Lecture 2 (January 30)

Elliptic curves. Last time, we introduced the Weierstrass $\wp$-function

$$P(z) = \frac{1}{z^2} + \sum_{\gamma \in \Gamma \setminus \{0\}} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right),$$

where $\Gamma = \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2$ is a lattice in $\mathbb{C}$. We showed that it is meromorphic and Γ-periodic, and that it satisfies the differential equation

$$P'(z)^2 = 4P(z)^3 - g_2 P(z) - g_3,$$

where g_2, g_3 are certain constants that depend on Γ. We are really interested in the compact Riemann surface $E = \mathbb{C}/\Gamma$, which is topologically a torus. Using the differential equation, we concluded that the image of the holomorphic mapping

$$h \colon E \to \mathbb{P}^2, \quad z + \Gamma \mapsto [P(z), P'(z), 1],$$

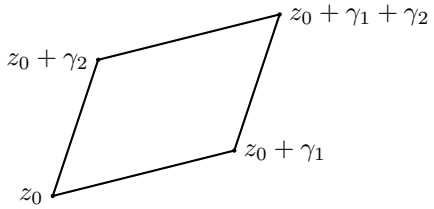
is contained in the cubic curve C with equation $y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3$. Now we are going to argue that h is an isomorphism between E and this cubic curve.

For that, we need two basic facts about doubly periodic meromorphic functions. Let f be a meromorphic function on $\mathbb{C}$ that is Γ-periodic. We may also view f as a holomorphic mapping from E to $\mathbb{P}^1$. If f has a zero or pole at a point $x \in E$, we let $\operatorname{ord}_x(f)$ denote the order of the zero (with a plus sign) or the order of the pole (with a minus sign); if x is neither a zero nor a pole, we set $\operatorname{ord}_x(f) = 0$. The fact that f is Γ-periodic constrains the number and location of the zeros and poles, in the following way:

(1) We have $\displaystyle\sum_{x \in E} \operatorname{ord}_x(f) = 0.$

(2) We have $\displaystyle\sum_{x \in E} \operatorname{ord}_x(f) \cdot x = 0$ as points in E.

Remember that we can add and subtract points in $E = \mathbb{C}/\Gamma$, because the quotient is an abelian group. Both formulas are consequences of the residue theorem. Let's quickly look at how this works. Consider the parallelogram D spanned by the two basis vectors $\gamma_1, \gamma_2 \in \Gamma$, with one corner at a point $z_0 \in \mathbb{C}$, and choose z_0 such that the boundary ∂D of the parallogram does not pass through any zeros or poles of f.



At each zero or pole of f, the meromorphic function f'/f has a simple pole with residue equal to the order of the zero or pole. The residue theorem therefore gives

$$\sum_{z \in D} \operatorname{ord}_z(f) = \frac{1}{2\pi i} \int_{\partial D} \frac{f'(z)}{f(z)}\, dz.$$

The integral on the right-hand side is equal to zero because f is Γ-periodic. Since D is a fundamental domain for the action of Γ on $\mathbb{C}$, the left-hand side is equal to $\sum_{x \in E} \operatorname{ord}_x(f)$, and so we get the formula in (1). The formula in (2) is proved in a similar manner. Again by the residue theorem, we have

$$\sum_{z \in D} \operatorname{ord}_z(f) \cdot z = \frac{1}{2\pi i} \int_{\partial D} \frac{z f'(z)}{f(z)}\, dz.$$

This time, the integral on the right-hand side evaluates to an element in $\mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2$, and so we get

$$\sum_{z \in D} \operatorname{ord}_z(f) \cdot z \in \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2,$$

which translates to the formula in (2).

We can now prove that $E = \mathbb{C}/\Gamma$ is isomorphic to the cubic curve C.

