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
$\arcsin, \arccos$ $\int R(x, \sqrt{f(x)})\, dx, \quad \deg(f) = 2$	elliptic integrals $\int R(x, \sqrt{f(x)})\, dx, \quad \deg(f) = 3, 4$
$\sin, \cos$ (periodic with period 2π)	elliptic functions (doubly periodic with periods ω_1, ω_2)

(0.0.2) Geometry:

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

(0.0.3) Arithmetic:

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

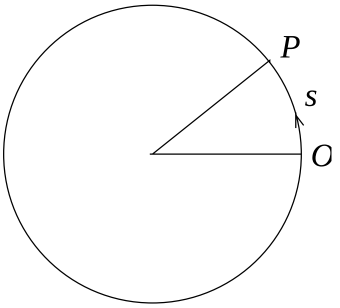
0.1. The circle

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

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

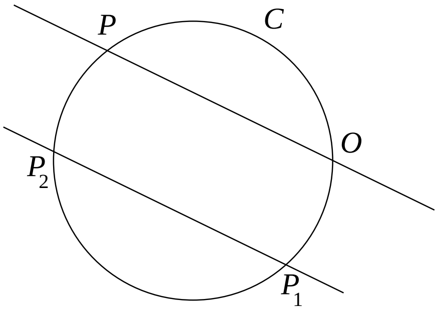
where

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

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

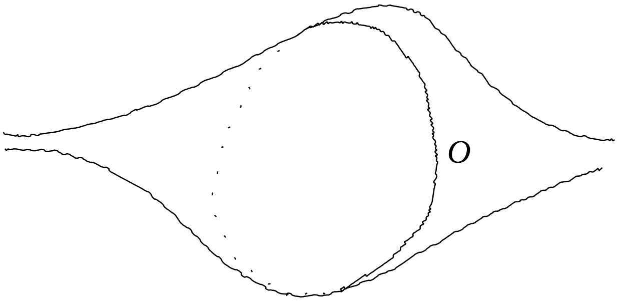
Attentive readers will have noticed that the discussion in Sect. 0.1 was not completely correct. The problem lies in the square root $\sqrt{1-y^2}$, whis is not a single-valued function. How does one keep track of the correct square root?

(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

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

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

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



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.

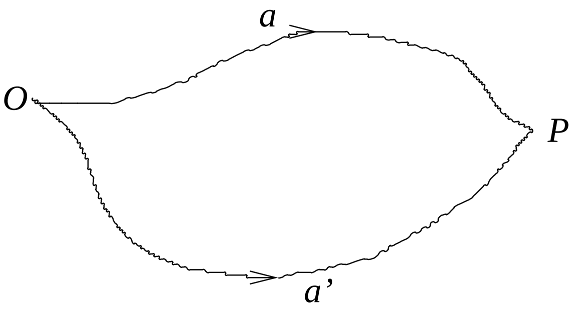
(0.2.1) The Abel-Jacobi map. In our new formulation, the integral (0.1.0.0) should be replaced by

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

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 ω along γ', 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'

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

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

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

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

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

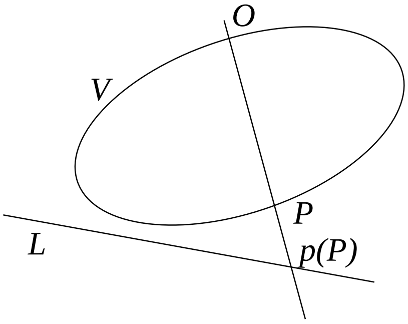
which is obtained from C by adding two points at infinity

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

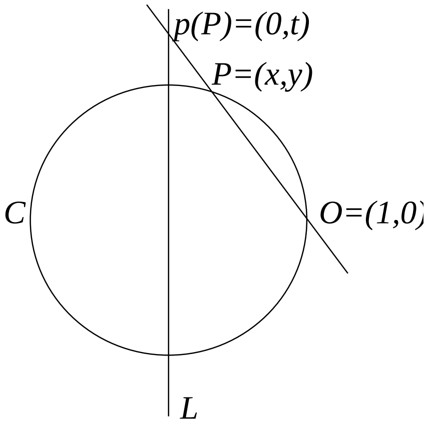
(0.3.1) Circle = line. This is one of the small miracles that occur in the projective world. In fact, much more is true (if you are not sure about the precise definitions, see I.3.7 below):

(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 σ 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

$$a + ib = (u + iv)^2 \qquad (0.4.2.1.0)$$

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

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

(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

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

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 π 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 λ^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: $\mathbf{F}_{p^n}^* = \{a \in \overline{\mathbf{F}}_p^* \mid a^{p^n-1}=1\}$.]*
(iv) *Show that*

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

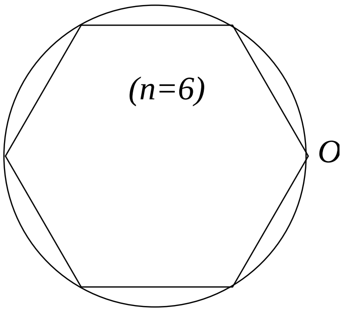
(0.5.4) Exercise (Structure of $C(\mathbf{Q})$). (i) *The torsion subgroup of $C(\mathbf{Q})$ is equal to*

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

(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

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

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 μ_n is, in fact, generated by any primitive n-th root of unity (i.e. a generator of the cyclic group μ_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 Φ_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 μ_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 μ_n and commutes with its group law (= multiplication). It follows that its action on μ_n is given by

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

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 χ_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 μ_n (i.e. the set $\mu_n(F) = \{x \in F \mid x^n = 1\}$ 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 δ 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. $n > 4$).

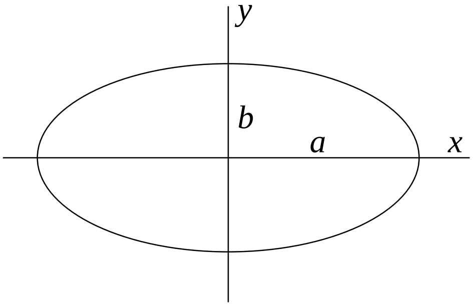
If $n = 1, 2$, the integral is an elementary function; for example, if $f(x) = 1 - x^2$, then the substitution $x = (t^2-1)/(t^2+1)$ from 0.3.1.2 transforms I into an integral of a rational function of t.

