13 it follows that $\wp(w_i/2), i = 1, 2, 3$ are the three roots of f. We are left to show that they are distinct.
As $\wp$ is an even elliptic function, so is the function $\psi_i(z) := \wp(z) - \wp(w_i/2)$, for every $i = 1, 2, 3$. As $\wp'(w_i/2)$ is zero, then $w_i/2$ is a zero of order at least 2. Notice that $\psi_i(z)$ has exactly one pole of order 2 (inside a fundamental domain) at $z = 0$ (as $\wp$ does) and so $w_i/2$ has order exactly 2 and it is the only zero. This shows that $\wp(w_i/2) \neq \wp(w_j/2)$ for $i \neq j$, proving the statement. □

Proposition 7.17. *The map*

$$\begin{aligned}\phi\colon \mathbb{C}/\Lambda &\to \bar{E}(\Lambda)\\ z &\mapsto (\wp(z) : \wp'(z)/2 : 1)\\ 0 &\mapsto \mathcal{O}\end{aligned}$$

is an isomorphism of Riemann surfaces which is also a group homomorphism.

Proof. See [2, Proposition 3.6.(b)]. □

Remark 7.18. The elliptic curve $E(\Lambda)$ has j-invariant $j(\Lambda) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$. This construction allows us to define the j-invariant of a complex lattice.

Remark 7.19. If we did not already define the group structure on E, we could use the bijection given by ϕ to define it. In this case it would be immediately follow that the addition on E is associative and commutative.

Example 7.20. Consider the lattice $\Lambda = \mathbb{Z}[i] = \langle 1, i \rangle$. We will see that $E(\Lambda)\colon y^2 = x^3 - x$.

The construction given in Definition 7.15 has also a converse.

Theorem 7.21 (Uniformization theorem)**.** *Let $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. Then, up to homotheties, there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that $g_2(\Lambda) = a$ and $g_3(\Lambda) = b$.*

Proof. Later. □

7.4. **Exercises.**

5.1 Let E be an elliptic curve given by the Weierstrass equation

$$E\colon y^2 = x^3 + ax + b.$$

(a) Prove that there is a $\lambda \in \mathbb{R} - \{0, 1\}$ such that E can be put in Lagrange form

$$y^2 = x(x-1)(x-\lambda).$$

(b) For given a, b, find all possible values of λ; vice versa, for a given λ, find all possible values of a and b.

(c) Express $j(E)$ in terms of λ.

5.2 Prove that the arclength of the ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

is given by

$$4aT(\sqrt{1 - (b/a)^2}),$$

with T defined as in (15). [Hint: use the formula for the length of a plane curve $y = f(x)$ given by:

$$\int_a^b \sqrt{1 + \left(\frac{dy}{dx}\right)^2}\, dx.$$

Also, recall the parametrization of the ellipse given by $(a\cos\theta, b\sin\theta)$.]

5.3 Prove Equation (16).

8. Isogenies and j-invariant: revisited

So we have seen that given a lattice inside $\mathbb{C}$ we can associate an elliptic curve to it. From this construction many questions arise: is this association unique? How maps of lattices translate into the language of elliptic curves?

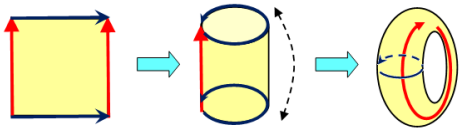


Figure 7. A visual explanation of Remark 8.1.

Remark 8.1. In the previous section we have mentioned the quotient $\mathbb{C}/\Lambda$, with Λ being a complex lattice. Recall that this quotient is isomorphic to a complex torus.