Proposition 2.1. *The mapping $h\colon E \to \mathbb{P}^2$ induces an isomorphism between E and the cubic curve C.*

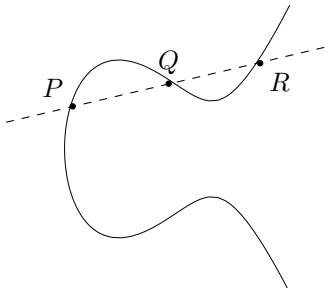
Proof. Let's first show that h is surjective. The point $[0, 1, 0]$ is the image of $0 \in E$, so let's consider points of the form $[a, b, 1]$ with $b^2 = 4a^3 - g_2 a - g_3$. We need to find $z_0 \in \mathbb{C}$ such that $P(z) = a$ and $P'(z) = b$. The function $P(z) - a$ is Γ-periodic and meromorphic, and has (up to translation by by Γ) a unique pole of order 2. According to the discussion above, it must therefore have exactly two zeros; since $P(z)$ is even, these will be of the form $\pm z_0$ for some $z_0 \in \mathbb{C}$. The differential equation for $P(z)$ then gives $P'(z_0)^2 = 4P(z_0)^3 - g_2 P(z_0) - g_3 = b^2$, and therefore $P'(z_0) = \pm b$. If $P(z_0) = b$, we can take $z = z_0$; otherwise, we take $z = -z_0$.

Now let's prove that h is injective. It is easy to see that the points in Γ are the only points mapping to $[0, 1, 0]$, so it is enough to consider two points $z_1, z_2 \in \mathbb{C}$ such that $P(z_1) = P(z_2)$ and $P'(z_1) = P'(z_2)$. We need to argue that $z_1 = z_2$. As before, $P(z) - P(z_1)$ must have exactly two zeros, which are z_1 and $-z_1$, and so either $z_2 \equiv z_1 \mod \Gamma$ and we are done, or $z_2 \equiv -z_1 \mod \Gamma$. In the second case, we get $P'(z_1) = P'(z_2) = -P'(z_1)$, and so $P'(z_1) = 0$. But we will see in a moment that the only zeros of $P'(z)$ are the translates of $\gamma_1/2$, $\gamma_2/2$, and $(\gamma_1 + \gamma_2)/2$, and no two of these differ by an element of Γ.

Next, we argue that the cubic curve C is nonsingular, and therefore a compact Riemann surface. This amounts to saying that all three roots of the cubic polynomial $4x^3 - g_2 x - g_3$ are distinct. Because h is surjective, these roots are of the form $P(z)$, where $z \in \mathbb{C}$ is any point such that $P'(z) = 0$. Now $P'(z)$ has (up to translation by Γ) a unique pole of order 3, and so it must have exactly 3 zeros. Because $P'(z)$ is odd, each of $\gamma_1/2$, $\gamma_2/2$, and $(\gamma_1 + \gamma_2)/2$ is a zero, and so these are all the zeros. They are different modulo Γ, and so our cubic polynomial has three distinct roots.

Now $h\colon E \to C$ is a bijective holomorphic mapping between two complex manifolds, and therefore biholomorphic (by the inverse function theorem). This proves that $E = \mathbb{C}/\Gamma$ is isomorphic to the cubic curve C. □

Let's also briefly discuss the group structure. As you know, the points of a nonsingular cubic curve form a group; three points P, Q, R on the cubic are collinear (in $\mathbb{P}^2$) if and only if they satisfy $P + Q + R = 0$ as elements of the group.



In fact, the isomorphism $u\colon E \to C$ also respects the group structure, because of the following proposition.

Proposition 2.2. *Let $u, v, w \in \mathbb{C}$ be three distinct points. Then $u + v + w \in \Gamma$ if and only if the points $h(u)$, $h(v)$, and $h(w)$ are collinear in $\mathbb{P}^2$.*

Proof. I promised to put the proof in the notes, so here it is. Because h is bijective, we only need to prove one implication. Let's focus on the case where $u, v, w \notin \Gamma$. The fact that the three points are collinear then says that

$$\det \begin{pmatrix} P(u) & P(v) & P(w) \\ P'(u) & P'(v) & P'(w) \\ 1 & 1 & 1 \end{pmatrix} = 0.$$

