# ELLIPTIC FUNCTIONS AND ELLIPTIC CURVES

## (A Classical Introduction)

**Jan Nekovář**

### 0. Introduction

**(0.0)** Elliptic curves are perhaps the simplest 'non-elementary' mathematical objects. In this course we are going to investigate them from several perspectives: analytic (= function-theoretic), geometric and arithmetic.

Let us begin by drawing some parallels to the 'elementary' theory, well-known from the undergraduate curriculum.

**(0.0.1) Function theory:** (below, $R(x,y)$ is a rational function)

| Elementary theory | This course |
|---|---|
| $\arcsin, \arccos$<br>$\int R(x, \sqrt{f(x)})\,dx, \quad \deg(f) = 2$ | elliptic integrals<br>$\int R(x, \sqrt{f(x)})\,dx, \quad \deg(f) = 3, 4$ |
| $\sin, \cos$<br>(periodic with period $2\pi$) | elliptic functions<br>(doubly periodic with periods $\omega_1, \omega_2$) |

**(0.0.2) Geometry:**

| Elementary theory | This course |
|---|---|
| conics (e.g. circle, parabola ...)<br>$g(x,y) = 0, \quad \deg(g) = 2$ | elliptic curves<br>$g(x,y) = 0, \quad \deg(g) = 3$<br>(e.g. $y^2 = f(x), \quad \deg(f) = 3$) |
| | families of elliptic curves<br>(parametrized by modular functions) |

**(0.0.3) Arithmetic:**

| Elementary theory | This course |
|---|---|
| Pythagorean triples<br>$a^2 + b^2 = c^2 \qquad (a, b, c \in \mathbf{N})$ | rational solutions of<br>$g(x,y) = 0, \quad \deg(g) = 3$ |
| division of the circle (roots of unity)<br>cyclotomic fields | division values of elliptic functions<br>two-dimensional Galois representations<br>complex multiplication |

**(0.0.4) Elementary theory from a non-elementary viewpoint.** In the rest of this Introduction we are going to look at the left hand columns in 0.0.1-3 from an 'advanced' perspective, which will be subsequently used to develop the theory from the right hand columns.

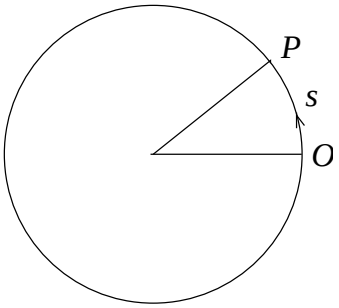
## 0.1. The circle

Consider the unit circle

$$C : x^2 + y^2 = 1$$

with a distinguished point $O = (1, 0)$.

**(0.1.0) Transcendental parametrization of the circle.** The points on $C$ can be parametrized by the (oriented) arclength $s$ measured from the point $O$:




The formulas

$$(ds)^2 = (dx)^2 + (dy)^2, \quad 0 = d(x^2 + y^2) = 2(x\,dx + y\,dy)$$

yield

$$dx = -\frac{y}{x}\,dy, \quad (ds)^2 = \frac{(dy)^2}{x^2}, \quad ds = \frac{dy}{x} = -\frac{dx}{y},$$

hence

$$s = \int_0^y \frac{dt}{\sqrt{1-t^2}}, \tag{0.1.0.0}$$

with the inverse function

$$y = y(s) = \sin(s)$$

and

$$x = x(s) = \frac{dy}{ds} = \cos(s),$$

i.e.

$$P = (x(s), y(s)) = (\cos(s), \sin(s)).$$

**(0.1.1) Addition of points on $C$ ("abelian group law").** We can use the parametrization from (0.1.0) to add points on $C$ by adding their corresponding arclengths from $O$. In other words, if we are given two points

$$P_j = (x_j, y_j) = (\cos(s_j), \sin(s_j)) \qquad (j = 1, 2)$$

on $C$ corresponding to $s_1$ resp. $s_2$, we let

$$P = P_1 \boxplus P_2 = (\cos(s_1 + s_2), \sin(s_1 + s_2))$$

be the point of $C$ corresponding to $s_1 + s_2$. This makes the points of the circle $C$ into an abelian group with neutral element $O$.

The addition formulas

$$\begin{aligned}\cos(s_1+s_2) &= \cos(s_1)\cos(s_2) - \sin(s_1)\sin(s_2)\\ \sin(s_1+s_2) &= \cos(s_1)\sin(s_2) + \cos(s_2)\sin(s_1)\end{aligned} \tag{0.1.1.0}$$

for the *transcendental* functions $\cos, \sin$ becomes *algebraic* when written in terms of the coordinates of the points on $C$:

$$(x_1, y_1) \boxplus (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \tag{0.1.1.1}$$

(and similarly for the inverse $-(x, y) = (x, -y)$). If we consider (0.1.0.0) as a *definition* of the (inverse of) sin, then the formulas (0.1.1.0-1) can be written as

$$\int_0^{y_1} \frac{dt}{\sqrt{1-t^2}} + \int_0^{y_2} \frac{dt}{\sqrt{1-t^2}} = \int_0^{y_3} \frac{dt}{\sqrt{1-t^2}}, \tag{0.1.1.2}$$

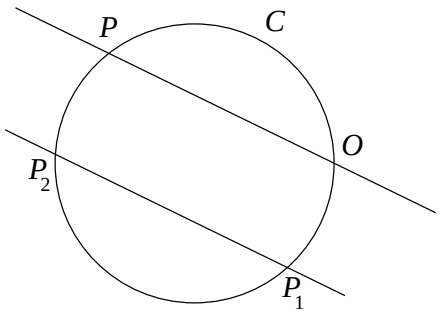
where

$$y_3 = y_1\sqrt{1-y_2^2} + y_2\sqrt{1-y_1^2}. \tag{0.1.1.3}$$

Let us repeat the key point once again: (0.1.1.2) is an addition formula for the *transcendental* function $\arcsin(y)$ (defined as the integral of the algebraic function $1/\sqrt{1-t^2}$), given by an *algebraic* rule (0.1.1.3).

Is this just an accident, or a special case of some general principle? We shall come back to this question several times during the course.

**(0.1.2) Geometric description of the group law on $C$.** There is a simple geometric way to construct the point $P = P_1 \boxplus P_2$:




draw a line through $O$ parallel to the line $P_1P_2$; its second intersection with $C$ (apart from $O$) is $P = P_1 \boxplus P_2$.

**(0.1.3) Exercise.** *Why is the statement in 0.1.2 true? What happens if $P_1 = P_2$?*

## 0.2. A rigorous formulation

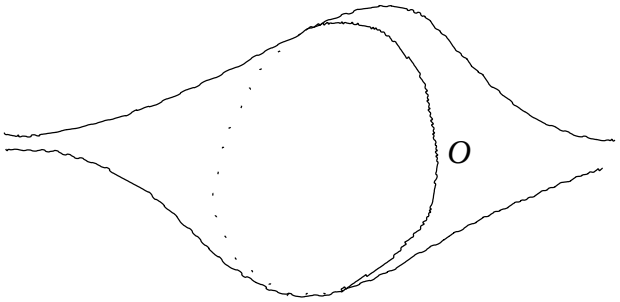
Attentive readers will have noticed that the discussion in Sect. 0.1 was not completely correct. The problem lies in the square root $\sqrt{1-y^2}$, whis is not a single-valued function. How does one keep track of the correct square root?

**(0.2.0) The idea of a Riemann surface.** The solution, proposed by Riemann, is very simple: one works, in the complex domain, with *both* square roots simultaneously. This means that the set of the real points of the circle $C$

$$C(\mathbf{R}) = \{(x, y) \in \mathbf{R}^2 \,|\, x^2 + y^2 = 1\}$$

(previously denoted simply by $C$) should be considered as a subset of its complex points

$$C(\mathbf{C}) = \{(x, y) \in \mathbf{C}^2 \,|\, x^2 + y^2 = 1\} :$$




The set $C(\mathbf{C})$ is a "Riemann surface", realized as a (ramified) two-fold covering of $\mathbf{C}$ by the projection map $p_2(x,y) = y$. The function $p_1(x,y) = x$ (resp. the differential $\omega = dy/x = -dx/y$) is a well-defined (i.e. single-valued) holomorphic function (resp. holomorphic differential) on $C(\mathbf{C})$, replacing the multivalued function $\sqrt{1-y^2}$ (resp. differential $dy/\sqrt{1-y^2}$) from 0.1.

Informally, a Riemann surface is an object on which one can define holomorphic (resp. meromorphic) functions and differentials in one complex variable. Riemann surfaces are natural domains of definitions of (holomorphic) functions that would otherwise be multivalued when considered as functions defined on open subsets of $\mathbf{C}$ (such as $\sqrt{1-y^2}$ in the above example). We shall recall basic concepts of this theory in I.3 below.

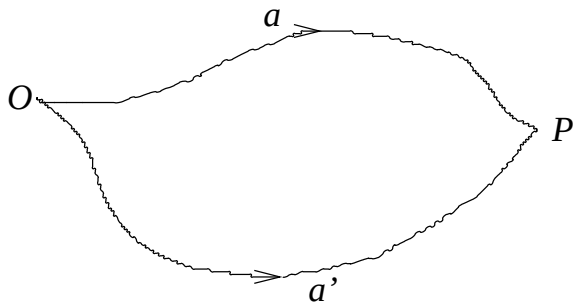
**(0.2.1) The Abel-Jacobi map.** In our new formulation, the integral (0.1.0.0) should be replaced by

$$\int_O^P \omega = \int_O^P \frac{dy}{x}, \tag{0.2.1.0}$$

where $P = (x_P, y_P) \in C(\mathbf{C})$ is a fixed complex point on $C$. At this point another ambiguity appears: the integral (0.2.1.0) depends not just on the point $P$, but also on the choice of a path (say, piece-wise infinitely differentiable)

$$a : O \rightsquigarrow P.$$

What happens if we choose another path $a' : O \rightsquigarrow P$:




The composite path $a \star (-a')$, which is obtained by going first from $O$ to $P$ along $a$ and then from $P$ to $O$ along $-a'$ ($= a'$ in the opposite direction), is then a closed path. As

$$d\omega = 0$$

(which is true for every holomorphic differential on every Riemann surface), Stokes' theorem

$$\int_{\partial A} \omega = \int_A d\omega = 0$$

implies that the integral

$$\int_b \omega$$

along any *closed* path $b$ (more generally, along any differentiable 1-cycle $b$) depends only on the homology class of $b$ in the homology group

$$[b] \in H_1(C(\mathbf{C}), \mathbf{Z}).$$

In our case,

$$H_1(C(\mathbf{C}), \mathbf{Z}) = \mathbf{Z}[\gamma]$$

is an infinite cyclic group generated by the homology class of the cycle $\gamma = C(\mathbf{R})$ (say, with the positive orientation). This means that

$$[a \star (-a')] = n[\gamma]$$

for some integer $n \in \mathbf{Z}$, hence the ambiguity of the integral (0.2.1.0)

$$\int_a \omega - \int_{a'} \omega = n \int_\gamma \omega = 2\pi n \in 2\pi\mathbf{Z}$$

is an integral multiple of the 'period of $\omega$ along $\gamma$', namely

$$\int_\gamma \omega = 2 \int_{-1}^{1} \frac{dt}{\sqrt{1-t^2}} = 2\pi.$$

To sum up, the integral (0.2.1.0) is well-defined only modulo the group of periods

$$\{ \int_b \omega \mid [b] \in H_1(C(\mathbf{C}), \mathbf{Z}) \} = 2\pi\mathbf{Z}.$$

The corresponding 'Abel-Jacobi map'

$$C(\mathbf{C}) \longrightarrow \mathbf{C}/2\pi\mathbf{Z}, \qquad P \mapsto \int_O^P \omega \ (\mathrm{mod}\, 2\pi\mathbf{Z}) \tag{0.2.1.1}$$

is then a complex variant of arcsin.

**(0.2.2) Exercise.** *Show that the map (0.2.1.1) defines a bijection* $C(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}/2\pi\mathbf{Z}$ *(resp.* $C(\mathbf{R}) \xrightarrow{\sim} \mathbf{R}/2\pi\mathbf{Z}$*), the inverse of which is given by the map* $s \mapsto (\cos(s), \sin(s))$.

**(0.2.3) A useful substitution.** Using the complex variable $z = x + iy$, one can identify the set of real points $C(\mathbf{R})$ of the circle with the subset

$$\{z \in \mathbf{C}^* \mid z\overline{z} = 1\} \subset \mathbf{C}^*$$

of the multiplicative group of $\mathbf{C}$. The discussion from 0.2.1 then applies to $\mathbf{C}^*$ and the holomorphic differential $dz/z$ on $\mathbf{C}^*$, with period

$$\int_\gamma \frac{dz}{z} = 2\pi i$$

(as $H_1(\mathbf{C}^*, \mathbf{Z}) = \mathbf{Z}[\gamma]$). The corresponding variant of (0.2.1.1) is the (bijective) logarithm map

$$\log : \mathbf{C}^* \longrightarrow \mathbf{C}/2\pi i\mathbf{Z}, \qquad P \mapsto \int_1^P \frac{dz}{z} \ (\mathrm{mod}\, 2\pi i\mathbf{Z}), \tag{0.2.3.0}$$

which restricts to a bijection between $C(\mathbf{R})$ and $2\pi i\mathbf{R}/2\pi i\mathbf{Z}$ and whose inverse is given by exp.

### 0.3. Geometry of the circle

In this section we consider only geometric properties of $C$ involving rational functions of the coordinates $x$ and $y$, not the transcendental parametrization by $(\cos(s), \sin(s))$.

**(0.3.0) Projectivization of $C$.** Writing the affine coordinates $x, y$ in the form $x = X/Z, y = Y/Z$, where $X, Y, Z$ are the homogeneous coordinates in the projective plane $\mathbf{P}^2(\mathbf{C})$, we embed the affine circle $C$ into its projectivization

$$\widetilde{C} : X^2 + Y^2 = Z^2,$$

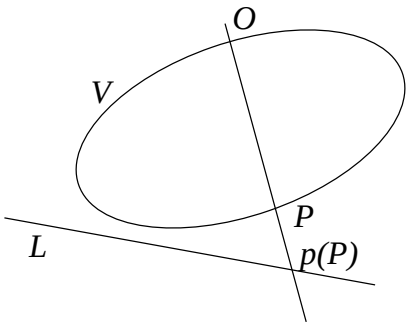
which is obtained from $C$ by adding two points at infinity

$$\widetilde{C}(\mathbf{C}) \cap \{Z = 0\} = \{(1 : \pm i : 0)\}.$$

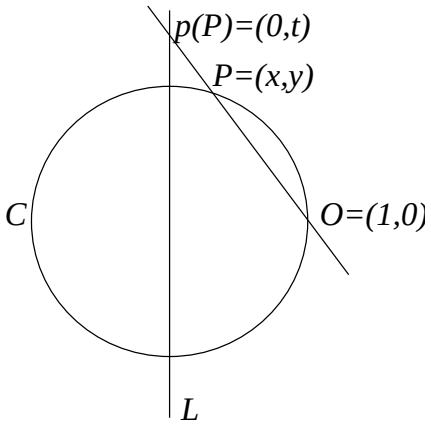
**(0.3.1) Circle = line.** This is one of the small miracles that occur in the projective world. In fact, much more is true (if you are not sure about the precise definitions, see I.3.7 below):

**(0.3.1.0) Exercise.** *If $V \subset \mathbf{P}^2_F$ is a smooth projective conic over a field $F$, $O \in V(F)$ an $F$-rational point of $V$ and $L \subset \mathbf{P}^2_F$ an $F$-rational line not passing through $O$, then the central projection from $O$ to $L$ defines an isomorphism of curves (over $F$)*

$$p : V \xrightarrow{\sim} L \ (\xrightarrow{\sim} \mathbf{P}^1_F)$$




**(0.3.1.1) Example.** $F = \mathbf{Q}$, $V = \widetilde{C} : X^2 + Y^2 = Z^2$, $L : X = 0$:




As

$$x^2 + y^2 = 1, \quad y = (1 - x)t,$$

a short calculation yields

$$x = \frac{t^2-1}{t^2+1}, \quad y = \frac{2t}{t^2+1}, \quad t = \frac{y}{1-x} = \frac{1+x}{y}. \tag{0.3.1.1.0}$$

These formulas define $p$ on the affine parts of $\widetilde{C}$ resp. $L$; using homogeneous coordinates $x = X/Z, y = Y/Z$ and $t = u/v$, we see that the inverse of $p$ is given by the formula

$$p^{-1} : (u : v) \mapsto (X : Y : Z) = (u^2 - v^2 : 2uv : u^2 + v^2).$$

Note that $p$ induces a bijection between $C(\mathbf{C}) - \{O\}$ and $\mathbf{C} - \{\pm i\}$, sends $O$ to the point at infinity ($t = \infty$) of $L$ and $p((1 : \pm i : 0)) = \mp i$.

**(0.3.1.2) Exercise.** *Can one generalize 0.3.1.0 to higher dimensions, e.g. to the case of smooth quadrics $V \subset \mathbf{P}^3_F$ (such as $X_0^2 + X_1^2 + X_2^2 = X_3^2$, if 2 is invertible in $F$)?*

## 0.4. Pythagorean triples

It is time to turn our attention to number theory (at last!).

**(0.4.0)** A **Pythagorean triple** $a, b, c$ is a solution of the diophantine equation

$$a^2 + b^2 = c^2, \qquad (a, b, c \in \mathbf{N});$$

it is *primitive* if $\gcd(a, b, c) = 1$. The first few primitive Pythagorean triples are

$$\begin{aligned} 3^2 + 4^2 &= 5^2 \\ 5^2 + 12^2 &= 13^2 \\ 8^2 + 15^2 &= 17^2 \\ 7^2 + 24^2 &= 25^2. \end{aligned} \tag{0.4.0.0}$$

Each Pythagorean triple defines a rational point $(a/c, b/c) \in C(\mathbf{Q})$ on the circle. Conversely, a rational point $(x, y) \in C(\mathbf{Q})$ with $xy \neq 0$ defines a unique primitive Pythagorean triple $a, b, c$ satisfying $(|x|, |y|) = (a/c, b/c)$.

The set of (primitive) Pythagorean triples has a well-known explicit description, which can be deduced by many different methods. We shall recall only three of them:

**(0.4.1) Geometric method.** One can explicitly describe the rational points on $C$ as follows.

**(0.4.1.0)** The isomorphism $p^{-1} : \mathbf{P}^1 \xrightarrow{\sim} \widetilde{C}$ from 0.3.1.1 is defined over $\mathbf{Q}$, hence induces a bijection between the sets of rational points

$$p^{-1} : \mathbf{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\} \xrightarrow{\sim} \widetilde{C}(\mathbf{Q}) = C(\mathbf{Q}),$$

given by the formula

$$p^{-1} : t = \frac{u}{v} \mapsto \left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2}\right) = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right) \tag{0.4.1.0.0}$$

(and $p^{-1}(\infty) = O = (1, 0)$).

**(0.4.1.1) Exercise.** *Show that (0.4.1.0.0) yields the following parametrization (up to a permutation of $a$ and $b$) of all Pythagorean triples:*

$$a = (u^2 - v^2)w, \quad b = 2uvw, \quad c = (u^2 + v^2)w, \quad u, v, w \in \mathbf{N}, \quad u > v, \quad \gcd(u, v) = 1.$$

*Where does the permutation of $a$ and $b$ enter the picture?*

**(0.4.2) Algebraic method.** The following statement is a special case of "Hilbert's Theorem 90".

**(0.4.2.0) Exercise.** *If $L/K$ is a finite Galois extension of fields with $\mathrm{Gal}(L/K)$ cyclic, then the sequence*

$$L^* \xrightarrow{1-\sigma} L^* \xrightarrow{N_{L/K}} K^*,$$

*where $\sigma$ is a generator of $\mathrm{Gal}(L/K)$, is exact. In other words, for $\lambda \in L^*$,*

$$\lambda \cdot \sigma(\lambda) \cdot \sigma^2(\lambda) \cdots \sigma^{n-1}(\lambda) = 1 \iff (\exists \mu \in L^*)\ \lambda = \frac{\mu}{\sigma(\mu)}.$$

**(0.4.2.1) Special case:** $K = \mathbf{Q}$, $L = \mathbf{Q}(i)$, $\lambda = x + iy$ $(x, y \in \mathbf{Q})$, $\sigma(\lambda) = x - iy$. Then

$$N_{L/K}(\lambda) = x^2 + y^2 = 1 \iff (\exists u, v \in \mathbf{Q})\ \lambda = \frac{u + iv}{u - iv},$$

which is equivalent to

$$x + iy = \frac{(u + iv)^2}{(u - iv)(u + iv)} = \frac{u^2 - v^2}{u^2 + v^2} + i\frac{2uv}{u^2 + v^2},$$

which is nothing but the formula (0.4.1.0.0)! This observation leads to an elegant description

$$a + ib = (u + iv)^2 \tag{0.4.2.1.0}$$

of all primitive Pythagorean triples (up to a permutation of $a$ and $b$):

$$\begin{aligned} (2 + i)^2 &= 3 + 4i \\ (3 + 2i)^2 &= 5 + 12i \\ (4 + 3i)^2 &= 7 + 24i \\ (4 + i)^2 &= 15 + 8i. \end{aligned} \tag{0.4.2.1.1}$$

**(0.4.3) Arithmetic method.** This is based on the factorization

$$(a + ib)(a - ib) = a^2 + b^2 = c^2.$$

**(0.4.3.0) Arithmetic of Gaussian integers.** The ring

$$\mathbf{Z}[i] = \{x + iy \,|\, x, y \in \mathbf{Z}\}$$

is a unique factorization domain with units

$$\mathbf{Z}[i]^* = \{\pm 1, \pm i\}.$$

A prime number $p$ factors into a product of irreducible factors in $\mathbf{Z}[i]$ as follows:

(i) $2 = (-i)(1 + i)^2$, with $1 + i$ irreducible.
(ii) If $p \equiv 3 \pmod 4$, then $p$ is irreducible.
(iii) If $p \equiv 1 \pmod 4$, then $p = \pi\overline{\pi}$, where $\pi = u + iv$, $u^2 + v^2 = p$; both $\pi$ and $\overline{\pi}$ are irreducible.

**(0.4.3.1) Exercise.** *If $a, b, c$ is a primitive Pythagorean triple, then $c$ is odd and $\gcd(a + ib, a - ib) = 1$ in $\mathbf{Z}[i]$. Deduce that either $a + ib = d^2$ or $b + ia = d^2$ is a square of some $d \in \mathbf{Z}[i]$; writing $d = u + iv$, we obtain again (0.4.2.1.0).*

**(0.4.4)** Do the methods from 0.4.1-3 generalize? Try to apply them to the following questions.

**(0.4.4.0) Exercise.** *Suppose that we replace the square in (0.4.2.1.0) by a higher power. What is the arithmetical meaning of the numbers we obtain, such as*

$$(2+i)^3 = 2+11i, \quad (3+2i)^3 = -9+46i\,?$$

*Are they again solutions of some diophantine equations? If yes, are there any other solutions?*

**(0.4.4.1) Exercise.** *Let $d \in \mathbf{Z}$, $\sqrt{d} \notin \mathbf{Z}$. Find all solutions of*

$$x^2 - dy^2 = 1 \qquad\qquad (x, y \in \mathbf{Q}).$$

**(0.4.4.2) Exercise.** *Can one use 0.3.1.2 to describe explicitly all rational points on the $n$-dimensional unit sphere, i.e. all solutions of*

$$x_0^2 + x_1^2 + \cdots + x_n^2 = 1 \qquad\qquad (x_0, \ldots, x_n \in \mathbf{Q})?$$

## 0.5. The group law on the circle revisited

**(0.5.0) Multiplication formulas for the group law.** For an integer $n \geq 1$, put

$$[n](x,y) = \underbrace{(x,y) \boxplus \cdots \boxplus (x,y)}_{n \text{ factors}}$$

and

$$[-n](x,y) = [n](x,-y)$$

(= multiplication by $n$ (resp. $-n$) in the sense of the group law on $C$). The expression $[n](x,y)$ is given by a pair of polynomials of degree $n$ with integral coefficients, the first few of which are

$$\begin{aligned}
[1](x,y) &= (x,y)\\
[2](x,y) &= (2x^2-1, 2xy)\\
[3](x,y) &= (4x^3-3x, 3y-4y^3)\\
[4](x,y) &= (8x^4-8x^2+1, 8x^3y-4xy)\\
[5](x,y) &= (16x^5-20x^3+5, 16y^5-20y^3+5y).
\end{aligned}$$

Note that

$$[-3](x,y) \equiv (x^3, y^3) \pmod 3, \quad [5](x,y) \equiv (x^5, y^5) \pmod 5.$$

The following exercise shows that this is no accident.

**(0.5.1) Exercise (Congruences for the multiplication).** *Let $p > 2$ be a prime; put $p^* = (-1)^{(p-1)/2}p$. Then*

$$[p^*](x,y) \equiv (x^p, y^p) \pmod p.$$

*[Hint: use the substitution $z = x + iy$.]*

**(0.5.2) Exercise.** (i) *For every (commutative) ring $A$, the formula (0.1.1.1) defines a structure of an abelian group on*

$$C(A) = \{(x,y) \in A^2 \mid x^2 + y^2 = 1\}.$$

(ii) *If 2 is invertible in $A$ and there exists $\lambda \in A$ satisfying $\lambda^2 + 1 = 0$, then the formula*

$$(x,y) \mapsto z = x + \lambda y$$

*defines an isomorphism of abelian groups*

$$C(A) \xrightarrow{\sim} A^*$$

*(here $A^*$ denotes the multiplicative group of invertible elements of $A$).*
(iii) *Assume that $F$ is a field of characteristic $\mathrm{char}(F) \neq 2$ over which the polynomial $\lambda^2 + 1$ is irreducible. For a fixed root $\sqrt{-1}$ of $\lambda^2 + 1 = 0$ (contained in some extension of $F$), the map*

$$(x, y) \mapsto z = x + \sqrt{-1}y$$

*defines an isomorphism of abelian groups*

$$C(F) \xrightarrow{\sim} \mathrm{Ker}\left(N_{F(\sqrt{-1})/F} : F(\sqrt{-1})^* \longrightarrow F^*\right);$$

*the latter group is isomorphic to $F(\sqrt{-1})^*/F^*$ [Hint: see (0.4.2.0).]*

**(0.5.3) Exercise (Structure of $C(F)$ for finite fields).** *Let $p > 2$ be a prime and $\overline{\mathbf{F}}_p$ an algebraic closure of $\mathbf{F}_p$.*
(i) *Describe the structure of $C(\overline{\mathbf{F}}_p)$ as an abstract abelian group.*
(ii) *For each $n \geq 1$, describe the structure of $C(\mathbf{F}_{p^n})$, using 0.5.2.*
(iii) *Describe the structure of $C(\mathbf{F}_{p^n})$, using (i) and 0.5.1. [Hint: $\mathbf{F}_{p^n}^* = \{a \in \overline{\mathbf{F}}_p^* \,|\, a^{p^n-1} = 1\}$.]*
(iv) *Show that*

$$\exp\left(\sum_{n=1}^{\infty} \frac{|C(\mathbf{F}_{p^n})|}{n} T^n\right) = \begin{cases} \frac{1-T}{1-pT}, & \text{if } p \equiv 1 \pmod 4 \\ \frac{1+T}{1-pT}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

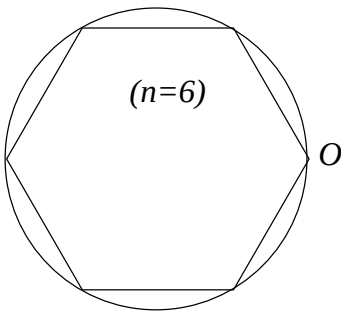
**(0.5.4) Exercise (Structure of $C(\mathbf{Q})$).** (i) *The torsion subgroup of $C(\mathbf{Q})$ is equal to*

$$C(\mathbf{Q})_{tors} = \{(\pm 1, 0), (0, \pm 1)\}.$$

(ii) *The quotient group $C(\mathbf{Q})/C(\mathbf{Q})_{tors}$ is a free abelian group with countably many generators. Can one explicitly describe a set of its (free) generators? [Hint: combine 0.4.2 with 0.4.3.0.]*

## 0.6. Galois theory

**(0.6.0) Division of the circle (Gauss).** For every integer $n \geq 1$, the points dividing the circumference of the (real) circle $C(\mathbf{R})$ into $n$ equal parts




form the $n$-torsion subgroup of $C$

$$C(\mathbf{R})_n = \{(x, y) \in C(\mathbf{R}) \,|\, [n](x, y) = O\} \ (= C(\mathbf{C})_n). \tag{0.6.0.0}$$

Under the transcendental parametrization

$$(\cos, \sin) : \mathbf{R}/2\pi\mathbf{Z} \xrightarrow{\sim} C(\mathbf{R}),$$

the subgroup $C(\mathbf{R})_n$ corresponds to $\frac{1}{n}2\pi\mathbf{Z}/2\pi\mathbf{Z}$; the formula (0.6.0.0) implies that the coordinates of points in $C(\mathbf{R})_n$ are algebraic numbers of degree $\leq n$.

It is more convenient to use the isomorphism 0.2.3 (+ 0.5.2)

$$C(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}^*, \quad (x, y) \mapsto z = x + iy,$$

under which $C(\mathbf{R})_n = C(\mathbf{C})_n$ corresponds to the group of $n$-th roots of unity $\mu_n = \mu_n(\mathbf{C})$; here we use the notation

$$\mu_n(A) = \{x \in A \,|\, x^n = 1\}$$

for any (commutative) ring $A$.

The field $\mathbf{Q}(\mu_n)$ generated over $\mathbf{Q}$ by the elements of $\mu_n$ is, in fact, generated by any primitive $n$-th root of unity (i.e. a generator of the cyclic group $\mu_n$). These primitive roots of unity form a subset $\mu_n^0 = \{\zeta^a \,|\, a \in (\mathbf{Z}/n\mathbf{Z})^*\} \subset \mu_n$ (for fixed $\zeta \in \mu_n^0$) of cardinality $\varphi(n)$; they are the roots of the $n$-th *cyclotomic polynomial*

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^0} (X - \zeta).$$

The first few polynomials $\Phi_n(X)$ are equal to

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1, \quad \Phi_4(X) = X^2 + 1,$$
$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1, \quad \Phi_6(X) = X^2 - X + 1, \quad \Phi_{12}(X) = X^4 - X^2 + 1.$$

**(0.6.1) Exercise (Properties of $\Phi_n$).** (i) *The polynomial $\Phi_n(X)$ is equal to*

$$\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)},$$

*where $\mu(d)$ is the Möbius function*

$$\mu(d) = \begin{cases} 0, & \text{if } d \text{ is not square-free} \\ (-1)^l, & \text{if } d \text{ is a product of } l \geq 0 \text{ distinct primes.} \end{cases}$$

(ii) *The polynomial $\Phi_n(X)$ has coefficients in $\mathbf{Z}$.*
(iii) *If $n = p^k$ is a prime power, then $\Phi_n(X)$ is irreducible over $\mathbf{Q}$. [Hint: Consider $\Phi_{p^k}(X + 1)$.]*
*(iv) *If $n = p^k$ is a prime power and $p \nmid m$, then $\Phi_n(X)$ is irreducible over $\mathbf{Q}(\mu_m)$. [Hint: Combine the method from (iii) with elementary algebraic number theory.]*
(v) *For each $n \geq 1$, $\Phi_n(X)$ is irreducible over $\mathbf{Q}$.*

**(0.6.2) The Galois representation on $\mu_n$.** It follows from 0.6.1(ii) and (iv) that $\mathbf{Q}(\mu_n)$ is the splitting field of $\Phi_n(X)$ (hence Galois) over $\mathbf{Q}$, of degree

$$[\mathbf{Q}(\mu_n) : \mathbf{Q}] = \deg(\Phi_n) = |\mu_n^0| = |(\mathbf{Z}/n\mathbf{Z})^*| = \varphi(n).$$

The action of any field automorphism $\sigma \in \mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$ of $\mathbf{Q}(\mu_n)$ (over $\mathbf{Q}$) preserves $\mu_n$ and commutes with its group law (= multiplication). It follows that its action on $\mu_n$ is given by

$$\sigma : \zeta \mapsto \zeta^a \qquad (\forall \zeta \in \mu_n)$$

for some element

$$a = \chi_n(\sigma) \in (\mathbf{Z}/n\mathbf{Z})^* = GL_1(\mathbf{Z}/n\mathbf{Z}).$$

The corresponding map

$$\chi_n : \mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q}) \longrightarrow GL_1(\mathbf{Z}/n\mathbf{Z})$$

(the "cyclotomic character") is a homomorphism of groups; it is perhaps the simplest example of a *Galois representation*.

The Galois theory of the extension $\mathbf{Q}(\mu_n)/\mathbf{Q}$ can be summed up by the statement that $\chi_n$ is an *isomorphism* (it is injective almost by definition, and its domain and target have the same number of elements).

**(0.6.3) Kummer theory.** Suppose that $F$ is a field containing $\mu_n$ (i.e. the set $\mu_n(F) = \{x \in F \,|\, x^n = 1\}$ has $n$ elements) and $a \in F^*$. Fix a separable closure $F^{sep}$ of $F$ and an element $b = \sqrt[n]{a} \in F^{sep}$ satisfying $b^n = 1$. Then the formula

$$\sigma \mapsto \sigma(\sqrt[n]{a})/\sqrt[n]{a}$$

defines a homomorphism of groups

$$\delta_a : \mathrm{Gal}(F^{sep}/F) \longrightarrow \mu_n(F),$$

which does not depend on the choice of $b$ and whose kernel is equal to $\mathrm{Gal}(F^{sep}/F(\sqrt[n]{a}))$. The map

$$a \mapsto \delta_a$$

defines an homomorphism of abelian groups

$$\delta : F^* \longrightarrow \mathrm{Hom}(\mathrm{Gal}(F^{sep}/F), \mu_n(F))$$

with kernel

$$\mathrm{Ker}(\delta) = F^{*n}.$$

The special case of Hilbert's Theorem 90 stated in 0.4.2.0 implies that the map $\delta$ is surjective, hence induces an isomorphism of abelian groups

$$\delta : F^*/F^{*n} \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(F^{sep}/F), \mu_n(F)). \tag{0.6.1.0}$$

In fact, it is possible to give a unified interpretation of both the logarithm map (0.2.3.0) and the isomorphism (0.6.1.0).

# I. Elliptic Integrals and Elliptic Functions

This chapter covers selected topics from classical theory of (hyper)elliptic integrals and elliptic functions. It is impossible to give an exhaustive list of references for this enormous subject. For general theory (and practice), the following books can be useful: [McK-Mo], [La], [Web].

## 1. Elliptic Integrals

By definition, an *elliptic* (resp. *hyperelliptic*) integral is an expression of the form

$$I = \int R(x, \sqrt{f(x)})\, dx,$$

where $R(x, y) \in \mathbf{C}(x, y)$ is a rational function and $f(x) \in \mathbf{C}[x]$ a square-free polynomial of degree $n = 3, 4$ (resp. $n > 4$).

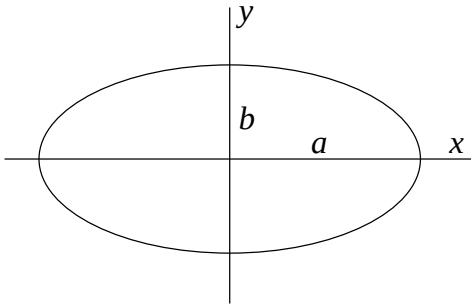
If $n = 1, 2$, the integral is an elementary function; for example, if $f(x) = 1 - x^2$, then the substitution $x = (t^2 - 1)/(t^2 + 1)$ from 0.3.1.2 transforms $I$ into an integral of a rational function of $t$.

Where do (hyper)elliptic integrals occur in nature? We begin by two geometric examples.

### 1.1 Arclength of an ellipse

**(1.1.1)** An ellipse

$$\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 = 1 \qquad (a \geq b > 0)$$




can be parametrized by $x = a\cos\theta, y = b\sin\theta$. Its arclength $s$ satisfies

$$(ds)^2 = (dx)^2 + (dy)^2 = (a^2\sin^2\theta + b^2\cos^2\theta)(d\theta)^2 = a^2(1 - k^2\cos^2\theta)(d\theta)^2,$$

where $k^2 = 1 - b^2/a^2$. Normalizing the long axis of the ellipse by taking $a = 1$, we have $b = \sqrt{1 - k^2}$ and

$$dx = -\sin\theta\, d\theta, \quad (dx)^2 = (1 - x^2)(d\theta)^2, \quad (ds)^2 = \frac{1 - k^2x^2}{1 - x^2}(dx)^2,$$

hence

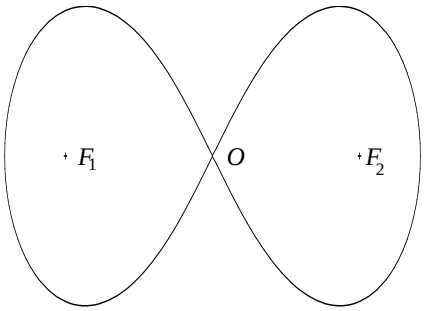
$$s = \int \sqrt{\frac{1 - k^2x^2}{1 - x^2}}dx = \int \frac{1 - k^2x^2}{\sqrt{(1 - x^2)(1 - k^2x^2)}}dx.$$

### 1.2 Arclength of a lemniscate

**(1.2.1) Lemniscate.** Recall that, given two distinct points $F_1, F_2$ in the plane, the *lemniscate* with the foci $F_1, F_2$ is the set of points $P$ in the plane satisfying

$$|F_1P| \cdot |F_2P| = |F_1O| \cdot |F_2O|, \tag{1.2.1.1}$$

where $O$ is the midpoint of the segment $F_1F_2$.




Choosing a coordinate system in which $O = (0,0), F_1 = (-a,0), F_2 = (a,0)$, the (square of the) equation (1.2.1.1) for the point $P = (x,y)$ can be written as

$$a^4 = ((x+a)^2 + y^2)((x-a)^2 + y^2) = (x^2 + y^2 + a^2)^2 - (2ax)^2,$$

which is equivalent to

$$(x^2 + y^2)^2 = 2a^2(x^2 - y^2).$$

For $a = 1/\sqrt{2}$ we obtain a particularly nice equation

$$(x^2 + y^2)^2 = x^2 - y^2,$$

which becomes

$$r^2 = \cos 2\theta \tag{1.2.1.2}$$

in the polar coordinates $x = r\cos\theta$, $y = r\sin\theta$.

**(1.2.2) Arclength.** The equation (1.2.1.2) implies that $rdr = -\sin(2\theta)d\theta$, hence

$$r^2(dr)^2 = (2\sin^2\theta)(2\cos^2\theta)(d\theta)^2 = (1-r^2)(1+r^2)(d\theta)^2 = (1-r^4)(d\theta)^2.$$

It follows that the arclength $s$ of the lemniscate satisfies

$$(ds)^2 = (dr)^2 + r^2(d\theta)^2 = (dr)^2\left(1 + \frac{r^4}{1-r^4}\right) = \frac{(dr)^2}{1-r^4},$$

hence

$$s = \int \frac{dr}{\sqrt{1-r^4}}. \tag{1.2.2.1}$$

## 1.3 The lemniscate sine

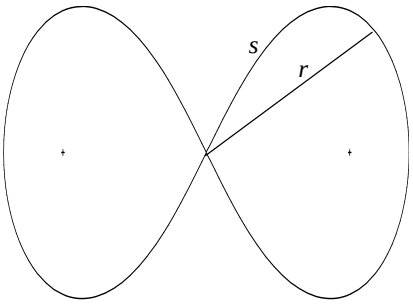
**(1.3.1)** The sine function is defined as the inverse of the integral (0.1.0.0) that computes the arclength of the unit circle. In a similar vein, the 'sine of the lemniscate' $sl$ is defined as the inverse function to the integral (1.2.2.1). In other words, if

$$s = \int_0^r \frac{dt}{\sqrt{1-t^4}}, \tag{1.3.1.1}$$

then we put

$$r = sl(s),$$

which corresponds to the following picture:




As in 0.2, the integral (1.3.1.1) can be interpreted as an integral on the Riemann surface

$$V(\mathbf{C}) = \{(x, y) \,|\, y^2 = 1 - x^4\}$$

associated to the curve

$$V : y^2 = 1 - x^4. \tag{1.3.1.2}$$

As a result, the function $sl(s)$ will make sense also for complex values of $s$.

The substitution $t := -t$ (resp. $t = it$) implies that

$$sl(-s) = -sl(s), \quad sl(is) = i\, sl(s). \tag{1.3.1.3}$$

Denoting by

$$\frac{\Omega}{2} = \int_0^1 \frac{dt}{\sqrt{1 - t^4}}$$

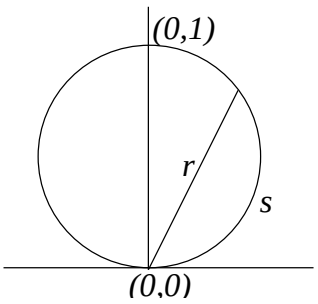
the length of the 'quarter-arc' of the lemniscate between $(0, 0)$ and $(1, 0)$, then

$$sl(\frac{\Omega}{2}) = 1, \quad sl(\Omega) = 0, \quad sl(\Omega + s) = sl(-s) = -sl(s). \tag{1.3.1.4}$$

**(1.3.2)** The previous discussion should be compared to the corresponding picture for the circle, given by the equation

$$r = \sin\theta$$

in polar coordinates (this is a slightly different parametrization than in 0.1):




In this case

$$(ds)^2 = (dr)^2 + r^2(d\theta)^2 = (\cos^2\theta + \sin^2\theta)(d\theta)^2 = (d\theta)^2 = \frac{(dr)^2}{1-r^2},$$

hence

$$s = \int_0^r \frac{dt}{\sqrt{1-t^2}} = \theta, \quad r = \sin(s), \quad \frac{\pi}{2} = \int_0^1 \frac{dt}{\sqrt{1-t^2}}$$
$$\sin(\frac{\pi}{2}) = 1, \quad \sin(\pi) = 0, \quad \sin(\pi + s) = \sin(-s) = -\sin(s).$$

**(1.3.3)** The main difference between the functions sin and *sl* is the following: the sine function is periodic

$$\sin(s + 2\pi) = \sin(s)$$

with periods $2\pi\mathbf{Z}$, while the formulas (1.3.1.3-4) imply that

$$sl(s + 2\Omega) = sl(s)$$
$$sl(s + 2i\Omega) = i\, sl(s/i + 2\Omega) = i\, sl(s/i) = sl(s),$$

hence *sl* is *doubly periodic*, with periods (at least) in the square lattice $2\Omega\mathbf{Z} + 2i\Omega\mathbf{Z}$.

### 1.4 Fagnano's doubling formula for *sl*

**(1.4.1)** Recall that integrals of the form $\int R(x, \sqrt{1-x^2})\, dx$ can be computed by the substitution

$$x = \frac{2t}{1+t^2}, \quad 1 - x^2 = \left(\frac{1-t^2}{1+t^2}\right)^2. \tag{1.4.1.1}$$

The lemniscatic integral (1.3.1.1) involves $\sqrt{1-r^4}$ instead of $\sqrt{1-x^2}$, so it would be fairly natural to try to apply the substitution (1.4.1.1) with

$$x = r^2, \qquad t = u^2,$$

i.e. change the variables by

$$r^2 = \frac{2u^2}{1+u^4}, \qquad r = \frac{\sqrt{2}u}{\sqrt{1+u^4}}, \qquad 1 - r^4 = \left(\frac{1-u^4}{1+u^4}\right)^2.$$

It follows that

$$2r\,dr = \frac{4u(1-u^4)}{(1+u^4)^2}\, du, \qquad dr = \frac{\sqrt{2}(1-u^4)}{(1+u^4)^{3/2}}\, du,$$

hence

$$\frac{dr}{\sqrt{1-r^4}} = \sqrt{2}\frac{du}{\sqrt{1+u^4}} \tag{1.4.1.1}$$

This is almost the same integral as before, except for the factor $\sqrt{2}$ and a change of sign inside the square root. In order to get back the minus sign, we make another substitution

$$u = e^{2\pi i/8} v = \frac{1+i}{\sqrt{2}} v \qquad (\Longrightarrow u^4 = -v^4),$$

which yields

$$r = \frac{(1+i)v}{\sqrt{1-v^4}}, \qquad 1 - r^4 = \left(\frac{1+v^4}{1-v^4}\right)^2 \tag{1.4.1.2}$$

and

$$\frac{dr}{\sqrt{1-r^4}} = (1+i)\frac{dv}{\sqrt{1-v^4}}. \tag{1.4.1.3}$$

**(1.4.2) Doubling formula for the sine.** An elementary variant of (1.4.1.2-3) is provided by the doubling formula for the sine function: if $u = \sin(s)$, then

$$\sin(2s) = 2u\sqrt{1-u^2}. \tag{1.4.2.1}$$

The substitution

$$y = 2u\sqrt{1-u^2}$$

therefore yields

$$y^2 = 4u^2(1-u^2), \qquad 1 - y^2 = (1-2u^2)^2, \qquad 2ydy = 8u(1-2u^2)\,du,$$

hence

$$\frac{dy}{\sqrt{1-y^2}} = 2\frac{du}{\sqrt{1-u^2}}. \tag{1.4.2.2}$$

Integrating the formula (1.4.2.2), we obtain the identity

$$\int_0^y \frac{dt}{\sqrt{1-t^2}} = 2s = 2\int_0^u \frac{dt}{\sqrt{1-t^2}}$$

we started with.

**(1.4.3) Complex multiplication by $1+i$.** In the similar vein, the formula (1.4.1.3) can be integrated into

$$\int_0^r \frac{dt}{\sqrt{1-t^4}} = (1+i)x = (1+i)\int_0^v \frac{dt}{\sqrt{1-t^4}},$$

where

$$x = \int_0^v \frac{dt}{\sqrt{1-t^4}};$$

the first identity in (1.4.1.2) then can be rewritten as

$$sl((1+i)x) = \frac{(1+i)sl(x)}{\sqrt{1-sl^4(x)}}. \tag{1.4.3.1}$$

This formula, which should be compared with (1.4.2.1), is the simplest non-trivial example of what is usually referred to as "complex multiplication".

**(1.4.4) The doubling formula.** In order to obtain a formula for multiplication by $2 = (1+i)(1-i)$, we iterate the substitution (1.4.1.2), with $i$ replaced by $-i$:

$$v = \frac{(1-i)w}{\sqrt{1-w^4}}, \qquad 1 - v^4 = \left(\frac{1+w^4}{1-w^4}\right)^2, \qquad \frac{dv}{\sqrt{1-v^4}} = (1-i)\frac{dw}{\sqrt{1-w^4}},$$

which yields

$$r = \frac{(1+i)(1-i)w}{\sqrt{1-v^4}\sqrt{1-w^4}} = \frac{2w\sqrt{1-w^4}}{1+w^4}, \qquad \frac{dr}{\sqrt{1-r^4}} = 2\frac{dw}{\sqrt{1-w^4}}.$$

This can be rewritten as

$$sl(2x) = \frac{2sl(x)\sqrt{1-sl^4(x)}}{1+sl^4(x)}, \tag{1.4.4.1}$$

which is Fagnano's doubling formula.

**(1.4.5) Addition formula.** Is there an *addition formula* for $sl(x_1+x_2)$ in terms of $sl(x_1)$ and $sl(x_2)$ which would specialize to (1.4.4.1) if $x_1 = x_2 = x$? A natural guess, namely that

$$sl(x_1+x_2) \stackrel{?}{=} \frac{sl(x_1)\sqrt{1-sl^4(x_2)} + sl(x_2)\sqrt{1-sl^4(x_1)}}{1+sl^2(x_1)sl^2(x_2)}, \tag{1.4.5.1}$$

which is equivalent to the addition formula

$$\int_0^{w_1} \frac{dt}{\sqrt{1-t^4}} + \int_0^{w_2} \frac{dt}{\sqrt{1-t^4}} = \int_0^{w_3} \frac{dt}{\sqrt{1-t^4}} \ (\mathrm{mod}\, 2\Omega\mathbf{Z} + 2i\Omega\mathbf{Z})$$

with

$$w_3 = \frac{w_1\sqrt{1-w_2^4} + w_2\sqrt{1-w_1^4}}{1+w_1^2w_2^2}, \tag{1.4.5.2}$$

turns out to be correct.

**(1.4.6) Euler's addition formula.** In fact, Euler discovered and proved a common generalization of both (1.4.5.2) and the addition formula for $\sin(s)$. Euler's result is the following: if

$$f(t) = 1 + mt^2 + nt^4,$$

then

$$\int_0^u \frac{dt}{\sqrt{f(t)}} + \int_0^v \frac{dt}{\sqrt{f(t)}} = \int_0^w \frac{dt}{\sqrt{f(t)}} \tag{1.4.6.1}$$

(modulo periods), where

$$w = \frac{u\sqrt{f(v)} + v\sqrt{f(u)}}{1-nu^2v^2}. \tag{1.4.6.2}$$

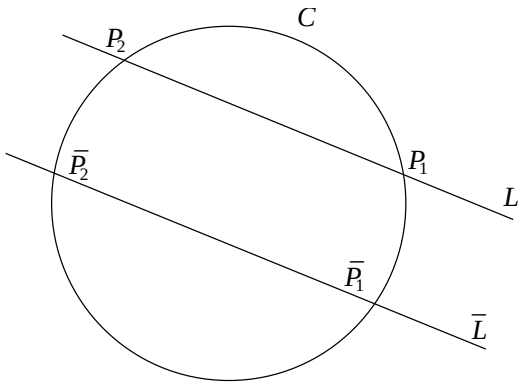
For $(m,n) = (-1,0)$ (resp. $= (0,-1)$) this reduces to the addition formula for sin (resp. for $sl$).

Euler's proof of (1.4.6.1-2) was based on a clever calculation, and therefore was not interesting at all (it can be found, e.g., in [Mar]). What was missing was a general principle behind various addition formulas, not a verification – however ingenious – of a particular formula. Such a principle was discovered by Abel; his approach will be discussed in the next section (where we also deduce Euler's formula from Abel's general results).

## 2. Abel's Method

### 2.1 Addition formulas for $\cos, \sin$ revisited

**(2.1.1)** We are going to analyze in great detail the geometric interpretation of the addition formulas for $\cos, \sin$ from 0.1.1-2:




if $L, \overline{L}$ are lines intersecting the circle $C(\mathbf{R})$ in pairs of points

$$L \cap C(\mathbf{R}) = \{P_1, P_2\}, \qquad \overline{L} \cap C(\mathbf{R}) = \{\overline{P}_1, \overline{P}_2\},$$

then (using the usual notation $\omega = dy/x = -dx/y$, $O = (1,0)$)

$$L \text{ is parallel to } \overline{L} \Longrightarrow \int_O^{P_1} \omega + \int_O^{P_2} \omega = \int_O^{\overline{P}_1} \omega + \int_O^{\overline{P}_2} \omega \pmod{2\pi\mathbf{Z}}. \tag{2.1.1.1}$$

Assuming that neither $L$ nor $\overline{L}$ is vertical, we can write their equations in the form

$$L : y = ax + b, \qquad \overline{L} : y = \overline{a}x + \overline{b}; \tag{2.1.1.2}$$

then

$$L \text{ is parallel to } \overline{L} \iff a = \overline{a}. \tag{2.1.1.3}$$

**(2.1.2) Exercise.** *Show that, conversely, (2.1.1.1) implies the addition formula (0.1.1.1). [Hint: Choose $\overline{L}$ such that $O \in \overline{L}$.]*

**(2.1.3)** We shall try to prove (2.1.1.1) algebraically, by computing the partial derivatives of its left hand side with respect to the parameters $a, b$. It will be natural to consider the parameters $a, b$ as having *complex* values.

Denoting the line $L$ from (2.1.1.2) by $L_{a,b}$, the coordinates $(x, y)$ of the points in the intersection $L_{a,b}(\mathbf{C}) \cap C(\mathbf{C})$ are the solutions of the equations

$$y = ax + b, \qquad x^2 + y^2 = 1;$$

thus $y$ is uniquely determined by $x$, which is in turn a root of the polynomial

$$F(x) = x^2 + (ax + b)^2 - 1 = (a^2 + 1)x^2 + 2abx + (b^2 - 1) = 0.$$

This is a quadratic equation of discriminant

$$\operatorname{disc}(F) = 4(a^2b^2 - (b^2 - 1)(a^2 + 1)) = 4(a^2 + 1 - b^2),$$

*unless* $a = \pm i$. What makes these two values of $a$ so special?

**(2.1.4) About $a = \pm i$.** The answer is simple if we pass to homogeneous coordinates: by Bézout's Theorem, every projective line in $\mathbf{P}^2(\mathbf{C})$ intersects the projectivization $\widetilde{C}(\mathbf{C})$ of the affine circle $C(\mathbf{C})$ in two points (if we count them with multiplicities). Recalling that $\widetilde{C}(\mathbf{C})$ has precisely two points at infinity $P_\pm = (1 : \pm i : 0)$, we see that the projectivization

$$\widetilde{L}_{a,b} : Y = aX + bZ$$

of the affine line $L_{a,b}$ contains $P_\pm$ if and only if $a = \pm i$. This implies that

$$[\widetilde{C}(\mathbf{C}) \cap \widetilde{L}_{a,b}(\mathbf{C}) = C(\mathbf{C}) \cap L_{a,b}(\mathbf{C})] \iff a \neq \pm i.$$

Perhaps we could remedy the situation by working with $\widetilde{C}$ and $\widetilde{L}_{a,b}$ from the very beginning? Unfortunately, the differential $\omega$ has a pole at each of the points $P = P_\pm$, which means that the integral

$$\int_O^P \omega$$

cannot be defined at them. As a result, we have to exclude the values $a = \pm i$ and work with a smaller parameter space

$$B = \{(a, b) \,|\, a, b \in \mathbf{C},\ a \neq \pm i\}.$$

Denote by

$$\Sigma = \{(a, b) \in B \,|\, a^2 + 1 - b^2 = 0\}$$

the "discriminant curve" of the polynomial $F$.

**(2.1.5) Intersecting $C$ with $L_{a,b}$.** If $(a, b) \in B$, then the discussion in 2.1.3 implies the following description of $C(\mathbf{C}) \cap L_{a,b}(\mathbf{C})$:

(2.1.5.1) If $(a, b) \notin \Sigma$, then the line $L_{a,b}(\mathbf{C})$ intersects $C(\mathbf{C})$ transversally at two points $P_j = (x_j, y_j)$ $(j = 1, 2)$, where $y_j = ax_j + b$,

$$F(x) = (a^2 + 1)(x - x_1)(x - x_2), \qquad x_1 + x_2 = -\frac{2ab}{a^2 + 1}, \qquad x_1 x_2 = \frac{b^2 - 1}{a^2 + 1}.$$

(2.1.5.2) If $(a, b) \in \Sigma$, then the line $L_{a,b}(\mathbf{C})$ is tangent to $C(\mathbf{C})$ at a point $P_1 = (x_1, y_1)$ (and has no other intersection with $C(\mathbf{C})$), where

$$F(x) = (a^2 + 1)(x - x_1)^2, \qquad x_1 = -a/b, \qquad y_1 = ax_1 + b = 1/b.$$

In order to emphasize the dependence of the points $P_j$ on the parameters, we sometimes write $P_j(a, b)$ for $P_j$. In the case (2.1.5.2), we formally denote $P_2 = P_1$.

**(2.1.6) The key calculation.** For $(a, b) \in B$, put

$$I(a, b) = \int_O^{P_1(a,b)} \omega + \int_O^{P_2(a,b)} \omega \ (\mathrm{mod}\, 2\pi\mathbf{Z}) \in \mathbf{C}/2\pi\mathbf{Z}.$$

In 2.1.7 we prove the following simple formula for the infinitesimal variation of $I(a, b)$, assuming that $(a, b) \notin \Sigma$:

$$dI(a, b) = I'_a\, da + I'_b\, db = \omega_1 + \omega_2, \qquad \omega_j = \begin{cases} dy_j/x_j, & \text{if } x_j \neq 0 \\ -dx_j/y_j, & \text{if } y_j \neq 0, \end{cases} \tag{2.1.6.1}$$

where $I'_a = \partial I/\partial a$ denotes the partial derivative with respect to $a$ (and similarly for $b$).

Perhaps the best way to understand this formula is to compute its right hand side: by differentiating the equations

$$x^2 + y^2 = 1, \qquad y = ax + b$$

satisfied by the pairs $(x_j, y_j)$ $(j = 1, 2)$ **with respect to all variables**, we obtain

$$2x\, dx + 2y\, dy = 0, \qquad dy = a\, dx + x\, da + db = -\frac{ay}{x}\, dy + x\, da + db,$$

hence

$$(x+ay)\frac{dy}{x} = x\,da + db.$$

As

$$x + ay = (a^2+1)x + ab,$$

we obtain

$$\omega_j = \frac{dy_j}{x_j} = \frac{x_j}{(a^2+1)x_j + ab}\,da + \frac{1}{(a^2+1)x_j+ab}\,db. \tag{2.1.6.2}$$

Combined with (2.1.6.1), this yields the following formulas for the partial derivatives of $I$ on $B - \Sigma$:

$$\begin{aligned} I'_a &= \frac{x_1}{(a^2+1)x_1+ab} + \frac{x_2}{(a^2+1)x_2+ab} = \frac{2x_1x_2(a^2+1)+ab(x_1+x_2)}{(a^2+1)^2x_1x_2+(a^2+1)ab(x_1+x_2)+a^2b^2} = \\ &= \frac{2(b^2-1)-2a^2b^2/(a^2+1)}{(a^2+1)(b^2-1)-2a^2b^2+a^2b^2} = \frac{2(b^2-a^2-1)/(a^2+1)}{b^2-a^2-1} = \frac{2}{a^2+1}, \\ I'_b &= \frac{1}{(a^2+1)x_1+ab} + \frac{1}{(a^2+1)x_2+ab} = \frac{(a^2+1)(x_1+x_2)+2ab}{b^2-a^2-1} = 0. \end{aligned}$$

As observed in 2.1.1-2, the vanishing of $I'_b = 0$ implies the addition formula (0.1.1.1). Our calculation is a priori valid for $(a,b) \in B - \Sigma$, and therefore establishes (0.1.1.1) only for $(x_1,y_1) \neq (x_2,y_2)$. However, both sides of

$$\int_O^{x_1,y_1} \omega + \int_O^{x_2,y_2} \omega = \int_O^{x_1x_2-y_1y_2,\,x_1y_2+x_2y_1} \omega \ (\mathrm{mod}\, 2\pi\mathbf{Z})$$

are holomorphic functions of $P_1 = (x_1,y_1)$ and $P_2 = (x_2,y_2)$, hence the formula is still valid if we let $P_1$ tend to $P_2$.

**(2.1.7)** In this section we give the promised proof of (2.1.6.1), which is just a variant of the fact that the derivative of the integral of a fuction is the function itself. For fixed $(a,b) \in B - \Sigma$, let $P_1 = (x_1,y_1) \neq P_2 = (x_2,y_2)$ be the intersection points of $L_{a,b}(\mathbf{C})$ with $C(\mathbf{C})$. For all values of $(\overline{a},\overline{b})$ in a sufficiently small neighbourhood $U$ of $(a,b)$ in $B - \Sigma$, the intersection points $\overline{P}_1 = (\overline{x}_1,\overline{y}_1) \neq \overline{P}_2 = (\overline{x}_2,\overline{y}_2)$ of $L_{\overline{a},\overline{b}}(\mathbf{C})$ with $C(\mathbf{C})$ are holomorphic functions of $(\overline{a},\overline{b})$ (by Theorem on Implicit Functions; see 3.4.2 below) and each $\overline{P}_j$ lies in a contractible neighbourhood $U_j$ of $P_j$. If $x_j \neq 0$ (resp. $y_j \neq 0$), we can also assume that $\overline{x}_j \neq 0$ (resp. $\overline{y}_j \neq 0$), by shrinking $U$ if necessary. We wish to compute the partial derivatives of

$$I(\overline{a},\overline{b}) = \int_O^{\overline{P}_1} \omega + \int_O^{\overline{P}_2} \omega$$

at $(a,b)$. If $x_j \neq 0$ (resp. $y_j \neq 0$), then

$$\int_O^{\overline{P}_j} \omega - \int_O^{P_j} \omega = \int_{P_j}^{\overline{P}_j} \omega = \int_{y_j}^{\overline{y}_j} \frac{dy}{x} \qquad \left(\text{resp.} \quad = \int_{x_j}^{\overline{x}_j} -\frac{dx}{y}\right).$$

This equality is to be understood as follows: we fix a path $p_j$ from $O$ to $P_j$ and a path $q_j$ from $P_j$ to $\overline{P}_j$ contained in $U_j$. As $U_j$ is contractible,

$$\int_{p_j \star q_j} \omega - \int_{p_j} \omega = \int_{q_j} \omega \in \mathbf{C}$$

does not depend on the choices of the paths.

Observing that

$$\frac{\partial}{\partial \overline{a}} \left( \int_{y_j}^{\overline{y}_j} \frac{dy}{x} \right) (a,b) = \frac{1}{x_j} \left( \frac{\partial \overline{y}_j}{\partial \overline{a}} \right) (a,b),$$

(and similarly for partial derivatives with respect to $\overline{b}$), we obtain

$$d \left( \int_{y_j}^{\overline{y}_j} \frac{dy}{x} \right) (a,b) = \frac{1}{x_j} \left( \frac{\partial \overline{y}_j}{\partial \overline{a}}(a,b)\, d\overline{a} + \frac{\partial \overline{y}_j}{\partial \overline{b}}(a,b)\, d\overline{b} \right) = \left( \frac{d\overline{y}_j}{\overline{x}_j} \right) (a,b), \tag{2.1.7.1}$$

at least in the case $x_j \neq 0$; if $x_j = 0$, then

$$d \left( \int_{y_j}^{\overline{y}_j} \frac{dy}{x} \right) (a,b) = \left( -\frac{d\overline{x}_j}{\overline{y}_j} \right) (a,b). \tag{2.1.7.2}$$

Taking the sum of (2.1.7.1) (resp. (2.1.7.2) if $x_j = 0$) over $j = 1, 2$ yields the formula (2.1.6.1), save for the notation: the variables from 2.1.6 did not have bars above them.

**(2.1.8)** What is a correct interpretation of the sum $\omega_1 + \omega_2$ in (2.1.6.1)? Put

$$S = \{(x, y, a, b) \,|\, (a,b) \in B,\, x^2 + y^2 = 1,\, y = ax + b\};$$

then the projection

$$p : S \longrightarrow B, \qquad\qquad p(x,y,a,b) = (a,b)$$

is a covering of degree 2, unramified above $B - \Sigma$ (and ramified above $\Sigma$). Viewing $\omega = dy/x = -dx/y$ as a holomorphic differential on $S$, then

$$\omega_1 + \omega_2 = p_* \omega$$

is the "trace" of $\omega$ with respect to the map $p$. The definition of $p_*$ above $B - \Sigma$ is not difficult (see ?? below), but its extension to the ramified region above $\Sigma$ requires some work. In our calculation of $dI(a,b)$ in 2.1.6, the term $b^2 - a^2 - 1$ disappeared from the denominators; this indicates that $p_*\omega$ should indeed make sense everywhere in $B$.

## 2.2 Example: Hyperelliptic integrals

Let us try to generalize the calculation from 2.1.6.

**(2.2.1)** The first thing that we need to understand is the vanishing of the sum

$$\frac{1}{(a^2+1)x_1 + ab} + \frac{1}{(a^2+1)x_2 + ab} = 0 \tag{2.2.1.1}$$

over the roots $x_1, x_2$ of the polynomial

$$F(x) = (a^2+1)x^2 + 2abx + (b^2 - 1).$$

Noting that

$$(a^2+1)x + ab = \frac{1}{2} F'(x),$$

we see that (2.2.1.1) is a special case of the following

**(2.2.2) Exercise.** *Let $F(x) \in \mathbf{C}[x]$ be a polynomial of degree $\deg(F) = n \geq 2$ with $n$ distinct roots $x_1, \ldots, x_n$, and $\varphi(x) \in \mathbf{C}[x]$ a polynomial of degree $\deg(\varphi) \leq n-2$. Then*

$$\sum_{j=1}^{n} \frac{\varphi(x_j)}{F'(x_j)} = 0.$$

**(2.2.3) Exercise.** *According to the calculation in 2.1.6,*

$$F'(x_1)F'(x_2) = 4((a^2+1)x_1 + ab)((a^2+1)x_2 + ab) = 4(b^2 - a^2 - 1) = \operatorname{disc}(F).$$

*Does this identity generalize to polynomials of arbitrary degree?*

**(2.2.4) Hyperelliptic integrals.** We are now ready to generalize the calculation from 2.1.6 (cf. [Web], Sect. 13). Instead of the circle $C$ we consider the curve

$$V : y^2 = f(x),$$

where $f(x) \in \mathbf{C}[x]$ is a polynomial of even degree $\deg(f) = 2m \geq 2$ with $2m$ distinct roots. We shall be interested in addition formulas for integrals of the form

$$\int_O^P \frac{x^k\,dx}{\sqrt{f(x)}} = \int_O^P \frac{x^k\,dx}{y}$$

on $V(\mathbf{C})$, where $O \in V(\mathbf{C})$ is fixed (for $k \geq 0$).

As $y^2 = f(x)$ on $V$, intersecting $V$ with a general family of curves

$$R_0(x,a) + R_1(x,a)y + \cdots + R_m(x,a)y^m = 0 \qquad (R_j \in \mathbf{C}[x,a])$$

(where $a = (a_1, \ldots, a_r)$) amounts to intersecting $V$ with a simpler family

$$D_a : P(x,a) - Q(x,a)y = 0,$$

where

$$P = R_0 + fR_2 + f^2R_4 + \cdots, \qquad -Q = R_1 + fR_3 + f^2R_5 + \cdots$$

are polynomials $P, Q \in \mathbf{C}[x,a] = \mathbf{C}[x, a_1, \ldots, a_r]$. The $x$-coordinates of the points in the intersection $V(\mathbf{C}) \cap D_a(\mathbf{C})$ are the roots of the polynomial

$$F(x,a) = P^2(x,a) - f(x)Q^2(x,a),$$

which generalizes the polynomial $F(x)$ from 2.1.6. We have

$$P(x,a) = p(a)\,x^{d_P} + \cdots, \qquad Q(x,a) = q(a)\,x^{d_Q} + \cdots, \qquad f(x) = r\,x^{2m} + \cdots,$$

where

$$d_P := \deg_x(P), \qquad d_Q := \deg_x(Q), \qquad p, q \in \mathbf{C}[a] - \{0\}, \qquad r \in \mathbf{C}^*.$$

We make the following assumptions:

(2.2.4.1) The degree of $F$ in the variable $x$ is equal to

$$\deg_x(F) = 2N := \max(\deg_x(P^2), \deg_x(fQ^2)) = 2\,\max(d_P, d_Q + m).$$

This is always true if $d_P \neq d_Q + m$; if $d_P = d_Q + m$, then this condition amounts to the requirement that

$$p(a)^2 - r\,q(a)^2 \in \mathbf{C}[a] - \{0\}.$$

(2.2.4.2) The discriminant $\mathrm{disc}_x(F)$ of $F$ with respect to the variable $x$ (a generalization of $4(b^2-a^2-1)$ from 2.1) is not identically equal to zero as a polynomial in $a$.

(2.2.4.3) The resultant $\mathrm{Res}_x(P,Q)$ of $P$ and $Q$ with respect to the variable $x$ is not identically equal to zero as a polynomial in $a$.

Put

$$H(a) = (p(a)^2 - r\,q(a)^2)\mathrm{disc}_x(F)\mathrm{Res}_x(P,Q), \qquad B = \{a \in \mathbf{C}^r \mid H(a) \neq 0\}.$$

The assumptions (2.2.4.1-3) imply that, for each $a \in B$, the polynomial $F(x,a)$ has $2N$ distinct roots $x_1, \ldots, x_{2N}$ depending on $a$ (as holomorphic functions of $a$), none of which is a root of the polynomial $Q(x,a)$. This means that

$$(\forall a \in B) \qquad V(\mathbf{C}) \cap D_a(\mathbf{C}) = \{P_1, \ldots, P_{2N}\}, \qquad P_j = P_j(a) = (x_j, y_j) = (x_j, P(x_j,a)/Q(x_j,a)).$$

**(2.2.5)** For $a \in B$ we can imitate the calculation from 2.1.6 to compute the infinitesimal variation

$$dI = I'_a\,da := I'_{a_1}\,da_1 + \cdots + I'_{a_r}\,da_r$$

of the sum

$$I(a) = \sum_{j=1}^{2N} \int_O^{P_j(a)} \frac{x^k\,dx}{y} \qquad\qquad (k \geq 0),$$

which should be understood as in 2.1.7: we consider only the values of $I(\overline{a})$ for $\overline{a} \in B$ lying in a sufficiently small neighbourhood of $a$, and we let the paths $O \rightsquigarrow P_j(\overline{a})$ vary only in small neighbourhoods of the endpoints. The differential $dI$ is then well defined and independent of the choices of the paths. A global definition of the integrals $I(a)$ requires a non-trivial analysis of their periods; see ?? below.

We begin by differentiating the equations

$$y^2 = f(x), \qquad yQ - P = 0,$$

obtaining

$$2y\,dy = f'_x\,dx, \qquad (yQ'_x - P'_x)\,dx + Q\,dy + (yQ'_a - P'_a)\,da = 0,$$

hence

$$\left(yQ'_x - P'_x + \frac{Qf'_x}{2y}\right)dx + (yQ'_a - P'_a)\,da = 0. \tag{2.2.5.1}$$

Differentiating $F = P^2 - fQ^2$ and using $yQ = P$, we see that

$$yQ'_x - P'_x + \frac{Qf'_x}{2y} = \frac{2fQQ'_x - 2PP'_x + Q^2f'_x}{2yQ} = -\frac{F'_x}{2yQ}.$$

Substituting to (2.2.5.1) we obtain

$$\frac{dx}{y} = \frac{2Q(yQ'_a - P'_a)}{F'_x}\,da = \frac{2(PQ'_a - QP'_a)}{F'_x}\,da,$$

hence

$$\sum_{j=1}^{2N} \left(\frac{x^k\,dx}{y}\right)_{(x_j,y_j)} = \sum_{j=1}^{2N} \left.\frac{2x^k(PQ'_a - QP'_a)}{F'_x}\right|_{x=x_j} da,$$

which implies (as in 2.1.7) that

$$\frac{\partial}{\partial a_l}\left(\sum_{j=1}^{2N}\int_O^{P_j(a)}\frac{x^k\,dx}{y}\right)=\sum_{j=1}^{2N}\frac{2x^k(PQ'_{a_l}-QP'_{a_l})}{F'_x}\Big|_{x=x_j}. \tag{2.2.5.2}$$

Combining (2.2.5.2) with Exercise 2.2.2, we obtain the following addition theorem (a special case of Abel's Theorem).

**(2.2.6) Proposition.** *If the assumptions (2.2.4.1-3) are satisfied, $k\geq 0$ and*

$$(\forall l=1,\dots,r)\qquad k+\deg_x(PQ'_{a_l}-QP'_{a_l})\leq 2N-2, \tag{2.2.6.1}$$

*then the sum $I(a)$, defined locally on $B$ after appropriate choices of the paths, is locally constant.*

**(2.2.7)** Let us analyze the condition (2.2.6.1) in more detail. Firstly,

$$PQ'_{a_l}-QP'_{a_l}=W_l(a)\,x^{d_P+d_Q}+\cdots,$$

where

$$W_l(a)=pq'_{a_l}-qp'_{a_l}=\begin{vmatrix} p & q\\ p'_{a_l} & q'_{a_l}\end{vmatrix}$$

is the Wronskian of $p,q\in\mathbf{C}[a_1,\dots,a_r]$ with respect to the variable $a_l$. This implies that

$$(\forall a\in B)\qquad \deg_x(PQ'_{a_l}-QP'_{a_l})=\begin{cases} d_P+d_Q, & \text{if } W_l(a)\neq 0\\ \leq d_P+d_Q-1, & \text{if } W_l(a)=0.\end{cases}$$

Secondly,

$$2N-2-(d_P+d_Q)=2\max(d_P,d_Q+m)-(d_P+d_Q)-2=\begin{cases} m-2, & \text{if } d_P=d_Q+m\\ \geq m-1, & \text{if } d_P\neq d_Q+m.\end{cases}$$

It follows that (2.2.6.1) is satisfied in each of the following cases:

(2.2.7.1) $\quad d_P\neq d_Q+m,\qquad 0\leq k\leq m-1.$

(2.2.7.2) $\quad d_P=d_Q+m,\qquad 0\leq k\leq m-2.$

(2.2.7.3) $\quad d_P=d_Q+m,\qquad 0\leq k\leq m-1,\qquad (\forall a\in B)\,(\forall l=1,\dots r)\qquad W_l(a)=0.$

The last condition is equivalent to

$$(\forall a,b\in B)\qquad \text{the vectors}\quad (p(a),q(a)),\ \ (p(b),q(b))\quad \text{are linearly dependent}$$

(which is a generalization of (2.1.1.3)).

In particular, if we fix the degrees $d_P,d_Q\geq 0$ and consider the intersections of $V$ with the universal family

$$C_{a,b}:(a_0+a_1x+\cdots+a_{d_P}x^{d_P})=y\,(b_0+b_1x+\cdots+b_{d_Q}x^{d_Q}) \tag{2.2.7.4}$$

(where $a_0,\dots,b_{d_Q}$ are independent variables), we obtain **common addition formulas** for all integrals

$$\int_O^P\frac{x^k\,dx}{y},$$

provided

$$\begin{aligned} &0\leq k\leq m-1, && d_P\neq d_Q+m\\ &0\leq k\leq m-2, && d_P=d_Q+m\\ &k=m-1, && d_P=d_Q+m, \qquad b_{d_Q}=c\,a_{d_P}\qquad (c\in\mathbf{C}^*\text{ constant}).\end{aligned} \tag{2.2.7.5}$$

**(2.2.8) Change of variables in hyperelliptic integrals.** Suppose that $f(x) \in \mathbf{C}[x]$ is a polynomial of degree $n \geq 1$ with $n$ distinct roots $\alpha_1, \ldots, \alpha_n$. For every invertible complex matrix

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{C}),$$

the change of variables

$$x = g(\overline{x}) = \frac{a\overline{x} + b}{c\overline{x} + d}$$

transforms $f(x)$ into

$$f\left(\frac{a\overline{x} + b}{c\overline{x} + d}\right) = (c\overline{x} + d)^{-n}\overline{f}(\overline{x})$$

and $dx$ into

$$d\left(\frac{a\overline{x} + b}{c\overline{x} + d}\right) = \frac{(ad - bc)\, d\overline{x}}{(c\overline{x} + d)^2},$$

where $\overline{f}(\overline{x}) \in \mathbf{C}[\overline{x}]$ is a polynomial of degree $n$ (or $n-1$) with the set of roots $\{g^{-1}(\alpha_1), \ldots, g^{-1}(\alpha_n)\} - \{\infty\}$. If $n = 2m$ is even, it follows that the hyperelliptic integral

$$\int R(x, \sqrt{f(x)})\, dx \qquad\qquad (R(x, y) \in \mathbf{C}(x, y))$$

is transformed into

$$\int \overline{R}(\overline{x}, \sqrt{\overline{f}(\overline{x})})\, d\overline{x} \qquad\qquad (R(\overline{x}, \overline{y}) \in \mathbf{C}(\overline{x}, \overline{y})).$$

If $m \geq 2$, then we can choose $g$ such that $g^{-1}$ maps three of the roots $\alpha_j$ into $0, \infty, 1$, which yields $\overline{f}$ of the form

$$\overline{f}(\overline{x}) = a\, \overline{x}(\overline{x} - 1) \prod_{j=1}^{2m-3} (\overline{x} - \beta_j).$$

In particular, for $n = 4$, we obtain the *Legendre normalization*:

$$\overline{f}(\overline{x}) = \overline{x}(\overline{x} - 1)(\overline{x} - \lambda).$$

Other normalizations of elliptic integrals were considered by Jacobi:

$$f(x) = (1 - x^2)(1 - k^2x^2)$$

(cf. 1.1) and Weierstrass:

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

(cf. 7.1.8 below).

## 2.3 Euler's addition formula

**(2.3.1)** Let us prove Euler's formula (1.4.6.1-2) by Abel's method. The formula involves the differential $\omega = dx/y$ on the Riemann surface $V(\mathbf{C})$, where $V$ is the curve

$$V : y^2 = f(x) = 1 + mx^2 + nx^4$$

(assuming that $f$ has four distinct roots). We shall consider intersections of $V$ with auxiliary curves

$$D_{a,b} : y = 1 + ax + bx^2.$$

The intersection $V(\mathbf{C}) \cap D_{a,b}(\mathbf{C})$ consists of the point $O = (0, 1)$ and three other points – possibly with multiplicities – $(x_j, y_j)$ $(j = 1, 2, 3)$, where

$$y_j = 1 + ax_j + bx_j^2$$

and $x_1, x_2, x_3$ are the roots of the polynomial

$$\frac{(1 + ax + bx^2)^2 - (1 + mx^2 + nx^4)}{x} = (b^2 - n)x^3 + 2abx^2 + (a^2 + 2b - m)x + 2a = \\ = (b^2 - n)(x - x_1)(x - x_2)(x - x_3).$$

It follows that

$$x_1 + x_2 + x_3 = -\frac{2ab}{b^2 - n} = bx_1x_2x_3,$$

hence

$$-x_3 = \frac{x_1 + x_2}{1 - bx_1x_2}.$$

Dividing the formulas

$$x_1y_2 - x_2y_1 = (x_1 - x_2) + b(x_1x_2^2 - x_1^2x_2) = (x_1 - x_2)(1 - bx_1x_2)$$
$$x_1^2y_2^2 - x_2^2y_1^2 = (x_1^2 - x_2^2)(1 - nx_1^2x_2^2)$$

by each other, we obtain

$$x_1y_2 + x_2y_1 = \frac{(x_1 + x_2)(1 - nx_1^2x_2^2)}{1 - bx_1x_2},$$

hence

$$-x_3 = \frac{x_1y_2 + x_2y_1}{1 - nx_1^2x_2^2}. \tag{2.3.1.1}$$

The special case of Abel's Theorem proved in 2.2.7 (for $m = 2$, $k = 0$, $d_P = 4$, $d_Q = 0$) implies that the sum

$$\int_O^{(x_1,y_1)} \omega + \int_O^{(x_2,y_2)} \omega + \int_O^{(x_3,y_3)} \omega \tag{2.3.1.2}$$

(modulo periods) is equal to a constant independent of $(a, b)$, at least if $x_1, x_2, x_3$ are distinct. Taking $a = 0$, we have $(x_1, y_1) = O$ and $(x_2, y_2) = (-x_3, y_3)$, which implies that the constant is equal to

$$\int_0^{x_2} \frac{dx}{\sqrt{f(x)}} + \int_0^{-x_2} \frac{dx}{\sqrt{f(x)}} = 0, \tag{2.3.1.3}$$

as $f(-x) = f(x)$. Combining (2.3.1.2-3), we obtain

$$\int_O^{(x_1,y_1)} \omega + \int_O^{(x_2,y_2)} \omega = \int_O^{(-x_3,y_3)} \omega \tag{2.3.1.4}$$

(modulo periods), with $-x_3$ given by (2.3.1.1). This is precisely Euler's formula, assuming that $x_1, x_2, x_3$ are distinct. However, the left hand side of (2.3.1.4) is a holomorphic function of $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in V(\mathbf{C})$, and so is the right hand side, provided the denominator in (2.3.1.1) does not vanish. This implies that (2.3.1.4) also holds in the case $(x_1, y_1) = (x_2, y_2)$, provided $nx_1^4 \neq 1$.

**(2.3.2) Question.** *We have found 4 intersection points of $V(\mathbf{C})$ and $D_{a,b}(\mathbf{C})$. According to Bézout's Theorem, the projective curves associated to $V$ and $D_{a,b}$ should have $2 \cdot 4 = 8$ intersection points. Where are the remaining $8 - 4 = 4$ points?*

**(2.3.3) Exercise.** *Let $f(x) = x^3 + Ax + B$ be a cubic polynomial with distinct roots. Show that Abel's method applies to the differential $\omega = dx/y$ on the curve $V : y^2 = f(x)$ and the family of lines $L_{a,b} : y = ax+b$. Deduce an explicit addition formula for the integral*

$$\int_O^P \frac{dx}{\sqrt{x^3 + Ax + B}}.$$

*Are some choices of the base point $O$ better than others?*

**(2.3.4) Exercise.** *Generalize the calculations from 2.2.5-7 to the case when $\deg(f) = 2m - 1 \geq 3$ is an arbitrary odd integer.*

### 2.4 General Remarks on Abel's Theorem

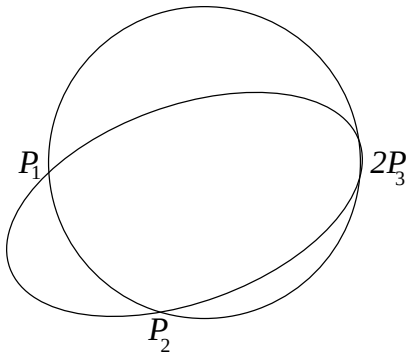
**(2.4.1)** Abel was interested in addition formulas for general integrals of the form

$$\int_O^P \omega,$$

where $\omega$ is an algebraic differential on the set of complex points $V(\mathbf{C})$ of an algebraic curve $V$, $O \in V(\mathbf{C})$ is a fixed base point and $P \in V(\mathbf{C})$ a variable point. His main insight was to consider sums

$$\int_O^{P_1(\lambda)} \omega + \cdots + \int_O^{P_d(\lambda)} \omega,$$

where $P_1(\lambda), \ldots, P_d(\lambda)$ are the intersection points of $V$ with an auxiliary algebraic curve $C_\lambda$, depending on a parameter $\lambda = (\lambda_1, \ldots, \lambda_r) \in \mathbf{C}^r$. More precisely, the points in the intersection $V(\mathbf{C}) \cap C_\lambda(\mathbf{C})$ naturally appear with multiplicities reflecting the order of contact between the two curves:




Formally, we consider $V(\mathbf{C}) \cap C_\lambda(\mathbf{C})$ as a "divisor" on $V(\mathbf{C})$, i.e. a formal linear combination

$$D(\lambda) = \sum_j n_j(\lambda)(P_j(\lambda)) \qquad\qquad (n_j(\lambda) \in \mathbf{Z},\ P_j(\lambda) \in V(\mathbf{C}))$$

(in our case all coefficients $n_j(\lambda)$ are positive) and put

$$\int_O^{D(\lambda)} \omega = \sum_j n_j(\lambda) \int_O^{P_j(\lambda)} \omega \tag{2.4.1.1}$$

(which is well defined modulo the periods of $\omega$).

**(2.4.2)** Abel's Theorem states that, for suitable differentials $\omega$ and certain families of auxiliary curves $C_\lambda$, the "Abel sum" (2.4.1.1) (modulo periods) does not depend on $\lambda$. This can be reformulated intrinsically as follows: geometric properties of $V$ and of the family $C_\lambda$ define an equivalence relation

$$D(\lambda) \sim D(\lambda')$$

on the intersection divisors, and the value of

$$\int_O^D \omega$$

(modulo periods) depends only on the equivalence class of the divisor $D$. We have seen several examples of this phenomenon:

**(2.4.3) Circle.** $V = C : x^2 + y^2 = 1$, $\omega = dy/x$, $C_\lambda = L_{a,b} : y = ax + b$, where $a \neq \pm i$ is *fixed* and $\lambda = b$ is variable.

