Complex torus and elliptic curves
Lecture notes

Salim Rivière

March 2014

Abstract

These are notes on the uniformization of complex elliptic curves via Weierstrass functions. Everything is taken out from references [1], [2] and [3], our contribution is just to give a self-contained exposition and more details for certain parts of the original proofs.

Contents

1 Lattices, tori and meromorphic functions

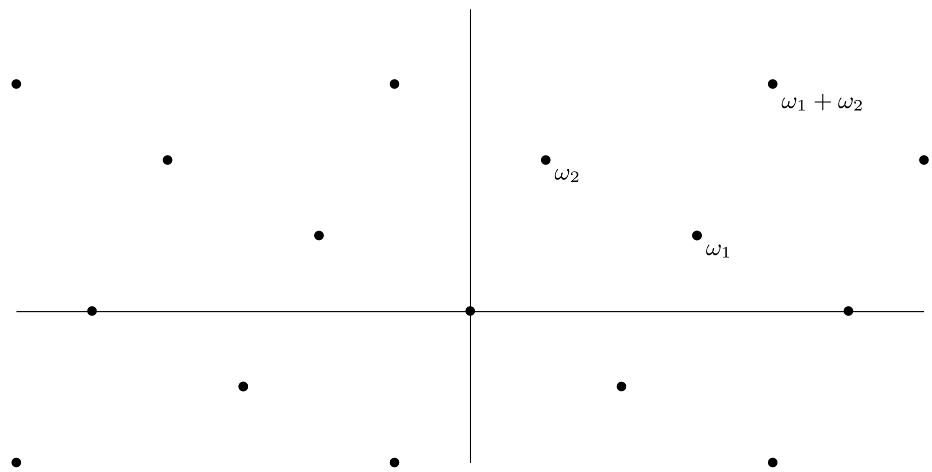
1.1 Change of lattices, complex tori

Let ω_1 and ω_2 be two complex numbers in $\mathbb{C}$ that are free over $\mathbb{R}$ ($\lambda_1\omega_1 + \lambda_2\omega_2 = 0$, λ_1, $\lambda_2 \in \mathbb{R} \Rightarrow \lambda_1 = \lambda_2 = 0$).

They define a 2-dimensional **lattice**

$$\Gamma := \{m\omega_1 + n\omega_2 \mid m,\ n \in \mathbb{Z}\}$$

which is a discrete abelian group in $\mathbb{C}$. For example, when $\omega_1 = 3 + i$ and $\omega_2 = 1 + 2i$ we get



We can define a torus $\mathbb{T}$ by setting

Definition 1.1.1. *The* ***complex torus*** *associated to the lattice* Γ *is the quotient space*

$$\mathbb{T} := \mathbb{C}/_{\Gamma}$$

An element of $\mathbb{T}$ is thus an equivalence class of elements of $\mathbb{C}$ for the equivalence relation

$$z \sim z' \quad \Leftrightarrow \quad \exists n,\, m \in \mathbb{Z} \,/ z = z' + n\omega_1 + m\omega_2$$

The complex structure of $\mathbb{C}$ induces a complex structure on $\mathbb{T}$ such that the projection $\mathbb{C} \to \mathbb{T}$ is holomorphic. This complex structures depends on the lattice Γ. However, if we define Γ' to be the lattice

$$\Gamma' := \{m + n\tau \mid m,\, n \in \mathbb{Z}\}$$

where $\tau := \omega_2/\omega_1$, and $\mathbb{T}'$ to be the torus $\mathbb{C}/\Gamma'$, then the bijective "multiplication by ω_1" map

$$\begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \omega_1 z \end{array}$$

sends Γ' bijectively to Γ.

Proposition 1.1.2. *Multiplication by* ω_1 *induces a biholomorphic isomorphism*

$$\mathbb{T}' \xrightarrow{\cong} \mathbb{T}$$

Thus, we can reduce ourselves to the study of tori given by lattices with $\omega_1 = 1$ and $\omega_2 = \tau$. We can even suppose that $\operatorname{Im} \tau > 0$ since the lattice generated by 1 and τ is the same as the lattice generated by 1 and $-\tau$.

1.2 Meromorphic functions

We now fix a lattice $\Gamma := \{m + n\tau \mid m,\, n \in \mathbb{Z}\}$ and denote by $\mathbb{T} := \mathbb{C}/_{\Gamma}$ the associated torus with projection $\pi : \mathbb{C} \to \mathbb{T}$.