This means that there are constants $A, B, C \in \mathbb{C}$ such that $AP(z)+BP'(z)+C = 0$ for $z \in \{u, v, w\}$. Because this function has a unique pole of order 3, these must be the only zeros (up to translation by Γ). In particular, they are simple zeros, and so the second consequence of the residue theorem tells us that $u + v + w \in \Gamma$. A similar argument works when one of the three points belongs to the lattice Γ. □

Exercise 2.1. The lemniscate sine is related to the Weierstrass $\wp$-function, but perhaps not quite in the way one would expect. Prove the formula

$$\frac{\varpi^2}{\mathrm{sl}^2(\varpi z)} = P(z),$$

where $P(z)$ is the Weierstrass $\wp$-function for the lattice $\mathbb{Z}+\mathbb{Z}i$ of Gaussian integers. (*Hint:* Look at the first few terms in the Laurent series.) Can you find the equation of the cubic curve for this lattice?

Abelian varieties. Let's now start looking at abelian varieties, from the point of view of complex geometry. Consider a compact and connected complex Lie group X. This means that X is a complex manifold, say of dimension n, that is compact and connected; it also means that the group operations

$$X \times X \to X, \quad (x, y) \mapsto x \cdot y, \qquad X \to X, \quad x \mapsto x^{-1},$$

are *holomorphic* mappings. Let $e \in X$ denote the identity element. We are going to prove that X is commutative, and that it has the form V/Λ, where V is an n-dimensional complex vector space, and $\Lambda \subseteq V$ is a discrete subgroup of rank $2n$.

First, we need to review a few basic facts about 1-parameter subgroups. Let $V = T_eX$ denote the tangent space to X at the identity element $e \in X$; this is an n-dimensional complex vector space. The result we need is that for every vector $v \in V$, there is a unique holomorphic mapping

$$\phi_v \colon \mathbb{C} \to X$$

that is a group homomorphism and whose differential

$$(d\phi_v)_e \colon \mathbb{C} = T_0\mathbb{C} \to V = T_eX$$

maps $1 \in \mathbb{C}$ to the given vector $v \in V$. This is a consequence of the existence and uniqueness result for solutions to ordinary differential equations. (Briefly, the tangent vector $v \in T_eX$ can be extended in a unique way to a holomorphic tangent vector field $\tilde{v}$ on all of X, using the group structure. Then ϕ_v solves the initial value problem $\phi'(t) = \tilde{v}_{\phi(t)}$, $\phi(0) = e$. The solution is holomorphic by Cauchy's theorem, which is a nice but fairly elementary result.) We need three additional facts:

(1) The mapping

$$\phi \colon \mathbb{C} \times V \to X, \quad (t, v) \mapsto \phi_v(t),$$

is holomorphic (because the solution to a holomorphic initial value problem depends holomorphically on the initial data).

(2) Let us define the *exponential mapping* by the formula

$$\exp\colon V \to X, \quad \exp(v) = \phi_v(1).$$

This is a holomorphic mapping by (1). The uniqueness of ϕ_v implies that $\phi_v(st) = \phi_{sv}(t)$ for every $s, t \in \mathbb{C}$; therefore

$$\phi_v(t) = \exp(tv)$$

for $t \in \mathbb{C}$ and $v \in V$. By construction, the differential

$$(d\exp)_e\colon V = T_0V \to V = T_eX$$

is the identity mapping. By the (holomorphic) inverse function theorem, exp is therefore a biholomorphic isomorphism between a neighborhood of $0 \in V$ and a neighborhood of $e \in X$.

(3) Suppose that $h\colon X_1 \to X_2$ is both a holomorphic mapping and a group homomorphism. Then one has

$$h\big(\exp_{X_1}(v)\big) = \exp_{X_2}\big((dh)_e(v)\big)$$

for every $v \in V$. The reason is that the composition

$$h \circ \phi_v\colon \mathbb{C} \to X_2$$

is a holomorphic group homomorphism with

$$d(h \circ \phi_v)_e(1) = (dh)_e \circ (d\phi_v)_e(1) = (dh)_e(v).$$

The result we want therefore follows from the uniqueness statement.