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

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



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

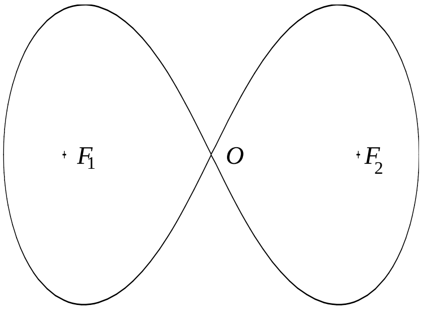
$$s = \int \sqrt{\frac{1-k^2x^2}{1-x^2}} dx = \int \frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}} dx.$$

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

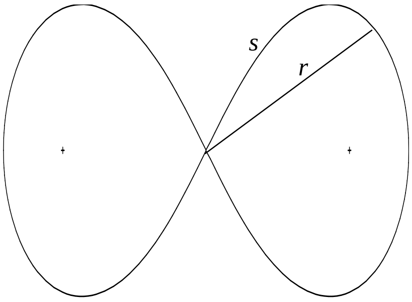
(1.3.1) The sine function is defined as the inverse of the integral (0.1.0.0) that computes the arclength of the unit circle. In a similar vein, the 'sine of the lemniscate' *sl* is defined as the inverse function to the integral (1.2.2.1). In other words, if

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

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

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

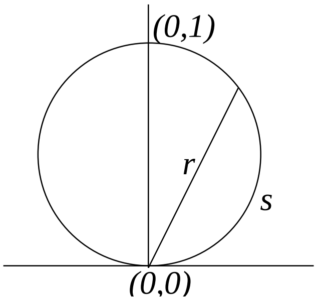
the length of the 'quarter-arc' of the lemniscate between $(0, 0)$ and $(1, 0)$, then

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

(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

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

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

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

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

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

which is equivalent to the addition formula

$$\int_0^{w_1} \frac{dt}{\sqrt{1-t^4}} + \int_0^{w_2} \frac{dt}{\sqrt{1-t^4}} = \int_0^{w_3} \frac{dt}{\sqrt{1-t^4}} \pmod{2\Omega\mathbf{Z} + 2i\Omega\mathbf{Z}}$$

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

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

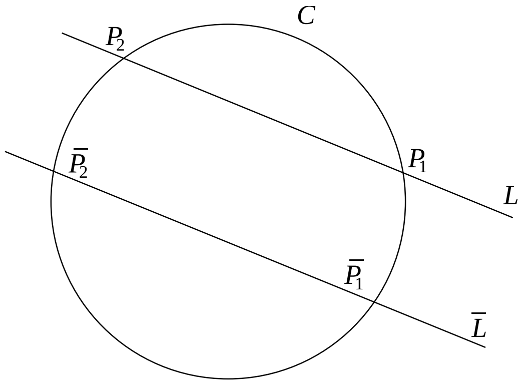
For $(m,n) = (-1,0)$ (resp. $= (0,-1)$) this reduces to the addition formula for sin (resp. for sl).

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 ω 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 $y_j = ax_j + b$,

$$F(x) = (a^2+1)(x-x_1)(x-x_2), \qquad x_1 + x_2 = -\frac{2ab}{a^2+1}, \qquad x_1x_2 = \frac{b^2-1}{a^2+1}.$$

(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

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

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 Σ). Viewing $\omega = dy/x = -dx/y$ as a holomorphic differential on S, then

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

is the "trace" of ω 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 Σ 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

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

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*

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

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 $p,q\in\mathbf{C}[a_1,\ldots,a_r]$ 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) $\quad d_P\neq d_Q+m,\quad 0\leq k\leq m-1.$
(2.2.7.2) $\quad d_P=d_Q+m,\quad 0\leq k\leq m-2.$
(2.2.7.3) $\quad d_P=d_Q+m,\quad 0\leq k\leq m-1,\qquad (\forall a\in B)\,(\forall l=1,\ldots r)\qquad W_l(a)=0.$

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

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

provided

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

(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 α_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

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

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

$$\begin{aligned}&x_1y_2 - x_2y_1 = (x_1 - x_2) + b(x_1x_2^2 - x_1^2x_2) = (x_1 - x_2)(1 - bx_1x_2)\\ &x_1^2y_2^2 - x_2^2y_1^2 = (x_1^2 - x_2^2)(1 - nx_1^2x_2^2)\end{aligned}$$

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

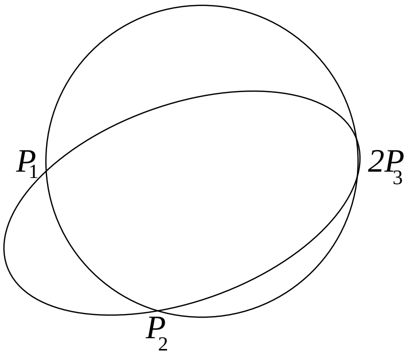
(2.4.1) Abel was interested in addition formulas for general integrals of the form

$$\int_O^P \omega,$$

where ω 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_λ, 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 ω).

(2.4.2) Abel's Theorem states that, for suitable differentials ω and certain families of auxiliary curves C_λ, the "Abel sum" (2.4.1.1) (modulo periods) does not depend on λ. This can be reformulated intrinsically as follows: geometric properties of V and of the family C_λ 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_λ?

(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 ω, 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 μ_1, μ_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_α, ϕ_α), where $\{U_\alpha\}$ is an open covering of X and $\phi_\alpha : U_\alpha \overset{\sim}{\longrightarrow} \phi_\alpha(U_\alpha)$ is a homeomorphism between U_α and an open subset of $\mathbf{C}$. The local charts are required to be compatible in the following sense: for each pair (U_α, ϕ_α), (U_β, ϕ_β) 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_α, z_α) 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_α 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 $\phi_j : U_j \overset{\sim}{\longrightarrow} \mathbf{C}$ 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_α, ϕ_α), $x \in U_\alpha$ on X and (V_β, ψ_β), $f(x) \in V_\beta$ 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_α, z_α) 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_α.

(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) 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_α (resp. z_β) 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*

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

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 α, 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_α 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** *ω 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_α, ϕ_α) be an atlas of X and assume that ω 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_β, ψ_β) of Y such that, for each β, $f(V_\beta) \subset U_\alpha$ for some $\alpha = j(\beta)$. In terms of the standard coordinates z_β on V_β (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_α, z_α) 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 ω 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_α 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_β 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_α 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 ω_1, ω_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 $\omega_1 = f\omega_2$.