**(2.4.4) Hyperelliptic integrals.** $V : y^2 = f(x)$, where $f(x)$ is a polynomial of even degree $2m \geq 4$ with distinct roots, $\omega = x^k\, dx/y$ $(0 \leq k \leq m-2)$,

$$C_\lambda = C_{a,b} : (a_0 + a_1 x + \cdots + a_{d_P} x^{d_P}) = y\,(b_0 + b_1 x + \cdots + b_{d_Q} x^{d_Q}).$$

This also works for $k = m-1$, if we require in addition that $b_{d_Q} = c\, a_{d_P}$ $(c \in \mathbf{C}^*$ constant) if $d_P = d_Q + m$.

**(2.4.5) Elliptic integrals.** $V : y^2 = f(x)$, where $f(x)$ is a polynomial of degree 3 with distinct roots, $\omega = dx/y$, $C_\lambda : y = ax + b$ $(\lambda = (a, b))$.

**(2.4.6) Questions:** (i) In each of the above examples, what exactly is the equivalence relation on divisors defined by the intersections with the family $C_\lambda$?

(ii) Does this equivalence relation admit an intrinsic description in terms of $V$ alone?

(iii) For which differentials does Abel's Theorem hold?

(iv) Conversely, if the integrals

$$\int_O^D \omega = \int_O^{D'} \omega$$

are equal (modulo periods) for sufficietly many differentials $\omega$, does it follow that $D \sim D'$? Consider, for example, the intersections of the circle $C(\mathbf{C})$ with the family of conics

$$C'_\mu : a_1 x^2 + a_2 xy + a_3 y^2 + a_4 x + a_5 y + a_6 = 0, \qquad \mu = (a_1, \ldots, a_6).$$

Denoting the intersection divisor $C(\mathbf{C}) \cap C'_\mu$ by $D'(\mu)$, under what conditions on $\mu_1, \mu_2$ does one have

$$\int_O^{D'(\mu_1)} \omega \equiv \int_O^{D'(\mu_2)} \omega \pmod{2\pi\mathbf{Z}}?$$

See 3.8 below for the answer.

## 3. A Crash Course on Riemann Surfaces

This section contains a brief survey of basic facts on Riemann Surfaces. More details can be found in ([Fo], Ch. 1, Sect. 1,2,9,10; [Fa-Kr 1], Ch. 1; [Ki], Ch. 5,6). For elementary properties of holomorphic functions in one variable we refer to ([Ru 2], Ch. 10). Complex manifolds of higher dimension are discussed in [Gr-Ha] and [Wei 1].

### 3.1 What is a Riemann surface?

**(3.1.1)** A Riemann surface is a geometric object $X$ locally isomorphic to an open subset of $\mathbf{C}$. These local pieces are glued together so that one can work with holomorphic (resp. meromorphic) functions and differentials globally on $X$. We have already encountered several examples of Riemann surfaces, such as $\mathbf{P}^1(\mathbf{C})$, $C(\mathbf{C})$ (= the complex points of the circle), $\mathbf{C}/2\pi\mathbf{Z}$ (= a cylinder), $\mathbf{C}/\mathbf{Z} + \mathbf{Z}i$ (= a torus). Here is the standard (fairly impenetrable) definition.

**(3.1.2) Definition.** *A* **Riemann surface** $X$ *is a connected Hausdorff topological space with countable basis of open sets, equipped with a (holomorphic) atlas (more precisely, an equivalence class of atlases). An* **atlas** *on $X$ consists of a set of* **local charts** $(U_\alpha, \phi_\alpha)$*, where $\{U_\alpha\}$ is an open covering of $X$ and $\phi_\alpha : U_\alpha \xrightarrow{\sim} \phi_\alpha(U_\alpha)$ is a homeomorphism between $U_\alpha$ and an open subset of $\mathbf{C}$. The local charts are required to be compatible in the following sense: for each pair $(U_\alpha, \phi_\alpha)$, $(U_\beta, \phi_\beta)$ of local charts, the transition function*

$$\phi_\beta \circ \phi_\alpha^{-1} : \phi_\alpha(U_\alpha \cap U_\beta) \longrightarrow \phi_\beta(U_\alpha \cap U_\beta)$$

*is holomorphic. Two atlases are* **equivalent** *if their union is also an atlas.*

**(3.1.3) Definition.** *Let $X$ be a Riemann surface. A* **local coordinate** *at a point $x \in X$ is a local chart $(U_\alpha, z_\alpha)$ satisfying $x \in U_\alpha$ and $z_\alpha(x) = 0$.*

**(3.1.4) Remarks and examples.** (1) One can replace $\mathbf{C}$ by $\mathbf{C}^n$ in 3.1.2; the geometric object $X$ is then called a *complex manifold of dimension $n$*.
(2) Morally, $X$ is constructed by gluing the open sets $\phi_\alpha(U_\alpha) \subset \mathbf{C}$ together along $\phi_\alpha(U_\alpha \cap U_\beta)$, using the transition functions $\phi_\beta \circ \phi_\alpha^{-1}$.
(3) If $z_\alpha$ is a local coordinate at $x \in X$, other local coordinates are given by power series $\sum_{n\geq 1} c_n z_\alpha^n$ with non-zero radius of convergence and $c_1 \neq 0$.
(4) An open connected subset $U \subset \mathbf{C}$ is a Riemann surface, with one chart $U \hookrightarrow \mathbf{C}$ given by the inclusion. For each $a \in U$, $z_\alpha(z) = z - a$ is a local coordinate at $a$.
(5) $X = \mathbf{P}^1(\mathbf{C})$ is a (compact) Riemann surface, with two charts $U_1 = X - \{\infty\}$, $U_2 = X - \{0\}$, and $\phi_j : U_j \xrightarrow{\sim} \mathbf{C}$ given by $\phi_1(z) = z$, $\phi_2(z) = 1/z$. The intersection $U_1 \cap U_2 = \mathbf{C}^*$, which means that $X$ is obtained from two copies of $\mathbf{C}$ glued along $\mathbf{C}^*$ by the map $z \mapsto 1/z$ (this can be visualized using the stereographic projection). For $x = a \in \mathbf{C}$ (resp. $x = \infty$), $z_\alpha(z) = z - a$ (resp. $z_\alpha(z) = 1/z$) is a local coordinate at $x$.

## 3.2 Holomorphic and meromorphic maps

### (3.2.1) Holomorphic maps and functions

**(3.2.1.1) Definition.** *A map $f : X \longrightarrow Y$ between Riemann surfaces $X, Y$ is* **holomorphic at a point** *$x \in X$ if there exist local charts $(U_\alpha, \phi_\alpha)$, $x \in U_\alpha$ on $X$ and $(V_\beta, \psi_\beta)$, $f(x) \in V_\beta$ on $Y$ such that the function*

$$\psi_\beta \circ f \circ \phi_\alpha^{-1} : \phi_\alpha(U_\alpha) \longrightarrow \psi_\beta(V_\beta)$$

*is holomorphic at $\phi_\alpha(x)$. The map $f$ is* **holomorphic** *if it is holomorphic at all points $x \in X$.*

**(3.2.1.2)** In the above definition, one can replace "there exist local charts" by "for all local charts".

**(3.2.1.3)** If $f$ is holomorphic (at $x$), it is continuous (at $x$).

**(3.2.1.4) Definition.** *A* **holomorphic function** *on a Riemann surface $X$ is a holomorphic map $f : X \longrightarrow \mathbf{C}$. Denote by $\mathcal{O}(X)$ the set of holomorphic functions on $X$ (it is a commutative ring containing $\mathbf{C}$).*

**(3.2.1.5)** If $Y$ is a Riemann surface, $X$ a topological space and $f : X \longrightarrow Y$ an unramified covering, then there exists a unique structure of a Riemann surface on $X$ for which $f$ is a holomorphic map.

**(3.2.1.6)** If $Y$ is a Riemann surface and $G$ a group of holomorphic automorphisms of $Y$ satisfying

$$(\forall y \in Y)\,(\exists U \ni y \text{ open})\,(\forall g \in G - \{1\})\ g(U) \cap U = \emptyset,$$

then the projection $f : Y \longrightarrow G\backslash Y = X$ is an unramified covering and there exists a unique structure of a Riemann surface on $X$ (equipped with the quotient topology) for which $f$ is a holomorphic map.

**(3.2.1.7) Example:** 3.2.1.6 applies, in particular, to quotients $f : \mathbf{C} \longrightarrow \mathbf{C}/L$ of $\mathbf{C}$ by discrete (additive) subgroups, i.e. by $L = \mathbf{Z}u$ or $L = \mathbf{Z}u + \mathbf{Z}v$, where $u, v \in \mathbf{C}$ are linearly independent over $\mathbf{R}$.

**(3.2.2) Meromorphic functions**

**(3.2.2.1) Definition.** *A* **meromorphic function** *on a Riemann surface $X$ is a holomorphic map $f : X \longrightarrow \mathbf{P}^1(\mathbf{C})$ such that $f(X) \neq \{\infty\}$. Denote by $\mathcal{M}(X)$ the set of meromorphic functions on $X$ (it is a field containing $\mathbf{C}$).*

**(3.2.2.2)** If $X \subset \mathbf{C}$ is an open subset of $\mathbf{C}$, then 3.2.2.1 is equivalent to the usual definition.

**(3.2.2.3)** If $(U_\alpha, z_\alpha)$ is a local coordinate at $x \in X$ and $f \in \mathcal{M}(X)$, then $f \circ z_\alpha^{-1}$ has a Laurent expansion

$$(f \circ z_\alpha^{-1})(z) = \sum_{n \geq n_0} a_n z^n$$

converging in some punctured disc $\{z \in \mathbf{C} \,|\, 0 < |z| < r\}$. One often writes "$f = \sum_n a_n z_\alpha^n$" in $U_\alpha$.

**(3.2.2.4) Definition. The order of vanishing** *of a non-zero meromorphic function $f \in \mathcal{M}(X) - \{0\}$ at $x \in X$ is defined as*

$$\mathrm{ord}_x(f) = \min\{n \in \mathbf{Z} \,|\, a_n \neq 0\} \in \mathbf{Z}$$

**(3.2.2.5)** The integer $\mathrm{ord}_x(f)$ does not depend on the choice of a local coordinate; $f$ is holomorphic at $x \iff \mathrm{ord}_x(f) \geq 0$.

**(3.2.2.6) Example:** Let $X = \mathbf{P}^1(\mathbf{C})$ and $f(z) = \prod_j (z - a_j)^{n_j}$, where $a_j \in \mathbf{C}$ are distinct and $n_j \in \mathbf{Z}$. The description of local coordinates on $X$ from 3.1.4(5), together with the identity

$$f(z) = (1/z)^{-\sum n_j} \prod_j (1 - a_j/z)^{n_j}$$

imply that

$$\mathrm{ord}_{a_j} = n_j, \qquad \mathrm{ord}_\infty(f) = -\sum_j n_j.$$

**(3.2.2.7)** $\mathrm{ord}_x$ **is a discrete valuation:** If $f, g \in \mathcal{M}(X) - \{0\}$, then

$$\mathrm{ord}_x(fg) = \mathrm{ord}_x(f) + \mathrm{ord}_x(g), \qquad \mathrm{ord}_x(f+g) \geq \min(\mathrm{ord}_x(f), \mathrm{ord}_x(g))$$

(with equality if $\mathrm{ord}_x(f) \neq \mathrm{ord}_x(g)$).

**(3.2.2.8)** If $f \in \mathcal{M}(X) - \{0\}$, then the set $Z(f) = \{x \in X \,|\, \mathrm{ord}_x(f) \neq 0\}$ is a closed discrete (= the induced topology on $Z(f)$ is discrete) subset of $X$. In particular, if $X$ is compact, then $Z(f)$ is finite.

**(3.2.2.9)** If $g, h \in \mathcal{M}(X)$ satisfy $g(x) = h(x)$ for all $x \in A$, where $A \subset X$ is a closed non-discrete subset of $X$, then $g = h$ (apply 3.2.2.8 to $f = g - h$).

**(3.2.2.10)** If $f : X \longrightarrow Y$ is a non-constant holomorphic map and $g : Y \longrightarrow \mathbf{P}^1(\mathbf{C})$ a meromorphic function on $Y$, then $f^*(g) = g \circ f : X \longrightarrow \mathbf{P}^1(\mathbf{C})$ is a meromorphic function on $X$. The map $f^* : \mathcal{M}(Y) \longrightarrow \mathcal{M}(X)$ is an embedding of fields (over $\mathbf{C}$).

**(3.2.3) Structure of non-constant holomorphic maps**

**(3.2.3.1) Proposition–Definition.** *Let $f : X \longrightarrow Y$ be a non-constant holomorphic map between Riemann surfaces and $x \in X$. Then there exist local coordinates $z_\alpha$ (resp. $z_\beta$) at $x$ (resp. $f(x) \in Y$) such that*

$$(z_\beta \circ f \circ z_\alpha^{-1})(z) = z^e \qquad (\text{“}z_\beta = z_\alpha^e\text{”}),$$

*where $e = e_x \geq 1$ is an integer, called the* **ramification index** *of $f$ at $x$ (it does not depend on any choices). The* **ramification points of** *$f$ are the points $x \in X$ with $e_x > 1$; they form a discrete subset of $X$.*

**(3.2.3.2) Corollary.** *A non-constant holomorphic map between Riemann surfaces is open.*

**(3.2.3.3) Corollary of Corollary.** *If $X$ is a compact Riemann surface, then $\mathcal{O}(\mathbf{C}) = \mathbf{C}$.*

*Proof.* If not, then there is a non-constant holomorphic map $f : X \longrightarrow \mathbf{C}$; its image $f(X) \subset \mathbf{C}$ is both compact and open, which is impossible.

**(3.2.3.4) Corollary.** *If $f : X \longrightarrow Y$ (as in 3.2.3.1) is bijective, then $e_x = 1$ for every $x \in X$ and $f^{-1} : Y \longrightarrow X$ is holomorphic.*

**(3.2.3.5) Proposition.** *Let $f : X \longrightarrow Y$ be as in 3.2.3.1. Assume, in addition, that $f$ is proper, i.e. $f^{-1}(K) \subset X$ is compact for every compact subset $K \subset Y$ (this holds, for example, if both $X$ and $Y$ are compact). Then there is an integer $\deg(f) \geq 1$ ("the degree of $f$") such that*

$$(\forall y \in Y) \sum_{x \in f^{-1}(y)} e_x = \deg(f).$$

*If $e_x = 1$ for all $x \in X$, then $f$ is an unramified covering.*

**(3.2.3.6) Example:** If $X = Y = \mathbf{C}$ and $f(z) = z^2$, then $e_x = 1$ (resp. $e_x = 2$) for $x \neq 0$ (resp. $x = 0$) and $\deg(f) = 2$.

**(3.2.3.7) Example:** If $X$ is compact, $f : X \longrightarrow Y = \mathbf{P}^1(\mathbf{C})$ is a non-constant meromorphic function and $y = 0$ (resp. $y = \infty$), then $e_x = \mathrm{ord}_x(f)$ (resp. $e_x = -\mathrm{ord}_x(f)$) for each $x \in f^{-1}(y)$. In particular,

$$\deg(f) = \sum_{f(x)=0} \mathrm{ord}_x(f) = - \sum_{f(x)=\infty} \mathrm{ord}_x(f).$$

### 3.3 Holomorphic and meromorphic differentials

**(3.3.1) Holomorphic functions revisited.** Let $X$ be a Riemann surface with an atlas $\{(U_\alpha, \phi_\alpha)\}$. A holomorphic function $f : X \longrightarrow \mathbf{C}$ defines, for each $\alpha$, a holomorphic function $f_\alpha = f \circ \phi_\alpha^{-1} \in \mathcal{O}(\phi_\alpha(U_\alpha))$. On $\phi_\alpha(U_\alpha \cap U_\beta)$ these functions satisfy the compatibility relation

$$f_\beta \circ \psi_{\alpha\beta} = f_\alpha,$$

where $\psi_{\alpha\beta} = \phi_\beta \circ \phi_\alpha^{-1}$ denotes the transition function. Writing $z_\alpha$ for the standard coordinate on $\mathbf{C} \supset \phi_\alpha(U_\alpha)$, we can reformulate the compatibility relation as follows:

$$f_\alpha(z_\alpha) = f_\beta(z_\beta) = f_\beta(\psi_{\alpha\beta}(z_\alpha)).$$

Meromorphic functions on $X$ admit an analogous description, with $f_\alpha \in \mathcal{M}(\phi_\alpha(U_\alpha))$.

**(3.3.2) Definition.** *A* **holomorphic differential** *$\omega$ on $X$ is defined by a collection of holomorphic functions $g_\alpha \in \mathcal{O}(\phi_\alpha(U_\alpha))$ such that the formal expressions $\omega_\alpha = g_\alpha(z_\alpha)\, dz_\alpha$ are compatible on $\phi_\alpha(U_\alpha \cap U_\beta)$ as follows:*

$$g_\alpha(z_\alpha)\, dz_\alpha = g_\beta(\psi_{\alpha\beta}(z_\alpha))\, dz_\beta = g_\beta(\psi_{\alpha\beta}(z_\alpha))\, \psi'_{\alpha\beta}(z_\alpha)\, dz_\alpha,$$

*i.e. $g_\alpha = (g_\beta \circ \psi_{\alpha\beta})\psi'_{\alpha\beta}$. The set of holomorphic differentials on $X$ will be denoted by $\Omega^1(X)$ (it is an $\mathcal{O}(X)$-module).*

**(3.3.3) Definition.** *A* **meromorphic differential** *on $X$ is defined by a collection of meromorphic functions $g_\alpha \in \mathcal{M}(\phi_\alpha(U_\alpha))$ satisfying the same compatibility relations as in 3.3.2. Meromorphic differentials form a vector space over $\mathcal{M}(X)$, which will be denoted by $\Omega^1_{\mathrm{mer}}(X)$.*

**(3.3.4) Examples:** (i) If $f \in \mathcal{O}(X)$ (resp. $\in \mathcal{M}(X)$) is given by a collection $f_\alpha(z_\alpha)$ as in 3.3.1, then the collection of functions $g_\alpha = f'_\alpha(z_\alpha)$ defines a differential $df \in \Omega^1(X)$ (resp. $\in \Omega^1_{\mathrm{mer}}(X)$), for which $(df)_\alpha = f'_\alpha(z_\alpha)\, dz_\alpha = df_\alpha$.
(ii) If $f : Y \longrightarrow X$ is a holomorphic map and $\omega \in \Omega^1(X)$, one can define the pull-back $f^*(\omega) \in \Omega^1(Y)$ as follows: let $(U_\alpha, \phi_\alpha)$ be an atlas of $X$ and assume that $\omega$ is given is given by a collection $g_\alpha \in \mathcal{O}(\phi_\alpha(U_\alpha))$ as in 3.3.2. Choose an atlas $(V_\beta, \psi_\beta)$ of $Y$ such that, for each $\beta$, $f(V_\beta) \subset U_\alpha$ for some $\alpha = j(\beta)$. In terms of the standard coordinates $z_\beta$ on $V_\beta$ (resp. $z_\alpha = z_{j(\beta)}$ on $U_\alpha = U_{j(\beta)}$, the map $f$ is defined by the formula $z_\alpha = f_\beta(z_\beta)$, where $f_\beta = \phi_\alpha \circ f \circ \psi_\beta^{-1}$. The differential $f^*(\omega)$ is then given by the collection of functions $(g_{j(\beta)} \circ f_\beta) f'_\beta \in \mathcal{O}(\psi_\beta(V_\beta))$. The same construction works for meromorphic differentials. In particular, $f^*(dh) = d(h \circ f)$ for any $h \in \mathcal{M}(X)$.

**(3.3.5) Definition.** *Let $\omega \in \Omega^1_{\mathrm{mer}}(X) - \{0\}$ and $x \in X$. Choose a local coordinate $(U_\alpha, z_\alpha)$ at $x$ and write $\omega_\alpha = f_\alpha(z_\alpha)\, dz_\alpha$,*

$$f_\alpha(z_\alpha) = \sum_{n \geq n_0}^{\infty} a_n z_\alpha^n.$$

*The* **order of zero** *of $\omega$ and its* **residue** *at $x$ are defined as*

$$\mathrm{ord}_x(\omega) = \mathrm{ord}_x(f_\alpha), \qquad \mathrm{res}_x(\omega) = a_{-1}.$$

**(3.3.6) Exercise.** Show that both $\mathrm{ord}_x(\omega)$ and $\mathrm{res}_x(\omega)$ are independent on the choice of a local coordinate.

**(3.3.7) Example:** For $X = \mathbf{P}^1(\mathbf{C})$ and $\omega = dz$ (where $z$ is the standard coordinate on $\mathbf{C} = X - \{\infty\}$), $\omega = d(z-a)$ for every $a \in \mathbf{C}$, hence $\mathrm{ord}_a(dz) = 0$. Taking $u = 1/z$ as a local coordinate at $\infty \in X$, the identity $dz = -u^{-2}\, du$ shows that $\mathrm{ord}_\infty(dz) = -2$.

**(3.3.8) Lemma.** *If $f \in \mathcal{M}(X) - \{0\}$ and $\mathrm{ord}_x(f) \neq 0$, then $\mathrm{ord}_x(df) = \mathrm{ord}_x(f) - 1$.*

*Proof.* In a local coordinate $z_\alpha$ at $x$, we have $f_\alpha(z_\alpha) = \sum_{n \geq m} a_n z_\alpha^n$, where $m = \mathrm{ord}_x(f) \neq 0$ and $a_m \neq 0$. Then $(df)_\alpha = \sum_{n \geq m} n a_n z_\alpha^{n-1}\, dz_\alpha$, hence $\mathrm{ord}_x(df) = m - 1$.

**(3.3.9)** The statements in 3.2.2.8-9 hold for meromorphic differentials.

**(3.3.10) The Residue Theorem.** *If $X$ is a compact Riemann surface and $\omega \in \Omega^1_{\mathrm{mer}}(X) - \{0\}$, then*

$$\sum_{x \in X} \mathrm{res}_x(\omega) = 0.$$

**(3.3.11) Corollary.** *If $X$ is a compact Riemann surface and $f \in \mathcal{M}(X) - \{0\}$, then*

$$\sum_{x \in X} \mathrm{ord}_x(f) = 0.$$

*Proof.* The meromorphic differential $\omega = df/f$ satisfies $\mathrm{res}_x(\omega) = \mathrm{ord}_x(f)$ for each $x \in X$. (Alternatively, one can apply 3.2.3.5 to $f : X \longrightarrow \mathbf{P}^1(\mathbf{C})$, using 3.2.3.7.)

**(3.3.12) Exercise.** *Deduce 2.2.2 from 3.3.10.*

**(3.3.13) Lemma.** *If $f : X \longrightarrow Y$ is a non-constant holomorphic map between Riemann surfaces, $x \in X$ and $z_\beta$ a local coordinate at $f(x) \in Y$, then*

$$\mathrm{ord}_x(f^*(dz_\beta)) = e_x - 1.$$

*Proof.* Using 3.2.3.1, we can assume that $f$ is given by $z_\beta = z_\alpha^{e_x}$, where $z_\alpha$ is a local coordinate at $x$, hence

$$\mathrm{ord}_x(f^*(dz_\beta)) = \mathrm{ord}_x(d(z_\alpha^{e_x})) = \mathrm{ord}_x(e_x z_\alpha^{e_x - 1} dz_\alpha) = e_x - 1.$$

**(3.3.14) Lemma.** *Let $X$ be a Riemann surface. If $\omega_1, \omega_2 \in \Omega^1_{\mathrm{mer}}(X) - \{0\}$, then there exists a meromorphic function $f \in \mathcal{M}(X) - \{0\}$ such that $\omega_1 = f\omega_2$.*

*Proof.* If $\omega_1, \omega_2$ are given locally by (non-zero) meromorphic functions $g_{1,\alpha}, g_{2,\alpha}$ satisfying the compatibility relations from 3.3.2, then the quotients $(g_{1,\alpha}/g_{2,\alpha})$ define a (non-zero) meromorphic function $f$, as in 3.3.1. Thus $\omega_1 = f\omega_2$.

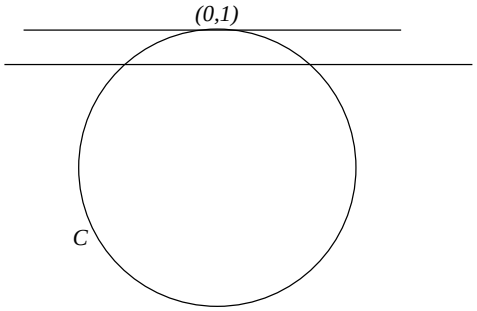
**(3.3.15) Theorem [Fa-Kr 1, Ch. 2].** *Let $X$ be a Riemann surface. Then $\mathcal{M}(X) \neq \mathbf{C}$ and $\Omega^1_{\mathrm{mer}}(X) \neq \{0\}$.*

**(3.3.16) Corollary.** *For every Riemann surface $X$, the vector space $\Omega^1_{\mathrm{mer}}(X)$ has dimension 1 over $\mathcal{M}(X)$.*

**(3.3.17)** We refer to ([Fo], Ch. 1, Sect. 9, 10; [Fa-Kr 1], 1.3, 1.4 and [Ki], Sect. 6.1) for the calculus of differential forms and their integration on Riemann surfaces.

### 3.4 Theorem on implicit functions

**(3.4.1) Example:** Consider the circle $C : f(x,y) = x^2 + y^2 - 1 = 0$.




As $\partial f/\partial x(0,1) = 0$, the tangent to $C$ at the point $(0,1)$ is horizontal. Moreover, for every open set $U \ni (0,1)$ (either in $\mathbf{R}^2$ or in $\mathbf{C}^2$), the intersection of $U$ with $C$ (i.e. with either $C(\mathbf{R})$ or $C(\mathbf{C})$) is *not* a graph of any function $y \mapsto (x(y))$, because there are two possible values of $x$ for $y$ arbitrarily close to 1. On the other hand, it is given by a graph of a function $x \mapsto y(x))$ (for sufficiently small $U$). This is a special case of the following result.

**(3.4.2) Theorem on Implicit Functions (holomorphic version).** *Let $U \subset \mathbf{C}^2$ be an open set, $f \in \mathcal{O}(U)$ a holomorphic function of $(x,y) \in U$ and $Z = \{(x,y) \in U \mid f(x,y) = 0\}$ its set of zeros. Assume that $P = (x_P, y_P) \in Z$ is a point satisfying $\partial f/\partial x(P) \neq 0$ (i.e. "the tangent to $Z$ at $P$ is not horizontal"). Then there exists an open set $V \subset U$, $V \ni P$, such that $\partial f/\partial x(Q) \neq 0$ for all $Q \in Z \cap V$, the horizontal projection*

$$p_2 : Z \cap V \longrightarrow p_2(Z \cap V) \ni y_P, \qquad p_2(x,y) = y$$

*is a homeomorphism and its inverse is given by $y \mapsto (x(y), y)$, where $x(y)$ is a holomorphic function on the open set $p_2(Z \cap V) \ni y_P$.*

**(3.4.3) Exercise.** Generalize 3.4.2 to a system of holomorphic equations

$$f_1(z_1, \ldots, z_n) = \cdots = f_m(z_1, \ldots, z_n) = 0 \qquad (m < n).$$

### 3.5 Orientation of Riemann surfaces

**(3.5.1) Orientation of real vector spaces.** Let $V$ be a (non-zero) real vector space of finite dimension $n$. The set $\mathcal{B}(V)$ of (ordered) bases of $V$ is a principal homogeneous space under $GL(V)$ (i.e. for each pair of bases $u, v$ there exists a unique element $g \in GL(V)$ satisfying $g(u) = v$). This defines a natural topology on the set $\mathcal{B}(V)$ (exercise: how?). By definition, two bases $u, v$ define the same orientation of $V$ iff they lie in the same connected component of $\mathcal{B}(V)$, i.e. iff $v = g(u)$ with $g \in GL(V)^\circ$ contained in the connected component of the identity of $GL(V)$, i.e. iff $\det(g) > 0$.

Equivalently, fix a volume element $\omega$ on $V$ (i.e. a non-zero element of the highest exterior power of the dual space $V^*$). Then the bases $u, v$ define the same orientation of $V$ iff $\omega(u_1, \ldots, u_n)$ and $\omega(v_1, \ldots, v_n)$ have the same sign.

**(3.5.2) Orientation of C.** The standard orientation of $\mathbf{C}$ (considered as a real vector space) is given by the ordered basis $1, i$. Let $x, y$ be the real and imaginary part, respectively, of the canonical complex

coordinate $z = x + iy$ on $\mathbf{C}$. Then the standard volume element $\omega = x \wedge y$ satisfies $\omega(1, i) > 0$. In spite of appearances, this "standard" orientation of $\mathbf{C}$ is not canonical: it depends on the choice of $i$. Some algebraic geometers therefore keep track of $i$ (more precisely, of $2\pi i$) in all the formulas.

**(3.5.3) Orientation of a Riemann surface.** The construction from 3.5.2 can be used to define an orientation of any Riemann surface $X$. If $\{(U_\alpha, \phi_\alpha)\}$ is an atlas of $X$, one can use the local charts to transport the standard orientation of $\mathbf{C}$ to $X$, at least infinitesimally (i.e. to the tangent spaces of $X$). We must check that these orientations agree on the intersections $U_\alpha \cap U_\beta$. Let us decompose the local coordinates $z_\alpha, z_\beta$ (at the same point $x \in X$) into their real and imaginary components $z_\alpha = x_\alpha + iy_\alpha$, $z_\beta = x_\beta + iy_\beta$. For small $\varepsilon > 0$, the vectors $\varepsilon, i\varepsilon$ based at $0 = z_\alpha(x)$ are mapped by the transition function $\psi_{\alpha\beta} = z_\beta \circ z_\alpha^{-1}$ to

$$\varepsilon \mapsto \frac{\partial x_\beta}{\partial x_\alpha} + i\frac{\partial y_\beta}{\partial x_\alpha} + O(\varepsilon^2)$$
$$i\varepsilon \mapsto \frac{\partial x_\beta}{\partial y_\alpha} + i\frac{\partial y_\beta}{\partial y_\alpha} + O(\varepsilon^2).$$

This implies that the infinitesimal change of orientations is given by the sign of the determinant of the (non-singular) Jacobian matrix

$$M = \begin{pmatrix} \frac{\partial x_\beta}{\partial x_\alpha} & \frac{\partial y_\beta}{\partial x_\alpha} \\ \frac{\partial x_\beta}{\partial y_\alpha} & \frac{\partial y_\beta}{\partial y_\alpha} \end{pmatrix}.$$

Hovever, the Cauchy-Riemann equations tell us that the matrix $M$ is of the form

$$M = \begin{pmatrix} A & -B \\ B & A \end{pmatrix},$$

where $A, B$ are real valued functions; thus $\det(M) = A^2 + B^2 > 0$, which proves the compatibility of the two orientations.

**(3.5.4)** Explicitly, if $(U_\alpha, z_\alpha)$ is a local coordinate on $X$, $V \subset U_\alpha$ an open subset and $f : V \longrightarrow \mathbf{R}_{\geq 0}$ a non-negative (differentiable) function for which $f^{-1}(0) \subset V$ is a discrete set, then

$$\frac{i}{2} \int_V f \, dz_\alpha \wedge d\overline{z}_\alpha > 0,$$

as

$$\frac{i}{2} \, d(x + iy) \wedge d(x - iy) = dx \wedge dy.$$

In particular, if $\omega \in \Omega^1(V) - \{0\}$, then

$$\frac{i}{2} \int_V \omega \wedge \overline{\omega} = \frac{i}{2} \int_V |f_\alpha(z_\alpha)|^2 \, dz_\alpha \wedge d\overline{z}_\alpha > 0 \tag{3.5.4.1}$$

(writing $\omega_\alpha = f_\alpha(z_\alpha) \, dz_\alpha$).

### 3.6 Genus and the Riemann-Hurwitz formula

**(3.6.1) The genus.** Let $X$ be a compact Riemann surface. By 3.5.3, $X$ is orientable, hence homeomorphic to a sphere with $g$ handles. The integer $g = g(X) \geq 0$ is called the **(topological) genus** of $X$.

**(3.6.2) The Euler (– Poincaré) formula.** For every triangulation of $X$, denote by $s_i$ the number of simplices of dimension $i = 0, 1, 2$ in the triangulation. Then

$$s_0 - s_1 + s_2 = 2 - 2g(X).$$

**(3.6.3) The Riemann-Hurwitz formula.** *Let $f : X \longrightarrow Y$ be a non-constant holomorphic map between compact Riemann surfaces. Then*

$$2g(X) - 2 = (2g(Y) - 2)\deg(f) + \sum_{x \in X} (e_x - 1).$$

**(3.6.4) Exercise.** *Prove 3.6.3 by considering suitably compatible triangulations of $X$ and $Y$.*

**(3.6.5) Example:** If $X$ is a compact Riemann surface and $f : X \longrightarrow \mathbf{P}^1(\mathbf{C})$ is a holomorphic map of degree $\deg(f) = 2$, then

$$2g(X) - 2 = -4 + |S|, \qquad S = \{x \in X \mid e_x = 2\} = \{x \in X \mid e_x \neq 1\};$$

thus there are $|S| = 2n$ $(n \geq 1)$ ramification points of $f$ and $g(X) = n - 1$.

## 3.7 Smooth complex plane curves are Riemann surfaces

**(3.7.1) Smooth affine plane curves**

**(3.7.1.1)** An **affine plane curve** over a field $K$ is a polynomial equation

$$V : f(x, y) = 0,$$

where $f(x, y) \in K[x, y]$ is a polynomial with coefficients in $K$. Note that, with this definition, the curves "$y = 0$" and "$y^2 = 0$" are not the same objects.

**(3.7.1.2) Definition.** *Let $L \supset K$ be a field and $P = (x_P, y_P) \in V(L)$ a point on $V$ with coordinates in $L$. We say that $P$ is a* **smooth point** *of $V$ if*

$$\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) \neq (0, 0).$$

**(3.7.1.3) Examples:** (i) Each point of $V_1 : y = 0$ is smooth.
(ii) No point of $V_2 : y^2 = 0$ is smooth.
(iii) The point $(0, 0)$ is not smooth on either of the curves

$$V_3 : y^2 - x^3 = 0, \qquad V_4 : y^2 - x^2(x + 1).$$

All other points on $V_3, V_4$ are smooth.

**(3.7.1.4) Exercise.** *Smoothness of $P$ on $V$ is invariant under every affine change of coordinates*

$$x = ax' + by' + c, \qquad Y = dx' + ey' + f, \qquad ae - bd \neq 0.$$

**(3.7.1.5) Definition.** *We say that $V$ is a* **smooth affine plane curve over** *$K$ if every point $P \in V(\overline{K})$ is smooth on $V$ (where $\overline{K}$ is an algebraic closure of $K$).*

**(3.7.1.6) Exercise.** *If $V$ is smooth, then*

$$(\forall \text{ field } L \supset K)\,(\forall\, Q \in V(L))\ Q \text{ is smooth on } V.$$

*[Hint: Use the Nullstellensatz.]*

**(3.7.2) Proposition.** *If $K \subset \mathbf{C}$ is a subfield of $\mathbf{C}$ and $V$ is a smooth affine plane curve over $K$, then:*
(i) *The set of complex points $V(\mathbf{C})$ of $V$ has only finitely many connected components.*
(ii) *Each connected component $X$ of $V(\mathbf{C})$ has a natural structure of a Riemann surface (in which the functions $x, y$ are holomorphic on $X$).*

(iii) *If $V : f(x,y) = 0$ is geometrically irreducible (i.e. if the polynomial $f$ is irreducible in $\overline{K}[x,y] \iff f$ is irreducible in $\mathbf{C}[x,y]$), then $V(\mathbf{C})$ is connected.*

*Proof.* We can assume that $K = \mathbf{C}$. (i) Exercise. (ii) Put

$$X_x = \{P = (x_P, y_P) \in X \,|\, \partial f/\partial x(P) \neq 0\}, \qquad X_y = \{P = (x_P, y_P) \in X \,|\, \partial f/\partial y(P) \neq 0\}.$$

By 3.7.1.6, $X = X_x \cup X_y$. If $P \in X_x$ (resp. $P \in X_y$), then 3.4.2 (Theorem on Implicit Functions) tells us that there exists an open neighbourhood $U_{P,x}$ (resp. $U_{P,y}$) of $P$ contained in $X_x$ (resp. in $X_y$) such that the function $y - y_P$ (resp. $x - x_P$) defines a homeomorphism between $U_{P,x}$ (resp. $U_{P,y}$) and an open neighbourhood $W_P$ of $0 \in \mathbf{C}$, and that $X \cap U_{P,x} = \{(f_P(z), z + y_P) \,|\, z \in W_P\}$ (resp. $X \cap U_{P,y} = \{(z + x_P, f_P(z) \,|\, z \in W_P\})$, where $f_P(z)$ is a holomorphic function in $W_P$.

We want to show that the collection $\{(U_{P,x}, y - y_P) \,|\, P \in X_x\} \cup \{(U_{P,y}, x - x_P) \,|\, P \in X_y\}$ defines an atlas on $X$.

If $P, Q \in X_x$, then the local coordinates $y - y_P$ and $y - y_Q$ are compatible on $U_{P,x} \cap U_{Q,x}$, as $y - y_Q = y - y_P + (y_P - y_Q)$ is a holomorphic function in $y - y_P$ (and similarly for the local coordinates $x - x_P$ and $x - x_Q$ for $P, Q \in X_y$).

If $P \in X_x$, $Q \in X_y$ and $U = U_{P,x} \cap U_{Q,y} \neq \emptyset$, then $U \subset X_x \cap X_y$ and for $R \in U$, $x(R) - x_Q$ is a holomorphic function of $y(R) - y_P$ (and vice versa), again by 3.4.2.

(iii) After a linear change of coordinates we can assume that

$$f(x,y) = y^n + a_1(x)y^{n-1} + \cdots + a_n(x) \qquad (a_j(x) \in \mathbf{C}[x],\ n \geq 1)$$

(by an elementary case of the Noether normalization Lemma). As $f$ is ireducible in $\mathbf{C}[x,y] = \mathbf{C}[x][y]$, it is irreducible in $\mathbf{C}(x)[y]$, hence the discriminant of $f$ with respect to the $y$-variable $\mathrm{disc}_y(f) \in \mathbf{C}[x]$ is non-zero. It follows that

$$S = \{x \in \mathbf{C} \,|\, \mathrm{disc}_y(f)(x) = 0\}$$

is a finite subset of $\mathbf{C}$. The projection $p : V(\mathbf{C}) \longrightarrow \mathbf{C}$ $(p(x,y) = x)$ on the first coordinate axis has the following properties:

(a) $(\forall x \in \mathbf{C}) \quad \#p^{-1}(x) \leq n.$
(b) $(\forall x \in \mathbf{C} - S) \quad \#p^{-1}(x) = n.$
(c) $(\forall (x,y) \in p^{-1}(\mathbf{C} - S)) \quad \partial f/\partial y(x,y) \neq 0.$

The Theorem on Implicit Functions implies that the restriction of $p$ to $Y = p^{-1}(\mathbf{C} - S) = V(\mathbf{C}) - p^{-1}(S)$ is an unramified covering. As $Y$ is dense in $V(\mathbf{C})$, it is sufficient to prove that $Y$ is connected.

Elementary properties of unramified coverings imply that, for each connected component $Y_j$ of $Y$, the restriction of $p$ to $p_j : Y_j \longrightarrow \mathbf{C} - S$ is also an unramified covering. In particular, $Y = Y_1 \cup \cdots Y_N$ is a disjoint union of $N \leq n$ connected components, thanks to (a). Applying the Theorem on Implicit Functions again, we see that, locally on $\mathbf{C} - S$, the projection $p_j$ admits sections given by the formulas

$$x \mapsto (x, s_i(x)), \qquad (1 \leq i \leq r_j),$$

where each $s_i$ is holomorphic. The coefficients of the polynomial

$$f_j = \prod_{i=1}^{r_j} (y - s_i(x)) \in \mathcal{O}(\mathbf{C} - S)[y]$$

are holomorphic functions defined globally on $\mathbf{C} - S$, which yields a factorization

$$f = f_1 \cdots f_N \in \mathbf{C}[x,y].$$

The same argument as in the proof of the Gauss Lemma ("the contents of a product of polynomials is equal to the product of the contents of the factors") shows that each factor $f_j$ is contained in $\mathbf{C}[x,y]$. Irreducibility of $f$ then implies that $N = 1$ as claimed.

See also ([Ki], 7.22) or ([Fo], 8.9) for variants of this proof.

**(3.7.3) Example:** For the circle $V = C : x^2 + y^2 - 1 = 0$ and $P = (x_P, y_P) \in C(\mathbf{C})$, $y - y_P$ is a local coordinate at all $P \neq (0, \pm 1)$ and $x - x_P$ is a local coordinate at all $P \neq (\pm 1, 0)$.

**(3.7.4) Smooth projective plane curves**

**(3.7.4.1)** A **projective plane curve** over a field $K$ is a polynomial equation

$$\widetilde{V} : F(X, Y, Z) = 0,$$

where $F(X, Y, Z) \in K[X, Y, Z]$ is a homogeneous polynomial of degree $d \geq 1$ with coefficients in $K$.

**(3.7.4.2)** Let $P = (X_P : Y_P : Z_P) \in \widetilde{V}(L)$ be a point on $\widetilde{V}$ with homogeneous coordinates in a field $L \supset K$. The point $P$ is contained in one of the standard affine planes $\{X \neq 0\}$, $\{Y \neq 0\}$, $\{Z \neq 0\}$ covering $P^2$. If, for example, $Y_P \neq 0$, then $P \in V(L)$, where

$$V : f(u, v) = F(u, 1, v) = 0$$

is the equation of the affine plane curve

$$\widetilde{V} \cap \{Y \neq 0\} \subset \{Y \neq 0\} = \mathbf{A}^2$$

written in the affine coordinates $u = X/Y, v = Z/Y$ on $\{Y \neq 0\} = \mathbf{A}^2$. We say that $P$ is a **smooth point** of $\widetilde{V}$ if it is a smooth point of $V$.

**(3.7.4.3) Exercise.** *Show that $P$ is a smooth point of $\widetilde{V}$ if and only if*

$$\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) \neq (0, 0, 0).$$

*Deduce that the definition of smoothness in 3.7.4.2 does not depend on any choices and is invariant under a projective change of coordinates (by an element of $PGL_3$). [Hint: Use the fact that $XD_X + YD_Y + ZD_Z$ (where $D_T = \partial/\partial T$) acts on $F$ by multiplication by* $\deg(F)$*.]*

**(3.7.5) Proposition.** *If $K \subset \mathbf{C}$ is a subfield of $\mathbf{C}$ and $\widetilde{V}$ is a smooth projective plane curve over $K$, then:*
(i) *The polynomial $F(X, Y, Z)$ is irreducible in $\mathbf{C}[X, Y, Z]$.*
(ii) *The set of complex points $\widetilde{V}(\mathbf{C})$ of $\widetilde{V}$ is connected.*
(iii) *$\widetilde{V}(\mathbf{C})$ has a natural structure of a compact Riemann surface.*

*Proof.* (i) Exercise (use Bézout's Theorem). (ii) See 3.7.2(iii). (iii) Exercise (use 3.7.2 and the compactness of $P^2(\mathbf{C})$).

**(3.7.6) Example:** For the projective circle $\widetilde{V} = \widetilde{C} : X^2 + Y^2 - Z^2 = 0$, $\widetilde{C}(\mathbf{C}) \xrightarrow{\sim} \mathbf{P}^1(\mathbf{C})$ (cf. 0.3.1.0 and 3.8.4 below).

**(3.7.7) A hyperelliptic example:** Let $K$ be a field of characteristic $\mathrm{char}(K) \neq 2$ and

$$f(x) = a_0(x - \alpha_1) \cdots (x - \alpha_n) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$$

a polynomial with coefficients in $K$ of degree $n \geq 3$ with distinct roots $\alpha_1, \ldots, \alpha_n \in \overline{K}$. Consider the affine plane curve

$$V : y^2 - f(x) = 0$$

and the corresponding projective plane curve

$$\widetilde{V} : Y^2 Z^{n-2} - a_0(X - \alpha_1 Z) \cdots (X - \alpha_n Z) = Y^2 Z^{n-2} - (a_0 X^n + a_1 X^{n-1} Z + \cdots + a_n Z^n) = 0$$

(where $x = X/Z, y = Y/Z$).

We are looking for non-smooth points on $\widetilde{V}$. If $P = (x, y) \in V(\overline{K})$ is a non-smooth point on $V$, then

$$y^2 - f(x) = 0, \qquad 2y = 0, \qquad -f'(x) = 0.$$

As 2 is invertible in $K$, it follows that $y = 0$, hence $f(x) = f'(x) = 0$. This contradicts our assumption that $f$ has only simple roots, hence the affine curve $V$ is smooth.

What about the points at infinity? There is only one such point $O$, as

$$\widetilde{V}(\overline{K}) - V(\overline{K}) = \widetilde{V}(\overline{K}) \cap \{Z = 0\} = \{O = (0 : 1 : 0)\},$$

contained in the standard affine piece $\{Y \neq 0\}$. Passing to the affine coordinates $u = X/Y = x/y, v = Z/Y = 1/y$, the point $O$ corresponds to $(u, v) = (0, 0)$, and the affine curve $\widetilde{V} \cap \{Y \neq 0\}$ is given by the equation

$$\left(\frac{Z}{Y}\right)^{n-2} - a_0 \left(\frac{X}{Y} - \alpha_1 \frac{Z}{Y}\right) \cdots \left(\frac{X}{Y} - \alpha_n \frac{Z}{Y}\right) = 0,$$

i.e.

$$g(u, v) = v^{n-2} - (a_0 u^n + a_1 u^{n-1} v + \cdots + a_n v^n) = 0.$$

As

$$\frac{\partial g}{\partial u}(0, 0) = 0, \qquad \frac{\partial g}{\partial v}(0, 0) = \begin{cases} 1, & \text{if } n = 3 \\ 0, & \text{if } n > 3, \end{cases}$$

it follows that $O = (0 : 1 : 0)$ is a smooth point of $\widetilde{V}$ if and only if $n = 3$.

**(3.7.8) The hyperelliptic example continued:** If $n = 2m \geq 4$ is *even*, then there is a simple way to resolve the singularity of the curve $\widetilde{V}$ at $O$: the polynomial

$$g(u) = u^{2m} f(1/u) = a_{2m} u^{2m} + \cdots + a_1 u + a_0$$

has distinct roots and satisfies $g(0) = a_0 \neq 0$. Consider the affine plane curves

$$V : y^2 - f(x) = 0, \qquad W : v^2 - g(u) = 0;$$

they are both smooth. The formulas

$$u = 1/x, \qquad v = y/x^m, \qquad x = 1/u, \qquad y = v/u^m. \tag{3.7.8.1}$$

define an isomorphism

$$V \cap \{x \neq 0\} \xrightarrow{\sim} W \cap \{u \neq 0\}$$

Imitating the construction of $P^1(\mathbf{C})$ by gluing together two copies of $\mathbf{C}$ along $\mathbf{C}^*$ via the map $1/z$ (cf. 3.1.4(5)), we can glue together $V$ and $W$ along their open subsets $V \cap \{x \neq 0\}$ (resp. $W \cap \{u \neq 0\}$) according to the formulas (3.7.8.1). The resulting object will be a projective curve $U$ (exercise!) which is smooth (although we have not yet defined smoothness for non-plane curves). There are exactly two points $O_\pm$ in

$$U(\overline{K}) - V(\overline{K}) = \{O_\pm = (u, v) = (0, \pm\sqrt{a_0})\};$$

they correspond to the two branches of $\widetilde{V}$ meeting at $O$, i.e. to the two choices of a sign in the asymptotic behaviour

$$(x, y) \longrightarrow O_\pm \iff x \longrightarrow \infty, \quad y/x^m \longrightarrow \pm\sqrt{a_0}.$$

**(3.7.9) Exercise.** *Resolve the singularity of $V$ at $O$ if $n = 2m - 1 \geq 5$ is odd.*

### 3.8 Geometry of the circle revisited

We are now ready to answer Question 2.4.6(iv) about the values of integrals of $\omega = dy/x$ on (the complex points of) the circle $C : x^2 + y^2 = 1$.

**(3.8.1)** Let us return to the situation considered in 2.1 (in the light of the discussion in 2.4): intersecting the affine circle $C(\mathbf{C})$ with two lines

$$L_{a,b} : y - ax - b = 0, \qquad L_{a',b'} : y - a'x - b' = 0$$

(where $a, a' \in \mathbf{C} - \{\pm i\}$) we obtain intersection divisors

$$D = (P_1) + (P_2), \qquad D' = (P_1') + (P_2')$$

on $C(\mathbf{C})$. We know that (using the notation from (2.4.1.1))

$$a = a' \Longrightarrow \int_O^D \omega \equiv \int_O^{D'} \omega \pmod{2\pi\mathbf{Z}}$$

(in fact, it is easy to see that the converse implication also holds). Our goal is to find an abstract reformulation of the condition "$a = a'$". To this end, consider the function

$$f = c \cdot \frac{y - ax - b}{y - a'x - b'} = c \cdot \frac{Y - aX - bZ}{Y - a'X - b'Z},$$

where $c \in \mathbf{C}^*$ is a constant, to be specified later. What can we say about $f$? It is a meromorphic function on the projective circle $\widetilde{C}(\mathbf{C})$, with zeros at $P_1$, $P_2$ and poles at $P_1'$, $P_2'$. More precisely, the *divisor of* $f$, defined as

$$\mathrm{div}(f) = \sum_P \mathrm{ord}_P(f)(P),$$

is equal to

$$\mathrm{div}(f) = (P_1) + (P_2) - (P_1') - (P_2') = D - D'.$$

We can also look at the behaviour of $f$ at the two points at infinity $P_\pm = (1 : \pm i : 0) \in \widetilde{C}(\mathbf{C}) - C(\mathbf{C})$:

$$f(P_+) = c\frac{i - a}{i - a'}, \qquad f(P_-) = c\frac{-i - a}{-i - a'}.$$

Choosing $c$ so that $f(P_+) = 1$, we have

$$f(P_-) = \frac{(i - a')(-i - a)}{(i - a)(-i - a')} = \frac{1 + aa' + i(a' - a)}{1 + aa' - i(a' - a)},$$

hence

$$a = a' \iff f(P_+) = f(P_-) = 1.$$

This suggests the following tentative answer to Question 2.4.6(iv).

**(3.8.2) Conjecture.** *Let $D_1 = \sum_j m_j(P_j)$, $D_2 = \sum_k n_k(Q_k)$ be two divisors on $\widetilde{C}(\mathbf{C})$ of the same degree $\sum_j m_j = \sum_k n_k$ and such that $P_j \neq P_\pm \neq Q_k$ for all $j, k$. Then*

$$\int_O^{D_1} \omega \equiv \int_O^{D_2} \omega \pmod{2\pi\mathbf{Z}} \iff (\exists g \in \mathcal{M}(\widetilde{C}(\mathbf{C}))^*) \quad g(P_+) = g(P_-) = 1,\ D_1 - D_2 = \mathrm{div}(g)$$

*(the implication "$\Longleftarrow$" being a special case of Abel's Theorem).*

**(3.8.3) Exercise.** *Generalize the calculation from 3.8.1 to the case when $L_{a,b}$ is replaced by the curve (2.2.7.4). What is the relation to the conditions (2.2.7.5) and to 3.8.2?*

**(3.8.4) Exercise.** *The map*

$$C(\mathbf{C}) \longrightarrow \mathbf{C}^*, \qquad (x,y) \mapsto z = x + iy$$

*extends to a holomorphic isomorphism of Riemann surfaces $\lambda : \widetilde{C}(\mathbf{C}) \xrightarrow{\sim} P^1(\mathbf{C})$, under which $P_+$ (resp. $P_-$) is mapped to 0 (resp. $\infty$) and $\lambda^*(dz/z) = i\,dy/x = i\omega$.*

**(3.8.5) Proof of Conjecture 3.8.2.** Applying $\lambda$, we are reduced to prove the following statement about the multiplicative group $\mathbf{C}^*$:
Let $D_1 = \sum_j m_j(P_j)$, $D_2 = \sum_k n_k(Q_k)$ be two divisors on $\mathbf{P}^1(\mathbf{C})$ of the same degree $\sum_j m_j = \sum_k n_k$ and such that $P_j \neq 0, \infty \neq Q_k$ for all $j,k$. Writing $D = D_1 - D_2 = \sum_j(b_j) - \sum_j(a_j)$, then

$$\int_D \frac{dz}{z} := \sum_j \int_{a_j}^{b_j} \frac{dz}{z} = 0 \in \mathbf{C}/2\pi i\mathbf{Z} \iff (\exists g \in \mathcal{M}(\mathbf{P}^1(\mathbf{C}))^*) \quad g(0) = g(\infty) = 1,\ \mathrm{div}(g) = D.$$

Noting that (cf. 3.9.7 below)

$$f(z) = \prod_j \frac{z - b_j}{z - a_j} \tag{3.8.5.1}$$

is the unique function $f \in \mathcal{M}(\mathbf{P}^1(\mathbf{C}))^*$ satisfying $\mathrm{div}(f) = D$ and $f(\infty) = 1$, the statement follows from the fact that

$$\exp\left(\int_D \frac{dz}{z}\right) = \prod_j \frac{b_j}{a_j} = f(0),$$

as

$$\int_D \frac{dz}{z} = 0 \in \mathbf{C}/2\pi i\mathbf{Z} \iff \exp\left(\int_D \frac{dz}{z}\right) = 1 \in \mathbf{C}^*.$$

**(3.8.6) The additive group $(\mathbf{C}, +)$.** Let us try to apply the same argument to the differential $\omega = dz \in \Omega^1(\mathbf{C})$. If $D = \sum_j(b_j) - \sum_j(a_j)$ $(a_j, b_j \in \mathbf{C})$ is a divisor of degree zero, then the function $f(z)$ defined by (3.8.5.1) is, as in 3.8.5, the unique function $f \in \mathcal{M}(\mathbf{P}^1(\mathbf{C}))^*$ satisfying $\mathrm{div}(f) = D$ and $f(\infty) = 1$. The integral

$$\int_D dz := \sum_j \int_{a_j}^{b_j} dz = \sum_j b_j - \sum_j a_j \in \mathbf{C}$$

has a well-defined value in $\mathbf{C}$ (there are no periods, as $\mathbf{C}$ is simply connected). Writing the power series expansion of $f$ at the point $\infty$ in terms of the local coordinate $w = 1/z$, we see that

$$f = \prod_j \frac{1 - b_j w}{1 - a_j w} = 1 + \left(\sum_j a_j - \sum_j b_j\right) w + O(w^2),$$

hence

$$\int_D dz = 0 \iff \sum_j a_j - \sum_j b_j = 0 \iff \mathrm{ord}_\infty(f - 1) \geq 2.$$

### 3.9 Divisors on Riemann surfaces

Throughout 3.9, $X$ is a Riemann surface. The results from 3.8 suggest that the following objects could be of interest.

**(3.9.1) Definition.** *A* **divisor on** $X$ *is a locally finite formal sum*

$$D = \sum_{P \in X} n_P(P) \qquad\qquad (n_P \in \mathbf{Z}),$$

*where "locally finite" means the following: denoting by* $\operatorname{supp}(D) := \{P \in X \mid n_P \neq 0\}$ *the* **support of** $D$*, we require that, for each compact subset* $K \subset X$*, the intersection* $K \cap \operatorname{supp}(D)$ *be finite (in particular, if* $X$ *itself is compact, then "locally finite" = "finite"). The set* $\operatorname{Div}(X)$ *of all divisors on* $X$ *is an abelian group with respect to addition. The divisor* $D$ *is* **effective** *(notation:* $D \geq 0$*) if all coefficients* $n_P \geq 0$ *are non-negative.*

**(3.9.2) Definition.** *The* **divisor of a meromorphic function** $f \in \mathcal{M}(X)^*$ *(resp. the* **divisor of a meromorphic differential** $\omega \in \Omega^1_{\mathrm{mer}}(X) - \{0\}$*) is*

$$\operatorname{div}(f) = \sum_{P \in X} \operatorname{ord}_P(f)(P), \qquad \operatorname{div}(\omega) = \sum_{P \in X} \operatorname{ord}_P(\omega)(P)$$

*(the sums are locally finite, as observed in 3.2.2.8 and 3.3.9, respectively). The divisors of the form* $\operatorname{div}(f)$ *(*$f \in \mathcal{M}(X)^*$*) are called* **principal divisors***; they form a subgroup* $P(X) \subset \operatorname{Div}(X)$*.*

**(3.9.3) Definition.** *If* $X$ *is* **compact***, then the* **degree** *of a divisor* $D = \sum_P n_P(P) \in \operatorname{Div}(X)$ *is* $\deg(D) = \sum_P n_P \in \mathbf{Z}$ *(a finite sum!). Denote by* $\operatorname{Div}^0(X) = \operatorname{Ker}(\deg : \operatorname{Div}(X) \longrightarrow \mathbf{Z})$ *the subgroup of divisors of degree zero. By 3.3.11,* $P(X)$ *is in fact contained in* $\operatorname{Div}^0(X)$*.*

**(3.9.4)** The map $\operatorname{div} : \mathcal{M}(X)^* \longrightarrow \operatorname{Div}(X)$ is a homomorphism of groups (because of the first statement in 3.2.2.7) with image $P(X)$. If $X$ is compact, then the kernel of div is equal to $\mathbf{C}^*$, by 3.2.3.3.

**(3.9.5) Definition.** *The* **divisor class group of** $X$ *is the quotient abelian group* $Cl(X) = \operatorname{Div}(X)/P(X)$*. If* $X$ *is compact, then the subgroup of divisor classes of degree zero is denoted by* $Cl^0(X) = \operatorname{Div}^0(X)/P(X)$*.*

**(3.9.6)** To sum up, if $X$ is compact, then there are exact sequences

$$\begin{gathered} 0 \longrightarrow \mathbf{C}^* \longrightarrow \mathcal{M}(X)^* \xrightarrow{\operatorname{div}} \operatorname{Div}(X) \longrightarrow Cl(X) \longrightarrow 0 \\ 0 \longrightarrow \mathbf{C}^* \longrightarrow \mathcal{M}(X)^* \xrightarrow{\operatorname{div}} \operatorname{Div}^0(X) \longrightarrow Cl^0(X) \longrightarrow 0 \\ 0 \longrightarrow Cl^0(X) \longrightarrow Cl(X) \xrightarrow{\deg} \mathbf{Z} \longrightarrow 0. \end{gathered}$$

**(3.9.7) Exercise.** *Show that* $Cl^0(\mathbf{P}^1(\mathbf{C})) = 0$*.*

**(3.9.8) Exercise.** *Show that* $\mathcal{M}(\mathbf{P}^1(\mathbf{C})) = \mathbf{C}(z)$*, i.e. every meromorphic function* $f$ *on* $\mathbf{P}^1(\mathbf{C})$ *is a rational function in the standard coordinate* $z$*. [Hint: Consider the divisor of* $f$*.]*

**(3.9.9)** If $X$ is **not** compact, then every divisor on $X$ is principal, i.e. $Cl(X) = 0$ ([Fo], 26.5).

**(3.9.10) Exercise-Definition.** *Let* $f : X \longrightarrow Y$ *be a non-constant proper holomorphic map between Riemann surfaces. Then the map*

$$f^* : \sum_{y \in Y} n_y(y) \mapsto \sum_{x \in X} e_x n_{f(x)}(x)$$

*defines a homomorphism of abelian groups* $f^* : \operatorname{Div}(Y) \longrightarrow \operatorname{Div}(X)$ *satisfying*

$$\begin{gathered} (\forall g \in \mathcal{M}(Y)^*) \qquad f^*(\operatorname{div}(g)) = \operatorname{div}(g \circ f) \\ (\forall D \in \operatorname{Div}(Y)) \qquad \deg(f^*(D)) = \deg(f)\deg(D) \qquad \text{(provided } X \text{ is compact).} \end{gathered}$$

**(3.9.11) Definition.** *Let* $X$ *be a compact Riemann surface and* $\mathfrak{m} = \sum \mathfrak{m}_P(P) \geq 0$ *an effective divisor with support* $S = \operatorname{supp}(\mathfrak{m})$*. Define*

$$\begin{gathered} \operatorname{Div}_S(X) = \{D \in \operatorname{Div}(X) \mid \operatorname{supp}(D) \cap S = \emptyset\}, \qquad \operatorname{Div}^0_S(X) = \operatorname{Div}_S(X) \cap \operatorname{Div}^0(X), \\ P_{\mathfrak{m}}(X) = \{\operatorname{div}(f) \mid f \in \mathcal{M}(X)^*,\ (\forall P \in S)\ \operatorname{ord}_P(f-1) \geq \mathfrak{m}_P\} \\ Cl_{\mathfrak{m}}(X) = \operatorname{Div}_S(X)/P_{\mathfrak{m}}(X), \qquad Cl^0_{\mathfrak{m}}(X) = \operatorname{Div}^0_S(X)/P_{\mathfrak{m}}(X). \end{gathered}$$

*The abelian group* $Cl_{\mathfrak{m}}(X)$ *is called the* **divisor class group of** $X$ **with respect to the modulus** $\mathfrak{m}$*.*

**(3.9.12)** Using this notation, the calculations from 3.8.5-6 can be reformulated as follows.

**(3.9.13) Proposition.** (i) *The maps*

$$D \mapsto \int_D \omega, \qquad \begin{cases} \mathrm{Div}^0_{\{0,\infty\}}(\mathbf{P}^1(\mathbf{C})) \longrightarrow \mathbf{C}/2\pi i\mathbf{Z}, & \omega = dz/z \\ \mathrm{Div}^0_{\{\infty\}}(\mathbf{P}^1(\mathbf{C})) \longrightarrow \mathbf{C}, & \omega = dz \end{cases}$$

*induce isomorphisms of abelian groups*

$$Cl^0_{(0)+(\infty)}(\mathbf{P}^1(\mathbf{C})) \xrightarrow{\sim} \mathbf{C}/2\pi i\mathbf{Z}, \qquad Cl^0_{2(\infty)}(\mathbf{P}^1(\mathbf{C})) \xrightarrow{\sim} \mathbf{C}.$$

(ii) *The maps*

$$(\mathbf{C}^*, \times) \longrightarrow Cl^0_{(0)+(\infty)}(\mathbf{P}^1(\mathbf{C})), \qquad a \mapsto \text{ the class of } (a) - (1)$$
$$(\mathbf{C}, +) \longrightarrow Cl^0_{2(\infty)}(\mathbf{P}^1(\mathbf{C})), \qquad a \mapsto \text{ the class of } (a) - (0)$$

*are isomorphisms of abelian groups.*

**(3.9.14) Corollary.** *The maps*

$$P \mapsto \text{ the class of } (P) - (O), \qquad D \mapsto \int_D \frac{dy}{x}$$

*induce isomorphisms of abelian groups*

$$(C(\mathbf{C}), \boxplus) \xrightarrow{\sim} Cl^0_{(P_+)+(P_-)}(\widetilde{C}(\mathbf{C})) \xrightarrow{\sim} \mathbf{C}/2\pi\mathbf{Z}.$$

*Proof.* Apply the isomorphism $\lambda$ from Exercise 3.8.4.

**(3.9.15) Why is this interesting?** The point is that the group law "$\boxplus$" on $C(\mathbf{C})$, which was originally defined by transporting the additive group law "+" on $\mathbf{C}/2\pi\mathbf{Z}$ via the composite bijection

$$C(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}/2\pi\mathbf{Z}, \qquad P \mapsto \int_O^P \frac{dy}{x},$$

admits a purely algebraic description, via the bijection

$$C(\mathbf{C}) \xrightarrow{\sim} Cl^0_{(P_+)+(P_-)}(\widetilde{C}(\mathbf{C})), \qquad P \mapsto \text{ the class of } (P) - (O).$$

**(3.9.16) Exercise.** *Let $\mathfrak{m} = (a_1) + \cdots + (a_n) + (\infty) \in \mathrm{Div}(\mathbf{P}^1(\mathbf{C}))$, where $a_1, \ldots, a_n \in \mathbf{C}$ ($n \geq 0$) are distinct points in $\mathbf{C}$. Determine $Cl^0_{\mathfrak{m}}(\mathbf{P}^1(\mathbf{C}))$, by generalizing 3.9.13(i).*

## 4. Cubic curves $y^2 = f(x)$

### 4.1 Basic facts

**(4.1.1)** Let

$$f(x) = (x - e_1)(x - e_2)(x - e_3) = x^3 + ax^2 + bx + c \in \mathbf{C}[x]$$

be a cubic polynomial with distinct roots $e_j \in \mathbf{C}$. Let $E$ be the projectivization of the affine plane curve $y^2 = f(x)$, i.e.

$$E : Y^2Z = (X - e_1Z)(X - e_2Z)(X - e_3Z)$$

(where $x = X/Z, y = Y/Z$). We know from 3.7.7 that $E$ is a smooth projective plane curve over $\mathbf{C}$ with a single point at infinity $O = (0 : 1 : 0)$ ($E(\mathbf{C}) \cap \{Z = 0\} = \{O\}$). By 3.7.5, $E(\mathbf{C})$ is a compact Riemann surface (one can observe directly that $E(\mathbf{C})$ is connected; see the pictures in [Re], p.44 or [Cl], 2.3).

**(4.1.2) Exercise.** *Show that the projection map*

$$p : E(\mathbf{C}) \longrightarrow \mathbf{P}^1(\mathbf{C}), \qquad p(x,y) = x, \qquad p(O) = \infty$$

*is holomorphic, of degree* 2 *and the set of ramification points* $\{(e_1,0),(e_2,0),(e_3,0),O\}$ *(with ramification indices equal to* 2*).*

**(4.1.3) Corollary.** *By the Riemann-Hurwitz formula, the genus* $g = g(E(\mathbf{C}))$ *of* $E(\mathbf{C})$ *satisfies* $2g-2 = (-2)\cdot 2 + 4(2-1) = 0$*, hence* $g = 1$*.*

### 4.2 Holomorphic differentials on $E(\mathbf{C})$

**(4.2.1)** The affine coordinates $x$ and $y$ are non-constant meromorphic functions on $E(\mathbf{C})$ satisfying $y^2 = f(x)$; thus

$$\omega = \frac{dx}{2y} = \frac{dy}{f'(x)} \in \Omega^1_{\mathrm{mer}}(E(\mathbf{C}))$$

is a (non-zero) meromorphic differential on $E(\mathbf{C})$.

**(4.2.2) Proposition.** *$\omega$ is a holomorphic differential on $E(\mathbf{C})$ without zeros, i.e. $\mathrm{ord}_P(\omega) = 0$ for all $P \in E(\mathbf{C})$ ($\iff \mathrm{div}(\omega) = 0$).*

*Proof.* Let $P = (x_P, y_P) \in E(\mathbf{C}) - \{O\}$ be a point on the affine curve

$$V = E - \{O\} : h(x,y) = y^2 - f(x) = 0.$$

We know that $P$ is a smooth point; this means that either $0 \neq \partial h/\partial x(P) = -f'(x_P)$, in which case $y - y_P$ is a local coordinate at $P$ and

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P\left(\frac{d(y-y_P)}{f'(x)}\right) = 0,$$

or $0 \neq \partial h/\partial y(P) = 2y_P$, in which case $x - x_P$ is a local coordinate at $P$ and

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P\left(\frac{d(x-x_P)}{2y}\right) = 0.$$

For $P = O$ we pass to the coordinates $u = x/y, v = 1/y$ used in 3.7.7; then $O$ corresponds to $(u,v) = (0,0)$ and the affine part $E \cap \{Y \neq 0\}$ of $E$ is given by the equation

$$g(u,v) = v - (u - e_1 v)(u - e_2 v)(u - e_3 v) = 0.$$

As $\partial g/\partial v(0,0) \neq 0$, $u$ is a local coordinate at $O$, hence

$$\mathrm{ord}_O(u) = 1, \qquad \mathrm{ord}_O(v) \geq 1, \qquad \mathrm{ord}_O(u - e_j v) \geq 1, \qquad \mathrm{ord}_O(v) = \sum_{j=1}^{3} \mathrm{ord}_O(u - e_j v) \geq 3.$$

By 3.2.2.7, we have

$$\mathrm{ord}_O(u - e_j v) = \min(1, \mathrm{ord}_O(v)) = 1, \qquad \mathrm{ord}_O(v) = \sum_{j=1}^{3} \mathrm{ord}_O(u - e_j v) = 3,$$

hence (using 3.3.8)

$$\mathrm{ord}_O(y) = \mathrm{ord}_O(1/v) = -3, \qquad \mathrm{ord}_O(x) = \mathrm{ord}_O(u/v) = -2, \qquad \mathrm{ord}_O(dx) = -3, \qquad \mathrm{ord}_O(dx/2y) = 0,$$

as claimed.

**(4.2.3) Proposition.** *$\omega$ generates the space of holomorphic differentials on $E(\mathbf{C})$: $\Omega^1(E(\mathbf{C})) = \mathbf{C} \cdot \omega$.*

*Proof.* If $\omega_1 \in \Omega^1(E(\mathbf{C})) - \{0\}$, then $\omega_1 = f \cdot \omega$ for some (non-zero) meromorphic function $f \in \mathcal{M}(E(\mathbf{C}))$ (by 3.3.14). As $\omega_1$ is holomorphic, we obtain from 4.2.2

$$(\forall P \in E(\mathbf{C})) \quad 0 \leq \mathrm{ord}_P(\omega_1) = \mathrm{ord}_P(\omega) + \mathrm{ord}_P(f) = \mathrm{ord}_P(f),$$

hence $f \in \mathcal{O}(E(\mathbf{C}))$ is holomorphic; however, $\mathcal{O}(E(\mathbf{C})) = \mathbf{C}$, by 3.2.3.3.

**(4.2.4) Analytic genus.** Let $X$ be an arbitrary compact Riemann surface. The dimension of the space of holomorphic differentials

$$g_{an}(X) := \dim_{\mathbf{C}} \Omega^1(X)$$

is sometimes referred to as the **analytic genus of** $X$. It follows from the Riemann-Roch Theorem (see ?? below) that

$$(\forall \omega \in \Omega^1_{\mathrm{mer}}(X) - \{0\}) \qquad \deg(\mathrm{div}(\omega)) = 2g_{an}(X) - 2 \tag{4.2.4.1}$$

(note that $\deg(\mathrm{div}(\omega))$ does not depend on the choice of $\omega$, by combining 3.3.16 and 3.3.11).

If $f : X \longrightarrow Y$ is a non-constant holomorphic map between compact Riemann surfaces and $\omega \in \Omega^1_{\mathrm{mer}}(Y) - \{0\}$, then Lemma 3.3.13 implies that

$$\mathrm{div}(f^*(\omega)) = f^*(\mathrm{div}(\omega)) + \sum_{x \in X} (e_x - 1)(x). \tag{4.2.4.2}$$

Combining (4.2.4.1-2) with 3.9.10 we obtain the Riemann-Hurwitz formula 3.6.3, this time for the **analytic** genus. As $g_{an}(\mathbf{P}^1(\mathbf{C})) = 0 = g(\mathbf{P}^1(\mathbf{C}))$ (exercise!), letting $f : X \longrightarrow \mathbf{P}^1(\mathbf{C}))$ be any non-constant meromorphic function, the comparison of the two Riemann-Hurwitz formulas shows that

$$g_{an}(X) = g(X). \tag{4.2.4.3}$$

In particular,

$$\text{if } g(X) = 1, \text{ then} \qquad (\forall \omega \in \Omega^1(X) - \{0\}) \quad \mathrm{div}(\omega) = 0, \tag{4.2.4.4}$$

as $\mathrm{div}(\omega)$ is an effective divisor of degree 0.

For $X = E(\mathbf{C})$, we have verified (4.2.4.1,3,4) explicitly.

**(4.2.5) Hyperelliptic curves.** Let $f(x) \in \mathbf{C}[x]$ be a polynomial of even degree $\deg(f) = 2m \geq 4$ with distinct roots. As in 3.7.8, put $g(u) = u^{2m} f(1/u) \in \mathbf{C}[u]$ and consider the smooth affine plane curves over $\mathbf{C}$

$$V : y^2 - f(x) = 0, \qquad W : v^2 - g(u) = 0$$

and the isomorphism

$$u = 1/x, \qquad v = y/x^m, \qquad x = 1/u, \qquad y = v/u^m \tag{4.2.5.1}$$

between $V \cap \{x \neq 0\} = V - \{P_+, P_-\}$ and $W \cap \{u \neq 0\} = W - \{O_+, O_-\}$, where $P_\pm = (x, y) = (0, \pm\sqrt{f(0)})$, $O_\pm = (u, v) = (0, \pm\sqrt{g(0)})$ (we have $O_+ \neq O_-$, but the points $P_+, P_-$ are not necessarily distinct). Glueing together $V(\mathbf{C})$ and $W(\mathbf{C})$ along their open subsets $V(\mathbf{C}) - \{P_+, P_-\}$, $W(\mathbf{C}) - \{O_+, O_-\}$ using the formulas (4.2.5.1), we obtain a Riemann surface $X$ (cf. 4.2.6(i)). In fact, $X = U(\mathbf{C})$, where $U$ is the curve from 3.7.8.

**(4.2.6) Exercise.** *Let $p : X \longrightarrow \mathbf{P}^1(\mathbf{C})$ be the map*

$$p(x, y) = (x : 1), \qquad (x, y) \in V(\mathbf{C}); \qquad p(u, v) = (1 : u), \qquad (u, v) \in W(\mathbf{C}).$$

*Show that*

(i) *The natural topology on $X$ is Hausdorff.*

(ii) *$X$ is connected (draw a picture! – see [Ki], 1.2.3).*
(iii) *$p$ is a proper holomorphic map of degree* $\deg(p) = 2$.
(iv) *$X$ is compact.*
(v) *The ramification points of $p$ are $(x, y) = (x_j, 0)$, where $x_1, \dots, x_{2m} \in \mathbf{C}$ are the (distinct) roots of $f(x)$.*

**(4.2.7)** It follows from 4.2.6 and 3.6.5 that $g(X) = m - 1$. The same calculation as in the first half of the proof of Proposition 4.2.2 shows that the meromorphic differential

$$\omega := \frac{dx}{y} = \frac{2\,dy}{f'_x} \in \Omega^1_{\mathrm{mer}}(X)$$

is holomorphic on $V(\mathbf{C})$ and has no zeros there. Similarly, $du/v$ is holomorphic on $W(\mathbf{C})$ and has no zeros there. The formulas (4.2.5.1) imply that, for each $k \in \mathbf{Z}$,

$$x^k\omega = \frac{x^k\,dx}{y} = -\frac{u^{m-k-2}\,du}{v},$$

hence

$$\mathrm{div}(x^k\omega) = k(P_+) + k(P_-) + (m-k-2)(O_+) + (m-k-2)(O_-), \qquad \deg(\mathrm{div}(x^k\omega)) = 2m-4 = 2g(X)-2,$$

as

$$\mathrm{div}(x) = (P_+) + (P_-) - (O_+) - (O_-), \qquad \mathrm{div}(u) = -\mathrm{div}(x).$$

It follows that

$$\frac{x^k\,dx}{y} \in \Omega^1(X) \iff 0 \le k \le m-2; \tag{4.2.7.1}$$

in fact, the differentials (4.2.7.1) form a basis of $\Omega^1(X)$, as $\dim_{\mathbf{C}}(\Omega^1(X)) = g(X) = m-1$. This is why they appeared in (2.2.7.5)!

In the special case $m = 2$ ( $\iff$ $\deg(f) = 4$), we obtain that $\mathrm{div}(\omega) = 0$, verifying (4.2.4.4) explicitly. The proof of 4.2.3 then yields directly $\Omega^1(X) = \mathbf{C} \cdot \omega$, without using the general theory invoked in 4.2.4.

**(4.2.8) Exercise.** *Let $V : f(x, y) = 0$ be a smooth affine plane curve over $\mathbf{C}$ of degree $\deg(f) = d \ge 1$ such that its projectivization $\widetilde{V} : F(X, Y, Z) = Z^d f(X/Z, Y/Z) = 0 \subset \mathbf{P}^2$ intersects the line at infinity at $d$ distinct points $\widetilde{V}(\mathbf{C}) \cap \{Z = 0\} = \{P_1, \dots, P_d\}$. Show that $\widetilde{V}$ is smooth and that the divisor of the meromorphic differential*

$$\omega = \frac{dx}{f'_y} = -\frac{dy}{f'_x} \in \Omega^1_{\mathrm{mer}}(\widetilde{V}(\mathbf{C})) - \{0\}$$

*is equal to*

$$\mathrm{div}(\omega) = (d-3)\sum_{j=1}^{d}(P_j),$$

*hence the genus of $\widetilde{V}(\mathbf{C})$ is equal to*

$$g(\widetilde{V}(\mathbf{C})) = 1 + \mathrm{div}(\omega)/2 = \frac{(d-1)(d-2)}{2}.$$

*Deduce that the differentials*

$$x^i y^j \omega \qquad (0 \le i, j;\ i + j \le d-3)$$

form a basis of $\Omega^1(\widetilde{V}(\mathbf{C}))$, hence

$$\Omega^1(\widetilde{V}(\mathbf{C})) = \{h(x,y)\,\omega \,|\, h(x,y) \in \mathbf{C}[x,y],\ \deg(h) \leq d-3\}.$$

### 4.3 Topology of $E(\mathbf{C})$

**(4.3.1)** We know from 4.1.3 that $E(\mathbf{C})$ is a compact oriented surface of genus $g = 1$. This implies that the fundamental group $\pi_1(E(\mathbf{C}), O)$ is abelian, naturally isomorphic to the first homology group $H_1(E(\mathbf{C}), \mathbf{Z}) \xrightarrow{\sim} \mathbf{Z}^2$. Choose a $\mathbf{Z}$-basis $[\gamma_1], [\gamma_2]$ of $H_1(E(\mathbf{C}), \mathbf{Z}) = \mathbf{Z}[\gamma_1] \oplus \mathbf{Z}[\gamma_2]$ and put

$$\omega_j = \int_{[\gamma_j]} \omega \in \mathbf{C} \qquad\qquad (j = 1, 2).$$

The group of periods of $\omega$ on $E(\mathbf{C})$ is then equal to

$$L = \{\int_\gamma \omega \,|\, \gamma \text{ a closed path on } E(\mathbf{C})\} = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 \subset \mathbf{C}.$$

**(4.3.2) Proposition.** *$L$ is a lattice in $\mathbf{C}$, i.e. the periods $\omega_1, \omega_2 \in \mathbf{C}$ are linearly independent over $\mathbf{R}$. More precisely, if $[\gamma_1], [\gamma_2]$ are represented by closed paths $\gamma_1, \gamma_2$ based at $O$, disjoint outside $O$, with tangent vectors to $\gamma_2, \gamma_1$ (in this order) forming a positively oriented basis of the tangent space at $O$, then $\mathrm{Im}(\omega_1\overline{\omega}_2) > 0$.*

*Proof.* Cutting $E(\mathbf{C})$ along the paths $\gamma_1, \gamma_2$, we obtain a simply connected domain $D$. For $P \in D$, define $f(P) = \int_O^P \omega$, where the integral is taken along (any) path in $D$. This defines a holomorphic function $f \in \mathcal{O}(D)$ satisfying $df = \omega$. As

$$d(f\overline{\omega}) = df \wedge \overline{\omega} + f d\overline{\omega} = \omega \wedge \overline{\omega}$$

in $D$, Stokes' theorem yields

$$\frac{i}{2} \int_{E(\mathbf{C})} \omega \wedge \overline{\omega} = \frac{i}{2} \int_{\partial D} f\overline{\omega}. \tag{4.3.2.1}$$

As the values of $f(P)$ on two points of $\partial D$ corresponding to the same point of $\gamma_1$ (resp. $\gamma_2$) differ by $\omega_2$ (resp. by $\omega_1$), the integral (4.3.2.1) is equal to

$$\frac{i}{2}\,(\overline{\omega}_1\omega_2 - \omega_1\overline{\omega}_2) = \mathrm{Im}(\omega_1\overline{\omega}_2).$$

(see ([Gr-Ha], Sect. 2.2; [MK], 3.9) for a more general calculation). Proposition follows, as (4.3.2.1) is positive by (3.5.4.1)

**(4.3.3) Corollary.** *The quotient $\mathbf{C}/L$ is a compact Riemann surface and the canonical projection $\mathbf{C} \longrightarrow \mathbf{C}/L$ is an unramified covering.*

**(4.3.4)** Attentive readers will have noticed that the proof of Proposition 4.3.2 works for any non-zero holomorphic differential $\varphi$ on any compact Riemann surface $X$ of genus 1. However, it follows from the Riemann-Roch Theorem that every such pair $(X, \varphi)$ is isomorphic to $(E(\mathbf{C}), \omega)$, for a suitable cubic polynomial $f(x)$.

### 4.4 The Abel-Jacobi map

**(4.4.1)** As in 0.2.1, one can define the **Abel-Jacobi map** for $E(\mathbf{C})$ by the formula

$$\alpha : E(\mathbf{C}) \longrightarrow \mathbf{C}/L, \qquad \alpha(P) = \int_O^P \omega \ (\mathrm{mod}\, L).$$

This is a holomorphic map satisfying $\alpha^*(dz) = \omega$ and the induced map on homology groups

$$\alpha_* : H_1(E(\mathbf{C}), \mathbf{Z}) \longrightarrow H_1(\mathbf{C}/L, \mathbf{Z}) = L$$

is an isomorphism, as

$$\{\int_\gamma dz \,|\, \gamma \text{ a closed path on } \mathbf{C}/L\} = L.$$

Above, the canonical identification of $L$ and the first homology group of $\mathbf{C}/L$ is defined as follows: one associates to each $u \in L$ the homology class of the projection to $\mathbf{C}/L$ of any path in $\mathbf{C}$ from 0 to $u$ (this is well-defined, as $\mathbf{C}$ is contractible).

**(4.4.2) Theorem.** *The map $\alpha : E(\mathbf{C}) \longrightarrow \mathbf{C}/L$ is an isomorphism of compact Riemann surfaces.*

*Proof.* By 3.2.3.4 it is sufficient to show that $\alpha$ is bijective. For each $P \in E(\mathbf{C})$,

$$\mathrm{ord}_P(\alpha^*(d(z - \alpha(P)))) = \mathrm{ord}_P(\alpha^*(dz)) = \mathrm{ord}_P(\omega) = 0,$$

hence $e_P = 1$, by 3.3.13 (in other words, we use (4.2.4.2) for $f = \alpha$ and $\omega = dz$). This implies that $\alpha$ is an unramified covering, by 3.2.3.5. As the induced map on fundamental groups

$$\pi_1(E(\mathbf{C}), O) = H_1(E(\mathbf{C}), \mathbf{Z}) \xrightarrow{\alpha_*} H_1(\mathbf{C}/L, \mathbf{Z}) = \pi_1(\mathbf{C}/L, 0)$$

is an isomorphism, theory of covering spaces implies that $\alpha$ is a bijection, as required.

**(4.4.3) The inverse of $\alpha$.** The Abel-Jacobi map $\alpha$ is an analogue of the function arcsin (resp. log) from 0.1 (resp. 0.2.3). Its inverse is then a natural generalization of the functions $(\sin, \cos)$ (resp. exp).

For $z \in \mathbf{C}/L - \{0\}$, $\alpha^{-1}(z) \in E(\mathbf{C}) - \{O\}$ is given by a pair of holomorphic functions $U, V$ on $\mathbf{C}/L - \{0\}$:

$$\alpha^{-1}(z) = (U(z), V(z)) = (x, y).$$

The relations $y^2 = f(x)$ and $dx/2y = \alpha^*(dz)$ imply that

$$V(z)^2 = f(U(z)) = U(z)^3 + aU(z)^2 + bU(z) + c,$$
$$U'(z)\, dz/2V(z) = dz \Longrightarrow U'(z) = 2V(z),$$

hence

$$U'(z)^2 = 4(U(z)^3 + aU(z)^2 + bU(z) + c).$$

The functions $U(z), V(z)$ are meromorphic on $\mathbf{C}/L$ and satisfy

$$\mathrm{ord}_0(U(z)) = \mathrm{ord}_O(x) = -2, \qquad \mathrm{ord}_0(V(z)) = \mathrm{ord}_O(y) = -3,$$

by the calculation at the end of the proof of 4.2.2.