8.1. **Isogenies.** Let Λ_1 and Λ_2 be two lattices. A map $\mathbb{C} \to \mathbb{C}$ induces a well defined map $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ if and only it sends Λ_1 into Λ_2. One example is given by considering the multiplication by $\alpha \in \mathbb{C}$, with α such that $\alpha\Lambda_1 \subseteq \Lambda_2$. It induces the map

$$\begin{aligned} \phi_\alpha \colon \mathbb{C}/\Lambda_1 &\to \mathbb{C}/\Lambda_2 \\ z &\mapsto \alpha z \bmod \Lambda_2 \ . \end{aligned}$$

Theorem 8.2. *Keeping the notation as above, the following statements hold:*

i) The association

$$\begin{aligned} \{\alpha \in \mathbb{C} \ : \ \alpha\Lambda_1 \subset \Lambda_2\} &\to \{\textit{holomorphic maps } \phi \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \textit{ with } \phi(0) = 0\} \\ \alpha &\mapsto \phi_\alpha \end{aligned}$$

is a bijection;

ii) let E_1 and E_2 be the elliptic curves corresponding to the lattices Λ_1 and Λ_2 (cf. 7.15), then the natural inclusion

$$\{\textit{isogenies } \phi \colon E_1 \to E_2\} \to \{\textit{holomorphic maps } \phi \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \textit{ with } \phi(0) = 0\}$$

is a bijection.

Proof. i) First we proof the injectivity of the association. Let $\alpha, \beta \in \mathbb{C}$ be such that $\phi_\alpha = \phi_\beta$, that is $\alpha z \equiv \beta z \bmod \Lambda_2$ for every $z \in \mathbb{C}$ or, equivalently, that $g(z) := z(\alpha - \beta) \in \Lambda_2$ for every $z \in \mathbb{C}$. As Λ_2 is discrete, this implies that g is constant and hence $\alpha = \beta$.

To prove the surjectivity, consider a holomorphic map $\phi \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\phi(0)$. As $\mathbb{C}$ is simply connected, we can lift it to a map $f \colon \mathbb{C} \to \mathbb{C}$ such that the following diagram commutes.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow[\phi]{} & \mathbb{C}/\Lambda_2 \end{array}$$

As the diagram commutes, for any $z \in \mathbb{C}$ and $w \in \Lambda$ we have $f(z + w) \equiv f(z) \bmod \Lambda_2$. As before, since Λ_2 is discrete, the function $f(z + w) - f(z)$ is constant in z, and so its derivative is zero and so $f'(z + w) = f'(z)$ for every $z \in \mathbb{C}$ and $w \in \Lambda_1$. It follows that f' is a holomorphic elliptic function. Then, by Proposition 7.8.i), f' is constant. This implies that $f(z) = \alpha z + \beta$, for some $\alpha, \beta \in \mathbb{C}$. The condition $\phi(0) = 0$ implies $\beta = 0$. The fact that $f(\Lambda_1) \subseteq \Lambda_2$ implies that $\alpha\Lambda_1 \subseteq \Lambda_2$.

ii) First notice that since an isogeny is defined everywhere, the map induced on the corresponding complex torus is holomorphic. Hence the association

$$\mathrm{Hom}(E_1, E_2) \to \text{Holo. } \mathrm{Map}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$$

is well-defined and it is clearly injective.

To prove the surjectivity, using *i)*, it is enough to consider maps of the form ϕ_α with $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_1 \subset \Lambda_2$. The induced map on the Weierstrass equation is given by

$$\begin{aligned} E_1 &\to E_2 \\ (\wp(z; \Lambda_1) : \wp'(z; \Lambda_1)/2 : 1) &\mapsto (\wp(\alpha z; \Lambda_2) : \wp'(\alpha z; \Lambda_2)/2 : 1). \end{aligned}$$

Using the fact $\alpha\Lambda_1 \subseteq \Lambda_2$, one can easily show that $\wp(\alpha z;\Lambda_2)$ and $\wp'(\alpha z;\Lambda_2)$ are elliptic functions for Λ_1 and so the map above is the desired isogeny.

□

Corollary 8.3. *Let E_1, E_2 be the complex elliptic curves corresponding to the lattices $\Lambda_1, \Lambda_2 \subset \mathbb{C}$. Then E_1 and E_2 are isomorphic (over $\mathbb{C}$) if and only if there is a $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 = \Lambda_2$ (that is, Λ_1 and Λ_2 are homothetic).*

We can summarise the previous results in the following theorem.