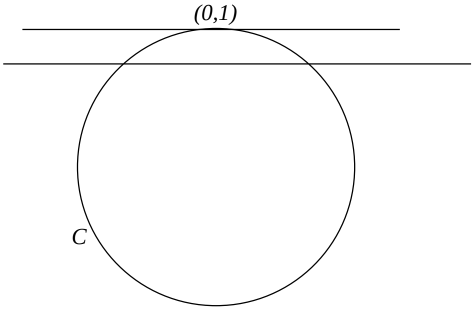
(3.3.15) Theorem [Fa-Kr 1, Ch. 2]. *Let X be a Riemann surface. Then $\mathcal{M}(X) \neq \mathbf{C}$ and $\Omega^1_{\rm mer}(X) \neq \{0\}$.*

(3.3.16) Corollary. *For every Riemann surface X, the vector space $\Omega^1_{\rm mer}(X)$ 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*

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

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

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

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 ω 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_α, z_β (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

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

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_α, z_α) 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

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

(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

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

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 $X \cap U_{P,x} = \{(f_P(z), z + y_P) \mid z \in W_P\}$ (resp. $X \cap U_{P,y} = \{(z + x_P, f_P(z)) \mid z \in W_P\}$), where $f_P(z)$ is a holomorphic function in W_P.

We want to show that the collection $\{(U_{P,x}, y - y_P) \mid P \in X_x\} \cup \{(U_{P,y}, x - x_P) \mid P \in X_y\}$ 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

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

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))

$$a = a' \Longrightarrow \int_O^D \omega \equiv \int_O^{D'} \omega \ (\mathrm{mod}\, 2\pi\mathbf{Z})$$

(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*

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

(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. ∞) and $\lambda^*(dz/z) = i\,dy/x = i\omega$.

(3.8.5) Proof of Conjecture 3.8.2. Applying λ, 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 ∞ 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 $\mathrm{supp}(D) := \{P \in X \mid n_P \neq 0\}$ *the* **support of** D, *we require that, for each compact subset* $K \subset X$, *the intersection* $K \cap \mathrm{supp}(D)$ *be finite (in particular, if* X *itself is compact, then "locally finite" = "finite"). The set* $\mathrm{Div}(X)$ *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*

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

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

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

(3.9.4) The map $\mathrm{div} : \mathcal{M}(X)^* \longrightarrow \mathrm{Div}(X)$ 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* $Cl(X) = \mathrm{Div}(X)/P(X)$. *If* X *is compact, then the subgroup of divisor classes of degree zero is denoted by* $Cl^0(X) = \mathrm{Div}^0(X)/P(X)$.

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

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

(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 $f^* : \mathrm{Div}(Y) \longrightarrow \mathrm{Div}(X)$ *satisfying*

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

(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* $S = \mathrm{supp}(\mathfrak{m})$. *Define*

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

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*

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

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 λ 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.

$$E : Y^2 Z = (X - e_1 Z)(X - e_2 Z)(X - e_3 Z)$$

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

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. *ω 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 ω_1 is holomorphic, we obtain from 4.2.2

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

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 ω, 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 $\deg(f) = 2m \ge 4$ 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 $x_1, \ldots, x_{2m} \in \mathbf{C}$ 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 $\widetilde{V}(\mathbf{C}) \cap \{Z = 0\} = \{P_1, \ldots, P_d\}$. 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

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

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 ω on $E(\mathbf{C})$ is then equal to

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

(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 γ_1, γ_2 based at O, disjoint outside O, with tangent vectors to γ_2, γ_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 γ_1, γ_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 ∂D corresponding to the same point of γ_1 (resp. γ_2) differ by ω_2 (resp. by ω_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 φ on any compact Riemann surface X of genus 1. However, it follows from the Riemann-Roch Theorem that every such pair (X, φ) 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

$$\alpha : E(\mathbf{C}) \longrightarrow \mathbf{C}/L, \qquad \alpha(P) = \int_O^P \omega \pmod{L}.$$

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 α 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 α 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 α is a bijection, as required.

(4.4.3) The inverse of α. The Abel-Jacobi map α 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 ω_1 and ω_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 ω 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 ω_1, ω_2, i.e. those for which $\mathrm{Im}(\omega_1/\omega_2) > 0$. In that case the new basis ω_1', ω_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

$$F(z+u) = F(z) \qquad\qquad (z \in \mathbf{C},\ u \in L).$$

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 ∂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 ∂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 τ 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*

$$F(z+u) = e^{a(u)z+b(u)}F(z) \qquad\qquad (z \in \mathbf{C},\ u \in L) \tag{6.1.1.1}$$

(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 $t = \exp(2\pi i z)$, 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*

$$\begin{tikzcd} p^{-1}(U_\alpha) \arrow[r, "\sim"] \arrow[d, "p"] & U_\alpha \times \mathbf{C} \arrow[d, "pr"] \\ U_\alpha \arrow[r, equal] & U_\alpha \end{tikzcd}$$

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 $f : \mathscr{L} \overset{\sim}{\longrightarrow} \mathscr{L}'$ 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

$$\mathcal{O}(X) \overset{\sim}{\longrightarrow} \Gamma(X, X \times \mathbf{C}), \qquad\qquad f \mapsto s(x) = (x, f(x)).$$

(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

$$f^*\mathscr{L} = \{(y, \ell) \in Y \times \mathscr{L} \mid f(y) = p(\ell)\}$$

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

$$\mathscr{L} = \{(v, V) \in \mathbf{C}^{N+1} \times \mathbf{P}^N(\mathbf{C}) \mid v \in V\}$$

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:

$$\begin{tikzcd} Y \times \mathbf{C} \arrow[r, "\widehat{g}"] \arrow[d, "pr"] & Y \times \mathbf{C} \arrow[d, "pr"] \\ Y \arrow[r, "g"] & Y, \end{tikzcd} \tag{6.2.5.1}$$

acts on each fiber $\{y\} \times \mathbf{C}$ by a linear automorphism and such that

$$\widehat{g_1 g_2} = \widehat{g_1}\widehat{g_2} \qquad\qquad (g_1, g_2 \in G). \tag{6.2.5.2}$$

In concrete terms, the linearity on the fibers amounts to

$$\widehat{g}(y, t) = (gy, \alpha_g(y)\, t), \qquad\qquad (y \in Y,\ t \in \mathbf{C}) \tag{6.2.5.3}$$