$U(z)$ and $V(z)$ are prototypical examples of *elliptic functions*, i.e. doubly periodic (with respect to $\omega_1$ and $\omega_2$) meromorphic functions on $\mathbf{C}$. It would be interesting to have a more direct construction of these functions. This will be (among others) the subject matter of the next three sections.

**(4.4.4)** It follows from (4.2.4.4) that the discussion in 4.4.1 and the proof of Theorem 4.4.2 apply to any compact Riemann surface $X$ of genus 1 and any non-zero holomorphic differential $\omega \in \Omega^1(X) - \{0\}$ (in particular, to $X$ and $\omega$ from 4.2.7 for $m = 2$).

## 5. Elliptic functions (general theory)

### 5.1 Basic facts

Throughout Section 5, $L \subset \mathbf{C}$ is a lattice, i.e. an additive subgroup of the form $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, where $\omega_1, \omega_2 \in \mathbf{C}$ are linearly independent over $\mathbf{R}$.

**(5.1.1) Change of basis.** We have $L = \mathbf{Z}\omega_1' + \mathbf{Z}\omega_2'$ if and only if

$$\begin{aligned} \omega_1' &= a\omega_1 + b\omega_2 \\ \omega_2' &= c\omega_1 + d\omega_2, \end{aligned} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z}).$$

Recall that $GL_n(R)$ denotes, for every commutative ring $R$, the group of those invertible $n \times n$ matrices with coefficients in $R$ whose inverse also has entries in $R$ (i.e. whose determinant is invertible in $R$).

We often consider only *positively oriented* bases $\omega_1, \omega_2$, i.e. those for which $\mathrm{Im}(\omega_1/\omega_2) > 0$. In that case the new basis $\omega_1', \omega_2'$ is positively oriented if and only if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \{g \in GL_2(\mathbf{Z}) \,|\, \det(g) > 0\} = SL_2(\mathbf{Z}).$$

**(5.1.2)** A function $F : \mathbf{C} \longrightarrow \mathbf{C}$ (resp. $\longrightarrow \mathbf{P}^1(\mathbf{C})$) is called *L-periodic* if it factors as

$$F : \mathbf{C} \xrightarrow{pr} \mathbf{C}/L \xrightarrow{f} \mathbf{C} \qquad (\text{resp. } \xrightarrow{f} \mathbf{P}^1(\mathbf{C})),$$

i.e. if

$$F(z+u) = F(z) \qquad (z \in \mathbf{C},\ u \in L).$$

As the projection $pr$ is an unramified covering, $F$ is holomorphic (resp. meromorphic) if and only $f$ is.

**(5.1.3) Definition.** *An* **elliptic function** *(with respect to L) is a meromorphic function $f \in \mathcal{M}(\mathbf{C}/L)$ (equivalently, an L-periodic meromorphic function $F = f \circ pr \in \mathcal{M}(\mathbf{C})$).*

**(5.1.4) Lemma.** *A holomorphic elliptic function is constant.*

*Proof.* $\mathbf{C}/L$ is a compact Riemann surface.

**(5.1.5)** Our goal is to describe explicitly all elliptic functions with respect to $L$. We begin by investigating their divisors.

### 5.2 Divisors of elliptic functions

**(5.2.1) Proposition.** *Let $f \in \mathcal{M}(\mathbf{C}/L) - \{0\}$. Then*

$$\sum_{x \in \mathbf{C}/L} \mathrm{ord}_x(f) = 0 \in \mathbf{Z}$$

$$\sum_{x \in \mathbf{C}/L} \mathrm{ord}_x(f) \cdot x = 0 \in \mathbf{C}/L$$

*(in the second statement, the sum is taken with respect to the addition on $\mathbf{C}/L$).*

*Proof.* Compute the integral of $f'(z)/f(z)\,dz$ (resp. of $zf'(z)/f(z)\,dz$) over the boundary $\partial D$ of a fundamental parallelogram $D = \{z = \alpha + t_1\omega_1 + t_2\omega_2 \,|\, 0 \le t_1, t_2 \le 1\}$ for the action of $L$ on $\mathbf{C}$ (for $\alpha \in \mathbf{C}$ chosen in such a way that $f(z)$ has no zeros nor poles on $\partial D$). See ([La], Ch.1, Thm. 2,3; [Si 1], Ch. VI, Thm. 2.2) for more details.

**(5.2.2)** This result can be reformulated as follows: the group of principal divisors $P(\mathbf{C}/L) \subset \mathrm{Div}^0(\mathbf{C}/L)$ is contained in the kernel of the "sum" homomorphism

$$\boxplus : \mathrm{Div}(\mathbf{C}/L) \longrightarrow \mathbf{C}/L, \qquad \sum n_j(P_j) \mapsto \sum n_j P_j \tag{5.2.2.1}$$

(where the second sum is the addition on $\mathbf{C}/L$). In other words, $\boxplus$ induces a homomorphism (surjective)

$$\boxplus : Cl^0(\mathbf{C}/L) \longrightarrow \mathbf{C}/L. \tag{5.2.2.2}$$

The next step is to show that the conditions in 5.2.1 characterize divisors of elliptic functions, i.e. that (5.2.2.2) is an isomorphism generalizing the isomorphisms from 3.9.13(ii) and 3.9.14.

## 5.3 Construction of elliptic functions (Jacobi's method)

**(5.3.1) Change of variables.** It is often useful to normalize the lattice $L$ and the torus $\mathbf{C}/L$ by the following changes of variables (isomorphisms of compact Riemann surfaces):

$$\mathbf{C}/(\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) \xrightarrow{\sim} \mathbf{C}/(\mathbf{Z}\tau + \mathbf{Z}), \qquad z \mapsto z/\omega_2 \tag{5.3.1.1}$$

(where $\tau = \omega_1/\omega_2$, $\mathrm{Im}(\tau) > 0$) and

$$\mathbf{C}/(\mathbf{Z}\tau + \mathbf{Z}) \xrightarrow{\sim} \mathbf{C}^*/q^{\mathbf{Z}}, \qquad z \mapsto t = e^{2\pi i z} \qquad (q = e^{2\pi i \tau},\ 0 < |q| < 1). \tag{5.3.1.2}$$

In other words, we get rid of the period 1 by applying the exponential map

$$\mathbf{C}/\mathbf{Z} \xrightarrow{\sim} \mathbf{C}^*, \qquad z \mapsto e^{2\pi i z},$$

which replaces the additive periodicity with respect to $\tau$ by the multiplicative periodicity with respect to $q$.

**(5.3.2) Multiplicative periodicity.** In terms of the multiplicative variable $t = \exp(2\pi i z)$, an elliptic function $f \in \mathcal{M}(\mathbf{C}^*/q^{\mathbf{Z}})$ is the same thing as a meromorphic function $f \in \mathcal{M}(\mathbf{C}^*)$ satisfying

$$f(qt) = f(t) \qquad (t \in \mathbf{C}^*,\ |q| < 1). \tag{5.3.2.1}$$

A natural attempt to construct such a function would be to consider the following infinite product:

$$f(t) = \prod_{n \in \mathbf{Z}} g(q^n t) \tag{5.3.2.2}$$

for a suitable function $g(t)$. Taking the simplest choice of $g(t) = 1 - t$ (which has a simple zero at the origin $t = 1$ of the multiplicative group $\mathbf{C}^*$), we see that the two parts of the infinite product

$$\prod_{n \in \mathbf{Z}} (1 - q^n t) = \prod_{n \geq 0} (1 - q^n t) \prod_{n < 0} (1 - q^n t) \tag{5.3.2.3}$$

have a completely different behaviour: as $\sum_{n \geq 0} |q^n| < \infty$, the product over $n \geq 0$ is convergent, but the terms of the product over $n < 0$ have absolute values tending to infinity (since $|q^{-1}| > 1$).

This means that we have to modify the terms corresponding to $n < 0$ in (5.3.2.3) to ensure the convergence. A natural guess would be to replace $(1 - q^n t)$ by $(1 - q^{-n} t^{-1})$, i.e. to consider the function

$$a(t) = (1 - t) \prod_{n=1}^{\infty} (1 - q^n t)(1 - q^n t^{-1}) \qquad (t \in \mathbf{C}^*,\ |q| < 1). \tag{5.3.2.4}$$

**(5.3.3) Proposition.** (i) *The infinite product (5.3.2.4) is uniformly convergent on compact subsets of* $\mathbf{C}^*$ *to a holomorphic function* $a(t) \in \mathcal{O}(\mathbf{C}^*)$.
(ii) *The function* $a(t)$ *has simple zeros at the points* $t = q^n r$ $(n \in \mathbf{Z})$ *and no other zeros in* $\mathbf{C}^*$.
(iii) $a(qt) = (1 - t^{-1})/(1 - t)a(t) = -t^{-1}a(t)$ $\qquad (t \in \mathbf{C}^*)$.

*Proof.* (i),(ii) This follows from the convergence of $\sum_n |q|^n$, by ([Ru 2], Thm. 15.6). The formula in (iii) is proved by a direct calculation.

**(5.3.4) Back to the additive variables.** Rewriting $a(t)$ in terms of the additive variable $z \in \mathbf{C}$, we define

$$A(z) = a(e^{2\pi i z}).$$

By 5.3.3, $A(z)$ is a holomorphic function on $\mathbf{C}$ with simple zeros at the points of the lattice $z \in \mathbf{Z}\tau + \mathbf{Z}$ (and no other zeros) satisfyng

$$\begin{aligned} A(z+1) &= A(z) \\ A(z+\tau) &= -e^{-2\pi i z} A(z). \end{aligned} \tag{5.3.4.1}$$

Using these properties of $A(z)$ we are now ready to prove the promised converse of 5.2.1.

**(5.3.5) Proposition.** *Let $L \subset \mathbf{C}$ be a lattice and $D = \sum_j n_j(P_j) \in \mathrm{Div}(\mathbf{C}/L)$ a divisor satisfying $\sum n_j = 0 \in \mathbf{Z}$ and $\sum n_j P_j = 0 \in \mathbf{C}/L$. Then $D = \mathrm{div}(f)$ for some meromorphic function $f \in \mathcal{M}(\mathbf{C}/L) - \{0\}$ ($f$ is determined up to multiplication by a constant, by 3.9.4).*

*Proof.* Applying (5.3.1.1), we can assume that $L = \mathbf{Z}\tau + \mathbf{Z}$, $\mathrm{Im}(\tau) > 0$. Writing $D = \sum((P_j) - (Q_j))$ with $\sum P_j = \sum Q_j \in \mathbf{C}/L$ (where the points $P_j, Q_j \in \mathbf{C}/L$ are *not* necessarily distinct), there exist representatives $a_j$ (resp. $b_j$) of $P_j$ (resp. $Q_j$) in $\mathbf{C}$ such that $\sum a_j = \sum b_j \in \mathbf{C}$. Define

$$F(z) = \prod_j \frac{A(z-a_j)}{A(z-b_j)}.$$

This is a meromorphic function on $\mathbf{C}$ satisfying $F(z+1) = F(z)$ and

$$\frac{F(z+\tau)}{F(z)} = \prod_j \frac{A(z-a_j+\tau)}{A(z-a_j)} \frac{A(z-b_j)}{A(z-b_j+\tau)} = \prod_j \exp(-2\pi i((z-a_j)-(z-b_j))) = 1,$$

since $\sum a_j = \sum b_j$. This means that $F$ is $L$-periodic, $F = f \circ pr$ for some $f \in \mathcal{M}(\mathbf{C}/L)$. As each term

$$\frac{A(z-a_j)}{A(z-b_j)}$$

has simple zeros (resp. simple poles) at the points $a_j + L$ (resp. $b_j + L$), the divisor of $f$ is equal to $\sum((pr(a_j)) - (pr(b_j))) = \sum((P_j) - (Q_j)) = D$.

**(5.3.6) Theorem.** *The homomorphism $\boxplus : \mathrm{Div}(\mathbf{C}/L) \longrightarrow \mathbf{C}/L$ defined in (5.2.2.1) induces an isomorphism of abelian groups*

$$Cl^0(\mathbf{C}/L) \xrightarrow{\sim} \mathbf{C}/L,$$

*with inverse given by the map*

$$a \mapsto \text{ the class of } (a) - (0).$$

*Proof.* Combine 5.2.1 and 5.3.5.

**(5.3.7)** One can deduce from this isomorphism all function theory on the torus $\mathbf{C}/L$.

## 6. Theta functions

We shall only scratch the surface of the enormously rich theory of theta functions, which is treated in great detail in [Mu TH] (and also in [Web], [Mu AV], Ch. 1; [MK]; [Gr-Ha], 2.6, [Wei 1] and [Fa-Kr 2]).

### 6.1 What is a theta function?

**(6.1.1) Definition.** *A* **theta function** *(with respect to a lattice $L \subset \mathbf{C}$) is a holomorphic function $F(z) \in \mathcal{O}(\mathbf{C})$ satisfying the functional equations*

$$F(z+u) = e^{a(u)z+b(u)}F(z) \qquad (z \in \mathbf{C},\ u \in L) \tag{6.1.1.1}$$

*(for some constants $a(u), b(u) \in \mathbf{C}$ depending on $u \in L$).*

**(6.1.2)** It is sufficient to check the condition (6.1.1.1) for $u$ belonging to a set of generators of $L$. This means that a theta function with respect to $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ is characterized by the functional equations

$$\begin{aligned} F(z+\omega_1) &= e^{a_1 z+b_1}F(z) \\ F(z+\omega_2) &= e^{a_2 z+b_2}F(z), \end{aligned} \tag{6.1.2.1}$$

where $a_1, a_2, b_1, b_2 \in \mathbf{C}$. Jacobi's method of constructing elliptic functions (with respect to $L$) consists in taking a quotient $F_1/F_2$ of two non-zero solutions of (6.1.2.1).

**(6.1.3) Example:** If $L = \mathbf{Z}\tau + \mathbf{Z}$, $q = \exp(2\pi i\tau)$ and $t = \exp(2\pi iz)$, then the function

$$A(z) = (1-t)\prod_{n=1}^{\infty}(1-q^n t)(1-q^n t^{-1})$$

from 5.3.4 is a theta function (with respect to $L$).

**(6.1.4) Question.** What is a theta function? It is certainly *not* a function on $\mathbf{C}/L$ (unless it is constant).

**(6.1.5) Answer.** Theta functions are sections of line bundles on $\mathbf{C}/L$.

### 6.2 A digression on line bundles

Line bundles on Riemann surfaces are discussed in ([Fo], Sect. 29, 30); general theory of vector bundles over complex manifolds is treated in [Gr-Ha]. We follow closely (a small part of) [Mu AV], Ch. 1.

**(6.2.1) Definition.** *Let $X$ be a complex manifold (e.g. a Riemann surface). A* **(holomorphic) line bundle** *over $X$ is a complex manifold $\mathscr{L}$ equipped with a surjective holomorphic map $p : \mathscr{L} \longrightarrow X$ such that:*
(i) *The fibre $\mathscr{L}_x = p^{-1}(x)$ over each $x \in X$ is a vector space over $\mathbf{C}$ of dimension 1.*
(ii) *$\mathscr{L}$ is locally isomorphic to the product $X \times \mathbf{C}$ in the following sense: there exists an open covering $\{U_\alpha\}$ of $X$ and holomorphic isomorphisms $f_\alpha : p^{-1}(U_\alpha) \xrightarrow{\sim} U_\alpha \times \mathbf{C}$ which make the diagram*

$$\begin{array}{ccc} p^{-1}(U_\alpha) & \xrightarrow{\sim} & U_\alpha \times \mathbf{C} \\ \big\downarrow{\scriptstyle p} & & \big\downarrow{\scriptstyle pr} \\ U_\alpha & = & U_\alpha \end{array}$$

*commutative and induce linear maps on the fibres over each $x \in U_\alpha$ (above, $pr$ denotes the projection on the first factor). A* **(holomorphic) section** *of $\mathscr{L}$ is a holomorphic map $s : X \longrightarrow \mathscr{L}$ such that $p \circ s = \mathrm{id}$. The set $\Gamma(X, \mathscr{L})$ of holomorphic sections of $\mathscr{L}$ is a module over $\mathcal{O}(X)$. An* **isomorphism** *between $\mathscr{L}$ and*

*another (holomorphic) line bundle $p' : \mathscr{L}' \longrightarrow X$ is a holomorphic isomorphism $f : \mathscr{L} \xrightarrow{\sim} \mathscr{L}'$ satisfying $p' \circ f = p$, which is linear on each fibre $p^{-1}(x)$ $(x \in X)$.*

**(6.2.2)** More generally, if we replace $\mathbf{C}$ in 6.2.1(ii) by $\mathbf{C}^N$ (and 1 in 6.2.1(i) by $N$), we obtain the definition of a (holomorphic) vector bundle of rank $N$ over $X$. Line bundles are much easier to study then vector bundles of rank $N > 1$; the main reason being that the group of automorphisms of the fibre $GL_1(\mathbf{C}) = \mathbf{C}^*$ is abelian.

**(6.2.3) Examples:** (1) The **trivial** line bundle is the product $pr : X \times \mathbf{C} \longrightarrow X$. There is a canonical isomorphism

$$\mathcal{O}(X) \xrightarrow{\sim} \Gamma(X, X \times \mathbf{C}), \qquad f \mapsto s(x) = (x, f(x)).$$

(2) If $p : \mathscr{L} \longrightarrow X$ is a (holomorphic) line bundle and $f : Y \longrightarrow X$ is a holomorphic map (where $Y$ is another complex manifold), then the pull-back of $\mathscr{L}$ via $f$

$$f^*\mathscr{L} = \{(y, \ell) \in Y \times \mathscr{L} \,|\, f(y) = p(\ell)\}$$

with the map $q(y, \ell) = y$ is a (holomorphic) line bundle over $Y$.
(3) By definition of the projective space,

$$\mathbf{P}^N(\mathbf{C}) = \{V \subset \mathbf{C}^{N+1} \mid \dim(V) = 1\}.$$

The **tautological line bundle** over $\mathbf{P}^N(\mathbf{C})$ is

$$\mathscr{L} = \{(v, V) \in \mathbf{C}^{N+1} \times \mathbf{P}^N(\mathbf{C}) \,|\, v \in V\}$$

together with the map $p(v, V) = V$.

**(6.2.4) The basic setup.** Assume that $Y$ is a complex manifold, $G$ a group acting on $Y$ by holomorphic automorphisms and that the action of each $g \in G - \{e\}$ has no fixed points (i.e. $gy \neq y$ for all $y \in Y$).

We are going to construct line bundles on the quotient $X = G\backslash Y$ from lifts of the $G$-action from $Y$ to the trivial line bundle $Y \times \mathbf{C}$. The reader should keep in mind the following two examples:

(A) $Y = \mathbf{C}$, $G = L$ (a lattice acting by translations), $X = \mathbf{C}/L$.
(B) $Y = \mathbf{C}^{N+1} - \{0\}$, $G = \mathbf{C}^*$ (acting by multiplication), $X = \mathbf{P}^N(\mathbf{C})$ $(N \geq 1)$.

**(6.2.5) Lifted action.** In order to lift the $G$-action from $Y$ to the trivial line bundle $Y \times \mathbf{C}$ we must construct, for each $g \in G$, a holomorphic map $\widehat{g} : Y \times \mathbf{C} \longrightarrow Y \times \mathbf{C}$ which makes the following diagram commutative:

$$\begin{array}{ccc} Y \times \mathbf{C} & \xrightarrow{\widehat{g}} & Y \times \mathbf{C} \\ \downarrow{\scriptstyle pr} & & \downarrow{\scriptstyle pr} \\ Y & \xrightarrow{g} & Y, \end{array} \tag{6.2.5.1}$$

acts on each fiber $\{y\} \times \mathbf{C}$ by a linear automorphism and such that

$$\widehat{g_1 g_2} = \widehat{g}_1 \widehat{g}_2 \qquad (g_1, g_2 \in G). \tag{6.2.5.2}$$

In concrete terms, the linearity on the fibers amounts to

$$\widehat{g}(y, t) = (gy, \alpha_g(y)\, t), \qquad (y \in Y,\ t \in \mathbf{C}) \tag{6.2.5.3}$$

where $\alpha_g : Y \longrightarrow \mathbf{C}^*$ is an invertible holomorphic function on $Y$. The identity (6.2.5.2) is then equivalent to

$$\alpha_{g_1 g_2}(y) = \alpha_{g_1}(g_2(y))\, \alpha_{g_2}(y). \tag{6.2.5.4}$$

Conversely, if $\alpha_g : Y \longrightarrow \mathbf{C}^*$ is a set of holomorphic functions satisfying the identity (6.2.5.4), then (6.2.5.3) defines the lift of the $G$-action from $Y$ to $Y \times \mathbf{C}$.

**(6.2.6) A remark for Bourbakists (only).** The identity (6.2.5.4) is, essentialy, a 1-cocycle identity for the $G$-action on the group $\mathcal{O}(Y)^*$ of invertible holomorphic functions on $Y$. Note, however, that $G$ acts on $\mathcal{O}(Y)^*$ on the right (by $\alpha * g(y) = \alpha(gy)$), since we have started with a left $G$-action on $Y$. It is more customary to let $G$ act on $Y$ on the right, which then leads to the "usual" 1-cocycle relation for a left $G$-action on $\mathcal{O}(Y)^*$. Of course, if the group $G$ is abelian (which is the case in the two examples 6.2.4(A),(B)), there is no difference between left and right actions.

**(6.2.7) Example:** If, for each $g \in G$, $\alpha_g(y) = \alpha_g$ is a constant function, then (6.2.5.4) says that the map

$$\rho : G \longrightarrow \mathbf{C}^*, \qquad \rho(g) = \alpha_g$$

is a group homomorphism. Using this observation, we can define for each integer $d \in \mathbf{Z}$ a lifted action in Example 6.2.4(B) by the formula

$$\widehat{g}(y,t) = (gy, g^d t). \tag{6.2.7.1}$$

**(6.2.8) Definition of $\mathscr{L}$.** Given the lifted action as in 6.2.5, the commutativity of the diagram (6.2.5.1) implies that the projection $pr$ induces a map between the quotient spaces

$$p : \mathscr{L} = G\backslash(Y \times \mathbf{C}) \longrightarrow G\backslash Y = X, \qquad p(\widehat{\pi}(y,t)) = \pi(y).$$

where

$$\pi : Y \longrightarrow G\backslash Y, \qquad \widehat{\pi} : Y \times \mathbf{C} \longrightarrow G\backslash(Y \times \mathbf{C})$$

denote the canonical projections. In the generality we are considering, $\mathscr{L}$ and $G$ are merely topological spaces (equipped with the quotient topology) and $p$ is a continuous map. However, the fact that $G$ acts on $Y$ without fixed points implies that

$$\widehat{\pi}(y,t_1) = \widehat{\pi}(y,t_2) \iff t_1 = t_2, \tag{6.2.8.1}$$

hence each fibre $p^{-1}(\pi(y))$ consists of the *distincts* points $\widehat{\pi}(y,t)$ ($t \in \mathbf{C}$). Moreover, the structure of the complex vector space on $p^{-1}(\pi(y))$ (using the coordinate $t$) depends only on $\pi(y)$ (as each $\widehat{g}$ acts linearly on the fibers of $pr$).

**(6.2.9) Sections of $\mathscr{L}$.** Disregarding for the moment the question of holomorphic structure, we want to describe set-theoretical sections of $p : \mathscr{L} \longrightarrow X$, i.e. maps $s : X \longrightarrow \mathscr{L}$ satisfying $p \circ s = \mathrm{id}$. The commutative diagram

$$\begin{array}{ccc} Y \times \mathbf{C} & \xrightarrow{\widehat{\pi}} & G\backslash(Y \times \mathbf{C}) \\ \downarrow{\scriptstyle pr} & & \downarrow{\scriptstyle p} \\ Y & \xrightarrow{\pi} & G\backslash Y \end{array}$$

together with (6.2.8.1) imply that that there is a uniquely determined function $F : Y \longrightarrow \mathbf{C}$ such that

$$s \circ \pi(y) = \widehat{\pi}(y, F(y)) \qquad (\forall y \in Y). \tag{6.2.9.1}$$

For which functions $F$ does (6.2.9.1) define a (set-theoretical) section $s$ of $\mathscr{L}$? The necessary and sufficient condition is that the R.H.S. of (6.2.9.1) should depend only on $\pi(y)$, i.e.

$$\widehat{\pi}(gy, F(gy)) = \widehat{\pi}(y, F(y)) \qquad (\forall y \in Y,\ \forall g \in G),$$

which is equivalent to

$$\widehat{\pi}(gy, F(gy)) = \widehat{\pi}(y, F(y)) = \widehat{\pi}(\widehat{g}(y, F(y))) = \widehat{\pi}(gy, \alpha_g(y)\, F(y)),$$

hence, by (6.2.8.1), to

$$F(gy) = \alpha_g(y)\, F(y) \qquad (\forall y \in Y,\ \forall g \in G). \tag{6.2.9.2}$$

Note the similarity to the functional equation (6.1.1.1) of theta functions!

**(6.2.10)** In good circumstances, both $X$ and $\mathscr{L}$ are complex manifolds, $p : \mathscr{L} \longrightarrow X$ is a line bundle and the description (6.2.9.1-2) of the sections of $\mathscr{L}$ also holds in the holomorphic category, inducing a bijection between

$$\Gamma(X, \mathscr{L}) \xrightarrow{\sim} \{F \in \mathcal{O}(Y) \,|\, F \text{ satisfies (6.2.9.2)}\}.$$

The line bundles $\mathscr{L}$ on $X$ obtained by this construction are not completely arbitrary: by definition, their pull-backs to $Y$ are trivial, $\pi^*(\mathscr{L}) = Y \times \mathbf{C}$.

**(6.2.11) Exercise.** *Show that such "good circumstances" occur in the situation of 3.2.1.6 (in particular, in Example 6.2.4(A)).*

**(6.2.12) Example:** In the situation of 6.2.4(B), $\Gamma(X, \mathscr{L})$ is isomorphic to the complex vector space of holomorphic functions

$$F : \mathbf{C}^{N+1} - \{0\} \longrightarrow \mathbf{C}, \qquad F(gy) = g^d\, F(y) \qquad (\forall g \in \mathbf{C}^*). \tag{6.2.12.1}$$

**(6.2.13) Exercise.** *Show that the space (6.2.12.1) consists of all homogeneous polynomials of degree $d$ (resp. is trivial) if $d \geq 0$ (resp. if $d < 0$). Show that the case $d = -1$ corresponds to the tautological line bundle from 6.2.3(3).*

**(6.2.14) Equivalent lifts.** We obtain isomorphic objects if we reparametrize the trivial line bundle $Y \times \mathbf{C} \longrightarrow Y$ (linearly along the fibers), i.e. by a holomorphic isomorphism (a "gauge transformation")

$$r : Y \times \mathbf{C} \xrightarrow{\sim} Y \times \mathbf{C}, \qquad (y, t) \mapsto (y, \beta(y)\, t),$$

where $\beta : Y \longrightarrow \mathbf{C}^*$ is an invertible holomorphic function. This leads to a new lift $\widehat{g}^{\text{new}}$ of the $G$-action, given by the commutative diagram

$$\begin{array}{ccc} Y \times \mathbf{C} & \xrightarrow{\widehat{g}} & Y \times \mathbf{C} \\ \big\downarrow \wr r & & \big\downarrow \wr r \\ Y \times \mathbf{C} & \xrightarrow{\widehat{g}^{\text{new}}} & Y \times \mathbf{C}. \end{array}$$

Inother words,

$$(gy, \alpha_g^{\text{new}}(y)\, \beta(y)\, t) = g^{\text{new}}(r(y,t)) = r(\widehat{g}(y,t)) = r(gy, \alpha_g(y)\, t) = (gy, \beta(gy)\, \alpha_g(y)\, t),$$

which is equivalent to

$$\alpha_g^{\text{new}}(y) = \frac{\beta(gy)}{\beta(y)}\, \alpha_g(y) \qquad (y \in Y,\ g \in G). \tag{6.2.14.1}$$

In other words, $\alpha_g^{\text{new}}$ and $\alpha_g$ differ by a 1-coboundary.

Under this reparametrization, $\mathscr{L}$ does not change, but the projection map $\widehat{\pi} : Y \times \mathbf{C} \longrightarrow \mathscr{L}$ is replaced by $\widehat{\pi}^{\text{new}}$ satisfying $\widehat{\pi}^{\text{new}} \circ r = \widehat{\pi}$. Similarly, the description of the sections (6.2.9.1-2) of $\mathscr{L}$ still holds, if we replace $F(y)$ by

$$F^{\text{new}}(y) = \beta(y)\, F(y). \tag{6.2.14.2}$$

**(6.2.15) Tensor products.** All standard constructions of linear algebra can be applied to vector bundles. In particular, given two (holomorphic) line bundles $\mathscr{L}, \mathscr{L}'$ on $X$, one can form new line bundles $\mathscr{L} \otimes \mathscr{L}'$ and $\mathscr{L}^{-1}$ (the dual of $\mathscr{L}$).

We do not give here the definition in the general case, only for $\mathscr{L}$ constructed as in 6.2.8: if $\mathscr{L}$ (resp. $\mathscr{L}'$) is constructed from the functions $\{\alpha_g(y)\}$ (resp. $\{\alpha'_g(y)\}$) satisfying (6.2.5.4), then $\mathscr{L}\otimes\mathscr{L}'$ (resp. $\mathscr{L}^{-1}$) is defined using $\{\alpha_g(y)\alpha'_g(y)\}$ (resp. $\{\alpha_g(y)^{-1}\}$). In particular, there is a product

$$\Gamma(X,\mathscr{L})\otimes_{\mathbf{C}}\Gamma(X,\mathscr{L}')\longrightarrow\Gamma(X,\mathscr{L}\otimes\mathscr{L}'),$$

defined as follows: if $s\in\Gamma(X,\mathscr{L})$ (resp. $s'\in\Gamma(X,\mathscr{L}')$) corresponds to a function $F:Y\longrightarrow\mathbf{C}$ (resp. $F':Y\longrightarrow\mathbf{C}$) satisfying (6.2.9.2) (resp. its analogue with $\alpha'_g(y)$ instead of $\alpha_g(y)$), then the tensor product $s\otimes s'$ corresponds to the function $F(y)F'(y)$.

**(6.2.16) Exercise.** *Let $\mathscr{L}$ be a line bundle on a compact Riemann surface $X$. If both $\mathscr{L}$ and $\mathscr{L}^{-1}$ have a non-zero holomorphic section, then $\mathscr{L}$ is (isomorphic to) the trivial line bundle. [This gives a quick proof of the case $d<0$ in 6.2.13.]*

## 6.3 Theta functions revisited

**(6.3.1)** Let us apply the general discussion from 6.2.4-15 to the objects from Example 6.2.4(A): $Y=\mathbf{C}$, $G=L$ (a lattice in $\mathbf{C}$ acting by translations), $X=\mathbf{C}/L$. Following 6.2.5, we need a collection of holomorphic functions $\alpha_u(z)\in\mathcal{O}(\mathbf{C})$ $(u\in L)$ satisfying

$$\alpha_{u+v}(z)=\alpha_u(z+v)\,\alpha_v(z)\qquad\qquad(u,v\in L,\ z\in\mathbf{C});\tag{6.3.1.1}$$

they define an action

$$\widehat{u}(z,t)=(z+u,\alpha_u(z)\,t)\qquad\qquad(u\in L)$$

on $\mathbf{C}\times\mathbf{C}$ and – by 6.2.11 – a holomorphic line bundle $\mathscr{L}=L\backslash(\mathbf{C}\times\mathbf{C})$ over $X$. The sections of $\mathscr{L}$ correspond to holomorphic functions $F\in\mathcal{O}(\mathbf{C})$ satisfying

$$F(z+u)=\alpha_u(z)\,F(z)\qquad\qquad(u\in L,\ z\in\mathbf{C}).\tag{6.3.1.2}$$

If the functions $\alpha_u(z)$ are replaced equivalent functions

$$\alpha_u^{\mathrm{new}}(z)=\frac{\beta(z+u)}{\beta(z)}\,\alpha_u(z),\tag{6.3.1.3}$$

where $\beta:\mathbf{C}\longrightarrow\mathbf{C}^*$ is an invertible holomorphic function, then the line bundle remains the same.

**(6.3.2) Proposition.** (i) *Every holomorphic line bundle on $\mathbf{C}/L$ is obtained by the above construction.*
(ii) *For every solution $\{\alpha_u(z)\}$ of (6.3.1.1) there is an equivalent solution (6.3.1.3) of the form*

$$\alpha_u^{\mathrm{new}}(z)=e^{a(u)z+b(u)}\qquad\qquad(a(u),b(u)\in\mathbf{C}).$$

**(6.3.3)** We are not going to prove 6.3.2 in this course. However, a few comments may be helpful:
(1) The statement (i) is a consequence of the fact that every (holomorphic) line bundle on $\mathbf{C}$ is trivial.
(2) In fact, if $Y$ is a *non-compact* Riemann surface, every (holomorphic) line bundle on $Y$ is trivial ([Fo], 30.3). This applies, in particular, to $\mathbf{C}$ and the unit disc $\Delta=\{z\in\mathbf{C}\,|\,|z|<1\}$. If $X$ is a Riemann surface not isomorphic to $P^1(\mathbf{C})$, the the universal covering $Y$ of $X$ is isomorphic either to $\mathbf{C}$ or to $\Delta$, and $X=G\backslash Y$, where the fundamental group $G=\pi_1(X,x_0)$ acts on $Y$ as in 3.2.1.6. This implies that every (holomorphic) line bundle on $X$ can be obtained by the construction 6.2.8 applied to this particular pair $Y,G$.
(3) An elegant cohomological proof of the classification of line bundles over $n$-dimensional complex tori $\mathbf{C}^n/L$ can be found in ([Mu AV], Ch. 1). See also [Wei 1] and [MK].

**(6.3.4) The integrality condition.** Assume that $\mathscr{L}$ is the line bundle on $\mathbf{C}/L$ defined by the collection of functions

$$\alpha_u(z)=e^{a(u)z+b(u)}\qquad\qquad(a(u),b(u)\in\mathbf{C}).$$

The associativity condition (6.3.1.1) is then equivalent to

$$\begin{aligned} a(u+v) &= a(u) + a(v) \\ b(u+v) &\equiv b(u) + b(v) + a(u)v \pmod{2\pi i\mathbf{Z}}. \end{aligned} \tag{6.3.4.1}$$

Interchanging $u$ and $v$ in (6.3.4.1), we see that the alternating bilinear form

$$(u,v) \mapsto \begin{vmatrix} u & v \\ a(u) & a(v) \end{vmatrix} \in 2\pi i\mathbf{Z} \qquad\qquad (u,v \in L) \tag{6.3.4.2}$$

on $L$ has values in $2\pi i\mathbf{Z}$. Topologists will recognize in this bilinear form the first Chern class of $\mathscr{L}$

$$c_1(\mathscr{L}) \in H^2(\mathbf{C}/L, 2\pi i\mathbf{Z}) = \mathrm{Hom}(\Lambda^2 H_1(\mathbf{C}/L, \mathbf{Z}), 2\pi i\mathbf{Z}).$$

If $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, then the relations (6.3.4.1) determine the constants $a(u), b(u)$ $(u \in L)$, as long as we know the values of $a(\omega_j), b(\omega_j) \in \mathbf{C}$ $(j = 1, 2)$, which should satisfy

$$\begin{vmatrix} \omega_1 & \omega_2 \\ a(\omega_1) & a(\omega_2) \end{vmatrix} \in 2\pi i\mathbf{Z}. \tag{6.3.4.3}$$

See ([Mu AV], I.2) for general formulas for $a(u), b(u)$.

**(6.3.5) The simplest line bundle on $\mathbf{C}/L$.** Assume that $\omega_2 = 1$, $\omega_1 = \tau$ $(\mathrm{Im}(\tau) > 0)$. After a reparametrization (6.3.1.3) with $\beta(z) = \exp(Az^2 + Bz + C)$ (for suitable $A, B, C \in \mathbf{C}$), we can assume that $a(1) = b(1) = 0$. The integrality condition (6.3.4.3) then becomes

$$-a(\tau) = \begin{vmatrix} \tau & 1 \\ a(\tau) & 0 \end{vmatrix} \in 2\pi i\mathbf{Z}.$$

Consider the simplest non-trivial value $-a(\tau) = 2\pi i$. The sections of the associated line bundle $\mathscr{L}$ then correspond to holomorphic functions $F \in \mathcal{O}(\mathbf{C})$ satisfying

$$\begin{aligned} F(z+1) &= F(z) \\ F(z+\tau) &= e^{-2\pi i z + b(\tau)} F(z). \end{aligned}$$

Is there a "simplest" choice of the parameter $b(\tau)$? After a change of variables by the translation

$$T_c : z \mapsto z + c$$

(which amounts to replacing $\mathscr{L}$ by its pull-back $T_c^*\mathscr{L}$), the constant $b(\tau)$ is replaced by $b(\tau) - 2\pi i c$. It is natural to choose $c$ for which $F(z) = F(-z)$ would be an *even* holomorphic section; putting $z = -\tau/2$ we obtain $b(\tau) = -\pi i\tau$.

We denote by $\mathscr{L}$ (until the end of Sect. 6) the line bundle on $\mathbf{C}/\mathbf{Z}\tau + \mathbf{Z}$ corresponding to the values

$$a(1) = b(1) = 0, \qquad a(\tau) = -2\pi i, \qquad b(\tau) = -\pi i\tau.$$

A section $s \in \Gamma(\mathbf{C}/\mathbf{Z}\tau + \mathbf{Z}, \mathscr{L})$ is then given by $F(z) \in \mathcal{O}(\mathbf{C})$ satisfying

$$\begin{aligned} F(z+1) &= F(z) \\ F(z+\tau) &= e^{-2\pi i(z+\frac{\tau}{2})} F(z). \end{aligned} \tag{6.3.5.1}$$

**(6.3.6) Proposition (Basic theta function).** *The space of holomorphic solutions of (6.3.5.1) is equal to* $\mathbf{C} \cdot \theta(z)$, *where*

$$\theta(z) = \theta(z;\tau) = \sum_{n \in \mathbf{Z}} q^{n^2/2} t^n = \sum_{n \in \mathbf{Z}} e^{\pi i n^2 \tau + 2\pi i n z}.$$

*In other words,* $\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L})=\mathbf{C}\cdot\theta(z)$.

*Proof.* Assume that $F\in\mathcal{O}(\mathbf{C})$ satisfies (6.3.5.1). The first relation implies that $F(z)=f(e^{2\pi iz})$ for some $f\in\mathcal{O}(\mathbf{C}^*)$ which can be expanded to a convergent Laurent series

$$f(t)=\sum_{n\in\mathbf{Z}}a_nt^n \qquad\qquad (t=e^{2\pi iz}).$$

The second relation is equivalent to

$$\sum_{n\in\mathbf{Z}}a_nq^nt^n=f(qt)=t^{-1}q^{-1/2}f(t)=\sum_{n\in\mathbf{Z}}a_nq^{-1/2}t^{n-1}=\sum_{n\in\mathbf{Z}}a_{n+1}q^{-1/2}t^n$$

(where $q^{1/2}=e^{\pi i\tau}$), hence to

$$a_{n+1}=q^{n+1/2}a_n \qquad (n\in\mathbf{Z}) \iff a_n=q^{n^2/2}a_0 \qquad (n\in\mathbf{Z}) \iff f(t)=a_0\sum_{n\in\mathbf{Z}}q^{n^2/2}t^n=a_0\,\theta(z).$$

As $|q|<1$, the series defining $\theta(z)$ is uniformly convergent for $t$ contained in a compact subset of $\mathbf{C}^*$, and so defines a holomorphic function. Reversing the calculation, we see that $\theta(z)$ satisfies (6.3.5.1).

**(6.3.7) Further theta functions.** For fixed $a,b\in\{0,1\}=\mathbf{Z}/2\mathbf{Z}$, denote by $\chi_{a,b}:L\longrightarrow L/2L\longrightarrow\{\pm1\}$ (where $L=\mathbf{Z}\tau+\mathbf{Z}$) the character

$$\chi_{a,b}(m+n\tau)=(-1)^{ma+nb} \qquad\qquad (m,n\in\mathbf{Z}).$$

By 6.2.7, the constant functions $\{\chi_{a,b}(u)\}$ define a line bundle on $\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z}$, which will also be denoted by $\chi_{a,b}$. For each $m\in\mathbf{Z}$, a section $s\in\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L}^{\otimes m}\otimes\chi_{a,b})$ corresponds to a holomorphic function $F\in\mathcal{O}(\mathbf{C})$ satisfying

$$\begin{aligned}F(z+1)&=(-1)^aF(z)\\ F(z+\tau)&=(-1)^be^{-2\pi im(z+\frac{\tau}{2})}F(z).\end{aligned} \tag{6.3.7.1}$$

We first consider the case $m=1$.

**(6.3.8) Proposition.** *For $m=1$ and $a,b\in\{0,1\}$, the space of holomorphic solutions of (6.3.7.1) is equal to $\mathbf{C}\cdot\theta_{ab}(z)$, where*

$$\theta_{ab}(z)=\theta_{ab}(z;\tau)=\sum_{n\in\mathbf{Z}}e^{\pi i(n+\frac{a}{2})^2\tau+2\pi i(n+\frac{a}{2})(z+\frac{b}{2})}=\theta_{a0}(z+\frac{b}{2};\tau)=e^{\pi ia(z+\frac{b}{2})+\frac{\pi ia\tau}{4}}\theta_{00}(z+\frac{a\tau+b}{2};\tau).$$

*In other words,* $\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L}\otimes\chi_{a,b})=\mathbf{C}\cdot\theta_{ab}(z)$. *(Of course, $\theta_{00}(z)=\theta(z)$.)*

*Proof.* As in 6.3.6.

**(6.3.9) Warning about normalizations.** Our definition of $\theta_{ab}(z)$ is the same as in [MK] and [Mu TH] (except that Mumford uses $a/2,b/2$ instead of $a,b$), but the "classical" $\theta_{11}(z)$ used in [Web] is equal to our $-\theta_{11}(z)$.

**(6.3.10) Degenerate values.** If we let $\mathrm{Im}(\tau)$ tend to $+\infty$ ("$\tau\longrightarrow i\infty$"), then $q=\exp(2\pi i\tau)$ tends to 0. The expansions of $\theta_{ab}(z;\tau)$ then yield the following asymptotics as $\tau\longrightarrow i\infty$:

$$\theta_{00}(z;\tau)\sim\theta_{01}(z;\tau)\sim1, \qquad \theta_{10}(z;\tau)\sim(t^{1/2}+t^{-1/2})\,q^{1/8}, \qquad \theta_{11}(z;\tau)\sim i(t^{1/2}-t^{-1/2})\,q^{1/8}.$$

**(6.3.11) Relation to $A(z)$.** The function $A(z)$ from (5.3.4.1) is also a theta function. A short calculation shows that

$$B(z) = A(z + \frac{\tau+1}{2})$$

satisfies (6.3.5.1), hence

$$\theta(z;\tau) = c(\tau)A(z + \frac{\tau+1}{2}) \tag{6.3.11.1}$$

for some $c(\tau) \in \mathbf{C}^*$, by 6.3.6.

**(6.3.12) Proposition.** (i) *The function $\theta(z)$ has simple zeros at $z \in \frac{\tau+1}{2} + \mathbf{Z}\tau + \mathbf{Z}$ (and no other zeros).* (ii) *For $a, b \in \{0,1\}$, the function $\theta_{ab}(z)$ has simple zeros at $z \in \frac{(a+1)\tau+(b+1)}{2} + \mathbf{Z}\tau + \mathbf{Z}$ (and no other zeros).*

*Proof.* For (i), combine 5.3.4 and (6.3.11.1); (ii) then follows from the formulas relating $\theta_{ab}(z)$ and $\theta(z)$.

**(6.3.13) Exercise.** *Using only the functional equation (6.3.5.1) of $\theta(z)$, show that*

$$\frac{1}{2\pi i}\int_{\partial D} \frac{\theta'(z)}{\theta(z)}\,dz = 1, \qquad \frac{1}{2\pi i}\int_{\partial D} z\frac{\theta'(z)}{\theta(z)}\,dz \in \frac{\tau+1}{2} + \mathbf{Z}\tau + \mathbf{Z},$$

*where the integral is taken over the boundary of a fundamental parallelogram $D = \{z = \alpha + t_1\tau + t_2 1 \,|\, 0 \leq t_1, t_2 \leq 1\}$ for the action of $\mathbf{Z}\tau + \mathbf{Z}$ on $\mathbf{C}$. [This calculation gives another proof of 6.3.12(i).]*

**(6.3.14) General line bundles on $\mathbf{C}/L$.** Is it possible to classify all line bundles (up to isomorphism) on $\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z}$? The discussion in 6.3.5 implies that each line bundle $\mathscr{L}'$ is defined, after a suitable reparametrization, by the functions

$$\alpha_1(z) = 1, \qquad \alpha_\tau(z) = e^{-2\pi i m(z+\frac{\tau}{2}+c)} \qquad\qquad (m \in \mathbf{Z},\, c \in \mathbf{C}), \tag{6.3.14.1}$$

with $\alpha_u(z)$ for general $u \in \mathbf{Z}\tau + \mathbf{Z}$ defined by the associativity relation (6.3.1.1). In other words, $\mathscr{L}'$ is isomorphic to $(T_c^*\mathscr{L})^{\otimes m}$, where $T_c(z) = z+c$ is the translation by $c \in \mathbf{C}$ (for example, $\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\, T_c^*\mathscr{L}) = \mathbf{C}\cdot\theta(z+c)$).

**(6.3.15) Line bundles and divisors.** If $c, d \in \mathbf{C}$ satisfy $m(c-d) \in \mathbf{Z}\tau + \mathbf{Z}$, then the functions (6.3.14.1) differ by a reparametrization (6.3.1.3) (exercise!). This means that the isomorphism class of $(T_c^*\mathscr{L})^{\otimes m}$ depends on two invariants: an integer and an element of $\mathbf{C}/\mathbf{Z}\tau + \mathbf{Z}$, which is strongly reminiscent of the description of the divisor class group given in 5.3.6:

$$0 \longrightarrow \mathbf{C}/\mathbf{Z}\tau + \mathbf{Z} \longrightarrow Cl(\mathbf{C}/\mathbf{Z}\tau + \mathbf{Z}) \xrightarrow{\deg} \mathbf{Z} \longrightarrow 0.$$

This is no accident; in fact, there is a direct correspondence between (isomorphism classes of) line bundles on an arbitrary Riemann surface $X$ and divisor classes on $X$, given as follows. First of all, one can define *meromorphic sections* of a line bundle $\mathscr{L}$ over $X$. For example, in the situation of 6.3.3(2), such a section corresponds to a *meromorphic* function $F(y)$ satisfying 6.2.9.2. The zeros and poles (including multiplicities) of such a (non-zero) meromorphic section $s$ are invariant under the action of $G$, hence come from a divisor $\mathrm{div}(s) \in \mathrm{Div}(X)$. Non-zero meromorphic sections of $\mathscr{L}$ always exist, and form a one-dimensional vector space over $\mathcal{M}(X)$ (by the same argument as in 3.3.16). If $s' = fs$ is another meromorphic section of $\mathscr{L}$ (with $f \in \mathcal{M}(X) - \{0\}$), then $\mathrm{div}(s') = \mathrm{div}(s) + \mathrm{div}(f)$; thus the class of the divisor $\mathrm{div}(s)$ does not depend on the choice of $s$. Associating to $\mathscr{L}$ the class of $\mathrm{div}(s)$ then defines a homomorphism of abelian groups

$$\{\text{isomorphism classes of line bundles on } X\} \longrightarrow Cl(X), \tag{6.3.15.1}$$

with tensor product as the group operation on the left hand side. In fact, (6.3.15.1) is always an isomorphism (both sides being trivial if $X$ is not compact). With an appropriate notion of a divisor, all of the above holds for (smooth) complex varieties of any dimension embeddable into $P^N(\mathbf{C})$; see [Gr-Ha], 1.2.

### 6.4 Relations between theta functions

Theta functions satisfy a large number of interesting identities (see [Web], [Mu TH], [McK-Mo]); a few of them will be proved in this section (following closely [Web]).

**(6.4.1)** The basic principle is very simple: in general, the tensor products

$$\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L}^{\otimes m}\otimes\chi_{a,b})\otimes_{\mathbf{C}}\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L}^{\otimes n}\otimes\chi_{c,d})\longrightarrow\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L}^{\otimes m+n}\otimes\chi_{a+c,b+d})$$

have non-trivial kernels, which yield non-trivial linear relations between products of theta functions. The existence of such relations can be often established by a simple count of dimensions.

**(6.4.2) Exercise.** *The four functions $\theta_{ab}(z)$ are linearly independent over $\mathbf{C}$. [Hint: The characters of $L/2L$ are linearly independent.]*

**(6.4.3) Proposition.** *For $m\in\mathbf{Z}$ and $a,b\in\{0,1\}$,*

$$\dim_{\mathbf{C}}\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L}^{\otimes m}\otimes\chi_{a,b})=\begin{cases}m, & \text{if } m>0\\ \\ 0, & \text{if } m<0.\end{cases}$$

*Proof.* (Sketch) If $m>0$, expand a holomorphic solution of (6.3.7.1) into a Laurent series $\sum_{n\in\mathbf{Z}}a_nt^{n+a/2}$; the functional equation yields recursive relations between $a_n$ and $a_{n+m}$ ($n\in\mathbf{Z}$), which leaves the values of $a_0,\dots,a_{m-1}$ undetermined. Conversely, any choice of these first $m$ coefficients defines a holomorphic solution. If $m<0$, we obtain again recursive relations between $a_n$ and $a_{n+m}$, but every non-zero choice of $(a_0,\dots,a_{m-1})$ leads to a divergent series (alternatively, one can also appeal to 6.2.16)).

**(6.4.4) Examples:** (1) The four functions $\theta_{ab}^2(z)$ all lie in the two-dimensional space $\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L}^{\otimes 2})$. In fact, it follows from 6.4.2 that they generate this space. As a result, there exist two linearly independent linear relations between $\theta_{00}^2(z),\theta_{01}^2(z),\theta_{10}^2(z),\theta_{11}^2(z)$.
(2) The four functions $\theta_{ab}(2z)$ all lie in the four-dimensional space $\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L}^{\otimes 4})$; by 6.4.2 they form its basis. By 6.3.12, these functions have no common zeros, hence the map

$$f:\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z}\longrightarrow\mathbf{P}^3(\mathbf{C}),\qquad z\mapsto(\theta_{00}(2z):\theta_{01}(2z):\theta_{10}(2z):\theta_{11}(2z))$$

is well-defined. By (1), the image of $f$ is contained in the intersection of two quadrics $Q_1(\mathbf{C})\cap Q_2(\mathbf{C})\subset\mathbf{P}^3(\mathbf{C})$, where

$$Q_1:a_0X_0^2+a_1X_1^2+a_2X_2^2+a_3X_3^2=0,\qquad Q_2:b_0X_0^2+b_1X_1^2+b_2X_2^2+b_3X_3^2=0.$$

**(6.4.5) Exercise.** (i) *Write down explicitly two relations from 6.4.4(1).*
(ii) *For $a,b,c,d\in\{0,1\}$, express the values $\theta_{ab}(\frac{c\tau+d}{2})$ in terms of $\theta_{(a+c)(b+d)}$.*
(iii) *Deduce that $\theta_{00}^4=\theta_{01}^4+\theta_{10}^4$.*
(iv) *Show that $f:\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z}\longrightarrow Q_1(\mathbf{C})\cap Q_2(\mathbf{C})$ is a bijection ([McK-Mo], 3.4).*

**(6.4.6) Notation.** For $n\geq 0$ and $a,b\in\{0,1\}$, we shall denote

$$\theta_{ab}^{(n)}(z)=\left(\frac{\partial}{\partial z}\right)^n\theta_{ab}(z),\qquad\theta_{ab}=\theta_{ab}(0;\tau),\qquad\theta_{ab}^{(n)}=\left(\frac{\partial}{\partial z}\right)^n\theta_{ab}(z;\tau)\Big|_{z=0}.$$

**(6.4.7) Exercise.** *Show that*

$$\theta_{ab}(-z)=\theta_{ab}(z)\cdot\begin{cases}1, & \text{if } ab=00,01,10\\ \\ -1, & \text{if } ab=11.\end{cases}$$

**(6.4.8) Exercise.** *Show that, for $a, b, c, d \in \{0, 1\}$,*

$$\begin{vmatrix} \theta'_{ab}(z) & \theta'_{cd}(z) \\ \theta_{ab}(z) & \theta_{cd}(z) \end{vmatrix} \in \Gamma(\mathbf{C}/\mathbf{Z}\tau + \mathbf{Z},\, \mathscr{L}^{\otimes 2} \otimes \chi_{a+c,b+d}).$$

**(6.4.9) Corollary.** *We have*

$$\begin{vmatrix} \theta'_{11}(z) & \theta'_{01}(z) \\ \theta_{11}(z) & \theta_{01}(z) \end{vmatrix} = \frac{\theta'_{11}\theta_{01}}{\theta_{00}\theta_{10}}\, \theta_{00}(z)\, \theta_{10}(z).$$

*Proof.* The function $f(z)$ (resp. $g(z)$) on the left (resp. right) hand side is even (by 6.4.7) and lies in

$$\Gamma(\mathbf{C}/\mathbf{Z}\tau + \mathbf{Z},\, \mathscr{L}^{\otimes 2} \otimes \chi_{1,0}) = \mathbf{C} \cdot \theta_{00}(z)\, \theta_{10}(z) \oplus \mathbf{C} \cdot \theta_{11}(z)\, \theta_{01}(z).$$

As the function $\theta_{11}(z)\, \theta_{01}(z)$ is odd, we must have $f(z) = \lambda g(z)$ for some $\lambda = \lambda(\tau) \in \mathbf{C}^*$; the exact value of $\lambda$ is obtained by putting $z = 0$ (and using $\theta_{11} = 0$).

**(6.4.10) Proposition.** *There exists $c \in \mathbf{C}^*$ such that*

$$\theta'_{11} = c\, \theta_{00}\, \theta_{01}\, \theta_{10}.$$

*Proof.* Applying $(\partial/\partial z)^2$ to the identity in 6.4.9 and putting $z = 0$, we obtain

$$\theta'''_{11}\, \theta_{01} - \theta''_{01}\, \theta'_{11} = \frac{\theta'_{11}\theta_{01}}{\theta_{00}\theta_{10}}\, (\theta''_{10}\, \theta_{00} + \theta''_{00}\, \theta_{10}),$$

hence

$$\frac{\theta'''_{11}}{\theta'_{11}} = \frac{\theta''_{01}}{\theta_{01}} + \frac{\theta''_{10}}{\theta_{10}} + \frac{\theta''_{00}}{\theta_{00}}.$$

Using Lemma 6.4.11 below, this can be rewritten as

$$\frac{\partial}{\partial \tau}\, \log(\theta'_{11}) = \frac{\partial}{\partial \tau}\, \log(\theta_{01}\, \theta_{10}\, \theta_{00}),$$

proving the claim.

**(6.4.11) Lemma (Heat equation).** *For $a, b \in \{0, 1\}$,*

$$(D_z^2 - 4\pi i D_\tau)\, \theta_{ab}(z; \tau) = 0$$

*(where $D_z = \partial/\partial z$, $D_\tau = \partial/\partial \tau$).*

*Proof.* As

$$\frac{1}{2\pi i}\, D_\tau : \left\{ \begin{array}{l} q^m \mapsto m q^m \\ t^m \mapsto 0 \end{array} \right\}, \qquad \frac{1}{2\pi i}\, D_z : \left\{ \begin{array}{l} q^m \mapsto 0 \\ t^m \mapsto m t^m \end{array} \right\},$$

the operator $1/2\pi i\, D_\tau - \frac{1}{2}(1/2\pi i\, D_z)^2$ annihilates each term of the series

$$\theta_{ab}(z; \tau) = \sum_{n \in \mathbf{Z}} e^{\pi i b (n + \frac{a}{2})} q^{(n + \frac{a}{2})^2/2} t^{n + \frac{a}{2}}.$$

**(6.4.12)** We are now ready to evaluate the factor $c(\tau)$ in (6.3.11.1):

$$\theta_{00}(z; \tau) = c(\tau) \prod_{n=1}^{\infty} (1 + q^{n-1/2} t)(1 + q^{n-1/2} t^{-1}) \qquad (t = e^{2\pi i z},\, q^\alpha = e^{2\pi i \alpha \tau}).$$

It follows from 6.3.8 that

$$\begin{aligned}
\theta_{01}(z;\tau) &= c(\tau)\prod_{n=1}^{\infty}(1-q^{n-1/2}t)(1-q^{n-1/2}t^{-1}) \\
\theta_{10}(z;\tau) &= (t^{1/2}+t^{-1/2})\,q^{1/8}c(\tau)\prod_{n=1}^{\infty}(1+q^{n}t)(1+q^{n}t^{-1}) \\
\theta_{11}(z;\tau) &= i(t^{1/2}-t^{-1/2})\,q^{1/8}c(\tau)\prod_{n=1}^{\infty}(1-q^{n}t)(1-q^{n}t^{-1}).
\end{aligned} \tag{6.4.12.1}$$

Letting $z \mapsto 0$ (when $t \sim 1+2\pi i z$), we obtain

$$\begin{aligned}
\theta_{00} &= c(\tau)\prod_{n=1}^{\infty}(1+q^{n-1/2})^2 \\
\theta_{01} &= c(\tau)\prod_{n=1}^{\infty}(1-q^{n-1/2})^2 \\
\theta_{10} &= 2\,c(\tau)\,q^{1/8}\prod_{n=1}^{\infty}(1+q^{n})^2 \\
\theta'_{11} &= -2\pi\,c(\tau)\,q^{1/8}\prod_{n=1}^{\infty}(1-q^{n})^2.
\end{aligned} \tag{6.4.12.2}$$

The identity $\theta'_{11} = c\,\theta_{00}\,\theta_{01}\,\theta_{10}$ from 6.4.10 implies that

$$-2\pi\,c(\tau)\,q^{1/8}\prod_{n=1}^{\infty}(1-q^{n})^2 = c\cdot 2\,c(\tau)^3\,q^{1/8}\prod_{n=1}^{\infty}\frac{(1-q^{2n-1})^2(1-q^{2n})^2}{(1-q^{n})^2} = c\cdot 2\,c(\tau)^3\,q^{1/8},$$

hence

$$c(\tau)^2 = (-\pi/c)\prod_{n=1}^{\infty}(1-q^{n})^2.$$

Letting $\mathrm{Im}(\tau) \longrightarrow \infty$ (when $q \longrightarrow 0$) and using 6.3.10, we see that $c(\tau) \longrightarrow 1$. This implies that

$$c = -\pi, \qquad c(\tau) = \prod_{n=1}^{\infty}(1-q^{n}). \tag{6.4.12.3}$$

We have thus proved

**(6.4.13) Proposition.** *$\theta'_{11} = -\pi\,\theta_{00}\,\theta_{01}\,\theta_{10}$ (cf. 6.3.9).*

**(6.4.14) Theorem (Jacobi's Triple Product Formula).**

$$\sum_{n\in\mathbf{Z}} q^{n^2/2}t^{n} = \prod_{n=1}^{\infty}(1-q^{n})(1+q^{n-1/2}t)(1+q^{n-1/2}t^{-1}).$$

**(6.4.15) Exercise (Another proof of Jacobi's Triple Product Formula).** *Substituting to the product formula (6.3.11.1) the values $\tau = \frac{1}{2}, \frac{1}{4}$ and using the fact that $\theta(4z, \frac{1}{2}) = \theta(z, \frac{1}{4})$, deduce that the holomorphic function $c(\tau)/\prod_{n\geq 1}(1-q^n)$ ($\mathrm{Im}(\tau) > 0$) is invariant under $\tau \mapsto 4\tau$ and $\tau \mapsto \tau + 2$, hence constant.*

**(6.4.16) Proposition.**

$$\prod_{n=1}^{\infty}(1-q^{n})^3 = \sum_{n=0}^{\infty}(-1)^{n}(2n+1)\,q^{n(n+1)/2} = 1-3q+5q^3-7q^6+9q^{10}-11q^{15}+\cdots$$

*Proof.* This follows from the expansion

$$\theta'_{11} = -2\pi\, q^{1/8} \sum_{n\in\mathbf{Z}} (n+1/2)(-1)^n q^{n(n+1)/2} = -2\pi\, q^{1/8} \sum_{n=0}^{\infty} (-1)^n (2n+1)\, q^{n(n+1)/2}$$

and the product formula

$$\theta'_{11} = -2\pi\, q^{1/8} \prod_{n=1}^{\infty} (1-q^n)^3,$$

which is obtained by combining (6.4.12.2-3).

## 7. Construction of elliptic functions (Weierstrass' method)

### 7.1 The Weierstrass $\sigma$, $\zeta$ and $\wp$-functions

Let $L \subset \mathbf{C}$ be a lattice.

**(7.1.1)** Recall that Jacobi's method of construction of elliptic functions with respect to $L$ consisted in taking a quotient

$$\frac{\theta_1(z)}{\theta_2(z)}$$

of two theta functions, i.e. of two solutions of (6.1.1.1). By contrast, Weierstrass showed that the function $U(z)$ from 4.4.3 (i.e. the inverse of the Abel-Jacobi map) can be written directly as

$$\left(\frac{\partial}{\partial z}\right)^2 \log \sigma(z),$$

where $\sigma(z)$ is a particular theta function with simple zeros at $z \in L$. Morally,

$$\text{“}\sigma(z) = \prod_{u\in L} (z-u)\text{”}, \tag{7.1.1.1}$$

but this infinite product does not converge for any $z \in \mathbf{C}$.

An elementary version of $\sigma(z)$ is the function $\sin(z)$, which is holomorphic in $\mathbf{C}$ and has simple zeros at $z \in \pi\mathbf{Z}$. The infinite product

$$g(z) = z \prod_{n=1}^{\infty} \left(1 - \frac{z}{\pi n}\right)\left(1 + \frac{z}{\pi n}\right) = z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{\pi^2 n^2}\right) \tag{7.1.1.2}$$

has the same properties, as the series

$$\sum_{n=1}^{\infty} \frac{|z^2|}{\pi^2 n^2}$$

is uniformly convergent on compact subsets of $\mathbf{C}$ ([Ru 2], Thm. 15.6). In fact,

$$g(z) = \sin(z).$$

**(7.1.2) Exercise–Definition.** *For $s \in \mathbf{R}$,*

$$\sum_{u\in L}{}' \frac{1}{|u|^s} < \infty \iff s > 2, \tag{7.1.2.1}$$

*where we have used the notation*

$$\sum_{u\in L}{}' = \sum_{u\in L-\{0\}}$$

*In particular, the series*

$$G_{2k}(L) = \sum_{u\in L}{}' \frac{1}{u^{2k}} \tag{7.1.2.2}$$

*is absolutely convergent for every integer $k \geq 2$.*

**(7.1.3) Definition of the $\sigma$-function.** The divergence of the sum (7.1.2.1) for $s = 1, 2$ implies that one cannot work directly with the products

$$\prod_{u\in L}{}' \left(1 - \frac{z}{u}\right), \qquad \prod_{u\in\Sigma} \left(1 - \frac{z^2}{u^2}\right),$$

where $L - \{0\} = \Sigma \cup -\Sigma$, $\Sigma \cap -\Sigma = \emptyset$. However, the power series expansion

$$-\log\left(1 - \frac{z}{u}\right) = \frac{z}{u} + \frac{1}{2}\left(\frac{z}{u}\right)^2 + \frac{1}{3}\left(\frac{z}{u}\right)^3 + \cdots \qquad (|z| < |u|)$$

implies (together with 7.1.2) that the infinite product

$$\sigma(z) = \sigma(z; L) = z\prod_{u\in L}{}' \left(1 - \frac{z}{u}\right) e^{\frac{z}{u} + \frac{1}{2}\left(\frac{z}{u}\right)^2} \tag{7.1.3.1}$$

is uniformly convergent on compact subsets of $\mathbf{C}$ and defines a holomorphic function with simple zeros at $z \in L$ and no other zeros ([Ru 2], Thm. 15.6).

As we shall see in 7.4.9 below,

$$\sigma(z; \mathbf{Z}\tau + \mathbf{Z}) = c_1 e^{c_2 z^2} \theta_{11}(z; \tau), \tag{7.1.3.2}$$

for suitable constants $c_i = c_i(\tau) \in \mathbf{C}$.

**(7.1.4) Definition of the $\zeta$- and $\wp$-functions.** The convergence properties of the infinite product (7.1.3.1) imply that its logarithmic derivative $\zeta(z; L)$ can be computed term by term:

$$\zeta(z; L) = \frac{\sigma'(z)}{\sigma(z)} = \frac{1}{z} + \sum_{u\in L}{}' \left(\frac{1}{z-u} + \frac{1}{u} + \frac{z}{u^2}\right), \tag{7.1.4.1}$$

where the infinite series is uniformly convergent on compact subsets of $\mathbf{C} - L$ to a holomorphic function; it is meromorphic on $\mathbf{C}$, with simple poles at all $z \in L$.

The power series expansion

$$\frac{1}{z-u} + \frac{1}{u} + \frac{z}{u^2} = -\sum_{n=2}^{\infty} \frac{z^n}{u^{n+1}} \qquad (|z| < |u|)$$

and the absolute convergence of the double sum

$$\sum_{u\in L}{}' \sum_{n=2}^{\infty} \frac{z^n}{u^{n+1}}$$

imply that

$$\zeta(z; L) = \frac{1}{z} - \sum_{k=1}^{\infty} G_{2k+2} z^{2k+1}. \tag{7.1.4.2}$$

Differentiating (7.1.4.1) and using (7.1.4.2), we obtain the function

$$\wp(z;L) = -\zeta'(z;L) = \frac{1}{z^2} + \sum_{u\in L}{}' \left(\frac{1}{(z-u)^2} - \frac{1}{u^2}\right) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)\,G_{2k+2}z^{2k} \tag{7.1.4.3}$$

and its derivative

$$\wp'(z;L) = -2\sum_{u\in L}\left(\frac{1}{(z-u)^3}\right) = -\frac{2}{z^3} + \sum_{k=1}^{\infty}(2k+1)2k\,G_{2k+2}z^{2k-1}. \tag{7.1.4.4}$$

The function $\wp(z)$ (resp. $\wp'(z)$) is an even (resp. odd) meromorphic function on $\mathbf{C}$, holomorphic on $\mathbf{C} - L$ and having poles of order 2 (resp. 3) at $z \in L$.

**(7.1.5) Proposition.** *Both $\wp(z)$ and $\wp'(z)$ are elliptic functions with respect to $L$, i.e. $\wp(z), \wp'(z) \in \mathcal{M}(\mathbf{C}/L)$.*

*Proof.* By 7.1.2 (for $s = 3$), the infinite series (7.1.4.4) for $\wp'(z)$ is absolutely convergent for all $z \in \mathbf{C} - L$. It follows that, for every $v \in L$ and $z \in \mathbf{C} - L$,

$$\wp'(z+v) = -2\sum_{u\in L}\left(\frac{1}{(z+v-u)^3}\right) = -2\sum_{w=u-v}\left(\frac{1}{(z-w)^3}\right) = \wp'(z),$$

hence

$$\wp(z+v) - \wp(z) = c(v) \in \mathbf{C}.$$

Choosing a basis $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ of $L$ and putting $v = \omega_j$, $z = -\omega_j/2$, we obtain

$$c(\omega_j) = \wp\left(\frac{\omega_j}{2}\right) - \wp\left(-\frac{\omega_j}{2}\right) = 0,$$

as $\wp$ is an even function. Thus both $\wp$ and $\wp'$ are $L$-periodic.

**(7.1.6) Rescaling $L$.** It follows from the definitions that, for every $\lambda \in \mathbf{C}^*$,

$$\sigma(\lambda z;\lambda L) = \lambda\sigma(z;L), \qquad \zeta(\lambda z;\lambda L) = \lambda^{-1}\zeta(z;L),$$
$$\left(\frac{d}{dz}\right)^n \wp(\lambda z;\lambda L) = \lambda^{-2-n}\left(\frac{d}{dz}\right)^n \wp(z;L), \qquad G_{2k}(\lambda L) = \lambda^{-2k}G_{2k}(L).$$

**(7.1.7) Laurent expansions at $z = 0$.** The expansions (7.1.4.3-4) imply that

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3\,G_4 z^2 + 5\,G_6 z^4 + \cdots \\
-\wp'(z) &= \frac{2}{z^3} - 6\,G_4 z - 20\,G_6 z^3 + \cdots \\
\wp(z)^2 &= \frac{1}{z^4} + 6\,G_4 + 10\,G_6 z^2 + \cdots \\
\wp'(z)^2 &= \frac{4}{z^6} - \frac{24\,G_4}{z^2} - 80\,G_6 + \cdots \\
\wp(z)^3 &= \frac{1}{z^6} + \frac{9\,G_4}{z^2} + 15\,G_6 + \cdots
\end{aligned}$$

(where we write $G_{2k}$ for $G_{2k}(L)$). It follows that the elliptic function

$$f(z) = \wp'(z)^2 - (4\wp(z)^3 - 60\,G_4\wp(z) - 140\,G_6) \in \mathcal{M}(\mathbf{C}/L)$$

is holomorphic on $\mathbf{C}/L - \{0\}$ and has Laurent expansion of the form

$$f(z) = c_2 z^2 + c_4 z^4 + \cdots$$

at $z = 0$; thus $f \in \mathcal{O}(\mathbf{C}/L) = \mathbf{C}$ is constant, equal to $f(z) = f(0) = 0$. We have proved, therefore, the following result.

**(7.1.8) Theorem.** *The function $\wp(z)$ satisfies the differential equation*

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

*where*

$$g_2 = 60\,G_4(L) = 60{\sum_{u\in L}}' \frac{1}{u^4}, \qquad g_3 = 140\,G_6(L) = 140{\sum_{u\in L}}' \frac{1}{u^6}.$$

**(7.1.9) Proposition.** *Fix a basis $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ of $L$ and put $\omega_3 = \omega_1 + \omega_2$. Then*
(i) $\operatorname{div}(\wp(z) - \wp(\omega_j/2)) = 2(\omega_j/2) - 2(0)$.
(ii) $\operatorname{div}(\wp'(z)) = (\omega_1/2) + (\omega_2/2) + (\omega_3/2) - 3(0)$.
(iii) *The cubic polynomial $4X^3 - g_2X - g_3 = 4(X-e_1)(X-e_2)(X-e_3)$ has three distinct roots satisfying $\{e_1, e_2, e_3\} = \{\wp(\omega_1/2), \wp(\omega_2/2), \wp(\omega_3/2)\}$.*

*Proof.* For each $j = 1, 2, 3$,

$$-\wp'(\omega_j/2) = \wp'(-\omega_j/2) = \wp'(-\omega_j/2 + \omega_j) = \wp'(\omega_j/2) \Longrightarrow \wp'(\omega_j/2) = 0.$$

It follows that the function $\wp'(z)$ (resp. $\wp(z) - \wp(\omega_j/2)$) has a zero of order $\geq 1$ (resp. $\geq 2$) at $\omega_j/2 \in \mathbf{C}/L$; as its only pole is at $z = 0$ and has order 3 (resp. 2), the statements (i), (ii) follow from the fact that the degree of a principal divisor is equal to zero. The differential equation 7.1.8 implies that each number $a_j = \wp(\omega_j/2)$ is a root of $4X^3 - g_2X - g_3$; these numbers are distinct, since the divisors $\operatorname{div}(\wp(z) - a_j)$ are distinct, proving (iii).

**(7.1.10) The discriminant and the $j$-invariant.** Writing

$$4X^3 - g_2X - g_3 = 4(X^3 + aX + b) = 4(X-e_1)(X-e_2)(X-e_3)$$

with $a = -g_2/4$, $b = -g_3/4$, it follows from 7.1.9(iii) that the discriminant

$$\operatorname{disc}(X^3 + aX + b) = \prod_{i<j}(e_i - e_j)^2 = -4a^3 - 27b^2 \neq 0$$

is *non-zero*. It is customary to get rid of the denominators and define the **discriminant of** $L$ as

$$\Delta(L) = 16\prod_{i<j}(e_i - e_j)^2 = 16\left(-4(-g_2/4)^3 - 27(-g_3/4)^2\right) = g_2^3 - 27g_3^2 \neq 0 \tag{7.1.10.1}$$

and the **$j$-invariant of** $L$ as

$$j(L) = \frac{(12g_2)^3}{\Delta(L)} = \frac{1728g_2^3}{\Delta(L)}. \tag{7.1.10.2}$$

Under rescaling,

$$\Delta(\lambda L) = \lambda^{-12}\Delta(L), \qquad j(\lambda L) = j(L) \qquad\qquad (\lambda \in \mathbf{C}^*).$$

**(7.1.11) Exercise.** *What are the analogues of 7.1.4-10 if we replace $\sigma(z)$ by $\sin(z)$?*

## 7.2 The elliptic curve $E$ associated to $\mathbf{C}/L$

**(7.2.1)** It follows from 7.1.9(iii) that the projective curve

$$E : Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3 = 4(X - e_1Z)(X - e_2Z)(X - e_3Z)$$

is of the type considered in 4.1.1 (apart from the harmless factor of 4). Using the affine coordinates $x = X/Z, y = Y/Z$ on

$$E - \{O\} : y^2 = 4x^3 - g_2x - g_3$$

(where $O = (0:1:0)$ is the unique point at infinity of $E$), we define a map

$$\varphi : \mathbf{C}/L \longrightarrow E(\mathbf{C}), \qquad (z \neq 0) \mapsto (x, y) = (\wp(z), \wp'(z)), \qquad 0 \mapsto O.$$

**(7.2.2) Theorem.** *The lattice of periods of the holomorphic differential $\omega = dx/y$ on $E(\mathbf{C})$ is equal to $L$ and the map $\varphi$ is a holomorphic isomorphism, inverse to the Abel-Jacobi map*

$$\alpha : E(\mathbf{C}) \longrightarrow \mathbf{C}/L, \qquad \alpha(P) = \int_O^P \omega \pmod{L}.$$

*Proof.* The map $\varphi$ is holomorphic on $\mathbf{C} - \{0\}$; as $z$ (resp. $x/y$) is a local coordinate at $z = 0$ (resp. at $O$) on $\mathbf{C}/L$ (resp. on $E(\mathbf{C})$) and

$$\left(\frac{x}{y} \circ \varphi\right)(z) = \frac{\wp(z)}{\wp'(z)} = -\frac{z}{2} + \cdots$$

is holomorphic at $z = 0$, it follows that $\varphi$ is holomorphic everywhere. The composition of $\varphi$ with the projection $p$ from 4.1.2 is given by

$$\mathbf{C}/L \xrightarrow{\varphi} E(\mathbf{C}) \xrightarrow{p} \mathbf{P}^1(\mathbf{C}), \qquad z \mapsto \wp(z).$$

The only singularity of $\wp(z)$ is a double pole at $z = 0 \in \mathbf{C}/L$; thus $\deg(p \circ \varphi) = 2$, by 3.2.3.7. It follows that $\deg(\varphi) = \deg(p \circ \varphi)/\deg(p) = 2/2 = 1$, hence $\varphi$ is a holomorphic isomorphism (by 3.2.3). As $x \circ \varphi = \wp(z)$ and $y \circ \varphi = \wp'(z)$, we have

$$\varphi^*(\omega) = \varphi^*(\frac{dx}{y}) = \frac{d\wp(z)}{\wp'(z)} = dz$$

and

$$\int_\gamma dz = \int_{\varphi \circ \gamma} \omega, \tag{7.2.2.1}$$

for any path $\gamma$ in $\mathbf{C}/L$. Letting $\gamma$ in (7.2.2.1) run through a set of representatives of $H_1(\mathbf{C}/L, \mathbf{Z})$ proves the equality of the period lattices; taking for $\gamma$ the projection of any path from 0 to $z$ in $\mathbf{C}$ shows that

$$z = \int_0^z dz = \int_{\varphi(0)=O}^{\varphi(z)} \omega \pmod{L} = \alpha(\varphi(z)).$$

**(7.2.3) Theorem.** *The field of meromorphic functions on $\mathbf{C}/L$ is equal to $\mathcal{M}(\mathbf{C}/L) = \mathbf{C}(\wp(z), \wp'(z))$ (i.e. $\varphi$ induces an isomorphism between the field of rational functions $\mathbf{C}(x, y) = \mathrm{Frac}(\mathbf{C}[x, y]/(y^2 - (4x^3 - g_2x - g_3)))$ on $E$ and $\mathcal{M}(\mathbf{C}/L)$).*

*Proof.* Any elliptic function $f \in \mathcal{M}(\mathbf{C}/L)$ is of the form $f = f_+ + f_-$, where $f_\pm(z) = (f(z) \pm f(-z))/2$. As both $f_+(z)$ and $f_-(z)/\wp'(z)$ are even functions, we can assume that $f = f_+$ is even (and non-zero). We are going to show that, in this case, $f \in \mathbf{C}(\wp(z))$. As the divisor of $f$ is invariant under the map $z \mapsto -z$ on $\mathbf{C}/L$, it follows that

$$\mathrm{div}(f) = \sum_k n_k \left((a_k) + (-a_k) - 2(0)\right) + \sum_{j=1}^3 m_j \left(\left(\frac{\omega_j}{2}\right) - (0)\right),$$

where $n_k, m_j \in \mathbf{Z}$ and $a_k \neq -a_k \in \mathbf{C}/L$. By 5.2.1, we have

$$\sum_{j=1}^3 m_j \frac{\omega_j}{2} \in L \Longrightarrow m_j = m + 2n_j \qquad (m,\, n_j \in \mathbf{Z}).$$

This implies that the elliptic function

$$g(z) = \wp'(z)^m \prod_k (\wp(z) - \wp(a_k))^{n_k} \prod_{j=1}^{3} \left(\wp(z) - \wp\left(\frac{\omega_j}{2}\right)\right)^{n_j} \in \mathbf{C}(\wp(z), \wp'(z))$$

has the same divisor as $f$, hence $f(z) = c\,g(z)$ ($c \in \mathbf{C}^*$) also lies in $\mathbf{C}(\wp(z), \wp'(z))$. More precisely, $m \in 2\mathbf{Z}$ has to be even, as $f = f_+$, hence $f \in \mathbf{C}(\wp(z), \wp'(z)^2) = \mathbf{C}(\wp(z))$.
One could have also argued directly that $m_j = \mathrm{ord}_{\omega_j/2} f(z)$ is even, by substituting $n = 2k-1$ and $z = \omega_j/2$ to the formula $f^{(n)}(-z) = (-1)^n f^{(n)}(z)$.

**(7.2.4)** The algebraicity statement 7.2.3 is a special case of the following general results proved by Riemann:

(A) Every compact Riemann surface $X$ is isomorphic to $C(\mathbf{C})$, for some smooth projective irreducible curve $C$ over $\mathbf{C}$ (in general, $C$ is not a smooth plane curve).
(B) Every holomorphic map $X_1 = C_1(\mathbf{C}) \longrightarrow X_2 = C_2(\mathbf{C})$ between compact Riemann surfaces is induced by a (unique) morphism of algebraic curves $C_1 \longrightarrow C_2$ (thus the curve $C$ in (A) is unique up to isomorphism).
(C) The field of meromorphic functions on $X = C(\mathbf{C})$ coincides with the field of rational functions on $C$ (this follows from (B), if we consider a meromorphic function on $X$ as a holomorphic map $X \longrightarrow \mathbf{P}^1(\mathbf{C})$).

The nontrivial point is the existence of a non-constant meromorphic function on $X$; once this is established, the statements (A), (B), (C) follow in a relatively straightforward way.

**(7.2.5)** The analogous statements are false in higher dimensions. For example, if $L \xrightarrow{\sim} \mathbf{Z}^{2n}$ is a "generic" lattice in $\mathbf{C}^n$ ($n \geq 2$), then the $n$-dimensional complex torus $\mathbf{C}^n/L$ is not algebraic ([Mu AV], Ch. 1).

**(7.2.6) Exercise.** *Assume that the coefficients $g_2, g_3 \in \mathbf{R}$ in the equation of $E$ are real. Show that:*
(i) *If $\Delta(L) > 0$, then the roots $e_j$ are all real. Ordering them by $e_1 < e_3 < e_2$, then $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, where*

$$\frac{\omega_2}{2} = \int_{e_2}^{\infty} \frac{dx}{2\sqrt{(x-e_1)(x-e_2)(x-e_3)}} \in \mathbf{R}_{>0}, \qquad \frac{\omega_1}{2} = i\int_{e_3}^{e_2} \frac{dx}{2\sqrt{(x-e_1)(e_2-x)(x-e_3)}} \in i\mathbf{R}_{>0}$$

*(above, the square roots are taken to be non-negative). In particular,* $\mathrm{Re}(\omega_1/\omega_2) = 0$.
(ii) *If $\Delta(L) < 0$, then $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, where $\omega_2 \in \mathbf{R}_{>0}$ and $\omega_1 - \omega_2/2 \in i\mathbf{R}_{>0}$ (hence* $\mathrm{Re}(\omega_1/\omega_2) = 1/2$*).*

## 7.3 Relations between $\wp(z)$ and $\theta_{ab}(z)$

In this section $L = \mathbf{Z}\tau + \mathbf{Z}$, where $\mathrm{Im}(\tau) > 0$. We put $\omega_1 = \tau$, $\omega_2 = 1$ ($\Longrightarrow \omega_3 = \tau + 1$) and $e_j = \wp(\omega_j/2)$.

**(7.3.1) Proposition.** *In the notation of 6.3.8 and 6.4.6,*

$$\wp(z) - e_1 = \wp(z) - \wp(\tau/2) = \left(\frac{\theta_{01}(z)}{\theta_{11}(z)}\frac{\theta'_{11}}{\theta_{01}}\right)^2$$
$$\wp(z) - e_2 = \wp(z) - \wp(1/2) = \left(\frac{\theta_{10}(z)}{\theta_{11}(z)}\frac{\theta'_{11}}{\theta_{10}}\right)^2$$
$$\wp(z) - e_3 = \wp(z) - \wp((\tau+1)/2) = \left(\frac{\theta_{00}(z)}{\theta_{11}(z)}\frac{\theta'_{11}}{\theta_{00}}\right)^2$$

*Proof.* Both functions $\wp(z) - e_1$ and $g(z) = \theta_{01}^2(z)/\theta_{11}^2(z)$ lie in $\mathcal{M}(\mathbf{C}/L)$ and have the same divisor $\mathrm{div}(f) = \mathrm{div}(g) = 2(\tau/2) - 2(0)$; thus $f(z) = c\,g(z)$ for some $c \in \mathbf{C}^*$. If $z \longrightarrow 0$ tends to zero, then $f(z) \sim 1/z^2$, $\theta_{01}(z) \sim \theta_{01}$ and $\theta_{11}(z) \sim \theta'_{11} z$, hence $c = (\theta'_{11}/\theta_{01})^2$. The other two formulas are proved in the same way.