Theorem 8.4. *The following categories are equivalent:*

(i) (Elliptic curves over $\mathbb{C}$; Isogenies);
(ii) (Complex tori; Complex analytic maps taking 0 to 0);
(iii) (Lattices up to homothety; $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\}$).

A first application of the study of elliptic curves over $\mathbb{C}$ is given by the following result about torsion points.

Proposition 8.5. *Let $E/\mathbb{C}$ be an elliptic curve and $m \geq 1$, then the following statements hold.*

(a) As abstract groups,

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

(b) The multiplication-by-m map $[m]$ has degree m^2.

Proof. Exercise. □

8.2. **The group $\mathrm{SL}_2(\mathbb{Z})$.** In order to prove Theorem 7.21 we need to introduce some notions.

Definition 8.6. We define the *upper-half plane* to be the region $\mathbb{H}$ of $\mathbb{C}$ defined by

$$\mathbb{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

Definition 8.7. We define the *general linear group of* $\mathbb{C}$ to be the group

$$\mathrm{GL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z},\ ad - bc = \pm 1 \right\}.$$

We define the *special linear group* of $\mathbb{C}$ to be the normal subgroup of $\mathrm{GL}_2(\mathbb{Z})$ defined by

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

Sometimes, we might denote $\mathrm{SL}_2(\mathbb{Z})$ by simply Γ.

Define $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Lemma 8.8. *The group Γ is generated by S and T.*

Proof. Just notice that $S^2 = -\mathrm{Id}$ and then follow the proof of [7, Proposition III.1.4]. □

We define an action of the group $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{P}^1_{\mathbb{C}}$ in the following way. For every $z \in \mathbb{H}$ and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we define:

$$gz := \frac{az+b}{cz+d},$$
$$g\infty := \frac{a}{c},$$

where $z := (z:1)$ and $\infty := (1:0)$.

Lemma 8.9. *The action of* $\mathrm{SL}_2(\mathbb{Z})$ *on* $\mathbb{P}^1_{\mathbb{C}}$ *is well defined. Furthermore, it preserves* $\mathbb{H}$.

Proof. Exercise. □

As $\mathbb{H}$ is preserved by the action of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, we can consider the action induced on it, and hence consider the quotient $\mathbb{H}/\Gamma$. Let $\mathcal{F}$ be the region of the upper-half plane defined as

$$\mathcal{F} := \{z \in \mathbb{H} \ : \ |z| \geq 1 \text{ and } -\frac{1}{2} \leq \Re(z) < \frac{1}{2}\}.$$

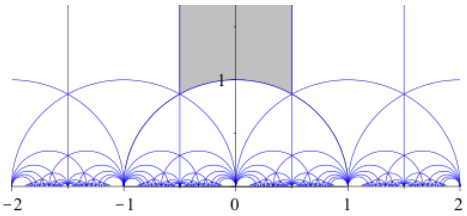


Figure 8. A visual rendition of the region $\mathcal{F}$ (the one in grey). The boundaries of other fundamental domains are also shown (the blue lines).

Lemma 8.10. *The region* $\mathcal{F}$ *is a fundamental domain of* $\mathbb{H}/\Gamma$.

Proof. Let z be any point in $\mathbb{H}$. Use a power T^j of T to move z to a point z' inside the strip $-\frac{1}{2} \leq \Re(z) < \frac{1}{2}$. If it is outside the unit circle, then it is in $\mathcal{F}$; otherwise use S to move the point outside the unit circle, and the again a power T^k to move it inside the strip. Go on like this until you get a point in $\mathcal{F}$. We leave the details of the proof as an exercise. (Note that they can be found in [7, Proposition 1]) □

8.3. **The j-function.** In Subsection 7.2 we have seen how to construct an elliptic curves starting from a complex lattice. We used this construction to define the j-invariant of a lattice (cf. Remark 7.18). In this subsection we will justify such a name and we will see how to extend this definition to a complex function.