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

$$\begin{tikzcd}
Y \times \mathbf{C} \arrow[r, "\widehat{\pi}"] \arrow[d, "pr"] & G\backslash(Y \times \mathbf{C}) \arrow[d, "p"] \\
Y \arrow[r, "\pi"] & G\backslash Y
\end{tikzcd}$$

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

$$F(gy) = \alpha_g(y)\, F(y) \qquad\qquad (\forall y \in Y,\ \forall g \in G). \tag{6.2.9.2}$$

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

$$\Gamma(X, \mathscr{L}) \xrightarrow{\sim} \{F \in \mathcal{O}(Y) \mid F \text{ satisfies } (6.2.9.2)\}.$$

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

$$F : \mathbf{C}^{N+1} - \{0\} \longrightarrow \mathbf{C}, \qquad F(gy) = g^d\, F(y) \qquad\qquad (\forall g \in \mathbf{C}^*). \tag{6.2.12.1}$$

(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")

$$r : Y \times \mathbf{C} \xrightarrow{\sim} Y \times \mathbf{C}, \qquad\qquad (y, t) \mapsto (y, \beta(y)\, t),$$

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

$$\begin{tikzcd}
Y \times \mathbf{C} \arrow[r, "\widehat{g}"] \arrow[d, "\wr r"] & Y \times \mathbf{C} \arrow[d, "\wr r"] \\
Y \times \mathbf{C} \arrow[r, "\widehat{g}^{\text{new}}"] & Y \times \mathbf{C}.
\end{tikzcd}$$

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

$$\alpha_g^{\text{new}}(y) = \frac{\beta(gy)}{\beta(y)}\, \alpha_g(y) \qquad\qquad (y \in Y,\ g \in G). \tag{6.2.14.1}$$

In other words, α_g^{new} and α_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

$$\alpha_u^{\rm new}(z)=\frac{\beta(z+u)}{\beta(z)}\,\alpha_u(z),\tag{6.3.1.3}$$

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*

$$\alpha_u^{\rm new}(z)=e^{a(u)z+b(u)}\qquad\qquad(a(u),b(u)\in\mathbf{C}).$$

(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 Δ, 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

$$\theta(z;\tau) = c(\tau)A(z + \frac{\tau+1}{2}) \qquad (6.3.11.1)$$

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 $D = \{z = \alpha + t_1\tau + t_2 1 \mid 0 \leq t_1, t_2 \leq 1\}$ 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

$$\alpha_1(z) = 1, \qquad \alpha_\tau(z) = e^{-2\pi i m(z+\frac{\tau}{2}+c)} \qquad (m \in \mathbf{Z},\ c \in \mathbf{C}), \qquad (6.3.14.1)$$

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

$$\{\text{isomorphism classes of line bundles on } X\} \longrightarrow Cl(X), \qquad (6.3.15.1)$$

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 $a,b\in\{0,1\}$,*

$$\dim_{\mathbf{C}}\Gamma(\mathbf{C}/\mathbf{Z}\tau+\mathbf{Z},\,\mathscr{L}^{\otimes m}\otimes\chi_{a,b})=\begin{cases}m, & \textit{if } m>0\\ 0, & \textit{if } m<0.\end{cases}$$

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 $a_0,\ldots,a_{m-1}$ 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 $(a_0,\ldots,a_{m-1})$ 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

$$\theta_{ab}^{(n)}(z)=\left(\frac{\partial}{\partial z}\right)^n\theta_{ab}(z),\qquad\theta_{ab}=\theta_{ab}(0;\tau),\qquad\theta_{ab}^{(n)}=\left(\frac{\partial}{\partial z}\right)^n\theta_{ab}(z;\tau)\bigg|_{z=0}.$$

(6.4.7) Exercise. *Show that*

$$\theta_{ab}(-z)=\theta_{ab}(z)\cdot\begin{cases}1, & \textit{if } ab=00,01,10\\ -1, & \textit{if } ab=11.\end{cases}$$

(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 λ 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

$$\frac{1}{2\pi i}\, D_\tau : \left\{ \begin{matrix} q^m \mapsto mq^m \\ t^m \mapsto 0 \end{matrix} \right\}, \qquad \frac{1}{2\pi i}\, D_z : \left\{ \begin{matrix} q^m \mapsto 0 \\ t^m \mapsto mt^m \end{matrix} \right\},$$

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

$$\begin{aligned}\theta_{01}(z;\tau) &= c(\tau)\prod_{n=1}^{\infty}(1-q^{n-1/2}t)(1-q^{n-1/2}t^{-1})\\ \theta_{10}(z;\tau) &= (t^{1/2}+t^{-1/2})\,q^{1/8}c(\tau)\prod_{n=1}^{\infty}(1+q^nt)(1+q^nt^{-1})\\ \theta_{11}(z;\tau) &= i(t^{1/2}-t^{-1/2})\,q^{1/8}c(\tau)\prod_{n=1}^{\infty}(1-q^nt)(1-q^nt^{-1}).\end{aligned}\tag{6.4.12.1}$$

Letting $z\mapsto 0$ (when $t\sim 1+2\pi iz$), 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 σ, ζ 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 σ-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 ζ- 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

$$\wp(z;L) = -\zeta'(z;L) = \frac{1}{z^2} + \sum_{u\in L}{}' \left(\frac{1}{(z-u)^2} - \frac{1}{u^2}\right) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)\, G_{2k+2} z^{2k} \qquad (7.1.4.3)$$

and its derivative

$$\wp'(z;L) = -2\sum_{u\in L}\left(\frac{1}{(z-u)^3}\right) = -\frac{2}{z^3} + \sum_{k=1}^{\infty}(2k+1)2k\, G_{2k+2} z^{2k-1}. \qquad (7.1.4.4)$$

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) $\mathrm{div}(\wp(z) - \wp(\omega_j/2)) = 2(\omega_j/2) - 2(0)$.
(ii) $\mathrm{div}(\wp'(z)) = (\omega_1/2) + (\omega_2/2) + (\omega_3/2) - 3(0)$.
(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 ≥ 1 (resp. ≥ 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 $\mathrm{div}(\wp(z) - a_j)$ 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

$$\mathrm{disc}(X^3 + aX + b) = \prod_{i<j}(e_i - e_j)^2 = -4a^3 - 27b^2 \neq 0$$