**(7.3.2) Corollary.** *The function $\wp'(z)$ is equal to*

$$\wp'(z) = -2\,\frac{\theta_{00}(z)\theta_{01}(z)\theta_{10}(z)}{\theta_{11}(z)^3}\,\frac{(\theta'_{11})^3}{\theta_{00}\theta_{01}\theta_{10}} \qquad \left(= 2\pi(\theta'_{11})^2\,\frac{\theta_{00}(z)\theta_{01}(z)\theta_{10}(z)}{\theta_{11}(z)^3}\right).$$

*Proof.* Multiplying the three identities in 7.3.1 yields a formula for $\wp'(z)^2/4$; the correct sign of its square root $\wp'(z)/2$ is determined by the asymtotics $\wp'(z) \sim -2/z^3$ as $z \longrightarrow 0$.

**(7.3.3) Proposition.** *We have*

$$e_3 - e_1 = \wp((\tau+1)/2) - \wp(\tau/2) = \left(\frac{\theta_{10}\theta'_{11}}{\theta_{00}\theta_{01}}\right)^2 \qquad (= \pi^2\theta_{10}^4)$$

$$e_1 - e_2 = \quad \wp(\tau/2) - \wp(1/2) \quad = \left(\frac{\theta_{00}\theta'_{11}}{\theta_{01}\theta_{10}}\right)^2 \qquad (= -\pi^2\theta_{00}^4)$$

$$e_2 - e_3 = \wp(1/2) - \wp((\tau+1)/2) = \left(\frac{\theta_{01}\theta'_{11}}{\theta_{10}\theta_{00}}\right)^2 \qquad (= \pi^2\theta_{01}^4)$$

*Proof.* Substitute $z = \tau/2, 1/2, (\tau+1)/2$ to 7.3.1 and use 6.4.5(ii) (resp. 6.4.13 for the values involving $\pi^2$).

**(7.3.4) Corollary.** *The functions*

$$\theta_{00} = \sum_{n\in\mathbf{Z}} q^{n^2/2}, \qquad \theta_{01} = \sum_{n\in\mathbf{Z}} (-1)^n q^{n^2/2}, \qquad \theta_{10} = -q^{1/8}\sum_{n\in\mathbf{Z}} q^{n(n+1)/2}$$

*satisfy*

$$\theta_{00}^4 = \theta_{01}^4 + \theta_{10}^4. \tag{7.3.4.1}$$

**(7.3.5)** Note that the proof of (7.3.4.1) sketched in 6.4.5 is much simpler; it does not use the identity 6.4.10.

**(7.3.6) Proposition (Jacobi's formula).** *The discriminant function $\Delta$ from (7.1.10.1) is given by*

$$\Delta(\mathbf{Z}\tau + \mathbf{Z}) = 2^4\left(\frac{(\theta'_{11})^3}{\theta_{00}\theta_{01}\theta_{10}}\right)^4 = (2\pi)^{12} q\prod_{n=1}^{\infty}(1-q^n)^{24} \qquad (= (2\pi)^4(\theta'_{11})^8).$$

*Proof.* Combine (7.1.10.1) with 7.3.3 and the product formulas (6.4.12.2) (note that the exact value of the factor $c(\tau)$ in (6.4.12.2) is irrelevant).

**(7.3.7)** The formulas in 7.3.1 are also useful for numerical calculations, as the infinite series defining the theta fonctions converge very rapidly.

## 7.4 Properties of $\sigma(z)$

Let $L \subset \mathbf{C}$ be an arbitrary lattice.

**(7.4.1)** Recall that $\sigma'(z)/\sigma(z) = \zeta(z)$ and $-\zeta'(z) = \wp(z) \in \mathcal{M}(\mathbf{C}/L)$. This implies that, for each $u \in L$, the function

$$\zeta(z+u;L) - \zeta(z;L) = \eta(u;L) \in \mathbf{C} \tag{7.4.1.1}$$

is constant. In fact,

$$\eta(u) = \eta(u;L) = \int_\gamma \zeta'(z)\,dz = -\int_\gamma \wp(z)\,dz,$$

where $\gamma$ is any path in $\mathbf{C} - L$ whose projection to $\mathbf{C}/L$ is closed and has class equal to $u \in L = H_1(\mathbf{C}/L, \mathbf{Z})$. The value of the integral does not depend on $\gamma$, as $\zeta'(z)dz = d\zeta(z)$ is the differential of a holomorphic function on $\mathbf{C} - L$ and the residues $\mathrm{res}_a(\zeta'(z)dz) = 0$ vanish at all $a \in L$. Using the isomorphism $\varphi : \mathbf{C}/L \xrightarrow{\sim} E(\mathbf{C})$ from 7.2.1, we can also write

$$\eta(u) = -\int_{\gamma_E} \frac{x\,dx}{y} \qquad (\gamma_E = \varphi(pr(\gamma))),$$

as $\varphi^*(x\,dx/y) = \wp(z)\,d\wp(z)/\wp'(z) = \wp(z)\,dz$.

**(7.4.2) Proposition (Legendre's relation).** *Fix a basis $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ of $L$ satisfying $\mathrm{Im}(\omega_1/\omega_2) > 0$ and put $\eta_j = \eta(\omega_j; L)$ $(j = 1, 2)$. Then*

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \eta_1 & \eta_2 \end{vmatrix} = 2\pi i.$$

*Proof.* Fix a fundamental parallelogram $D = \{z = \alpha + t_1\omega_1 + t_2\omega_2 \,|\, 0 \le t_1, t_2 \le 1\}$ for the action of $L$ on $\mathbf{C}$ containing 0 in its interior. As the only singularity of $\zeta(z)$ inside $D$ is a simple pole at $z = 0$, the residue theorem yields

$$2\pi i = 2\pi i \,\mathrm{res}_0(\zeta(z)\,dz) = \int_{\partial D} \zeta(z)\,dz = \int_\alpha^{\alpha+\omega_2} \underbrace{(\zeta(z) - \zeta(z+\omega_1))}_{-\eta_1}\,dz +$$
$$+ \int_\alpha^{\alpha+\omega_1} \underbrace{(\zeta(z+\omega_2) - \zeta(z))}_{\eta_2}\,dz = \omega_1\eta_2 - \omega_2\eta_1.$$

**(7.4.3) Lemma.** *For $u \in L$, put $\psi(u) = 1$ (resp. $= -1$) if $u/2 \in L$ (resp. if $u/2 \notin L$). Then*

$$\sigma(z+u) = \psi(u)\sigma(z)e^{\eta(u)(z+\frac{u}{2})}. \tag{7.4.3.1}$$

*Proof.* Integrating (7.4.1.1) we obtain (7.4.3.1) with some $\psi(u) \in \mathbf{C}^*$. If $u/2 \notin L$, evaluation at $z = -u/2$ yields $\psi(u) = \sigma(-u/2)/\sigma(u/2) = -1$. If $u/2 \in L$, we can assume $u \neq 0$ (the case $u = 0$ is trivial). As $\psi(2u) = \psi(u)^2$, writing $u = 2^n v$ with $v \in L$, $v/2 \notin L$ and $n \ge 1$ gives $\psi(u) = 1$.

**(7.4.4) Construction of elliptic functions using $\sigma(z)$.** The formula (7.4.3.1) implies that the construction from the proof of 5.3.5 can be performed using the $\sigma$-function: if $a_1, \ldots, a_n; b_1, \ldots, b_n \in \mathbf{C}$ (not necessarily distinct) satisfy $\sum_j a_j = \sum_j b_j \in \mathbf{C}$, then the function

$$f(z) = \prod_{j=1}^n \frac{\sigma(z-a_j)}{\sigma(z-b_j)}$$

lies in $\mathcal{M}(\mathbf{C}/L)$ and its divisor is equal to $\mathrm{div}(f) = \sum_j((P_j) - (Q_j))$, where $P_j$ (resp. $Q_j$) is the image of $a_j$ (resp. of $b_j$) in $\mathbf{C}/L$. Here is a simple example:

**(7.4.5) Lemma.** *For $a \in \mathbf{C} - L$,*

$$\wp(z) - \wp(a) = -\frac{\sigma(z-a)\sigma(z+a)}{\sigma(z)^2\sigma(a)^2}$$

*Proof.* The functions $\wp(z) - \wp(a)$ and $f(z) = \sigma(z-a)\sigma(z+a)/\sigma(z)^2$ both lie in $\mathcal{M}(\mathbf{C}/L) - \{0\}$ and have the same divisor $\mathrm{div}(\wp(z) - \wp(a)) = (a) + (-a) - 2(0) = \mathrm{div}(f)$; thus $\wp(z) - \wp(a) = c\,f(z)$ for some $c \in \mathbf{C}^*$. If $z \longrightarrow 0$, then $\wp(z) - \wp(a) \sim 1/z^2$ and $f(z) \sim -\sigma(a)^2/z^2$, hence $c = -1/\sigma(a)^2$.

**(7.4.6)** In the special case when $\omega_1 = \tau$ $(\mathrm{Im}(\tau) > 0)$ and $\omega_2 = 1$, The Legendre relation 7.4.2 becomes

$$\eta_1 = \tau\eta_2 - 2\pi i. \tag{7.4.6.1}$$

**(7.4.7) Lemma.** *The function*

$$g(z) = e^{-\frac{1}{2}\eta_2 z^2 + \pi i z}\sigma(z; \mathbf{Z}\tau + \mathbf{Z})$$

*satisfies*

$$g(z+1) = g(z)$$
$$g(z+\tau) = -e^{-2\pi i z}g(z).$$

*Proof.* Direct calculation – combine 7.4.3 with (7.4.6.1).

**(7.4.8) Corollary.** *We have*

$$g(z) = -\left(\frac{1}{2\pi i}\right)(1-t)\prod_{n=1}^{\infty}\frac{(1-q^n t)(1-q^n t^{-1})}{(1-q^n)^2} \qquad (t = e^{2\pi i z},\ q = e^{2\pi i \tau}).$$

*Proof.* The function $g(z)$ is holomorphic in $\mathbf{C}$, has simple zeros at $z \in \mathbf{Z}\tau + \mathbf{Z}$ (and no other zeros) and satisfies 7.4.7. Thus $g(z)/A(z)$ (where $A(z)$ is the function defined in 5.3.4) is a meromorphic function on $\mathbf{C}/L$ without zeros, hence constant. The value of this constant is determined by the asymptotic behaviour for $z \longrightarrow 0$:

$$g(z) \sim z, \qquad (1-t) \sim -2\pi i z, \qquad A(z)/(1-t) \sim \prod_{n=1}^{\infty}(1-q^n)^2.$$

**(7.4.9) Corollary.** *If* $\mathrm{Im}(\tau) > 0$ *and* $\eta_2 = \eta(1; \mathbf{Z}\tau + \mathbf{Z})$, *then*

$$\sigma(z; \mathbf{Z}\tau + \mathbf{Z}) = (2\pi i)^{-1} e^{\eta_2 z^2/2}(t^{1/2} - t^{-1/2})\prod_{n=1}^{\infty}\frac{(1-q^n t)(1-q^n t^{-1})}{(1-q^n)^2} =$$

$$= \theta_{11}(z;\tau)(-2\pi i)^{-1} q^{-1/8} e^{\eta_2 z^2/2}\prod_{n=1}^{\infty}\frac{1}{(1-q^n)^3} \qquad (t^\alpha = e^{2\pi i \alpha z},\ q^\alpha = e^{2\pi i \alpha \tau}).$$

*Proof.* This follows from 7.4.8, the definition of $g(z)$ and the product formula (6.4.12.1) (together with the exact value of $c(\tau)$ given by (6.4.12.3)).

**(7.4.10)** One can give another (?) proof of 7.3.6 using the properties of the $\sigma$-function, beginning with

$$e_j - e_k = \wp(\omega_j/2) - \wp(\omega_k/2) = -\frac{\sigma((\omega_j - \omega_k)/2)\sigma((\omega_j + \omega_k)/2)}{\sigma(\omega_j/2)^2 \sigma(\omega_k/2)^2}$$

(by 7.4.5) and using the product formula 7.4.9 to evaluate $\sigma(\omega_j/2)$ (for $\omega_j = \tau, 1, \tau + 1$).

## 7.5 Addition formulas for $\wp(z)$ and the group law on $E(\mathbf{C})$

**(7.5.1)** The torus $(\mathbf{C}/L, +)$ is an abelian group with respect to addition, with neutral element 0. The mutually inverse bijections

$$\begin{array}{lll} \varphi : \mathbf{C}/L \longrightarrow E(\mathbf{C}) & \alpha : E(\mathbf{C}) \longrightarrow \mathbf{C}/L & \varphi^*(dx/y) = dz \\ \quad z \mapsto (\wp(z), \wp'(z)) & \quad P \mapsto \displaystyle\int_O^P \frac{dx}{y} \pmod{L} & \alpha^*(dz) = dx/y \\ \quad 0 \mapsto O & & \end{array}$$

from 4.4.2 (resp. 7.2.2) transport this abelian group structure to $E(\mathbf{C})$. The corresponding addition $\boxplus$ on $E(\mathbf{C})$ has neutral element $O$ and satisfies

$$(\wp(z_1), \wp'(z_1)) \boxplus (\wp(z_2), \wp'(z_2)) = (\wp(z_1 + z_2), \wp'(z_1 + z_2)).$$

**(7.5.2) Characterization of "+" on $\mathbf{C}/L$.** The addition on $\mathbf{C}/L$ admits an abstract characterization in terms of the isomorphism

$$\boxplus : Cl^0(\mathbf{C}/L) \xrightarrow{\sim} \mathbf{C}/L$$

from 5.3.6. In concrete terms, if $a_j, b_j \in \mathbf{C}$ $(j = 1, \ldots, N)$ are complex numbers (not necessarily distinct) and $P_j = pr(a_j)$, $Q_j = pr(b_j)$ their projections (under $pr : \mathbf{C} \longrightarrow \mathbf{C}/L$) to the torus, then the following statements are equivalent:

$$\begin{gathered} P_1 + \cdots + P_N = Q_1 + \cdots + Q_N \in \mathbf{C}/L \\ (\exists f \in \mathcal{M}(\mathbf{C}/L)^*) \qquad \sum_{j=1}^{N} ((P_j) - (Q_j)) = \operatorname{div}(f) \\ a_1 + \cdots + a_N \equiv b_1 + \cdots + b_N \pmod{L} \\ \sum_{j=1}^{N} \int_0^{a_j} dz \equiv \sum_{j=1}^{N} \int_0^{b_j} dz \pmod{L}. \end{gathered} \tag{7.5.2.1}$$

**(7.5.3) Characterization of "$\boxplus$" on $E(\mathbf{C})$.** Application of the bijections $\varphi, \alpha$ from 7.5.1 to 5.3.6 yields an isomorphism of abelian groups

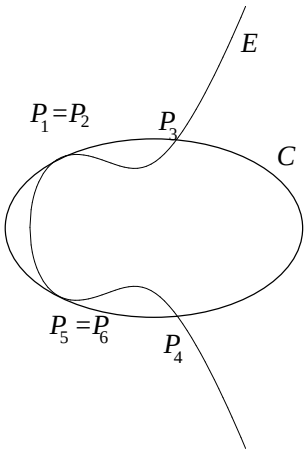
$$\begin{aligned} \boxplus : Cl^0(E(\mathbf{C})) &\xrightarrow{\sim} E(\mathbf{C}) \\ \sum n_j(P_j) &\mapsto \boxplus[n_j]P_j, \end{aligned}$$

where $[n]P$ (for $n \in \mathbf{Z}$) is defined as in 0.5.0. Furthermore, if $P_j, Q_j \in E(\mathbf{C})$ $(j = 1, \ldots, N)$ are points (not necessarily distinct) on $E$, then (7.5.2.1) translates into the following equivalent statements:

$$\begin{gathered} P_1 \boxplus \cdots \boxplus P_N = Q_1 \boxplus \cdots \boxplus Q_N \in E(\mathbf{C}) \\ (\exists f \in \mathcal{M}(E(\mathbf{C}))^*) \qquad \sum_{j=1}^{N} ((P_j) - (Q_j)) = \operatorname{div}(f) \\ \sum_{j=1}^{N} \int_O^{P_j} \frac{dx}{y} \equiv \sum_{j=1}^{N} \int_O^{Q_j} \frac{dx}{y} \pmod{L}. \end{gathered} \tag{7.5.3.1}$$

**(7.5.4) Example: Abel's Theorem revisited.** Let $F(X, Y, Z) \in \mathbf{C}[X, Y, Z]$ be a homogeneous polynomial of degree $d = \deg(F) \geq 1$ and $C : F = 0$ the corresponding projective plane curve $C \subset \mathbf{P}^2$.

Assume that the intersection $E(\mathbf{C}) \cap C(\mathbf{C})$ is *finite*; then the intersection divisor $E(\mathbf{C}) \cap C(\mathbf{C}) = (P_1) + \cdots + (P_{3d})$ has degree $3d$, by Bézout's Theorem (the points $P_j$ are not necessarily distinct).




As

$$f = \frac{F(X, Y, Z)}{Z^d} \in \mathcal{M}(E(\mathbf{C}))^*, \qquad \operatorname{div}(f) = \sum_{j=1}^{3d} (P_j) - 3d(O),$$

it follows from (7.5.3.1) that

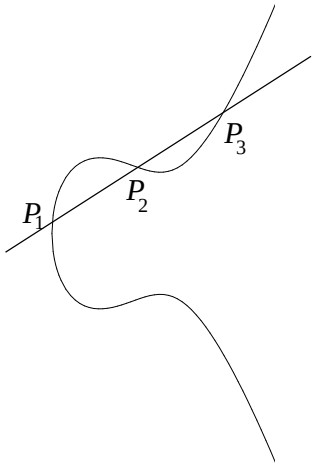
$$P_1 \boxplus \cdots \boxplus P_{3d} = [3d]O = O \tag{7.5.4.1}$$

on $E(\mathbf{C})$. Equivalently,

$$\sum_{j=1}^{3d} \int_O^{P_j} \frac{dx}{y} \equiv 0 \pmod{L},$$

which is a special case of Abel's theorem.

**(7.5.5) Example (continued).** If $d = 1$, i.e. if $F = a_0X + a_1Y + a_2Z$ is linear (and non-zero), then $C : F = 0$ is a line in $P^2$ and the intersection divisor $E(\mathbf{C}) \cap C(\mathbf{C}) = (P_1) + (P_2) + (P_3)$ consists of three points (not necessarily distinct).




The divisor of $f = F/Z = a_0x + a_1y + a_2 \in \mathcal{M}(E(\mathbf{C}))^*$ is equal to $\operatorname{div}(f) = (P_1) + (P_2) + (P_3) - 3(O)$, hence

$$P_1 \boxplus P_2 \boxplus P_3 = [3]O = O \tag{7.5.5.1}$$

and

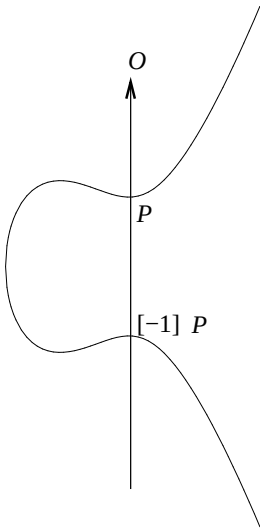
$$\int_O^{P_1} \frac{dx}{y} + \int_O^{P_2} \frac{dx}{y} + \int_O^{P_3} \frac{dx}{y} \equiv 0 \pmod{L},$$

which was already proved in 2.3.3.

Each "vertical" line $C' : X + cZ = 0$ ($c \in \mathbf{C}$) contains the point $O$; thus the intersection divisor $E(\mathbf{C}) \cap C'(\mathbf{C})$ is equal to $(O) + (P) + (P')$. If $P = (x, y) \neq O$, then necessarily $P' = (x, -y)$. As $O \boxplus P \boxplus P' = O$, it follows that

$$(x, -y) = P' = [-1]P = [-1](x, y) \tag{7.5.5.2}$$

is the inverse of $P$ with respect to the group law.




Equivalently, one can argue that

$$P = (\wp(z), \wp'(z))$$

for some $z \in \mathbf{C} - L$, hence

$$[-1]P = (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z)).$$

**(7.5.6) Geometric description of the group law $\boxplus$.** Given two distinct (resp. equal) points $P, Q \in E(\mathbf{C})$ on $E$, let $C = \overline{PQ} \subset \mathbf{P}^2$ be the unique line passing through them (resp. the tangent line to $E$ containing $P = Q$). The intersection divisor $E(\mathbf{C}) \cap C(\mathbf{C})$ is then equal to $(P) + (Q) + (R)$, for a uniquely determined point $R \in E(\mathbf{C})$. We denote this third intersection point by

$$P * Q := R. \tag{7.5.6.1}$$

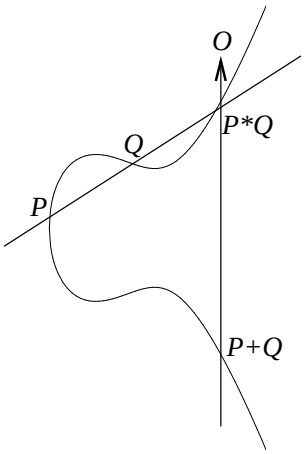
The discussion in 7.5.5 implies that

$$P * Q = [-1](P \boxplus Q), \qquad O * R = [-1]R,$$

hence

$$P \boxplus Q = O * (P * Q), \tag{7.5.6.2}$$

which gives a very simple geometric characterization of the group law $\boxplus$.



It is tempting to take (7.5.6.2) as a *definition* of $\boxplus$. However, this presents several problems: firstly, the verification of the associative law

$$(P \boxplus Q) \boxplus R \stackrel{?}{=} P \boxplus (Q \boxplus R)$$

becomes rather non-trivial (see 10.2.6 below for more details). Secondly, the "linear" nature of (7.5.6.2) conceals the more general "non-linear" identity (7.5.4.1). We have avoided both problems by taking the isomorphism

$$Cl^0(E(\mathbf{C})) \xrightarrow{\sim} E(\mathbf{C})$$

as a starting point.

**(7.5.7) Formulas for $\boxplus$.** On the other hand, (7.5.6.2) gives an explicit formula for $P_1 \boxplus P_2$. For example, if we assume that none of the three intersection points $P_j = (x_j, y_j)$ from 7.5.5 is equal to $O$, then we can work with the affine line $C \cap \{Z \neq 0\}$, given by the equation $y = ax + b$. Solving the system of equations

$$y = ax + b, \qquad y^2 = 4x^3 - g_2 x - g_3,$$

we obtain the polynomial identity

$$4x^3 - g_2 x - g_3 - (ax + b)^2 = 4(x - x_1)(x - x_2)(x - x_3).$$

Comparing the coefficients at $x^2$ yields

$$x_1 + x_2 + x_3 = \frac{a^2}{4} = \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2$$

(assuming that $P_1 \neq P_2$), hence

$$x_3 = \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2. \tag{7.5.7.1}$$

The $y$-coordinate of $P_3$ is equal to

$$y_3 = ax_3 + b, \qquad b = y_1 - ax_1 = y_1 - x_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right). \tag{7.5.7.2}$$

To sum up, if $P_1 \neq P_2$, then (7.5.7.1-2) give explicit formulas for the coordinates of

$$(x_1, y_1) \boxplus (x_2, y_2) = [-1](x_3, y_3) = (x_3, -y_3)$$

as rational functions in $x_1, x_2, y_1, y_2$ (with coefficients in $\mathbf{Q}$).

If $P_1 = P_2$, then the line $y = ax + b$ is tangent to $E$ at $P_1$. Differentiating the equation

$$y^2 = 4x^3 - g_2 x - g_3$$

yields

$$2y\,dy = (12x^2 - g_2)\,dx \Longrightarrow \frac{dy}{dx} = \frac{1}{y}\left(6x^2 - \frac{g_2}{2}\right),$$

hence

$$a = \frac{1}{y_1}\left(6x_1^2 - \frac{g_2}{2}\right)$$

and

$$x_3 = \frac{(6x_1^2 - g_2/2)^2}{4y_1^2} - 2x_1 = \frac{(3x_1^2 - g_2/4)^2 - 2x_1(4x_1^3 - g_2x_1 - g_3)}{y_1^2} = \frac{x_1^4 + \frac{g_2}{2}x_1^2 + 2g_3x_1 + \frac{g_2^2}{16}}{4x_1^3 - g_2x_1 - g_3}. \quad (7.5.7.3)$$

**(7.5.8) Addition formulas for $\wp(z)$.** The formulas (7.5.7.1-3) can be rewritten in terms of the bijection $\varphi : \mathbf{C}/L \xrightarrow{\sim} E(\mathbf{C})$. Writing

$$P_j = (x_j, y_j) = (\wp(z_j), \wp'(z_j)), \qquad z_1 + z_2 + z_3 = 0 \in \mathbf{C}/L,$$

we obtain

$$\wp(z_1 + z_2) = \frac{1}{4}\left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)}\right)^2 - \wp(z_1) - \wp(z_2) \quad (7.5.8.1)$$

in the case $z_1 \neq z_2 \in \mathbf{C}/L$ and

$$\wp(2z) = \frac{\wp(z)^4 + \frac{g_2}{2}\wp(z)^2 + 2g_3\wp(z) + \frac{g_2^2}{16}}{4\wp(z)^3 - g_2\wp(z) - g_3}. \quad (7.5.8.2)$$

Differentiating (7.5.8.1-2) with respect to $z_1$ (resp. $z$) yields explicit formulas for $\wp'(z_1 + z_2)$ resp. $\wp'(2z)$.

**(7.5.9) Exercise.** *Show that, for each $j = 1, 2, 3$, there exists $f_j(z) \in \mathcal{M}(\mathbf{C}/L)$ such that*

$$\wp(2z) - e_j = \wp(2z) - \wp(\omega_j/2) = f_j^2(z).$$

**(7.5.10) Proposition.** *For each $n \in \mathbf{Z} - \{0\}$, the multiplication by $n$ map $[n] : E(\mathbf{C}) \longrightarrow E(\mathbf{C})$ is given by rational functions of the coordinates, with coefficients in $\mathbf{Q}(g_2, g_3)$. In other words,*

$$\wp(nz), \wp'(nz) \in \mathbf{Q}(g_2, g_3, \wp(z), \wp'(z)).$$

*Proof.* Induction on $|n|$, using (7.5.5.1) and (7.5.8.1-2).

**(7.5.11) Torsion points.** For each $n \geq 1$, denote by

$$E(\mathbf{C})_n = \{P \in E(\mathbf{C}) \,|\, [n]P = O\}$$

the $n$-torsion subgroup of $E(\mathbf{C})$ (which is an elliptic analogue of the group of $n$-th roots of unity from 0.6.0). As

$$(\mathbf{C}/L)_n = \frac{1}{n}L/L = \left(\frac{1}{n}\mathbf{Z}/\mathbf{Z}\right)\omega_1 \oplus \left(\frac{1}{n}\mathbf{Z}/\mathbf{Z}\right)\omega_2,$$

it follows that

$$E(\mathbf{C})_n = \{O\} \cup \{(\wp((a\omega_1 + b\omega_2)/n), \wp'((a\omega_1 + b\omega_2)/n)) \,|\, (a, b) \in (\mathbf{Z}/n\mathbf{Z})^2 - \{(0, 0)\}\}.$$

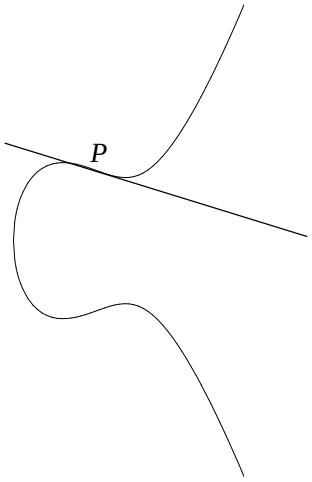
For $n = 2$, a point $P = (x, y) \in E(\mathbf{C}) - \{O\}$ satisfies

$$[2]P = O \iff P = [-1]P \iff (x, y) = (x, -y) \iff y = 0;$$

Thus

$$E(\mathbf{C})_2 = \{O\} \cup \{(e_1, 0), (e_2, 0), (e_3, 0)\}.$$

For $n = 3$, a point $P \in E(\mathbf{C})$ satisfies $[3]P = O$ iff $[2]P \boxplus P = O$, i.e. iff the tangent line to $E$ at $P$ has intersection multiplicity with $E$ at $P$ equal to 3. Geometrically, this amounts to $P$ being an inflection point of $E(\mathbf{C})$.




### 7.6 Morphisms $\mathbf{C}/L_1 \longrightarrow \mathbf{C}/L_2$

Let $L_1, L_2 \subset \mathbf{C}$ be lattices and $E_1, E_2$ the corresponding cubic curves (as in 7.2.1).

**(7.6.1) Proposition.** (i) *The set of holomorphic maps $f : \mathbf{C}/L_1 \longrightarrow \mathbf{C}/L_2$ satisfying $f(0) = 0$ is equal to*

$$\{f(z) = \lambda z \,|\, \lambda \in \mathbf{C}, \lambda L_1 \subseteq L_2\}.$$

*In particular, each such map is a homomorphism of abelian groups ($f(z_1 + z_2) = f(z_1) + f(z_2)$).*
(ii) *The map $E_1(\mathbf{C}) \longrightarrow E_2(\mathbf{C})$ corresponding to $f$ is given by*

$$(\wp(z; L_1), \wp'(z; L_1)) \mapsto (\wp(\lambda z; L_2), \wp'(\lambda z; L_2))$$

*(and is also a homomorphism of abelian groups).*
(iii) *$f$ is an isomorphism of Riemann surfaces $\iff \lambda L_1 = L_2$.*

*Proof.* As $\mathbf{C}$ is simply connected and the projection $pr_2 : \mathbf{C} \longrightarrow \mathbf{C}/L_2$ is an unramified covering, there exists a unique holomorphic map $F : \mathbf{C} \longrightarrow \mathbf{C}$ satisfying $F(0) = 0$ and making the following diagram commutative:

$$\begin{array}{ccc} \mathbf{C} & \xrightarrow{F} & \mathbf{C} \\ \downarrow{\scriptstyle pr_1} & & \downarrow{\scriptstyle pr_2} \\ \mathbf{C}/L_1 & \xrightarrow{f} & \mathbf{C}/L_2. \end{array}$$

For each $u \in L_1$, the function

$$g(z) = F(z + u) - F(z)$$

is holomorphic in $\mathbf{C}$ and has discrete image $g(\mathbf{C}) \subseteq L_2$; thus $g(z)$ is constant and

$$0 = g'(z) = F'(z + u) - F'(z),$$

which implies that $F'(z) \in \mathcal{O}(\mathbf{C}/L) = \mathbf{C}$ is constant as well, hence $F(z) = \lambda z + F(0) = \lambda z$ for some $\lambda \in \mathbf{C}$. As $pr_2 \circ F = f \circ pr_1$, we have $\lambda L_1 = F(L_1) \subseteq L_2$, proving the non-trivial implication in (i). The statements (ii) and (iii) are immediate consequences of (i).

**(7.6.2) Corollary.** *The $j$-function (7.1.10.2) defines a map*

$$j : \{\text{Isomorphism classes of tori } \mathbf{C}/L\} \longrightarrow \mathbf{C}.$$

*Proof.* This follows from 7.6.1(iii) and $j(\lambda L) = j(L)$.

**(7.6.3) Definition.** *An* **isogeny** $f : \mathbf{C}/L_1 \longrightarrow \mathbf{C}/L_2$ *is a non-constant holomorphic map* $f$ *satisfying* $f(0) = 0$.

**(7.6.4)** In other words, 7.6.1 implies that an isogeny is given by

$$\begin{aligned} f : \mathbf{C}/L_1 &\longrightarrow \mathbf{C}/L_2 \\ z &\mapsto \lambda z, \qquad\qquad \lambda L_1 \subseteq L_2,\ \lambda \neq 0. \end{aligned} \tag{7.6.4.1}$$

It is a proper unramified covering of degree

$$\deg(f) = |\mathrm{Ker}(f)| = |\lambda^{-1}L_2/L_1| = |L_2/\lambda L_1|.$$

A typical example of an isogeny is the multiplication map

$$[n] : \mathbf{C}/L \longrightarrow \mathbf{C}/L, \qquad z \mapsto nz \qquad\qquad (n \in \mathbf{Z} - \{0\}),$$

which has degree

$$\deg[n] = \left|\frac{1}{n}L/L\right| = n^2.$$

**(7.6.5) Dual isogeny.** In the situation of (7.6.4.1), we have

$$\deg(f) \cdot \mathrm{Ker}(f) = 0 \Longrightarrow \deg(f) \cdot \lambda^{-1}L_2 \subseteq L_1.$$

This implies that the map

$$\widehat{f} : \mathbf{C}/L_2 \xrightarrow{\lambda^{-1}} \mathbf{C}/\lambda^{-1}L_2 \xrightarrow{\deg(f)} \mathbf{C}/L_1$$

is well defined, and in fact is an isogeny – the *dual isogeny to* $f$. It is characterized by the properties

$$\begin{aligned} \widehat{f} \circ f &= [\deg(f)] : \mathbf{C}/L_1 \longrightarrow \mathbf{C}/L_1 \\ f \circ \widehat{f} &= [\deg(f)] : \mathbf{C}/L_2 \longrightarrow \mathbf{C}/L_2. \end{aligned}$$

For example,

$$\widehat{[n]} = [n] \qquad\qquad (n \in \mathbf{Z} - \{0\}).$$

**(7.6.6) Proposition.** *Let* $f : \mathbf{C}/L_1 \longrightarrow \mathbf{C}/L_2$ *be an isogeny. Then:*
(i) $\mathrm{Ker}(f)$ *acts on* $\mathcal{M}(\mathbf{C}/L_1)$ *by* $(u * g)(z) = g(z - u)$ *and the fixed field of this action is equal to*

$$\mathcal{M}(\mathbf{C}/L_1)^{\mathrm{Ker}(f)} = f^*(\mathcal{M}(\mathbf{C}/L_2)) = \{f^*(h) = h \circ f \,|\, h \in \mathcal{M}(\mathbf{C}/L_2)\}.$$

(ii) $\mathcal{M}(\mathbf{C}/L_1)$ *is a finite Galois extension of* $f^*(\mathcal{M}(\mathbf{C}/L_2))$*, with Galois group isomorphic to* $\mathrm{Ker}(f)$.

*Proof.* (i) We use the notation (7.6.4.1). A function $g \in \mathcal{M}(\mathbf{C}/L_1)$ satisfies $u*g = g$ for all $u \in \mathrm{Ker}(f) \iff$ $g(z)$ is $\lambda^{-1}L_2$-periodic $\iff$ $h(z) = g(\lambda^{-1}z)$ is $L_2$-periodic $\iff$ $g(z) = h(\lambda z) = f^*(h)$, $h \in \mathcal{M}(\mathbf{C}/L_2)$.
(ii) This follows from (i), by E. Artin's Theorem.

**(7.6.7) Definition.** *Let* $L \subset \mathbf{C}$ *be a lattice. The* **endomorphism ring** *of* $\mathbf{C}/L$ *is*

$$\mathrm{End}(\mathbf{C}/L) = \{f : \mathbf{C}/L \longrightarrow \mathbf{C}/L \,|\, f \text{ holomorphic}, f(0) = 0\} = \{\lambda \in \mathbf{C} \,|\, \lambda L \subseteq L\} \subset \mathbf{C}.$$

*Above, we have identified* $\lambda$ *with the corresponding map* $[\lambda] : \mathbf{C}/L \longrightarrow \mathbf{C}/L$.

**(7.6.8) Proposition.** *Let* $L \subset \mathbf{C}$ *be a lattice. Then*
(i) $\mathrm{End}(\mathbf{C}/L) = \mathrm{End}(\mathbf{C}/\lambda L) \qquad (\lambda \in \mathbf{C}^*)$.
(ii) *Let* $L = \mathbf{Z}\tau + \mathbf{Z}$*, where* $\mathrm{Im}(\tau) > 0$. *Then*

$$\mathrm{End}(\mathbf{C}/\mathbf{Z}\tau + \mathbf{Z}) = \begin{cases} \mathbf{Z}A\tau + \mathbf{Z}, & \text{if } A\tau^2 + B\tau + C = 0,\ A, B, C \in \mathbf{Z},\ (A, B, C) = 1 \\ \mathbf{Z}, & \text{otherwise.} \end{cases}$$

*Proof.* The statement (i) is clear. In (ii), assume that $\lambda \in \mathbf{C} - \mathbf{Z}$ satisfies $\lambda L \subseteq L$. Then there exist $a, b, c, d \in \mathbf{Z}$, $a \neq 0$ such that

$$\left.\begin{aligned} \lambda \cdot 1 &= a\tau + b \\ \lambda \cdot \tau &= c\tau + d \end{aligned}\right\} \Longrightarrow a\tau^2 + (b-c)\tau - d = 0.$$

Divide this quadratic equation by the gcd of the coefficients, in order to obtain $A\tau^2 + B\tau + C = 0$ as in the statement of the Proposition. Then

$$\lambda = a\tau + b \in \mathbf{Z}a\tau + \mathbf{Z} \subseteq \mathbf{Z}A\tau + \mathbf{Z} \qquad (\text{as } A|a).$$

Conversely, the identities

$$A\tau \cdot 1 = A\tau \in L, \qquad A\tau \cdot \tau = A\tau^2 = -B\tau - C \in L$$

imply that $\mathbf{Z}A\tau + \mathbf{Z}$ is contained in $\mathrm{End}(\mathbf{C}/\mathbf{Z}\tau + \mathbf{Z})$.

**(7.6.9) Definition-Exercise.** *If* $\mathrm{End}(\mathbf{C}/L) \neq \mathbf{Z}$, *we say that* $\mathbf{C}/L$ *has* **complex multiplication**. *Show that* $K = \mathrm{End}(\mathbf{C}/L) \otimes \mathbf{Q}$ *is then an imaginary quadratic field and* $\deg([\lambda]) = N_{K/\mathbf{Q}}(\lambda)$ $(\lambda \in \mathrm{End}(\mathbf{C}/L))$.

**(7.6.10) Examples:** (1) $L = \mathbf{Z}i\omega + \mathbf{Z}\omega$, in which case $\mathrm{End}(\mathbf{C}/L) = \mathbf{Z}[i]$, $g_3 = 0$ and $g_2 \neq 0$, i.e.

$$E - \{O\} : y^2 = 4x^3 - g_2 x.$$

(2) $L = \mathbf{Z}\rho\omega + \mathbf{Z}\omega$, where $\rho = e^{2\pi i/3}$; then $\mathrm{End}(\mathbf{C}/L) = \mathbf{Z}[\rho]$, $g_2 = 0$ and $g_3 \neq 0$, hence

$$E - \{O\} : y^2 = 4x^3 - g_3.$$

**(7.6.11) Definition-Exercise.** *Let* $L \subset \mathbf{C}$ *be a lattice. The* **group of automorphisms** *of* $\mathbf{C}/L$ *is defined as the group of invertible elements of* $\mathrm{End}(\mathbf{C}/L)$*:*

$$\mathrm{Aut}(\mathbf{C}/L) = \mathrm{End}(\mathbf{C}/L)^*.$$

*Show that* $\mathrm{Aut}(\mathbf{C}/L) = \{f \in \mathrm{End}(\mathbf{C}/L) \mid \deg(f) = 1\}$ *and*

$$\mathrm{Aut}(\mathbf{C}/L) = \begin{cases} \{\pm 1, \pm i\}, & \text{if } L = \mathbf{Z}i\omega + \mathbf{Z}\omega \\ \{\pm 1, \pm\rho, \pm\rho^2\}, & \text{if } L = \mathbf{Z}\rho\omega + \mathbf{Z}\omega \\ \{\pm 1\}, & \text{otherwise.} \end{cases}$$

## 8. Lemniscatology or Complex Multiplication by $\mathbf{Z}[i]$

Throughout this section, $\sqrt{x}$ will denote the non-negative square root of a non-negative real number $x$.

### 8.1 The curve $y^2 = 1 - x^4$

**(8.1.1)** According to 3.7.7-8, the affine plane curve

$$V_{\mathrm{aff}} : y^2 = 1 - x^4$$

(over $\mathbf{C}$) is smooth and its projectivization admits a smooth desingularization $V = V_{\mathrm{aff}} \cup \{O_+, O_-\}$ with two points at infinity, which correspond to the 'asymptotics'

$$(x, y) \longrightarrow O_\pm \iff x \longrightarrow \infty, \quad y/x^2 \longrightarrow \pm i.$$

In coordinates, let $V'_{\mathrm{aff}}$ be the smooth affine plane curve

$$V'_{\mathrm{aff}} : y'^2 = x'^4 - 1.$$

The change of variables

$$x' = 1/x, \qquad y' = y/x^2, \qquad x = 1/x', \qquad y = y'/x'^2 \tag{8.1.1.1}$$

defines an isomorphism of curves

$$V_{\mathrm{aff}} - \{(x,y) = (0,\pm 1)\} \xrightarrow{\sim} V'_{\mathrm{aff}} - \{(x',y') = (0,\pm i) = O_{\pm}\} \tag{8.1.1.2}$$

and $V$ is obtained by gluing $V_{\mathrm{aff}}$ and $V'_{\mathrm{aff}}$ along the common open subset $V_{\mathrm{aff}} - \{(0,\pm 1)\} \xrightarrow{\sim} V'_{\mathrm{aff}} - \{O_{\pm}\}$ via (8.1.1.2).

We shall need this construction only in the analytic context: as $V_{\mathrm{aff}}(\mathbf{C})$ and $V'_{\mathrm{aff}}(\mathbf{C})$ are Riemann surfaces and (8.1.1.2) is a holomorphic isomorphism, we obtain a structure of a Riemann surface on $V(\mathbf{C})$ (cf. 8.1.2(i)).

**(8.1.2) Exercise-Reminder (cf. 4.2.4-7).** *Let $p : V(\mathbf{C}) \longrightarrow \mathbf{P}^1(\mathbf{C})$ be the map defined by*

$$p(x,y) = (x:1), \qquad (x,y) \in V_{\mathrm{aff}}(\mathbf{C}); \qquad p(x',y') = (1:x'), \qquad (x',y') \in V'_{\mathrm{aff}}(\mathbf{C}).$$

*Show that*
(i) *The natural topology on $V(\mathbf{C})$ is Hausdorff.*
(ii) *$p$ is a proper holomorphic map of degree* $\deg(p) = 2$.
(iii) *$V(\mathbf{C})$ is compact.*
(iv) *The ramification points of $p$ are* $(x,y) = (\pm 1, 0), (\pm i, 0)$.
(v) *The genus of $V(\mathbf{C})$ is equal to* $g(V) = 1$.
(vi) *The differential $\omega_V = dx/y = -dx'/y'$ is holomorphic on $V(\mathbf{C})$ and has no zeros (i.e. $(\forall P \in V(\mathbf{C}))$, $\mathrm{ord}_P(\omega_V) = 0$).*

**(8.1.3)** As observed in 4.4.4, the same arguments as in 4.3-4 show that the group of periods

$$L_V = \{\int_\gamma \omega_V \,|\, \gamma \in H_1(V(\mathbf{C}), \mathbf{Z})\} \subset \mathbf{C}$$

is a lattice and the Abel-Jacobi map

$$\alpha_V : V(\mathbf{C}) \longrightarrow \mathbf{C}/L_V, \qquad \alpha_V(Q) = \int_{(0,1)}^{Q} \omega_V \pmod{L_V} \tag{8.1.3.1}$$

is an isomorphism of Riemann surfaces.

**(8.1.4)** Let us compute a few values of $\alpha_V$. By definition,

$$\begin{aligned}
\alpha_V((0,1)) &= 0, \\
\alpha_V((1,0)) &= \int_0^1 \frac{dx}{\sqrt{1-x^4}} = \frac{\Omega}{2} \pmod{L_V} \\
\alpha_V((0,-1)) &= \Omega \pmod{L_V} \\
\alpha_V((-1,0)) &= \frac{3}{2}\Omega \pmod{L_V} = -\frac{\Omega}{2} \pmod{L_V}.
\end{aligned}$$

Indeed, the set of real points $V(\mathbf{R}) = V_{\mathrm{aff}}(\mathbf{R})$ of $V$ (say, with the negative orientation) is a closed path on $V(\mathbf{C})$, hence

$$\int_{V(\mathbf{R})} \omega_V = 4\int_0^1 \frac{dx}{\sqrt{1-x^4}} = 2\Omega \in L_V.$$

Similarly, the substitution $x = t^{-1}$ gives

$$\alpha_V(O_\pm) - \alpha_V((1,0)) = \int_{(1,0)}^{O_\pm} \omega_V = \frac{1}{\pm i}\int_1^\infty \frac{dx}{\sqrt{x^4-1}} = \frac{1}{\pm i}\int_0^1 \frac{dt}{\sqrt{1-t^4}} = \mp i\frac{\Omega}{2},$$

hence

$$\alpha_V(O_\pm) = \frac{1 \mp i}{2}\Omega \ (\mathrm{mod}\, L_V). \tag{8.1.4.1}$$

## 8.2 The lemniscate sine revisited

**(8.2.1)** The inverse of the Abel-Jacobi map (8.1.3.1) is an isomorphism of Riemann surfaces

$$\varphi_V : \mathbf{C}/L_V \xrightarrow{\sim} V(\mathbf{C}).$$

By (8.1.4.1), $\varphi_V$ restricts to a holomorphic isomorphism

$$\mathbf{C}/L_V - \{\frac{1 \pm i}{2}\Omega \ (\mathrm{mod}\, L_V)\} \xrightarrow{\sim} V_{\mathrm{aff}}(\mathbf{C}), \qquad z \mapsto (x(z), y(z)),$$

where $x(z), y(z)$ are holomorphic functions on $\mathbf{C}/L_V - \{\frac{1\pm i}{2}\Omega \ (\mathrm{mod}\, L_V)\}$ satisfying

$$y(z)^2 = 1 - x(z)^4, \qquad \frac{dx(z)}{dz} = y(z) \quad (\text{as } \alpha_V^*(dz) = dx/y) \Longrightarrow x'(z)^2 = 1 - x(z)^4.$$

**(8.2.2) Definition of $sl(z)$.** In fact, $x(z)$ is the restriction of the meromorphic function

$$sl : \mathbf{C}/L_V \xrightarrow{\varphi_V} V(\mathbf{C}) \xrightarrow{p} \mathbf{P}^1(\mathbf{C}),$$

where $p$ is the map from 8.1.2. The function $sl(z)$ is meromorphic on $\mathbf{C}/L_V$, holomorphic outside the two points $\frac{1\pm i}{2}\Omega \ (\mathrm{mod}\, L_V)$ and satisfies

$$sl'(z)^2 = 1 - sl(z)^4.$$

The isomorphism $\varphi_V$ is given by the formulas

$$\varphi_V : \begin{cases} z \mapsto (sl(z), sl'(z)), & z \neq \frac{1\pm i}{2}\Omega \ (\mathrm{mod}\, L_V) \\ \frac{1\pm i}{2}\Omega \mapsto O_\mp. \end{cases}$$

The calculations from 8.1.4 imply that

$$sl(0) = sl(\Omega) = 0, \qquad sl(\frac{\Omega}{2}) = 1 = -sl(-\frac{\Omega}{2}),$$
$$sl'(0) = 1 = -sl'(\Omega), \qquad sl'(\frac{\Omega}{2}) = sl'(-\frac{\Omega}{2}) = 0.$$

**(8.2.3) Properties of $sl(z)$.** The maps $[\pm i] : V(\mathbf{C}) \longrightarrow V(\mathbf{C})$ defined by

$$[\pm i](x,y) = (\pm ix, y), \qquad (x,y) \in V_{\mathrm{aff}}(\mathbf{C}); \qquad [\pm i](x',y') = (\mp ix', -y'), \qquad (x',y') \in V'_{\mathrm{aff}}(\mathbf{C})$$

are mutually inverse holomorphic isomorphisms satisfying $[\pm i]^*(\omega_V) = \pm i\,\omega_V$. This implies that

$$\pm i\int_\gamma \omega_V = \int_\gamma [\pm i]^*(\omega_V) = \int_{[\pm i]\circ\gamma} \omega_V,$$

for any path $\gamma$ on $V(\mathbf{C})$. In particular, letting $\gamma$ run through the representatives of $H_1(V(\mathbf{C}), \mathbf{Z})$ we obtain

$$iL_V = L_V.$$

Taking for $\gamma$ a path from $(0,1)$ to $Q$ yields

$$\alpha_V([\pm i]Q) = \pm i\,\alpha_V(Q) \iff (sl(\pm iz), sl'(\pm iz)) = (\pm i sl(z), sl'(z)) \tag{8.2.3.1}$$

If $0 \leq x \leq 1$, let $y = \sqrt{1-x^4}$. Then

$$\alpha_V((x,y)) = \int_0^x \frac{dt}{\sqrt{1-t^4}}$$
$$\alpha_V((-x,-y)) = \alpha_V((0,-1)) + \int_0^x \frac{dt}{\sqrt{1-t^4}} = \Omega + \alpha_V((x,y)),$$

hence

$$sl(z+\Omega) = -sl(z) \tag{8.2.3.2}$$

for $z \in [0, \Omega/2]$. It follows from 3.2.2.9 that (8.2.3.2) holds everywhere on $\mathbf{C}/L_V$. The relations (8.2.3.1-2) imply that

$$sl(z+i\Omega) = i\,sl(z/i+\Omega) = -i\,sl(z/i) = -sl(z)$$
$$sl(z+(1+i)\Omega) = -sl(z+i\Omega) = sl(z),$$

hence

$$\mathbf{Z}\cdot(1+i)\Omega + \mathbf{Z}\cdot 2\Omega = (1+i)\mathbf{Z}[i]\cdot\Omega \subseteq L_V. \tag{8.2.3.3}$$

As we shall see in 8.3.5 below, the inclusion (8.2.3.3) is in fact an equality.

As in 7.5.1, the bijection $\varphi_V$ induces an abelian group law $\boxplus$ on $V(\mathbf{C})$ with neutral element $(0,1)$, characterized by

$$(sl(z_1), sl'(z_1)) \boxplus (sl(z_2), sl'(z_2)) = (sl(z_1+z_2), sl'(z_1+z_2)).$$

## 8.3 Relations between $sl(z)$ and $\wp(z)$

**(8.3.1) The cubic curve $E$.** The smooth plane curves (over $\mathbf{C}$)

$$E_{\text{aff}} : v^2 = 4u^3 - 4u = 4(u+1)u(u-1)$$
$$E = E_{\text{aff}} \cup \{O\}, \qquad O = (0:1:0)$$

are of the type considered in 7.2. In particular, $\omega_E = du/v$ is a holomorphic differential without zeros on $E(\mathbf{C})$ and the Abel-Jacobi map

$$\alpha : E(\mathbf{C}) \longrightarrow \mathbf{C}/L, \qquad \alpha(P) = \int_O^P \omega_E \pmod{L}$$

is an isomorphism of Riemann surfaces, where

$$L = \{\int_\gamma \omega_E \,|\, \gamma \in H_1(E(\mathbf{C}), \mathbf{Z})\}$$

is the period lattice of $\omega_E$. According to 7.2.6(i), we have $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, where

$$\frac{\omega_2}{2} = \int_1^\infty \frac{dx}{\sqrt{4x^3-4x}}, \qquad \frac{\omega_1}{2} = i\int_0^1 \frac{dx}{\sqrt{4x-4x^3}} \overset{(x=t^{-1})}{=\!=} i\int_1^\infty \frac{dt}{\sqrt{4t^3-4t}} = i\,\frac{\omega_2}{2},$$

hence

$$\omega_1 = i\,\omega_2, \qquad L = \mathbf{Z}[i]\cdot\omega_2.$$

**(8.3.2) A map between $V$ and $E$.** In terms of the variable $z \in \mathbf{C}$, the inverse maps to $\alpha$, $\alpha_V$ are given by

$$\begin{aligned} \varphi : \mathbf{C}/L &\xrightarrow{\sim} E(\mathbf{C}), \qquad z \mapsto (\wp(z;L), \wp'(z;L)), \\ \varphi_V : \mathbf{C}/L_V &\xrightarrow{\sim} V(\mathbf{C}), \qquad z \mapsto (sl(z), sl'(z)), \end{aligned}$$

where

$$\wp(z) \sim z^{-2}, \qquad sl(z) \sim z \qquad \text{as } z \longrightarrow 0. \tag{8.3.2.1}$$

The asymptotic relations (8.3.2.1) seem to suggest the following *educated guess*: perhaps

$$\wp(z;L) \overset{??}{=} \frac{1}{sl(z)^2} \qquad\qquad ?? \tag{8.3.2.2}$$

Does (8.3.2.2) hold? If true, then the identity

$$\left(\frac{1}{sl(z)^2}\right)' = -\frac{2sl'(z)}{sl(z)^3}$$

tells us that we should consider the map

$$f : \begin{cases} (x,y) \mapsto (1/x^2, -2y/x^3), & (x,y) \in V_{\text{aff}}(\mathbf{C}) - \{(0,\pm 1)\} \\ (0,\pm 1) \mapsto O, & \\ (x',y') \mapsto (x'^2, -2x'y'), & (x',y') \in V'_{\text{aff}}(\mathbf{C}). \end{cases}$$

**(8.3.3) Exercise.** *$f$ defines a proper holomorphic map $f : V(\mathbf{C}) \longrightarrow E(\mathbf{C})$ of degree $\deg(f) = 2$, which is everywhere unramified.*

**(8.3.4)** The formula

$$f^*(\omega_E) = \frac{d(u\circ f)}{v\circ f} = \frac{d(1/x^2)}{-2y/x^3} = \frac{dx}{y} = \omega_V = \alpha_V^*(dz)$$

implies that $\varphi_V^* \circ f^*(\omega_E) = dz$ and

$$\frac{\Omega}{2} = \int_{(0,1)}^{(1,0)} \omega_V = \int_{(0,1)}^{(1,0)} f^*(\omega_E) = \int_O^{(1,0)} = \frac{\omega_2}{2},$$

hence

$$L = \mathbf{Z}[i]\cdot\Omega = \mathbf{Z}\cdot i\Omega + \mathbf{Z}\cdot\Omega.$$

**(8.3.5) Proposition.** *The lattice $L_V$ is equal to*

$$L_V = \mathbf{Z}\cdot(1+i)\Omega + \mathbf{Z}\cdot 2\Omega = (1+i)L \subset L = \mathbf{Z}\cdot i\Omega + \mathbf{Z}\cdot\Omega,$$

*and the following diagram is commutative:*

$$\begin{array}{ccccc} \mathbf{C} & \xrightarrow{pr} & \mathbf{C}/L_V & \xrightarrow{\varphi_V} & V(\mathbf{C}) \\ \| & & \downarrow & & \downarrow f \\ \mathbf{C} & \xrightarrow{pr} & \mathbf{C}/L & \xrightarrow{\varphi} & E(\mathbf{C}). \end{array}$$

*In particular,*

$$\wp(z;L) = \frac{1}{sl(z)^2}$$

*and $f$ is a homomorphism of abelian groups.*

*Proof.* For each closed path $\gamma$ on $V(\mathbf{C})$,

$$\int_\gamma \omega_V = \int_\gamma f^*(\omega_E) = \int_{f(\gamma)} \omega_E;$$

this implies that $L_V \subseteq L$. Similarly, for each point $Q \in V(\mathbf{C})$ we have

$$\alpha_V(Q) = \int_{(0,1)}^{Q} \omega_V \pmod{L_V} = \int_{(0,1)}^{Q} f^*(\omega_E) \pmod{L_V} = \int_O^{f(Q)} \omega_E \pmod{L_V},$$

hence

$$\alpha_V(Q) \pmod{L} = \alpha(f(Q)) \pmod{L}.$$

This proves the commutativity of the diagram, as $\varphi = \alpha^{-1}$ and $\varphi_V = \alpha_V^{-1}$. We know from (8.2.3.3) that $L' = \mathbf{Z} \cdot (1+i)\Omega + \mathbf{Z} \cdot 2\Omega \subseteq L_V$. On the other hand, our diagram together with 7.6.4 imply that $|L/L_V| = \deg(f) = 2 = |L/L'|$, hence $L' = L_V$.

**(8.3.6) The dual isogeny.** The duplication formula (7.5.8.2) and its derivative imply that the multiplication by 2 on $E(\mathbf{C})$ is given by

$$[2]_E(u,v) = \left( \left( \frac{u^2+1}{v} \right)^2, \frac{2(u^2+1)(u^4-6u^2+1)}{v^3} \right).$$

Define a map $\widehat{f} : E(\mathbf{C}) \longrightarrow V(\mathbf{C})$ by $\widehat{f}(O) = (0,1)$ and

$$\widehat{f}((u,v)) = \begin{cases} (x,y) = \left( -\frac{v}{u^2+1}, \frac{u^4-6u^2+1}{(u^2+1)^2} \right), & \text{if } u \neq \pm i \\ (x',y') = \left( -\frac{u^2+1}{v}, \frac{u^4-6u^2+1}{v^2} \right), & \text{if } v \neq 0. \end{cases}$$

The map $\widehat{f}$ is holomorphic (exercise!) and satisfies

$$f \circ \widehat{f} = [2]_E, \qquad \widehat{f} \circ f = [2]_V.$$

**(8.3.7) Exercise.** (i) *Show that the map $[1+i]_V : V(\mathbf{C}) \longrightarrow V(\mathbf{C})$ has the same kernel as $f$.*
(ii) *Show that there exists an isomorphism of Riemann surfaces $g : V(\mathbf{C}) \xrightarrow{\sim} E(\mathbf{C})$ such that $g \circ [1+i]_V = f$.*
(iii) *Find explicit formulas for $g$ and $g^{-1}$.*

**(8.3.8) Proposition.** *For each $k \geq 1$,*

$$G_{4k+2}(\mathbf{Z}[i]) = 0, \qquad G_{4k}(\mathbf{Z}[i]) = {\sum_{m,n \in \mathbf{Z}}}' \frac{1}{(m+ni)^{4k}} = c_k \cdot \Omega^{4k},$$

*where $c_k \in \mathbf{Q}$ is a (positive) rational number. For example, $c_1 = 1/15$.*

*Proof.* As $i\mathbf{Z}[i] = \mathbf{Z}[i]$, the last formula in 7.1.6 implies that

$$G_{4k+2}(\mathbf{Z}[i]) = G_{4k+2}(i\mathbf{Z}[i]) = i^{-4k-2} G_{4k+2}(\mathbf{Z}[i]) \implies G_{4k+2}(\mathbf{Z}[i]) = 0.$$

The Weierstrass function $\wp(z) = \wp(z;L)$ satisfies the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - 4\wp(z);$$

differentiating, we obtain

$$\wp''(z) = 6\wp(z)^2 - 2. \tag{8.3.8.1}$$

As

$$4 = g_2(L) = 60\, G_4(L) = 60\, G_4(\mathbf{Z}[i] \cdot \Omega),$$

it follows that

$$G_4(\mathbf{Z}[i]) = \Omega^4\, G_4(\mathbf{Z}[i] \cdot \Omega) = \frac{\Omega^4}{15}.$$

Substituting to (8.3.8.1) the Laurent series expansions

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (4k-1)\, G_{4k}(L) z^{4k-2}$$
$$\wp'(z)^2 = \frac{6}{z^4} + \sum_{k=1}^{\infty} (4k-1)(4k-2)(4k-3)\, G_{4k}(L) z^{4k-4}$$

and comparing the coefficients, we obtain, for each $k > 1$,

$$(4k-1)((4k-2)(4k-3) - 12)\, G_{4k}(L) = 6 \sum_{\substack{j+l=k \\ j,l \geq 1}} (4j-1)(4l-1)\, G_{4j}(L)\, G_{4l}(L),$$

hence

$$G_{4k}(\mathbf{Z}[i]) \cdot \Omega^{-4k} = G_{4k}(\mathbf{Z}[i] \cdot \Omega) = G_{4k}(L) \in \mathbf{Q}$$

is rational (and positive), by induction.

**(8.3.9) Exercise.** (i) *What is the analogue of 8.3.8 (and of its proof) if we replace $\sigma(z)$ by $\sin(z)$?*
(ii) *Compute the first few values of $c_k$. What can one say about the denominators of the numbers $(4k-1)!\cdot c_k$?*
(iii) *What is the analogue of (ii) in the context of (i)?*

## 8.4 The action of $\mathbf{Z}[i]$

**(8.4.1)** As $iL = L$ and $iL_V = L_V$, both $\mathbf{C}/L$ and $\mathbf{C}/L_V$ are $\mathbf{Z}[i]$-modules. Transporting this structure to $E(\mathbf{C})$ (resp. $V(\mathbf{C})$) by $\varphi$ (resp. $\varphi_V$), we obtain an action of $\mathbf{Z}[i]$ on $E(\mathbf{C})$ (resp. $V(\mathbf{C})$) given by

$$\begin{aligned} [\alpha]_E(\wp(z), \wp'(z)) &= (\wp(\alpha z), \wp'(\alpha z)) \\ [\alpha]_V(sl(z), sl'(z)) &= (sl(\alpha z), sl'(\alpha z)) \end{aligned} \qquad (\alpha \in \mathbf{Z}[i]).$$

The maps $f, \widehat{f}$ from 8.3.2,6 are then homomorphisms of $\mathbf{Z}[i]$-modules.

For example, the relations (7.1.6) and (8.2.3.1) imply that

$$\begin{aligned} [\pm i]_E(u,v) &= (-u, \pm iv), & [-1]_E(u,v) &= (u,-v) \\ [\pm i]_V(x,y) &= (\pm ix, y), & [-1]_V(x,y) &= (-x,y). \end{aligned} \tag{8.4.1.1}$$

Denoting the $\alpha$-torsion submodules by

$$\begin{aligned} E(\mathbf{C})_\alpha &= E(\mathbf{C})[\alpha] = \{P \in E(\mathbf{C}) \mid [\alpha]_E P = O\} \\ V(\mathbf{C})_\alpha &= V(\mathbf{C})[\alpha] = \{Q \in V(\mathbf{C}) \mid [\alpha]_V Q = (0,1)\}, \end{aligned}$$

then it follows from (8.4.1.1) that

$$E(\mathbf{C})[1+i] = \{O, (0,0)\}, \qquad V(\mathbf{C})[1+i] = \{(0, \pm 1)\}.$$

**(8.4.2) Group law on $V(\mathbf{C})$.** The addition formula (1.4.5.1) (whose more general form was proved in 2.3.1) can be written as

$$sl(z_1+z_2)=\frac{sl(z_1)sl'(z_2)+sl'(z_1)sl(z_2)}{1+sl^2(z_1)sl^2(z_2)}. \tag{8.4.2.1}$$

Differentiating (8.4.2.1) with respect to $z_1$, we obtain an explicit formula for the group law $\boxplus$ on $V(\mathbf{C})$:

$$(x_1,y_1)\boxplus(x_2,y_2)=\left(\frac{x_1y_2+x_2y_1}{1+x_1^2x_2^2},\frac{y_1y_2(1-x_1^2x_2^2)-2x_1x_2(x_1^2+x_2^2)}{(1+x_1^2x_2^2)^2}\right). \tag{8.4.2.2}$$

Above, $(x_j,y_j)=(sl(z_j),sl'(z_j))\in V_{\mathrm{aff}}(\mathbf{C})$.

Multiplying together the formulas (8.4.2.1) for $\pm z_2$, we obtain

$$sl(z_1+z_2)sl(z_1-z_2)=\frac{x_1^2y_2^2-x_2^2y_1^2}{(1+x_1^2x_2^2)^2}=\frac{x_1^2(1-x_2^4)-x_2^2(1-x_1^4)}{(1+x_1^2x_2^2)^2}=\frac{x_1^2-x_2^2}{1+x_1^2x_2^2}=\frac{sl^2(z_1)-sl^2(z_2)}{1+sl^2(z_1)sl^2(z_2)}. \tag{8.4.2.3}$$

**(8.4.3) Exercise.** *Show that, for $(x,y)\in V_{\mathrm{aff}}(\mathbf{C})$,*

$$(x,y)\boxplus O_\pm=\left(\pm\frac{i}{x},\mp iyx^2\right).$$

*[Hint: Rewrite (8.4.2.2) in the variables $x',y'$.]*

**(8.4.4) Examples.** Combining (8.4.1.1) with (8.4.2.2), we recover Fagnano's formulas from 1.4.3-4:

$$\begin{aligned}[1\pm i](x,y)=(x,y)\boxplus(\pm ix,y)&=\left(\frac{(1\pm i)x}{y},\frac{1+x^4}{y^2}\right)=\left(\frac{(1\pm i)x}{y},\frac{1+x^4}{1-x^4}\right)\\ [2](x,y)=(x,y)\boxplus(x,y)&=\left(\frac{2xy}{1+x^4},\frac{1-6x^4+x^8}{(1+x^4)^2}\right),\end{aligned} \tag{8.4.4.1}$$

where $(x,y)\in V_{\mathrm{aff}}(\mathbf{C})$ (i.e. $y^2=1-x^4$).

Note that $sl'(\alpha z)$ can be obtained from $sl(\alpha z)$ by differentiation. If $(x,y)=(sl(z),sl'(z))$, then

$$[\alpha](x,y)=(x_\alpha,y_\alpha)=(sl(\alpha z),sl'(\alpha z)),$$

where $x_\alpha,y_\alpha$ are rational functions of $x,y$ with coefficients in $\mathbf{Q}(i)$, satisfying

$$dx_\alpha=\alpha\,sl'(\alpha z)\,dz=\alpha\,y_\alpha\,dz,\qquad dx=sl'(z)\,dz=y\,dz,$$

hence

$$y_\alpha\frac{dx}{y}=\frac{1}{\alpha}\,dx_\alpha. \tag{8.4.4.2}$$

This means that one can obtain $y_\alpha$ from $x_\alpha$ by a very simple calculation.

For example, for $\alpha=1+i$, we have $x_{1+i}=(1+i)x/y$. Combining (8.4.4.2) with

$$d(x^4+y^2-1)=0\Longrightarrow 4x^3\,dx+2y\,dy=0\Longrightarrow dy=-2x^3/y\,dx,$$

we obtain

$$\frac{dx_{1+i}}{1+i}=\frac{dx}{y}-\frac{x\,dy}{y^2}=\frac{dx}{y}\left(\frac{y^2+2x^4}{y^2}\right),$$

hence

$$y_{1+i}=\frac{y^2+2x^4}{y^2}=\frac{1+x^4}{y^2},$$

in line with (8.4.4.1).

**(8.4.5) Examples (continued).** Let us compute

$$[1+2i](x,y) = [i](x,y) \boxplus [1+i](x,y) = (ix,y) \boxplus \left(\frac{(1+i)x}{y}, \frac{1+x^4}{1-x^4}\right) = (x_{1+2i}, y_{1+2i}).$$

As

$$x_{1+2i} = \frac{\frac{ix(1+x^4)}{1-x^4} + (1+i)x}{1 - \frac{2ix^4}{1-x^4}} = \frac{(1+2i)x - x^5}{1-(1+2i)x^4} = \frac{(1+2i) - x^4}{1-(1+2i)x^4}\, x, \tag{8.4.5.1}$$

it follows from (8.4.4.2) that

$$y_{1+2i}\,\frac{dx}{y} = \frac{dx_{1+2i}}{1+2i} = \frac{1-(1-2i)x^4}{1-(1+2i)x^4}\,dx + \frac{(1+2i)x - x^5}{(1-(1+2i)x^4)^2}\,4x^3dx = \frac{1+(2+8i)x^4+x^8}{(1-(1+2i)x^4)^2}\,dx,$$

hence

$$y_{1+2i} = \frac{1+(2+8i)x^4+x^8}{(1-(1+2i)x^4)^2}\,y. \tag{8.4.5.2}$$

In the similar vein,

$$[3](x,y) = (x,y) \boxplus \left(\frac{2xy}{1+x^4}, \frac{1-6x^4+x^8}{(1+x^4)^2}\right) = (x_3, y_3),$$

where

$$x_3 = \frac{\frac{x(1-6x^4+x^8)}{(1+x^4)^2} + \frac{2x(1-x^4)}{1+x^4}}{1 + \frac{4x^4(1-x^4)}{(1+x^4)^2}} = \frac{3-6x^4-x^8}{1+6x^4-3x^8}\,x \tag{8.4.5.3}$$

and

$$y_3\,\frac{dx}{y} = \frac{dx_3}{3} = \frac{1-10x^4-3x^8}{1+6x^4-3x^8}\,dx - \frac{(3-6x^4-x^8)(8x^4-8x^8)}{(1+6x^4-3x^8)^2}\,dx = \frac{1-28x^4+6x^8-28x^{12}+x^{16}}{(1+6x^4-3x^8)^2}\,dx,$$

hence

$$y_3 = \frac{1-28x^4+6x^8-28x^{12}+x^{16}}{(1+6x^4-3x^8)^2}\,y. \tag{8.4.5.4}$$

**(8.4.6) A change of sign.** The formulas (8.4.5.1-4) become more symmetric if we apply $[-1](x,y) = (-x,y)$:

$$[-1-2i]\,(x,y) = \left(\frac{x^4-(1+2i)}{1-(1+2i)x^4}\,x,\ \frac{1+(2+8i)x^4+x^8}{(1-(1+2i)x^4)^2}\,y\right) \tag{8.4.6.1}$$

$$[-3]\,(x,y) = \left(\frac{x^8+6x^4-3}{1+6x^4-3x^8}\,x,\ \frac{1-28x^4+6x^8-28x^{12}+x^{16}}{(1+6x^4-3x^8)^2}\,y\right). \tag{8.4.6.2}$$

**(8.4.7) Congruences.** Note that

$$1+(2+8i)x^4+x^8 \equiv (1-x^4)^2 \equiv y^4 \pmod{(-1-2i)},$$
$$1-28x^4+6x^8-28x^{12}+x^{16} \equiv (1-x^4)^4 \equiv y^8 \pmod{(-3)};$$

the formulas (8.4.6.1-2) then imply that

$$\begin{aligned}[-1-2i]\,(x,y) &\equiv (x^5,y^5)\ (\mathrm{mod}\,(-1-2i)),\\ [-3]\,(x,y) &\equiv (x^9,y^9)\ (\mathrm{mod}\,(-3)).\end{aligned} \tag{8.4.7.1}$$

These congruences should be interpreted as follows: $\alpha=-1-2i$ (resp. $\alpha=-3$) is an irreducible element of $\mathbf{Z}[i]$ of norm $N\alpha=\alpha\overline{\alpha}=5$ (resp. $N\alpha=9$) and both components $x_\alpha, y_\alpha$ of $[\alpha](x,y)$ are elements of the localization $R_{(\alpha)}$ of the polynomial ring $R=\mathbf{Z}[i][x,y]$ at the prime ideal generated by $\alpha$; it makes sense, therefore, to consider the residue classes of $x_\alpha, y_\alpha$ modulo $\alpha R_{(\alpha)}$ as elements of the residue field of $R_{(\alpha)}$, which is equal to

$$R_{(\alpha)}/\alpha R_{(\alpha)} = \mathrm{Frac}(k(\alpha)[x,y]) = k(\alpha)(x,y),$$

i.e. to the field of rational functions in $x,y$ over the finite field $k(\alpha)=\mathbf{Z}[i]/\alpha\mathbf{Z}[i]$ with $N\alpha$ elements.

**(8.4.8) Making a Conjecture.** What is the general form of (8.4.7.1)? What distinguishes the values $\alpha=-1-2i,-3$ from $1+2i,3$, for which we have

$$\begin{aligned}[1+2i]\,(x,y) &\equiv (-x^5,y^5)\ (\mathrm{mod}\,(1+2i)),\\ [3]\,(x,y) &\equiv (-x^9,y^9)\ (\mathrm{mod}\,(3))?\end{aligned} \tag{8.4.7.1}$$

Recall that the cogruences 0.5.1

$$[p^*]_C(x,y) \equiv (x^p,y^p)\ (\mathrm{mod}\,p) \tag{8.4.7.2}$$

for the group law on the circle involved multiplication by

$$p^* = (-1)^{(p-1)/2}p, \tag{8.4.7.3}$$

for odd prime numbers $p$. As

$$p^* \equiv 1\ (\mathrm{mod}\,4),$$

it is natural to ask whether there is a similar congruence condition characterizing $\alpha=-1-2i,-3\in\mathbf{Z}[i]$. In these two cases

$$\alpha-1=\begin{cases}(-1-2i)-1=-2-2i=(-1)(2+2i),\\ (-3)-1=-4=(-1+i)(2+2i),\end{cases}$$

which would suggest the following

**(8.4.9) Conjecture.** *If $\alpha\in\mathbf{Z}[i]$ is an irreducible element satisfying $\alpha\equiv 1\ (\mathrm{mod}\,(2+2i))$, then*

$$[\alpha](x,y)\equiv(x^{N\alpha},y^{N\alpha})\ (\mathrm{mod}\,\alpha),$$

*where $N\alpha=\alpha\overline{\alpha}$.*

**(8.4.10) What are these congruences good for?** In the case of the circle, the quantity (8.4.7.3) appears in the statement (and various proofs) of the *Quadratic Reciprocity Law*. In fact, as we shall see in 9.2 below, the congruence (8.4.7.2) can be used to *prove* the Quadratic Reciprocity Law.

Assuming that 8.4.9 holds, can one deduce from it a more general Reciprocity Law – perhaps for higher powers – involving elements of $\mathbf{Z}[i]$? We shall investigate this question in section 9.

## 8.5 Division of the lemniscate

**(8.5.1)** Algebraic properties of the numbers $\sin(\pi a/n)$ are intimately linked to geometry of regular polygons. Their lemniscatic counterparts $sl(a\Omega/n)$ are the polar coordinates of the points that divide the right half-lemniscate into $n$ arcs of equal length $\Omega/n$.

Note that, if $0 < a < n$, then

$$0 < sl(a\Omega/n) < 1, \qquad sgn(sl'(a\Omega/n)) = sgn(a - n/2). \tag{8.5.1.1}$$

**(8.5.2) Examples.** $(n = 3)$: let $(x, y) = (sl(\Omega/3), sl'(\Omega/3)) \in V(\mathbf{R})$. As

$$[3](x, y) = (sl(\Omega), sl'(\Omega)) = (0, -1),$$

the triplication formula (8.4.5.3) implies that $x$ is a root of

$$x^8 + 6x^4 - 3 = 0;$$

the only root of this equation contained in the interval $(0, 1)$ is $x = \sqrt[4]{2\sqrt{3} - 3}$; applying (8.5.1.1) once again we see that $y = \sqrt{1 - x^4}$ is the positive square root; thus

$$(sl(\Omega/3), sl'(\Omega/3)) = (\sqrt[4]{2\sqrt{3} - 3}, \sqrt{3} - 1). \tag{8.5.2.1}$$

The values (8.5.2.1) can also be deduced from Fagnano's duplication formula, as

$$[2](a, b) = (sl(\Omega - \Omega/3), sl'(\Omega - \Omega/3)) = (a, -b).$$

$(n = 4)$: The point $(x, y) = (sl(\Omega/4), sl'(\Omega/4))$ satisfies

$$[2](x, y) = (sl(\Omega/2), sl'(\Omega/2)) = (1, 0),$$

hence the duplication formula for $sl'$ (8.4.4.1) implies that $x$ is a root of

$$x^8 - 6x^4 + 1 = 0.$$

As in the case $n = 3$, there is precisely one root contained in the interval $(0, 1)$, which is easily calculated. The final result is

$$(sl(\Omega/4), sl'(\Omega/4)) = (\sqrt{\sqrt{2} - 1}, \sqrt{2\sqrt{2} - 2}). \tag{8.5.2.2}$$

**(8.5.3) Constructibility.** The attentive reader will have noticed that all values occurring in (8.5.2.1-2) involve only iterated square roots of rational numbers. Such expressions are precisely the 'constructible' numbers in the sense of Euclidean geometry, i.e. those equal to distances between points obtained by iterated intersections of lines and circles, starting from a segment of unit length.

The corresponding elementary counterparts of 8.5.2.1-2, namely the numbers

$$\sin(\pi/3) = \sqrt{3}/2, \qquad \sin(\pi/4) = \sqrt{2}/2,$$

are constructible for the simple reason that for the small values $n = 3, 4$ the regular $n$-gon is constructible.

**(8.5.4) Exercise.** (i) *Let $P = (a, b)$ $(a \geq 0)$ be a point on the lemniscate. Show that:*

$$\text{the two numbers } a, b \text{ are constructible } \iff r = \sqrt{a^2 + b^2} \text{ is constructible.}$$

*Of course, $r = sl(s)$, where $s$ is the length of the arc of the lemniscate from $(0, 0)$ to $P$; cf. 1.3.1.*
(ii) *$sl(s)$ is constructible $\iff$ $sl(2s)$ is constructible.*
(iii) *For each $m \geq 0$, the points dividing the half-lemniscate into $n = 2^m$ (resp. $n = 3 \cdot 2^m$) arcs of equal length $\Omega/n$ are all constructible.*
(iv) *What about the case $n = 5$? (Note that the regular pentagon is constructible, as $\cos(2\pi/5) = (\sqrt{5} - 1)/2$.) [Hint: $\Omega/(1 + 2i) + \Omega/(1 - 2i) = 2\Omega/5$; use (8.4.5.1-2).]*

## 9. Lemniscatology continued: Reciprocity Laws [1]

### 9.1 Quadratic Reciprocity Law

**(9.1.1)** Irreducible quadratic polynomials

$$f(x) = ax^2 + bx + c \qquad\qquad (a, b, c \in \mathbf{Z}, a \neq 0)$$

with integral coefficients have the following remarkable property: only 50 % of prime numbers appear in the factorization of the values $f(x)$ ($x \in \mathbf{Z}$); such prime numbers are characterized by suitable congruence conditions modulo $|b^2 - 4ac|$.

For example, the prime numbers $p \neq 2$ (resp. $p \neq 2, 3$) occurring as factors of the numbers of the form $x^2 + 1$ (resp. $x^2 + 3$) are precisely the prime numbers $p \equiv 1 \pmod 4$ (resp. $p \equiv 1 \pmod 3$).

By completing the square

$$4af(x) = (2ax + b)^2 - (b^2 - 4ac),$$

it is enough to consider the polynomials $f(x) = x^2 - a$; the answer can then be formulated in terms of the Legendre symbol.

**(9.1.2) The Legendre symbol.** If $a \in \mathbf{Z}$ and $p$ is a prime number not dividing $2a$, one defines

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & (\exists x \in \mathbf{Z}) \;\; x^2 \equiv a \pmod p \\ -1, & (\forall x \in \mathbf{Z}) \;\; x^2 \not\equiv a \pmod p. \end{cases}$$

The multiplicative group $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic of order $p - 1$; this implies that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p \tag{9.1.2.1}$$

("**Euler's criterion**"). In other words, the Legendre symbol induces an isomorphism of abelian groups

$$\mathbf{F}_p^*/\mathbf{F}_p^{*2} \xrightarrow{\sim} \{\pm 1\}, \qquad a \mapsto \left(\frac{a}{p}\right).$$

In particular,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{9.1.2.2}$$

and

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases} \tag{9.1.2.3}$$

**(9.1.3) Lemma (Gauss).** *Let $q \neq 2$ be a prime number; fix a subset $\Sigma \subset \mathbf{Z}/q\mathbf{Z} - \{0\}$ such that $\mathbf{Z}/q\mathbf{Z} - \{0\} = \Sigma \dot\cup (-\Sigma)$ (disjoint union). For example, we can take $\Sigma = \{1, 2, \ldots, (q-1)/2\}$. Fix an integer $a \in \mathbf{Z}$, $q \nmid a$. For each $\sigma \in \Sigma$ there is a unique pair $\epsilon_\sigma = \pm 1$ and $\sigma' \in \Sigma$ satisfying $a\sigma = \epsilon_\sigma \sigma' \in (\mathbf{Z}/q\mathbf{Z})^*$; then*

$$\prod_{\sigma \in \Sigma} \epsilon_\sigma = \left(\frac{a}{q}\right).$$

*Proof.* Dividing both sides of the equality

$$a^{\frac{q-1}{2}} \prod_{\sigma \in \Sigma} \sigma = \prod_{\sigma \in \Sigma} (a\sigma) = \left(\prod_{\sigma \in \Sigma} \epsilon_\sigma\right) \prod_{\sigma' \in \Sigma} \sigma' \in (\mathbf{Z}/q\mathbf{Z})^*$$

[1] Section 9 is not for examination.

by

$$\prod_{\sigma\in\Sigma}\sigma \in (\mathbf{Z}/q\mathbf{Z})^*$$

yields the result.

**(9.1.4) Exercise.** *Applying 9.1.3 to $a = 2$, show that*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

**(9.1.5) Quadratic Reciprocity Law.** *Let $p \neq q$ be prime numbers, $p, q \neq 2$. Then*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

**(9.1.6)** Using (9.1.2.1-2), the Quadratic Reciprocity Law can also be written as

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right), \qquad p^* = (-1)^{\frac{p-1}{2}}p.$$

**(9.1.7)** Let $a \in \mathbf{Z} - \{0, 1\}$ be a square-free integer. Writing $a$ in the form

$$a = (-1)^u 2^v p_1^* \cdots p_w^*, \qquad p_j^* = (-1)^{\frac{p_j-1}{2}}p_j,$$

where $u, v \in \{0, 1\}$ and $p_j$ are distinct odd primes, the Quadratic Reciprocity Law implies that we have, for each prime $q \nmid 2|a|$,

$$\left(\frac{a}{q}\right) = \left(\frac{-1}{q}\right)^u \left(\frac{2}{q}\right)^v \left(\frac{q}{p_1}\right)\cdots\left(\frac{q}{p_w}\right). \tag{9.1.7.1}$$

As the value of $\left(\frac{q}{p_j}\right)$ (resp. $\left(\frac{-1}{q}\right)$, resp. $\left(\frac{2}{q}\right)$) depends only on the residue class of $q$ modulo $p_j$ (resp. modulo 4, resp. modulo 8), it follows from (9.1.7.1) that $\left(\frac{a}{q}\right)$ depends only on the residue class of $q$ modulo $A$, where

$$A = \begin{cases} |a|, & a \equiv 1 \pmod 4 \\ 4|a|, & a \not\equiv 1 \pmod 4. \end{cases} \tag{9.1.7.2}$$

Moreover, if $q_j$ $(j = 1, 2, 3)$ are primes not dividing $2|a|$ satisfying

$$q_1 q_2 \equiv q_3 \pmod A,$$

then (9.1.7.1) together with (9.1.2.2-3) and 9.1.4 imply that

$$\left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right) = \left(\frac{a}{q_3}\right).$$

As each congruence class in $(\mathbf{Z}/A\mathbf{Z})^*$ contains a prime number, the previous discussion implies the following result.

**(9.1.8) Proposition.** *If $a \in \mathbf{Z} - \{0,1\}$ is a square-free integer and $A$ is defined by (9.1.7.2), then there exists a unique surjective homomorphism of abelian groups*

$$\chi_a : (\mathbf{Z}/A\mathbf{Z})^* \longrightarrow \{\pm 1\}$$

*satisfying*

$$\chi_a(q \pmod A) = \left(\frac{a}{q}\right)$$

*for all prime numbers $q \nmid 2|a|$.*

**(9.1.9) Example:** For $a = 3 = (-1)\cdot(-3) = (-1)\cdot 3^*$,

$$\left(\frac{3}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{q}{3}\right) = \begin{cases} +1, & q \equiv \pm 1 \pmod{12} \\ -1, & q \equiv \pm 5 \pmod{12} \end{cases}$$

for every prime $q \neq 2, 3$.

**(9.1.10)** If $a = p^*$, where $p \neq 2$ is a prime number, then $A = p$. There is only one surjective homomorphism

$$(\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \{\pm 1\},$$

namely the Legendre symbol; thus 9.1.8 implies that

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

for all primes $q \neq 2, p$. In other words, 9.1.8 is a strengthening of the Quadratic Reciprocity Law.

## 9.2 Quadratic Reciprocity Law and $\sin(z)$

In this section we deduce the Quadratic Reciprocity Law from the congruence 0.5.1 (cf. 9.2.3 below) and the following simple product formula.