By definition of the complex structure on $\mathbb{T}$, a function $f : \mathbb{T} \to \mathbb{C}$ is **meromorphic** if and only if the composite $f \circ \pi : \mathbb{C} \to \mathbb{C}$ is. Thus, we are interested in meromorphic functions on $\mathbb{C}$ that are invariant under addition of elements of Γ, i.e. Γ-periodic.

Remark 1.2.1. *Constant functions are holomorphic thus meromorphic. Note that Liouville's theorem implies that bounded holomorphic functions are constant. Since* $\mathbb{T}$ *is compact, any holomorphic function is bounded, thus constant.*

Among meromorphic periodic functions, some are of particular interest for us:

Definition 1.2.2. *The* ***Weierstrass function*** $\wp : \mathbb{C} \to \mathbb{C}$ *is defined by*

$$\wp(z) := \frac{1}{z^2} + \sum_{\substack{\omega \in \Gamma \\ \omega \neq 0}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

for all z *in* $\mathbb{C}$.

Proposition 1.2.3. *The Weierstrass function is*

- *well-defined and holomorphic on* $\mathbb{C} - \Gamma$,
- *meromorphic in each* z *of* Γ *with a pole of order* 2,
- *even and* Γ*-periodic.*

It's derived function is odd, Γ*-periodic, meromorphic with poles of order* 3 *on the lattice and is given by*

$$\wp'(z) = \sum_{\substack{\omega \in \Gamma \\ \omega \neq 0}} \frac{-2}{(z-\omega)^3}$$

Proof. Well defined amounts to prove that the sum involved in the definition of $\wp$ is convergent. For any ω in $\Gamma - \{0\}$

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{\omega^2 - z^2 + 2z\omega - \omega^2}{\omega^2(z-\omega)^2} = \frac{1}{\omega^3}\frac{2z - z^2/\omega}{z/\omega - 1}$$

Since

$$\lim_{\omega \to \infty} \left| \frac{2z - z^2/\omega}{z/\omega - 1} \right| = 2|z|$$

there exists a positive constant $C(z)$ such that

$$\left|\frac{2z - z^2/\omega}{z/\omega - 1}\right| < C(z)$$

for all ω in $\Gamma - \{0\}$. Thus

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| < \frac{C(z)}{|\omega|^3}$$

The fact that $\sum_{\substack{\omega\in\Gamma\\ \omega\neq 0}} \frac{C(z)}{|\omega|^3}$ is convergent implies that

$$\sum_{\substack{\omega\in\Gamma\\ \omega\neq 0}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \tag{1}$$

is absolutely convergent, thus convergent. This proves that $\wp$ is well-defined.

To see that $\wp$ is holomorphic in $z \in \mathbb{C} - \Gamma$, remark that there exists a neighbourhood V of z and a positive number such that the constants $C(z')$ are bounded by C when z' is in V i.e.

$$C(z') < C \quad \forall z' \in V$$

Thus the sum (1) is normaly convergent on V. Since each term $\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$ is holomorphic in z, the limit is also holomorphic in z. Morevover, $\wp'(z)$ can be obtained by deriving term by term so that

$$\wp'(z) = -\sum_{\omega\in\Gamma} \frac{2}{(z-\omega)^3}$$

t is clear that $\wp'$ is meromorphic with poles of order 3 on the lattice and that it is Γ-periodic.

It is clear that each element of the lattice is a pole of order 2 of $\wp$. To see that $\wp$ is even notice that one can reparametrize the sum (1) using $-\omega$ instead of ω.

The periodicity goes as follows: choose a point γ in Γ and set

$$\mathcal{Q}(z) := \wp(z+\gamma) - \wp(z)$$

for all z in $\mathcal{C} - \Gamma$. Then

$$\mathcal{Q}'(z) := \wp'(z+\gamma) - \wp'(z) = 0$$

because $\wp'$ is Γ-periodic. Thus, there exists a constant C (depending on γ *a priori*) such that

$$\mathcal{Q}(z) := \wp(z+\gamma) - \wp(z) = C$$

But for $z = -\gamma/2$ we have that

$$\mathcal{Q}(-\gamma/2) := \wp(\gamma/2) - \wp(-\gamma/2) = 0$$

because $\wp$ is even. Thus, $C = 0$ and $\wp(z+\gamma) = \wp(z)$ for all z in $\mathbb{C} - \Gamma$. This proves that $\wp$ is Γ-periodic.