Lemma 8.11. *Two complex lattices are homothetic if and only if they have the same* j *invariant.*

Proof. Let Λ_1 and Λ_2 two complex lattices, and assume they are homothetic, that is, there is a $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 = \Lambda_2$. Then $G_{2k}(\Lambda_2) = \alpha^{-2k} G_{2k}(\Lambda_1)$. From this it immediately follows that $j(\Lambda_2) = j(\Lambda_1)$.
On the other hand, if two lattices have the same j-invariant, the elliptic curves associated to them have the same j-invariant and, by Proposition 2.18, they are isomorphic. As they are both in (short) Weierstrass form, by Lemma 2.14 it follows

that there exists a $u \in \mathbb{C}^*$ such that t_u is the isomorphism between the two elliptic curves. This implies that $g_2(\Lambda_2) = g_2(\Lambda_1)/u^4$ and $g_3(\Lambda_2) = g_3(\Lambda_1)/u^6$. Then $g_k(u\Lambda_1) = g_k(\Lambda_2)$, for $k = 2, 3$. Using the relation $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, one can prove that this implies $\wp(z, u\Lambda_1) = \wp(z, \Lambda_2)$, for every $z \in \mathbb{C}$. So in particular, the two Weierstrass functions have the same set of poles, namely $\Lambda_2 = u\Lambda_1$. □

Lemma 8.12. *Every lattice is homothetic to a lattice $\langle 1, \tau\rangle$ with $\tau \in \mathbb{H}$.*

Proof. Let $\{w_1, w_2\}$ be any basis of Λ, and assume $\tau := w_2/w_1 \in \mathbb{H}$ (if this is not the case, take $\tau := -w_2/w_1$). Then $\langle 1, \tau\rangle$ is homothetic to Λ, via the multiplication by $1/w_1$. □

Lemma 8.13. *Let Λ_1, Λ_2 be the lattices generated by $\{1, w_1\}$ and $\{1, w_2\}$, respectively, with $w_1, w_2 \in \mathbb{C}$. Then the two lattices are homothetic if and only if $w_2 = \frac{aw_1+b}{cw_1+d}$, for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$.*

Proof. By Corollary 8.3 we know that two lattices are homothetic if and only if there is a $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_2 = \Lambda_1$. Then there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{aligned} \alpha &= a + bw_1 \\ \alpha w_2 &= c + dw_1 \\ ad - bc &= \pm 1. \end{aligned}$$

The statement follows by noticing that $w_2 = \frac{\alpha w_2}{\alpha}$. □

Corollary 8.14. *Let Λ_1, Λ_2 be the lattices generated by $\{1, w_1\}$ and $\{1, w_2\}$, respectively, with $w_1, w_2 \in \mathbb{H}$. Then the two lattices are homothetic if and only if $w_2 = \frac{aw_1+b}{cw_1+d}$, for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.*

Proof. The condition of preserving $\mathbb{H}$ implies that $ad - bc = 1$. □

Let τ be a complex number in $\mathbb{H}$. We define the complex lattice associated to τ as the lattice $\Lambda_\tau = \langle 1, \tau\rangle$.

Definition 8.15. We define the j-function as the function of $\mathbb{H}$ defined by

$$\begin{aligned} j \colon \mathbb{H} &\to \mathbb{C} \\ \tau &\mapsto j(\tau) := 1728 \frac{g_2(\Lambda_\tau)^3}{g_2(\Lambda_\tau)^3 + 27 g_3(\Lambda_\tau)^2}. \end{aligned}$$

Remark 8.16. For computational purposes, it might be useful to state the Laurent series in terms of $q = \exp(2\pi i\tau)$ associated to the j-function:

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots .$$

Lemma 8.17. *Let γ be an element of $\mathrm{SL}_2(\mathbb{Z}) = \Gamma$ and $\tau \in \mathbb{H}$. Then $j(\gamma\tau) = j(\tau)$.*

Proof. It immediately follows from Lemma 8.11 and Corollary 8.14. □

Lemma 8.17 tells us that the j-function induces a function on the quotient $\mathbb{H}/\Gamma$.