**(9.2.1) Proposition (Product Formula (P)).** *Let $n \in \mathbf{N}$, $2 \nmid n$. Fix a subset $\Sigma \subset \mathbf{Z}/n\mathbf{Z} - \{0\}$ such that $\mathbf{Z}/n\mathbf{Z} - \{0\} = \Sigma \dot\cup (-\Sigma)$ (disjoint union). Then*

$$\left(\prod_{\sigma\in\Sigma} 2\sin\frac{2\pi\sigma}{n}\right)^2 = n. \tag{P}$$

*Proof.* The addition formulas for $\sin(z)$ imply that

$$\begin{aligned} \sin(z_1+z_2) + \sin(z_1-z_2) &= 2\sin(z_1)\cos(z_2) \\ \sin(z_1+z_2)\cdot\sin(z_1-z_2) &= \sin^2(z_1) - \sin^2(z_2). \end{aligned}$$

Putting $z_1 = (n-2)z$ and $z_2 = 2z$ (thus $\cos(z_2) = 1 - 2\sin^2(z)$), it follows by induction that, for every $n \in \mathbf{N}$, $2 \nmid n$, there is a polynomial $Q_n(t) \in \mathbf{Z}[t]$ satisfying

$$\sin(nz) = Q_n(\sin(z)), \qquad Q_n(t) = (-1)^{\frac{n-1}{2}} 2^{n-1} t^n + \cdots + nt. \tag{9.2.1.1}$$

As the values of $\sin(z)$ at $z \in \frac{2\pi}{n}\mathbf{Z}$ are all roots of $Q_n$, we obtain from (9.2.1.1) that

$$Q_n(t) = t\prod_{\sigma\in\Sigma} 2^2\left(\sin\frac{2\pi\sigma}{n} - t\right)\left(\sin\frac{2\pi\sigma}{n} + t\right). \tag{9.2.1.2}$$

Putting $t = 0$ (and again using (9.2.1.1)) yields the product formula (P).

**(9.2.2) Lemma.** *If $n \in \mathbf{N}$, $2 \nmid n$ and $a \in \mathbf{Z}$, then $2^{n-1} \sin \frac{2\pi a}{n}$ is an algebraic integer. [In fact, one can replace in this statement $2^{n-1}$ by 2, but this is not important for what follows.]*

*Proof.* This follows from (9.2.1.1-2).

**(9.2.3) Proposition (Congruence Formula (C)).** *Let $p \neq 2$ be a prime. Then*

$$Q_p(t) \equiv (-1)^{\frac{p-1}{2}} t^p \pmod{p\mathbf{Z}[t]}. \tag{C}$$

*Proof.* As $\sin(-z) = -\sin(z)$, the polynomial $Q_p(t)$ is an odd function, hence of the form $Q_p(t) = tM(t^2)$, with $M(t) \in \mathbf{Z}[t]$. As

$$\cos(pz) = \sin(\tfrac{\pi}{2} - pz) = (-1)^{\frac{p-1}{2}} \sin(p(\tfrac{\pi}{2} - z)) = (-1)^{\frac{p-1}{2}} Q_p(\sin(\tfrac{\pi}{2} - z)) = (-1)^{\frac{p-1}{2}} Q_p(\cos(z)), \tag{9.2.3.1}$$

differentiating the relation $\sin(pz) = Q_p(\sin(z))$ we obtain

$$p(-1)^{\frac{p-1}{2}} Q_p(\cos(z)) = p\cos(pz) = Q_p'(\sin(z))\cos(z),$$

hence

$$\begin{aligned} Q_p'(\sin(z)) &= p(-1)^{\frac{p-1}{2}} M(\cos(z)^2), \\ Q_p'(t) &= p(-1)^{\frac{p-1}{2}} M(1-t^2) \in p\mathbf{Z}[t] \end{aligned} \tag{9.2.3.2}$$

As $Q_p(t) = \sum a_i t^i$ is a polynomial of degree $p$ with integral coefficients, the congruence (9.2.3.2) implies that

$$Q_p(t) \equiv a_p t^p \pmod{p\mathbf{Z}[t]}.$$

However,

$$a_p = (-1)^{\frac{p-1}{2}} 2^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

by (9.2.1.1).

**(9.2.4) Corollary.** *Assume that $\sin(\alpha) \in \overline{\mathbf{Q}}$ is an algebraic number ($\alpha \in \mathbf{C}$) and $\mathcal{O}$ a subring of $\overline{\mathbf{Q}}$ containing $\sin(\alpha)$. If $p \neq 2$ is a prime number, then $\sin(p^*\alpha) \in \mathcal{O}$ and*

$$\sin(p^*\alpha) \equiv \sin(\alpha)^p \pmod{p\mathcal{O}} \qquad\qquad (p^* = (-1)^{\frac{p-1}{2}} p).$$

**(9.2.5) Corollary.** *Let $p \neq 2$ be a prime number and $n \in \mathbf{N}$, $(n, 2p) = 1$. Let $\mathcal{O}_{K_n}$ be the ring of algebraic integers in the field $K_n = \mathbf{Q}(\sin \frac{2\pi a}{n} \mid a \in \mathbf{Z}/n\mathbf{Z})$. Then, for each $a \in \mathbf{Z}$,*

$$\sin\left(\frac{2\pi p^* a}{n}\right) \equiv \left(\sin \frac{2\pi a}{n}\right)^p \pmod{p\mathcal{O}_{K_n}[1/2]}.$$

**(9.2.6)** The congruence 0.5.1

$$[p^*](x, y) \equiv (x^p, y^p) \pmod{p\mathbf{Z}[x, y]}$$

is a simple combination of 9.2.3 with (9.2.3.1). This method of proof is much more complicated then the one suggested in 0.5.1, but it can be generalized (at least partially) to the lemniscatic case, as we shall see in 9.4 below.

**(9.2.7)** In fact, one can deduce the Congruence Formula (C) directly from the Product Formula (P), with a little help from algebraic number theory:

**(9.2.8) Proposition.** *Let $p \neq 2$ be a prime. Then the polynomial $R_p(t) = (-1)^{\frac{p-1}{2}} Q_p(t)/t \in \mathbf{Z}[t]$ satisfies*

$$R_p(t) \equiv t^{p-1} \pmod{p\mathbf{Z}[t]}.$$

*Proof.* By (9.2.1.2) and 9.2.2, we have

$$R_p(t) = 2^{p-1} \prod_{r=1}^{p-1} (t - \alpha_r), \qquad \alpha_r = \sin \frac{2\pi r}{p} \in \mathcal{O}_{K_p}[1/2].$$

The Product Formula (P) from 9.2.1

$$R_p(0) = 2^{p-1} \prod_{r=1}^{p-1} \alpha_r = p$$

implies that there exists a prime ideal $\mathfrak{p}|p$ in $\mathcal{O}_{K_p}$ and an index $1 \leq r_0 \leq p-1$ such that $\mathfrak{p}|\alpha_{r_0}$. For each $r \in (\mathbf{Z}/p\mathbf{Z})^*$ there exists $s \in \mathbf{N}$ satisfying $2 \nmid s$ and $t \equiv r_0 s \pmod{p}$. Then

$$\alpha_r = Q_s(\alpha_{r_0}), \qquad Q_s(t) \in \mathbf{Z}[t], \qquad Q_s(0) = 0 \implies \mathfrak{p}|\alpha_r.$$

This means that $\mathfrak{p}$ divides all $\alpha_r$, hence

$$R_p(t) \equiv 2^{p-1} t^{p-1} \pmod{\mathfrak{p}\mathcal{O}_{K_p}[1/2][t]}.$$

As $R_p(t) \in \mathbf{Z}[t]$, we conclude that

$$R_p(t) \equiv 2^{p-1} t^{p-1} \equiv t^{p-1} \pmod{p\mathbf{Z}[t]}.$$

**(9.2.9) Deducing Quadratic Reciprocity Law from (P), (C) and 9.1.3.** We are now ready to prove 9.1.6. Fix $\Sigma$ as in 9.1.3 and put

$$S = \prod_{\sigma \in \Sigma} \left( 2 \sin \frac{2\pi q}{q} \right), \qquad S' = \prod_{\sigma \in \Sigma} \left( 2 \sin \frac{2\pi p^* q}{q} \right) \in \mathcal{O}_{K_q}[1/2].$$

Applying 9.1.3 with $a = p^*$ and using the identity $\sin(-z) = -\sin(z)$, we obtain

$$S' = \prod_{\sigma \in \Sigma} \left( 2 \sin \frac{2\pi \epsilon_\sigma \sigma'}{q} \right) = \prod_{\sigma \in \Sigma} \left( 2\epsilon_\sigma \sin \frac{2\pi \sigma'}{q} \right) = \left( \prod_{\sigma \in \Sigma} \epsilon_\sigma \right) \prod_{\sigma' \in \Sigma} \left( 2 \sin \frac{2\pi \sigma'}{q} \right) = \left( \frac{p^*}{q} \right) S. \tag{9.2.9.1}$$

Combined with (C) in the form 9.2.5, this yields

$$\left( \frac{p^*}{q} \right) S = S' \equiv (2^{\frac{1-q}{2}})^{p-1} S^p \equiv S^p \pmod{p\mathcal{O}_{K_q}[1/2]}. \tag{9.2.9.2}$$

According to (P), we have $S^2 = q$; as $q$ is invertible in $\mathbf{Z}/p\mathbf{Z} \subset \mathcal{O}_{K_q}/p\mathcal{O}_{K_q} = \mathcal{O}_{K_q}[1/2]/p\mathcal{O}_{K_q}[1/2]$, it follows that we can divide (9.2.9.2) by $S$, obtaining (again using (P))

$$\left( \frac{p^*}{q} \right) \equiv S^{p-1} = (S^2)^{\frac{p-1}{2}} = q^{\frac{p-1}{2}} \pmod{p\mathcal{O}_{K_q}[1/2]}. \tag{9.2.9.3}$$

Applying Euler's criterion (9.1.2.1), we obtain from (9.2.9.3)

$$\left( \frac{p^*}{q} \right) \equiv \left( \frac{q}{p} \right) \pmod{p\mathcal{O}_{K_q}[1/2]} \implies \left( \frac{p^*}{q} \right) \equiv \left( \frac{q}{p} \right) \pmod{p\mathbf{Z}} \tag{9.2.9.4}$$

(as both sides are equal to $\pm 1$ and $\mathcal{O}_{K_q} \cap \mathbf{Q} = \mathbf{Z}$). Finally, the congruence (9.2.9.4) between elements of $\{\pm 1\}$ must be an equality, since $-1 \not\equiv 1 \pmod{p\mathbf{Z}}$.

**(9.2.10) Exercise.** *Using the values* $S = 2\sin\frac{2\pi}{8}$ *and* $S' = 2\sin\frac{2\pi p^*}{8}$, *show that*

$$\left(\frac{2}{p}\right) = \frac{S'}{S} = (-1)^{\frac{p^*-1}{4}} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8). \end{cases}$$

Conjecture 8.4.9 was stated and proved by Eisenstein in 1850

**(9.2.11) What next?** Is there a lemniscatic version of all that has been done in 9.1-2? Yes, there is. In fact, the congruence 8.4.9 was proved by Eisenstein in 1850 in order to deduce from it the Biquadratic Reciprocity Law ([Sc]).

**If Eisenstein could do it, why not you?**

The impatient readers may go straight away to sections 9.3-5. Others may want to pause and think about generalizing everything from 9.1-2 to the lemniscatic case, replacing $\mathbf{Z}, 2\pi$ and $\sin(z)$ by $\mathbf{Z}[i], \Omega$ and $sl(z)$, respectively. They would not regret this adventure!

### 9.3 The Product Formula for $sl(z)$

We follow the notation of Section 8 (in particular, $L = \mathbf{Z}[i] \cdot \Omega$).

**(9.3.1) Definition.** *Let $\alpha \in \mathbf{Z}[i]$, $2 \nmid N\alpha$. Fix a subset $\Sigma_\alpha \subset \left(\frac{1}{\alpha}L/L\right) - \{0\}$ satisfying $\left(\frac{1}{\alpha}L/L\right) - \{0\} = \Sigma_\alpha \dot\cup (i\Sigma_\alpha) \dot\cup (-\Sigma_\alpha) \dot\cup (-i\Sigma_\alpha)$ (thus $|\Sigma_\alpha| = (N\alpha - 1)/4$) and put*

$$P_\alpha(t) = \prod_{u \in \frac{1}{\alpha}L/L} (t - sl(u)) = t \prod_{u \in \Sigma_\alpha} (t^4 - sl^4(u)) \in \mathbf{C}[t]$$

$$Q_\alpha(t) = \prod_{u \in \left(\frac{1}{\alpha}L/L\right) - \{0\}} (1 - t\, sl(u)) = \prod_{u \in \Sigma_\alpha} (1 - t^4 sl^4(u)) \in \mathbf{C}[t]$$

*(the values of $sl(z)$ at $z = u \in \frac{1}{\alpha}L/L$ are finite, by 9.3.5 below). Note that*

$$Q_\alpha(t) = t^{N\alpha} P_\alpha(1/t). \tag{9.3.1.1}$$

**(9.3.2) Lemma.** *For each $\alpha \in \mathbf{Z}[i]$, $2 \nmid N\alpha$, we have*

$$Q_\alpha(sl(z + \tfrac{1\pm i}{2}\Omega)) = \frac{P_\alpha(sl(z))}{sl(z)^{N\alpha}}$$

*Proof.* This follows from 8.4.3, which reads as follows:

$$sl(z + \tfrac{1\pm i}{2}\Omega) = \frac{\mp i}{sl(z)} \tag{9.3.2.1}$$

**(9.3.3) Exercise.** *For $z_1, z_2 \in \mathbf{C}$,*

$$sl(z_1) = sl(z_2) \iff z_1 - z_2 \in L_V \text{ or } z_1 + z_2 \in L_V + \Omega$$

*(note that $L = L_V \dot\cup (L_V + \Omega)$).*

**(9.3.4) Lemma.** *If $\alpha, \beta \in \mathbf{Z}[i]$ and $2 \nmid (N\alpha)(N\beta)$, then $(P_\alpha(t), Q_\beta(t)) = 1$ (i.e. $P_\alpha(t)$ and $Q_\beta(t)$ have no common roots).*

*Proof.* If there were a common root, we would have $P_\alpha(sl(z)) = Q_\beta(sl(z)) = 0$ for some $z \in \mathbf{C}$. This would imply, by 9.3.2-3, that

$$z \in \frac{1}{\alpha}L/L \cap \left(\frac{1}{\beta}L + \frac{1 \pm i}{2}\Omega\right) \Longrightarrow \beta L \cap \left(\alpha L + \frac{\alpha\beta(1 \pm i)}{2}\Omega\right) \neq \emptyset \Longrightarrow \frac{\alpha\beta(1 \pm i)}{2}\Omega \in L = \mathbf{Z}[i] \cdot \Omega,$$

hence $\alpha\beta \in (1 + i)\mathbf{Z}[i]$, which contradicts the assumption $2 \nmid (N\alpha)(N\beta)$.

**(9.3.5) Lemma.** $\operatorname{div}(sl(z)) = (0) + (\Omega) - (\frac{1+i}{2}) - (\frac{1-i}{2}) \in \operatorname{Div}(\mathbf{C}/L_V)$.

*Proof.* This follows from the fact that

$$\operatorname{div}(x) = ((0,1)) + ((0,-1)) - (O_+) - (O_-) \in \operatorname{Div}(V(\mathbf{C})).$$

**(9.3.6) Corollary.** *The function $sl : \mathbf{C} \longrightarrow \mathbf{P}^1(\mathbf{C})$ has simple zeros (resp. simple poles) at $z \in L = L_V \dot\cup (L_V + \Omega)$ (resp. at $z \in L + \frac{1+i}{2}$) and no other zeros (resp. poles).*

**(9.3.7) Proposition.** *Let $\alpha \in \mathbf{Z}[i]$, $2 \nmid N\alpha$. Then there exists a (unique) constant $c_\alpha \in \mathbf{C}^*$ such that*

$$sl(\alpha z) = \frac{P_\alpha(sl(z))}{c_\alpha Q_\alpha(sl(z))} \qquad (z \in \mathbf{C}). \tag{9.3.7.1}$$

*Proof.* The functions $sl(\alpha z), P_\alpha(sl(z))$, and $Q_\alpha(sl(z))$ are $L_V$-periodic and meromorphic on $\mathbf{C}/L_V$. By 9.3.6, $sl(\alpha z)$ has simple zeros at $\frac{1}{\alpha}L$ and simple poles at

$$\frac{1}{\alpha}\left(L+\frac{1\pm i}{2}\Omega\right)=\frac{1}{\alpha}L+\frac{1\pm i}{2}\Omega$$

(the equality follows from the fact that $\alpha-1\in(1+i)\mathbf{Z}[i]$). Similarly, $P_\alpha(sl(z))$ has simple zeros at $\frac{1}{\alpha}L$ and poles order $N\alpha$ at $L+\frac{1+i}{2}\Omega$, while $Q_\alpha(sl(z))$ has poles of order $(N\alpha-1)$ at $L+\frac{1+i}{2}\Omega$ and simple zeros at $\left(\frac{1}{\alpha}L\setminus L\right)+\frac{1+i}{2}\Omega$, hence

$$\operatorname{div}(sl(\alpha z))=\operatorname{div}\left(\frac{P_\alpha(sl(z))}{Q_\alpha(sl(z))}\right)\in\operatorname{Div}(\mathbf{C}/L_V).$$

Proposition follows.

**(9.3.8) Corollary.** *If $\alpha\in\mathbf{Z}[i]$, $2\nmid N\alpha$, then*

$$\prod_{u\in\Sigma_\alpha}sl^4(u)=(-1)^{\frac{N\alpha-1}{4}}c_\alpha\cdot\alpha.$$

*Proof.* Differentiating (9.3.7.1) yields

$$\alpha\,sl'(\alpha z)=\frac{P'_\alpha Q_\alpha-P_\alpha Q'_\alpha}{c_\alpha Q_\alpha^2}(sl(z))\,sl'(z). \tag{9.3.8.1}$$

Putting $z=0$ (and using the fact that $sl'(0)=1\neq 0$), we obtain

$$c_\alpha\cdot\alpha=\frac{P'_\alpha(0)}{Q_\alpha(0)}=\prod_{u\in\Sigma_\alpha}(-sl(u))^4=(-1)^{\frac{N\alpha-1}{4}}\prod_{u\in\Sigma_\alpha}sl^4(u).$$

**(9.3.9) Normalization of $\alpha$.** There are 8 residue classes in $\mathbf{Z}[i]$ modulo $2+2i=-i(1+i)^3$, of which 4 are invertible. More precisely, the reduction map $\mathbf{Z}[i]\longrightarrow\mathbf{Z}[i]/(2+2i)$ induces an isomorphism

$$\{\pm1,\pm i\}=\mathbf{Z}[i]^*\xrightarrow{\sim}(\mathbf{Z}[i]/(2+2i))^*.$$

This implies that, for each $\alpha\in\mathbf{Z}[i]$ with $2\nmid N\alpha$, there is a unique element $d_\alpha\in\{\pm1,\pm i\}$ satisfying

$$\alpha\cdot d_\alpha\equiv 1\ (\mathrm{mod}\,(2+2i)).$$

This should be compared to the isomorphism

$$\{\pm1\}=\mathbf{Z}^*\xrightarrow{\sim}(\mathbf{Z}/4\mathbf{Z})^*$$

and the congruence

$$n^*:=n\cdot(-1)^{\frac{n-1}{2}}\equiv 1\ (\mathrm{mod}\,4)$$

(for $n\in\mathbf{Z}$, $2\nmid n$).

**(9.3.10) Proposition.** *Let $\alpha\in\mathbf{Z}[i]$, $2\nmid N\alpha$. Then $P_\alpha(t),Q_\alpha(t)\in\mathbf{Z}[i][t]$ and $c_\alpha=d_\alpha$.*

*Proof.* We use induction on $N\alpha$. Assume first that $N\alpha=1$. In this case $\alpha\in\{\pm1,\pm i\}$, $\Sigma_\alpha=\emptyset$, $P_\alpha(t)=t$, $Q_\alpha(t)=1$, $sl(\alpha z)=\alpha sl(z)$, hence $\alpha\cdot c_\alpha=1$ as required.

In general, applying (8.4.2.3) with $z_1=\alpha z$ and $z_2=(1\pm i)z$ and using 9.3.7, we obtain

$$\prod_{\epsilon=\pm1}\frac{P_{\alpha+\epsilon(1\pm i)}(t)}{c_{\alpha+\epsilon(1\pm i)}Q_{\alpha+\epsilon(1\pm i)}(t)}=\frac{(t^4-1)P_\alpha^2(t)\pm 2ic_\alpha^2t^2Q_\alpha^2(t)}{\mp 2it^2P_\alpha^2(t)+(t^4-1)c_\alpha^2Q_\alpha^2(t)}.$$

By 9.3.4, there is no cancellation of terms between the numerator and the denominator on the L.H.S. As the degree of the numerator (resp. the denominator) of the R.H.S. is equal to $2N\alpha+4$ (resp. is $\leq 2N\alpha+2$) and the leading term of each $P_\beta(t)$ is $t^{N\beta}$, it follows that we have exact equalities between the numerators and denominators on both sides:

$$\begin{aligned} P_{\alpha+(1\pm i)}(t)P_{\alpha-(1\pm i)}(t) &= (t^4-1)P_\alpha^2(t) \pm 2ic_\alpha^2 t^2 Q_\alpha^2(t) \\ (c\cdot Q)_{\alpha+(1\pm i)}(t)\,(c\cdot Q)_{\alpha-(1\pm i)}(t) &= \mp 2it^2P_\alpha^2(t) + (t^4-1)c_\alpha^2Q_\alpha^2(t). \end{aligned} \tag{9.3.10.1}$$

Assume that Proposition is already proved for $\alpha$ and $\alpha-\epsilon(1+\delta i)$ (for fixed $\epsilon,\delta=\pm 1$). The first line of (9.3.10.1) implies that $P(t)=P_{\alpha+\epsilon(1+\delta i)}(t)$ is a polynomial with coefficients in $\mathbf{Q}(i)$. Recall that the *contents* of such a polynomial is the principal fractional ideal of $\mathbf{Q}(i)$ generated by the coefficients. Multiplicativity of the contents ("Gauss' Lemma") then implies that the contents of $P(t)$ is equal to (1), hence $P(t)\in\mathbf{Z}[i][t]$. As the coefficients of $Q(t)=Q_{\alpha+\epsilon(1+\delta i)}(t)$ are the same as those of $P(t)$, only written backwards, we also have $Q(t)\in\mathbf{Z}[i][t]$.

Substituting $t=0$ to the second line of (9.3.10.1) yields

$$c_{\alpha+\epsilon(1+\delta i)}\cdot c_{\alpha-\epsilon(1+\delta i)} = -c_\alpha^2. \tag{9.3.10.2}$$

As

$$(\alpha+\epsilon(1+\delta i))(\alpha-\epsilon(1+\delta i)) = \alpha^2-2\delta i \equiv -\alpha^2 \pmod{(2+2i)},$$

we have

$$d_{\alpha+\epsilon(1+\delta i)}\cdot d_{\alpha-\epsilon(1+\delta i)} = -d_\alpha^2. \tag{9.3.10.3}$$

As $c_\beta=d_\beta$ for $\beta=\alpha,\alpha-\epsilon(1+\delta i)$ by induction hypothesis, the formulas (9.3.10.2-3) imply that $c_\beta=d_\beta$ also for $\beta=\alpha+\epsilon(1+\delta i)$. This concludes the induction step (the exact values of $\epsilon,\delta$ depend on the circumstances).

**(9.3.11) Corollary (Product Formula (P)).** *If $\alpha\in\mathbf{Z}[i]$, $2\nmid N\alpha$, then*

$$\prod_{u\in\Sigma_\alpha} sl^4(u) = (-1)^{\frac{N\alpha-1}{4}}\alpha\cdot d_\alpha. \tag{P}$$

*In particular, if $\alpha\equiv 1 \pmod{(2+2i)}$, then*

$$\prod_{u\in\Sigma_\alpha} sl^4(u) = (-1)^{\frac{N\alpha-1}{4}}\alpha.$$

**(9.3.12) Corollary.** *If $\alpha\in\mathbf{Z}[i]$, $2\nmid N\alpha$ and $u\in\frac{1}{\alpha}L$, then $sl(u)$ is an algebraic integer.*

## 9.4 The Congruence Formula for $sl(z)$

**(9.4.1)** If $\alpha\in\mathbf{Z}[i]$ is an irreducible element with $2\nmid N\alpha$, then 0.4.3.0 implies that the residue field $k(\alpha)=\mathbf{Z}[i]/\alpha\mathbf{Z}[i]$ is a finite field with $N\alpha=p^a$ elements, where $p\in\mathbf{N}$ is the unique prime number divisible by $\alpha$ and $a=1$ (resp. $a=2$) if $p\equiv 1 \pmod 4$ (resp. if $p\equiv 3 \pmod 4$).

**(9.4.2) Proposition.** *If $\alpha\in\mathbf{Z}[i]$, $2\nmid N\alpha$, put*

$$R_\alpha(t) = \prod_{u\in\left(\frac{1}{\alpha}L/L\right)-\{0\}} \left(t-sl\left(u+\tfrac{\Omega}{2}\right)\right)\left(t-sl\left(u+\tfrac{i\Omega}{2}\right)\right) = \prod_{u\in\Sigma_\alpha}\left(t^4-sl^4\left(u+\tfrac{\Omega}{2}\right)\right)\left(t^4-sl^4\left(u+\tfrac{i\Omega}{2}\right)\right).$$

*Then*

$$sl'(\alpha z) = \frac{R_\alpha(sl(z))}{Q_\alpha^2(sl(z))}\,sl'(z) \tag{9.4.2.1}$$

*and* $R_\alpha(t) \in \mathbf{Z}[i][t]$.

*Proof.* It follows from

$$\operatorname{div}(y) = \sum_{\zeta^4=1} ((\zeta, 0)) - 2(O_+) - 2(O_-) \in \operatorname{Div}(V(\mathbf{C})),$$

that

$$\operatorname{div}(sl'(z)) = \sum_{\zeta^4=1} \left(\tfrac{\zeta\Omega}{2}\right) - 2\left(\tfrac{1+i}{2}\Omega\right) - 2\left(\tfrac{1-i}{2}\Omega\right) \in \operatorname{Div}(\mathbf{C}/L_V).$$

In other words, $sl'(z)$ has simple zeros at $(\frac{\Omega}{2} + L)\dot{\cup}(\frac{i\Omega}{2} + L)$ and double poles at $\frac{1+i}{2}\Omega + L$. As in the proof of 9.3.7, this implies that

$$\operatorname{div}\left(\frac{sl'(\alpha z)}{sl'(z)}\right) = \operatorname{div}\left(\frac{R_\alpha(sl(z))}{Q_\alpha^2(sl(z))}\right),$$

showing that the ratio of the left and right hand sides of (9.4.2.1) is a constant. As the value of the L.H.S. (resp. the R.H.S.) at $z = 0$ is equal to 1 (resp. to $R_\alpha(0)$), it remains to prove that $R_\alpha(0) = 1$; this is a consequence of (9.3.2.1) for $z = u + \frac{i\Omega}{2}$.

The formula 9.3.8.1 implies that $R_\alpha(t) \in \mathbf{Q}(i)[t]$; it remains to show that each root of $R_\alpha(t)$ is an algebraic integer. Indeed, such a root is of the form $sl(u + \frac{\zeta\Omega}{2})$, where $u \in \frac{1}{\alpha}L$ and $\zeta \in \{\pm 1, \pm i\}$, hence it is also a root of the polynomial

$$P_\alpha(t) - d_\alpha sl(\alpha u + \tfrac{\zeta\Omega}{2})Q_\alpha(t) = P_\alpha(t) - d_\alpha sl(\tfrac{\zeta'\Omega}{2})Q_\alpha(t) = P_\alpha(t) - d_\alpha\zeta' Q_\alpha(t) = 0$$

(for some $\zeta' \in \{\pm 1, \pm i\}$), which is a monic polynomial with coefficients in $\mathbf{Z}[i][t]$ (by 9.3.10). Proposition follows.

**(9.4.3) Proposition (Congruence Formula (C)).** *If $\alpha \in \mathbf{Z}[i]$ is irreducible and $2 \nmid N\alpha$, then*

$$P_\alpha(t) \equiv t^{N\alpha} \pmod{\alpha\mathbf{Z}[i][t]}, \qquad Q_\alpha(t) \equiv 1 \pmod{\alpha\mathbf{Z}[i][t]}. \tag{C}$$

*Proof.* Let us try to generalize the "elementary" proof of 9.2.3. Combining (9.3.8.1) with (9.4.2.1), we obtain

$$P'_\alpha Q_\alpha - P_\alpha Q'_\alpha = \alpha d_\alpha Q_\alpha^2 R_\alpha \equiv 0 \pmod{\alpha\mathbf{Z}[i][t]}. \tag{9.4.3.1}$$

As

$$P_\alpha(t) = t^{N\alpha} + a_1 t^{N\alpha-1} + \cdots + a_{N\alpha-1}t, \qquad Q_\alpha(t) = a_{N\alpha-1}t^{N\alpha-1} + \cdots + a_1 t + 1, \qquad a_{N\alpha-1} = \alpha d_\alpha,$$

considering the coefficients of the L.H.S. of (9.4.2.1) modulo $\alpha\mathbf{Z}[i]$ yields consecutively

$$\begin{gathered}
-(N\alpha - 1)a_{N\alpha-1} \equiv 0 \Longrightarrow a_{N\alpha-1} \equiv 0 \pmod{\alpha\mathbf{Z}[i]} \\
-(N\alpha - 2)a_{N\alpha-2} \equiv 0 \Longrightarrow a_{N\alpha-2} \equiv 0 \pmod{\alpha\mathbf{Z}[i]} \\
\cdots \\
-(N\alpha - p + 1)a_{N\alpha-p+1} \equiv 0 \Longrightarrow a_{N\alpha-p+1} \equiv 0 \pmod{\alpha\mathbf{Z}[i]},
\end{gathered}$$

which proves the claim if $N\alpha = p$ (i.e. if $p \equiv 1 \pmod 4$).

It is not clear (at least to the author of these notes) whether one can prove the Proposition by this method also in the case $N\alpha = p^2$. Instead, we shall generalize the method of proof of 9.2.8. By 9.3.12, the values $sl(u)$ ($u \in \frac{1}{\alpha}L$) are contained in the ring of integers $\mathcal{O}_K$ of the number field $K = \mathbf{Q}(i)(sl(u) \,|\, u \in \frac{1}{\alpha}L)$. According to 9.3.7 and 9.3.10, we have

$$\prod_{u\in\left(\frac{1}{\alpha}L/L\right)-\{0\}} sl(u) = \alpha c_\alpha = \alpha d_\alpha, \qquad d_\alpha \in \{\pm 1, \pm i\},$$

which implies that there exists a prime ideal $\mathfrak{p}|\alpha$ in $\mathcal{O}_K$ and $u_0 \in \left(\frac{1}{\alpha}L/L\right) - \{0\}$ such that $\mathfrak{p}|sl(u_0)$. For each $u \in \left(\frac{1}{\alpha}L/L\right) - \{0\}$ there exists $\beta \in \mathbf{Z}[i]$ satisfying $2 \nmid N\beta$ and $u \equiv \beta u_0 \pmod{L}$.

As $\mathfrak{p}|sl(u_0)$ and $P_\beta(t), Q_\beta(t) \in \mathbf{Z}[i][t]$, it follows that

$$P_\beta(sl(u_0)) \equiv P_\beta(0) \equiv 0 \pmod{\mathfrak{p}}, \qquad Q_\beta(sl(u_0)) \equiv Q_\beta(0) \equiv 1 \pmod{\mathfrak{p}},$$

hence each non-zero root of $P_\alpha(t)$ satisfies

$$sl(u) = sl(\beta u_0) = \frac{P_\beta(sl(u_0))}{d_\beta Q_\beta(sl(u_0))} \equiv 0 \pmod{\mathfrak{p}}; \tag{9.4.3.2}$$

thus

$$P_\alpha(t) \equiv t^{N\alpha} \pmod{\mathfrak{p}\mathcal{O}_K[t]},$$

which implies the same congruence modulo $(\mathfrak{p}\mathcal{O}_K \cap \mathbf{Z}[i])[t] = \alpha\mathbf{Z}[i][t]$, as required. The desired congruence for $Q_\alpha(t)$ follows from (9.3.1.1).

**(9.4.4) Corollary.** *Assume that $\alpha \in \mathbf{Z}[i]$ is irreducible, $2 \nmid N\alpha$, $K$ is a number field containing $\mathbf{Q}(i)$ and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ dividing $\alpha$. If $z \in \mathbf{C}$ and $sl(z) \in \mathcal{O}_K$, then $sl(\alpha z) \in \mathcal{O}_K$ and*

$$d_\alpha sl(\alpha z) \equiv sl(z)^{N\alpha} \pmod{\mathfrak{p}}$$

*(with $d_\alpha \in \{\pm 1, \pm i\}$ defined in 9.3.9).*

**(9.4.5) Proposition.** *Assume that $\alpha \in \mathbf{Z}[i]$ is irreducible, $2 \nmid N\alpha$. Then*

$$R_\alpha(t) \equiv (1 - t^4)^{\frac{N\alpha - 1}{2}} \pmod{\alpha\mathbf{Z}[i][t]}.$$

*Proof.* Using the notation from the proof of 9.4.3, the formulas

$$sl\left(z + \tfrac{\Omega}{2}\right) = \frac{sl'(z)}{1 + sl^2(z)}, \qquad sl\left(z + \tfrac{i\Omega}{2}\right) = \frac{isl'(z)}{1 - sl^2(z)}$$

together with (9.4.3.2) imply that, for all $u \in \Sigma_\alpha$,

$$sl^4\left(u + \tfrac{\Omega}{2}\right) \equiv sl^4\left(u + \tfrac{i\Omega}{2}\right) \equiv sl'(u)^4 \equiv (1 - sl^4(u))^2 \equiv 1 \pmod{\mathfrak{p}},$$

hence

$$R_\alpha(t) \equiv (t^4 - 1)^{\frac{N\alpha - 1}{2}} \equiv (1 - t^4)^{\frac{N\alpha - 1}{2}} \pmod{\mathfrak{p}\mathcal{O}_K[t]} \implies R_\alpha(t) \equiv (1 - t^4)^{\frac{N\alpha - 1}{2}} \pmod{\alpha\mathbf{Z}[i][t]}.$$

**(9.4.6) Proposition.** *Assume that $\alpha \in \mathbf{Z}[i]$ is irreducible, $2 \nmid N\alpha$; put $\psi(\alpha) = d_\alpha \cdot \alpha \equiv 1 \pmod{(2 + 2i)}$, where $d_\alpha$ ($\in \{\pm 1, \pm i\}$) is as in 9.3.9. Then the group law on the curve $V$ satisfies*

$$[\psi(\alpha)](x, y) \equiv (x^{N\alpha}, y^{N\alpha}) \pmod{\alpha}$$

*(this congruence should be interpreted as in 8.4.7). In particular, if $\alpha \equiv 1 \pmod{(2 + 2i)}$, then 8.4.9 holds.*

*Proof.* By 9.3.7, 9.3.10 and (9.4.2.1), we have

$$[\alpha](x,y) = \left(\frac{P_\alpha(x)}{d_\alpha Q_\alpha(x)}, \frac{R_\alpha(x)}{Q_\alpha^2(x)}\, y\right).$$

The congruences 9.4.3,5 then yield

$$[\psi(\alpha)](x,y) = \left(\frac{P_\alpha(x)}{Q_\alpha(x)}, \frac{R_\alpha(x)}{Q_\alpha^2(x)}\, y\right) \equiv (x^{N\alpha}, (1-x^4)^{\frac{N\alpha-1}{2}} y) = (x^{N\alpha}, y^{N\alpha}) \pmod{\alpha}.$$

## 9.5 Biquadratic Reciprocity Law

Let us try to imitate the theory from 9.1-2 in the context of Gaussian integers $\mathbf{Z}[i]$. Our analytic approach will disregard many arithmetic aspects of the theory; these can be found, for example, in [Co] or [Ir-Ro].

**(9.5.1)** Let $\alpha \in \mathbf{Z}[i]$ be as in 9.4.1. As $\zeta \not\equiv 1 \pmod{\alpha}$ for any $\zeta \in \{-1, \pm i\}$, the reduction modulo $\alpha$ induces an *injective* homomorphism of abelian groups

$$\{\pm 1, \pm i\} \hookrightarrow k(\alpha)^* = (\mathbf{Z}[i]/\alpha\mathbf{Z}[i])^*. \tag{9.5.1.1}$$

As $k(\alpha)^*$ is a cyclic group order $N\alpha - 1$, it follows that $N\alpha \equiv 1 \pmod 4$ and that the following definition makes sense:

**(9.5.2) Definition (Biquadratic residue symbol).** *If $\alpha \in \mathbf{Z}[i]$ is irreducible, $2 \nmid N\alpha$, $a \in \mathbf{Z}[i]$ and $\alpha \nmid a$, denote by $\left(\frac{a}{\alpha}\right)_4$ the unique element of $\{\pm 1, \pm i\}$ satisfying the congruence*

$$\left(\frac{a}{\alpha}\right)_4 \equiv a^{\frac{N\alpha-1}{4}} \pmod{\alpha}$$

*("generalized Euler's criterion").*

**(9.5.3) Lemma.** (i) *The biquadratic residue symbol modulo $\alpha$ defines an isomorphism of abelian groups*

$$\left(\frac{\bullet}{\alpha}\right)_4 : k(\alpha)^*/k(\alpha)^{*4} \xrightarrow{\sim} \{\pm 1, \pm i\}.$$

(ii) *If $\alpha \nmid ab$ $(a, b \in \mathbf{Z}[i])$, then*

$$\left(\frac{ab}{\alpha}\right)_4 = \left(\frac{a}{\alpha}\right)_4 \left(\frac{b}{\alpha}\right)_4, \qquad \left(\frac{\overline{a}}{\overline{\alpha}}\right)_4 = \overline{\left(\frac{a}{\alpha}\right)_4} = \left(\frac{a}{\alpha}\right)_4^{-1}, \qquad \left(\frac{i}{\alpha}\right)_4 = i^{\frac{N\alpha-1}{4}}.$$

(iii) *If $N\alpha = p \equiv 1 \pmod 4$ and $a \in \mathbf{Z}$, $p \nmid a$, then*

$$\left(\frac{a}{\alpha}\right)_4 = 1 \iff a \pmod p \in \mathbf{F}_p^{*4} \iff (\exists x \in \mathbf{Z})\ x^4 \equiv a \pmod p.$$

(iv) *If $N\alpha = p^2$, $p \equiv 3 \pmod 4$ (i.e. $\alpha \in \{\pm p, \pm ip\}$) and $a \in \mathbf{Z}$, $p \nmid a$, then*

$$\left(\frac{a}{\alpha}\right)_4 = 1.$$

*Proof.* (i),(ii) This follows from the definitions (and the fact that $k(\alpha)^*$ is cyclic of order $N\alpha - 1$). (iii) is a special case of (i). Finally, (iv) is a consequence of

$$a^{\frac{p^2-1}{4}} = (a^{\frac{p+1}{4}})^{p-1} \equiv 1 \pmod{p\mathbf{Z}}.$$

**(9.5.4) Lemma.** *Let $\alpha \in \mathbf{Z}[i]$ be irreducible, $2 \nmid N\alpha$; let $\Sigma_\alpha$ be as in 9.3.1. Fix $a \in \mathbf{Z}[i]$ not divisible by $\alpha$. For each $u \in \Sigma_\alpha$ there is a unique pair $\zeta_u \in \{\pm 1, \pm i\}$ and $u' \in \Sigma_\alpha$ satisfying $au = \zeta_u u'$; then*

$$\prod_{u \in \Sigma_\alpha} \zeta_u = \left(\frac{a}{\alpha}\right)_4.$$

*Proof.* The proof of 9.1.3 applies with straightforward modifications.

**(9.5.5) Biquadratic Reciprocity Law.** *Let $\alpha, \beta \in \mathbf{Z}[i]$ be irreducible, $\alpha \nmid \beta$ and $\alpha \equiv \beta \equiv 1 \pmod{(2+2i)}$. Then*

$$\left(\frac{\beta}{\alpha}\right)_4 = \left(\frac{\alpha}{\beta}\right)_4 (-1)^{\frac{N\alpha-1}{4}\cdot\frac{N\beta-1}{4}}.$$

*Proof.* We shall follow the argument from 9.2.9. Fix $\Sigma_\alpha$ as in 9.3.1 and put

$$S = \prod_{u\in\Sigma_\alpha} sl(u), \qquad S' = \prod_{u\in\Sigma_\alpha} sl(\beta u) \in \mathcal{O}_K,$$

where $K = \mathbf{Q}(i, sl(u) \,|\, u \in \frac{1}{\alpha}L/L)$. As in (9.2.9.1), the identity $sl(\zeta z) = \zeta sl(z)$ ($\zeta \in \{\pm 1, \pm i\}$) together with 9.5.4 imply that

$$\left(\frac{\beta}{\alpha}\right)_4 S = S'.$$

Fix a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ dividing $\beta$. The congruence formula (C) in the form 9.4.4 then yields

$$\left(\frac{\beta}{\alpha}\right)_4 S = S' \equiv S^{N\beta} \pmod{\mathfrak{p}}.$$

According to the product formula (P) from 9.3.11,

$$S^4 = (-1)^{\frac{N\alpha-1}{4}}\alpha$$

is not divisible by $\mathfrak{p}$, hence

$$\left(\frac{\beta}{\alpha}\right)_4 \equiv S^{N\beta-1} = (S^4)^{\frac{N\beta-1}{4}} = (-1)^{\frac{N\alpha-1}{4}\cdot\frac{N\beta-1}{4}}\alpha^{\frac{N\beta-1}{4}} \pmod{\mathfrak{p}},$$

which is in turn congruent to

$$\left(\frac{\beta}{\alpha}\right)_4 \equiv (-1)^{\frac{N\alpha-1}{4}\cdot\frac{N\beta-1}{4}} \left(\frac{\alpha}{\beta}\right)_4 \pmod{\mathfrak{p}}.$$

Both sides of this congruence are elements of $\{\pm 1, \pm i\}$; as $\mathfrak{p} \cap \mathbf{Z}[i] = \beta\mathbf{Z}[i]$, it follows that

$$\left(\frac{\beta}{\alpha}\right)_4 \equiv (-1)^{\frac{N\alpha-1}{4}\cdot\frac{N\beta-1}{4}} \left(\frac{\alpha}{\beta}\right)_4 \pmod{\beta\mathbf{Z}[i]}.$$

However, both sides of the latter congruence must be equal, by the injectivity of (9.5.1.1) for $\beta$.

**(9.5.6) Exercise.** *Irreducible elements $\alpha \in \mathbf{Z}[i]$ satisfying $\alpha \equiv 1 \pmod{(2+2i)}$ are the following:*
(i) *$\alpha = u \pm iv$, where $u, v \in \mathbf{Z}$, $N\alpha = u^2 + v^2 = p \equiv 1 \pmod 4$ is a prime, $v \equiv 0 \pmod 2$, $u \equiv v + 1 \pmod 4$ (the pair $u \pm iv$ is determined by $p$ uniquely).*
(ii) *$\alpha = -p$, where $p \equiv 3 \pmod 4$ is a prime.*

**(9.5.7) Example:** Let us compute $\left(\frac{-3}{\alpha}\right)_4$ for $\alpha = u \pm iv$ as in 9.5.6(i). Applying 9.5.5, we obtain

$$\left(\frac{-3}{\alpha}\right)_4 = \left(\frac{\alpha}{-3}\right)_4.$$

There are 8 residue classes in $(\mathbf{Z}[i]/3\mathbf{Z}[i])^*$, represented by $a = \pm 1, \pm i, \pm(1+i), \pm(1-i)$. As

$$\left(\frac{a}{-3}\right)_4 \equiv a^2 \pmod{3\mathbf{Z}[i]},$$

it follows that

$$\left(\frac{\pm 1}{-3}\right)_4 = 1, \qquad \left(\frac{\pm i}{-3}\right)_4 = -1, \qquad \left(\frac{\pm(1+i)}{-3}\right)_4 = -i, \qquad \left(\frac{\pm(1-i)}{-3}\right)_4 = i,$$

hence

$$(\exists x \in \mathbf{Z})\ x^4 \equiv -3 \pmod p \iff \left(\frac{-3}{\alpha}\right)_4 = 1 \iff \alpha \equiv \pm 1 \pmod{3\mathbf{Z}[i]} \iff$$

$$\iff u \equiv \pm 1 \pmod 3,\ v \equiv 0 \pmod 3 \iff v \equiv 0 \pmod 6 \iff (\exists a, b \in \mathbf{Z})\ \ p = a^2 + (6b)^2.$$

**(9.5.8) Exercise.** *Show that, for a prime number* $p \equiv 1 \pmod 4$, $p \neq 5$,

$$(\exists x \in \mathbf{Z})\ x^4 \equiv 5 \pmod p \iff (\exists a, b \in \mathbf{Z})\ \ p = a^2 + (10b)^2.$$

**(9.5.9)** If $p$ is a prime number satisfying $p \equiv 3 \pmod 4$, then the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic of order $p-1$, where $(p-1, 4) = 2$. This implies that $\mathbf{F}_p^{*4} = \mathbf{F}_p^{*2}$, hence

$$(\exists x \in \mathbf{Z})\ x^4 \equiv a \pmod p \iff (\exists y \in \mathbf{Z})\ y^2 \equiv a \pmod p \iff \left(\frac{a}{p}\right) = 1 \qquad (a \in \mathbf{Z},\ p \nmid a).$$

**(9.5.10)** Similarly, if $p$ is a prime number satisfying $p \equiv 2 \pmod 3$, then $(p-1, 3) = 1$, hence $\mathbf{F}_p^{*3} = \mathbf{F}_p^*$. In other words, the congruence

$$x^3 \equiv a \pmod p \tag{9.5.10.1}$$

has a (unique) solution modulo $p$ for every $a \in \mathbf{Z}$.

**(9.5.11)** On the other hand, if $p \equiv 1 \pmod 3$, then the solvability of (9.5.10.1) depends on $a$ in a non-trivial way. One can define the Cubic residue symbol and prove the Cubic Reciprocity Law by working with $\mathbf{Z}[\rho]$ (where $\rho = e^{2\pi i/3}$) instead of $\mathbf{Z}[i]$ (see [Co], [Ir-Ro]).

**(9.5.12) Exercise.** *Prove the Cubic Reciprocity Law using the function* $\wp(z)$ *associated to a lattice* $L' = \mathbf{Z}[\rho] \cdot \Omega'$ *for suitable* $\Omega'$ *(e.g. such that* $\wp'(z)^2 = 4\wp(z)^3 - 4$*).*

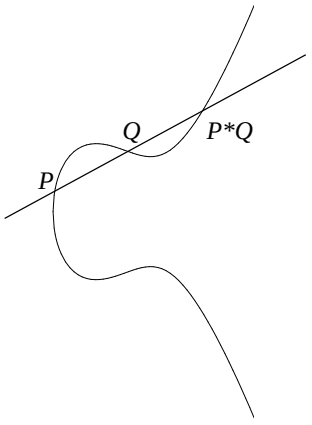
## 10. Group law on smooth cubic curves

### 10.1 The geometric definition of the group law

**(10.1.1)** Let $K$ be a field and $F = F(X, Y, Z) \in K[X, Y, Z]$ a homogeneous polynomial of degree $\deg(F) = 3$. We assume that the corresponding cubic (projective) plane curve $C : F = 0$ is smooth (this implies that $F$ is irreducible over any extension of $K$).

Fix a point $O \in C(K)$. For $P, Q \in C(K)$, we define $P * Q, P \boxplus Q \in C(K)$ as in 7.5.6: $P * Q$ is the third intersection point of $C$ with the line $\overline{PQ}$ (resp. with the tangent to $C$ at $P$) if $P \neq Q$ (resp. $P = Q$), and

$$P \boxplus Q = O * (P * Q). \tag{10.1.1.1}$$



**(10.1.2) Theorem.** *$(C(K), \boxplus)$ is an abelian group with neutral element $O$.*

**(10.1.3)** It is easy to check that $P * Q$ lies indeed in $C(K)$, so the only non-trivial point is the associativity law for $P, Q, R \in C(K)$:

$$(P \boxplus Q) \boxplus R \stackrel{?}{=} P \boxplus (Q \boxplus R) \tag{10.1.3.1}$$

We shall explain in 10.2.6 below how to deduce (10.1.3.1) from a suitable configuration theorem for points on cubic curves.

**(10.1.4) Exercise.** *Show that the following statements are equivalent:*

$$O \text{ is an inflection point of } C \iff O * O = O \iff (\forall P \in C(K)) \quad P * O = -P.$$

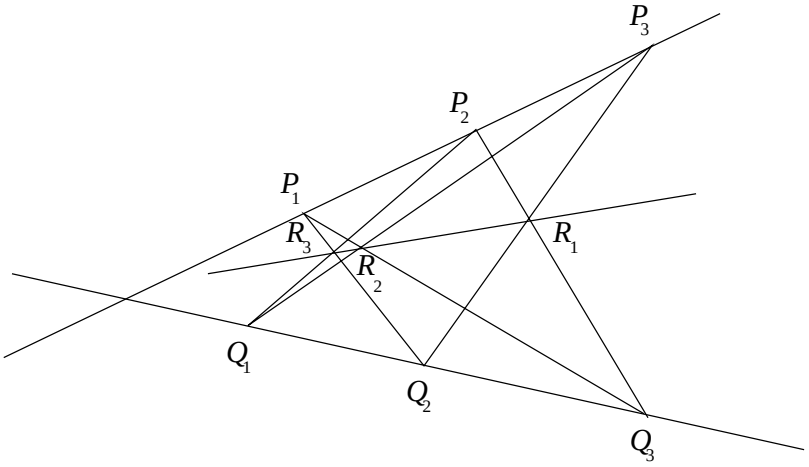
## 10.2 Configuration theorems

We begin by recalling two classical geometric results.

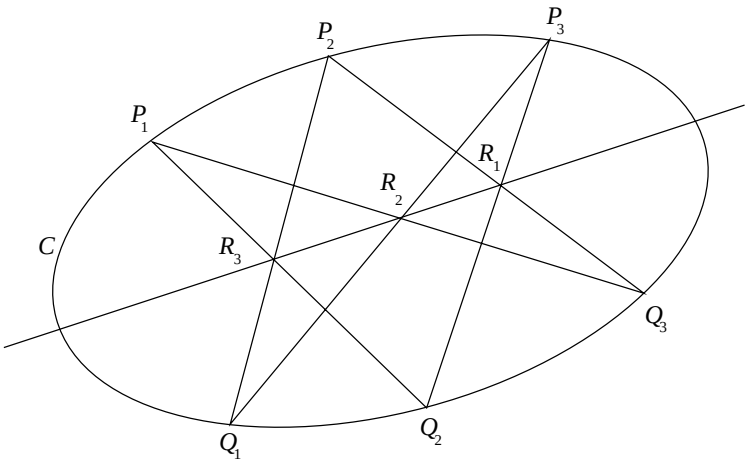
**(10.2.1) Theorem of Pappus.** *Let $P_1, P_2, P_3$ (resp. $Q_1, Q_2, Q_3$) be two triples of collinear points in the plane. Let*

$$R_k = \overline{P_i Q_j} \cap \overline{P_j Q_i} \qquad (\{i, j, k\} = \{1, 2, 3\})$$

*be the intersection points of the pairs of lines $\overline{P_i Q_j}$ and $\overline{P_j Q_i}$. Then the points $R_1, R_2, R_3$ are collinear.*




**(10.2.2) Pascal's Theorem.** *Let $P_1, P_2, P_3, Q_1, Q_2, Q_3$ be six distinct points on a conic $C$. Then the points $R_1, R_2, R_3$ (defined as in 10.2.1) are collinear.*



**(10.2.3)** Theorem of Pappus is a special case of Pascal's Theorem, when the conic $C$ is reducible. Pascal's Theorem, in turn, is a special case of the following result on cubic curves.

**(10.2.4) Theorem of Cayley-Bacharach for cubic curves (weak wersion).** *Let $C_1, C_2 \subset \mathbf{P}^2$ be projective cubic curves over an algebraically closed field $K = \overline{K}$ such that $C_1(K) \cap C_2(K)$ consists of 9 distinct points $S_1, \ldots, S_9 \in C(K)$. If $D \subset \mathbf{P}^2$ is another projective cubic curve such that $P_1, \ldots, P_8 \in D(K)$, then $P_9 \in D(K)$.*

**(10.2.5) Cayley-Bacharach $\Longrightarrow$ Pascal.** In the situation of 10.2.2, let

$$C_1 : \overline{P_1Q_3} \cup \overline{P_2Q_1} \cup \overline{P_3Q_2}, \qquad C_2 : \overline{P_3Q_1} \cup \overline{P_1Q_2} \cup \overline{P_2Q_3}, \qquad D : C \cup \overline{R_1R_2}.$$

As

$$C_1 \cap C_2 = \{P_1, P_2, P_3, Q_1, Q_2, Q_3, R_1, R_2, R_3\}, \qquad C_1 \cap C_2 - \{R_3\} \in D,$$

it follows from 10.2.4 that

$$R_3 \in D \Longrightarrow R_3 \in \overline{R_1R_2}.$$

**(10.2.6) Cayley-Bacharach $\Longrightarrow$ associativity of $\boxplus$.** In the situation of 10.1.3 (after replacing $K$ by its algebraic closure), consider the cubic curves

$$C_1 = \overline{O(P \boxplus Q)} \cup \overline{QR} \cup \overline{P(Q \boxplus R)}, \qquad C_2 = \overline{O(Q \boxplus R)} \cup \overline{PQ} \cup \overline{R(P \boxplus Q)}, \qquad D = C.$$

*DIAGRAM UNDER CONSTRUCTION*

As

$$C_1 \cap C_2 = \{O, P, Q, R, P * Q, P \boxplus Q, Q * R, Q \boxplus R, S\}, \qquad S = \overline{P(Q \boxplus R)} \cap \overline{R(P \boxplus Q)}, \qquad (10.2.6.1)$$

it follows from 10.2.4 – assuming that the 9 points in (10.2.6.1) are distinct – that

$$S \in C \Longrightarrow P * (Q \boxplus R) = (P \boxplus Q) * R \Longrightarrow P \boxplus (Q \boxplus R) = (P \boxplus Q) \boxplus R.$$

If the points in (10.2.6.1) are not distinct, note that both sides of (10.1.3.1) are given by a morphism $C \times C \times C \longrightarrow C$ (cf. II.1.2.6 below). We have shown that the two morphisms agree on a dense open subset; as $C$ is projective (hence separated), they must agree everywhere.

Alternatively, one can appeal to the "strong version" of the Cayley-Bacharach Theorem:

**(10.2.7) Theorem of Cayley-Bacharach.** *Let $C, D, E \subset \mathbf{P}^2$ be curves of degrees $\deg(C) = m$, $\deg(D) = n$, $\deg(E) \leq m + n - 3$ over an algebraically closed field $K$. Then:*
(i) (weak wersion) *If $C(K) \cap D(K)$ consists of $mn$ distinct points $P_1, \ldots, P_{mn}$ and $P_1, \ldots, P_{mn-1} \in E(K)$, then $P_{mn} \in E(K)$.*
(ii) (strong wersion) *Assume that the intersection divisor $C(K) \cap D(K) = \sum_{j \in J} n_j(P_j)$, where each $P_j \in C(K)$ is a smooth point of $C$. If the local intersection multiplicities of $C$ and $E$ satisfy*

$$(C \cdot E)_{P_j} \geq \begin{cases} n_j, & j \in J - \{j_0\} \\ n_j - 1, & j = j_0 \end{cases}$$

*for some $j_0 \in J$, then*

$$(C \cdot E)_{P_{j_0}} \geq n_{j_0}.$$

**(10.2.8) Exercise.** *Deduce Pascal's Theorem 10.2.2 from Bézout's Theorem (see [Ki], 3.15).*

## 10.3 Residues

Rather surprisingly, 10.2.7 can be proved using a two-dimensional residue theorem. In this section we shall indicate the argument for 10.2.7(i). The general theory of multidimensional residues in the analytic context (i.e. over $K = \mathbf{C}$), as well as a proof of 10.2.7(ii) in this case, can be found in ([Gr-Ha], Ch. 5). The algebraic theory of residues forms a part of the Grothendieck Duality Theory, which is discussed in [Al-Kl] (and also in [Gr-Ha], Ch. 5).

**(10.3.1)** Recall the statement of Exercise I.2.2.2: if $F \in \mathbf{C}[x]$ is a polynomial of degree $\deg(F) \geq 2$ with $d$ distinct roots $x_1, \ldots, x_d \in \mathbf{C}$ and $g \in \mathbf{C}[x]$ a polynomial of degree $\deg(g) \leq d-2$, then

$$\sum_{j=1}^{d} \frac{g(x_j)}{F'(x_j)} = 0. \tag{10.3.1.1}$$

One can deduce (10.3.1.1) from the residue formula for the meromorphic differential

$$\omega = \frac{g(z)\,dz}{F(z)} \in \Omega^1_{\mathrm{mer}}(\mathbf{P}^1(\mathbf{C}))$$

on $\mathbf{P}^1(\mathbf{C})$. As $t = 1/z$ is a local coordinate at the point $\infty$, it follows from

$$dz = -t^{-2}\,dt, \qquad \mathrm{ord}_\infty(g) = -\deg(g) \geq 2-d, \qquad \mathrm{ord}_\infty(1/F) = \deg(F) = d$$

that

$$\mathrm{ord}_\infty(\omega) \geq (-2) + (2-d) + d \geq 0,$$

i.e. $\omega$ is holomorphic at $\infty$. The Residue Theorem I.3.3.10 then gives

$$0 = \sum_{x \in \mathbf{P}^1(\mathbf{C})} \mathrm{res}_x(\omega) = \sum_{x \in \mathbf{C}} \mathrm{res}_x(\omega) = \sum_{j=1}^{d} \mathrm{res}_{x_j}(\omega) = \sum_{j=1}^{d} \frac{g(x_j)}{F'(x_j)}.$$

A higher-dimensional version of (10.3.1.1) is the following formula:

**(10.3.2) Theorem (Jacobi).** *Let $F_1, \ldots, F_n \in \mathbf{C}[x_1, \ldots, x_n]$ be polynomials of degrees $\deg(F_j) = d_j \geq 1$. Assume that the hypersurfaces $Z_j = \{F_j = 0\} \subset \mathbf{C}^n$ intersect at exactly $d = d_1 \cdots d_n$ distinct points $P_\alpha \in C^n$ $(1 \leq \alpha \leq d)$. Let $g \in \mathbf{C}[x_1, \ldots, x_n]$ be a polynomial of degree $\deg(g) \leq (d_1 + \cdots + d_n) - (n+1)$. Then*

$$\sum_{\alpha=1}^{d} \frac{g(P_\alpha)}{J_F(P_\alpha)} = 0,$$

*where $J_F = \det(\partial F_i/\partial x_j)$ is the Jacobian of $F = (F_1, \ldots, F_n) : \mathbf{C}^n \longrightarrow \mathbf{C}^n$.*

*Proof (sketch).* Firstly, the $n$-dimensional variant of Bézout's Theorem implies that the local intersection multiplicity of the hypersurfaces $Z_j$ $(j = 1, \ldots, n)$ at each point $P_\alpha$ is equal to one, which is equivalent to the non-vanishing of $J_F(P_\alpha)$. Secondly, the assumption on $\deg(g)$ is equivalent to the fact that the meromorphic differential $n$-form

$$\omega = \frac{g(x)\,dx_1 \wedge \cdots \wedge dx_n}{F_1(x) \cdots F_n(x)} = \frac{g(x)}{J_F(x)} \frac{dF_1 \wedge \cdots \wedge dF_n}{F_1 \cdots F_n}$$

on $\mathbf{P}^n(\mathbf{C})$ has no pole along the hyperplane at infinity $\mathbf{P}^n(\mathbf{C}) - \mathbf{C}^n$. The $n$-dimentional residue theorem then implies

$$0 = \sum_{\alpha=1}^{d} \mathrm{res}_{P_\alpha}(\omega) = \sum_{\alpha=1}^{d} \frac{g(P_\alpha)}{J_F(P_\alpha)} \mathrm{res}_{P_\alpha}\left(\frac{dF_1 \wedge \cdots \wedge dF_n}{F_1 \cdots F_n}\right) = \sum_{\alpha=1}^{d} \frac{g(P_\alpha)}{J_F(P_\alpha)},$$

where the last equality follows from the fact that $F_1, \ldots, F_n$ form a system of local coordinates at each $P_\alpha$.

**(10.3.3) Corollary.** *If $g(P_\alpha) = 0$ for $\alpha = 1, \ldots, d-1$, then $g(P_d) = 0$.*

**(10.3.4)** In particular, for $n = 2$ we obtain the variant 10.2.7(i) of the Cayley-Bacharach Theorem with $C_1 : F_1 = 0$, $C_2 : F_2 = 0$, $E : g = 0$.

**(10.3.5)** As explained in ([Gr-Ha], 5.2), a variant of the above calculation can be used to prove 10.2.7(ii).

**(THIS IS VERSION 20/9/2004)**

## References


[Al-Kl] A.Altman, S.Kleiman, *Introduction to Grothendieck duality theory*, Lecture Notes in Mathematics **146**, Springer, 1970.

[Be] D. Bernardi, private communication.

[B-SD] B.J. Birch, H.P.F. Swinnerton-Dyer , *Notes on Elliptic Curves. II*, J. reine und angew. Math. **218** (1965), 79–108.

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

[Ca 1] J.W.S. Cassels, *Lectures on Elliptic Curves*, London Math. Society Student Texts **24**, Cambridge Univ. Press, 1991.

[Ca 2] J.W.S. Cassels, *Arithmetic on curves of genus* 1*. I. On a conjecture of Selmer*, J. Reine Angew. Math. **202** (1959), 52–99.

[Ca 3] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[Cl] C.H. Clemens, *A Scrapbook of Complex Curve Theory*, Plenum Press, 1980.

[Co-Wi] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.

[Col] P. Colmez, *La Conjecture de Birch et Swinnerton-Dyer p-adique*, Séminaire Bourbaki, Exp. 919, juin 2003.

[Ei] D. Eisenbud, *Commutative Algebra (with a view toward algebraic geometry)*, Graduate Texts in Mathematics **150**, Springer, 1995.

[Fa-Kr 1] H.M. Farkas, I. Kra, *Riemann surfaces*, Graduate Texts in Mathematics **71**, Springer, 1992.

[Fa-Kr 2] H.M. Farkas, I. Kra, *Theta constants, Riemann surfaces and the modular group*, Graduate Studies in Mathematics **37**, American Math. Society, 2001.

[Fo] O. Forster, *Lectures on Riemann surfaces*, Graduate Texts in Mathematics **81**, Springer, 1991.

[Gr-Ha] P. Griffiths, J. Harris, *Principles of algebraic geometry*, Wiley-Interscience, 1978.

[Gr-Za] B.H. Gross, D. Zagier *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

[Hu] D. Husemöller, *Elliptic Curves*, Graduate Texts in Mathematics **111**, Springer, 1987.

[Ir-Ro] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics **84**, Springer, 1982

[Ka] K. Kato, *P-adic Hodge theory and values of zeta functions of modular forms*, preprint, 2000.

[Ki] F. Kirwan, *Complex algebraic curves*, London Math. Society Student Texts **23**, Cambridge Univ. Press, 1992.

[Ko] V.A. Kolyvagin, *Euler systems*, in: The Grothendieck Festschrift, Vol. II, Progress in Math. **87** , Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[La] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics **112**, Springer, 1987.

[Mar] A.I. Markushevich, *Introduction to the classical theory of abelian functions*, Translations of Mathematical Monographs **96**, American Math. Society, 1992.

[Mat] H. Matsumura, *Commutative ring theory*, Cambridge Univ. Press, 1986.

[McK-Mo] H. McKean, V. Moll, *Elliptic curves*, Cambridge Univ. Press, 1997.

[Mi] J. Milne, *Elliptic curves*, lecture notes, `http://www.jmilne.org/math/`.

[Mu AV] D. Mumford, *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5; Oxford Univ. Press, 1970.

[Mu TH] D. Mumford, *Tata lectures on theta. I,II,III*, Progress in Mathematics **28**, **43**, **97**, Birkhäuser, 1983, 1984, 1991.

[MK] V.K. Murty, *Introduction to abelian varieties*, CRM Monograph Series **3**, American Math. Society, 1993.

[Ne] J. Nekovář, *On the parity of ranks of Selmer groups II*, C.R.A.S. Paris Sér. I Math. **332** (2001), no. 2, 99–104.

[Re] M. Reid, *Undergraduate Algebraic Geometry*, London Math. Society Student Texts **12**, Cambridge Univ. Press, 1988.

[Ru 1] W. Rudin, *Principles of mathematical analysis*, McGraw-Hill, 1976.

[Ru 2] W. Rudin, *Real and complex analysis*, McGraw-Hill, 1987.

[Sc] N. Schappacher, *Some milestones of lemniscatomy*, in: Algebraic geometry (Ankara, 1995), Lect. Notes in Pure and Appl. Math. **193**, Dekker, New York, 1997, pp. 257–290.

[Se] E.S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362.

[Si 1] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, 1986.

[Si 2] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994.

[Si-Ta] J.H. Silverman, J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer, 1992.

[Tu] J.B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), 323–334.

[Web] H. Weber, *Lehrbuch der Algebra. III*, 1908.

[Wei 1] A. Weil, *Introduction à l'étude des variétés kähleriennes*, Hermann, 1958.

[Wei 2] A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Ergebnisse der Mathematik und ihrer Grenzgebiete **88**, Springer, 1976.

## II. Algebraic Theory of Elliptic Curves

In this chapter we sketch the general theory of elliptic curves from an algebraic viewpoint. This material is fairly standard, although some of our proofs may differ from the ones appearing in standard textbooks (cf. [Si 1], [Mi], [Ca 1], [Hu]). The reader may prefer to stick to the usual old-fashioned algebraic geometry (see [Si 1], Ch. 1,2) and ignore any discussion of non-perfect fields.

### 1. Elliptic Curves - Generalities

#### 1.1 What is an elliptic curve?

**(1.1.1) Elliptic curves over C.** Informally, an elliptic curve over $\mathbf{C}$ is a smooth projective curve $E$ (over $\mathbf{C}$) such that the corresponding Riemann surface $E(\mathbf{C})$ is isomorphic to $\mathbf{C}/L$, for some lattice $L \in \mathbf{C}$. In other words, $E(\mathbf{C})$ can be parametrized by elliptic functions with respect to $L$.

**(1.1.2) Examples:** (1) The projectivization of the affine cubic curve $y^2 = f(x)$, where $f \in \mathbf{C}[x]$ is a polynomial of degree $\deg(f) = 3$ with three distinct roots (by I.4.4.2).
(2) The desingularized projectivization $V \cup \{O_+, O_-\}$ of the affine curve $V : y^2 = f(x)$, where $f \in \mathbf{C}[x]$ is a polynomial of degree $\deg(f) = 4$ with four distinct roots (I.3.7.8, I.4.2.5-7).
(3) A smooth intersection of two quadrics in $\mathbf{P}^3(\mathbf{C})$ (as in I.6.4.4-5).

**(1.1.3) Definition.** *An* **elliptic curve** *over a field $K$ is a pair $(E, O)$, where $E$ is a smooth projective curve over $K$, geometrically irreducible (i.e. irreducible over $\overline{K}$), of genus $g = 1$, and $O \in E(K)$ is a $K$-rational point of $E$ ("the origin").*

**(1.1.4)** (1) Recall that, if $X$ is a smooth projective curve over $K$, irreducible over $\overline{K}$, then the *genus* of $X$ is defined as the dimension of the space of regular differentials on $E$:

$$g(X) = \dim_K \Gamma(X, \Omega_{X/K}).$$

(2) For any field extension $L/K$, the curve $X_L = X \otimes_K L$ (defined by the same polynomial equations as $X$, but considered as a curve over $L$) is again a smooth projective curve over $L$, irreducible over $\overline{L}$, and

$$\Gamma(X_L, \Omega_{X_L/L}) = \Gamma(X, \Omega_{X/K}) \otimes_K L \implies g(X_L) = g(X).$$

(3) In particular, if $(E, O)$ is an elliptic curve over $K$, then $(E_L, O)$ is an elliptic curve over $L$, for any field extension $L/K$.
(4) If $K = \mathbf{C}$, then the set of complex points $X(\mathbf{C})$ has a natural structure of a compact Riemann surface and $\Gamma(X, \Omega_{X/\mathbf{C}}) = \Omega^1(X(\mathbf{C}))$, which implies that

$$g(X) = g_{an}(X(\mathbf{C})) = g(X(\mathbf{C})).$$

**(1.1.5) Notation.** Let $X$ be as in 1.1.4.

(1) The field of rational functions on $X$ will be denoted by $R(X)$.
(2) If $K = \overline{K}$ is algebraically closed, then the abelian group of divisors on $X$ is defined as

$$\mathrm{Div}(X) = \{\sum n_P(P) \,|\, n_P \in \mathbf{Z}, P \in X(K), \text{ the sum is finite}\}.$$

The degree of a divisor $D = \sum n_P(P)$ is defined to be $\deg(D) = \sum n_P \in \mathbf{Z}$. The divisor $D$ is *effective* (notation: $D \geq 0$) if $n_P \geq 0$ for all $P$.
(3) If $K$ is a perfect field, then the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ of $K$ acts on $\mathrm{Div}(X_{\overline{K}})$ (through its action on $X(\overline{K})$). The abelian group of divisors on $X$ is defined as the subgroup of $G_K$-invariant divisors on $X_{\overline{K}}$:

$$\mathrm{Div}(X) = \mathrm{Div}(X_{\overline{K}})^{G_K}.$$

We denote by $\deg_K$ the restriction of the degree map $\deg : \mathrm{Div}(X_{\overline{K}}) \longrightarrow \mathbf{Z}$ to $\mathrm{Div}(X)$; its kernel will be denoted by $\mathrm{Div}^0(X) = \mathrm{Ker}(\deg_K)$.

(4) If $K$ is not perfect, then one must use a scheme-theoretical language:

$$\mathrm{Div}(X) = \{\sum n_x(x) \,|\, n_x \in \mathbf{Z}, x \in |X|, \text{ the sum is finite}\},$$

where $|X|$ denotes the set of closed points of $X$ (if $K$ is perfect, then closed points of $X$ correspond to $G_K$-orbits in $X(\overline{K})$). The degree of a divisor is defined as

$$\deg_K(\sum n_x(x)) = \sum n_x \cdot [k(x) : K],$$

where $k(x)$ is the residue field of $x$.

(5) Each (non-zero) rational function $f \in R(X)^*$ has a divisor $\mathrm{div}(f) \in \mathrm{Div}(X)$, which has degree zero. One defines the abelian group $Cl(X)$ of divisor classes on $X$ (resp. its subgroup $Cl^0(X)$ of divisor classes of degree zero) as in the analytic case (see I.3.9).

(6) For any field extension $L/K$, a divisor $D \in \mathrm{Div}(X)$ defines a divisor $D_L \in \mathrm{Div}(X_L)$. If $D = \mathrm{div}(g)$ is principal, so is $D_L = \mathrm{div}(g_L)$ (where $g_L = g$, but considered as an element of the field $R(X_L) \supset R(X)$).

**(1.1.6)** If $K$ is perfect and $X$ has a $K$-rational point, then the canonical maps

$$Cl(X) \longrightarrow Cl(X_{\overline{K}})^{G_K}, \qquad Cl^0(X) \longrightarrow Cl^0(X_{\overline{K}})^{G_K}$$

are isomorphisms (but we are not going to use this fact).

**(1.1.7) The Riemann-Roch Theorem.** Let $X$ be as in 1.1.4. For each divisor $D \in \mathrm{Div}(X)$, put

$$L(D) = \{0\} \cup \{f \in R(X)^* \,|\, D + \mathrm{div}(f) \geq 0\}, \qquad \ell(D) = \dim_K L(D) \quad (< \infty).$$

(1) If $\deg_K(D) < 0$, then $L(D) = \{0\}$ and $\ell(D) = 0$ (as $\deg_K(\mathrm{div}(f)) = 0$).

(2) If $g \in R(X)^*$ and $D' = D + \mathrm{div}(g)$, then the map $f \mapsto fg$ defines an isomorphism of vector spaces $L(D') \xrightarrow{\sim} L(D)$; in particular, $\ell(D)$ depends only on the class of the divisor $D$ in $Cl(X)$.

(3) The rational differentials on $X$ form a vector space $\Omega_{R(X)/K}$ over $R(X)$ of dimension one. If $\omega, \omega' \in \Omega_{R(X)/K} - \{0\}$, then $\omega' = g\omega$ for some $g \in R(X)^*$; it follows that the class of the divisor $\mathrm{div}(\omega') = \mathrm{div}(\omega) + \mathrm{div}(g)$ is independent of any choices; it is the *canonical class* $\mathcal{K} \in Cl(X)$ of $X$.

(4) The map

$$L(\mathrm{div}(\omega)) \longrightarrow \Gamma(X, \Omega_{X/K}), \qquad f \mapsto f\omega$$

is an isomorphism; thus $\ell(\mathcal{K}) = g(X) = g$.

(5) The Riemann-Roch Theorem states that, for each $D \in \mathrm{Div}(X)$,

$$\ell(D) - \ell(\mathcal{K} - D) = 1 - g + \deg_K(D).$$

(6) Letting $D = \mathcal{K}$ (i.e. $D = \mathrm{div}(\omega)$ as in (3)), then we obtain

$$\deg_K(\mathcal{K}) = \deg_K(\mathrm{div}(\omega)) = 2g - 2.$$

(7) If $\deg_K(D) > 2g - 2$, then $\deg_K(\mathcal{K} - D) < 0$, which implies that $\ell(\mathcal{K} - D) = 0$ (by (1)), hence

$$\ell(D) = 1 - g + \deg_K(D).$$

## 1.2 The group law

**(1.2.1) Proposition.** *Let $(E, O)$ be an elliptic curve over $K$. Then the map*

$$\begin{aligned} E(K) &\longrightarrow Cl^0(E) \\ P &\mapsto \text{ the class of } (P) - (O) \end{aligned}$$

*is bijective (hence the same formula defines a bijection $E(L) \xrightarrow{\sim} Cl^0(E_L)$, for any field over $L \supset K$).*

*Proof.* (cf. [Si 1], Prop. III.3.4, if $K$ is perfect). *Injectivity:* assume that $P, Q \in E(K)$ and $(P) - (O) = (Q) - (O) + \mathrm{div}(f)$ for some $f \in R(E)^*$. If $P \neq Q$, then $\mathrm{div}(f) = (P) - (Q) \neq 0$. This implies that $f$ defines a non-constant rational map (hence a morphism) $f : E \longrightarrow \mathbf{P}^1_K$ of degree $\deg(f) = 1$. It follows that $f$ is an isomorphism $f : E \xrightarrow{\sim} \mathbf{P}^1_K$, which contradicts the fact that $g(E) = 1 \neq 0 = g(\mathbf{P}^1_K)$; thus $P = Q$.
*Surjectivity:* if $D \in \mathrm{Div}^0(E)$, then the Riemann-Roch Theorem implies that $\ell(D + (O)) = 1$; fixing $f \in L(D + (O)) - \{0\}$, then $D' := D + (O) + \mathrm{div}(f) \geq 0$ is an effective divisor of degree $\deg_K(D') = 1$, hence $D' = (P)$ for a $K$-rational point $P \in E(K)$. As $D = (P) - (O) - \mathrm{div}(f)$, the class of $D$ coincides with that of $(P) - (O)$.

**(1.2.2) Corollary.** (i) *The addition "+" on $Cl^0(E)$ induces the structure of an abelian group $(E(K), \boxplus)$ on $E(K)$, with neutral element $O$, characterized by*

$$P \boxplus Q = R \iff (\exists f \in R(E)^*) \quad (P) + (Q) = (R) + (O) + \mathrm{div}(f).$$

(ii) *For any field extension $L/K$, the group law induced on $E(L)$ by the bijection $E(L) \xrightarrow{\sim} Cl^0(E_L)$ restricts to the group law $\boxplus$ on $E(K)$.*

**(1.2.3) Smooth plane cubics.** Let $E \subset \mathbf{P}^2_K$,

$$E : F(X, Y, Z) = 0 \qquad\qquad (F \in K[X, Y, Z] \text{ homogeneous of degree } 3)$$

be a smooth projective plane cubic curve and $O \in E(K)$. The pair $(E, O)$ is an elliptic curve over $K$, since $g(E) = (3-1)(3-2)/2 = 1$ (irreducibity of $E$ over $\overline{K}$ follows from Bézout's Theorem; cf. 3.7.5(i)). We claim that the abstract group law $\boxplus$ on $(E, O)$ is given by the formula (I.10.1.1.1): if $L$ is a field containing $K$ and $P, Q \in E(L)$, let

$$\ell : aX + bY + cZ = 0, \qquad \ell' : a'X + b'Y + c'Z = 0 \qquad\qquad (a, \ldots, c' \in L)$$

be the equations of the lines $\overline{PQ}$ and $\overline{(P * Q)O}$, respectively. The rational function $f = \ell/\ell' \in R(E_L)^*$ has divisor

$$\mathrm{div}(f) = (P) + (Q) + (P * Q) - (P * Q) - (O) - ((P * Q) * O) = (P) + (Q) - (O) - ((P * Q) * O),$$

hence

$$(P * Q) * O = P \boxplus Q$$

as claimed (note that, in general, the inverse $-P$ with respect to the group law is *not* equal to $P * O$; cf. I.10.1.4).

This discussion applies, in particular, to the pair $(C, O)$ from the next Proposition.

**(1.2.4) Proposition (The generalized Weierstrass equation).** *Let $(E, O)$ be an elliptic curve over $K$. There exist rational functions $x, y \in R(E)^*$ such that the map*

$$\begin{aligned} \alpha : E &\longrightarrow \mathbf{P}^2_K \\ P &\mapsto (x(P) : y(P) : 1) \qquad\qquad (P \neq O) \\ O &\mapsto O = (0 : 1 : 0) \end{aligned}$$

*induces an isomorphism between $(E,O)$ and $(C,O)$, where $C$ is the (smooth) cubic projective curve*

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.2.4.1}$$

*for some $a_j \in K$ (we say that $C$ is an elliptic curve in a* **generalized Weierstrass form**. *(Conversely, if $C$ in (1.2.4.1) is smooth, then $(C,O)$ is an elliptic curve over $K$, by 1.2.3.)*

*Proof.* (cf. [Si 1], Prop. III.3.1). It follows from the Riemann-Roch Theorem that $\ell(n(O)) = n$ for each $n \geq 1$ ($\Longrightarrow L((O)) = K$). In particular, there exist rational functions $x \in L(2(O)) - K$ (an analogue of $\wp(z)$) and $y \in L(3(O)) - L(2(O))$ (an analogue of $\wp'(z)$). The triple $x, y, 1$ forms a basis of $L(3(O))$ and defines a non-constant rational map

$$(x : y : 1) : E - - - - \succ \mathbf{P}^2_K \ ,$$

which extends to a (unique) morphism $\alpha : E \longrightarrow \mathbf{P}^2_K$, since $E$ is a regular curve and $\mathbf{P}^2_K$ is projective. As

$$x^2 \in L(4(O)) - L(3(O)), \qquad xy \in L(5(O)) - L(4(O)),$$

it follows that the rational functions $1, x, y, x^2, xy$ form a basis of $L(5(O))$. Going one step further, we have

$$x^3, y^2 \in L(6(O)) - L(5(O)), \qquad \dim_K(L(6(O))/L(5(O))) = 1,$$

which implies that there exists a linear relation

$$x^3 - ay^2 \in L(5(O)) \qquad\qquad (a \in K^*).$$

Replacing $x$ (resp. $y$) by $ax$ (resp. $a^2y$), we can assume that $a = 1$; thus there exists a linear relation

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \qquad\qquad (a_j \in K), \tag{1.2.4.2}$$

which is an algebraic version of the differential equation I.7.1.8 satisfied by the Weierstrass function $\wp(z)$. In particular, the morphism $\alpha$ factors as

$$E \xrightarrow{\beta} C \hookrightarrow \mathbf{P}^2_K,$$

where $C$ is the projectivization of (1.2.4.2), i.e. the projective curve (1.2.4.1) (where $x = X/Z$ and $y = Y/Z$, as usual). It is easy to see that the polynomial $f(x,y)$ is irreducible in $\overline{K}[x,y]$; thus $C$ is a reduced and geometrically irreducible curve.

The affine coordinates $x, y \in R(C)$ define rational functions on $C$, hence rational maps $x, y : C - - - \succ \mathbf{P}^1_K$ . As before, the composite rational maps $x \circ \beta, y \circ \beta$ (again defined by $x, y \in R(E)$) extend to morphisms $x \circ \beta, y \circ \beta : E \longrightarrow \mathbf{P}^1_K$, of degrees 2 and 3, respectively; thus $\deg(\beta) = [R(E) : \beta^* R(C)] = 1$, as it divides both 2 and 3. This means that $\beta$ is birational, i.e. induces an isomorphism $E \xrightarrow{\sim} \widetilde{C}$, where $\widetilde{C}$ is the normalization (canonical desingularization) of $C$. We claim that $C$ is smooth over $K$ (which implies that $\widetilde{C} = C$, concluding the proof): if not, then the discussion in 1.3.4-5 below shows that $\widetilde{C}_L \xrightarrow{\sim} \mathbf{P}^1_L$ over a suitable finite extension $L \supset K$, which contradicts the fact that $g(\widetilde{C}_L) = g(E_L) = 1 \neq 0 = g(\mathbf{P}^1_L)$.

**(1.2.5)** The affine curve $C \cap \{Z \neq 0\} = C - \{O\}$ is given by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2.5.1}$$

(where $x = X/Z, y = Y/Z$). If $char(K) \neq 2$ (resp. $char(K) \neq 3$), one can simplify (1.2.5.1) by completing the square (resp. the cube), i.e. by the substitution $y + (a_1x + a_3)/2 \mapsto y$ (resp. $x + a_2/3 \mapsto x$). As a result, we obtain the following simplified forms of (1.2.5.1).

(i) If $char(K) \neq 2, 3$, then

$$y^2 = x^3 + a_4x + a_6. \tag{1.2.5.2}$$

(ii) If $char(K) = 3$, then

$$y^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{1.2.5.3}$$

(iii) If $char(K) = 2$, then

$$y^2 + a_1xy + a_3y = x^3 + a_4x + a_6. \tag{1.2.5.4}$$

**(1.2.6) The variable (= general = tautological) points. Examples:** (i) Let $(E, O) = (C, O)$ be an elliptic curve given by the generalized Weierstrass equation (1.2.4.1). We would like to consider a "general point" $(x, y)$ on $E - \{O\}$, whose coordinates would satisfy the equation (1.2.5.1) (and its consequences), but no other polynomial equations with coefficients in $K$. Such a point can be constructed as follows: put

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

and let

$$A = K[x, y]/(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6) = K[x, y]/(f(x, y))$$

be the ring of functions on the affine curve $E - \{O\} = \mathrm{Spec}(A)$; its field of fractions is equal to the field of rational functions on $E$: $R(E) = \mathrm{Frac}(A)$. Let $\overline{x}, \overline{y}$ be, respectively, the images of $x, y$ in $A$; the "tautological point" (or "general point") of $E$ is the point with affine coordinates

$$(\overline{x}, \overline{y}) \in (E - \{O\})(A) \subset (E - \{O\})(\mathrm{Frac}(A)) \subset E(\mathrm{Frac}(A)) = E(R(E)).$$

(ii) Sometimes we shall use several "independent" general points of $E$: for $j = 1, \dots, n$, put

$$A_j = K[x_j, y_j]/(f(x_j, y_j)), \qquad B = A_1 \otimes_K \cdots \otimes_K A_n = K[x_1, y_1, \dots, x_n, y_n]/(f(x_1, y_1), \dots, f(x_n, y_n))$$

and denote by $\overline{x}_j$ (resp. $\overline{y}_j$) the image of $x_j$ (resp. of $y_j$) in $B$; then

$$\mathrm{Spec}(B) = (E - \{O\})^n = (E - \{O\}) \times_K \cdots \times_K (E - \{O\}) \subset \underbrace{E \times_K \cdots \times_K E}_{n \text{ factors}} = E^n, \qquad \mathrm{Frac}(B) = R(E^n)$$

and the "tautological point" of $E^n$

$$((\overline{x}_1, \overline{y}_1), \dots, (\overline{x}_n, \overline{x}_n)) \in (E - \{O\})^n(B) \subset (E - \{O\})^n(\mathrm{Frac}(B)) \subset E^n(\mathrm{Frac}(B)) = E^n(R(E^n))$$

can be viewed as an $n$-tuple of independent general points of $E$.
(iii) This construction makes sense for an arbitrary reduced irreducible scheme $X$: if $\mathrm{Spec}(A) \subset X$ is any (non-empty) open affine subset, then $A$ is an integral domain and the ring of rational functions on $X$ is a field, equal to $R(X) = \mathrm{Frac}(A)$. The canonical maps

$$\mathrm{Spec}(R(X)) = \mathrm{Spec}(\mathrm{Frac}(A)) \longrightarrow \mathrm{Spec}(A) \hookrightarrow X$$

then define the tautological point $P \in X(R(X))$.