□

The Weirestrass function associated to the lattice Γ satisfies a nice differential equation:

Proposition 1.2.4. *The Weierstrass function $\wp$ and its derivative $\wp'$ satisfy*

$$(\wp')^2 = 4\wp^3 + g_2\wp + g_3 \tag{2}$$

*where g_2 and g_3 are the **Eisenstein series** (of the lattice Γ) defined by*

$$g_2 = g_2(\tau) := \sum_{\substack{\omega\in\Gamma\\ \omega\neq 0}} \frac{-60}{\omega^4} = \sum_{\substack{(m,n)\in\mathbb{Z}^2\\ (m,n)\neq(0,0)}} \frac{-60}{(m+n\tau)^4} \quad ; \quad g_3 = g_3(\tau) := \sum_{\substack{\omega\in\Gamma\\ \omega\neq 0}} \frac{-140}{\omega^6} = \sum_{\substack{(m,n)\in\mathbb{Z}^2\\ (m,n)\neq(0,0)}} \frac{-140}{(m+n\tau)^6}$$

Theorem 1.2.5. *The field of meromorphic functions on $\mathbb{T}$, denoted $\mathcal{M}(\mathbb{T})$ is generated by $\wp$ and $\wp'$ i.e.*

$$\mathcal{M}(\mathbb{T}) \cong \mathbb{C}(\wp, \wp')$$

More precisely, relation (2) is the "smallest relation" satisfied by $\wp$ and $\wp'$ i.e.

$$\begin{array}{rcl} \phi : \mathbb{C}(X)[Y]/(Y^2 - 4X^3 - g_2X - g_3) & \longrightarrow & \mathcal{M}(\mathbb{T}) \\ X & \longmapsto & \wp \\ Y & \longmapsto & \wp' \end{array}$$

is an isomorphism of fields.

Proof. We only prove the surjectivity of ϕ. Let $f : \mathbb{T} \to \mathbb{C}$ be a meromorphic function on the torus. If z_0 is a pole of order k of $f \circ \pi$ which is not on the lattice Γ, then setting $f \circ \pi(\wp - \wp(z_0))^k$ gives a holomorphic function in z_0. Indeed, since z_0 doesn't belong to Γ, $\wp$ is homolorphic in z_0 and admits a Taylor expansion near z_0 of the form

$$\wp(z) = \wp(z_0) + \wp'(z_0)(z - z_0) + o(|z - z_0|)$$

This implies that $z \mapsto f(\pi(z))(\wp(z) - \wp(z_0))^k$ admits a finite limit in z_0 ans thus is holomorphic in z_0. Proceeding in the same fashion for all poles that are not on the lattice we get a Γ-periodic function $z \mapsto f(\pi(z))Q(\wp(z))$, where $Q(\wp)$ is a polynomial in $\wp$, which has only possible poles on the lattice (this means that the induced function on the $\mathbb{T}$ can just have a pole in $0 := \pi(\Gamma)$). If we suppose that $z \mapsto f(\pi(z))Q(\wp(z))$ has a pole of even order $2k$ in 0, then there exists a constant c such that

$$z \mapsto f(\pi(z))Q(\wp(z)) - c\wp(z)^k$$

has a pole of order at most $2k - 1$ in 0. Similarly, if the pole as odd order $2k - 1$ we can substract a good multiple of $\wp'$ to lower the order of this pole. We see that repeating this procedure leads to a function that is holomorphic in zero. In other words, there exists a polynomial in two variables $R(X, Y)$ such that the function on the torus $fQ(\wp) - R(\wp, \wp')$ is holomorphic. Since $\mathbb{T}$ is compact, this function is bounded thus constant (by Liouville's theorem). Hence, there exists a constant C in $\mathbb{C}$ such that

$$fQ(\wp) - R(\wp, \wp') = C$$

i.e.

$$f = \frac{C + R(\wp, \wp')}{Q(\wp)}$$

This proves that any meromorphic function f is a rational function in $\wp$ and $\wp'$ which implies that ϕ is surjective. □