Proposition 8.18. *The function $\mathbb{H}/\Gamma \to \mathbb{C}$ induced by j is a bijection.*

Proof. Here we follow [6, Proof of Theorem 3.6]. The injectivity comes from Corollary 8.14. We are left to prove the surjectivity. We will show it by proving that the image $j(\mathbb{H})$ is both open and closed in $\mathbb{C}$. Then, by the connectedness of $\mathbb{C}$, the result will follow.
As j is a non-constant holomorphic function on $\mathbb{H}$, its image is open in $\mathbb{C}$.
Let $j = \lim_{n\to\infty} j(z_n)$ be a limit point of $j(\mathbb{H})$ in $\mathbb{C}$. Without loss of generality, we may and do assume that all the z_n lie in $\mathcal{F}$. If the values $\Im(z)$ are bounded, the sequence $\{z_n\}$ lie in a bounded subset of $\mathcal{F}$, that is compact. Hence they converge to a limit point $z \in \mathbb{H}$ and so $j = j(z) \in j(\mathbb{H})$. So assume that the values $\Im(z_n)$ are not bounded. Then we can pass to a subsequence and assume $\lim_{n\to\infty} \Im(z_n) = +\infty$. Then

$$\lim_{n\to\infty} g_2(z_n) = \frac{4\pi^4}{3}$$
$$\lim_{n\to\infty} g_3(z_n) = \frac{8\pi^6}{27},$$

and so

$$\lim_{n\to\infty} \Delta(z_n) = \lim_{n\to\infty} (g_2(z_n)^3 - 27g_3(z_n)^3) = 0,$$

from which it follows that $j = \lim_{n\to\infty} |j(z_n)| = \infty$, contradicting the assumption that the $j(z_n)$ converge. □

We are now ready to prove the Uniformization theorem.

Proof of Theorem 7.21. By Proposition 8.18 we know that, up to homotheties, there exists a unique lattice Λ such that $j(\Lambda) = \frac{a^3}{a^3-27b^2}$. This means that the elliptic curve $E_\Lambda \colon y^2 = x^3 - g_2/4x - g_3/4$ is isomorphic to the elliptic curve given by $y^2 = x^3 + a/4x + b/4$ and so there is a $u \in \mathbb{C}$ such that $g_2(\Lambda) = u^{-4}a$ and $g_3(\Lambda) = u^{-6}b$. Then the lattice $\frac{1}{u}\Lambda$ is the one required in the statement. □

8.4. **Exercises.**

6.1 Prove Proposition 8.5.
6.2 Prove Lemma 8.9.
6.3 Find in $\mathcal{F}$ an $\mathrm{SL}_2(\mathbb{Z})$-representative of $\frac{1+2i}{100}$.
6.4 Let E be a complex elliptic curve given by a Legendre equation

$$E \colon y^2 = x(x-1)(x-\lambda).$$

(a) Prove that there is a $k \in \mathbb{C} - \{0, \pm 1\}$ such that E can be put in the Jacobi equation

$$E \colon y^2 = (1-x^2)(1-k^2x^2).$$

[Hint: consider a transformation of the form $x' = (ax+b)/(cx+d)$ and $y' = ey/(cx+d)$ for appropriate $a, b, c, d, e \in \mathbb{C}$.]
(b) For a given value of λ find all possible values of k, and vice versa.
(c) Express $j(E)$ in terms of k.

References

[1] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves*. Undergraduate Texts in Mathematics, Springer, Cham, second ed., 2015.
[2] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second ed., 2009.

[3] R. Hartshorne, *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.
[4] S. Lang, *Algebra*, vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third ed., 2002.
[5] D. J. H. Garling, *A course in Galois theory*. Cambridge University Press, Cambridge, 1986.
[6] P. Stevenhagen, "Elliptic curves." Notes available at `http://pub.math.leidenuniv.nl/~luijkrmvan/elliptic/2011/ec.pdf`, 2008.
[7] N. Koblitz, *Introduction to elliptic curves and modular forms*, vol. 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second ed., 1993.