**(1.2.7) Theorem ($E$ is a "commutative group scheme" over $K$).** (i) *There exist (unique) morphisms $m : E \times_K E \longrightarrow E$ and $\iota : E \longrightarrow E$ such that, for each field $L \supset K$ and all $P, Q \in E(L)$,*

$$P \boxplus Q = m(P, Q), \qquad -P = [-1]P = \iota(P).$$

(ii) **"Associativity".** *The following diagram is commutative:*

$$\begin{array}{ccc} E \times_K E \times_K E & \xrightarrow{\mathrm{id} \times m} & E \times_K E \\ \downarrow{\scriptstyle m \times \mathrm{id}} & & \downarrow{\scriptstyle m} \\ E \times_K E & \xrightarrow{m} & E. \end{array}$$

(iii) **"Commutativity".** *Let $s : E \times_K E \longrightarrow E \times_K E$ be the morphism $s(P,Q) = (Q,P)$; then $m \circ s = m$.*
(iv) **"Inverse".** *The composite morphism*

$$E \xrightarrow{\Delta} E \times_K E \xrightarrow{\mathrm{id}\times\iota} E \times_K E \xrightarrow{m} E$$

*(where $\Delta(P) = (P,P)$ is the diagonal map) is the constant map with value $O$.*

*Proof.* (i) (cf. [Si 1], Thm. III.3.6, if $K$ is perfect). *The inverse:* thanks to 1.2.4, we can assume that $(E,O) = (C,O)$, in which case $O$ is an inflection point of $E$, hence $-P = O * P$ (cf. I.10.1.4). It follows that, if $P = (x_P, y_P) \in (E - \{O\})(L)$, then $-P$ lies on the vertical line $x - x_P = 0$, hence

$$-(x_P, y_P) = (x_P, -y_P - a_1 x_P - a_3). \tag{1.2.7.1}$$

The formula

$$\iota(x,y) = (x, -y - a_1 x - a_3)$$

defines a morphism $E - \{O\} \longrightarrow E - \{O\}$, hence a rational map

$$E - - \succ E\ ,$$

which automatically extends to a (unique) morphism $\iota : E \longrightarrow E$. As $\iota$ is non-constant, it is surjective, hence $\iota(O) = O$, proving that $-P = \iota(P)$ for all $P \in E(L)$ (and all fields $L \supset K$).

One can see directly (without using the formula (1.2.7.1)) that the inverse map is induced, on the points of a suitable (non-empty) open subset $U \subset E - \{O\}$, by a morphism $\iota_U : U \longrightarrow E - \{O\}$: let $P = (\overline{x}, \overline{y}) \in (E - \{O\})(R(E))$ be the tautological point of $E$ constructed in 1.2.6(i); then the point $-P \in (E - \{O\})(R(E))$ (defined using the group law on $E_{R(E)}$) is a morphism $-P : \mathrm{Spec}(R(E)) \longrightarrow E - \{O\}$. The coordinates of $-P$ are rational functions on $E - \{O\}$; removing from $E - \{O\}$ the union of their poles (which turns out to be empty in this case, as $-P = (\overline{x}, -\overline{y} - a_1\overline{x} - a_3)$) we obtain the sought for morphism $\iota_U : U \longrightarrow E - \{O\}$. Note that, in this argument, it was not necessary to assume that $(E,O) = (C,O)$; one could have used the abstract definition of the tautological point from 1.2.6(iii).
*The sum $\boxplus$:* A similar argument applied to two independent points

$$((\overline{x}_1, \overline{y}_1), (\overline{x}_2, \overline{x}_2)) \in (E - \{O\})^2(R(E \times_K E))$$

shows that there exists a (non-empty) open subset $U \subset E \times_K E$ and a morphism $m_U : U \longrightarrow E$ such that, for all fields $L \supset K$ and all $P, Q \in U(L)$, we have $P \boxplus Q = m_U(P,Q)$. They are several ways to conclude the argument; for example, one can assume that $(E,O) = (C,O)$, in which case the sum $(x_1,y_1) \boxplus (x_2,y_2)$ can be computed explicitly, as in I.7.5.7. The resulting formulas show that the map $(P,Q) \mapsto P \boxplus Q$ is, indeed, defined by a morphism $m_U : U \longrightarrow E$, where $E \times_K E - U = \{(P,P)\} \cup \{(P,-P)\} \cup \{(P,O)\} \cup \{(O,P)\}$. One then shows, again by an explicit calculation, that $\boxplus$ is defined by a morphism on a suitable open set containing $E \times_K E - U$ (see [Si 1], 3.6.1). There is an alternative argument which uses translation maps (see [Si 1], 3.6); in our case one has to be careful, as the field $K$ is not necessarily perfect; hovewer, the set of points $E(K^{sep})$ defined over the separable closure of $K$ is dense in $E$ (as $E$ is smooth over $K$), which is sufficient for the argument.
(ii) Let $L = R(E \times_K E \times_K E) = R(E^3)$ be the field of rational functions on $E^3$. As in 1.2.6(ii), we have three independent general points $P_j = (\overline{x}_j, \overline{y}_j) \in E(L)$ $(j = 1,2,3)$ of $E$, defining the tautological point $(P_1,P_2,P_3) : \mathrm{Spec}(L) \longrightarrow E^3$. As the group operation $\boxplus$ is associative on $E(L)$, we have equalities

$$\begin{gathered} m \circ (m \times \mathrm{id}) \circ (P_1,P_2,P_3) = m \circ (P_1 \boxplus P_2, P_3) = (P_1 \boxplus P_2) \boxplus P_3 = P_1 \boxplus (P_2 \boxplus P_3) = \\ = m \circ (P_1, P_2 \boxplus P_3) = m \circ (\mathrm{id} \times m) \circ (P_1,P_2,P_3) \in E(L). \end{gathered}$$

Interpreting both sides as rational maps $E \times_K E \times_K E - - - - - \succ E$, it follows that the morphisms $m \circ (m \times \mathrm{id})$ and $m \circ (\mathrm{id} \times m)$ define the same rational map. As the target $E$ is projective (hence separated), the two morphisms must be equal. A similar argument proves (iii) and (iv).

**(1.2.8) Corollary.** (i) *For each $n \in \mathbf{Z}$, multiplication by $n$ (defined as in 0.5.0) on $E$ is given by a morphism $[n] = [n]_E : E \longrightarrow E$.*
(ii) *For each $P \in E(K)$, there is a morphism $\tau_P : E \longrightarrow E$ (the "translation map") such that, for each field $L \supset K$ and each point $Q \in E(L)$, $\quad P \boxplus Q = \tau_P(Q)$.*

*Proof.* (i) $[0]$ is the constant map equal to $O$ and $[1] = \mathrm{id}$. For $n > 1$, one defines inductively $[n] = m \circ ([n-1] \times \mathrm{id}) \circ \Delta$, where $\Delta$ is the diagonal map $\Delta : E \longrightarrow E \times_K E$, $\Delta(P) = (P, P)$. For $n < 0$, $[n] = \iota \circ [-n]$.
(ii) $\tau_P$ is defined as the composite morphism

$$E = \mathrm{Spec}(K) \times_K E \xrightarrow{P \times \mathrm{id}} E \times_K E \xrightarrow{m} E.$$

**(1.2.9) Exercise.** *Let $(E, O)$ be as in 1.2.3.*
(i) *If $O$ is an inflection point of $E$, show that there exists a linear change of homogeneous coordinates defined over $K$ transforming $(E, O)$ into $(C, O)$ of the form (1.2.4.1).*
(ii) *If $O$ is not an inflection point of $E$, choose new homogeneous coordinates $(X : Y : Z)$ in such a way that $O = (1 : 0 : 0)$, $\{Z = 0\}$ is the tangent line to $E$ at $O$, $\{Z = 0\} \cap E = 2(O) + (P)$, where $P = (0 : 1 : 0)$ and $\{X = 0\}$ is the tangent line to $E$ at $P$. Show that the (rational) change of variables $x' = x$, $y' = xy$ ($x = X/Z$, $y = Y/Z$, as usual) transforms $E$ into a smooth projective cubic curve $E'$ and $P$ into an inflection point $P'$ of $E'$ (see [Cl], 2.4).*

## 1.3 Non-smooth Generalized Weierstrass Equations

**(1.3.1)** Assume that the projective plane curve

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

(where $a_j \in K$) is not smooth, i.e. that there exists at least one singular (= non-smooth) point $S \in C(\overline{K})$.

If there were another singular point $T \in C(\overline{K})$, then the intersection of the line $\overline{ST}$ with $C$ would contradict Bézout's Theorem; thus $S$ is unique.

In particular, $S$ is fixed by any element of the automorphism group $\mathrm{Aut}(\overline{K}/K)$, which implies that $K(S)$ (the field of definition of $S$) is a purely inseparable extension of $K$.

**(1.3.2)** The point $S = (x_S, y_S)$ necessarily lies on the affine curve $C_{\mathrm{aff}} = C - \{O\}$, given by the equation

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

hence

$$\begin{aligned} \partial f/\partial x(S) &= a_1y_S - 3x_S^2 - 2a_2x_S - a_4 = 0, \\ \partial f/\partial y(S) &= 2y_S + a_1x_S + a_3 = 0, \end{aligned}$$

which implies that

$$\begin{aligned} -y_S^2 &= x_S^3 + a_2x_S^2 + a_4x_S + a_6, \\ 2(3x_S^2 + 2a_2x_S + a_4) + a_1(a_1x_S + a_3) &= 0. \end{aligned}$$

If $char(K) \neq 2, 3$, these equations show that

$$[K(S) : K] \leq [K(S) : K(x_S)] \cdot [K(x_S) : K] \leq 2 \cdot 2 = 4,$$

hence $S \in C(K)$ is defined over $K$.

On the other hand, if $K$ is a non-perfect field of characteristic $p = 2$ (resp. $p = 3$) and $a \in K^*$, $a \notin K^{*p}$, then the curve

$$y^2 = x^3 + a$$

has a non-smooth point $S = (0, a^{1/2})$ (resp. $S = (-a^{1/3}, 0)$) defined over a purely inseparable extension $K(a^{1/p})/K$ of degree $p$.

**(1.3.3)** Assume, from now on, that $S \in C(K)$ is defined over $K$. Applying the change of variables $x \mapsto x - x_S, y \mapsto y - y_S$, we can assume that $S = (0, 0)$, which implies that $a_6 = a_3 = a_4 = 0$, hence $C_{\text{aff}}$ is given by

$$y^2 + a_1xy - a_2x^2 = x^3. \tag{1.3.3.1}$$

The tangent cone to $C$ at $S$ is given by the vanishing of the quadratic form on the L.H.S. of (1.3.3.1). In other words, writing $y = \lambda x$, then the roots of

$$Q(\lambda) = \lambda^2 + a_1\lambda - a_2 = 0 \tag{1.3.3.2}$$

are the slopes of the tangents to the various branches of $C$ passing through $S$.

The geometry of $C$ strongly depends on the nature of the solutions of (1.3.3.2).

**(1.3.4) The multiplicative case.** Assume that the polynomial $Q(\lambda)$ has two distinct roots $\lambda_1, \lambda_2 \in \overline{K}$. Then $K(\lambda_1, \lambda_2)$ is either equal to $K$, or is a separable quadratic extension of $K$.

Let $L \supset K(\lambda_1, \lambda_2)$ be any extension of $K$ over which $Q$ splits. Then the base change of $C_{\text{aff}}$ to $L$ is given by

$$(C_L)_{\text{aff}} : (y - \lambda_1 x)(y - \lambda_2 x) = x^3$$

and the rational function

$$t = \frac{y - \lambda_1 x}{y - \lambda_2 x} = \frac{u}{v} \in R(C_L) \tag{1.3.4.1}$$

on $C_L$ – viewed as a rational map to $\mathbf{P}^1_L$ – admits an inverse, which is a birational *morphism*

$$\mathbf{P}^1_L \longrightarrow C_L, \qquad (u : v) \mapsto \left( \frac{u - v}{\lambda_2 - \lambda_1} : \frac{\lambda_2 u - \lambda_1 v}{\lambda_2 - \lambda_1} : \left( \frac{u - v}{\lambda_2 - \lambda_1} \right)^3 \frac{1}{uv} \right), \qquad (1 : 0), (0 : 1) \mapsto S, \tag{1.3.4.2}$$

which identifies $\mathbf{P}^1_L$ with the normalization of $C_L$. This morphism has a very simple geometric description: $\mathbf{P}^1_L$ parametrizes the set of lines in $\mathbf{P}^2_L$ containing $S$ (with the point $0 = (0 : 1) \in \mathbf{P}^1(L)$ (resp. $\infty = (1 : 0) \in \mathbf{P}^1(L)$) corresponding to the tangent line $y = \lambda_1 x$ (resp. $y = \lambda_2 x$) at $S$). Each such line $\ell$ intersects $C$ at $S$ with intersection multiplicity $\geq 2$; the map (1.3.4.2) associates to $\ell$ its third intersection point with $C$.

**(1.3.5) The additive case.** Assume that $Q(\lambda)$ has a double root $\lambda \in \overline{K}$. Then $K(\lambda)$ is either equal to $K$, or is a purely inseparable quadratic extension of $K$ (the latter case can occur only if $K$ is a non-perfect field of characteristic $char(K) = 2$). It follows that $a_1 = 2b_1$ for some $b_1 \in K$; the change of variables $y \mapsto y - b_1 x$ reduces to the case

$$C_{\text{aff}} : y^2 - b_2x^2 = x^3, \qquad b_2 = \lambda^2 \in K, \qquad 2b_2 = 0.$$

Over any field $L \supset K(\lambda)$, we have

$$(C_L)_{\text{aff}} : (y - \lambda x)^2 = x^3$$

and the rational function

$$t = \frac{x}{y - \lambda x} = \frac{u}{v} \tag{1.3.5.1}$$

on $C_L$ has an inverse, which is a morphism

$$\mathbf{P}^1_L \longrightarrow C_L, \qquad (u:v) \mapsto \left(\frac{u^2}{v^2} : \frac{u^3}{v^3} + \lambda\frac{u^2}{v^2} : 1\right), \qquad (1:0) \mapsto S \tag{1.3.5.2}$$

identifying $\mathbf{P}^1_L$ with the normalization of $C_L$. This morphism has the same geometric description as the map (1.3.4.2).

**(1.3.6) The group law on the smooth part of $C$.** If $L \supset K$ is an extension of $K$, it is tempting to use the same geometric construction as in 1.2.3 to define an abelian group law on $C(L)$ (with $O = (0:1:0)$ as a neutral element). This does not quite work if the line $\ell$ contains the singular point $S$, which means that we have to consider only the smooth part of $C(L)$

$$C^{\mathrm{sm}}(L) = C(L) - \{S\}$$

and lines $\ell \subset \mathbf{P}^2_L$ that do not contain $S$. If $Q_1, Q_2 \in C^{\mathrm{sm}}(L)$, then the line $\ell = \overline{Q_1Q_2}$ (defined to be the tangent to $C$ at $Q_1$ if $Q_1 = Q_2$) does not contain $S$ – by Bézout's Theorem – and the third intersection $Q_3$ of $\ell$ with $C$ also lies in $C^{\mathrm{sm}}(L)$. We put

$$Q_3 := Q_1 * Q_2, \qquad Q_1 \boxplus Q_2 := O * (Q_1 * Q_2). \tag{1.3.6.1}$$

Does (1.3.6.1) define an abelian group structure on $C^{\mathrm{sm}}(L)$ (with neutral element $O = (0:1:0)$)? Let us analyze the situation in more detail.

**(1.3.7) The split multiplicative case.** Assume that we are in the multiplicative case 1.3.4 and that $L \supset K(\lambda_1, \lambda_2)$. In the homogeneous coordinates $(U_1 : U_2 : Z)$, where $U_j = Y - \lambda_j X$, the curve $C_L$ is given by

$$C_L : (\lambda_2 - \lambda_1)^3 U_1 U_2 Z = (U_1 - U_2)^3, \qquad S = (0:0:1)$$

and the rational function (1.3.4.1) defines a bijection

$$t = \frac{U_1}{U_2} : C^{\mathrm{sm}}(L) \xrightarrow{\sim} \mathbf{P}^1(L) - \{0, \infty\} = L^*.$$

Assume that the line $\ell : Z = aU_1 + bU_2$ intersects $C^{\mathrm{sm}}$ at three points $Q_1, Q_2, Q_3$. Then

$$(t-1)^3 - (\lambda_2 - \lambda_1)^3 t(at+b) = (t - t(Q_1))(t - t(Q_2))(t - t(Q_3)),$$

which implies that

$$t(Q_1)t(Q_2)t(Q_3) = 1,$$

hence $t$ defines an isomorphism of abelian groups

$$(C^{\mathrm{sm}}(L), \boxplus) \xrightarrow{\sim} (L^*, \times).$$

**(1.3.8) The split additive case.** Assume that we are in the additive case 1.3.5 and that $L \supset K(\lambda)$. In the homogeneous coordinates $(X : Y : Z)$, the curve $C_L$ is given by

$$C_L : (Y - \lambda X)^2 Z = X^3, \qquad S = (0:0:1)$$

and the rational function (1.3.5.1) defines a bijection

$$t = \frac{X}{Y - \lambda X} : C^{\mathrm{sm}}(L) \xrightarrow{\sim} \mathbf{P}^1(L) - \{\infty\} = L.$$

Assume that the line $\ell : Z = aX + bY$ intersects $C^{\mathrm{sm}}$ at three points $Q_1, Q_2, Q_3$. Then

$$t^3 - (at+b) = (t - t(Q_1))(t - t(Q_2))(t - t(Q_3)),$$

which implies that

$$t(Q_1) + t(Q_2) + t(Q_3) = 0,$$

hence $t$ defines an isomorphism of abelian groups

$$(C^{\mathrm{sm}}(L), \boxplus) \xrightarrow{\sim} (L, +).$$

**(1.3.9) The non-split multiplicative case.** Assume that we are in the multiplicative case 1.3.4 and that $K' := K(\lambda_1, \lambda_2)$ is not equal to $K$. Then $K'/K$ is a Galois extension of degree 2; let $\sigma$ be the non-trivial element of $\mathrm{Gal}(K'/K)$. Then $\lambda_2 = \sigma(\lambda_1)$ and the discussion in 1.3.7 implies that the rational function

$$t = \frac{y - \lambda_1 x}{y - \sigma(\lambda_1)x}$$

induces an isomorphism of abelian groups

$$t : C^{\mathrm{sm}}(K) \xrightarrow{\sim} \{w/\sigma(w) \,|\, w \in (K')^*\} = \mathrm{Ker}\left(N_{K'/K} : (K')^* \longrightarrow K^*\right) \tag{1.3.9.1}$$

(the last equality by Hilbert's Theorem 90, as in 0.4.2.0). The group on the R.H.S. of (1.3.9.1) is usually referred to as the "twisted multiplicative group". We have already encountered it in our discussion of the group of points on the circle $x^2 + y^2 = 1$ in 0.4.2.

**(1.3.10) The non-split additive case.** Assume that we are in the additive case 1.3.5 and that $K' := K(\lambda)$ is not equal to $K$. Then $char(K) = 2$ and $K'/K$ is a purely inseparable extension of degree 2, with $\lambda^2 = b_2 \in K$.

For $Q = (x, y) \in C^{\mathrm{sm}}_{\mathrm{aff}}(K)$, write the value $t(Q)$ in the basis $1, -\lambda$ of $K'/K$:

$$t(Q) = \frac{x}{y - \lambda x} = \frac{y - \lambda x}{x^2} = \alpha - \lambda\beta, \qquad \alpha, \beta \in K.$$

Then

$$\alpha^2 - b_2\beta^2 = (\alpha - \lambda\beta)^2 = \frac{(y - \lambda x)^2}{x^4} = \frac{1}{x} = \beta,$$

and the discussion in 1.3.8 implies that $t$ induces an isomorphism of abelian groups

$$t : C^{\mathrm{sm}}(K) \xrightarrow{\sim} \left(\{\alpha - \lambda\beta \,|\, \alpha, \beta \in K,\, \alpha^2 - b_2\beta^2 = \beta\}, +\right)$$

(the "twisted additive group").

**(1.3.11) Exercise ([Be]).** *Let $Q \subset \mathbf{P}^2_K$ be a smooth conic and $L \subset \mathbf{P}^2_K$ a line (both defined over $K$). Fix a point $O \in Q(K) - L(K)$.*
(i) *Show that the recipe (I.10.1.1.1) applied to the* **reducible** *cubic curve $Q \cup L \subset \mathbf{P}^2_K$ defines an abelian group law on $Q(K) - L(K)$.*
(ii) *Describe the structure of this group (it depends on the nature of the intersection $Q \cap L$).*
(iii) *What is the relation to the group law on the circle (0.1.1)?*

**(1.3.12) Exercise.** *Relate the discussion in 1.3.7-8 to (an algebraic version of) I.3.9.13(ii), using 1.3.4-5.*

## 2. Isogenies (definitions and examples)

### 2.1 Definitions and basic properties

**(2.1.1) Definition.** *Let $(E,O)$ and $(E',O')$ be elliptic curves over $K$. An* **isogeny** *$\lambda : E \longrightarrow E'$ is a non-constant morphism of curves over $K$ satisfying $\lambda(O) = O'$ (hence $\lambda$ induces an isogeny $\lambda_L = \lambda \times \mathrm{id} : E_L = E \otimes_K L \longrightarrow E'_L = E' \otimes_K L$, for any field $L \supset K$). The* **degree** *of the isogeny $\lambda$ is the degree of the field extension $R(E)/\lambda^*(R(E'))$.*

**(2.1.2) Proposition.** *If $\lambda : E \longrightarrow E'$ is an isogeny, then the induced map on $K$-rational points $\lambda : E(K) \longrightarrow E'(K)$ is a homomorphism of abelian groups.*

*Proof.* (cf. [Si 1], Thm. III.4.8, if $K$ is perfect). This follows from the commutative diagram

$$\begin{array}{ccc} E(K) & \xrightarrow{\lambda} & E'(K) \\ \downarrow\wr & & \downarrow\wr \\ Cl^0(E) & \xrightarrow{\lambda_*} & Cl^0(E'), \end{array}$$

where the map $\lambda_*$ is defined on the level of divisors by $\lambda_*(\sum n_P(P)) = \sum n_P(\lambda(P))$ if $K$ is perfect, and by $\lambda_*(\sum n_x(x)) = \sum n_x[k(x) : k(\lambda(x))](x)$ in general.

**(2.1.3) Proposition (Isogenies are "homomorphisms of groups schemes").** *If $\lambda : E \longrightarrow E'$ is an isogeny, then:*
(i) *$\lambda$ commutes with the group laws on $E$ and $E'$, i.e. the following diagram is commutative:*

$$\begin{array}{ccc} E \times_K E & \xrightarrow{\lambda\times\lambda} & E' \times_K E' \\ \downarrow m & & \downarrow m' \\ E & \xrightarrow{\lambda} & E'. \end{array}$$

(ii) $(\forall n \in \mathbf{Z}) \quad \lambda \circ [n]_E = [n]_{E'} \circ \lambda$.

*Proof.* The statement (i) is proved by the same argument as in 1.2.8(ii): let $L = R(E \times_K E)$ be the field of rational functions on $E \times_K E$ and $((\overline{x}_1, \overline{y}_1), (\overline{x}_2, \overline{y}_2)) \in (E \times_K E)(L)$ the tautological point of $E \times_K E$, defined in 1.2.6(ii). Applying 2.1.2 to $\lambda_L : E_L \longrightarrow E'_L$, we obtain

$$\lambda_L((\overline{x}_1, \overline{y}_1) \boxplus (\overline{x}_2, \overline{y}_2)) = \lambda_L(\overline{x}_1, \overline{y}_1) \boxplus \lambda_L(\overline{x}_2, \overline{y}_2) \in E'(L).$$

Interpreting both sides as rational maps $\beta : E \times_K E \dashrightarrow E'$, it follows that the morphisms $\lambda \circ m, m' \circ (\lambda \times \lambda) : E \times_K E \longrightarrow E'$ define the same rational map. As the target $E'$ is projective (hence separated), the morphisms $\lambda \circ m$ and $m' \circ (\lambda \times \lambda)$ must be equal. The statement (ii) follows from (i) by induction on $|n|$.

**(2.1.4) Notation.** For elliptic curves $E, E'$ over $K$ and a field $L \supset K$, we denote

$$\begin{aligned} \mathrm{Hom}_L(E,E') &= \{0\} \cup \{\lambda : E_L \longrightarrow E'_L \mid \lambda \text{ is an isogeny}\} \\ \mathrm{Isom}_L(E,E') &= \{\lambda \in \mathrm{Hom}_L(E,E') \mid \lambda \text{ is an isomorphism}\} = \{\lambda \in \mathrm{Hom}_L(E,E') \mid \deg(\lambda) = 1\} \\ \mathrm{End}_L(E) &= \mathrm{Hom}_L(E,E), \qquad \mathrm{Aut}_L(E) = \mathrm{Isom}_L(E,E), \end{aligned}$$

where 0 is the constant morphism with value $O'$. If $\lambda : E \longrightarrow E'$ is an isogeny, we put

$$\mathrm{Ker}(\lambda)(L) = \{P \in E(L) \mid \lambda(P) = O'\}.$$

**(2.1.5) Exercise.** *Show that $\mathrm{End}_L(E)$ is a ring with respect to the operations $\lambda \boxplus \mu$ and $\lambda\mu = \lambda \circ \mu$, where*

$$\lambda \boxplus \mu : E \xrightarrow{\Delta} E \times_K E \xrightarrow{\lambda\times\mu} E \times_K E \xrightarrow{m} E$$

*($\Delta(P) = (P, P)$ is the diagonal map). [Hint: The proof of one of the distributive laws requires 2.1.3.]*

**(2.1.6) Exercise.** *If $\lambda \in \mathrm{Hom}_L(E, E')$, $\mu \in \mathrm{Hom}_L(E', E'')$ and $\mu \circ \lambda = 0$, then $\lambda = 0$ or $\mu = 0$. In particular, the ring $\mathrm{End}_L(E)$ does not have zero divisors.*

**(2.1.7) Proposition.** *Let $k = \mathbf{Q}$ (resp. $k = \mathbf{F}_p$) if $char(K) = 0$ (resp. if $char(K) = p > 0$). If $E, E'$ are elliptic curves over $K$ and $\lambda \in \mathrm{Hom}_K(E, E')$, then there exists a subfield $K_0 \subset K$ of finite type over $k$, elliptic curves $E_0, E_0'$ over $K_0$ and an element $\lambda_0 \in \mathrm{Hom}_{K_0}(E_0, E_0')$ such that $\lambda = (\lambda_0)_K$ is the base change of $\lambda_0$.*

*Proof.* We take $K_0$ to be the field generated over $k$ by the coefficients of the (finitely many) polynomials defining $E, E'$ and $\lambda$.

**(2.1.8)** Assume that $(E, O)$ and $(E', O')$ are elliptic curves over $\mathbf{C}$ and $\lambda \in \mathrm{Hom}_{\mathbf{C}}(E, E') - \{0\}$ an isogeny. Fix isomorphisms $(E, O) \xrightarrow{\sim} (C, O)$, $(E', O') \xrightarrow{\sim} (C', O')$ (defined over $\mathbf{C}$) with elliptic curves in the form (1.2.4.1). The Abel-Jacobi maps from I.4.4.1 then define isomorphisms of Riemann surfaces $C(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}/L$, $C'(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}/L'$ (under which $O, O'$ correspond to 0), for suitable lattices $L, L' \subset \mathbf{C}$. The holomorphic map $\lambda^{an} : E(\mathbf{C}) \longrightarrow E'(\mathbf{C})$ (given by $\lambda$) then gives rise, via the above isomorphisms, to a non-constant holomorphic map $\mu : \mathbf{C}/L \longrightarrow \mathbf{C}/L'$ satisfying $\mu(0) = 0$, i.e. an isogeny in the analytic sense (cf. I.7.6.3). Conversely, any such $\mu$ is algebraic, i.e. comes from a (unique) isogeny $\lambda : E \longrightarrow E'$ (this follows from I.7.6.6(ii)). In particular, we have, in the notation of I.7.6.7,

$$\mathrm{End}_{\mathbf{C}}(E) = \mathrm{End}(\mathbf{C}/L).$$

**(2.1.9) Exercise.** *Let $E$ be an elliptic curve over a field $K$ of characteristic $char(K) = 0$. Then there exists a subfield $K_0 \subset K$ of finite type over $\mathbf{Q}$, an elliptic curve $E_0$ over $K_0$ satisfying $(E_0)_K \xrightarrow{\sim} E$ and*

$$\mathrm{End}_K(E) = \mathrm{End}_{K_0}(E_0) = \mathrm{End}_{\mathbf{C}}(E_0) = \begin{cases} \mathbf{Z} \\ \\ \mathbf{Z} + \mathbf{Z}\alpha, \qquad \alpha^2 + a\alpha + b = 0,\ a, b \in \mathbf{Z},\ a^2 - 4b < 0. \end{cases}$$

*(for some embedding $K_0 \hookrightarrow \mathbf{C}$).*

## 2.2 Isomorphisms (= isogenies of degree one)

**(2.2.1)** Let $E, E'$ be elliptic curves over $K$. We would like to determine the set $\mathrm{Isom}_L(E, E')$ of isomorphisms between $E_L$ and $E_L'$ over various extensions $L$ of $K$. Thanks to 1.2.4 we can assume that both $E$ and $E'$ are given by a generalized Weierstrass equation, with the corresponding affine curves of the form

$$\begin{aligned} E - \{O\} &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ E' - \{O'\} &: y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6' \end{aligned} \tag{2.2.1.1}$$

(where $a_i, a_i' \in K$).

**(2.2.2) Proposition.** *Any element of $\mathrm{Isom}_K(E, E')$ is given by the formulas*

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned} \qquad (r, s, t \in K,\ u \in K^*). \tag{2.2.2.1}$$

*Conversely, any change of variables (2.2.2.1) transforms $E$ into an elliptic curve $E'$ over $K$ in a generalized Weierstrass form.*

*Proof.* (cf. [Si 1], III.3.1(b)). Any $\lambda \in \mathrm{Isom}_K(E, E')$ induces isomorphisms of vector spaces

$$\lambda^* : L(n(O')) \xrightarrow{\sim} L(n(O)), \qquad f' \mapsto f \circ \lambda$$

(for all $n \in \mathbf{Z}$). This implies, by the definition of $x, y, x', y'$ (see the proof of 1.2.4), that

$$x = \lambda^*(ax' + b), \qquad y = \lambda^*(cy' + dx' + e),$$

for some constants $a, b, c, d, e \in K$ with $a, c \neq 0$. As

$$y^2 - x^3 \in L(5(O)), \qquad y'^2 - x'^3 \in L(5(O')),$$

it follows that $c^2 = a^3$; putting $u = c/a \in K^*$, we obtain $a = u^2$ and $c = u^3$, as claimed. The converse statement is trivial (as the map (2.2.2.1) has an inverse of the same form).

**(2.2.3) Special case:** *$char(K) \neq 2, 3$.* If the characteristic of $K$ is not equal to 2 or 3, then we can assume (by 1.2.5) that the curves $E, E'$ are in the form

$$E - \{O\} : y^2 = x^3 + a_4x + a_6, \qquad E' - \{O'\} : y'^2 = x'^3 + a'_4x' + a'_6. \tag{2.2.3.1}$$

The only transformations (2.2.2.1) preserving the equations (2.2.3.1) are given by

$$x = u^2x', \qquad y = u^3y' \qquad\qquad (u \in K^*). \tag{2.2.3.2}$$

The substitution (2.2.3.2) transforms $E - \{O\}$ into

$$E' - \{O'\} : (u^3y')^2 = (u^2x')^3 + a_4(u^2x') + a_6 \iff y'^2 = x'^3 + u^{-4}a_4x' + u^{-6}a_6,$$

hence

$$a'_4 = u^{-4}a_4, \qquad a'_6 = u^{-6}a_6. \tag{2.2.3.3}$$

We have thus proved the following

**(2.2.4) Proposition.** *Let $E, E'$ be elliptic curves of the form (2.2.3.1) over a field $K$ of characteristic $char(K) \neq 2, 3$. Then, for any field $L \supset K$, the formulas (2.2.3.2) define a bijection*

$$\mathrm{Isom}_L(E, E') \xrightarrow{\sim} \{u \in L^* \mid u^{-4}a_4 = a'_4,\ u^{-6}a_6 = a'_6\}.$$

**(2.2.5) Corollary.** *Under the assumptions of 2.2.4,*

$$\mathrm{Aut}_L(E) = \begin{cases} \mu_2(L) = \{\pm 1\}, & a_4, a_6 \neq 0 \\ \mu_4(L), & a_6 = 0 \ (\Longrightarrow a_4 \neq 0) \\ \mu_6(L), & a_4 = 0 \ (\Longrightarrow a_6 \neq 0), \end{cases}$$

*where* $\mu_n(L) = \{u \in L^* \mid u^n = 1\}$.

**(2.2.6) The discriminant and the $j$-invariant (*$char(K) \neq 2, 3$*).** Let us write the equation of $E$ in the form

$$E - \{O\} : y^2 = x^3 + Ax + B \qquad\qquad (A, B \in K).$$

By I.3.7.7,

$$E \text{ is smooth} \iff 0 \neq \mathrm{disc}(x^3 + Ax + B) = -4A^3 - 27B^2.$$

Mimicking the formulas from the analytic theory over $\mathbf{C}$ (I.7.1.10), we write

$$(2y)^2 = 4x^3 - g_2x - g_3 \qquad\qquad (g_2 = -4A,\ g_3 = -4B)$$

and put

$$\Delta = g_2^3 - 27g_3^2 = -16(4A^3 + 27B^2), \qquad j(E) = \frac{(12g_2)^3}{\Delta} = \frac{4(12A)^3}{4A^3 + 27B^2}.$$

Similarly, write $E'$ in the form

$$E' - \{O'\} : y'^2 = x'^3 + A'x' + B' \qquad\qquad (A', B' \in K).$$

If there is an isomorphism $\lambda : E_L \xrightarrow{\sim} E'_L$ (over some field $L \supset K$), then there exists $u \in L^*$ satisfying

$$u^{-4}A = A', \qquad u^{-6}B = B' \tag{2.2.6.1}$$

(by 2.2.4), hence

$$j(E') = \frac{4(12A)^3 u^{-12}}{4A^3 u^{-12} + 27B^2 u^{-12}} = j(E).$$

Conversely, if $j(E) = j(E') \neq 0$, then $B^2/A^3 = B'^2/A'^3$, hence (2.2.6.1) holds for suitable $u \in \overline{K}^*$ (this is also true if $j(E) = j(E') = 0$, for trivial reasons). We have thus proved the following

**(2.2.7) Proposition.** *Let $E, E'$ be elliptic curves over a field $K$ of characteristic $char(K) \neq 2, 3$. Then the following conditions are equivalent:*
(i) $j(E) = j(E')$.
(ii) *There exists a field $L \supset K$ and an isomorphism $E_L \xrightarrow{\sim} E'_L$.*
(iii) *There exists a field $L \supset K$ of finite degree over $K$ and an isomorphism $E_L \xrightarrow{\sim} E'_L$.*

**(2.2.8) Examples:** Let $A, B \in K$, $D \in K^*$.
(1) If $2(4A^3 + 27B^2) \neq 0 \in K$, then the elliptic curves

$$E : y^2 = x^3 + Ax + B, \qquad E' : Dy'^2 = x'^3 + Ax' + B$$

(written in the affine form) become isomorphic over $L = K(\sqrt{D})$. The curve $E'$ is usually referred to as the **quadratic twist of $E$ over $K(\sqrt{D})/K$**, as its isomorphism class over $K$ depends only on the field $K(\sqrt{D})$.
(2) If $2A \neq 0 \in K$, then the elliptic curves

$$E : y^2 = x^3 + Ax, \qquad E' : y'^2 = x'^3 + DAx'$$

become isomorphic over $L = K(\sqrt[4]{D})$.
(3) If $6B \neq 0 \in K$, then the elliptic curves

$$E : y^2 = x^3 + B, \qquad E' : y'^2 = x'^3 + DB$$

become isomorphic over $L = K(\sqrt[6]{D})$.

**(2.2.9) Exercise.** *Let $E, E'$ be as in 2.2.8(n); show that $E$ is isomorphic to $E'$ (over $K$) $\iff$ $D \in K^{*2n}$ $(n = 1, 2, 3)$.*

**(2.2.10) Exercise.** *Let $E, E'$ be elliptic curves over a field $K$ of characteristic $char(K) \neq 2, 3$. Assume that there exists an extension $L \supset K$ and an isomorphism $E_L \xrightarrow{\sim} E'_L$. Show that the pair $(E, E')$ is isomorphic (over $K$) to one of the pairs in 2.2.8, for suitable $D \in K^*$.*

**(2.2.11) Exercise.** *Let $K$ be a field of characteristic $char(K) \neq 2, 3$ and $j \in K$. Show that there exists an elliptic curve $E$ over $K$ with $j(E) = j$.*

**(2.2.12) Exercise.** *Let $L, L' \subset \mathbf{C}$ be lattices satisfying $j(L) = j(L')$. Show that there exists $\lambda \in \mathbf{C}^*$ such that $L' = \lambda L$.*

**(2.2.13) Exercise.** *Give an explicit list of isomorphism classes of elliptic curves over $\mathbf{F}_2$. Which among them become isomorphic over $\mathbf{F}_4$?*

### 2.3 Multiplication maps

**(2.3.1) Proposition.** *Let $E$ be an elliptic curve over a field $K$. Then, for each $n \in \mathbf{Z} - \{0\}$, the multiplication by $n$ is an isogeny $[n] : E \longrightarrow E$ (i.e. $[n]$ is not constant).*

*Proof.* We only sketch the argument; see ([Si 1], III.4.2(a)) for more details. We can assume that $n > 1$; as $[n](O) = O$, we have to show that $[n]$ is not the constant map with value $O$. If $char(K) \neq 2$, then an explicit calculation of $[2](x, y)$ shows that the set $E(\overline{K})[2] = \mathrm{Ker}([2])(\overline{K})$ is finite ($\Longrightarrow$ [2] in not constant $\Longrightarrow$ $[2^k]$ is not constant for all $k \geq 1$) and contains a point $P \neq O$; thus, if $2 \nmid m$, then $[m](P) = P \neq O$, hence $[m]$ is not constant. It follows that $[2^k \cdot m]$ is not constant, either. For $char(K) = 2$ one applies the same argument, with [2] replaced by [3].

**(2.3.2) Corollary.** *The map $n \mapsto [n]$ is an injective homomorphism $\mathbf{Z} \hookrightarrow \mathrm{End}_K(E)$.*

**(2.3.3)** We shall see later on that $\deg([n]) = n^2$, and that $[n]$ is 'unramified' $\iff$ $char(K) \nmid n$.

### 2.4 Isogenies of degree two ($char(K) \neq 2$)

**(2.4.1) The analytic version.** If $L \subset L' \subset \mathbf{C}$ are lattices in $\mathbf{C}$ such that $L'/L \xrightarrow{\sim} \mathbf{Z}/2\mathbf{Z}$, then the identity on $\mathbf{C}$ induces a holomorphic map

$$\lambda : \mathbf{C}/L \longrightarrow \mathbf{C}/L' \tag{2.4.1.1}$$

of degree $\deg(\lambda) = 2$. Conversely, it follows from I.7.6.1 that every holomorphic map $\lambda : \mathbf{C}/L \longrightarrow \mathbf{C}/L'$ of degree $\deg(\lambda) = 2$ between two tori is given by the above construction, possibly after replacing $L$ by $\alpha L$ (for suitable $\alpha \in \mathbf{C}^*$).

The Theorem on Elementary Divisors implies that there is a basis $\omega_1, \omega_2$ of $L$ such that $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, $L' = \mathbf{Z}\frac{\omega_1}{2} + \mathbf{Z}\omega_2$. The kernel of $\lambda$ is then equal to $\mathrm{Ker}(\lambda) = \{0, \omega_1/2 \ (\mathrm{mod}\, L)\}$, where $\omega_1/2 \ (\mathrm{mod}\, L)$ is a point of exact order 2 on $\mathbf{C}/L$.

**(2.4.2) The algebraic version.** Let $E$ be an elliptic curve over a field $K$ of characteristic $char(K) \neq 2$ and $P_0 \in E(K) - \{O\}$ a $K$-rational point satisfying $[2]P_0 = O$.

We can assume that $E$ is given in the generalized Weierstrass form

$$E - \{O\} : y^2 = f(x) = x^3 + ax^2 + bx + c \qquad\qquad (a, b, c \in K),$$

where the polynomial $f \in K[x]$ has distinct roots $e_1, e_2, e_3 \in \overline{K}$. As $P_0 = (e_1, 0)$ (say) is $K$-rational, we can replace $x$ by $x - e_1$, hence assume that $E$ is in the form

$$E - \{O\} : y^2 = x(x^2 + ax + b), \qquad P_0 = (0, 0), \qquad a, b \in K, \qquad b(a^2 - 4b) \neq 0$$

(the last condition is equivalent to $E$ being smooth).

We would like to construct an isogeny $\lambda : E \longrightarrow E'$ of degree two with "$\mathrm{Ker}(\lambda)$" equal to $\{O, P_0\}$. Morally, this means that (the pull-backs under $\lambda$) of rational functions on $E'$ will correspond to those rational functions on $E$ which are invariant under the translation $\tau_{P_0} : P \mapsto P \boxplus P_0$ (as in I.7.6.6).

**(2.4.3)** In the analytic case 2.4.1, the functions

$$f(z) = \wp(z; L) + \wp(z + \frac{\omega_1}{2}; L), \qquad f'(z) = \wp'(z; L) + \wp'(z + \frac{\omega_1}{2}; L)$$

are both $L'$-periodic, have poles of order 2 (resp. 3) at $z \in L'$ (and no other poles) and have Laurent expansions

$$f(z) = z^{-2} + c_0 + \cdots, \qquad f'(z) = -2z^{-3} + c_1 z + \cdots$$

at $z = 0$. This implies that

$$f(z) = \wp(z; L') + c_0, \qquad f'(z) = \wp'(z; L'), \tag{2.4.3.1}$$

hence the isogeny $\lambda$ is given by the formula

$$\lambda(\wp(z;L),\wp'(z;L)) = (f(z)-c_0, f'(z)).$$

It remains to express the functions $f(z), f'(z)$ in terms of $(x,y) = (\wp(z;L),\wp'(z;L))$.

**(2.4.4)** We shall do this calculation in the algebraic setup: denote the coordinates of a point $P \in E - \{O\}$ by $(x(P), y(P))$ and put

$$X := x(P) + x(P \boxplus P_0) + c, \qquad Y := y(P) + y(P \boxplus P_0),$$

where $c \in K$ is a constant, to be determined later. As the line

$$y = \frac{y(P)}{x(P)}x$$

intersects $E$ at the points

$$P_0 = (0,0), \qquad P = (x(P), y(P)), \qquad [-1](P \boxplus P_0) = (x(P \boxplus P_0), -y(P \boxplus P_0)),$$

it follows that

$$x(x^2+ax+b) - \left(\frac{y(P)}{x(P)}x\right)^2 = x(x-x(P))(x-x(P \boxplus P_0)),$$

hence

$$a + x(P) + x(P \boxplus P_0) = \left(\frac{y(P)}{x(P)}\right)^2, \qquad x(P)x(P \boxplus P_0) = b.$$

Taking $c = a$ and dropping $P$ from the notation, we obtain

$$X = x + a + \frac{b}{x} = \left(\frac{y}{x}\right)^2, \qquad Y = \frac{y}{x}\left(x - \frac{b}{x}\right) \tag{2.4.4.1}$$

and

$$Y^2 = X\left(x^2 - 2b + \frac{b^2}{x^2}\right) = X\left(\left(x+\frac{b}{x}\right)^2 - 4b\right) = X((X-a)^2 - 4b).$$

To sum up, $E'$ is given by the equation

$$E' - \{O'\} : Y^2 = X(X^2 - 2aX + (a^2-4b)) = X(X^2 + a'X + b') \tag{2.4.4.2}$$

and $\lambda : E \longrightarrow E'$ by (2.4.4.1). Note that $E'$ is smooth, as

$$b'(a'^2 - 4b') = (a^2-4b)\cdot 16b \neq 0.$$

**(2.4.5) Exercise.** *Express $j = j(E)$ and $j' = j(E')$ in terms of the parameter $u = 4b/a^2 \in \mathbf{P}^1(K)$. For which values of $u$ is $j = j'$?*

**(2.4.6) Relation to Complex Multiplication.** Assume that, in the analytic situation, there is an element $\lambda \in \mathcal{O} = \mathrm{End}(\mathbf{C}/L)$ satisfying $\lambda\overline{\lambda} = 2$. Multiplication by $\lambda$ then induces an isogeny $[\lambda] : \mathbf{C}/L \longrightarrow \mathbf{C}/L$ of degree $\deg([\lambda]) = 2$, so in this case $E'$ is isomorphic to $E$, hence $j = j'$.

The possible values of $\lambda$ (up to the action of $\mathrm{Aut}(\mathbf{C}/L)$) are the following:

$$\begin{aligned} &\mathcal{O} = \mathbf{Z}[i], && \lambda = 1+i \\ &\mathcal{O} = \mathbf{Z}[i\sqrt{2}], && \lambda = i\sqrt{2} \\ &\mathcal{O} = \mathbf{Z}[\frac{1+i\sqrt{7}}{2}], && \lambda = \frac{1\pm i\sqrt{7}}{2}. \end{aligned} \tag{2.4.6.1}$$

**(2.4.7) Exercise.** *Compute $j(\mathcal{O})$ for $\mathcal{O}$ from (2.4.6.1).*

**(2.4.8) Iterating this construction.** If we apply the procedure from 2.4.4 to the curve $E'$, we obtain an isogeny $\lambda' : E' \longrightarrow E''$, where $E''$ is given by

$$E'' - \{O''\} : v^2 = u(u^2 + 4au + 16b)$$

and

$$\lambda'(X,Y) = (u,v) = \left( \left( \frac{Y}{X} \right)^2, \frac{Y}{X} \left( X - \frac{a^2 - 4b}{X} \right) \right).$$

Note that the formulas

$$x = u/4, \qquad y = v/8$$

define an isomorphism $E'' \xrightarrow{\sim} E$; denote by $\widehat{\lambda} : E' \longrightarrow E$ its composition with $\lambda'$.

**(2.4.9) Exercise.** *Show that $\widehat{\lambda} \circ \lambda = [2]$, i.e. $\widehat{\lambda}$ is the "dual isogeny" to $\lambda$.*

**(2.4.10)** This implies that, in the analytic setup 2.4.1, $E'' = \mathbf{C}/L''$, where $L'' = \mathbf{Z}\frac{\omega_1}{2} + \mathbf{Z}\frac{\omega_2}{2} = \frac{1}{2}L$ and $\lambda'$ is again induced by the identity on $\mathbf{C}$.

## 2.5 Complex Multiplication by $\mathbf{Z}[i]$

**(2.5.1)** The projective curves $V$ and $E$ from I.8.1-3, which were constructed from the affine curves

$$V_{\text{aff}} : y^2 = 1 - x^4, \qquad E_{\text{aff}} : v^2 = 4u^3 - 4u,$$

can be considered over an arbitrary field $K$. If $char(K) \neq 2$, which we shall assume throughout Sect. 2.5, both $V$ and $E$ are smooth over $K$. In fact, $V$ and $E$ are elliptic curves with distinguished points $O_V = (0,1)$, $O_E = (0:1:0)$ and the map $f : V \longrightarrow E$, $f(x,y) = (1/x^2, -2y/x^3)$ from I.8.3.2 is an isogeny of degree 2. The group law on both $V$ and $E$ is given by the same formulas as over $\mathbf{C}$ (see (I.8.4.2.2)).

**(2.5.2) Action of $\mathbf{Z}[i]$.** Assume that the polynomial $T^2 + 1$ is reducible over $K$; fix one of its roots $I \in K$, $I^2 = -1$.

**(2.5.2.1) Definition.** *Define morphisms $[i]_X : X \longrightarrow X$ ($X = V, E$) by the same formulas as in the analytic case (I.8.4.1.1)):*

$$[i]_V : V \longrightarrow V, \qquad (x,y) \mapsto (Ix, y); \qquad [i]_E : E \longrightarrow E, \qquad (u,v) \mapsto (-u, Iv).$$

**(2.5.2.2) Exercise.** *For $X = V, E$, the morphism $[i]_X$ is an automorphism $[i]_X \in \mathrm{Aut}_K(X)$ satisfying*

$$[i]_X \circ [i]_X = [-1]_X, \qquad (\forall n \in \mathbf{Z}) \;\; [i]_X \circ [n]_X = [n]_X \circ [i]_X, \qquad [i]_E \circ f = f \circ [i]_V.$$

**(2.5.2.3) Definition.** *For $X = V, E$ and $m + ni \in \mathbf{Z}[i]$ ($m, n \in \mathbf{Z}$), define a morphism $[m+ni]_X \in \mathrm{End}_K(X)$ by*

$$[m + ni]_X = [m]_X \boxplus ([n]_X \circ [i]_X) : X \longrightarrow X.$$

**(2.5.2.4) Exercise.** *For $X = V, E$ and $\alpha, \beta \in \mathbf{Z}[i]$,*

$$[\alpha]_X \boxplus [\beta]_X = [\alpha + \beta]_X, \qquad [\alpha]_X \circ [\beta]_X = [\alpha\beta]_X, \qquad [\alpha]_E \circ f = f \circ [\alpha]_V.$$

**(2.5.2.5) Exercise.** *The formulas from I.8.3.7(ii) define an isomorphism of curves $g : V \xrightarrow{\sim} E$ (over $K$) satisfying $f(O_V) = O_E$. [This shows that $V$ is, indeed, an elliptic curve.]*

**(2.5.3) Lemma.** *Let $X = V, E$. For each $\alpha \in \mathbf{Z}[i] - \{0\}$, the morphism $[\alpha]_X : X \longrightarrow X$ is an isogeny (hence the map $\alpha \mapsto [\alpha]_X$ induces an injective ring homomorphism $\mathbf{Z}[i] \longrightarrow \mathrm{End}_K(X)$).*

*Proof.* As $\alpha \neq 0$, the composite morphism $[\alpha]_X \circ [\overline{\alpha}]_X = [\alpha\overline{\alpha}]_X$ is non-zero (by 2.3.1), hence $[\alpha]_X$ is non-zero as well.

**(2.5.4) Exercise.** *Show that, for each* $\alpha \in \mathbf{Z}[i] - \{0\}$, $\deg([\alpha]_X) = N\alpha = \alpha\overline{\alpha}$. *[Hint: if* $char(K) = p > 0$, *factorize* $\alpha$ *in* $\mathbf{Z}[i]$ *and use I.9.3.7,10.]*

**(2.5.5) A supersingular example.** If $p \equiv 3 \pmod 4$ is a prime number, then $K = \mathbf{Z}[i]/p\mathbf{Z}[i]$ is a field isomorphic to $\mathbf{F}_{p^2}$; let $I \in K$ be the image of $i$ in $K$.

The endomorphism ring $\mathrm{End}_K(V)$ contains the following elements: $[i]_V$ satisfying $[i]_V^2 = -1$ (where we simplify the notation and write $n$ instead of $[n]_V$, for $n \in \mathbf{Z}$) and also the *Frobenius morphism*

$$\phi_p : V \longrightarrow V, \qquad (x, y) \mapsto (x^p, y^p),$$

which will be investigated in more detail in 3.1 below. The congruence I.8.4.9 for $\alpha = -p$ and the formulas

$$\phi_p \circ [i]_V(x, y) = \phi_p(Ix, y) = (I^p x^p, y^p) = (-Ix^p, y^p) = [-i]_V(x^p, y^p) = [-i]_V \circ \phi_p(x, y)$$

imply that

$$\phi_p^2 = [-p]_V = -p, \qquad \phi_p \circ [i]_V = [-i]_V \circ \phi_p.$$

To sum up, we have constructed a (non-zero) homomorphism of rings

$$\begin{gathered} \mathbf{Z}[I, J]/ < I^2 = -1, J^2 = -p, IJ = -JI > \longrightarrow \mathrm{End}_K(V) \\ I \mapsto [i]_V, \qquad J \mapsto \phi_p. \end{gathered} \tag{2.5.5.1}$$

Tensoring (2.5.5.1) with $\mathbf{Q}$ we obtain a (non-zero) homomorphism of $\mathbf{Q}$-algebras

$$B := \mathbf{Q}[I, J]/ < I^2 = -1, J^2 = -p, IJ = -JI > \longrightarrow \mathrm{End}_K(V) \otimes_{\mathbf{Z}} \mathbf{Q}. \tag{2.5.5.2}$$

Knowledgeable readers will recognize in the L.H.S. of (2.5.5.2) the quaternion algebra

$$B = \left(\frac{-1, -p}{\mathbf{Q}}\right)_2 = \mathbf{Q} \cdot 1 + \mathbf{Q} \cdot I + \mathbf{Q} \cdot J + \mathbf{Q} \cdot IJ, \qquad I^2 = -1,\ J^2 = -p,\ IJ = -JI,$$

which is a central simple algebra over $\mathbf{Q}$ (i.e. $B$ has no non-trivial bilateral ideals and its centre is equal to $\mathbf{Q}$). This implies that the homomorphism (2.5.5.2), being non-zero, must be injective. In fact, it is an *isomorphism*, but we are not going to prove this.

**(2.5.6)** In general, elliptic curves with non-commutative endomorphism rings are quite rare; they occur only over fields of characteristic $p > 0$, and for each $p$ there are only finitely many of them (up to isomorphism over some extension of the base field). For such curves, $\mathrm{End}_K(-) \otimes \mathbf{Q}$ is isomorphic to the unique quaternion algebra over $\mathbf{Q}$ ramified exactly at $p$ and $\infty$ (see [Hu], Ch. 13.6; [Si 1], V.3).

## 2.6 Complex Multiplication by $\mathbf{Z}[\rho]$

**(2.6.1)** Let $\rho = e^{2\pi i/3}$; then $\rho^2 + \rho + 1 = 0,\ \rho - \rho^2 = i\sqrt{3}$.

**(2.6.2) Exercise.** *Let* $K$ *be a field of characteristic* $char(K) \neq 3$ *and* $D \in K^*$.
(i) *Show that* $E : X^3 + Y^3 = DZ^3$ *is an elliptic curve over* $K$ *(with origin* $O = (1 : -1 : 0)$*).*
(ii) *Find a change of variables transforming* $(E, O)$ *into a curve in a generalized Weierstrass form.*
(iii) *If* $char(K) \neq 2$, *show that, for suitable* $A \in K^*$, $E$ *is isomorphic over* $K$ *to the elliptic curve*

$$E_A : y^2 = x^3 + A.$$

(iv) *Assume that* $\zeta \in \overline{K}$ *is a primitive cubic root of unity, i.e.* $\zeta^3 = 1 \neq \zeta$. *Define* $[\rho] : E_{K(\zeta)} \longrightarrow E_{K(\zeta)}$ *by* $[\rho](X : Y : Z) \mapsto (X : Y : \zeta Z)$ *and show that the map* $m + n\rho \mapsto [m] + ([n] \circ [\rho])$ *defines an injective ring homomorphism*

$$\mathbf{Z}[\rho] \longrightarrow \mathrm{End}_{K(\zeta)}(E).$$

(v) *Compute explicitly the action of* $[-1]$ *and* $[\rho - \rho^2]$ *on* $E$ *and find all points* $P \in E(\overline{K})$ *satisfying* $[\rho - \rho^2]P = O$ *(resp.* $[3]P = O$*).*

(vi) *If $char(K) \neq 2$, show that the isomorphism from (iii) transforms $[\rho - \rho^2] \in \mathrm{End}_{K(\zeta)}(E)$ into an isogeny $\lambda : E_A \longrightarrow E_{-27A}$ of degree 3 defined over $K$. Determine* $\mathrm{Ker}(\lambda)(\overline{K})$.

**(2.6.3) Exercise.** *Consider the elliptic curve $E : X^3 + Y^3 = Z^3$ (with $O = (1 : -1 : 0)$) over a field $K$ of characteristic $char(K) = 2$.*
(i) *Show that* $\phi_2^2 = \phi_4 = [-2] \in \mathrm{End}_K(E)$.
(ii) *If $K \supset \mathbf{F}_4$, show that there is an injective homomorphism*

$$R := \mathbf{Z}[\rho][\phi]/ < \phi^2 = -2,\ \phi\rho = \rho^{-1}\phi > \longrightarrow \mathrm{End}_K(E).$$

(iii) *Show that the map*

$$\rho \mapsto \frac{-1 + i + j + k}{2}, \qquad \phi \mapsto i - j$$

*induces an injective homomorphism $R \hookrightarrow \mathbf{H}$ into the algebra of Hamilton quaternions; determine its image.*
(iv) *Determine* $\mathrm{Aut}_K(E)$ *(for $K \supset \mathbf{F}_4$).*

## 3. Isogenies (main properties)

### 3.1 The dual isogeny

**(3.1.1) Example:** Let $L \subset L' \subset \mathbf{C}$ be lattices satisfying $L'/L \xrightarrow{\sim} \mathbf{Z}/2\mathbf{Z}$ and let

$$\lambda : \mathbf{C}/L \longrightarrow \mathbf{C}/L', \qquad z \ (\mathrm{mod}\, L) \mapsto z \ (\mathrm{mod}\, L')$$

be the (analytic) isogeny of degree 2 studied in 2.4. According to the general recipe from I.7.6.5, the formula

$$\widehat{\lambda} : \mathbf{C}/L' \longrightarrow \mathbf{C}/L, \qquad z \ (\mathrm{mod}\, L') \mapsto 2z \ (\mathrm{mod}\, L)$$

defines an (analytic) isogeny of degree 2 satisfying

$$\widehat{\lambda} \circ \lambda = [2], \qquad \lambda \circ \widehat{\lambda} = [2].$$

Choosing a basis $\omega_1, \omega_2 \in L$ such that $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, $L' = \mathbf{Z}\frac{\omega_1}{2} + \mathbf{Z}\omega_2$, we have

$$\lambda^{-1}\,(z \ (\mathrm{mod}\, L')) = \{z \ (\mathrm{mod}\, L),\ (z + \omega_1/2) \ (\mathrm{mod}\, L)\},$$
$$2z \ (\mathrm{mod}\, L) = z + (z + \omega_1/2) \ (\mathrm{mod}\, L) - \omega_1/2 \ (\mathrm{mod}\, L).$$

The latter formula can be rewritten as

$$\widehat{\lambda}(Q) = \boxplus_{P \in \lambda^{-1}(Q)} P \boxminus \boxplus_{P \in \lambda^{-1}(O)} P; \tag{3.1.1.1}$$

in other words, $\widehat{\lambda}(Q)$ corresponds to the class of the divisor $\lambda^*((Q) - (O))$ under the isomorphism $\boxplus : Cl^0(\mathbf{C}/L) \xrightarrow{\sim} \mathbf{C}/L$ from I.5.3.6.

**(3.1.2) Proposition.** *Let $\lambda : E' \longrightarrow E$ be an isogeny between elliptic curves over $K$ of degree* $\deg(\lambda) = n$. *Then there is a unique isogeny $\widehat{\lambda} : E \longrightarrow E'$ (the* **dual isogeny** *to $\lambda$) satisfying $\lambda \circ \widehat{\lambda} = [n]_E$.*

*Proof. Uniqueness:* If $\mu, \nu : E \longrightarrow E'$ are isogenies satisfying $\lambda \circ \mu = \lambda \circ \nu$, then $\lambda \circ (\mu \boxminus \nu) = 0$, hence $\mu \boxminus \nu = 0$ (by 2.1.6), i.e. $\mu = \nu$.
*Existence:* We shall try to construct $\widehat{\lambda}$ by generalizing the formula (3.1.1.1). It is natural to expect that, for each field $L \supset K$, $\widehat{\lambda}$ should act on the $L$-rational points by the following composite map:

$$E(L) \xrightarrow{\sim} Cl^0(E_L) \xrightarrow{\lambda_L^*} Cl^0(E'_L) \xleftarrow{\sim} E'(L), \tag{3.1.2.1}$$

where the isomorphisms are those from 1.2.1; we apply this observation to the field $L = R(E)$ and the "general point" $Q \in E(L)$ defined in 1.2.6. Denote by $Q'(\lambda) \in E'(L)$ the image of $Q$ under the map (3.1.2.1); then $Q'(\lambda)$ defines a rational map $E - - \succ E'$, which extends to a (unique) morphism $\widetilde{\lambda} : E \longrightarrow E'$.

In the scheme theoretical language, the points $Q$ and $Q'(\lambda)$ correspond to morphisms

$$Q : \mathrm{Spec}(L) \longrightarrow E, \qquad Q'(\lambda) = \widetilde{\lambda} \circ Q : \mathrm{Spec}(L) \xrightarrow{Q} E \xrightarrow{\widetilde{\lambda}} E'.$$

As the composite map

$$(\lambda_L)_* \circ (\lambda_L)^* : \mathrm{Div}(E_L) \longrightarrow \mathrm{Div}(E'_L) \longrightarrow \mathrm{Div}(E_L)$$

is given by multiplication by $n$, it follows that $\lambda_L(Q'(\lambda)) = [n]_E(Q)$, hence

$$\lambda \circ Q'(\lambda) : \mathrm{Spec}(L) \xrightarrow{Q} E \xrightarrow{\widetilde{\lambda}} E' \xrightarrow{\lambda} E$$

is equal to

$$[n]_E \circ Q : \mathrm{Spec}(L) \xrightarrow{Q} E \xrightarrow{[n]_E} E.$$

In other words, the morphisms $\lambda \circ \widetilde{\lambda}, [n]_E : E \longrightarrow E$ define the same rational map $E - - \succ E$, which implies that they are equal:

$$\lambda \circ \widetilde{\lambda} = [n]_E.$$

In particular, $\widetilde{\lambda} : E \longrightarrow E'$ is a non-constant morphism. Instead of proving directly that $\widetilde{\lambda}(O) = O'$ (i.e. that $\widetilde{\lambda}$ is an isogeny), we use the following trick: the point $P := \widetilde{\lambda}(O) \in E'(K)$ satisfies $\lambda(P) = [n](O) = O$; putting

$$\widehat{\lambda} = \tau_{-P} \circ \widetilde{\lambda} : E \xrightarrow{\widetilde{\lambda}} E' \xrightarrow{\tau_{-P}} E'$$

(where $\tau_{-P}$ denotes the translation map by $-P = \boxminus P$), then $\widehat{\lambda} : E \longrightarrow E'$ will be an isogeny (as $\widehat{\lambda}(O) = O'$) satisfying

$$\lambda \circ \widehat{\lambda} = \lambda \circ \tau_{-P} \circ \widetilde{\lambda} = \lambda \circ \widetilde{\lambda} = [n]_E$$

(as $\lambda(P) = 0$), as required.

**(3.1.3)** (i) It is convenient to define $\widehat{0} = 0$ and $\deg(0) = 0$; then $\widehat{\lambda}$ makes sense for all elements of $\mathrm{Hom}_L(E', E)$.

(ii) If $L \supset K$ is any field, then $\widehat{\lambda_L} = (\widehat{\lambda})_L$ (as $([n]_E)_L = [n]_{E_L}$).

(iii) In the situation of 2.5.2, $\widehat{[\alpha]}_X = [\overline{\alpha}]_X$ $(X = V, E)$, thanks to 2.5.4.

(iv) In the situation of 2.5.5, $\widehat{\phi}_p = -\phi_p$; combined with (iii), this implies that the map $\lambda \mapsto \widehat{\lambda}$ on $\mathrm{End}_K(E)$ induces the standard involution $I \mapsto -I$, $J \mapsto -J$, $IJ \mapsto -IJ$ on the quaternion algebra $B$.

**(3.1.4) Theorem.** *Let $\lambda : E' \longrightarrow E$ be an isogeny of degree $\deg(\lambda) = n$. Then*

(i) $\widehat{\lambda} \circ \lambda = [n]_{E'}, \quad \lambda \circ \widehat{\lambda} = [n]_E$.

(ii) *If $\mu : E'' \longrightarrow E'$ is an isogeny, then* $\widehat{\lambda \circ \mu} = \widehat{\mu} \circ \widehat{\lambda}$.

(iii) *If $\mu : E' \longrightarrow E$ is an isogeny, then* $\widehat{\lambda \boxplus \mu} = \widehat{\lambda} \boxplus \widehat{\mu}$.

(iv) *For all $m \in \mathbf{Z}$,* $\widehat{[m]} = [m], \quad \deg[m] = m^2$.

(v) $\deg(\widehat{\lambda}) = \deg(\lambda)$.

(vi) $\widehat{\widehat{\lambda}} = \lambda$.

*Proof.* (cf. [Si 1], III.6.2). (i) We know that $\lambda \circ \widehat{\lambda} = [n]_E$, hence

$$(\widehat{\lambda} \circ \lambda) \circ \widehat{\lambda} = \widehat{\lambda} \circ (\lambda \circ \widehat{\lambda}) = \widehat{\lambda} \circ [n]_E = [n]_{E'} \circ \widehat{\lambda} \implies \widehat{\lambda} \circ \lambda = [n]_{E'}.$$

(using 2.1.3 and 2.1.6).
(ii) If $r = \deg(\mu)$, then

$$\lambda \circ \mu \circ \widehat{\mu} \circ \widehat{\lambda} = \lambda \circ [r]_{E'} \circ \widehat{\lambda} = [r]_E \circ \lambda \circ \widehat{\lambda} = [r]_E \circ [n]_E = [rn]_E = [\deg(\lambda \circ \mu)] = \lambda \circ \mu \circ \widehat{\lambda \circ \mu},$$

which implies the result (again using 2.1.3 and 2.1.6).
(iii) This is a non-trivial statement, which will be proved in 3.1.6-9 below.
(iv) The equality $\widehat{[m]} = [m]$ follows from (iii) (and the case $m = -1$) by induction on $|m|$. It implies that

$$[\deg([m])] = [m] \circ \widehat{[m]} = [m^2] \implies \deg([m]) = m^2$$

(using 2.3.2).
(v) This follows from the fact that

$$\deg(\lambda)\deg(\widehat{\lambda}) = \deg(\lambda \circ \widehat{\lambda}) = \deg([n]) = n^2 = \deg(\lambda)^2.$$

(vi) Combining (i) and (v), we obtain

$$[n]_E \circ \widehat{\widehat{\lambda}} = \lambda \circ \widehat{\lambda} \circ \widehat{\widehat{\lambda}} = \lambda \circ [n]_{E'} = \lambda \circ \widehat{\lambda} \circ \lambda = [n]_E \circ \lambda \implies \widehat{\widehat{\lambda}} = \lambda.$$

**(3.1.5) Corollary.** *The function*

$$\deg : \mathrm{Hom}_L(E', E) \longrightarrow \mathbf{Z}$$

*is quadratic, i.e. the function*

$$(\lambda, \mu) \mapsto \deg(\lambda \boxplus \mu) - \deg(\lambda) - \deg(\mu)$$

*is a bilinear form on* $\mathrm{Hom}_L(E', E)$.

**(3.1.6) Proof of 3.1.4(iii) (beginning).** A truly "functorial" proof would deduce the statement from the "Theorem of the square". Instead, we shall try to explain the "usual" proof (cf. [Si 1], III.6.2; [Ca 3], App. C; note that, if $char(K) > 0$, then the proof involves elliptic curves over non-perfect fields; this fact was glossed over in [Si 1]).

The idea of the proof is to consider the graphs $\Gamma_\nu$ of the isogenies $\nu = \lambda, \mu, \lambda \boxplus \mu$ as divisors on the surface $E' \times_K E$, and to study their restrictions to the elliptic curves $L' \times_K E = E_{L'}$ and $E' \times_K L = E'_L$ over the fields $L = R(E)$ and $L' = R(E')$, respectively. More precisely, consider the divisor

$$D = (\Gamma_{\lambda \boxplus \mu}) - (\Gamma_\lambda) - (\Gamma_\mu) + (\Gamma_0) \in \mathrm{Div}(E' \times_K E). \tag{3.1.6.1}$$

Restricting $D$ to $E_{L'}$, i.e. viewing the "horizontal" coordinate in the direction of $E'$ as constant, we deduce that $D$ is "almost" principal. Using this information and restricting $D$ to $E'_L$, i.e. viewing the "vertical" coordinate as constant, we obtain

$$Q'(\lambda \boxplus \mu) = Q'(\lambda) \boxplus Q'(\mu) \boxplus P_1 \tag{3.1.6.2}$$

for some $P_1 \in E'(K)$, which implies that

$$\widetilde{\lambda \boxplus \mu} = \tau_{P_1} \circ (\widetilde{\lambda} \boxplus \widetilde{\mu}) \implies \widehat{\lambda \boxplus \mu} = \widehat{\lambda} \boxplus \widehat{\mu},$$

as required. Let us first explain the terminology in a simplified setting.

**(3.1.7) A toy model.** Let $C_1 = \mathbf{A}^1_K = \mathrm{Spec}(K[x_1])$ and $C_2 = \mathbf{A}^1_K = \mathrm{Spec}(K[x_2])$ be two affine lines over $K$; denote by $L_j = R(C_j) = K(x_j)$ $(j = 1, 2)$ their fields of rational functions. The product $X = C_1 \times_K C_2 = \mathbf{A}^2_K = \mathrm{Spec}(K[x_1, x_2])$ is an affine plane; we view $x_1$ (resp. $x_2$) as the horizontal (resp. the vertical) coordinate on $X$.

**(3.1.7.1) Divisors on the surface $X = C_1 \times_K C_2$.** A **divisor** on $X$ is a formal finite linear combination $\sum_C n_C(C)$ of reduced irreducible curves $C \subset X$, with integral coefficients $n_C \in \mathbf{Z}$; they form an abelian group $\mathrm{Div}(X)$ with respect to addition. Each curve $C$ is given by an equation

$$C : f_C(x_1, x_2) = 0,$$

where $f_C \in K[x_1, x_2]$ is a non-constant irreducible polynomial. This polynomial is unique only up to multiplication by a constant in $K^*$; however, we fix $f_C$, for each curve $C$ as above.

If the polynomial $f_C(x_1, x_2)$ depends only on $x_1$ (resp. only on $x_2$), then the curve $C : f_C(x_1) = 0$ (resp. $C : f_C(x_2) = 0$) is vertical (resp. horizontal). Such curves generate the groups of vertical (resp. horizontal) divisors on $X$:

$$\mathrm{Div}(X)_{\mathrm{vert}} = \sum_{\text{vertical } C} n_C(C), \qquad \mathrm{Div}(X)_{\mathrm{hor}} = \sum_{\text{horizontal } C} n_C(C)$$

The (two-dimensional) ring $K[x_1, x_2]$ is factorial, which means that each non-zero rational function $g \in R(X)^* = K(x_1, x_2)^*$ factorizes uniquelly as

$$g = a \prod_C f_C^{\mathrm{ord}_C(g)}, \qquad (a \in K^*,\ \mathrm{ord}_C(g) \in \mathbf{Z}); \tag{3.1.7.1.1}$$

the **divisor of** $g$ is defined as

$$\mathrm{div}(g) = \sum_C \mathrm{ord}_C(g)(C) \in \mathrm{Div}(X).$$

As $\mathrm{div}(f_C) = (C)$, the **divisor class group of** $X$

$$Cl(X) = \mathrm{Div}(X)/\{\mathrm{div}(g) \,|\, g \in R(X)^*\} \tag{3.1.7.1.2}$$

vanishes: $Cl(X) = 0$.

**(3.1.7.2) Variables versus constants.** It is often useful to view one of the coordinates, say $x_2$, as being "constant", and consider only $x_1$ as a "true" variable. What does this mean?

For example, in the factorization (3.1.7.1.1), we disregard all horizontal curves $C : f_C(x_2) = 0$. Algebraically, this amounts to considering the factorization of $g$ in the localized (one-dimensional) ring

$$(K[x_2] - \{0\})^{-1} K[x_1, x_2] = K(x_2)[x_1] = L_2[x_1],$$

which is the ring of functions on a curve (= the affine line) over the field $L_2 = K(x_2)$. Geometrically, the localization

$$j_1^a : K[x_1, x_2] \hookrightarrow K(x_2)[x_1] = L_2[x_1]$$

defines an injective morphism

$$j_1 : \mathbf{A}^1_{L_2} = (C_1)_{L_2} = C_1 \times_K \mathrm{Spec}(L_2) = \mathrm{Spec}(L_2[x_1]) \longrightarrow \mathrm{Spec}(K[x_1, x_2]) = C_1 \times_K C_2,$$

whose image is obtained from $C_1 \times_K C_2$ by removing all horizontal curves $C : f_C(x_2) = 0$ (and the generic point).

The slogan "view $x_2$ as a constant" means that one restricts a given geometric object from $C_1 \times_K C_2$ to $(C_1)_{L_2}$, via the morphism $j_1$. For example, for the divisor group we obtain the map "forget all horizontal curves"

$$\begin{aligned} j_1^* : \mathrm{Div}(C_1 \times_K C_2) &\longrightarrow \mathrm{Div}((C_1)_{L_2}) \\ \sum_C n_C(C) &\mapsto \sum_{C \text{ not horizontal}} n_C(C_{L_2}), \end{aligned}$$

where $C_{L_2} = C \times_K L_2 : (j_1^a(f_C))(x_1, x_2) = 0$ is considered as a closed point on $\mathbf{A}^1_{L_2}$ (of course, $j_1^a(f_C)$ is the same polynomial as $f_C$, but this time considered as an element of $K(x_2)[x_1] = L_2[x_1]$: $x_1$ is variable, but $x_2$ is not). Note that

$$\mathrm{Ker}(j_1^*) = \mathrm{Div}(X)_{\mathrm{hor}}.$$

Similarly, viewing $x_1$ as being "constant" amounts to localizing

$$j_2^a : K[x_1, x_2] \hookrightarrow K(x_1)[x_2] = L_1[x_2]$$

and restricting via the morphism

$$j_2 : \mathbf{A}^1_{L_1} = (C_2)_{L_1} = \mathrm{Spec}(L_1) \times_K C_2 = \mathrm{Spec}(L_1[x_2]) \longrightarrow \mathrm{Spec}(K[x_1, x_2]) = C_1 \times_K C_2,$$

giving rise to the map "forget all vertical curves"

$$\begin{aligned} j_2^* : \mathrm{Div}(C_1 \times_K C_2) &\longrightarrow \mathrm{Div}((C_2)_{L_1}) \\ \sum_C n_C(C) &\mapsto \sum_{C \text{ not vertical}} n_C(C_{L_1}), \end{aligned}$$

where $C_{L_1} = L_1 \times_K C$, satisfying $\mathrm{Ker}(j_2^*) = \mathrm{Div}(X)_{\mathrm{vert}}$.

It is important to note that

$$\mathrm{div}(j_1^a(g)) = j_1^*(\mathrm{div}(g)), \qquad \mathrm{div}(j_2^a(g)) = j_2^*(\mathrm{div}(g)), \qquad (\forall g \in R(X)^*),$$

where we have also denoted by $j_1^a, j_2^a$ the canonical maps (in fact, the identity maps)

$$\begin{aligned} j_1^a : R(C_1 \times_K C_2) = \mathrm{Frac}(K[x_1, x_2]) &\longrightarrow \mathrm{Frac}(K(x_2)[x_1]) = R((C_1)_{L_2}) \\ j_2^a : R(C_1 \times_K C_2) = \mathrm{Frac}(K[x_1, x_2]) &\longrightarrow \mathrm{Frac}(K(x_1)[x_2]) = R((C_2)_{L_1}). \end{aligned}$$

**(3.1.7.3) Example:** Let $\Gamma_\alpha \subset C_1 \times_K C_2$ be the graph of the morphism $\alpha : C_1 \longrightarrow C_2$ given by "$\alpha(x_1) = x_1^2$", i.e. corresponding to the morphism of $K$-algebras

$$\alpha^a : K[x_2] \longrightarrow K[x_1], \qquad \alpha^a(x_2) = x_1^2.$$

In other words, $\Gamma_\alpha$ is the reduced irreducible curve

$$\Gamma_\alpha : x_1^2 - x_2 = 0$$

on $C_1 \times_K C_2 = \mathbf{A}^2_K$, i.e.

$$(\Gamma_\alpha) = \mathrm{div}(x_1^2 - x_2).$$

If we consider $x_1$ as being constant, then

$$\begin{aligned} j_2^*((\Gamma_\alpha)) = (\Gamma_\alpha)_{L_1} = (\text{the point with the coordinate } x_2 \text{ equal to } x_1^2 \text{ on } (C_2)_{L_1} = \mathbf{A}^1_{L_1}) = \\ = (\alpha_{L_1})_*(\text{the tautological point with the coordinate } x_1 \text{ equal to } x_1 \text{ on } (C_1)_{L_1} = \mathbf{A}^1_{L_1}) \end{aligned}$$

(in the last line, $x_1$ appears twice: first as a variable, then as a constant).
If we consider $x_2$ as being constant, then

$$\begin{aligned} j_1^*((\Gamma_\alpha)) = (\Gamma_\alpha)_{L_2} = (\text{the prime ideal } (x_1^2 - x_2) \text{ in } L_2[x_1]) = \\ = \text{"(the point with the coordinate } x_1 \text{ equal to } \sqrt{x_2})+ \\ +(\text{the point with the coordinate } x_1 \text{ equal to } -\sqrt{x_2}) \text{ on } (C_1)_{L_2} = \mathbf{A}^1_{L_2}\text{"} = \\ = (\alpha_{L_2})^*(\text{the tautological point with the coordinate } x_2 \text{ equal to } x_2 \text{ on } (C_2)_{L_2} = \mathbf{A}^1_{L_2}) \end{aligned}$$

(again, in the last line, $x_2$ appears first as a variable, then as a constant).

**(3.1.8) Divisors.** Intuitively, one would like to define a divisor on an arbitrary variety (or a scheme) as a linear combination of "subvarieties" of codimension one. There are two versions of this notion: "Weil divisors" and "Cartier divisors"; however, the two coincide on "nice" varieties, such as the surface $E' \times_K E$.

More precisely, let $X$ be a (separated, noetherian, irreducible) regular scheme ($X$ is regular, for example, if it is smooth over a field). If $X = \mathrm{Spec}(A)$ is affine, then a divisor on $X$ is a finite linear combination

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}}(\mathfrak{p}) \qquad\qquad (n_{\mathfrak{p}} \in \mathbf{Z}),$$

where each $\mathfrak{p} \subset A$ is a prime ideal of codimension one (i.e. such that $\dim(A_{\mathfrak{p}}) = 1$); in the example 3.1.7, $A = K[x_1, x_2]$ and $\mathfrak{p} = (f_C)$. In general, a divisor is a finite sum

$$\sum_{x} n_x(x) \qquad\qquad (n_x \in \mathbf{Z}),$$

where each $x \in X$ is a point of codimension one (i.e. such that $\dim(\mathcal{O}_{X,x}) = 1$). The closure of $\{x\}$ in $X$ is a reduced and irreducible subscheme of $X$ of codimension one.

As $X$ is assumed to be regular, each local ring $\dim(A_{\mathfrak{p}})$ (resp. $\mathcal{O}_{X,x}$) in codimension one is a discrete valuation ring, defining a discrete valuation $\mathrm{ord}_{\mathfrak{p}}$ (resp. $\mathrm{ord}_x$) on the field $R(X)$. The divisor of a rational function $g \in R(X)^*$ is then defined as

$$\mathrm{div}(g) = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(g)(\mathfrak{p}), \qquad \text{resp.} \quad \sum_{x} \mathrm{ord}_x(g)(x).$$

**(3.1.9) Proof of 3.1.4(iii) (end).** We can play the same game as in 3.1.7 with the surface $X = E' \times_K E$; the divisors on $X$ are linear combinations of reduced irreducible curves on $X$. Let

$$Q : \mathrm{Spec}(L) = \mathrm{Spec}(R(E)) \longrightarrow E, \qquad Q' : \mathrm{Spec}(L') = \mathrm{Spec}(R(E')) \longrightarrow E'$$

be the tautological points of the two elliptic curves and

$$j = Q' \times \mathrm{id} : L' \times_K E = E_{L'} \longrightarrow E' \times_K E, \qquad j' = \mathrm{id} \times Q : E' \times_K L = E'_L \longrightarrow E' \times_K E$$

the corresponding inclusions. For any element $\lambda \in \mathrm{Hom}_K(E', E)$ and any field $F \supset K$, let $\lambda_F \in \mathrm{Hom}_F(E', E)$ be the same morphism, but considered as being defined over $F$. The graph of $\lambda$, defined as the fibre product

$$\begin{array}{ccc} \Gamma_\lambda & \longrightarrow & E' \times_K E \\ \downarrow & & \downarrow{\scriptstyle \lambda \times \mathrm{id}} \\ E & \xrightarrow{\Delta} & E \times_K E, \end{array}$$

is a reduced irreducible curve on $E' \times_K E$. As in 3.1.7.3, the restrictions of the divisor $(\Gamma_\lambda)$ via the maps

$$j^* : \mathrm{Div}(E' \times_K E) \longrightarrow \mathrm{Div}(E_{L'}), \qquad j'^* : \mathrm{Div}(E' \times_K E) \longrightarrow \mathrm{Div}(E'_L)$$

are equal to

$$j^*\left((\Gamma_\lambda)\right) = (\lambda_{L'}(Q')) \tag{3.1.9.1}$$

$$j'^*\left((\Gamma_\lambda)\right) = \lambda_L^*\left((Q)\right). \tag{3.1.9.2}$$

For $\lambda = 0$, the curve $\Gamma_0 = E' \times \{O\}$ is horizontal, thus

$$j^*\left((\Gamma_0)\right) = (O)_{L'}, \qquad j'^*\left((\Gamma_0)\right) = 0. \tag{3.1.9.3}$$

Considering the horizontal coordinate in the direction of $E'$ as constant, i.e. applying (3.1.9.1) to the divisor (3.1.6.1), we see that

$$j^*(D) = ((\lambda \boxplus \mu)_{L'}(Q')) - (\lambda_{L'}(Q')) - (\mu_{L'}(Q')) + (O)_{L'} \in \mathrm{Div}(E_{L'})$$

is a principal divisor on the elliptic curve $E_{L'}$, thanks to 1.2.1. This implies that $D$ itself differs from a principal divisor by a vertical divisor, i.e.

$$D = \mathrm{div}(f) + d \times E \in \mathrm{Div}(E' \times_K E), \tag{3.1.9.4}$$

for some rational function $f \in R(E' \times_K E)^*$ and a divisor $d \in \mathrm{Div}(E')$. Considering now the vertical coordinate in the direction of $E$ as constant, i.e. applying (3.1.9.2), we obtain the equality

$$(\lambda \boxplus \mu)_L^* ((Q)) - \lambda_L^* ((Q)) - \mu_L^* ((Q)) = \mathrm{div}(j'^a f) + d_L \in \mathrm{Div}(E'_L),$$

where $j'^a f = f$, but considered as an element of $R(E'_L) = R(E' \times_K E)$. It follows that the class of the divisor

$$(\lambda \boxplus \mu)_L^* ((Q) - (O)_L) - \lambda_L^* ((Q) - (O)_L) - \mu_L^* ((Q) - (O)_L)$$

in $Cl^0(E'_L)$ is equal to the class of $d'_L$, where

$$d' = d - (\lambda \boxplus \mu)^* ((O)) + \lambda^* ((O)) + \mu^* ((O)) \in \mathrm{Div}^0(E').$$

The last statement is nothing but the equality (3.1.6.2), with the point $P_1 \in E'(K)$ corresponding to the class of $d'$ under the isomorphism 1.2.1. As observed in 3.1.6, this concludes the proof of 3.1.4(iii).