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

$$E - \{O\} : y^2 = 4x^3 - g_2 x - g_3$$

(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 φ 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 φ 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 φ is holomorphic everywhere. The composition of φ 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 φ 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 γ in $\mathbf{C}/L$. Letting γ 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 γ 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. φ induces an isomorphism between the field of rational functions $\mathbf{C}(x, y) = \mathrm{Frac}(\mathbf{C}[x, y]/(y^2 - (4x^3 - g_2 x - g_3)))$ 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*

$$\begin{aligned}
e_3 - e_1 &= \wp((\tau+1)/2) - \wp(\tau/2) = \left(\frac{\theta_{10}\theta'_{11}}{\theta_{00}\theta_{01}}\right)^2 && (= \pi^2\theta_{10}^4)\\
e_1 - e_2 &= \quad \wp(\tau/2) - \wp(1/2) \quad = \left(\frac{\theta_{00}\theta'_{11}}{\theta_{01}\theta_{10}}\right)^2 && (= -\pi^2\theta_{00}^4)\\
e_2 - e_3 &= \wp(1/2) - \wp((\tau+1)/2) = \left(\frac{\theta_{01}\theta'_{11}}{\theta_{10}\theta_{00}}\right)^2 && (= \pi^2\theta_{01}^4)
\end{aligned}$$

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 π^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 Δ 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 γ 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 γ, 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

$$2\pi i = 2\pi i \operatorname{res}_0(\zeta(z)\,dz) = \int_{\partial D} \zeta(z)\,dz = \int_\alpha^{\alpha+\omega_2} \underbrace{(\zeta(z) - \zeta(z+\omega_1))}_{-\eta_1} dz +$$
$$+ \int_\alpha^{\alpha+\omega_1} \underbrace{(\zeta(z+\omega_2) - \zeta(z))}_{\eta_2} dz = \omega_1\eta_2 - \omega_2\eta_1.$$

(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 σ-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 σ-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

$$\begin{aligned} \varphi : \mathbf{C}/L &\longrightarrow E(\mathbf{C}) \\ z &\mapsto (\wp(z), \wp'(z)) \\ 0 &\mapsto O \end{aligned} \qquad \begin{aligned} \alpha : E(\mathbf{C}) &\longrightarrow \mathbf{C}/L \\ P &\mapsto \int_O^P \frac{dx}{y} \pmod{L} \end{aligned} \qquad \begin{aligned} \varphi^*(dx/y) &= dz \\ \alpha^*(dz) &= dx/y \end{aligned}$$

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 φ, α from 7.5.1 to 5.3.6 yields an isomorphism of abelian groups

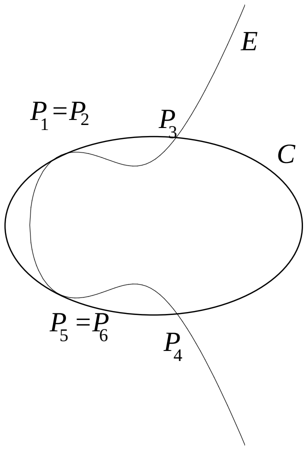
$$\begin{gathered}
\boxplus : Cl^0(E(\mathbf{C})) \xrightarrow{\sim} E(\mathbf{C}) \\
\sum n_j (P_j) \mapsto \boxplus [n_j] P_j,
\end{gathered}$$

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

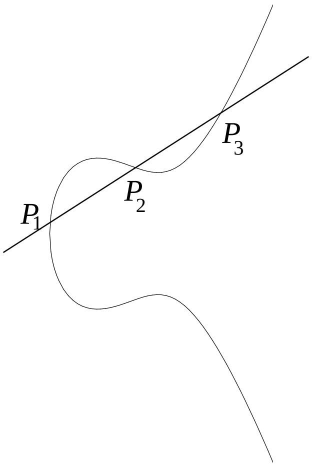
$$P_1 \boxplus \cdots \boxplus P_{3d} = [3d]O = O \tag{7.5.4.1}$$

on $E(\mathbf{C})$. Equivalently,

$$\sum_{j=1}^{3d} \int_O^{P_j} \frac{dx}{y} \equiv 0 \ (\mathrm{mod}\, L),$$

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 $\mathrm{div}(f) = (P_1) + (P_2) + (P_3) - 3(O)$, hence

$$P_1 \boxplus P_2 \boxplus P_3 = [3]O = O \tag{7.5.5.1}$$

and

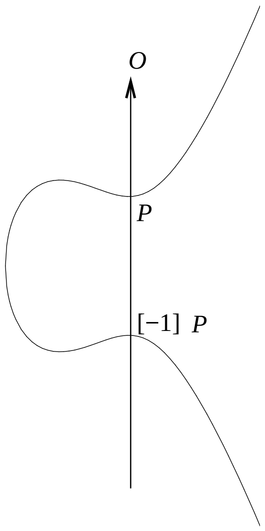
$$\int_O^{P_1} \frac{dx}{y} + \int_O^{P_2} \frac{dx}{y} + \int_O^{P_3} \frac{dx}{y} \equiv 0 \ (\mathrm{mod}\, L),$$

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

$$P * Q := R. \tag{7.5.6.1}$$

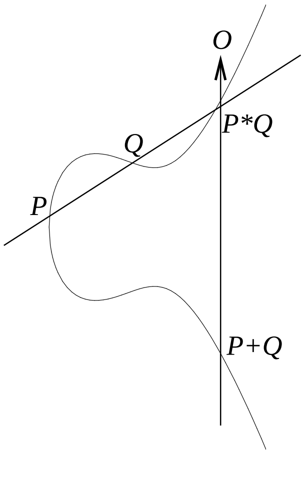
The discussion in 7.5.5 implies that

$$P * Q = [-1](P \boxplus Q), \qquad O * R = [-1]R,$$

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

$$x_3 = \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2. \qquad (7.5.7.1)$$

The y-coordinate of P_3 is equal to

$$y_3 = ax_3 + b, \qquad b = y_1 - ax_1 = y_1 - x_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right). \qquad (7.5.7.2)$$

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

$$x_3 = \frac{(6x_1^2 - g_2/2)^2}{4y_1^2} - 2x_1 = \frac{(3x_1^2 - g_2/4)^2 - 2x_1(4x_1^3 - g_2 x_1 - g_3)}{y_1^2} = \frac{x_1^4 + \frac{g_2}{2}x_1^2 + 2g_3 x_1 + \frac{g_2^2}{16}}{4x_1^3 - g_2 x_1 - g_3}. \qquad (7.5.7.3)$$