We can now prove that the group structure on X is commutative.

Lemma 2.3. *Every compact connected complex Lie group is abelian.*

Proof. For $x \in X$, consider the conjugation mapping

$$C_x\colon X \to X, \quad C_x(y) = xyx^{-1};$$

it is cleary biholomorphic and an automorphism of the group X. The differential

$$(dC_x)_e\colon V \to V$$

is therefore an automorphism of $V = T_eX$. This gives us a holomorphic mapping

$$X \to \mathrm{GL}(V), \quad x \mapsto (dC_x)_e.$$

Because $\mathrm{GL}(V)$ sits inside the vector space $\mathrm{End}(V) \cong \mathbb{C}^{n^2}$, and X is compact and connected, this mapping must be constant; the constant value is

$$(dC_x)_e = (dC_e)_e = \mathrm{id}_V\,.$$

We can now apply (3) from above and conclude that

$$C_x\big(\exp(v)\big) = \exp\big((dC_x)_e(v)\big) = \exp(v)$$

for every $x \in X$ and every $v \in V$. This says that the image $\exp(V)$ of the exponential mapping lies in the center of the group X. It also generates X as a group (because $\exp(V)$ contains a neighorhood of $e \in X$ and X is compact and connected); it follows that X is commutative. □

There are of course many compact real Lie groups that are not commutative; the magic comes from the fact that the group operations need to be holomorphic. Next, let's prove that X is isomorphic to the quotient of V by a discrete subgroup.

Lemma 2.4. *The exponential mapping* $\exp\colon V \to X$ *is a surjective group homomorphism. Its kernel* $\Lambda = \ker(\exp)$ *is a lattice in* V*, and* $X \cong V/\Lambda$.

Proof. For any two vectors $v, w \in V$, consider the holomorphic mapping

$$\mathbb{C} \to X, \quad t \mapsto \exp(tv)\exp(tw).$$

Because X is commutative, this is a group homomorphism; its differential takes $1 \in \mathbb{C}$ to the vector $v + w$. By uniqueness, it follows that

$$\exp(tv)\exp(tw) = \exp\bigl(t(v+w)\bigr).$$

Setting $t = 1$, we conclude that $\exp\colon V \to X$ is a group homomorphism. We already know that $\exp(V)$ generates X as a group; now $\exp(V)$ is also a subgroup, and so $\exp(V) = X$. The kernel $\Lambda = \ker(\exp)$ is a discrete subgroup of V (because exp is bijective in a neighborhood of $0 \in V$). The quotient V/Λ is isomorphic to X, hence compact; this means that Λ is a lattice in V. □

A bit of terminology. A discrete subgroup Λ of a complex vector space V is called a *lattice* if the quotient V/Λ is compact. It is easy to see that Λ must then be isomorphic, as a group, to $\mathbb{Z}^{2n}$, where $n = \dim V$. The quotient V/Λ is called a *compact complex torus*. So the result above is saying that every compact and connected complex Lie group is a compact complex torus.

From now on, we are going to use additive notation

$$X \times X \to X, \quad (x, y) \mapsto x + y, \qquad X \to X, \quad x \mapsto -x,$$

for the group operations; the identity element is always $0 \in X$. By choosing a basis for $\Lambda \cong \mathbb{Z}^{2n}$, we see that

$$X_{\mathbb{R}} \cong (\mathbb{R}/\mathbb{Z})^{2n} \cong (\mathbb{S}^1)^{2n}$$

as real Lie groups. We will consider the problem of how to keep track of the different possible complex manifold structures on this later on.

Corollary 2.5. *As a group, X is divisible, and for every $m \in \mathbb{Z}$, we have*

$$X[m] = \bigl\{\, x \in X \;\bigm|\; m \cdot x = 0 \,\bigr\} \cong (\mathbb{Z}/m\mathbb{Z})^{2n}.$$

Proof. This is clear from the fact that $X_{\mathbb{R}} \cong (\mathbb{R}/\mathbb{Z})^{2n}$. □