### 3.2 The Frobenius morphism

Let $K$ be a field of characteristic $char(K) = p > 0$; the map $\sigma(a) = a^p$ is then a field homomorphism $\sigma : K \longrightarrow K$. Fix a power $q = p^r$ $(r \geq 1)$ of $p$; then $\sigma^r(a) = a^q$.

**(3.2.1)** For a polynomial $f(x) = \sum_\alpha c_\alpha x^\alpha \in K[x]$, put $f^{(q)}(x) = \sum_\alpha c_\alpha^q x^\alpha \in K[x]$. As $f(x)^q = f^{(q)}(x^q)$, it follows that

$$\text{if } a \in \overline{K} \text{ is a root of } f(x) \Longrightarrow a^q \text{ is a root of } f^{(q)}(x). \tag{3.2.1.1}$$

Similar properties hold for polynomials in several variables.

**(3.2.2) A naive "definition".** If $X$ is an affine "variety" (more precisely, an affine scheme of finite type) over $K$ given by the polynomial equations

$$f_1(x) = \cdots = f_N(x) = 0 \qquad\qquad (f_j \in K[x] = K[x_1, \ldots, x_M]),$$

we denote by $X^{(q)}$ the affine "variety" over $K$ given by the equations

$$f_1^{(q)}(x) = \cdots = f_N^{(q)}(x) = 0.$$

In other words, if the ring of regular functions on $X$ is equal to

$$A = K[x_1, \ldots, x_M]/(f_1, \ldots, f_N), \tag{3.2.2.1}$$

the corresponding ring of functions on $X^{(q)}$ will be given by

$$A^{(q)} = K[x_1, \ldots, x_M]/(f_1^{(q)}, \ldots, f_N^{(q)}). \tag{3.2.2.2}$$

In the scheme theoretical language, $X = \mathrm{Spec}(A), X^{(q)} = \mathrm{Spec}(A^{(q)})$. The morphism of $K$-algebras

$$\psi_q : A^{(q)} \longrightarrow A, \qquad \sum_\alpha c_\alpha x^\alpha \mapsto \sum_\alpha c_\alpha x^{q\alpha} \tag{3.2.2.3}$$

then defines a morphism $\phi_q : X \longrightarrow X^{(q)}$ (over $K$). On coordinates, if $a = (a_1, \ldots, a_m) \in X(\overline{K})$, then $\phi_q(a) = (a_1^q, \ldots, a_m^q) \in X^{(q)}(\overline{K})$, as in (3.2.1.1).

By working with homogeneous polynomials one can use the same formulas to define $X^{(q)}$ and $\phi_q$ for projective "varieties" over $K$.

**(3.2.3) An invariant definition.** Unfortunately, it is not immediately clear that the $K$-algebra (3.2.2.2) and the morphism (3.2.2.3) depend only on $A$, not on its particular presentation (3.2.2.1).

**(3.2.3.1) Definition.** *For any $K$-algebra $A$ (commutative), put $A^{(q)} = A \otimes_{K,\sigma^r} K$. This is a $K$-algebra via the map $c \mapsto 1 \otimes c$ ($c \in K$).*

**(3.2.3.2)** This means that each element of $A^{(q)}$ is a finite sum of expressions $a \otimes c$ ($a \in A$, $c \in K$) satisfying $ac \otimes c' = a \otimes c^q c'$ ($a \in A$, $c, c' \in K$).

**(3.2.3.3) Exercise.** *Let $A$ be as in (3.2.2.1). The formula*

$$\sum_\alpha c_\alpha x^\alpha \otimes c \mapsto \sum_\alpha c_\alpha^q c\, x^\alpha \qquad\qquad (f(x) \otimes c \mapsto c f^{(q)}(x))$$

*defines an isomorphism of $K$-algebras*

$$K[x_1, \ldots, x_M] \otimes_{K,\sigma^r} K \xrightarrow{\sim} K[x_1, \ldots, x_M],$$

*which induces an isomorphism of $K$-algebras*

$$A \otimes_{K,\sigma^r} K \xrightarrow{\sim} K[x_1, \ldots, x_M]/(f_1^{(q)}, \ldots, f_N^{(q)}).$$

*Under this isomorphism, the map (3.2.2.3) corresponds to*

$$\psi_q : \sum_\alpha c_\alpha x^\alpha \otimes c \mapsto \sum_\alpha c_\alpha^q c\, x^{q\alpha}.$$

**(3.2.3.4)** In other words, 3.2.3.1 is the correct functorial definition of $A^{(q)}$. In the scheme-theoretical language, this means that $X^{(q)}$ can be defined for an *arbitrary* $K$-scheme $X$ as the fibre product

$$\begin{array}{ccc} X^{(q)} & \longrightarrow & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K) & \xrightarrow{(\sigma^r)^*} & \mathrm{Spec}(K) \end{array}$$

**(3.2.3.5) Example.** If $A = K[x]$ (i.e. $X$ is the affine line over $K$), then $A^{(q)} = K[x]$ and the morphism of $K$-algebras $\psi_q : A^{(q)} = K[x] \longrightarrow A = K[x]$ corresponding to $\phi_q$ is given by $\psi_q(x) = x^q$ (and $\psi_q(c) = c$).

In this example, the corresponding extension of the fields of rational functions $K(x) = \mathrm{Frac}(A) \supset \psi_q(\mathrm{Frac}(A^{(q)})) = K(x^q)$ is purely inseparable, of degree $q$.

If the field $K$ is perfect, then $K(x^q) = K^q(x^q) = K(x)^q$. Moreover, if $\mathfrak{p} = (f(x)) \subset A = K[x]$ is a maximal ideal (where $f \in K[x]$ is a non-constant irreducible polynomial), then $f(x) = g^{(q)}(x)$ for some irreducible polynomial $g \in K[x]$, and the maximal ideal $\mathfrak{q} = (g) \subset A^{(q)} = K[x]$ satisfies $\psi_q(\mathfrak{q})A = (g^{(q)}(x^q)) = (f(x))^q = \mathfrak{p}^q$; in other words, the morphism $\phi_q$ is totally ramified at the point $\mathfrak{p}$.

**(3.2.3.6)** $\phi_q$ is usually called the *relative Frobenius morphism*, where "relative" refers to the fact that $\psi_q$ is the identity on constants $c \in K$, but raises each variable $x_j$ to its $q$-th power.

**(3.2.3.7)** If $K \subseteq \mathbf{F}_q$, then $\sigma^r = \mathrm{id}$ on $K$, hence $X^{(q)} = X$ for every $K$-scheme $X$.

**(3.2.4) Proposition.** *Let $K$ be a perfect field of characteristic $p > 0$, $q = p^r$ $(r \geq 1)$ and $X$ a smooth projective curve over $K$ (ireducible over $\overline{K}$). Then:*
(i) *$X^{(q)}$ is also a smooth projective curve over $K$ (ireducible over $\overline{K}$).*
(ii) *The extension of the fields of rational functions $R(X)/\phi_q^* R(X^{(q)})$ corresponding to the morphism $\phi_q : X \longrightarrow X^{(q)}$ is purely inseparable, of degree $q$ (thus $\deg(\phi_q) = q$).*
(iii) *$\phi_q^* R(X^{(q)}) = R(X)^q$.*
(iv) *The morphism of curves $\phi_q : X \longrightarrow X^{(q)}$ is totally ramified at each (closed) point.*

*Proof.* (cf. [Si 1], II.2.11). The statement (i) follows from the fact that the horizontal arrows in the diagram 3.2.3.4 are isomorphisms, since the field $K$ is perfect. For the affine line over $K$, we have verified the statements (ii)-(iv) by hand in 3.2.3.5. The general case easily follows, but we include the details for the reader's convenience.
(ii), (iii) As $\pi : X \longrightarrow \mathrm{Spec}(K)$ is smooth of relative dimension one, there exists an open affine subset $\mathrm{Spec}(A) \subset X$ which is étale (i.e. smooth of relative dimension zero) over the affine line $\mathbf{A}^1_K = \mathrm{Spec}(K[t])$. This implies that the corresponding extension of the fields of rational functions $R(X)/K(t) = \mathrm{Frac}(A)/K(t)$ is separable (and finite). In the diagram of fields

$$\begin{array}{ccc} K(t) & \subset & R(X) \\ | & & | \\ K(t)^q = K(t^q) & \subset & R(X)^q \end{array}$$

the horizontal extensions are separable, while the vertical extensions are purely inseparable; thus

$$[R(X) : R(X)^q] = [K(t) : K(t^q)] = q.$$

For each open affine subset $\mathrm{Spec}(A) \subset X$, where $A = K[x_1, \ldots, x_m]/I = K[x_1, \ldots, x_m]/(f_1, \ldots, f_n)$, the image of the map $\psi_q : A^{(q)} \longrightarrow A$ is equal to

$$K[x_1^q, \ldots, x_m^q]/(f_1^{(q)}(x^q), \ldots, f_n^{(q)}(x^q)) = K[x_1^q, \ldots, x_m^q]/(f_1(x)^q, \ldots, f_n(x)^q) = A^q$$

(using the fact that $K = K^q$, as $K$ is perfect by assumption). This implies that $\phi_q^* R(X^{(q)}) = R(X)^q$.
(iv) For each $A$ as in the proof of (iii), $A$ is a Dedekind ring; let $\mathfrak{p} = (g_1 + I, \ldots, g_r + I) \in \mathrm{Max}(A)$ $(g_j \in K[x_1, \ldots, x_m])$ be any maximal ideal of $A$. Then $\mathfrak{p}^{(q)} = (g_1^{(q)} + I^{(q)}, \ldots, g_r^{(q)} + I^{(q)})$ is an ideal of $A^{(q)}$, satisfying

$$A^{(q)}/\mathfrak{p}^{(q)} = (A/\mathfrak{p}) \otimes_{K,\sigma} K \xrightarrow{\sim} A/\mathfrak{p} = k(\mathfrak{p})$$

(as $\sigma : K \longrightarrow K$ is an isomorphism, the field $K$ being perfect). It follows that $\mathfrak{p}^{(q)}$ is a maximal ideal of $A^{(q)}$ and

$$\psi_q(\mathfrak{p}^{(q)}) = (g_1^{(q)}(x^q) + I^{(q)}, \ldots, g_r^{(q)}(x^q) + I^{(q)}) = \mathfrak{p}^q,$$

which means that $\mathfrak{p}^{(q)} = \psi_q^{-1}(\mathfrak{p})$ is totally ramified in $\psi_q(A^{(q)}) \subset A$, with ramification index equal to $q$.

**(3.2.5) Corollary.** *If $K$ is as in 3.2.4 and $E$ is an elliptic curve over $K$, then, for each $r \geq 1$, $E^{(q)}$ is an elliptic curve over $K$ and $\phi_q : E \longrightarrow E^{(q)}$ is an isogeny (where we take $\phi_q(O)$ to be the distinguished $K$-rational point of $E^{(q)}$).*

**(3.2.6) Proposition.** *Let $K$ be a perfect field of characteristic $p > 0$, $\lambda : E \longrightarrow E'$ an isogeny of elliptic curves over $K$. Then $\lambda$ factors uniquelly as*

$$E \xrightarrow{\phi_q} E^{(q)} \xrightarrow{\mu} E',$$

*where $q = p^r$ for some $r \geq 0$, $\mu$ is an isogeny and the extension $R(E^{(q)})/\mu^* R(E')$ is separable.*

*Proof.* (cf. [Si 1], II.2.12). Let $F/\lambda^*(R(E'))$ be the maximal separable subextension of $R(E)/\lambda^*(R(E'))$. Then $R(E)/F$ is a purely inseparable extension of degree $q = p^r$ $(r \geq 0)$, hence $R(E)^q \subset F$. As

$$[R(E):F] = q = [R(E):\phi_q^* R(E^{(q)})] = [R(E):R(E)^q]$$

by 3.2.4(ii)-(iii), we have $F = R(E)^q = \phi_q^* R(E^{(q)})$. The tower of fields

$$R(E) \supset \phi_q^* R(E^{(q)}) \supset \lambda^*(R(E'))$$

then corresponds to a tower of (non-constant) morphisms

$$E \xrightarrow{\phi_q} E^{(q)} \xrightarrow{\mu} E'.$$

Define $O_{E^{(q)}} = \phi_q(O_E)$; then $\phi_q, \mu$ are isogenies and the extension $R(E^{(q)})/\mu^*(R(E'))$ is separable, being isomorphic to $F/\lambda^*(R(E'))$.

**(3.2.7) Corollary (of the proof).** *If, in the situation of 3.2.6, the extension of fields $R(E)/\lambda^*(R(E'))$ is purely inseparable, then the isogeny $\lambda : E \longrightarrow E'$ is isomorphic to the isogeny $\phi_q : E \longrightarrow E^{(q)}$.*

### 3.3 The invariant differential

We refer to ([Al-Kl]; [Ei], Ch. 16; [Mat], Ch. 9) for basic properties of Kähler differentials.

**(3.3.1)** If $E$ is an elliptic curve over $K$, then the space of regular differentials $\Gamma(E, \Omega_{E/K})$ on $E$ is one-dimensional (as $E$ has genus $g(E) = 1$).

**(3.3.2) Proposition.** (i) *If $\omega \in \Gamma(E, \Omega_{E/K}) - \{0\}$ is a non-zero regular differential, then* $\mathrm{div}(\omega) = 0$, *i.e. $\omega$ has no zeros (nor poles).*
(ii) *If $E$ is given by a generalized Weierstrass equation*

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

*then*

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} \tag{3.3.2.1}$$

*is a regular differential on $E$, hence $\Gamma(E, \Omega_{E/K}) = K \cdot \omega$ and $\omega$ has no zeros (nor poles).*

*Proof.* (i) $D = \mathrm{div}(\omega) \geq 0$ is an effective divisor of degree $\deg_K(D) = 2g - 2 = 0$, hence $D = 0$.
(ii) (cf. [Si 1], III.1.5). We know that

$$\Gamma(E_{\overline{K}}, \Omega_{E_{\overline{K}}/\overline{K}}) = \Gamma(E, \Omega_{E/K}) \otimes_K \overline{K}.$$

Consequently, to show that $\omega$ is regular (i.e. $\omega \in \Gamma(E, \Omega_{E/K})$), we can replace $E$ by $E_{\overline{K}}$ and $\omega$ by $\overline{\omega} = \omega \otimes 1 \in \Omega_{R(E)/K} \otimes_K \overline{K} \subset \Omega_{R(E_{\overline{K}})/\overline{K}}$. The same calculation as in the proof of I.4.2.2 then shows that $\mathrm{ord}_P(\overline{\omega}) = 0$ for all $P \in (E - \{O\})(\overline{K})$. As $\deg(\mathrm{div}(\overline{\omega})) = 2g - 2 = 0$, it follows that $\mathrm{ord}_O(\overline{\omega}) = 0$; thus $\mathrm{div}(\overline{\omega}) = 0$. In particular, $\overline{\omega}$ is regular, hence so is $\omega$.

**(3.3.3) Exercise.** *How does the direct calculation of* $\mathrm{ord}_O(\overline{\omega})$ *from I.4.2.2 have to be modified in the algebraic context? [Hint: what is the analogue of I.3.3.8?]*

**(3.3.4)** The existence of a regular differential without zeros on $E$ should come as a no surprise. $E$ is an algebraic group, which implies that its cotangent bundle is trivial: choose a basis of the cotangent space at the origin and use translation maps to transport this basis all over $E$. For a fixed trivialization of the cotangent bundle, a constant section of the trivial bundle then corresponds to a regular differential $\omega$ without zeros.

As $E$ is a curve, its cotangent bundle has rank one (it is a line bundle). Moreover, the only global sections of the trivial line bundle are the constants, since $E$ is projective; thus $\omega$ is unique up to a constant multiple.

Last but not least, the construction of the trivialization of the cotangent bundle using the (commutative) group law implies that the differential $\omega$ is invariant in the following sense.

**(3.3.5) Invariant differentials.** We are going to show that $\omega$ from (3.3.2.1) is an *invariant differential*, i.e. that

$$\omega(Q_1 \boxplus Q_2) = \omega(Q_1) + \omega(Q_2), \tag{3.3.5.1}$$

if we consider the coordinates of $Q_j = (x_j, y_j)$ $(j = 1, 2)$ as variables. This property makes $\omega$ into an important tool for "linearizing" the group law on $E$ (replacing the analytic uniformization $\mathbf{C}/L \xrightarrow{\sim} E(\mathbf{C})$ available in the complex case).

What are the basic examples of invariant differentials?

$$\text{The additive group : } \ dz \ \text{ satisfies } \ d(z_1 + z_2) = dz_1 + dz_2.$$
$$\text{The multiplicative group : } \ dz/z \ \text{ satisfies } \ d(z_1 z_2)/z_1 z_2 = dz_1/z_1 + dz_2/z_2.$$

In general, if $G \longrightarrow S$ is a "commutative group scheme" over a base scheme $S$ (such as $E$ over $K$), then a regular differential $\omega \in \Gamma(G, \Omega_{G/S})$ is *(translation) invariant* if

$$m^*(\omega) = p_1^*(\omega) + p_2^*(\omega), \tag{3.3.5.2}$$

where the morphisms

$$m : G \times_S G \longrightarrow G, \qquad p_1 : G \times_S G \longrightarrow G, \qquad p_2 : G \times_S G \longrightarrow G \tag{3.3.5.3}$$

denote the group law on $G$ and the projections on the first (resp. the second) factor, respectively. Note that (3.3.5.2) is merely a fancy reformulation of (3.3.5.1).

**(3.3.6) Proposition.** *If $E$ is an elliptic curve over $K$, then every regular differential $\omega \in \Gamma(E, \Omega_{E/K})$ on $E$ is translation invariant, i.e. satisfies*

$$m^*(\omega) = p_1^*(\omega) + p_2^*(\omega)$$

*in the notation of 3.3.5.3.*

*Proof.* See ([Si 1], p. 82), for an 'elementary' proof. The following argument formalizes the last remark made in 3.3.4.

We can assume that $\omega \neq 0$. By 3.3.2(i), $\omega$ has no zeros on $E$, which means that multiplication by $\omega$ induces an isomorphism of invertible sheaves on $E$

$$\mathcal{O}_E \xrightarrow{\sim} \Omega_{E/K}$$

(i.e. a trivialization of the cotangent bundle of $E$). For the same reason, the map

$$\mathcal{O}_{E \times_K E}^{\oplus 2} \xrightarrow{\sim} \Omega_{E \times_K E/K}, \qquad (f_1, f_2) \mapsto f_1 \cdot (p_1^*\omega) + f_2 \cdot (p_2^*\omega)$$

is an isomorphism of sheaves on $E \times_K E$. Explicitly, if $(Q_1, Q_2)$ is a variable point in some open subset $U$ of $E \times_K E$, then the above map is given by

$$(f_1(Q_1, Q_2), f_2(Q_1, Q_2)) \mapsto f_1(Q_1, Q_2) \cdot \omega(Q_1) + f_2(Q_1, Q_2) \cdot \omega(Q_2),$$

where $f_1, f_2$ are regular functions on $U$. Taking global sections, we obtain an isomorphism of $K$-vector spaces

$$K^{\oplus 2} \xrightarrow{\sim} \Gamma(E \times_K E, \Omega_{E \times_K E/K}), \qquad (c_1, c_2) \mapsto c_1 \cdot (p_1^*\omega) + c_2 \cdot (p_2^*\omega).$$

As $m^*(\omega) \in \Gamma(E \times_K E, \Omega_{E \times_K E/K})$, it is of the form

$$m^*(\omega) = c_1 \cdot (p_1^*\omega) + c_2 \cdot (p_2^*\omega)$$

for some constants $c_1, c_2 \in K$. These constants can be determined by restricting to the curves $E \times_K \{O\} = \mathrm{Im}(i_1)$ and $\{O\} \times_K E = \mathrm{Im}(i_2)$, where $i_j : E \longrightarrow E \times_K E$ $(j = 1, 2)$ are the morphisms

$$i_1(P) = (P, O), \qquad i_2(P) = (O, P).$$

Then

$$m \circ i_j = p_j \circ i_j = \mathrm{id}, \quad p_j \circ i_k = 0 \quad (j \neq k) \quad \Longrightarrow \quad \omega = i_j^* m^*(\omega) = c_j \cdot \omega \quad \Longrightarrow \quad c_1 = c_2 = 1.$$

**(3.3.7) Corollary.** *If $\lambda, \mu : E' \longrightarrow E$ are two isogenies between elliptic curves over $K$, then*

$$(\lambda \boxplus \mu)^*(\omega) = \lambda^*(\omega) + \mu^*(\omega)$$

*holds for every regular differential $\omega \in \Gamma(E, \Omega_{E/K})$.*

*Proof.* By definition,

$$\lambda \boxplus \mu = m \circ g, \qquad \lambda = p_1 \circ g, \qquad \mu = p_2 \circ g,$$

where

$$g : E' \xrightarrow{\Delta} E' \times_K E' \xrightarrow{\lambda \times \mu} E \times_K E$$

(and $\Delta(P) = (P, P)$). Applying $g^*$ to 3.3.6 yields the result:

$$(\lambda \boxplus \mu)^*(\omega) = g^* m^*(\omega) = g^* p_1^*(\omega) + g^* p_2^*(\omega) = \lambda^*(\omega) + \mu^*(\omega).$$

**(3.3.8) Corollary.** *If $E$ is an elliptic curve over $K$ and $\omega \in \Gamma(E, \Omega_{E/K})$ a regular differential on $E$, then*

$$[n]^*(\omega) = n\omega \qquad\qquad (n \in \mathbf{Z}).$$

*Proof.* Induction on $|n|$.

### 3.4 Separable (= unramified = étale) isogenies

**(3.4.1)** Let $\lambda : E' \longrightarrow E$ be an isogeny between elliptic curves over $K$. Choose non-zero regular differentials $\omega_E$ (resp. $\omega_{E'}$) on $E$ (resp. $E'$). The exact sequence of Kähler differentials associated to the triple

$$K \hookrightarrow R(E) \xrightarrow{\lambda^*} R(E')$$

reads as follows (note that $\Omega_{R(E)/K}$ is denoted by $\Omega_E$ in [Si 1]):

$$\begin{array}{ccccccc} \Omega_{R(E)/K} \otimes_{R(E),\lambda^*} R(E') & \xrightarrow{\lambda^*} & \Omega_{R(E')/K} & \longrightarrow & \Omega_{R(E')/\lambda^* R(E)} & \longrightarrow & 0 \\ \| & & \| & & \| & & \\ R(E') \cdot \omega_E & \xrightarrow{\lambda^*} & R(E') \cdot \omega_{E'} & \longrightarrow & \Omega_{R(E')/\lambda^* R(E)} & \longrightarrow & 0 \end{array} \tag{3.4.1.1}$$

**(3.4.2) Definition.** *An isogeny $\lambda : E' \longrightarrow E$ is* **separable** *if the extension $R(E')/\lambda^* R(E)$ of the fields of rational functions is separable.*

**(3.4.3) Lemma.** *An isogeny $\lambda : E' \longrightarrow E$ is separable $\iff$ $\lambda^*(\omega_E) \neq 0$ (where $\omega_E$ is any non-zero regular differential on $E$).*

*Proof.* This follows from the exactness of the bottom row of (3.4.1.1) and the fact that a finite field extension $L'/L$ is separable if and only if $\Omega_{L'/L} = 0$.

**(3.4.4) Example:** If $char(K) = p > 0$ and $\phi_q : E \longrightarrow E^{(q)}$ $(q = p^r,\ r \geq 1)$ is the relative Frobenius morphism, then $\phi_q^*(\omega_{E^{(q)}}) = 0$, as $d(x^q) = q x^{q-1}\, dx = 0$.

**(3.4.5) Proposition.** *Let $\lambda : E' \longrightarrow E$ be a separable isogeny.*
(i) *For each field $L \supset K$, the isogeny $\lambda_L : E'_L \longrightarrow E_L$ is also separable.*
(ii) *$\lambda$ is unramified at each (closed) point $x' \in E'$ ($\Longleftrightarrow$ the extension of the residue fields $k(x')/k(x)$, where $x = \lambda(x')$, is separable).*
(iii) *For each $P \in E(\overline{K})$, the set*

$$\lambda^{-1}(P)(\overline{K}) := \{Q \in E'(\overline{K}) \,|\, \lambda(Q) = P\}$$

*has $\deg(\lambda)$ elements.*
(iv) *If $P$ is defined over a separable extension of $K$, so are all elements of $\lambda^{-1}(P)(\overline{K})$.*
(v) *$\mathrm{Ker}(\lambda)(\overline{K}) = \lambda^{-1}(O)(\overline{K})$ is a finite subgroup of $E'(K^{sep})$ of order $\deg(\lambda)$, stable by the action of the Galois group $G_K = \mathrm{Gal}(K^{sep}/K)$ (where $K^{sep}$ denotes the maximal separable extension of $K$ contained in $\overline{K}$).*

*Proof.* (cf. [Si 1], III.4.10(c), if $K$ is perfect). (i) For any non-zero regular differential $\omega_E$ on $E$, we have $\lambda_L^*(\omega_E \otimes 1) = \lambda^*(\omega_E) \otimes 1 \neq 0$.
(ii) This is a local question, so we can consider $\lambda$ over a (non-empty) open subset $\mathrm{Spec}(A) = U \subset E$, where $A$ is a Dedekind ring, of finite type as a $K$-algebra, with fraction field $\mathrm{Frac}(A) = R(E)$. Then $\lambda^{-1}(U) = U' = \mathrm{Spec}(A')$, where $A'$ is the integral closure of $A$ in $\mathrm{Frac}(R(E'))$ (with respect to the embedding of fields $\lambda^* : R(E) \longrightarrow R(E')$); the point $x'$ corresponds to a maximal ideal $\mathfrak{p}' \subset A'$ and $x = \lambda(x')$ to the maximal ideal $\mathfrak{p} = (\lambda^*)^{-1}(\mathfrak{p}') \subset A$. The corresponding residue fields (= the fields of definitions of the points $x, x'$) are equal to $k(x) = k(\mathfrak{p}) = A/\mathfrak{p}$, $k(x') = k(\mathfrak{p}') = A'/\mathfrak{p}'$.

Recall that $\lambda$ is *unramified* at $x'$ if the extension of the discrete valuation rings $A_{\mathfrak{p}} \subset A'_{\mathfrak{p}'}$ is unramified, i.e. if $k(\mathfrak{p}')/k(\mathfrak{p})$ is a separable extension and the ramification index $e(\mathfrak{p}'|\mathfrak{p}) = 1$ is trivial. This is, in turn, equivalent to the vanishing of the module of differentials

$$\Omega_{A'_{\mathfrak{p}'}/A_{\mathfrak{p}}} = \big(\Omega_{A'/A}\big)_{\mathfrak{p}'} = 0. \tag{3.4.5.1}$$

The $A'$-module $M = \Omega_{A'/A}$ is finitely generated and torsion, since

$$M \otimes_A \mathrm{Frac}(A) = \Omega_{\mathrm{Frac}(A')/\mathrm{Frac}(A)} = 0$$

vanishes (as the field extension $\mathrm{Frac}(A')/\mathrm{Frac}(A)$ is separable, by assumption). This implies that (3.4.5.1) holds for all $\mathfrak{p}' \notin \Sigma$, for some *finite* bad set $\Sigma$ of maximal ideals of $A'$.

In the special case when the field $K = \overline{K}$ is algebraically closed, maximal ideals of $A$ (resp. $A'$) correspond to points in $U$ (resp. $U'$) with coordinates in $\overline{K}$. If $P' \in \Sigma \subset U'(\overline{K})$ is a bad point at which $\lambda$ is not unramified, then there is another point $Q' \in U'(\overline{K})$ such that $P' \boxplus Q' \in U'(\overline{K}) - \Sigma$. Applying the traslation by $Q'$, we see that the morphism

$$\lambda \circ \tau_{Q'} = \tau_Q \circ \lambda$$

(where $Q = \lambda(Q')$) is unramified at $P'$, hence so must be $\lambda$ (as $\tau_Q$ is an isomorphism). It follows that $\Sigma = \emptyset$, hence $\lambda$ is unramified everywhere.

If the field $K$ is arbitrary, the previous argument applies, thanks to (i), to the isogeny $\lambda_{\overline{K}} : E'_{\overline{K}} \longrightarrow E_{\overline{K}}$; thus $\lambda_{\overline{K}}$ is unramified everywhere, hence

$$\Omega_{A'/A} \otimes_K \overline{K} = \Omega_{A' \otimes_K \overline{K}/A \otimes_K \overline{K}} = 0,$$

which proves that $\Omega_{A'/A} = 0$, i.e. $\lambda$ is unramified everywhere.
(iii) We can replace $\lambda$ by $\lambda_{\overline{K}} : E'_{\overline{K}} \longrightarrow E_{\overline{K}}$ and assume that $K = \overline{K}$. In the notation of the proof of (ii), $P$ becomes a maximal ideal of $A$ and the set $S := \lambda^{-1}(P)(\overline{K})$ is the set of maximal ideals $Q \subset A'$ above $P$, i.e. such that $Q \cap A = P$. An algebraic version of I.3.2.3.5 states that

$$\sum_{Q \in S} e(Q|P) \cdot [k(Q) : k(P)] = [\mathrm{Frac}(A') : \mathrm{Frac}(A)] = \deg(\lambda).$$

However, the residue fields are equal to $k(Q) = A'/Q = \overline{K} = A/P = k(P)$ and each ramification index is equal to one, thanks to (ii); the formula then simply states that the number of elements of the set $S$ is equal to $\deg(\lambda)$.
The statement (iv) and much of (v) follow from (ii) and (iii). It remains to be proved that, if $Q \in E'(K^{sep})$ satisfies $\lambda(Q) = O$, then $\lambda(\sigma(Q)) = O$ for all $\sigma \in G_K$. This follows from the fact that

$$O = \sigma(O) = \sigma(\lambda(Q)) = \lambda(\sigma(Q)),$$

as $\lambda$ is defined over $K$.

**(3.4.6) A toy model:** Let $\mathbf{G}_m = \mathbf{A}^1_K - \{0\} = \mathrm{Spec}(K[x, 1/x])$ be the multiplicative group over a field $K$. This is an commutative algebraic group (or a group scheme, if you wish) over $K$, with the group law given by multiplication, i.e. by the morphism

$$\mathbf{G}_m \times_K \mathbf{G}_m = \mathrm{Spec}(K[x, 1/x] \otimes_K K[y, 1/y]) \xrightarrow{\sim} \mathrm{Spec}(K[x, 1/x, y, 1/y]) \xrightarrow{m} \mathrm{Spec}(K[t, 1/t])$$

corresponding to the $K$-algebra map

$$K[t, 1/t] \longrightarrow K[x, 1/x, y, 1/y], \qquad t \mapsto xy.$$

For each integer $n \geq 1$, the morphism $[n] : \mathbf{G}_m \longrightarrow \mathbf{G}_m$ corresponds to the map $x \mapsto x^n$. The invariant differential

$$\omega = \frac{dx}{x} \in \Gamma(\mathbf{G}_m, \Omega_{\mathbf{G}_m/K})$$

then satisfies

$$[n]^*(\omega) = \frac{d(x^n)}{x^n} = n\,\frac{dx}{x} = n\omega;$$

thus

$$[n]^*(\omega) \neq 0 \iff char(K) \nmid n, \tag{3.4.6.1}$$

which is equivalent to the separability of the extension of the fields of rational functions

$$R(\mathbf{G}_m)/[n]^*R(\mathbf{G}_m) = K(x)/K(x^n).$$

If (3.4.6.1) holds, then, for each point $P \in \mathbf{G}_m(\overline{K}) = \overline{K}^*$, the set of the $n$-th roots of $P$

$$[n]^{-1}(P)(\overline{K}) = \{Q \in \mathbf{G}_m(\overline{K}) = \overline{K}^* \mid Q^n = [n](Q) = P\}$$

consists of $n$ elements, each of them generating a separable extension of $K$. In particular, if $P = 1$ is the neutral element of $\mathbf{G}_m$, then $[n]^{-1}(P)(\overline{K}) = \mu_n(\overline{K})$ is the set of the $n$-th roots of unity in $\overline{K}$.

## 3.5 Points of finite order

Points of finite order on a given elliptic curve are analogues of the roots of unity in the elementary context. Their coordinates are interesting numbers in their own right (as we have seen in I.8.5); here we simply count the number of points of a given order.

**(3.5.1)** Throughout Sect. 3.5, $E$ will denote an elliptic curve over a field $K$ and $\omega$ a non-zero regular differential on $E$.

**(3.5.2) Proposition.** *If $n \geq 1$ and $(char(K), n) = 1$, then $[n] : E \longrightarrow E$ is a separable isogeny,*

$$\#E(\overline{K})_n = \deg[n] = n^2$$

*and the group of $n$-torsion points on $E$ is isomorphic to*

$$E(\overline{K})_n \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^2.$$

*Proof.* According to 3.3.8, $[n]^*(\omega) = n\omega$, which is non-zero, as $(char(K), n) = 1$; thus $[n]$ is a separable isogeny, by 3.4.3. Applying 3.4.5(iii) and 3.1.4(iv), we deduce that $\#E(\overline{K})_n = n^2$. In order to show that $E(\overline{K})_n \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^2$, it is sufficient to consider the case $n = p^r$, where $p$ is a prime number, $p \neq char(K)$. For $r = 1$, $E(\overline{K})_p$ is killed by $p$ and has order $\deg[p] = p^2$, hence $E(\overline{K})_p \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^2$. For $r > 1$ one proceeds by induction, using the result for $r - 1$ and the structure theory of finite abelian groups.

**(3.5.3) Corollary.** *If $char(K) = p > 0$, then there is an integer $a = a(E) \in \{0, 1\}$ (depending only on $E_{\overline{K}}$) such that*

$$(\forall r \geq 1) \quad E(\overline{K})_{p^r} \xrightarrow{\sim} (\mathbf{Z}/p^r\mathbf{Z})^a.$$

*Proof.* As $[p]^*\omega = p\omega = 0$, 3.4.3 together with 3.2.6 imply that $[p]$ factors as

$$[p] : E \xrightarrow{\phi_q} E^{(q)} \xrightarrow{\mu} E,$$

where $q = p^b$ $(b \geq 1)$ and $\mu$ is a separable isogeny. As $\deg[p] = p^2$ and $\deg \phi_q = q$, it follows that $b \in \{1, 2\}$ and $\deg(\mu) = p^{2-b}$. Applying 3.4.5 to $\mu$ gives $E(\overline{K})_p \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^a$ with $a = 2 - b$. For $r > 1$ use the same inductive argument as in the proof of 3.5.2.

**(3.5.4)** (1) If $a(E) = 1$ (resp. $a(E) = 0$), we say that $E$ is **ordinary** (resp. **supersingular**). The proof of 3.5.3 shows that

$$E \text{ is ordinary} \iff [p]_E \text{ is not purely inseparable} \iff \widehat{\phi}_p \text{ is a separable isogeny.}$$

(2) Assume that $K = \overline{K}$ is an algebraically closed field of characteristic $char(K) = p > 2$ and $X = V$ or $X = E$ one of the two elliptic curves with complex multiplication by $\mathbf{Z}[i]$ (as in 2.5.2, we fix a square root $I$ of $-1$ contained in $K$).

(2a) If $p \equiv 3 \pmod 4$, then $\widehat{\phi}_p = -\phi_p$ is not separable, hence the elliptic curve $X$ is supersingular.

(2b) If $p \equiv 1 \pmod 4$, then $p$ factors in $\mathbf{Z}[i]$ as $p = \alpha\overline{\alpha}$, where $\alpha = u + iv \equiv 1 \pmod{(2 + 2i)}$, $u^2 + v^2 = p$ $(u, v \in \mathbf{Z})$. We identify $\mathbf{Z}[i]/\alpha\mathbf{Z}[i]$ with the prime subfield $\mathbf{F}_p \subset K$ via the map $i \mapsto I$. The corresponding factorization $[p]_X = [\alpha]_X \circ [\overline{\alpha}]_X$ in $\mathrm{End}_K(X)$ then shows that

$$[\alpha]_X^*(\omega_X) = (u + vI)\omega_X = 0, \qquad [\overline{\alpha}]_X^*(\omega_X) = (u - vI)\omega_X = 2u\omega_X \neq 0.$$

It follows that the isogeny $[p]_X$ is not purely inseparable, hence the elliptic curve $X$ is ordinary. Incidentally, this argument also shows that $\phi_p = u \circ [\alpha]_X$, for some automorphism $u \in \mathrm{Aut}_K(X)$, which proves Eisenstein's congruence I.9.4.6 for $\alpha$ up to the unknown factor $u$.

(3) It is true in general that supersingular elliptic curves in characteristic $p > 0$ are precisely those for which $\mathrm{End}_{\overline{K}}(E) \otimes \mathbf{Q}$ is a quaternion algebra (cf. the references in 2.5.6).

**(3.5.5) Proposition.** *If $E$ is an elliptic curve over a field $K \subseteq \mathbf{F}_q$ $(q = p^r)$, then*

$$1 - \phi_q = [1] \boxminus \phi_q : E \longrightarrow E$$

*is a separable isogeny.*

*Proof.* We know from 3.2.4(ii) that the isogeny $\phi_q : E \longrightarrow E$ is not separable; thus $\phi_q^*(\omega) = 0$ (cf. 3.4.4). Applying 3.3.7, we obtain

$$(1 - \phi_q)^*(\omega) = [1]^*(\omega) - \phi_q^*(\omega) = \omega \neq 0,$$

which proves the result.

**(3.5.6) Exercise.** *Let $E$ be an elliptic curve over $K$, $L \supset K$ any field and $A \subset E(L)$ a finite subgroup. Then $A$ is isomorphic to the direct sum of at most two (finite) cyclic groups.*

# III. Arithmetic of Elliptic Curves

In this chapter we shall study elliptic curves over fields $K$ that are of interest to number theorists: finite fields, $p$-adic fields and number fields. In each case, the main question is to describe the set of $K$-rational points on a given elliptic curve. Our treatment will be rather minimalistic; the reader should consult [Hu], [Si 1] or [Ca 1] for more details.

## 1. Elliptic curves over finite fields

### 1.1 Elementary remarks

**(1.1.1)** Let $p$ be a prime, $q = p^r$ and $E$ an elliptic curve over $\mathbf{F}_q$. We are interested in counting the number of points $\#E(\mathbf{F}_{q^n})$ on $E$ that are rational over the various finite extensions of $\mathbf{F}_q$.

In the special case when $q = p$ and $E$ is given by the generalized Weierstrass equation (II.1.2.4.1), then $\#E(\mathbf{F}_p) - 1$ is equal to the number of solutions $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ of the congruence

$$y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}. \tag{1.1.1.1}$$

**(1.1.2) Exercise.** *For fixed $a, b, c \in \mathbf{Z}$, denote by $N_p(D)$ the number of solutions $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ of the congruence*

$$Dy^2 \equiv x^3 + ax^2 + bx + c \pmod{p},$$

*where $p$ is a prime and $D \in \mathbf{Z}$. Show that, if $p \nmid 2DD'$,*

$$N_p(D') = \begin{cases} N_p(D), & \text{if } \left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right) \\ 2p - N_p(D), & \text{if } \left(\frac{D}{p}\right) = -\left(\frac{D'}{p}\right) \end{cases}$$

*[Hint: Fix $x$.]*

**(1.1.3)** If $E$ has complex multiplication by $\mathbf{Z}[i]$ or $\mathbf{Z}[\rho]$, then (1.1.1.1) can be transformed into a diagonal congruence

$$Y^m \equiv aX^n + b \pmod{p} \tag{1.1.3.1}$$

with $(m, n) = (2, 4), (2, 3)$. In general, the number of solutions of (1.1.3.1) can be expressed in terms of Jacobi sums, or is given by an elementary expression (see [Ir-Ro] for more details).

**(1.1.4) Exercise.** *Reprove 0.5.3(iv), using the method from 1.1.2 (with a quadratic polynomial on the R.H.S.).*

### 1.2 Examples

**(1.2.1)** Let $E$ an elliptic curve over $\mathbf{F}_q$. Denote by $\phi_q : E \longrightarrow E^{(q)} = E$ the corresponding Frobenius morphism. If $E$ is in the generalized Weierstrass form, then $\phi_q(x, y) = (x^q, y^q)$. We shall identify $\mathbf{Z}$ with its image in $\mathrm{End}_K(E)$ (for any field $K \supset \mathbf{F}_q$); this means that we shall write $n$ instead of $[n]$ (for $n \in \mathbf{Z}$). We denote by $\mathbf{Z}[\phi_q]$ (resp. $\mathbf{Q}[\phi_q]$) the subring (resp. the $\mathbf{Q}$-subalgebra) of $\mathrm{End}_{\mathbf{F}_q}(E)$ (resp. of $\mathrm{End}_{\mathbf{F}_q}(E) \otimes \mathbf{Q}$) generated by $\phi_q$.

**(1.2.2) Lemma.** (i) $(\forall n \geq 1) \quad \#E(\mathbf{F}_{q^n}) = \deg(1 - \phi_q^n)$.
(ii) *If $\lambda : E' \longrightarrow E$ is an isogeny (over $\mathbf{F}_q$), then* $(\forall n \geq 1) \quad \#E'(\mathbf{F}_{q^n}) = \#E(\mathbf{F}_{q^n})$.

*Proof.* (i) By II.3.5.5, $1 - \phi_q^n = 1 - \phi_{q^n} : E \longrightarrow E$ is a separable isogeny, hence it follows from II.3.4.5(iii) that

$$\deg(1 - \phi_q^n) = \#\mathrm{Ker}(1 - \phi_q^n)(\overline{\mathbf{F}}_q) = \#\{P \in E(\overline{\mathbf{F}}_q) \mid \phi_q^n(P) = P\} = \#E(\mathbf{F}_{q^n}).$$

As regards (ii), the Snake Lemma applied to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E'(\overline{\mathbf{F}}_q) & \stackrel{\lambda}{\longrightarrow} & E(\overline{\mathbf{F}}_q) & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow 1-\phi_q^n & & \downarrow 1-\phi_q^n & & \\ 0 & \longrightarrow & A & \longrightarrow & E'(\overline{\mathbf{F}}_q) & \stackrel{\lambda}{\longrightarrow} & E(\overline{\mathbf{F}}_q) & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \end{array}$$

(where $A = \mathrm{Ker}(\lambda)(\overline{\mathbf{F}}_q)$ and $f$ is induced by $1-\phi_q^n$) yields an exact sequence

$$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow E'(\mathbf{F}_{q^n}) \stackrel{\lambda}{\longrightarrow} E(\mathbf{F}_{q^n}) \longrightarrow \mathrm{Coker}(f) \longrightarrow 0,$$

which implies the statement of (ii), as $\#\mathrm{Ker}(f) = \#\mathrm{Coker}(f)$ by the finiteness of $A$.

**(1.2.3) Examples:** (0) The discussion in 0.5.0-3 can be regarded as an elementary variant of 1.2.2, with 0.5.1 saying that $\phi_p = [p^*]$ on $C$.

(1) Consider the curves $V$, $E$ from II.2.5 over $\mathbf{F}_p$, where $p \neq 2$ is a prime. By 1.2.2(ii), $\#V(\mathbf{F}_{p^n}) = \#E(\mathbf{F}_{p^n})$ $(n \geq 1)$. Note that the affine curve $V_{\mathrm{aff}}$ is of the diagonal form 1.1.3.

(1a) If $p \equiv 3 \pmod 4$, denote by $C : y^2 = 1 - x^2$ the affine circle and by $\widetilde{C} \subset \mathbf{P}^2$ its projectivization. Then

$$V(\mathbf{F}_p) = V_{\mathrm{aff}}(\mathbf{F}_p) = C(\mathbf{F}_p) = \widetilde{C}(\mathbf{F}_p) \stackrel{\sim}{\longrightarrow} \mathbf{P}^1(\mathbf{F}_p).$$

Indeed, the second (resp. the first and the third) equality follow from the fact that $\mathbf{F}_p^{*4} = \mathbf{F}_p^{*2}$ (resp. $-1 \notin \mathbf{F}_p^{*2}$), and the last one is the isomorphism "circle = line" from 0.3.1.1. As a result,

$$\#V(\mathbf{F}_p) = \#E(\mathbf{F}_p) = \#\mathbf{P}^1(\mathbf{F}_p) = p + 1.$$

This elementary method breaks down over $\mathbf{F}_{p^2}$. However, the congruence I.8.4.9 for $\alpha = -p$ yields the equality $\phi_{p^2} = [-p] \in \mathrm{End}_{\mathbf{F}_p}(V)$, hence

$$\#V(\mathbf{F}_{p^2}) = \#E(\mathbf{F}_{p^2}) = \deg[p+1] = (p+1)^2.$$

(1b) If $p \equiv 1 \pmod 4$, then $p = \alpha\overline{\alpha}$, where $\alpha = a + ib \in \mathbf{Z}[i]$, $\alpha \equiv 1 \pmod{(2+2i)}$. Let $I \in \mathbf{F}_p$ be the image of $i \in \mathbf{Z}[i]$ under the projection $\mathbf{Z}[i] \longrightarrow \mathbf{Z}[i]/\alpha\mathbf{Z}[i] = \mathbf{F}_p$. The congruence I.8.4.9 for $\alpha$ then yields $\phi_p = [\alpha] \in \mathrm{End}_{\mathbf{F}_p}(V)$, hence

$$\#V(\mathbf{F}_p) = \#E(\mathbf{F}_p) = \deg[1-\alpha] = (1-\alpha)(1-\overline{\alpha}) = p + 1 - \alpha - \overline{\alpha} = p + 1 - 2a.$$

This result is usually deduced from a calculation of Jacobi sums ([Ir-Ro], Ch. 8,10,11).

(2) The same method also applies to "biquadratic twists" of the curves $V, E$ (in the sense of II.2.2.8(2)). More precisely, fix an integer $D \in \mathbf{Z} - \{0\}$, a prime number $p \nmid 2D$ and consider the affine curves

$$(V_D)_{\mathrm{aff}} : y_D^2 = 1 - Dx_D^4, \qquad (E_D)_{\mathrm{aff}} : v_D^2 = 4u_D^3 - 4Du_D$$

and the corresponding smooth projective curves $V_D, E_D$ (all defined over $\mathbf{F}_p$). As before, $V_D$ and $E_D$ are elliptic curves over $\mathbf{F}_p$ and the map $f_D(x,y) = (1/x_D^2, -2y_D/x_D^3)$ defines an isogeny $f_D : V_D \longrightarrow E_D$ of degree 2.

Fix a fourth root $D^{1/4} \in \overline{\mathbf{F}}_p$ of $D$ modulo $p$. Then the formulas

$$x = x_D D^{1/4}, \qquad y = y_D, \qquad u = u_D (D^{1/4})^{-2}, \qquad v = v_D (D^{1/4})^{-3}$$

define isomorphisms $\overline{X} \stackrel{\sim}{\longrightarrow} \overline{X}_D$ (where $X = V, E$ and $\overline{X} = X_{\overline{\mathbf{F}}_p}$ denotes the base change of $X$ to $\overline{\mathbf{F}}_p$) which make the following diagram commutative:

$$\begin{array}{ccc} \overline{V} & \xrightarrow{\sim} & \overline{V}_D \\ \big\downarrow{\scriptstyle f} & & \big\downarrow{\scriptstyle f_D} \\ \overline{E} & \xrightarrow{\sim} & \overline{E}_D \end{array}$$

(2a) If $p \equiv 3 \pmod 4$, then the same argument as in (1a) shows that

$$\#V_D(\mathbf{F}_p) = \#E_D(\mathbf{F}_p) = \#\mathbf{P}^1(\mathbf{F}_p) = p+1.$$

(2b) If $p \equiv 1 \pmod 4$, we again write $p = \alpha\overline{\alpha}$ and $\mathbf{F}_p = \mathbf{Z}[i]/\alpha\mathbf{Z}[i]$, as in (1b).

Let $(x,y) \in V_{\mathrm{aff}}(\overline{\mathbf{F}}_p)$; when is the corresponding point $(x_D, y_D) = (x(D^{1/4})^{-1}, y) \in (V_D)_{\mathrm{aff}}(\overline{\mathbf{F}}_p)$ defined over $\mathbf{F}_p$? We have

$$(x_D, y_D) \in V_D(\mathbf{F}_p) \iff (x_D, y_D) = (x_D^p, y_D^p) \iff (D^{\frac{p-1}{4}}x, y) = (x^p, y^p);$$

recalling that the biquadratic residue symbol

$$\left(\frac{D}{\alpha}\right)_4 \in \{\pm 1, \pm i\}$$

is defined by the generalized Euler's criterion

$$\left(\frac{D}{\alpha}\right)_4 \equiv D^{\frac{p-1}{4}} \pmod \alpha,$$

it follows that

$$(x_D, y_D) \in V_D(\mathbf{F}_p) \iff \left(\phi_p - \left[\left(\frac{D}{\alpha}\right)_4\right]\right)(x,y) = 0$$

(the same argument also applies to the points of $V - V_{\mathrm{aff}}$). The formulas

$$\phi_p = [\alpha], \qquad \left(\frac{D}{\alpha}\right)_4^{-1} = \left(\frac{D}{\overline{\alpha}}\right)_4,$$

together with 1.2.2 then imply

$$\#V_D(\mathbf{F}_p) = \#E_D(\mathbf{F}_p) = \deg\left(\left[\left(\frac{D}{\alpha}\right)_4^{-1}\right]\phi_p - 1\right) = \deg\left(\left[\left(\frac{D}{\overline{\alpha}}\right)_4\right]\alpha - 1\right) = p + 1 - \left(\frac{D}{\overline{\alpha}}\right)_4\alpha - \left(\frac{D}{\alpha}\right)_4\overline{\alpha}.$$

## 1.3 Theorem of Hasse

**(1.3.1) Proposition.** *Let $E$ be an elliptic curve over $\mathbf{F}_q$ ($q = p^r$); put $\phi = \phi_q \in \mathrm{End}_{\mathbf{F}_q}(E)$. Then*
(i) *$\phi + \widehat{\phi} = a$, where $a \in \mathbf{Z}$, $|a| \le 2\sqrt{q}$.*
(ii) *$\phi^2 - a\phi + q = \widehat{\phi}^2 - a\widehat{\phi} + q = 0$ holds in $\mathrm{End}_{\mathbf{F}_q}(E)$.*
(iii) *If $|a| = 2\sqrt{q}$, then $r \in 2\mathbf{Z}$, $\phi = \widehat{\phi} = a/2 = \pm p^{r/2} = \pm\sqrt{q}$, $\mathbf{Z}[\phi] = \mathbf{Z}$.*
(iv) *If $|a| < 2\sqrt{q}$, then $\mathbf{Q}[\phi] \xrightarrow{\sim} \mathbf{Q}(\sqrt{a^2 - 4q})$ is an imaginary quadratic field.*
(v) *The two roots $\alpha, \beta \in \mathbf{C}$ of the polynomial $T^2 - aT + q = (T-\alpha)(T-\beta)$ are complex conjugate (i.e. $\beta = \overline{\alpha}$) and satisfy $|\alpha| = |\beta| = \sqrt{q}$.*

*Proof.* For every pair of integers $u, v \in \mathbf{Z}$, we obtain from II.3.1.4(iii) and II.3.2.4(ii) that

$$\deg(u + v\phi) = (u + v\phi)(u + v\widehat{\phi}) = u^2 + uv(\phi + \widehat{\phi}) + v^2 \deg\phi = u^2 + uv(\phi + \widehat{\phi}) + qv^2 \in \mathrm{End}_{\mathbf{F}_q}(E).$$

As $\deg(u+v\phi)$ is an integer, it follows that $\phi+\widehat{\phi}=a\in\mathbf{Z}$ ($\Longrightarrow \widehat{\phi}=a-\phi\in\mathbf{Z}[\phi]$), proving (i) and (ii), as

$$\phi^2-a\phi+q=\phi^2-(\phi+\widehat{\phi})\phi+\phi\widehat{\phi}=0$$

(and similarly for $\widehat{\phi}$). Moreover, the integer $\deg(u+v\phi)$ is always non-negative, which implies that

$$Q(u,v)=u^2+auv+qv^2=\deg(u+v\phi)\geq 0$$

is a positive semi-definite quadratic form on $\mathbf{Z}\times\mathbf{Z}$. It follows that the discriminant $\mathrm{disc}(Q)=a^2-4q\leq 0$, hence $|a|\leq 2\sqrt{q}$. If $|a|=2\sqrt{q}$, then $r$ is even, $a/2=\pm p^{r/2}=\pm\sqrt{q}\in\mathbf{Z}$ and

$$(a/2-\phi)(a/2-\widehat{\phi})=Q(a/2,-1)=0,$$

proving (iii). If $|a|<2\sqrt{q}$, then the polynomial $T^2-aT+q$ has two complex conjugate (non-real) roots

$$\alpha,\overline{\alpha}=\tfrac{a\pm\sqrt{a^2-4q}}{2}\in\mathbf{C}.$$

This implies that the $\mathbf{Q}$-algebra $R=\mathbf{Q}[T]/(T^2-aT+q)$ is a field, isomorphic to $\mathbf{Q}(\sqrt{a^2-4q})$; the two isomorphisms are given by

$$R\xrightarrow{\sim}\mathbf{Q}(\sqrt{a^2-4q}),\qquad T\mapsto\alpha\quad(\text{resp. }\ T\mapsto\overline{\alpha}).$$

By (ii), $\phi\notin\mathbf{Q}\subset\mathrm{End}_{\mathbf{F}_q}(E)\otimes\mathbf{Q}$, hence the map $T\mapsto\phi$ yields an isomorphism $R\xrightarrow{\sim}\mathbf{Q}[\phi]$. The statement (v) follows from the previous discussion.

**(1.3.2) Theorem (Hasse).** *In the notation of 1.3.1, let $\alpha,\beta\in\mathbf{C}$ be the roots of $T^2-aT+q=(T-\alpha)(T-\beta)$. Then*

$$\begin{gathered}\beta=\overline{\alpha},\qquad \alpha\overline{\alpha}=q,\qquad \alpha+\overline{\alpha}=a,\qquad |\alpha|=|\overline{\alpha}|=\sqrt{q}\\ (\forall n\geq 1)\qquad \#E(\mathbf{F}_{q^n})=(1-\alpha^n)(1-\overline{\alpha}^n)=q^n+1-\alpha^n-\overline{\alpha}^n\\ |\#E(\mathbf{F}_{q^n})-q^n-1|\leq 2q^{n/2}.\end{gathered}$$

*Proof.* In the notation of the proof of 1.3.1, in the case $|a|<2\sqrt{q}$ we have the isomorphisms

$$\mathbf{Q}[\phi]\xleftarrow{\sim}\mathbf{Q}[T]/(T^2-aT+q)\xrightarrow{\sim}\mathbf{Q}(\sqrt{a^2-4q}),$$

under which $T$ corresponds to $\phi$ on the L.H.S. (resp. to $\alpha$ on the R.H.S.). This implies that $\widehat{\phi}=a-\phi$ on the L.H.S. corresponds to $a-\alpha=\overline{\alpha}$ on the R.H.S, hence

$$\#E(\mathbf{F}_{q^n})=\deg(1-\phi^n)=(1-\phi^n)(1-\widehat{\phi}^n)=(1-\alpha^n)(1-\overline{\alpha}^n)\in\mathbf{Z}\subset\mathrm{End}_{\mathbf{F}_q}(E),\tag{1.3.2.1}$$

by 1.2.2 and 3.1.4(iii). If $|a|=2\sqrt{q}$, then $\phi=\widehat{\phi}=\alpha=\overline{\alpha}=a/2=\pm\sqrt{q}\in\mathbf{Z}\subset\mathrm{End}_{\mathbf{F}_q}(E)$, hence (1.3.2.1) holds in this case, too. Everything else follows from 1.3.1.

**(1.3.3) Zeta function of $E$.** Let $E$ be an elliptic curve over $\mathbf{F}_q$. Consider the generating function

$$Z(E,t)=\exp\left(\sum_{n=1}^{\infty}\#E(\mathbf{F}_{q^n})\frac{t^n}{n}\right)\in\mathbf{Q}[[t]].\tag{1.3.3.1}$$

The equality of formal power series

$$\sum_{n=1}^{\infty}\frac{c^nt^n}{n}=-\log(1-ct)\qquad\qquad(c\in\mathbf{C})$$

together with Hasse's Theorem 1.3.2 imply that

$$Z(E,t) = \frac{(1-\alpha t)(1-\overline{\alpha}t)}{(1-t)(1-qt)} \tag{1.3.3.2}$$

is a *rational function*. The **zeta function** of $E$, defined by

$$\zeta(E,s) = Z(E,q^{-s}),$$

is then equal to

$$\zeta(E,s) = \frac{(1-\alpha q^{-s})(1-\overline{\alpha}q^{-s})}{(1-q^{-s})(1-q^{1-s})}, \tag{1.3.3.3}$$

which is a meromorphic function in $\mathbf{C}$ satisfying

$$\zeta(E,s) = \zeta(E,1-s).$$

The fact that

$$|\alpha| = |\overline{\alpha}| = \sqrt{q}$$

is equivalent to the **Riemann hypothesis for** $\zeta(E,s)$:

$$\zeta(E,s) = 0 \Longrightarrow \mathrm{Re}(s) = \frac{1}{2}.$$

**(1.3.4) Example:** In the situation of 1.2.3(2a), the formula $\#V_D(\mathbf{F}_p) = p+1$ together with 1.3.2 imply that $\widehat{\phi}_p = -\phi_p$, hence $\phi_p^2 = -\widehat{\phi}_p\phi_p = -p$ in $\mathrm{End}_{\mathbf{F}_p}(V_D)$. For $D=1$, we obtain Eisenstein's congruence I.8.4.9 (I.9.4.6) for $\alpha = -p$.

### 1.4 Vista: Zeta functions in geometry

**(1.4.1)** The Riemann zeta function can be written either as an infinite series, or as an infinite product:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \left(1-p^{-s}\right)^{-1}, \tag{1.4.1.1}$$

where the product is taken over all prime numbers. Noting that the set of primes corresponds to the set of maximal ideals $\mathrm{Max}(\mathbf{Z}) = \{(p)\}$ of the ring $\mathbf{Z}$, the following generalization of (1.4.1.1) is fairly natural.

**(1.4.2)** Let

$$A = \mathbf{Z}[T_1,\ldots,T_M]/(f_1,\ldots,f_N) \tag{1.4.2.1}$$

be a finitely generated ring (over $\mathbf{Z}$). By Hilbert's Nullstellensatz, an ideal $I \subset A$ is maximal $\iff$ $A/I$ is a finite field. We denote, for each maximal ideal $\mathfrak{m} \in \mathrm{Max}(A)$, by

$$N(\mathfrak{m}) = \#A/\mathfrak{m} = \#k(\mathfrak{m})$$

the number of elements of the residue field of $\mathfrak{m}$ (roughly speaking, $N(\mathfrak{m})$ measures the "size" of $\mathfrak{m}$). The **zeta function of** $A$ is then defined as

$$\zeta(A,s) = \prod_{\mathfrak{m}\in\mathrm{Max}(A)} \left(1-N(\mathfrak{m})^{-s}\right)^{-1}. \tag{1.4.2.2}$$

One can show that the product (1.4.2.2) is absolutely convergent in the half-plane $\mathrm{Re}(s) > \dim(A)$.

**(1.4.3) Examples:** (1) $\zeta(\mathbf{Z},s) = \zeta(s)$. More generally, for each integer $N \geq 1$,

$$\zeta(\mathbf{Z}[1/N],s)=\prod_{p\nmid N}\left(1-p^{-s}\right)^{-1}=\sum_{\substack{n=1\\(n,N)=1}}^{\infty}n^{-s}.$$

(2) As $\mathbf{Z}[i]$ is a principal ideal domain, the description of its irreducible elements in 0.4.3.0 implies that

$$\zeta(\mathbf{Z}[i],s)=\left(1-2^{-s}\right)^{-1}\prod_{p\equiv 1(4)}\left(1-p^{-s}\right)^{-2}\prod_{p\equiv 3(4)}\left(1-p^{-2s}\right)^{-1}=\zeta(s)\prod_{p\neq 2}\left(1-(-1)^{\frac{p-1}{2}}p^{-s}\right)^{-1}=$$
$$=\zeta(s)\sum_{\substack{n=1\\2\nmid n}}^{\infty}(-1)^{\frac{n-1}{2}}n^{-s}.$$

(3) More generally, if $\mathcal{O}_K$ is the ring of integers in a number field $K$, then $\zeta(\mathcal{O}_K,s)$ coincides with the "Dedekind zeta-function of $K$".

**(1.4.4)** Putting together all maximal ideals with the same residue characteristic $char(A/\mathfrak{m})=p$, we obtain

$$\zeta(A,s)=\prod_{p}\zeta(A/pA,s),\tag{1.4.4.1}$$

where

$$A/pA=\mathbf{F}_p[T_1,\dots,T_M]/(\overline{f}_1,\dots,\overline{f}_N),\qquad\qquad(\overline{f}_j=f_j\ (\mathrm{mod}\,p)).\tag{1.4.4.2}$$

Let us compute the factor $\zeta(A/pA,s)$ in the simplest non-trivial case $A=\mathbf{Z}[T]$. Maximal ideals of $A/pA=\mathbf{F}_p[T]$ are of the form $\mathfrak{m}=(f)$, where $f\in\mathbf{F}_p[T]$ is a monic irreducible polynomial of degree $d=\deg(f)\geq 1$; then $N(\mathfrak{m})=p^d$. Denote by $a_d$ the number of such polynomials with $\deg(f)=d$ fixed; factorizing the polynomial $T^{p^N}-T$ into irreducible factors yields

$$(\forall N\geq 1)\qquad\sum_{d|N}da_d=p^N.$$

Writing

$$\zeta(\mathbf{F}_p[T],s)=\prod_{d=1}^{\infty}(1-p^{-ds})^{-a_d}=Z(p^{-s}),$$

where

$$Z(t)=Z(\mathbf{F}_p[T],t)=\prod_{d=1}^{\infty}(1-t^d)^{-a_d},$$

we obtain

$$\log Z(t)=\sum_{d=1}^{\infty}a_d\sum_{n=1}^{\infty}\frac{t^{nd}}{n}=\sum_{N=1}^{\infty}\frac{t^N}{N}\sum_{d|N}da_d=\sum_{N=1}^{\infty}\frac{p^Nt^N}{N}=-\log(1-pt),$$

hence

$$Z(\mathbf{F}_p[T],t)=\frac{1}{1-pt},\qquad\zeta(\mathbf{F}_p[T],s)=\frac{1}{1-p^{1-s}}.$$

**(1.4.5)** This calculation can be generalized to arbitrary $A$ as follows. The ring $A$ from (1.4.2.1) is the ring of functions on the affine "variety over $\mathbf{Z}$"

$$X:f_1=\dots=f_N=0,\qquad X\subset\mathbf{A}_{\mathbf{Z}}^M\tag{1.4.5.1}$$

and $A/pA$ is the ring of functions on the affine "variety" over $\mathbf{F}_p$

$$X_p = X \otimes_{\mathbf{Z}} \mathbf{F}_p : \overline{f}_1 = \cdots = \overline{f}_N = 0, \qquad X_p \subset \mathbf{A}^M_{\mathbf{F}_p}. \tag{1.4.5.2}$$

The points on $X_p$ with coordinates in $\overline{\mathbf{F}}_p$ correspond bijectively to homomorphisms of $\mathbf{F}_p$-algebras $A/pA \longrightarrow \overline{\mathbf{F}}_p$, by the correspondence

$$\mathrm{Hom}_{\mathbf{F}_p - Alg}(A/pA, \overline{\mathbf{F}}_p) \xrightarrow{\sim} X_p(\overline{\mathbf{F}}_p), \qquad \alpha \mapsto a = (a_1, \ldots, a_M) = (\alpha(T_1), \ldots, \alpha(T_M)) \in \overline{\mathbf{F}}_p^M.$$

The kernel of $\alpha : A/pA \longrightarrow \mathbf{F}_p$ is a maximal ideal $\mathfrak{m} \in A/pA$, whose degree $d = \deg(\mathfrak{m})$ (defined by $N(\mathfrak{m}) = p^d$) is equal to the degree of the smallest extension $\mathbf{F}_p(a)/\mathbf{F}_p$ over which the coordinates of $a$ are defined. Two points $a, b \in X_p(\overline{F}_p)$ define the same $\mathfrak{m}$ if and only if they are conjugate by an element of $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$. Conversely, if $\mathfrak{m} \in A/pA$, then there are exactly $d = \deg(\mathfrak{m})$ embeddings $k(\mathfrak{m}) = (A/pA)/\mathfrak{m} \hookrightarrow \overline{\mathbf{F}}_p$; composing them with the canonical projection $(A/pA) \longrightarrow k(\mathfrak{m})$ we obtain $d$ conjugate points in $X_p(\overline{\mathbf{F}}_p)$. It follows that

$$(\forall N \geq 1) \qquad \sum_{d|N} d \sum_{\deg(\mathfrak{m})=d} 1 = \#X_p(\mathbf{F}_{p^N}). \tag{1.4.5.3}$$

In the case $A/pA = \mathbf{F}_p[T]$ this boils down to the correspondence between irreducible monic polynomials of degree $d$ in $\mathbf{F}_p[T]$ and the sets of their roots, which form $d$-tuples of conjugate points. The identity (1.4.5.3) then becomes (1.4.4.2).

As in 1.4.4, put

$$\zeta(A/pA, s) = Z(A/pA, p^{-s}).$$

The same calculation as in 1.4.4 then yields

$$\log Z(A/pA, t) = \sum_{d=1}^{\infty} \sum_{n=1}^{\infty} \frac{t^{dn}}{n} \sum_{\deg(\mathfrak{m})=d} 1 = \sum_{N=1}^{\infty} \frac{t^N}{N} \sum_{d|N} d \sum_{\deg(\mathfrak{m})=d} 1 = \sum_{N=1}^{\infty} \#X_p(\mathbf{F}_{p^N}) \frac{t^N}{N},$$

hence

$$Z(A/pA, t) = \exp\left( \sum_{N=1}^{\infty} \#X_p(\mathbf{F}_{p^N}) \frac{t^N}{N} \right), \qquad \zeta(A/pA, s) = \exp\left( \sum_{N=1}^{\infty} \#X_p(\mathbf{F}_{p^N}) \frac{p^{-sN}}{N} \right). \tag{1.4.5.4}$$

This explains the origin of the definition (1.3.3.1).

**(1.4.6)** One can translate the previous definitions into a purely geometric language, which will make sense also for non-affine "varieties", in fact for arbitrary schemes of finite type over $\mathrm{Spec}(\mathbf{Z})$. What does this mean? If $X$ is such a scheme, then it is a finite union of affine "varieties" of the type considered in 1.4.4 (i.e. $X = \mathrm{Spec}(A_1) \cup \cdots \cup \mathrm{Spec}(A_r)$, where each ring $A_i$ is as in (1.4.2.1)). A "closed point" $x \in |X|$ then corresponds to a maximal ideal $\mathfrak{m} \in A_i$ in one of the $A_i$'s; one defines $N(x) = N(\mathfrak{m})$ and

$$\zeta(X, s) = \prod_{x \in |X|} (1 - N(x)^{-s})^{-1}.$$

If $X = \mathrm{Spec}(A)$ is affine, then $\zeta(\mathrm{Spec}(A), s) = \zeta(A, s)$. The discussion from 1.4.4-5 makes sense in this more general context: (1.4.4.1) is replaced by

$$\zeta(X, s) = \prod_p \zeta(X_p, s), \tag{1.4.6.1}$$

where $X_p = X \otimes_{\mathbf{Z}} \mathbf{F}_p$ is the fibre of $X$ over $(p) \in \mathrm{Spec}(\mathbf{Z})$, and (1.4.5.4) reads as

$$\zeta(X_p, s) = \exp\left(\sum_{N=1}^{\infty} \#X_p(\mathbf{F}_{p^N})\frac{p^{-sN}}{N}\right). \tag{1.4.6.2}$$

**(1.4.7) Examples:** (1) **Affine space**. Let $A = \mathbf{Z}[T_1, \ldots, T_d]$, $X = \mathrm{Spec}(A) = \mathbf{A}^d_{\mathbf{Z}}$. Then $X_p = \mathbf{A}^d_{\mathbf{F}_p}$, hence $\#X_p(\mathbf{F}_{p^N}) = p^{dN}$,

$$Z(\mathbf{A}^d_{\mathbf{F}_p}, t) = \exp\left(\sum_{N=1}^{\infty} p^{dN}\frac{t^N}{N}\right) = \frac{1}{1-p^d t}, \qquad \zeta(\mathbf{A}^d_{\mathbf{F}_p}, s) = \frac{1}{1-p^{d-s}}, \qquad \zeta(\mathbf{A}^d_{\mathbf{Z}}, s) = \zeta(s-d).$$

(2) **Projective space**. Let $X = \mathbf{P}^d_{\mathbf{Z}}$ be the $d$-dimensional projective space over $\mathbf{Z}$; then $X_p = \mathbf{P}^d_{\mathbf{F}_p}$. For every field $F$ there is a decomposition of $\mathbf{P}^d(F)$ into a disjoint union

$$\mathbf{P}^d(F) = \mathbf{A}^d(F) \cup \mathbf{P}^{d-1}(F) = \mathbf{A}^d(F) \cup \mathbf{A}^{d-1}(F) \cup \cdots \cup \mathbf{A}^0(F). \tag{1.4.7.2.1}$$

Taking $F = \mathbf{F}_{p^N}$, we obtain $\#\mathbf{P}^d_{\mathbf{F}_p}(\mathbf{F}_{p^N}) = p^{dN} + p^{(d-1)N} + \cdots + 1$, hence

$$Z(\mathbf{P}^d_{\mathbf{F}_p}, t) = \frac{1}{(1-p^d t)(1-p^{d-1}t)\cdots(1-t)}, \qquad \zeta(\mathbf{P}^d_{\mathbf{F}_p}, s) = \frac{1}{(1-p^{d-s})(1-p^{d-1-s})\cdots(1-p^{-s})},$$
$$\zeta(\mathbf{P}^d_{\mathbf{Z}}, s) = \zeta(s-d)\zeta(s-d+1)\cdots\zeta(s).$$

(3) **Elliptic curve with CM by $\mathbf{Z}[i]$**. Let $V \subset \mathbf{P}^2_{\mathbf{Z}}$ be the projective curve from II.2.5, considered as a projective scheme over $\mathbf{Z}$. Combining the results of 1.2.3 with (1.3.3.2-3), we obtain

$$\zeta(V \otimes_{\mathbf{Z}} \mathbf{Z}[\tfrac{1}{2}], s) = \zeta(\mathbf{Z}[i][\tfrac{1}{2}], s)\zeta(\mathbf{Z}[i][\tfrac{1}{2}], s-1)L(V, s)^{-1},$$

where

$$L(V, s) = \prod_{\pi}(1 - \pi|\pi|^{-2s})^{-1} = \sum_{\alpha \equiv 1 \pmod{2+2i}} \frac{\alpha}{|\alpha|^{2s}},$$

and the product is taken over all irreducible elements $\pi \in \mathbf{Z}[i]$ satisfying $\pi \equiv 1 \pmod{2+2i}$.

**(1.4.8) Remarkable properties of zeta functions.** In the examples 1.4.7(2-3), the zeta function of the projective space (resp. of an elliptic curve with complex multiplication) naturally decomposes as a product. Is this a general phenomenon? If yes, does this decomposition have a geometric explanation?

For the projective space, the answer is fairly straightforward: the decomposition (1.4.7.2.1) makes sense for any field, in particular for $F = \mathbf{C}$. In this case the closure of $\mathbf{A}^j(\mathbf{C}) = \mathbf{C}^j$ $(j = 0, \ldots, d)$ in $\mathbf{P}^d(\mathbf{C})$ represents a generator of the homology group $H_{2j}(\mathbf{P}^d(\mathbf{C}), \mathbf{Z}) \xrightarrow{\sim} \mathbf{Z}$, and all other homology groups of $\mathbf{P}^d(\mathbf{C})$ vanish.

One can interpret in the similar vein the decomposition of $\zeta(V, s)$: the factor $\zeta(\mathbf{Z}[i], s)$ (resp. $\zeta(\mathbf{Z}[i], s-1)$) corresponds to the homology group $H_0(V(\mathbf{C}), \mathbf{Z})$ (resp. $H_2(V(\mathbf{C}), \mathbf{Z})$), while the "interesting" factor $L(V, s)$ is related to $H_1(V(\mathbf{C}), \mathbf{Z})$.

What happens in general? Assume that $X \longrightarrow \mathrm{Spec}(\mathbf{Z})$ is projective, flat, $X \otimes_{\mathbf{Z}} \mathbf{Q}$ is smooth over $\mathbf{Q}$, and $p$ is a prime number such that $X_p = X \otimes_{\mathbf{Z}} \mathbf{F}_p$ is smooth over $\mathbf{F}_p$ and irreducible; let $\mathbf{F}_q$ be the algebraic closure of $\mathbf{F}_p$ in the function field of $X_p$ and $d = \dim(X_p)$ the dimension of $X_p$. Then:

(1) The zeta function $\zeta(X_p, s)$ is a rational function of $q^{-s}$; more precisely,

$$\zeta(X_p, s) = \frac{P_1(q^{-s})\cdots P_{2d-1}(q^{-s})}{P_0(q^{-s})\cdots P_{2d}(q^{-s})}, \qquad P_i(t) \in \mathbf{Z}[t],\ P_i(0) = 1.$$

(2) There exists a functional equation relating $P_i(q^{-s})$ and $P_{2d-i}(q^{s-d})$.
(3) $\deg(P_i) = \dim_{\mathbf{Q}} H_i(X(\mathbf{C}), \mathbf{Q})$.

(4) For each $i = 0, \dots, 2d$,

$$P_i(t) = \prod_{j=1}^{\deg(P_i)} (1 - \alpha_{i,j} t), \qquad |\alpha_{i,j}| = q^{i/2}.$$

These are the famous "Weil Conjectures" formulated by A. Weil in 1949 (and proved in this generality by: (1) Dwork; (2) and (3) Grothendieck; (4) Deligne).

The most remarkable aspect of this story is the fact that there should be some natural geometric objects $h_i(X)$ ("motives", in Grothendieck's terminology) associated to $X$, which should be responsible for the topological homology groups $H_i(X(\mathbf{C}), \mathbf{Z})$ (which depend only on the set of complex points of $X$), and at the same time also for the individual factors $P_i(q^{-s})$ appearing in the decomposition of the zeta function $\zeta(X_p, s)$ (which is defined solely in terms of the geometry of $X_p$ over $\mathbf{F}_p$).

So what is a motive? Well, it is any %&!?*+ which has a zeta function ...

## 2. Elliptic curves over local fields

Throughout this section, $R$ will denote a discrete valuation ring, $K = \mathrm{Frac}(R)$ is fraction field, $\pi \in R$ a uniformizing element and $k = R/\pi R$ the residue field of $R$. Typical examples include $R = k[[\pi]]$ and $R = \mathbf{Z}_p$, $\pi = p$.

### 2.1 Minimal Weierstrass models

Given an elliptic curve $E$ over $K$, we would like to find a "nice" model $\mathcal{E}$ of $E$ over $R$ (and study its reduction $\widetilde{E} = \mathcal{E} \pmod{\pi}$ over $k$). Geometrically, $\mathcal{E} \longrightarrow \mathrm{Spec}(R)$ is a fibration over a one-dimensional base; its generic fibre $E$ is an elliptic curve over $K$, while its special fibre $\widetilde{E} = \mathcal{E} \otimes_R k$ can have singularities.

**(2.1.1) Definition.** *Let $E$ be an elliptic curve over $K$. A* **generalized Weierstrass model of $E$ over $R$** *is a generalized Weierstrass equation*

$$\mathcal{E} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1.1.1}$$

*of an elliptic curve isomorphic to $E$, in which all coefficients $a_i \in R$ lie in $R$. (In a fancy language, (2.1.1.1) is a projective $R$-scheme $\mathcal{E} \subset \mathbf{P}^2_R$ such that $\mathcal{E} \otimes_R K$ is isomorphic to $E$.)*

**(2.1.2) Discriminant.** Considering the coefficients $a_i$ of (the affine form of) the generalized Weierstrass equation

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \tag{2.1.2.1}$$

as variables, the intersection of the ideal $(f, \partial f/\partial x, \partial f/\partial y)$ in $\mathbf{Z}[x, y, a_1, \dots, a_6]$ with $\mathbf{Z}[a_1, \dots, a_6]$ is a principal ideal, generated by a polynomial $\Delta(a_1, \dots, a_6) \in \mathbf{Z}[a_1, \dots, a_6]$ (unique up to a sign). We refer to ([Si 1], III.1) for the general formulas; if $a_1 = a_2 = a_3 = 0$, then we have the usual formula

$$\Delta = -16(4a_4^3 + 27a_6^2),$$

which is also equal to

$$\Delta = 8(9(3a_6 - 2a_4x)(2f - y\,\partial f/\partial y) + 2(4a_4^2 - 9a_6x + 6a_4x^2)\,\partial f/\partial x).$$

In general, replacing $x, y$ by new variables $x', y'$ as in (I.2.2.2.1)

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned} \qquad (r, s, t \in K,\ u \in K^*) \tag{2.1.2.2}$$

has the effect of multiplying $\Delta$ by $u^{-12}$. One can also define the $j$-invariant $j(a_1, \ldots, a_6)$ for an arbitrary generalized Weierstrass equation; it coincides with the function

$$j = \frac{4(12a_4)^3}{4a_4^3 + 27a_6^2}$$

defined in II.2.2.6 if $a_1 = a_2 = a_3 = 0$ and is invariant under the transformations (2.1.2.2).

If $a_i \in K$, then the curve (2.1.2.1) is smooth over $K$ if and only if $\Delta \neq 0 \in K$.

**(2.1.3) Definition.** *We say that $\mathcal{E}$ in (2.1.1.1) is a* **minimal Weierstrass model** *of $E$ over $R$ if the valuation $\mathrm{ord}_\pi(\Delta(\mathcal{E})) \geq 0$ is minimal (among all generalized Weierstrass models of $E$ over $R$).*

**(2.1.4) Example.** Assume that $char(k) \neq 2, 3$. Then (the affine form of) the Weierstrass model $\mathcal{E}$

$$y^2 = x^3 + \pi^6$$

is *not* minimal, as the change of variables

$$x = \pi^2 x', \qquad y = \pi^3 y'$$

transforms $\mathcal{E}$ into a model $\mathcal{E}'$ given by

$$y'^2 = x'^3 + 1.$$

In this example, $\mathrm{ord}_\pi(\Delta(\mathcal{E})) = 12$, $\mathrm{ord}_\pi(\Delta(\mathcal{E}')) = 0$.

**(2.1.5) Proposition.** (i) *$E$ has a minimal Weierstrass model over $R$, which is unique up to transformations (2.1.2.2) with $u \in R^*$, $r, s, t \in R$.*
(ii) *If $\mathrm{ord}_\pi(\Delta(\mathcal{E})) < 12$, then $\mathcal{E}$ is a minimal Weierstrass model.*
(iii) *If $\mathcal{E}$ is a minimal Weierstrass model of $E$, then the $R$-submodule $R \cdot \omega_\mathcal{E} \subset \Gamma(E, \Omega_{E/K})$ (where $\omega_\mathcal{E} = dx/(2y + a_1x + a_3)$) does not depend on $\mathcal{E}$.*
(iv) *If $\mathcal{E}$ is any Weierstrass model of $E$ over $R$, then any change of variables (2.1.2.2) that transforms $\mathcal{E}$ to a minimal Weierstrass model has $u, r, s, t \in R$.*

*Proof.* See [Si 1], VII.1.3.

## 2.2 Reduction of Minimal Weierstrass models

**(2.2.1) Lemma-Definition.** *Let $E$ be an elliptic curve over $K$; fix a minimal Weierstrass model $\mathcal{E}$ of $E$ over $R$. The* **reduction** *$\widetilde{E} := \mathcal{E} \otimes_R k$ of $\mathcal{E}$, i.e. (the projectivization of) the curve*

$$y^2 + \overline{a}_1 xy + \overline{a}_3 y = x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6 \qquad (\overline{a}_i = a_i \pmod{\pi} \in k)$$

*is a cubic projective curve over $k$, whose isomorphism class depends only on $E$. Its discriminant is equal to $\Delta(\widetilde{E}) = \Delta(\mathcal{E}) \pmod{\pi}$.*

**(2.2.2) Definition.** *$E$ has* **good reduction** *if $\mathrm{ord}_\pi(\Delta(\mathcal{E})) = 0$ ($\iff \Delta(\widetilde{E}) \neq 0 \in k \iff \widetilde{E}$ is an elliptic curve over $k$). $E$ has* **bad reduction** *if $\pi | \Delta(\mathcal{E})$ ($\iff \widetilde{E}$ is not smooth over $k$).*

**(2.2.3) Example.** Assume that $char(k) \neq 2, 3$. Then

$$y^2 = x^3 + \pi$$

is (the affine form of) a minimal Weierstrass model $\mathcal{E}$ of $E$, by 2.1.5(ii); thus $E$ has bad reduction. Passing to the ramified extension $K' = K(\pi')$, where $\pi'^6 = \pi$, the base change $E' = E \otimes_K K'$ of $E$ has a Weierstrass model $\mathcal{E}'$ over $R'$ (= the ring of integers in $K'$) of the form

$$y'^2 = x'^3 + 1 \qquad (x' = x/\pi'^2,\ y' = y/\pi'^3),$$

hence $E'$ has good reduction.

**(2.2.4) The reduction map.** Every point $P \in E(K)$ can be represented by a point $(a : b : c) \in \mathcal{E}(R)$ with homogeneous coordinates $a, b, c \in R$; these coordinates are determined up to a common factor in $R^*$ and at least one of them lies in $R^*$. Taking their reductions modulo $\pi$, we obtain a point $(\overline{a} : \overline{b} : \overline{c}) \in \widetilde{E}(k)$, which depends only on $P$; it will be denoted by $\mathrm{red}(P)$. This defines a map

$$\mathrm{red} : E(K) \xleftarrow{\sim} \mathcal{E}(R) \xrightarrow{(\mathrm{mod}\,\pi)} \widetilde{E}(k) \tag{2.2.4.1}$$

which does not depend on the choice of $\mathcal{E}$ (by 2.1.5(i)).

**(2.2.5)** Let us assume, from now on, that if $\widetilde{E}$ is not smooth over $k$, then its (unique) non-smooth point $S$ is defined over $k$. This assumption is automatically satisfied if $char(k) \neq 2, 3$ or if $k$ is perfect (by II.1.3.1-2).