(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

$$\wp(z_1 + z_2) = \frac{1}{4}\left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)}\right)^2 - \wp(z_1) - \wp(z_2) \qquad (7.5.8.1)$$

in the case $z_1 \neq z_2 \in \mathbf{C}/L$ and

$$\wp(2z) = \frac{\wp(z)^4 + \frac{g_2}{2}\wp(z)^2 + 2g_3\wp(z) + \frac{g_2^2}{16}}{4\wp(z)^3 - g_2\wp(z) - g_3}. \qquad (7.5.8.2)$$

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

$$E(\mathbf{C})_n = \{P \in E(\mathbf{C}) \mid [n]P = O\}$$

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

$$E(\mathbf{C})_n = \{O\} \cup \{(\wp((a\omega_1 + b\omega_2)/n), \wp'((a\omega_1 + b\omega_2)/n)) \mid (a, b) \in (\mathbf{Z}/n\mathbf{Z})^2 - \{(0, 0)\}\}.$$

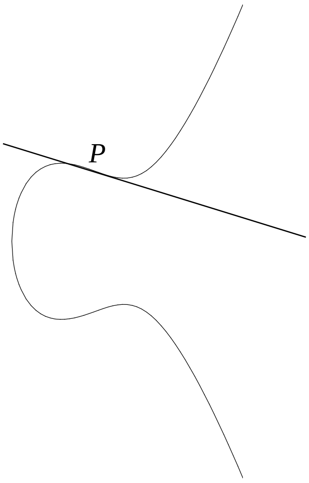
For $n = 2$, a point $P = (x, y) \in E(\mathbf{C}) - \{O\}$ satisfies

$$[2]P = O \iff P = [-1]P \iff (x, y) = (x, -y) \iff y = 0;$$

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*

$$\{f(z) = \lambda z \mid \lambda \in \mathbf{C}, \lambda L_1 \subseteq L_2\}.$$

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:

$$\begin{tikzcd}
\mathbf{C} \arrow[r, "F"] \arrow[d, "pr_1"] & \mathbf{C} \arrow[d, "pr_2"] \\
\mathbf{C}/L_1 \arrow[r, "f"] & \mathbf{C}/L_2.
\end{tikzcd}$$

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*

$$\mathcal{M}(\mathbf{C}/L_1)^{\mathrm{Ker}(f)} = f^*(\mathcal{M}(\mathbf{C}/L_2)) = \{f^*(h) = h \circ f \mid h \in \mathcal{M}(\mathbf{C}/L_2)\}.$$

(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*

$$\mathrm{End}(\mathbf{C}/L) = \{f : \mathbf{C}/L \longrightarrow \mathbf{C}/L \mid f \text{ holomorphic}, f(0) = 0\} = \{\lambda \in \mathbf{C} \mid \lambda L \subseteq L\} \subset \mathbf{C}.$$

Above, we have identified λ 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

$$\lambda = a\tau + b \in \mathbf{Z}a\tau + \mathbf{Z} \subseteq \mathbf{Z}A\tau + \mathbf{Z} \qquad\qquad (\text{as } A|a).$$

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*

$$\mathrm{Aut}(\mathbf{C}/L) = \begin{cases} \{\pm 1, \pm i\}, & \textit{if } L = \mathbf{Z}i\omega + \mathbf{Z}\omega \\ \{\pm 1, \pm\rho, \pm\rho^2\}, & \textit{if } L = \mathbf{Z}\rho\omega + \mathbf{Z}\omega \\ \{\pm 1\}, & \textit{otherwise.} \end{cases}$$

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'_{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_{aff} and V'_{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

$$L_V = \{\int_\gamma \omega_V \mid \gamma \in H_1(V(\mathbf{C}), \mathbf{Z})\} \subset \mathbf{C}$$

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 α_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), φ_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 φ_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

$$\begin{aligned} sl(0) = sl(\Omega) = 0, &\qquad sl(\frac{\Omega}{2}) = 1 = -sl(-\frac{\Omega}{2}), \\ sl'(0) = 1 = -sl'(\Omega), &\qquad sl'(\frac{\Omega}{2}) = sl'(-\frac{\Omega}{2}) = 0. \end{aligned}$$

(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 γ on $V(\mathbf{C})$. In particular, letting γ run through the representatives of $H_1(V(\mathbf{C}), \mathbf{Z})$ we obtain

$$iL_V = L_V.$$

Taking for γ a path from $(0,1)$ to Q yields

$$\alpha_V([\pm i]Q) = \pm i\,\alpha_V(Q) \iff (sl(\pm iz), sl'(\pm iz)) = (\pm isl(z), sl'(z)) \tag{8.2.3.1}$$

If $0 \leq x \leq 1$, let $y = \sqrt{1-x^4}$. Then

$$\begin{gathered}\alpha_V((x,y)) = \int_0^x \frac{dt}{\sqrt{1-t^4}}\\ \alpha_V((-x,-y)) = \alpha_V((0,-1)) + \int_0^x \frac{dt}{\sqrt{1-t^4}} = \Omega + \alpha_V((x,y)),\end{gathered}$$

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

$$\begin{gathered}sl(z+i\Omega) = i\,sl(z/i+\Omega) = -i\,sl(z/i) = -sl(z)\\ sl(z+(1+i)\Omega) = -sl(z+i\Omega) = sl(z),\end{gathered}$$

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 φ_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 $\mathbf{C}$)

$$\begin{gathered}E_{\mathrm{aff}} : v^2 = 4u^3 - 4u = 4(u+1)u(u-1)\\ E = E_{\mathrm{aff}} \cup \{O\}, \qquad O = (0:1:0)\end{gathered}$$

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

$$L = \{\int_\gamma \omega_E \mid \gamma \in H_1(E(\mathbf{C}), \mathbf{Z})\}$$

is the period lattice of ω_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 α, α_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:

$$\begin{tikzcd} \mathbf{C} \arrow[r, "pr"] \arrow[d, equal] & \mathbf{C}/L_V \arrow[r, "\varphi_V"] \arrow[d] & V(\mathbf{C}) \arrow[d, "f"] \\ \mathbf{C} \arrow[r, "pr"] & \mathbf{C}/L \arrow[r, "\varphi"] & E(\mathbf{C}). \end{tikzcd}$$

In particular,

$$\wp(z;L) = \frac{1}{sl(z)^2}$$

and f is a homomorphism of abelian groups.