2 The link with elliptic curves

2.1 The projective plane, complex elliptic curves

Definition 2.1.1. *The* ***complex projective plane****, denoted $\mathbb{C}P^2$ is the set of complex lines in $\mathbb{C}^3$. Any non-zero vector (z_1, z_2, z_3) in $\mathbb{C}^3$ spans a complex line i.e. an element of $\mathbb{C}P^2$ that we denote by $[z_1 : z_2 : z_3]$ (homogenous coordinates). $\mathbb{C}P^2$ is an affine complex variety with open affine cover given by U_1, U_2, U_3 where*

$$U_i := \{L = [z_1, z_2, z_3] \in \mathbb{C}P^2 \mid z_i \neq 0\}.$$

A ***projective curve*** *is a closed subset of $\mathbb{C}P^2$ which is the zero-locus of a homogenous polynomial P in $\mathbb{C}[X, Y, Z]$. It is said to be* ***non-singular*** *when the partial derivatives of P never vanish simultaneously on its zero locus.*

An ***elliptic curve*** *is a non-singular projective curve which is the zero locus of a polynomial P such that there exists an affine chart in which P takes the form*

$$Y^2 - 4X^3 - aX - b$$

Remark 2.1.2. *To any polynomial $P := \sum_{i,j} a_{i,i} X^i Y^j$ of degree n in $\mathbb{C}[X, Y]$, we can associate a homogenous polynomial $\tilde{P}$ of degree n in $\mathbb{C}[X, Y, Z]$ by setting*

$$\tilde{P} := \sum_{i,j} a_{i,i} X^i Y^j Z^{n-i-j}$$

*The projective curve corresponding to the zero locus of $\tilde{P}$ will be referred to as the projective curve a**ssociated to** P in the sequel.*

Proposition 2.1.3. *The projective curve associated to a polynomial*

$$P := Y^2 - X^3 - aX - b$$

is non singular (i.e. elliptic) if and only if the discriminant

$$\Delta(a, b) := 4a^3 + 27b^2$$

is not zero.

Proof. We have that $\frac{\partial P}{\partial Y}(x,y)=0$ if and only if $y=0$. Thus, the only points (x,y) of the zero locus of P (on the curve) where $\frac{\partial P}{\partial Y}$ vanishes are of the form $(x,0)$. But such a point is on the curve if and only if

$$P(x,0) = -x^3 - ax - b = 0$$

If x_1, x_2, x_3 are the roots of X^3+aX+b, this condition is equivalent to the fact that $x=x_i$ for some $i\in\{1,2,3\}$. But

$$\frac{\partial P}{\partial X} = -\frac{\partial}{\partial X}\big((X-x_1)(X-x_2)(X-x_3)\big) = -((X-x_2)(X-x_3)+(X-x_1)(X-x_3)+(X-x_1)(X-x_2))$$

thus we see that $\frac{\partial P}{\partial X}(x_i,0)=0$ if and only if there exists $j\neq i$ such that $x_i=x_j$ i.e. if and only if P has a root of multiplicity strictly greater than one (meaning that $\operatorname{card}\{x_1,x_2,x_3\}\leqslant 2$).

Now recall that the coefficients a and b of the polynomial X^3+aX+b can be expressed in terms of its roots x_i in the following manner

$$a = x_1x_2+x_1x_3+x_2x_3 \qquad \text{and} \qquad b=-x_1x_2x_3$$

so that

$$\Delta(a,b) := 4a^3+27b^2 = 4(x_1x_2+x_1x_3+x_2x_3)^3+27(x_1x_2x_3)^2$$

Since there is no term of degree 2 in x^3+aX+b the sum of the roots is zero thus $x_3=-x_2-x_1$. Hence

$$\begin{aligned}\Delta(a,b) =& -4(x_1^2+x_2x_1+x_2^2)^3+27(x_1^2x_2+x_1x_2^2)^2\\ =& -4(x_1^6+x_1^3x_2^3+x_2^6+3(x_1^5x_2+2x_1^4x_2^2+2x_1^2x_2^4+x_1x_2^5)+6x_1^3x_2^3)+27(x_1^4x_2^2+2x_1^3x_2^3+x_1^2x_2^4)\\ =& -4x_1^6-12x_1^5x_2+3x_1^4x_2^2+26x_1^3x_2^3+3x_1^2x_2^4-12x_1x_2^5-4x_2^6\end{aligned}$$