**(2.2.6) Proposition-Definition.** *Put*

$$\widetilde{E}^{\mathrm{sm}} = \begin{cases} \widetilde{E}, & \text{if } E \text{ has good reduction} \\ \widetilde{E} - \{S\}, & \text{if } E \text{ has bad reduction,} \end{cases}$$
$$E_0(K) = \mathrm{red}^{-1}(\widetilde{E}^{\mathrm{sm}}(k)).$$

*Then the reduction map*

$$\mathrm{red} : E_0(K) \longrightarrow \widetilde{E}^{\mathrm{sm}}(k)$$

*is a homomorphism of abelian groups (with the group operation on the target defined as in II.1.3.6).*

*Proof.* This follows from the fact that the usual geometric definition of the group law (in terms of intersections with lines in $\mathbf{P}^2$) defines an abelian group structure on $\mathcal{E}^{\mathrm{sm}}(R)$ (where $\mathcal{E}^{\mathrm{sm}} = \mathcal{E} - \{S\}$). [In fact, this defines on $\mathcal{E}^{\mathrm{sm}}$ a structure of a commutative group scheme over $R$, for which the natural maps $\mathcal{E}^{\mathrm{sm}} \otimes_R K \xrightarrow{\sim} E$ and $\mathcal{E}^{\mathrm{sm}} \otimes_R k \xrightarrow{\sim} \widetilde{E}^{\mathrm{sm}}$ are isomorphisms of group schemes.]

**(2.2.7) Lifting of points - Example:** The reduction map (2.2.4.1) need not be surjective, even if $R$ is complete. For example, if $R = \mathbf{Z}_p$, $\pi = p$, $k = \mathbf{F}_p$, let

$$\mathcal{E} : y^2 = x^3 + p, \qquad \widetilde{E} : y^2 = x^3, \qquad P = (0, 0) \in \widetilde{E}(\mathbf{F}_p).$$

Then there is no $Q \in \mathcal{E}(\mathbf{Z}_p)$ with $\mathrm{red}(Q) = P$. Note that the point $P$ in this example is the non-smooth point $P = S$ of $\widetilde{E}$.

**(2.2.8) Proposition.** *If $R$ is complete, then the homomorphism*

$$\mathrm{red} : E_0(K) \longrightarrow \widetilde{E}^{\mathrm{sm}}(k)$$

*is surjective.*

*Proof.* This follows from Hensel's Lemma (cf. [Si 1], VII.2.1).

**(2.2.9)** The group structure on $E^{\mathrm{sm}}(k')$ (for any field extension $k'/k$) was analyzed in II.1.3.7-10. We say that $E$ has **split multiplicative reduction**, resp. **non-split multiplicative reduction**, resp. **additive reduction**, if $\widetilde{E}$ is as in I.1.3.7, resp. I.1.3.9, resp. I.1.3.5.

**(2.2.10) Theorem (Kodaira, Néron).** *The group $E(K)/E_0(K)$ is finite. More precisely, if $E$ has split multiplicative reduction, then $E(K)/E_0(K)$ is cyclic of order $\mathrm{ord}_\pi(\Delta(\mathcal{E})) = -\mathrm{ord}_\pi(j(E))$; in all other cases it is an abelian group of order $\leq 4$.*

*"Proof".* The finiteness is easy to establish if the residue field $k$ is finite. In general one has to use the theory of Néron models. See [Si 1], VII.6.2; [Si 2], IV.9.2.

**(2.2.11)** Denote the kernel of the reduction map from 2.2.8 by $E_1(K)$. Then

$$E_1(K) = \{O\} \cup \{(x, y) \in E(K) \,|\, \mathrm{ord}_\pi(x), \mathrm{ord}_\pi(y) < 0\}$$

and there is exact sequence (assuming that $R$ is complete)

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \xrightarrow{\text{red}} \widetilde{E}^{\text{sm}}(k) \longrightarrow 0.$$

In Sect. 2.4 we shall investigate the torsion subgroup of $E_0(K)$ using a sequence of subgroups

$$E_0(K) \supset E_1(K) \supset E_2(K) \supset E_3(K) \cdots$$

analogous to the subgroups

$$R^* \supset 1 + \pi R \supset 1 + \pi^2 R \supset 1 + \pi^3 R \cdots$$

of the multiplicative group of $R$.

### 2.3 A digression on formal groups

**(2.3.1)** Given an elliptic curve $E$ in its generalized Weierstrass form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \tag{2.3.1.1}$$

we would like to study its local geometry around the point at infinity $O$. As in I.4.2.2, we have $\text{ord}_O(x) = -2$, $\text{ord}_O(y) = -3$; thus $z = -x/y$ is a local parameter at $O$. One can develop $x$ and $y$ into formal power series in $z$ as follows: rewriting (2.3.1.1) in the new variables

$$z = -\frac{x}{y}, \qquad w = -\frac{1}{y},$$

we obtain

$$w = w(z) = z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3.$$

Writing $w = z^3 + \cdots$ and substituting into (2.3.1.2), we obtain recursively

$$w = z^3 + a_1 z^4 + \cdots = z^3 + a_1 z^4 + (a_1^2 + a_2)z^5 + \cdots = z^3(1 + A_1 z + A_2 z^2 + \cdots) \in \mathbf{Z}[a_1, \ldots, a_6][[z]]$$

where $A_i \in \mathbf{Z}[a_1, \ldots, a_6]$ are some universal polynomials (i.e. we view the coefficients $a_i$ as variables). This yields formal expansions

$$\begin{aligned} x(z) &= \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z + \cdots \\ y(z) &= \frac{-1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + \cdots \\ \omega(z) &= \frac{dx}{2y + a_1 x + a_3} = (1 + a_1 z + (a_1^2 + a_2)z^2 + \cdots)\, dz \end{aligned} \tag{2.3.1.2}$$

with coefficients in $\mathbf{Z}[a_1, \ldots, a_6]$ (see [Si 1], IV.1 for more details).

**(2.3.2)** Similarly, the group law on $E$ can also be written in the variables $(z, w)$. For example, the inverse $P \mapsto -P = [-1]P$ is given in the $(x, y)$-coordinates by $[-1](x, y) = (x, -y - a_1 x - a_3)$. Passing to the $(z, w)$-coordinates, we obtain

$$[-1](z) = \frac{x(z)}{y(z) + a_1 x(z) + a_3} = -z + a_1 + \cdots \in \mathbf{Z}[a_1, \ldots, a_6][[z]]. \tag{2.3.2.1}$$

As regards the group law itself, note that a linear relation between $1, x, y$ is equivalent to a linear relation between $1, z, w$; thus we can use the standard geometric description of $\boxplus$ (I.10.1.1.1) also in the $(z, w)$-plane.

If $z_1, z_2$ are independent variables, put $P_i = (z_i, w(z_i))$ $(i = 1, 2)$ and consider the line $\ell = \overline{P_1 P_2} : w = az + b$ through the points $P_1, P_2$. Expanding both coefficients

$$a = a(z_1, z_2) = \frac{w(z_2) - w(z_1)}{z_2 - z_1}, \qquad b = b(z_1, z_2) = w(z_1) - a(z_1, z_2)z_1,$$

we obtain power series in $z_1, z_2$ with coefficients in $\mathbf{Z}[a_1, \ldots, a_6]$. Substituting $w = az + b$ to (2.3.1.2), we obtain a cubic equation for $z$ with roots $z_1, z_2, z_3$. Comparing the coefficients at $z^2$ (as in I.7.5.7) yields a power series expansion for the third root $z_3$, hence also for

$$F(z_1, z_2) = [-1](z_3) = z_1 + z_2 - a_1 z_1 z_2 + \cdots \in \mathbf{Z}[a_1, \ldots, a_6][[z_1, z_2]], \tag{2.3.2.2}$$

which is the formal group law $\boxplus$ in terms of the $z$-coordinate.

The series $F$ has the following properties:

$$F(z_1, z_2) = F(z_2, z_1), \qquad F(z_1, F(z_2, z_3)) = F(F(z_1, z_2), z_3), \qquad F(z, [-1]z) = 0,$$

which correspond to the commutativity, associativity and the inverse for $\boxplus$ on $E$ (again, see [Si 1], IV.1 for more details).

**(2.3.3) Definition.** *A formal group $\mathscr{F}$ (commutative, of dimension one) over a commutative ring $A$ is a power series $F(T_1, T_2) \in A[[T_1, T_2]]$ ("the formal group law of $\mathscr{F}$") with the following properties:*
(i) $F(T_1, T_2) = T_1 + T_2 + \cdots$.
(ii) $F(T_1, F(T_2, T_3)) = F(F(T_1, T_2), T_3)$.
(iii) $F(T_1, T_2) = F(T_2, T_1)$ *(this follows from (i)–(ii) for "good" rings $A$).*

**(2.3.4) Exercise.** *Given $F(T_1, T_2)$ satisfying (i)–(iii), show that $F(0, T) = F(T, 0) = T$ and that there is a unique power series $[-1](T) \in A[[T]]$ satisfying $F(T, [-1](T)) = 0$.*

**(2.3.5) Examples:** (1) **Formal additive group $\mathscr{F} = \widehat{\mathbf{G}}_a$:** $F(T_1, T_2) = T_1 + T_2$.
(2) **Formal multiplicative group $\mathscr{F} = \widehat{\mathbf{G}}_m$:** $F(T_1, T_2) = (1 + T_1)(1 + T_2) - 1 = T_1 + T_2 + T_1 T_2$.
(3) The construction from 2.3.2 gives a formal group $\widehat{\mathcal{E}}$ over $\mathbf{Z}[a_1, \ldots, a_6]$.

**(2.3.6) Definition.** *Let $\mathscr{F}$ be a formal group, with the formal group law $F(T_1, T_2)$. For an integer $n > 1$, put*

$$[n]_{\mathscr{F}}(T) = F(F(\cdots(F(\underbrace{T, T), T)\cdots, T}_{n-\text{times}}) \in A[[T]], \qquad [-n]_{\mathscr{F}}(T) = [n]_{\mathscr{F}}([-1](T)), \qquad [1]_{\mathscr{F}}(T) = T.$$

**(2.3.7) Examples:** (1) For $\mathscr{F} = \widehat{\mathbf{G}}_a$, $[n]_{\mathscr{F}}(T) = nT$. (2) For $\mathscr{F} = \widehat{\mathbf{G}}_m$, $[n]_{\mathscr{F}}(T) = (1 + T)^n - 1$.

**(2.3.8) Definition.** *Let $A$ be a complete local ring with maximal ideal $\mathfrak{m}$ and $\mathscr{F}$ a formal group over $A$. For each $i \geq 1$, denote by $\mathscr{F}(\mathfrak{m}^i)$ the set $\mathfrak{m}^i$ with the abelian group law $x \boxplus_F y = F(x, y)$ (note that $F(x, y)$ is convergent to an element of $\mathfrak{m}^i$, if $x, y \in \mathfrak{m}^i$).*

**(2.3.9) Examples:** (1) $\widehat{\mathbf{G}}_a(\mathfrak{m}^i) = (\mathfrak{m}^i, +)$. (2) $\widehat{\mathbf{G}}_m(\mathfrak{m}^i) \xrightarrow{\sim} (1 + \mathfrak{m}^i, \times)$.

### 2.4 The torsion subgroup of $E_1(K)$ via formal groups

In this section we assume that the discrete valuation ring $R$ is complete. Let $E$, $\mathcal{E}$ and $\widetilde{E}$ be as in 2.2, i.e. $E$ is an elliptic curve over $K = \mathrm{Frac}(R)$, $\mathcal{E}$ is a minimal Weierstrass model of $E$ over $R$ and $\widetilde{E}$ its reduction modulo $\pi$.

**(2.4.1)** Substituting to the universal power series (2.3.1.2) and (2.3.2.1-2) the values of the coefficients $a_i \in R$ of $\mathcal{E}$, we obtain power series $x(z), y(z) \in R[[z]]$ and a formal group over $R$, which will still be denoted by $\widehat{\mathcal{E}}$.

**(2.4.2) Proposition-Definition.** *For $i \geq 1$, put*

$$E_i(K) = \{O\} \cup \{(x,y) \in E(K) \,|\, \mathrm{ord}_\pi(x) \leq -2i,\ \mathrm{ord}_\pi(y) \leq -3i\}$$

*(for $i = 1$ this definition agrees with that from 2.2.11). The map $z \mapsto (x(z), y(z))$ defines a bijection $\pi^i R \xrightarrow{\sim} E_i(K)$, hence an isomorphism of abelian groups $\widehat{\mathcal{E}}(\pi^i R) \xrightarrow{\sim} E_i(K)$ (in particular, $E_i(K)$ is a subgroup of $E_0(K)$).*

*Proof.* See [Si 1], VII.2.2 in the case $i = 1$; the same argument applies for all $i \geq 1$.

**(2.4.3) Lemma.** *Let $\mathscr{F}$ be a formal group over $R$ in the sense of 2.3.3 (e.g. $\widehat{\mathbf{G}}_m$ or $\widehat{\mathcal{E}}$). Then:*
(i) *For each $i \geq 1$, there are canonical isomorphisms of abelian groups $\mathscr{F}(\pi^i R)/\mathscr{F}(\pi^{i+1}R) \xrightarrow{\sim} \pi^i R/\pi^{i+1}R \xrightarrow{\sim} (k,+)$.*
(ii) *If $n \in \mathbf{Z}$ and $char(k) \nmid n$, then the power series $[n]_{\mathscr{F}}(T) \in R[[T]]$ is invertible, in the sense that there exists (a unique) power series $g(T) \in R[[T]]$ such that $[n]_{\mathscr{F}}(g(T)) = T$. The power series $g(T)$ also satisfies $g([n]_{\mathscr{F}}(T)) = T$.*

*Proof.* (i) For $x, y \in \pi^j R$ $(j \geq 1)$, $F(x,y) \equiv x + y \pmod{\pi^{j+1}R}$ (where $F$ is the formal group law of $\mathscr{F}$).
(ii) The assumption on $n$ implies that $n \in R^*$ is invertible in $R$. As the power series $[n]_{\mathscr{F}}(T)$ begins with $nT + \cdots$, one constructs the coefficients of $g(T) = n^{-1}T + \cdots$ by induction (see [Si 1], IV.2.4).

**(2.4.4) Corollary.** *If $n \in \mathbf{Z}$ and $char(k) \nmid n$, then $\mathscr{F}(\pi R)_n = 0$. In particular, $E_1(K)_n = \widehat{\mathcal{E}}(\pi R)_n = 0$, i.e. there is no $n$-torsion in the kernel of the reduction map.*

**(2.4.5) Lemma.** *If $char(k) = p > 0$, then there exist power series $f(T), g(T) \in R[[T]]$ such that*

$$[p]_{\widehat{\mathcal{E}}}(T) = pf(T) + g(T^p) = pT + \cdots. \tag{2.4.5.1}$$

*Proof.* Denote the power series $[p]_{\widehat{\mathcal{E}}}(T) \in R[[T]]$ by $P(T)$. The translation invariance of the differential $\omega = \omega(z) = h(z)dz$ implies that

$$ph(T)dT = p\omega = [p]^*_{\widehat{\mathcal{E}}}\omega = h(P(T))P'(T)dT,$$

hence

$$h(P(T))P'(T) \in pR[[T]].$$

As $h(T) = 1 + h_1 T + \cdots$ (cf. (2.3.1.2)) and $P(T) = pT + \cdots$, we obtain $P'(T) \in pR[[T]]$; lemma follows.

**(2.4.6) A toy model:** For $\mathscr{F} = \widehat{\mathbf{G}}_m$, the torsion subgroup $\mathscr{F}(\pi R)_{tors}$ is just the group of roots of unity contained in $1 + \pi R$. If $char(k) = p > 0 = char(K)$, then each element $x \in \mathscr{F}(\pi R)_{tors} - \{0\}$ has order $m = p^n$ $(n \geq 1)$, i.e. $\zeta := 1 + x$ is a primitive $p^n$-th root of unity. It follows from

$$(\forall j \not\equiv 0 \pmod p) \quad (1-\zeta^j)/(1-\zeta) \in R^*, \qquad \prod_{\substack{0<j<p^n \\ p\nmid j}} (1-\zeta^j) = p$$

that the absolute ramification index of $R$ is equal to

$$e := \mathrm{ord}_\pi(p) = p^{n-1}(p-1)\,\mathrm{ord}_\pi(x) \implies p^{n-1}(p-1) \leq e.$$

**(2.4.7) Definition.** *For $Q \in \widehat{\mathcal{E}}(\pi R)$, put $\mathrm{ord}_\pi(Q) = \max\{i \geq 1 \,|\, Q \in \widehat{\mathcal{E}}(\pi^i R)\}$ (i.e. $\mathrm{ord}_\pi(x,y) = i \iff i = -\mathrm{ord}_\pi(x)/2 = -\mathrm{ord}_\pi(y)/3$, by 2.4.2).*

**(2.4.8) Theorem.** *Assume that $char(k) = p > 0$, $char(K) = 0$; denote by $e = \mathrm{ord}_\pi(p)$ the absolute ramification index of $R$. Let $Q \in \widehat{\mathcal{E}}(\pi R)_{tors}$ be a torsion element of exact order $m > 1$. Then $m = p^n$ with*

$$p^{n-1}(p-1) \leq e, \qquad \mathrm{ord}_\pi(Q) \leq \frac{e}{p^{n-1}(p-1)}.$$

*Proof.* Let $Q \in \widehat{\mathcal{E}}(\pi R)$. The formula (2.4.5.1) implies that

$$\mathrm{ord}_\pi([p]_{\widehat{\mathcal{E}}}(Q)) \begin{cases} \geq \min(e + \mathrm{ord}_\pi(Q), p \cdot \mathrm{ord}_\pi(Q)) & \\ = e + \mathrm{ord}_\pi(Q), & \text{if } (p-1)\mathrm{ord}_\pi(Q) > e. \end{cases} \tag{2.4.8.1}$$

Assume that $Q$ is torsion, of exact order $m > 1$. As there is no prime-to-$p$ torsion in $\widehat{\mathcal{E}}(\pi R)$ (by 2.4.4), we have $m = p^n$, $n \geq 1$. Assume first that $n = 1$. If $(p-1)\mathrm{ord}_\pi(Q) > e$, then (2.4.8.1) implies that $\mathrm{ord}_\pi([p]_{\widehat{\mathcal{E}}}(Q)) = e + \mathrm{ord}_\pi(Q) < \infty$, hence $[p]_{\widehat{\mathcal{E}}}(Q) \neq 0$, which is a contradiction. Thus $1 \leq \mathrm{ord}_\pi(Q) \leq e/(p-1)$, as claimed. If $n > 1$, then the same argument applied to $[p^{n-1}]_{\widehat{\mathcal{E}}}Q$ shows that $\mathrm{ord}_\pi([p^{n-1}]_{\widehat{\mathcal{E}}}Q) \leq e/(p-1)$, hence $\mathrm{ord}_\pi([p^i]_{\widehat{\mathcal{E}}}Q) \leq e/(p-1)$ for all $i = 0, \ldots, n-1$. Applying (2.4.8.1) to all $[p^i]_{\widehat{\mathcal{E}}}Q$ $(i = 0, \ldots, n-1)$ yields $\mathrm{ord}_\pi([p^{i+1}]_{\widehat{\mathcal{E}}}Q) \geq p \cdot \mathrm{ord}_\pi([p^i]_{\widehat{\mathcal{E}}}Q)$. The statement of the Theorem then follows by induction.

**(2.4.9) Corollary.** *If $e < p-1$, then $\widehat{\mathcal{E}}(\pi R)_{tors} = 0$, hence the restriction of the reduction map to the torsion subgroup*

$$E_0(K)_{tors} \hookrightarrow E_0(K) \xrightarrow{\mathrm{red}} \widetilde{E}^{\mathrm{sm}}(k)$$

*is* **injective**.

## 3. Elliptic curves over number fields

Throughout this section, $K$ will denote a number field, $\mathcal{O}_K$ its ring of integers, $M_K$ (resp. $M_K^f$) the set of all primes (resp. of all finite primes) of $K$. For each $v \in M_K^f$ we denote by $\mathcal{O}_v$ the localization of $\mathcal{O}_K$ at $v$ and by $\widehat{\mathcal{O}}_v$ (resp. $K_v = \mathrm{Frac}(\widehat{\mathcal{O}}_v)$) the $v$-adic completion of $\mathcal{O}_K$ (resp. of $K$). The (finite) residue field of $\mathcal{O}_v$ will be denoted by $k(v)$ and the valuation associated to $v$ by $\mathrm{ord}_v$. The basic example is that of $K = \mathbf{Q}$, when $\mathcal{O}_K = \mathbf{Z}$, $v = p$ is a usual prime, $\mathcal{O}_v$ consists of all rational numbers with denominators prime to $p$, $k(v) = \mathbf{F}_p$, $\widehat{\mathcal{O}}_v = \mathbf{Z}_p$ and $K_v = \mathbf{Q}_p$.

### 3.1 Minimal Weierstrass models

**(3.1.1)** Let $E$ be an elliptic curve over $K$. For each $v \in M_K^f$ there is a minimal Weierstrass model of $E$ over $\mathcal{O}_v$, with minimal discriminant $\Delta_{v,\min} \in \mathcal{O}_v - \{0\}$. Is it possible to find a *global* Weierstrass model $\mathcal{E}$ of $E$ in the (affine) form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in \mathcal{O}_K) \tag{3.1.1.1}$$

that would satisfy the minimality condition

$$\mathrm{ord}_v(\Delta(\mathcal{E})) = \mathrm{ord}_v(\Delta_{v,\min}) \tag{3.1.1.2}$$

for all $v \in M_K^f$? Let us investigate this question. Choosing any Weierstrass model $\mathcal{E}$ of $E$ of the form (3.1.1.1), we have

$$(\forall v \in M_K^f) \qquad \mathrm{ord}_v(\Delta(\mathcal{E})) \equiv \mathrm{ord}_v(\Delta_{v,\min}) \pmod{12}, \tag{3.1.1.3}$$

as any change of variables (2.1.2.2) multiplies $\Delta$ by $u^{-12}$. Defining the **global minimal discriminant ideal of** $E$ by

$$\Delta_{min} = \prod_{v \in M_K^f} \mathfrak{p}_v^{\mathrm{ord}_v(\Delta_{v,min})}$$

(where $\mathfrak{p}_v \subset \mathcal{O}_K$ is the prime ideal corresponding to $v$), we can rewrite (3.1.1.3) as

$$\Delta_{min} = \frac{\Delta(\mathcal{E})}{I^{12}},$$

where $I \subset \mathcal{O}_K$ is a non-zero *ideal*.

**(3.1.2)** If $I$ is not principal, then we cannot achieve (3.1.1.2) by any change of variables (2.1.2.2), hence there is no minimal Weierstrass model of the form (3.1.1.1). However, one can construct a slightly more general minimal Weierstrass model as follows. Let $S$ be the (finite) set of primes $v \in M_K^f$ such that our chosen $\mathcal{E}$ is not minimal at $v$, i.e.

$$S = \{v \in M_K^f \,|\, \mathrm{ord}_v(\Delta(\mathcal{E})) > \mathrm{ord}_v(\Delta_{v,min})\} \subset \{v \in M_K^f \,|\, \mathrm{ord}_v(\Delta(\mathcal{E})) \geq 12\}.$$

Denote by $\mathcal{O}_{K,S} = \mathcal{O}_K[1/S]$ the ring of $S$-integers in $K$. One can then glue together $\mathcal{E} \otimes \mathcal{O}_{K,S}$ with local minimal Weierstrass models of $E$ over each $\mathcal{O}_v$ ($v \in S$) along the common "general fibre" $E$. What one obtains is a minimal Weierstrass model $\mathcal{E}$ of $E$ which is not contained in $\mathbf{P}^2_{\mathcal{O}_K}$, but in a slightly more general version of $\mathbf{P}^2$. The point is that the usual construction of $\mathbf{P}^2 = \mathbf{P}(V)$ parametrizing lines (or hyperplanes) in a three-dimensional "vector space" $V$ works well over a field or a local ring, but not over a more general base, when one has to consider "families of vector spaces", i.e. vector bundles. In concrete terms, $\mathcal{E} \subset \mathbf{P}(V)$ will be contained in the "projective space" over $\mathcal{O}_K$ associated to a suitable projective $\mathcal{O}_K$-module $V$, which will not be free.

**(3.1.3)** If $I = (u)$ is principal, then for each $v \in S$ there is a change of variables

$$x = u_v^2 x_v + r_v, \qquad y = u_v^3 y_v + u_v^2 s_v x_v + t_v$$

producing a minimal Weierstrass model over $\mathcal{O}_v$, where $r_v, s_v, t_v, u_v \in \mathcal{O}_v$ are $v$-integral (by 2.1.5(iv)) and $\mathrm{ord}_v(u_v) = \mathrm{ord}_v(u)$. Choosing a triple $(r, s, t) \in \mathcal{O}_K^3$ that is $v$-adically close to $(r_v, s_v, t_v) \in \mathcal{O}_v^3$ for each $v \in S$, the transformation

$$x = u^2 x' + r \qquad y = u^3 y' + u^2 s x' + t$$

will produce the desired global minimal Weierstrass model of $E$ over $\mathcal{O}_K$ in the form (3.1.1.1) (see [Si 1], VIII.8.2 for more details).

**(3.1.4)** In particular, if $\mathcal{O}_K$ is a principal ideal domain (e.g. if $K = \mathbf{Q}$), every elliptic curve over $K$ admits a global minimal Weierstrass model in the form (3.1.1.1).

**(3.1.5) Definition.** *Let $E$ be an elliptic curve over $K$ and $v \in M_K^f$. We define* **the reduction $\widetilde{E}_v$ of $E$ modulo $v$** *to be the reduction modulo $v$ of any minimal Weierstrass model $\mathcal{E}_v$ of $E$ over $\mathcal{O}_v$. We say that $E$ has* **good reduction at** *$v$ if $\widetilde{E}_v$ is an elliptic curve over $k(v)$ ($\iff \mathrm{ord}_v(\Delta(\mathcal{E}_v)) = 0 \iff \mathrm{ord}_v(\Delta_{min}) = 0$).*

## 3.2 The torsion subgroup of $E(K)$

**(3.2.1).** *Let $E$ be an elliptic curve over $K$ and $v \in M_K^f$ a prime such that $E$ has good reduction at $v$ and $\mathrm{ord}_v(p) < p-1$ (where $p = char(k(v))$). Then the restriction of the reduction map $\mathrm{red}_v : E(K_v) \longrightarrow \widetilde{E}_v(k(v))$ to the torsion subgroup of $E(K)$*

$$E(K)_{tors} \hookrightarrow E(K_v)_{tors} \hookrightarrow E(K_v) \xrightarrow{\mathrm{red}_v} \widetilde{E}_v(k(v))$$

*is injective.*

*Proof.* By 2.4.9, already the restriction of $\mathrm{red}_v$ to $E(K_v)_{tors}$ is injective (note that $E_0(K_v) = E(K_v)$, as we are assuming that $E$ has good reduction at $v$).

**(3.2.2) Corollary.** *The torsion subgroup $E(K)_{tors}$ is finite and effectively computable.*

**(3.2.3) Proposition.** *Let $D \in \mathbf{Z}$ be a cube-free integer $D \geq 1$, and $E$ the elliptic curve over $K = \mathbf{Q}$ given by $E : X^3 + Y^3 = DZ^3$. Then*

$$E(\mathbf{Q})_{tors} = \begin{cases} \mathbf{Z}/3\mathbf{Z}, & D = 1 \\ \mathbf{Z}/2\mathbf{Z}, & D = 2 \\ 0, & D > 2. \end{cases}$$

*Proof.* $E$ has good reduction at each prime $p \nmid 3D$. Put

$$P_D = \{p \text{ prime} \,|\, p \equiv 5 \pmod 6, p \nmid D\}.$$

For each $p \in P_D$, the map $x \mapsto x^3$ is a bijection $\mathbf{F}_p \xrightarrow{\sim} \mathbf{F}_p$, hence the number of points in $\widetilde{E}_p(\mathbf{F}_p)$ is the same as in $C_D(\mathbf{F}_p)$, where $C_D : X + Y = DZ$. As $C_D \xrightarrow{\sim} \mathbf{P}^1$ (over $\mathbf{F}_p$), we have $\#\widetilde{E}_p(\mathbf{F}_p) = \#\mathbf{P}^1(\mathbf{F}_p) = p + 1$. It follows from 3.2.1 that

$$\#E(\mathbf{Q})_{tors} \,|\, \gcd\{p + 1 \,|\, p \in P_D\} = 6$$

(where the last equality is a consequence of Dirichlet's theorem on primes in arithmetic progressions). It remains to investigate the torsion points of order 2 and 3. As

$$E(\mathbf{C})_2 - \{O\} = \{(1 : 1 : \rho^j (2/D)^{1/3})\} \qquad (\rho = e^{2\pi i/3},\ O = (1 : -1 : 0)),$$

it follows that

$$E(\mathbf{Q})_2 = \begin{cases} \mathbf{Z}/2\mathbf{Z}, & D = 2 \\ 0, & D \neq 2. \end{cases}$$

Similarly,

$$E(\mathbf{C})_3 = \{(X : Y : Z) \in E(\mathbf{C}) \,|\, XYZ = 0\},$$

hence

$$E(\mathbf{Q})_3 = \begin{cases} \mathbf{Z}/3\mathbf{Z}, & D = 1 \\ 0, & D \neq 1. \end{cases}$$

Proposition follows.

**(3.2.4) Exercise.** *Let $E : y^2 = x^3 - Dx$, where $D \in \mathbf{Z} - \{0\}$ is an integer not divisible by the fourth power of any prime. Show that*

$$E(\mathbf{Q})_{tors} = \begin{cases} \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}, & D = n^2, n \in \mathbf{Z} \\ \mathbf{Z}/4\mathbf{Z}, & D = -4 \\ \mathbf{Z}/2\mathbf{Z}, & \textit{otherwise.} \end{cases}$$

**(3.2.5) Proposition.** *Let $E$ be an elliptic curve over a number field $K$ and $\mathcal{E}$ any Weierstrass model of $E$ over $\mathcal{O}_K$ (as in (3.1.1.1)). If $P = (x, y) \in \mathcal{E}(K)_{tors}$ is a torsion point of exact order $m > 1$, then*
(i) *If $m \neq p^n$ is not a prime power, then $x, y \in \mathcal{O}_K$.*
(ii) *If $m = p^n$ is a prime power, then*

$$(\forall v \in M_K^f) \qquad \mathrm{ord}_v(x) \geq -2r_v, \quad \mathrm{ord}_v(y) \geq -3r_v,$$

*where $r_v \geq 0$ is the largest integer satisfying $p^{n-1}(p-1)r_v \leq \mathrm{ord}_v(p)$ ($p = char(k(v))$).*

*Proof.* Fix $v$ and work with $\mathcal{E}_v := \mathcal{E} \otimes_{\mathcal{O}_K} \widehat{\mathcal{O}}_v$ over $\widehat{\mathcal{O}}_v$. If $x, y \in \mathcal{O}_K$, then there is nothing to prove. If not, then we can assume that $\mathcal{E}_v$ is minimal (if we pass to a minimal Weierstrass model via the transformation (2.1.2.2), the values of $\mathrm{ord}_v(x), \mathrm{ord}_v(y)$ decrease, by 2.1.5(iv)). If $\mathrm{ord}_v(x) < 0$ or $\mathrm{ord}_v(y) < 0$, then $(x, y) \in E_1(K_v) = \widehat{\mathcal{E}}_v(\pi_v \widehat{\mathcal{O}}_v)$, and we can apply the local result 2.4.8.

**(3.2.6) Theorem (Lutz, Nagell).** *Let $E$ be an elliptic curve over $\mathbf{Q}$ in the Weierstrass form*

$$y^2 = x^3 + Ax + B, \qquad (A, B \in \mathbf{Z}).$$

*Assume that $P = (x, y) \in E(\mathbf{Q})_{tors} - \{O\}$. Then*
(i) $x, y \in \mathbf{Z}$.
(ii) *Either $y = 0$ (i.e. $[2]P = O$), or $y^2 | 4A^3 + 27B^2$.*

*Proof.* (i) Let $m > 1$ be the exact order of $P$. If $m = 2$, then $y = 0$, which implies that $x \in \mathbf{Z}$ (as $A, B \in \mathbf{Z}$). If $m > 2$, then the integers $r_p$ in 3.2.5 are equal to $r_p = 0$ for all primes $p$, hence $x, y \in \mathbf{Z}$.
(ii) We can assume $y \neq 0$. Then $[2]P = (x_2, y_2) \in E(\mathbf{Q})_{tors} - \{O\}$, hence $x_2 \in \mathbf{Z}$. Explicit formulas for $x_2$ then give

$$4A^3 + 27B^2 = y^2(4(3x^2 + 4A)x_2 - (3x^3 - 5Ax - 27B)).$$

**(3.2.7) Exercise.** *Describe explicitly $E(\mathbf{Q})_{tors}$ (i.e. give the coordinates of all $\mathbf{Q}$-rational torsion points) for the following elliptic curves $E = E_j$:*

$$E_1 : y^2 = x^3 + 1, \qquad E_2 : y^2 = x^3 + 4x, \qquad E_3 : y^2 = x^3 - 4x, \qquad E_4 : y^2 - y = x^3 - x^2.$$

**(3.2.8)** The following general results on $E(K)_{tors}$ are much more difficult.

**(3.2.9) Theorem (Mazur, 1977).** *Let $E$ be an elliptic curve over $\mathbf{Q}$. Then*

$$E(\mathbf{Q})_{tors} \xrightarrow{\sim} \begin{cases} \mathbf{Z}/m\mathbf{Z}, & 1 \leq m \leq 10 \text{ or } m = 12 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2m\mathbf{Z}, & 1 \leq m \leq 4. \end{cases}$$

**(3.2.10) Theorem.** *For each $d \geq 1$ there is a constant $C(d)$ such that, for every number field $K$ of degree $[K : \mathbf{Q}] = d$ and every elliptic curve $E$ over $K$, $\#E(K)_{tors} \leq C(d)$.*

**(3.2.11)** This result was proved in the early 1990's for $d = 2, \ldots, 8$ by Kamieny-Mazur; their method was extended by Abramovich to $d = 9, \ldots, 14$. The general result is due to Merel (1994); subsequent work by Oesterlé and Parent yielded explicit upper bounds for $C(d)$.

### 3.3 The descent method

**(3.3.1) The Congruent Number Problem**. A **congruent number** is an integer $D \geq 1$ which occurs as the area of a right triangle with rational sides, i.e. such that there exist $a, b, c \in \mathbf{Q}^*_{>0}$ satisfying $a^2 + b^2 = c^2$ and $D = ab/2$. The parametrization (0.4.1.0.0) of the Pythagorean triples gives

$$(\exists t \in \mathbf{Q},\, t > 1) \qquad \frac{a}{c} = \frac{t^2 - 1}{t^2 + 1}, \qquad \frac{b}{c} = \frac{2t}{t^2 + 1} \quad \Longrightarrow \quad (\exists t \in \mathbf{Q},\, t > 1) \qquad D\left(\frac{t^2 + 1}{c}\right)^2 = t^3 - t. \tag{3.3.1.1}$$

This implies (possibly after replacing $t$ by $-1/t$ - exercise!) that $D$ is a congruent number if and only if the elliptic curve $E_D : Ds^2 = t^3 - t$ has a rational point $(t, s) \in E_D(\mathbf{Q})$ with $s \neq 0$. Note that the change of variables $D^2 s = s'$, $Dt = t'$ transforms $E_D$ into the curve $s'^2 = t'^3 - D^2 t'$. The same argument as in the proof of 3.2.3 then shows (with a little help from 1.2.3(2a)) that

$$\{O\} \cup \{(0, 0), (\pm 1, 0)\} = E_D(\mathbf{Q})_2 = E_D(\mathbf{Q})_{tors},$$

hence

$$D \text{ is a congruent number} \quad \Longleftrightarrow \quad E_D(\mathbf{Q}) \neq E_D(\mathbf{Q})_{tors}.$$

**(3.3.2) Theorem (Fermat).** *$D = 1$ is not a congruent number.*

*Proof.* Assume that $0 < a, b, c \in \mathbf{Q}$ satisfy $a^2 + b^2 = c^2$, $ab/2 = 1$. As in (3.3.1.1), these values give rise to a rational point $(t, s) \in E_1(\mathbf{Q}) - \{O\}$, with $t, s > 0$. Writing $t = u/v$, where $u > v \geq 1 \in \mathbf{Z}$ are relatively prime integers, we have $w := sv^2 \in \mathbf{Z}$, hence

$$w^2 = uv(u + v)(u - v). \tag{3.3.2.1}$$

Replacing $(u, v, w)$ by $((u + v)/2, (u - v)/2, w/2)$ if both $u, v$ are odd, we can assume that $u \not\equiv v \pmod 2$, which implies that the four numbers $u, v, u + v, u - v$ are pairwise relatively prime. The equation (3.3.2.1) then implies that

$$u = L^2, \qquad v = M^2, \qquad u + v = X^2, \qquad u - v = Y^2,$$

for positive integers $L, M, X, Y$. It follows from

$$\left(\frac{X+Y}{2}\right)^2 + \left(\frac{X-Y}{2}\right)^2 = \frac{X^2+Y^2}{2} = u = L^2, \qquad \frac{1}{2}\left(\frac{X+Y}{2}\right)\left(\frac{X-Y}{2}\right) = \frac{X^2-Y^2}{8} = \frac{v}{4} = \left(\frac{M}{2}\right)^2$$

that

$$a_1 = \frac{X+Y}{M}, \qquad b_1 = \frac{X-Y}{M}, \qquad c_1 = \frac{2L}{M}$$

is another triple of rational numbers satisfying $a_1^2 + b_1^2 = c_1^2$, $a_1 b_1/2 = 1$. Applying the parametrization (3.3.1.1) once again, we obtain another rational point $(t_1, s_1) = (u_1/v_1, w_1/v_1^2) \in E_1(\mathbf{Q})$, hence another solution of (3.3.2.1) in positive integers $u_1, v_1, w_1$. More precisely, we have

$$\frac{X+Y}{2L} = \frac{a_1}{c_1} = \frac{t_1^2 - 1}{t_1^2 + 1}, \qquad \frac{X-Y}{2L} = \frac{b_1}{c_1} = \frac{2t_1}{t_1^2+1}$$

for $t_1 = u_1/v_1 \in \mathbf{Q}$, where $u_1 > v_1 \geq 1 \in \mathbf{Z}$ are relatively prime integers. It follows that

$$t = \frac{u}{v} = \left(\frac{L}{M}\right)^2 = \frac{2L^2}{X^2 - Y^2} = \frac{(t_1^2+1)^2}{4t_1^3 - 4t_1} = \frac{(u_1^2+v_1^2)^2}{4u_1v_1(u_1^2 - v_1^2)}. \tag{3.3.2.2}$$

As $\gcd(u_1 v_1, u_1^2 + v_1^2) = 1$, we have $v \geq u_1 v_1 > v_1^2 \geq v_1$. Continuing this process we obtain an infinite decreasing sequence of positive integers $v > v_1 > v_2 > \cdots$ ("the infinite descent"), which is impossible.

**(3.3.3) Why does this argument work?** The point is that the formula (3.3.2.2), namely

$$t = \frac{(t_1^2+1)^2}{4t_1^3 - 4t_1},$$

is exactly the expression in the duplication formula on $E_1$ (cf. (I.7.5.8.2) in the analytic context); thus we have, for a suitable choice of the sign,

$$[2](t_1, \pm s_1) = (t, s).$$

In other words, the original point $P = (t, s)$ is equal to $[2]P_1$ for some $P_1 \in E(\mathbf{Q})$; repeating this procedure, we obtain $P = [2]P_1 = [4]P_2 = [8]P_3 = \cdots$, which will contradict the fact that multiplication by 2 "increases the size" of (non-torsion) points in $E(\mathbf{Q})$.

The fact that we were able to "divide" $P = (t, s)$ by 2 had something to do with the fact the factors in (3.3.2.1) were relatively prime to each other, hence each of them – not just their product – was a square.

These two observations, i.e. (I) the possibility of dividing rational points by 2, and (II) the fact that multiplication by 2 increases the "size" of rational points [in fact, 2 can be replaced by any integer $n > 1$] are at the basis of the proof of the following fundamental result.

**(3.3.4) Theorem ("Mordell-Weil Theorem").** *Let $E$ be an elliptic curve over a number field $K$. Then $E(K)$ is finitely generated, i.e. $E(K) \xrightarrow{\sim} E(K)_{tors} \times \mathbf{Z}^r$, with $E(K)_{tors}$ finite and $0 \le r < \infty$. [As we have seen in 3.2, the torsion subgroup $E(K)_{tors}$ can be determined quite easily. Effective determination of the "rank" $r = r(E/K)$ is a major open problem.]*

**(3.3.5) Proposition.** *$D = 2$ is not a congruent number.*

*Proof.* As in the proof of 3.3.2, we have to show that the diophantine equation

$$2w^2 = uv(u+v)(u-v) \tag{3.3.5.1}$$

has no integral solution $u, v, w \in \mathbf{Z}$ with $u, v, w > 0$ and $\gcd(u, v) = 1$. There are three possible cases:

$$(a)\ 2 \nmid uv; \qquad (b)\ 2|u,\ 2 \nmid v; \qquad (c)\ 2 \nmid u,\ 2|v.$$

As in 3.3.2, the case (a) gives rise to another solution $((u+v)/2, (u-v)/2, w/2)$, which satisfies (b) or (c).

In the case (b), the four numbers $u, v, u+v, u-v$ are pairwise relatively prime and $u$ is even, hence

$$u = 2L^2, \qquad v = M^2, \qquad u+v = X^2, \qquad u-v = Y^2,$$

for positive integers $L, M, X, Y$. As $2 \nmid XY$, we have

$$u + v \equiv u - v \equiv 1 \pmod 4,$$

which contradicts the fact that $2 \nmid v$.

In the case (c), we obtain

$$u = L^2, \qquad v = 2M^2, \qquad u+v = X^2, \qquad u-v = Y^2,$$

for positive integers $L, M, X, Y$. The formulas

$$\left(\frac{X+Y}{2}\right)^2 + \left(\frac{X-Y}{2}\right)^2 = u = L^2, \qquad \frac{1}{2}\left(\frac{X+Y}{2}\right)\left(\frac{X-Y}{2}\right) = \frac{v}{4} = 2\left(\frac{M}{2}\right)^2$$

then yields another right triangle with rational sides

$$a_1 = (X+Y)/M, \qquad b_1 = (X-Y)/M, \qquad c_1 = 2L/M$$

and area $a_1 b_1/2 = 2$, which gives rise to a new integral solution $(u_1, v_1, w_1)$ of (3.3.5.1) satisfying $w_1 < w$, leading to a contradiction.

**(3.3.6) Analysis of the 2-descent.** Let us investigate the division of points by 2 in more detail. Assume that $L$ is a field of characteristic $char(L) \neq 2$ and $E$ an elliptic curve over $L$ such that $E(\overline{L})_2 = E(L)_2$ (i.e. all 2-torsion points are defined over $L$). This means that $E$ can be given by a Weierstrass equation

$$E : y^2 = g(x) = (x - e_1)(x - e_2)(x - e_3),$$

where $g(x)$ has three distinct roots $e_1, e_2, e_3 \in L$ *contained in* $L$. Assume that $(x, y) \in E(L) - E(L)_2$. Following the same method as in the proof of 3.3.2, we shall write each of the factors $x - e_j = d_j z_j^2 \in L^*$ as a product of its "square-free part" $d_j$ and a square of $z_j \in L^*$. If the square-free parts $d_j$ are fixed (of course, $d_1 d_2 d_3 = (y/z_1 z_2 z_3)^2 \in L^{*2}$ has to be a square in $L$), elimination of the variable $x$ gives equations

$$\begin{aligned} d_1 z_1^2 - d_2 z_2^2 &= e_2 - e_1 \\ d_2 z_2^2 - d_3 z_3^2 &= e_3 - e_2 \\ d_3 z_3^2 - d_1 z_1^2 &= e_1 - e_3 \end{aligned} \tag{3.3.6.1}$$

for the values $z_j \in L^*$. In other words, a point $(x, y) \in E(L) - \{O\}$ satisfying $y \neq 0$ defines $L$-rational points $(\pm z_1, \pm z_2, \pm z_3)$ on the curve (3.3.6.1), for suitable $d_j \in L^*$ satisfying $d_1 d_2 d_3 \in L^{*2}$. Conversely,

any $L$-rational point $(z_1, z_2, z_3)$ on (3.3.6.1) gives rise to $L$-rational points $(e_1 + d_1 z_1^2, \pm(d_1 d_2 d_3)^{1/2} z_1 z_2 z_3) \in E(L) - \{O\}$.

More precisely, one needs to work also with points at infinity; passing to the homogeneous coordinates $(Z_0 : Z_1 : Z_2 : Z_3)$ in $\mathbf{P}^3$, consider for each triple $d = (d_1, d_2, d_3) \in (L^*)^{\oplus 3}$ the projectivization $C_d$ of (3.3.6.1), given by

$$\begin{aligned} d_1 Z_1^2 - d_2 Z_2^2 &= (e_2 - e_1) Z_0^2 \\ d_2 Z_2^2 - d_3 Z_3^2 &= (e_3 - e_2) Z_0^2 \\ d_3 Z_3^2 - d_1 Z_1^2 &= (e_1 - e_3) Z_0^2 \end{aligned} \tag{3.3.6.2}$$

(where $z_j = Z_j/Z_0$, $j = 1, 2, 3$). Note that if we replace each $d_j$ by $d'_j = d_j c_j^2$ (for $c_j \in L^*$), then the curve $C_{d'}$ will be isomorphic to $C_d$ (over $L$); one has to replace $Z_j$ by $c_j Z'_j$ $(j = 1, 2, 3)$.

Put

$$G(L) = \operatorname{Ker}\left(\text{product} : (L^*/L^{*2})^{\oplus 3} \longrightarrow L^*/L^{*2}\right);$$

this is a natural space of parameters for the triples $d = (d_1, d_2, d_3)$. We have just seen that the curve $C_d$ depends (up to isomorphism defined over $L$) only on the image of $d$ in $G(L)$.

If $L$ is a number field, then, as we shall see in 3.3.10 below, congruence considerations severely restrict the possible values of $d$ for which the curve $C_d$ admits an $L$-rational point.

**(3.3.7) Proposition.** *Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3) = g(x)$ be an elliptic curve over a field $L$, with $e_1, e_2, e_3 \in L$. For each $i = 1, 2, 3$, define a map $f_i : E(L) \longrightarrow L^*$ by*

$$f_i(O) = 1, \qquad f_i((x, y)) = x - e_i \quad (\text{if } x \neq e_i), \qquad f_i((e_i, 0)) = (e_j - e_i)(e_k - e_i) \qquad (\text{if } \{i, j, k\} = \{1, 2, 3\}).$$

*Then:* (i) *The map $f = (f_1, f_2, f_3) \pmod{(L^{*2})^{\oplus 3}} : E(L) \longrightarrow G(L)$ is a homomorphism of abelian groups.*
(ii) *The kernel of $f$ is equal to $\operatorname{Ker}(f) = 2E(L) = [2]E(L)$.*
(iii) *The image of $f$ consists of those $d = (d_1, d_2, d_3) \in G(L)$ for which $C_d(L) \neq \emptyset$, i.e. for which the curve $C_d$ has an $L$-rational point.*

*Proof.* (i) The equation of the curve implies that the image of the map $f$ is indeed contained in $G(L)$. By definition, $f_i(\boxminus P) = f_i(P) = f_i(P)^{-1} \pmod{L^{*2}}$; thus it is enough to check that

$$P \boxplus Q \boxplus R = O \quad \stackrel{?}{\Longrightarrow} \quad f_i(P) f_i(Q) f_i(R) \in L^{*2}$$

in the case when $\{P, Q, R\} \subset E(L)$ (possibly with multiplicities) is the intersection of $E$ with a non-vertical line $y = \ell(x) = ax + b$.

Assume first that $(e_i, 0) \neq P, Q, R$. Then

$$g(x) - \ell(x)^2 = (x - e_1)(x - e_2)(x - e_3) - \ell(x)^2 = (x - x(P))(x - x(Q))(x - x(R));$$

substituting $x = e_i$, we obtain $f_i(P) f_i(Q) f_i(R) = \ell(e_i)^2 \in L^{*2}$.

If $R = (e_i, 0)$, then $\ell(x) = c(x - e_i)$ with $c \in L$, hence

$$\frac{f_i(P) f_i(Q)}{f_i((e_j, 0)) f_i((e_k, 0))} = \frac{(x - x(P))(x - x(Q))}{(x - e_j)(x - e_k)}\bigg|_{x = e_i} = \frac{g(x) - \ell(x)^2}{g(x)}\bigg|_{x = e_i} = 1 - \frac{c^2(x - e_i)}{(x - e_j)(x - e_k)}\bigg|_{x = e_i} = 1,$$

proving (i). As regards (ii), we know from I.7.5.9 (or from II.1.2.1) that

$$f_i(2[P]) = h_i(P)^2 \tag{3.3.7.1}$$

for some rational function on $E$ (possibly defined over an extension of $L$). However, an explicit calculation shows that (3.3.7.1) holds for

$$h_i(x,y) = \frac{x^2 - 2e_i x - (e_i^2 + e_j e_k)}{2y} = \frac{(x-e_i)(x-e_j) + (e_j - e_i)(x-e_k)}{2y} = \frac{1}{2}\left(\frac{y}{x-e_k} + (e_j - e_i)\frac{x-e_k}{y}\right)$$

(where $\{i,j,k\} = \{1,2,3\}$). As $h_i$ is defined over $L$, it follows automatically from (i) and (3.3.7.1) that

$$[2]E(L) \subset \mathrm{Ker}(f).$$

In order to prove the converse, assume that $Q = (A,B) \in \mathrm{Ker}(f) \subset E(L)$. If $B \neq 0$, then $A - e_j = h_j^2$ and $B = h_1 h_2 h_3$ for some $h_j \in L^*$ $(j = 1,2,3)$. We would like to find $P = (x,y) \in E(L)$ satisfying $h_j(P) = h_j$ $(j = 1,2,3)$. Put

$$\begin{aligned} C &= h_1h_2 + h_1h_3 + h_2h_3 \\ x &= A + C = (h_i + h_j)(h_i + h_k) + e_i \in L \\ y &= (h_1 + h_2)(h_1 + h_3)(h_2 + h_3) \in L. \end{aligned}$$

Then $y^2 = (x-e_1)(x-e_2)(x-e_3)$, hence $P := (x,y) \in E(L)$, and

$$h_i + h_j = \frac{y}{x - e_k}, \qquad h_i - h_j = \frac{h_i^2 - h_j^2}{h_i + h_j} = (e_j - e_i)\frac{x-e_k}{y},$$

showing that $h_j = h_j(P)$ for all $j = 1,2,3$, hence $(A,B) = (A, h_1h_2h_3) = [2](x, \pm y)$ for a suitable choice of the sign. This proves (ii) (at least if $B \neq 0$; we leave the case $Q = (e_i, 0)$ to the reader). Finally, (iii) follows from the definitions (observing that $C_d$ has an $L$-rational point with $Z_0 = 0$ (i.e. "at infinity") if and only if $d = (1,1,1) \in G(L)$ is the neutral element of $G(L)$).

**(3.3.8) Why $f_i$?** The rational functions $f_i \in R(E)^*$ are characterized (up to a scalar) by their divisors

$$\mathrm{div}(f_i) = 2((e_i,0)) - 2(O), \qquad [2](e_i,0) = O.$$

This gives a hint how to generalize 3.3.7: if $n > 1$ is prime to the characteristic of $L$ and $E(L)_n = E(\overline{L})_n$, choose a basis $T_1, T_2$ of $E(L)_n = (\mathbf{Z}/n\mathbf{Z}) \cdot T_1 + (\mathbf{Z}/n\mathbf{Z}) \cdot T_2$. For each $i = 1,2$ there exist rational functions $f_i, h_i \in R(E)^*$ (unique up to scalar multiples) satisfying

$$\mathrm{div}(f_i) = n(T_i) - n(O), \qquad f_i([n]P) = h_i(P)^n.$$

Defining suitably the values of $f_i$ at $T_i$ and $O$, one obtains a map

$$f = (f_1, f_2) : E(L) \longrightarrow (L^*/L^{*n})^{\oplus 2},$$

which turns out to be a homomorphism with kernel $\mathrm{Ker}(f) = [n]E(L)$. We leave the details as an exercise to the reader (who will have to rediscover the Weil pairing in the process)!

**(3.3.9) Theorem ("Weak Mordell-Weil theorem").** *Let $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$ be an elliptic curve over a number field $K$, with $e_1, e_2, e_3 \in K$. Then $E(K)/2E(K)$ is finite.*

*Proof.* We are going to apply 3.3.6 for $L = K$ and all the completions $L = K_v$ of $K$ $(v \in M_K)$. For each $v$ the inclusion $K \subset K_v$ induces a commutative diagram

$$\begin{array}{ccc} f : E(K)/2E(K) & \xrightarrow{\sim} & \{d \in G(K) \mid C_d(K) \neq \emptyset\} \\ \downarrow & & \downarrow loc_v \\ f_v : E(K_v)/2E(K_v) & \xrightarrow{\sim} & \{d_v \in G(K_v) \mid C_{d_v}(K_v) \neq \emptyset\}. \end{array}$$

We define the **Selmer group** for the 2-descent on $E$ (over $K$) by

$$S(E/K,2) = \{d \in G(K) \mid (\forall v \in M_K) \quad loc_v(d) \in \mathrm{Im}(f_v)\} = \{d \in G(K) \mid (\forall v \in M_K) \quad C_d(K_v) \neq \emptyset\}.$$

What does this mean? The isomorphism $f$ is not particularly useful, as we do not know how to decide, in general, whether or not a given curve $C_d$ admits a $K$-rational point. Replacing $E(K)/2E(K)$ by the Selmer group simply means that, instead of testing solvability of the equations (3.3.6.2) in $Z_j \in \mathcal{O}_K$, we test solvability of the corresponding congruences modulo all ideals of $\mathcal{O}_K$.

By definition, $E(K)/2E(K) \subseteq S(E/K,2)$, so it is enough to prove the finiteness of $S(E/K,2)$. Put

$$S = \{v \in M_K^f \,|\, (\forall i < j) \quad \mathrm{ord}_v(e_i - e_j) \neq 0\},$$
$$K(S,2) = \{c \in K^*/K^{*2} \,|\, (\forall v \in M_K^f - S) \quad \mathrm{ord}_v(c) \equiv 0 \pmod 2\}.$$

**(3.3.10) Lemma.** *If $d = (d_1, d_2, d_3) \in S(E/K,2)$, then $d_j \in K(S,2)$ $(j = 1,2,3)$.*

*Proof.* Let $v \in M_K^f - S$; assume that there exists $P \in C_d(K_v)$. If $P \in \{Z_0 = 0\}$ lies at infinity, then $d_j \in K_v^{*2}$ for all $j = 1,2,3$, hence $\mathrm{ord}_v(d_j) \equiv 0 \pmod 2$. So we can assume that $P = (z_1, z_2, z_3) \in C_d(K_v)$ is not at infinity, with its affine coordinates $z_j$ satisfying 3.3.6.1. By assumption, $\mathrm{ord}_v(e_i - e_j) = 0$ for all $i < j$. Put $n_j = \mathrm{ord}_v(d_j z_j^2) \equiv \mathrm{ord}_v(d_j) \pmod 2$; then $n_1 + n_2 + n_3 \equiv 0 \pmod 2$, and we must show that all $n_i$ are even. If $n_i < 0$ for some $i$, then $n_1 = n_2 = n_3$, hence $n_i \equiv 0 \pmod 2$ for all $i$. If $n_i > 0$ for some $i$, then $n_j = n_k = 0$ for the remaining two, hence $n_i \equiv 0 \pmod 2$. Lemma is proved.

**(3.3.11) Corollary.** *The map $(d_1, d_2, d_3) \mapsto (d_1, d_2)$ induces an injective homomorphism $S(E/K,2) \hookrightarrow K(S,2) \oplus K(S,2)$.*

*End of Proof of Theorem 3.3.9.* In view of 3.3.11, it is enough to show:

**(3.3.12) Lemma.** *For every finite subset $S \subset M_K^f$, $K(S,2)$ is finite.*

*Proof.* Denote by $\mathcal{O}_{K,S} = \mathcal{O}_K[1/S]$ the ring of $S$-integers in $K$ and by $Cl(\mathcal{O}_{K,S})$ its group of classes of ideals. Then the homomorphism

$$K(S,2) \longrightarrow Cl(\mathcal{O}_{K,S}), \qquad c \pmod{K^{*2}} \mapsto \sum_{v \notin S} \left(\tfrac{1}{2}\mathrm{ord}_v(c)\right) \cdot v$$

sits in an exact sequence

$$0 \longrightarrow \mathcal{O}_{K,S}^*/\mathcal{O}_{K,S}^{*2} \longrightarrow K(S,2) \longrightarrow Cl(\mathcal{O}_{K,S})_2.$$

Dirichlet's unit theorem implies that $\mathcal{O}_{K,S}^*$ is a finitely generated abelian group, hence $\mathcal{O}_{K,S}^*/\mathcal{O}_{K,S}^{*2}$ is finite. The group $Cl(\mathcal{O}_{K,S})$ is finite, being a quotient of $Cl(\mathcal{O}_K)$. Lemma follows.

**(3.3.13)** Note that the proof of 3.3.9 gives an explicit upper bound for the number of generators of $E(K)/2E(K)$ (see [Si 1], X.1 for an example of explicit calculations). In fact, one can effectively compute the Selmer group $S(E/K,2)$ (not only in theory, but also in practice).

**(3.3.14) Exercise.** *Let $E$ be an elliptic curve over a field $L$, $L'/L$ a finite Galois extension and $n > 1$. Then the group* $\mathrm{Ker}(E(L)/nE(L) \longrightarrow E(L')/nE(L'))$ *is finite.*

**(3.3.15) Corollary.** *Let $E$ be an elliptic curve over a number field $K$. Then $E(K)/2E(K)$ is finite.*

**(3.3.16) Exercise ([Ca 1], [Se]).** *Let $L$ be a field of characteristic $char(L) \neq 3$ containing a primitive cubic root of unity $\rho$ (i.e. $\rho^3 = 1 \neq \rho$). For $A \in L^*$, consider the elliptic curve $E_A : X^3 + Y^3 = AZ^3$ (with $O = (1 : -1 : 0)$).*
(i) *Show that the map*

$$(x,y) \mapsto \left(\frac{x+y}{\rho - \rho^2}, \frac{\rho x + \rho^2 y}{\rho - \rho^2}, \frac{\rho^2 x + \rho y}{\rho - \rho^2}\right)$$

*(where $x = X/Z, y = Y/Z$) induces an injective homomorphism of groups*

$$f : E_A(L)/(\rho - \rho^2)E_A(L) \hookrightarrow (L^*/L^{*3})^{\oplus 3}.$$

(ii) *The image of $f$ consists of those triples $(a,b,c)$ with $abc = A \in L^*/L^{*3}$ for which the projective curve $aX^3 + bY^3 + cZ^3 = 0$ has a $L$-rational point.*
(iii) *If $L = K$ is a number field, give an upper bound for $\mathrm{Im}(f)$ in the spirit of 3.3.11.*
(iv) *Show that $E_1(\mathbf{Q}(\sqrt{-3})) = \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$.*

**(3.3.17) Exercise.** *Let $L$ be a field of characteristic $char(L) \neq 2$ and*

$$E : y^2 = x^3 + ax^2 + bx + c, \qquad E_D : Dy^2 = x^3 + ax^2 + bx + c$$

*elliptic curves (with $a, b, c, D \in L$). If $D \notin L^{*2}$ is not a square in $L$, show that there is a natural exact sequence*

$$0 \longrightarrow E(L) \longrightarrow E(L(\sqrt{D})) \longrightarrow E_D(L) \longrightarrow S \longrightarrow 0,$$

*where $2 \cdot S = 0$.*

**(3.3.18) Exercise.** *Let $L$ be a field of characteristic $char(L) \neq 3$ containing a primitive cubic root of unity. For $A, D \in L^*$, consider the elliptic curves*

$$E : X^3 + Y^3 = AZ^3, \qquad E_D : X^3 + Y^3 = ADZ^3, \qquad E_{D^2} : X^3 + Y^3 = AD^2Z^3.$$

*If $D \notin L^{*3}$ is not a cube in $L$, relate the groups $E(L), E_D(L), E_{D^2}(L)$ and $E(L(\sqrt[3]{D}))$.*

**(3.3.19) Exercise.** *If $D \equiv 3 \pmod 8$ is a prime number, show that $D$ is not a conguent number and that, in the notation of 3.3.1, $S(E_D/\mathbf{Q}, 2) = E_D(\mathbf{Q})_{tors}/2E_D(\mathbf{Q})_{tors} \xrightarrow{\sim} (\mathbf{Z}/2\mathbf{Z})^2$.*

**(3.3.20) Higher descent.** Let $E$ be an elliptic curve over a number field $K$ and $n > 1$ an integer. It is possible to define an auxilliary family of smooth projective curves $C_\alpha$ over $K$ that generalizes the family $C_d$ from (3.3.6.2). The parameter $\alpha$ is contained in a certain abelian group generalizing $G(K)$ from 3.3.6 and there is a natural isomorphism

$$E(K)/nE(K) \xrightarrow{\sim} \{\alpha \,|\, C_\alpha(K) \neq \emptyset\}.$$

The Selmer group for the $n$-descent is defined in the same way as for $n = 2$:

$$S(E/K, n) \xrightarrow{\sim} \{\alpha \,|\, (\forall v \in M_K) \quad C_\alpha(K_v) \neq \emptyset\}.$$

$S(E/K, n)$ is finite abelian group of exponent $n$; its number of generators can be bounded above in terms of the unit group and the ideal class group of the field generated over $K$ by the coordinates of all points from $E(\overline{K})_n$ (in analogy to 3.3.10-12). The Selmer group $S(E/K, n)$ is effectively computable, at least in theory, and for small values of $n$ even in practice.

In order to determine the rank $r$ of $E(K)$, one would need to know more about the difference between the Selmer group and $E(K)/nE(K)$. The quotient group $S(E/K, n)/(E(K)/nE(K))$ is equal to $Ш(E/K)_n$, the group of elements of order $n$ in the so-called Tate-Šafarevič group of $E$. Unfortunately, this group is very difficult to control, although $Ш(E/K)$ is conjectured to be always finite.

## 3.4 Heights

Roughly speaking, the height measures the size of a rational point on an elliptic curve by counting the number of digits necessary to write down the coordinates of the point (or perhaps just its $x$-coordinate).

If one makes a numerical experiments and calculates the coordinates of the multiples $[n]P$ of a (non-torsion) rational point $P$, a parabolic shape appears: the number of digits necessary to write $[n]P$ grows quadratically with $n$. This quadratic behaviour is the second ingredient used in the proof of the Mordell-Weil Theorem.

**(3.4.1) Heights on a projective space (over Q).** Consider the $n$-dimensional projective space $\mathbf{P}^n_{\mathbf{Q}}$ over $\mathbf{Q}$ with a fixed homogeneous coordinate system. Given a rational point $x \in \mathbf{P}^n(\mathbf{Q})$, we can write $x = (x_0 : \cdots : x_n)$, with $x_j \in \mathbf{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. This determines the values of the homogeneous

coordinates $x_j$ up to a common factor in $\{\pm 1\}$. One defines the **height** of $x$ (in fact, two heights: the "logarithmic height" $h$ will be more useful) by

$$H(x) = \max(|x_0|, \dots, |x_n|) \geq 1$$
$$h(x) = \log(H(x)) \geq 0.$$

In particular, a rational number $x = a/b$ (for $a, b \in \mathbf{Z}$, $\gcd(a,b) = 1$) is naturally a point of $\mathbf{P}^1(\mathbf{Q})$; its height will then be equal to

$$h\left(\frac{a}{b}\right) = \log(\max(|a|, |b|)).$$

**(3.4.2) Heights on a projective space (over $\overline{\mathbf{Q}}$).** If one works over a number field, one needs to use the *normalized valuations* on $K$, which are defined as follows (for $v \in M_K$):

$$\|x\|_v = \begin{cases} (Nv)^{-\mathrm{ord}_v(x)}, & v \in M_K^f \\ |x|^{[K_v:\mathbf{R}]}, & v|\infty, \end{cases}$$

where $Nv = \#k(v)$. The normalized valuations satisfy the product formula

$$(\forall x \in K^*) \qquad \prod_{v \in M_K} \|x\|_v = 1.$$

For $x \in \mathbf{P}^n(K)$, we choose any homogeneous coordinates $x = (x_0 : \cdots : x_n)$ of $x$ ($x_j \in K$) and put

$$H_K(x) = \prod_{v \in M_K} \max(\|x_0\|_v, \dots, \|x_n\|_v) \geq 1,$$

which is a finite product, independent of the choice of the homogeneous coordinates (thanks to the product formula). The quantities

$$H(x) = H_K(x)^{1/[K:\mathbf{Q}]}, \qquad h(x) = \log(H(x)) \geq 0$$

are then independent on the number field $K$; they define a function

$$h : \mathbf{P}^n(\overline{\mathbf{Q}}) \longrightarrow \mathbf{R}_{\geq 0},$$

which depends only on the fixed coordinate system in $\mathbf{P}^n$ (and which coincides on $\mathbf{P}^n(\mathbf{Q})$ with the height defined in 3.4.1).

**(3.4.3) Proposition-Definition.** (i) *Two real valued functions $f, f' : S \longrightarrow \mathbf{R}$ on a set $S$ are* **equivalent** *(notation: $f \sim f'$) if the function $|f(x) - f'(x)|$ is bounded on $S$.*
(ii) *If $h' : \mathbf{P}^n(\overline{\mathbf{Q}}) \longrightarrow \mathbf{R}_{\geq 0}$ is the height defined by another system of homogeneous coordinates, then $h' \sim h$.*

*Proof (Sketch).* The change of coordinates is given by a matrix $g \in GL_{n+1}(K)$; for every $v \in M_K^f$,

$$\max_i(\|\sum_j g_{ij} x_j\|_v) \leq (\max_{i,j} \|g_{ij}\|_v) \max_j \|x_j\|_v = C_v(g) \max_j \|x_j\|_v,$$

where $C_v(g) = 1$ for all but finitely many $v$; similar bounds exist for $v|\infty$ (see [Si 1], VIII.5.8 for more details).

**(3.4.4) Proposition.** *For every $C, D > 0$, the set*

$$\{x \in \mathbf{P}^n(\overline{\mathbf{Q}}) \,|\, h(x) \leq C,\ [k(x) : \mathbf{Q}] \leq D\}$$

*is finite (where $k(x)$ denotes the field of definition of $x$).*

*Proof.* It is enough to consider the points $x$ of a fixed degree $[k(x) : \mathbf{Q}] = d$. If $d = 1$, then the statement follows from the definition of the height given in 3.4.1. The general case can be reduced to the case $d = 1$ as follows: consider the map

$$f : \{x \in \mathbf{P}^n(\overline{\mathbf{Q}}) \mid [k(x) : \mathbf{Q}] = d\} \longrightarrow \{y \in \mathbf{P}^N(\mathbf{Q})\}$$

defined by sending $x = (x_0 : \cdots : x_n)$ to the coefficients $y = (y_0 : \cdots : y_N)$ of the norm form

$$N_{k(x)/\mathbf{Q}}(x_0T_0 + \cdots + x_nT_n) = \sum_\alpha y_\alpha T^\alpha$$

(where $\alpha$ is a multi-index). The map $f$ has finite fibres (more precisely, $\#f^{-1}(y) \leq d$ for each $y$) and

$$h(f(x)) \leq dh(x) + c(n, d),$$

where $c(n, d)$ is a constant depending only on $n, d$ (see [Si 1], VIII.5.11).

**(3.4.5) Heights on elliptic curves.** Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a number field $K$. Then the $x$-coordinate defines a morphism $x : E \longrightarrow \mathbf{P}^1_K$ of degree 2. We fix a coordinate system on $\mathbf{P}^1$ and define

$$\begin{aligned} h_x : E(\overline{K}) &\longrightarrow \mathbf{R}_{\geq 0} \\ P &\mapsto h(x(P)). \end{aligned}$$

This function is even, i.e. satisfies $h_x(\boxminus P) = h_x(P)$.

**(3.4.6) Theorem (Quadraticity of the height).** *The function $h_x$ is* **almost quadratic** *in the sense that the function*

$$\begin{gathered} \mathrm{Cube}(h_x) : (E \times E \times E)(\overline{K}) \longrightarrow \mathbf{R} \\ (P, Q, R) \mapsto h_x(P \boxplus Q \boxplus R) - h_x(P \boxplus Q) - h_x(P \boxplus R) - h_x(Q \boxplus R) + h_x(P) + h_x(Q) + h_x(R) \end{gathered}$$

*is bounded, i.e.* $\mathrm{Cube}(h_x) \sim 0$.

**(3.4.7)** In the lectures, Theorem 3.4.6 was related to the "Theorem of the cube". An elementary proof can be found in [Si 1], VIII.6.2 (+ 9.3).

**(3.4.8) Corollary.** (i) *(Tate) For each point $P \in E(\overline{K})$, the limit*

$$\widehat{h}(P) = \frac{1}{2} \lim_{N \longrightarrow \infty} \frac{h_x([m^N]P)}{m^{2N}} \geq 0$$

*exists and does not depend on the choice of $m \geq 2$ ($\widehat{h}$ is the* **canonical height** *= the* **Néron-Tate height***).*
(ii) $\widehat{h} \sim \frac{1}{2}h_x, \quad \widehat{h}(\boxminus P) = \widehat{h}(P)$.
(iii) $\mathrm{Cube}(\widehat{h}) = 0$, *i.e. $\widehat{h}$ is quadratic.*
(iv) $\langle P, Q\rangle := \frac{1}{2}(\widehat{h}(P \boxplus Q) - \widehat{h}(P) - \widehat{h}(Q))$ *is a bilinear symmetric form*

$$\langle\ ,\ \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbf{R}$$

*satisfying $\langle P, P\rangle \geq 0$ for all $P \in E(\overline{K})$.*
(v) *A point $P \in E(\overline{K})$ satisfies $\langle P, P\rangle = 0$ if and only if $P \in E(\overline{K})_{tors}$.*

*Proof .* This is an easy consequence of 3.4.6; see [Si 1], VIII.9.1-3 for more details.

**(3.4.9) Corollary (Weak properties of the height).** (i) *For every $P_0 \in E(K)$ there is a constant $C_1 = C_1(E, K, P_0)$ such that*

$$(\forall P \in E(K)) \quad h_x(P \boxplus P_0) \leq 2h_x(P) + C_1.$$

(ii) *There is a constant $C_2 = C_2(E, K)$ such that*

$$(\forall P \in E(K)) \quad h_x([2]P) \geq 4h_x(P) - C_2.$$

(iii) *For every $C > 0$, the set $\{P \in E(K) \,|\, h_x(P) < C\}$ is finite.*

**(3.4.10)** What really matters in 3.4.9 is the fact that $4 > 2$ (and the finiteness result 3.4.4, which implies (iii)). For $K = \mathbf{Q}$, the properties (i), (ii) can be established by an explicit calculation, without any elaborate machinery ([Si 1], VIII.4.2).

**(3.4.11) Proof of the Mordell-Weil Theorem.** Let $K$ be a number field and $E : y^2 = x^3 + Ax + B$ an elliptic curve over $K$. We want to prove that $E(K)$ is finitely generated. Extending $K$, we can assume that the roots of the cubic polynomial $x^3 + Ax + B$ are all contained in $K$; Theorem 3.3.9 then implies that $E(K)/2E(K)$ is finite (in fact, it was not necessary to extend $K$; cf. 3.3.14-15). This finiteness result, combined with 3.4.9(i)–(iii), is all one needs to prove that $E(K)$ is finitely generated:

Fix representatives $Q_1, \ldots, Q_m \in E(K)$ of all classes in $E(K)/2E(K)$. For every $P \in E(K)$ there exists a sequence $P_j \in E(K)$ of $K$-rational points obtained by "division by 2 with remainder":

$$P = P_0 = [2]P_1 \boxplus Q_{i_1}, \qquad P_1 = [2]P_2 \boxplus Q_{i_2}, \qquad P_2 = [2]P_3 \boxplus Q_{i_3} \qquad \text{etc.}$$

It follows that, for each $j \geq 1$,

$$h_x(P_j) \leq \frac{h_x([2]P_j) + C_2}{4} = \frac{(P_{j-1} \boxminus Q_{i_j}) + C_2}{4} \leq \frac{2h_x(P_{j-1}) + C_1 + C_2}{4} = \frac{1}{2}\, h_x(P_{j-1}) + \frac{C_1 + C_2}{4},$$

where $C_1 = \max C_1(Q_i)$. By induction, we obtain

$$h_x(P_j) \leq \frac{1}{2^j}\, h_x(P) + \left(1 + \frac{1}{2} + \cdots + \frac{1}{2^{j-1}}\right) \frac{C_1 + C_2}{4} < \frac{1}{2^j}\, h_x(P) + \frac{C_1 + C_2}{2}.$$

This implies that, for each $P \in E(K)$, there exists $j$ such that

$$h_x(P_j) \leq 1 + \frac{C_1 + C_2}{2},$$

which proves that $E(K)$ is generated by the finite set

$$\{Q_1, \ldots, Q_m\} \cup \{R \in E(K) \,|\, h_x(R) \leq 1 + (C_1 + C_2)/2\}.$$

Theorem 3.3.4 is proved.

## 3.5 The Conjecture of the Birch and Swinnerton-Dyer

None of the existing proofs of the Mordell-Weil theorem are effective; they yield an upper bound on the rank $r = r(E/K)$ of the group $E(K) \xrightarrow{\sim} E(K)_{tors} \times \mathbf{Z}^r$, but not the true value of $r$ nor a bound on the heights of a set of generators of $E(K)$.

**(3.5.1)** Numerical experiments involving a large number of elliptic curves over $\mathbf{Q}$ lead Birch and Swinnerton-Dyer [B-SD] to conjecture that the rank $r = r(E/K)$ can be read off from the asymptotic of the product

$$\prod_{Nv \leq x} \frac{\#\widetilde{E}_v(k(v))}{Nv} \sim c(\log x)^r. \tag{3.5.1.1}$$

At least formally, the asymptotic behaviour of the L.H.S. can be reformulated in terms of the $L$-function of $E$ (over $K$), which is defined as the infinite product over all finite primes of $K$

$$L(E/K, s) = \prod_v L_v(E/K, s) = \prod_v \left[(1 - \alpha_v(Nv)^{-s})(1 - \beta_v(Nv)^{-s})\right]^{-1}, \tag{3.5.1.2}$$

where

$$\beta_v = \overline{\alpha}_v, \qquad \#\widetilde{E}_v(k(v)) = (1 - \alpha_v)(1 - \beta_v)$$

if $E$ has good reduction at $v$, resp.

$$\beta_v = 0, \qquad \alpha_v = \begin{cases} 0, & \text{if } E \text{ has additive reduction at } v \\ 1, & \text{if } E \text{ has split multiplicative reduction at } v \\ -1, & \text{if } E \text{ has non-split multiplicative reduction at } v. \end{cases}$$

Hasse's Theorem 1.3.2 tells us that $|\alpha_v| = |\beta_v| = (Nv)^{1/2}$ for all primes of good reduction, which implies that the infinite product (3.5.1.2) is uniformly convergent and defines a holomorphic function in the region $Re(s) > 3/2$. The $L$-function $L(E/K, s)$ conjecturally admits holomorphic continuation to $\mathbf{C}$ and a functional equation with respect to the change of variables $s \longleftrightarrow 2 - s$. As

$$L_v(E/K, 1)^{-1} = \frac{\#\widetilde{E}_v^{sm}(k(v))}{Nv}$$

for all $v$, the asymptotics (3.5.1.1) can be formally replaced by

$$L(E/K, s) \sim C(s-1)^r \qquad\qquad (s \longrightarrow 1),$$

i.e. by a conjectural equality between the *analytic rank* of $E$ over $K$ and the rank $r(E/K)$:

$$(BSD) \qquad\qquad r_{an}(E/K) := \mathrm{ord}_{s=1} L(E/K, s) \stackrel{?}{=} r(E/K).$$

This is a weak version of the Conjecture of Birch and Swinnerton-Dyer. The strong version also predicts the value of the constant $C$, which involves, among others, the order of the Tate-Šafarevič group of $E$. In the words of Birch and Swinnerton-Dyer, the conjecture relates the behaviour of the $L$-function $L(E/K, s)$ at a point at which it is not known to be defined to the order of a group not known to be finite.

**(3.5.2)** What is known in the direction of this conjecture? For simplicity, we confine ourselves to elliptic curves defined over $K = \mathbf{Q}$.

(1) If $E$ has complex multiplication, then there is an explicit formula for $L(E/\mathbf{Q}, s)$ (proved by Deuring), which implies the analytic continuation and functional equation. For example, it follows from Eisenstein's result I.9.4.6 that the $L$-function of the curve $E - \{O\} : v^2 = u^3 - u$ (which is related to the congruent number problem for $D = 1$ treated in 3.3.2) is given by the formula from 1.4.7(3):

$$L(E_D/\mathbf{Q}, s) = \prod_{\pi} (1 - \pi|\pi|^{-2s})^{-1} = \sum_{\alpha \equiv 1 \pmod{2+2i}} \frac{\alpha}{|\alpha|^{2s}}.$$

A similar explicit formula holds for all curves $E_D : v^2 = u^3 - Du$ (cf. 1.2.3(2b)). In fact, it was these curves that served as guinea pigs for testing the conjecture (see [B-SD]). For curves $E_{D^2}$, which are related to the general congruent number problem, an explicit formula for $L(E_{D^2}/\mathbf{Q}, 1)$ is given in [Tu].

(2) If $E$ has complex multiplication and $L(E/\mathbf{Q}, 1) \neq 0$, then $E(\mathbf{Q})$ is finite (Coates-Wiles [Co-Wi]).

(3) In general, any elliptic curve over $\mathbf{Q}$ is modular, thanks to the pioneering work of Wiles, Taylor-Wiles (and their followers [BCDT]); this again implies the analytic continuation and functional equation for $L(E/\mathbf{Q}, s)$.

(4) If $r_{an}(E/\mathbf{Q}) \leq 1$, then the conjecture (BSD) holds and the group Ш$(E/\mathbf{Q})$ is finite; in fact, the strong version of the conjecture (BSD) holds, up to a controlled rational factor (Kolyvagin [Ko], combined with results of Gross-Zagier [Gr-Za] and others).

(5) If $E$ does not have additive reduction at $p$, then one can define a $p$-adic $L$-function $L_p(E, s)$. Kato [Ka] (see also [Col]) showed that

$$r(E/\mathbf{Q}) \leq \mathrm{ord}_{s=1} L_p(E, s).$$

(6) If $E$ has good ordinary reduction at a prime $p$ and if the $p$-primary component of Ш$(E/\mathbf{Q})$ is finite, then (see [Ne])

$$r(E/\mathbf{Q}) \equiv r_{an}(E/\mathbf{Q}) \pmod 2.$$

**(THIS IS VERSION 5/2/2004)**

## References


[Al-Kl] A.Altman, S.Kleiman, *Introduction to Grothendieck duality theory*, Lecture Notes in Mathematics **146**, Springer, 1970.

[Be] D. Bernardi, private communication.

[B-SD] B.J. Birch, H.P.F. Swinnerton-Dyer , *Notes on Elliptic Curves. II*, J. reine und angew. Math. **218** (1965), 79–108.

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

[Ca 1] J.W.S. Cassels, *Lectures on Elliptic Curves*, London Math. Society Student Texts **24**, Cambridge Univ. Press, 1991.

[Ca 2] J.W.S. Cassels, *Arithmetic on curves of genus* 1*. I. On a conjecture of Selmer*, J. Reine Angew. Math. **202** (1959), 52–99.

[Ca 3] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[Cl] C.H. Clemens, *A Scrapbook of Complex Curve Theory*, Plenum Press, 1980.

[Co-Wi] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.

[Col] P. Colmez, *La Conjecture de Birch et Swinnerton-Dyer p-adique*, Séminaire Bourbaki, Exp. 919, juin 2003.

[Ei] D. Eisenbud, *Commutative Algebra (with a view toward algebraic geometry)*, Graduate Texts in Mathematics **150**, Springer, 1995.

[Fa-Kr 1] H.M. Farkas, I. Kra, *Riemann surfaces*, Graduate Texts in Mathematics **71**, Springer, 1992.

[Fa-Kr 2] H.M. Farkas, I. Kra, *Theta constants, Riemann surfaces and the modular group*, Graduate Studies in Mathematics **37**, American Math. Society, 2001.

[Fo] O. Forster, *Lectures on Riemann surfaces*, Graduate Texts in Mathematics **81**, Springer, 1991.

[Gr-Ha] P. Griffiths, J. Harris, *Principles of algebraic geometry*, Wiley-Interscience, 1978.

[Gr-Za] B.H. Gross, D. Zagier *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

[Hu] D. Husemöller, *Elliptic Curves*, Graduate Texts in Mathematics **111**, Springer, 1987.

[Ir-Ro] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics **84**, Springer, 1982

[Ka] K. Kato, *P-adic Hodge theory and values of zeta functions of modular forms*, preprint, 2000.

[Ki] F. Kirwan, *Complex algebraic curves*, London Math. Society Student Texts **23**, Cambridge Univ. Press, 1992.

[Ko] V.A. Kolyvagin, *Euler systems*, in: The Grothendieck Festschrift, Vol. II, Progress in Math. **87** , Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[La] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics **112**, Springer, 1987.

[Mar] A.I. Markushevich, *Introduction to the classical theory of abelian functions*, Translations of Mathematical Monographs **96**, American Math. Society, 1992.

[Mat] H. Matsumura, *Commutative ring theory*, Cambridge Univ. Press, 1986.

[McK-Mo] H. McKean, V. Moll, *Elliptic curves*, Cambridge Univ. Press, 1997.

[Mi] J. Milne, *Elliptic curves*, lecture notes, `http://www.jmilne.org/math/`.

[Mu AV] D. Mumford, *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5; Oxford Univ. Press, 1970.

[Mu TH] D. Mumford, *Tata lectures on theta. I,II,III*, Progress in Mathematics **28**, **43**, **97**, Birkhäuser, 1983, 1984, 1991.

[MK] V.K. Murty, *Introduction to abelian varieties*, CRM Monograph Series **3**, American Math. Society, 1993.

[Ne] J. Nekovář, *On the parity of ranks of Selmer groups II*, C.R.A.S. Paris Sér. I Math. **332** (2001), no. 2, 99–104.

[Re] M. Reid, *Undergraduate Algebraic Geometry*, London Math. Society Student Texts **12**, Cambridge Univ. Press, 1988.

[Ru 1] W. Rudin, *Principles of mathematical analysis*, McGraw-Hill, 1976.

[Ru 2] W. Rudin, *Real and complex analysis*, McGraw-Hill, 1987.

[Sc] N. Schappacher, *Some milestones of lemniscatomy*, in: Algebraic geometry (Ankara, 1995), Lect. Notes in Pure and Appl. Math. **193**, Dekker, New York, 1997, pp. 257–290.

[Se] E.S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362.

[Si 1] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, 1986.

[Si 2] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994.

[Si-Ta] J.H. Silverman, J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer, 1992.

[Tu] J.B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), 323–334.

[Web] H. Weber, *Lehrbuch der Algebra. III*, 1908.

[Wei 1] A. Weil, *Introduction à l'étude des variétés kähleriennes*, Hermann, 1958.

[Wei 2] A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Ergebnisse der Mathematik und ihrer Grenzgebiete **88**, Springer, 1976.