Proof. For each closed path γ 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

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + \sum_{k=1}^{\infty}(4k-1)\,G_{4k}(L)z^{4k-2}\\ \wp'(z)^2 &= \frac{6}{z^4} + \sum_{k=1}^{\infty}(4k-1)(4k-2)(4k-3)\,G_{4k}(L)z^{4k-4}\end{aligned}$$

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 φ (resp. φ_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 α-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, $(x_j,y_j)=(sl(z_j),sl'(z_j))\in V_{\rm aff}(\mathbf{C})$.

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 $(x,y)\in V_{\rm aff}(\mathbf{C})$,*

$$(x,y)\boxplus O_\pm = \left(\pm\frac{i}{x}, \mp iyx^2\right).$$

[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 $(x,y)\in V_{\rm aff}(\mathbf{C})$ (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_α, y_α 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_α from x_α 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

$$y_{1+2i}\,\frac{dx}{y} = \frac{dx_{1+2i}}{1+2i} = \frac{1-(1-2i)x^4}{1-(1+2i)x^4}\,dx + \frac{(1+2i)x - x^5}{(1-(1+2i)x^4)^2}\,4x^3 dx = \frac{1+(2+8i)x^4+x^8}{(1-(1+2i)x^4)^2}\,dx,$$

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

$$\begin{gathered} 1+(2+8i)x^4+x^8 \equiv (1-x^4)^2 \equiv y^4 \pmod{(-1-2i)}, \\ 1-28x^4+6x^8-28x^{12}+x^{16} \equiv (1-x^4)^4 \equiv y^8 \pmod{(-3)}; \end{gathered}$$

the formulas (8.4.6.1-2) then imply that

$$\begin{gathered}[-1-2i]\,(x,y) \equiv (x^5,y^5)\ (\mathrm{mod}\,(-1-2i)),\\ [-3]\,(x,y) \equiv (x^9,y^9)\ (\mathrm{mod}\,(-3)).\end{gathered} \tag{8.4.7.1}$$

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_α, y_α 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 α; it makes sense, therefore, to consider the residue classes of x_α, y_α 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

$$\begin{gathered}[1+2i]\,(x,y) \equiv (-x^5,y^5)\ (\mathrm{mod}\,(1+2i)),\\ [3]\,(x,y) \equiv (-x^9,y^9)\ (\mathrm{mod}\,(3))?\end{gathered} \tag{8.4.7.1}$$

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 Ω/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 Ω/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

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right), \qquad\qquad p^* = (-1)^{\frac{p-1}{2}}p.$$

(9.1.7) Let $a \in \mathbf{Z} - \{0, 1\}$ be a square-free integer. Writing a in the form

$$a = (-1)^u 2^v p_1^* \cdots p_w^*, \qquad\qquad p_j^* = (-1)^{\frac{p_j-1}{2}}p_j,$$

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 $\mathbf{Z}/n\mathbf{Z} - \{0\} = \Sigma \overset{\bullet}{\cup} (-\Sigma)$ (disjoint union). Then*

$$\left(\prod_{\sigma\in\Sigma} 2\sin\frac{2\pi\sigma}{n}\right)^2 = n. \qquad (P)$$

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

$$\sin(nz) = Q_n(\sin(z)), \qquad Q_n(t) = (-1)^{\frac{n-1}{2}} 2^{n-1} t^n + \cdots + nt. \qquad (9.2.1.1)$$

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

$$Q_n(t) = t\prod_{\sigma\in\Sigma} 2^2\left(\sin\frac{2\pi\sigma}{n} - t\right)\left(\sin\frac{2\pi\sigma}{n} + t\right). \qquad (9.2.1.2)$$

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 α_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 Σ 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)

$$\left(\frac{p^*}{q} \right) \equiv \left(\frac{q}{p} \right) \pmod{p\mathcal{O}_{K_q}[1/2]} \Longrightarrow \left(\frac{p^*}{q} \right) \equiv \left(\frac{q}{p} \right) \pmod{p\mathbf{Z}} \tag{9.2.9.4}$$

(as both sides are equal to ± 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 $\left(\frac{1}{\alpha}L/L\right) - \{0\} = \Sigma_\alpha \overset{\bullet}{\cup} (i\Sigma_\alpha) \overset{\bullet}{\cup} (-\Sigma_\alpha) \overset{\bullet}{\cup} (-i\Sigma_\alpha)$ (thus $|\Sigma_\alpha| = (N\alpha - 1)/4$) and put*

$$\begin{aligned} P_\alpha(t) &= \prod_{u \in \frac{1}{\alpha}L/L} (t - sl(u)) = t \prod_{u \in \Sigma_\alpha} (t^4 - sl^4(u)) \in \mathbf{C}[t] \\ Q_\alpha(t) &= \prod_{u \in \left(\frac{1}{\alpha}L/L\right) - \{0\}} (1 - t\, sl(u)) = \prod_{u \in \Sigma_\alpha} (1 - t^4 sl^4(u)) \in \mathbf{C}[t] \end{aligned}$$

(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 $L = L_V \overset{\bullet}{\cup} (L_V + \Omega)$).

(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 $z \in L = L_V \overset{\bullet}{\cup} (L_V + \Omega)$ (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 $sl'(0)=1\neq0$), 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 α. 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

$$\alpha\cdot d_\alpha\equiv1\pmod{(2+2i)}.$$

This should be compared to the isomorphism

$$\{\pm1\}=\mathbf{Z}^*\xrightarrow{\sim}(\mathbf{Z}/4\mathbf{Z})^*$$

and the congruence

$$n^*:=n\cdot(-1)^{\frac{n-1}{2}}\equiv1\pmod 4$$

(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

$$\prod_{\epsilon=\pm1}\frac{P_{\alpha+\epsilon(1\pm i)}(t)}{c_{\alpha+\epsilon(1\pm i)}Q_{\alpha+\epsilon(1\pm i)}(t)}=\frac{(t^4-1)P_\alpha^2(t)\pm2ic_\alpha^2t^2Q_\alpha^2(t)}{\mp2it^2P_\alpha^2(t)+(t^4-1)c_\alpha^2Q_\alpha^2(t)}.$$

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:

$$\begin{aligned} P_{\alpha+(1\pm i)}(t)P_{\alpha-(1\pm i)}(t) &= (t^4-1)P_\alpha^2(t) \pm 2ic_\alpha^2 t^2 Q_\alpha^2(t) \\ (c\cdot Q)_{\alpha+(1\pm i)}(t)\,(c\cdot Q)_{\alpha-(1\pm i)}(t) &= \mp 2it^2 P_\alpha^2(t) + (t^4-1)c_\alpha^2 Q_\alpha^2(t). \end{aligned} \tag{9.3.10.1}$$