On the other hand,

$$\begin{aligned}(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2 =&(x_1-x_2)^2(2x_1+x_2)^2(x_1+2x_2)^2\\ =&(2x_1^3+3x_1^2x_2-3x_1x_2^2-2x_2^3)^2\\ =&4x_1^6+12x_1^5x_2-3x_1^4x_2^2-26x_1^3x_2^3-3x_1^2x_2^4+12x_1x_2^5+4x_2^6\\ =&-\Delta(a,b)\end{aligned}$$

Hence

$$\left\{\begin{array}{l}P(x,y)=0\\ \frac{\partial P}{\partial Y}(x,y)=0\\ \frac{\partial P}{\partial X}(x,y)=0\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}y=0\\ x\in\{x_1,x_2,x_3\}\\ \operatorname{card}\{x_1,x_2,x_3\}\leqslant 2\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}y=0\\ x\in\{x_1,x_2,x_3\}\\ (x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2=-\Delta(a,b)=0\end{array}\right.$$

Thus the curve is singular if and only if $\Delta(a,b)=0$.

□

2.2 The uniformization isomorphism

In the first section, we have seen that given τ in the upper half plane, the torus $\mathbb{T}:=\mathbb{C}/\Gamma$ (where Γ is the lattice generated by 1 and τ) is endowed with a particular meromorphic function: the Weierstrass function $\wp:\mathbb{T}\to\mathbb{C}$ which satisfies the differential equation:

$$(\wp')^2 = 4\wp^3+g_2\wp+g_3$$

or equivalently

$$(\frac{\wp'}{2})^2 = \wp^3+\frac{g_2}{4}\wp+\frac{g_3}{4}$$

This means that for any z in $\mathbb{C}-\Gamma$, the element $[\wp(z):\frac{\wp'(z)}{2}:1]$ of $\mathbb{C}P^2$ belongs to the projective curve associated to the polynomial $Y^2-X^3-\frac{g_2}{4}X-\frac{g_3}{4}$. Recall that g_2 and g_3 depend on the choice of τ.

Proposition 2.2.1. *For any τ with strictly positive imaginary part,*

$$\Delta(\frac{g_2}{4},\frac{g_3}{4})\neq 0.$$

Thus, the projective curve associated to $Y^2-X^3-\frac{g_2}{4}X-\frac{g_3}{4}$ is elliptic.

Let $\mathcal{C}(\tau)$ be the elliptic curve associated to $Y^2-X^3-\frac{g_2}{4}X-\frac{g_3}{4}$.

Theorem 2.2.2. [Uniformization isomorphism] *The map*

$$\begin{array}{ccl} \mathbb{T} & \to & \mathcal{C}(\tau) \subset \mathbb{C}P^2 \\ [z] & \mapsto & \begin{cases} [\wp(z) : \wp'(z)/2 : 1] & \textit{if } z \notin \Gamma, \\ [1 : 1 : 0] & \textit{if } z \in \Gamma. \end{cases} \end{array}$$

is a biholomorphism.

The reciproque of the preceeding theorem is true:

Theorem 2.2.3. *Any complex elliptic curve is "isomorphic" to an elliptic curve of the form $\mathcal{C}(\tau)$ for a certain τ, thus analytically isomorphic to a complex torus.*

Thus, we see that, thanks to the uniformization isomorphism theorem and its reciproque, any complex elliptic curve $\mathcal{C}$ can be identified with the complex torus $\mathbb{T}$ associated to a certain lattice Γ (associated to a certan choice of τ). But since $\mathbb{T}$ is a quotient of abelian groups, it is itself an abelian group (with neutral element $[0]$). This implies that any elliptic $\mathcal{C}$ can be endowed with an abelian group multiplication. Is there a way to describe this multiplication geometrically ? This might be the subject of next lectures...

References

[1] Martin Schlichenmaier, *An introduction to Riemann Surfaces, Algebraic Curves and Moduli Spaces.* Lecture Notes in Physics 322, Springer-Verlag, 1989.

[2] Christophe Delaunay, *Cryptographie sur les courbes elliptiques.* `http://math.univ-lyon1.fr/~wagner/coursDelaunay.pdf`

[3] Richard Schwartz, *Notes on Weiertrass Uniformization.* `http://www.math.brown.edu/~res/M154/notes9.pdf`