Assume that Proposition is already proved for α 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 ϵ, δ 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 α 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 $(\frac{\Omega}{2}+L)\overset{\bullet}{\cup}(\frac{i\Omega}{2}+L)$ 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

$$\begin{aligned}
-(N\alpha - 1)a_{N\alpha-1} \equiv 0 &\Longrightarrow a_{N\alpha-1} \equiv 0 \pmod{\alpha\mathbf{Z}[i]}\\
-(N\alpha - 2)a_{N\alpha-2} \equiv 0 &\Longrightarrow a_{N\alpha-2} \equiv 0 \pmod{\alpha\mathbf{Z}[i]}\\
&\cdots\\
-(N\alpha - p + 1)a_{N\alpha-p+1} \equiv 0 &\Longrightarrow a_{N\alpha-p+1} \equiv 0 \pmod{\alpha\mathbf{Z}[i]},
\end{aligned}$$

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 $K = \mathbf{Q}(i)(sl(u) \mid u \in \frac{1}{\alpha}L)$. 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 α. 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_α $(\in \{\pm 1, \pm i\})$ 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 α 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 α 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 Σ_α be as in 9.3.1. Fix $a \in \mathbf{Z}[i]$ not divisible by α. 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 Σ_α 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 β. 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 β.

(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

$$(\exists x \in \mathbf{Z})\ x^4 \equiv -3 \pmod{p} \iff \left(\frac{-3}{\alpha}\right)_4 = 1 \iff \alpha \equiv \pm 1 \ (\operatorname{mod} 3\mathbf{Z}[i]) \iff$$

$$\iff u \equiv \pm 1 \pmod{3},\ v \equiv 0 \pmod{3} \iff v \equiv 0 \pmod{6} \iff (\exists a, b \in \mathbf{Z})\ \ p = a^2 + (6b)^2.$$

(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 Ω' (e.g. such that $\wp'(z)^2 = 4\wp(z)^3 - 4$).*

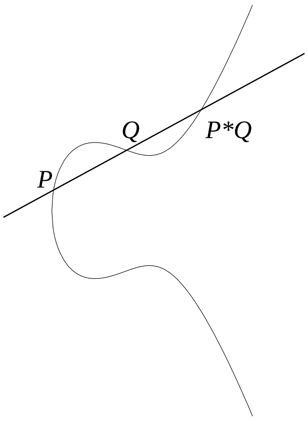
10. Group law on smooth cubic curves

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 $P, Q, R \in C(K)$:

$$(P \boxplus Q) \boxplus R \overset{?}{=} P \boxplus (Q \boxplus R) \tag{10.1.3.1}$$

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:*

$$O \text{ is an inflection point of } C \iff O * O = O \iff (\forall P \in C(K)) \quad P * O = -P.$$

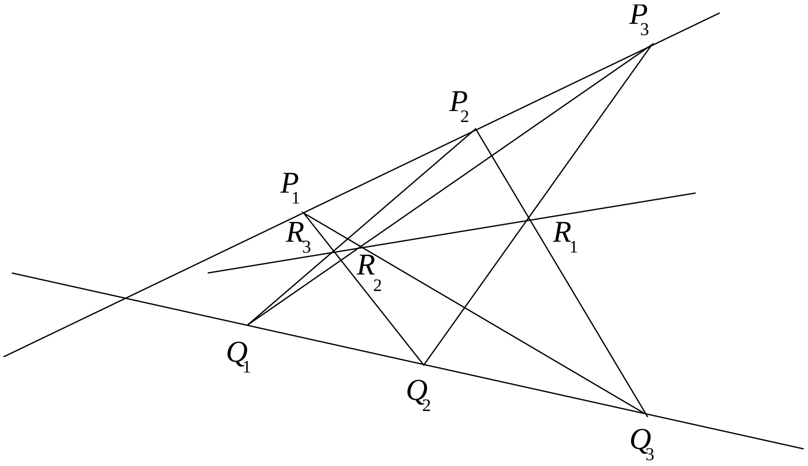
10.2 Configuration theorems

We begin by recalling two classical geometric results.

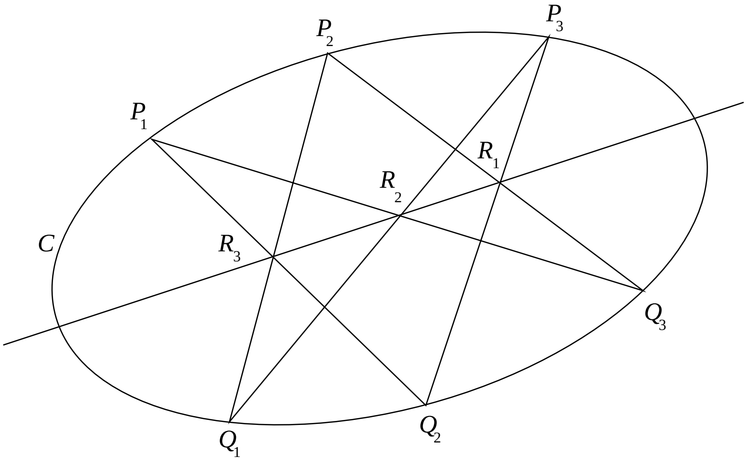
(10.2.1) Theorem of Pappus. *Let P_1, P_2, P_3 (resp. Q_1, Q_2, Q_3) be two triples of collinear points in the plane. Let*

$$R_k = \overline{P_iQ_j} \cap \overline{P_jQ_i} \qquad (\{i, j, k\} = \{1, 2, 3\})$$

be the intersection points of the pairs of lines $\overline{P_iQ_j}$ and $\overline{P_jQ_i}$. 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

$$C_1 \cap C_2 = \{O, P, Q, R, P * Q, P \boxplus Q, Q * R, Q \boxplus R, S\}, \qquad S = \overline{P(Q \boxplus R)} \cap \overline{R(P \boxplus Q)}, \tag{10.2.6.1}$$

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 ∞, 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. ω is holomorphic at ∞. 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_α 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_α.

(10.3.3) Corollary. *If $g(P_\alpha) = 0$ for $\alpha = 1, \dots, d-1$, 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.