ELLIPTIC CURVES: WITH A FOCUS ON COMPLEX ANALYSIS

ZIYANG GAO
LEIBNIZ UNIVERSITÄT HANNOVER

1. Lecture 1: Introduction

Let $f \in \mathbb{C}[X, Y]$ be a polynomial in 2 variables. Consider the set of complex solutions to $f = 0$, defined by

$$V(f) := \{(x, y) \in \mathbb{C}^2 : f(x, y) = 0\} \subseteq \mathbb{A}^2_{\mathbb{C}} := \mathbb{C}^2.$$

This set will be called *a complex plane affine algebraic curve* in $\mathbb{A}^2_{\mathbb{C}}$. More precisely we make the following definition.

Definition 1.1. *A complex plane affine (algebraic) curve C in $\mathbb{A}^2_{\mathbb{C}}$ is a subset of $\mathbb{A}^2_{\mathbb{C}}$ of the form $V(f) = \{(x, y) \in \mathbb{C}^2 : f(x, y) = 0\}$ for some non-zero $f \in \mathbb{C}[X, Y]$. We say that C is irreducible if f is irreducible as a polynomial. We also define the degree of C, denoted by $\deg C$, to be the degree of P (when P is irreducible).*

In practice, it is often more convenient to add points to C to make it compact. More precisely, embed $\mathbb{A}^2_{\mathbb{C}}$ into $\mathbb{P}^2_{\mathbb{C}}$, for example by sending $(x, y) \mapsto [x : y : 1]$, and then define

$$F(X_0, X_1, X_2) := X_2^{\deg f} f(\frac{X_0}{X_2}, \frac{X_1}{X_2}).$$

Then F is a homogeneous polynomial of degree $\deg f$. Define

$$V(F) := \{[x_0 : x_1 : x_2] \in \mathbb{P}^2_{\mathbb{C}} : F(x_0, x_1, x_2) = 0\} \subseteq \mathbb{P}^2_{\mathbb{C}}.$$

It can be checked that $V(F)$ is $V(f)$ with finitely many points added, and each of these added points has X_2-coordinate 0. Moreover, $V(F)$ is the closure of $V(f)$ in $\mathbb{P}^2_{\mathbb{C}}$ in the usual topology.

Definition 1.2. *A complex plane projective (algebraic) curve C in $\mathbb{P}^2_{\mathbb{C}}$ is a subset of $\mathbb{P}^2_{\mathbb{C}}$ of the form $V(P) = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{C}} : P(x, y, z) = 0\}$ for some non-zero $P \in \mathbb{C}[X, Y, Z]$. We say that C is irreducible if P is irreducible as a polynomial. We also define the degree of C, denoted by $\deg C$, to be the degree of P (when P is irreducible).*

Each algebraic curve has complex dimension 1 and hence real dimension 2. In this course, we will see that to each plane projective curve C we can associate a (unique) Riemann surface. Today let us illustrate this with some examples.

Before moving on, let us make a definition based on this fact. It is known that each Riemann surface has a genus g. So to each plane projective curve C we can define its genus g.

We start with the multi-valued function $w \mapsto \sqrt{w}$ on $\mathbb{C}$. The fact that this function is not single-valued is easy to see: For the polar coordinate $w = re^{i\theta}$, there are infinitely many choices of θ, resulting in infinitely many choices of $e^{i\theta/2}$.

To make this function single-valued, one needs to change the domain. Here is what we can do. Note that if we cut $\mathbb{C}$ along the non-negative real axis $[0,\infty)$ we can define two holomorphic functions $\pm\sqrt{w}$ on $\mathbb{C}-[0,\infty)$ by

$$\pm\sqrt{w} = \pm\sqrt{r}e^{i\theta/2} \tag{1.1}$$

for $\theta \in (0, 2\pi)$.

Take two copies of $\mathbb{C}-[0,\infty)$ and "glue" them together to get a space X. Perhaps a better way to see the glueing process is by adding a point ∞ to $\mathbb{C}$ and then cut it along $[0,\infty]$. Note that $\mathbb{C}\cup\{\infty\}$ is a sphere topologically. Open up the cuts and glue the two copies together to get $X\cup\{\infty\}$, which is again a sphere topologically. On the space X it makes sense to say that there is a single-valued holomorphic function $\mathtt{sqr}\colon X\cup\{\infty\}\to\mathbb{C}\cup\{\infty\}$ defined by $+\sqrt{w}$ on the first copy of the cut plane and by $-\sqrt{w}$ on the second. Note that in view of $\mathtt{sqr}$, there are two particular points on $\mathbb{C}\cup\{\infty\}$, 0 and ∞, in the following sense: $\#\mathtt{sqr}^{-1}(t)=2$ except when $t=0,\infty$. Similarly there are two particular points on $X\cup\{\infty\}$, 0 and ∞, because $\#\mathtt{sqr}^{-1}(\mathtt{sqr}(x))=2$ except for $x=0,\infty$.

Of course one should be careful with the glueing process to see which edges are glued in what direction. To do this one needs to go back to the functions (1.1). If $r\in[0,\infty)$ then $+\sqrt{w}$ tends to $\sqrt{r}$ and $-\sqrt{w}$ tends to $-\sqrt{r}$ as w tends to r *through values in the upper half plane*, and vice versa as w tends to r *through values in the lower half plane.* Thus from the last sentence of the previous paragraph, one glues the upper side of the cut in the first copy to the lower side of the cut in the second copy, and the lower side of the cut in the first copy to the upper side of the cut in the second copy. Now $X\cup\{\infty\}$ is a Riemann surface of genus 0.

Another way to think of X is being the complex plane affine curve

$$C_0 = \{(x,y)\in\mathbb{C}^2 : y^2 = x\}$$

where one copy of $\mathbb{C}-[0,\infty)$ corresponds to $\{(x,y)\in\mathbb{C}^2 : y=+\sqrt{x}\}$ and the other to $\{(x,y)\in\mathbb{C}^2 : y=-\sqrt{x}\}$. Then $\mathtt{sqr}$ corresponds to $C_0\to\mathbb{C}$, $(x,y)\mapsto y$. And $X\cup\{\infty\}$ is the projectification of the plane affine curve defined above.

The discussion above says that the plane projective curve $\{(x:y:z)\in\mathbb{C}^2 : y^2=xz\}$ is a Riemann surface of genus 0.

This process of relating plane projective curves to Riemann surfaces is more general. Let us see more examples.

Example 1.3. *Consider the plane affine curve*

$$C_0 = \{(x,y)\in\mathbb{C}^2 : y^2 = x^3 - x = x(x-1)(x+1)\}.$$

Its projectification is $C=\{[x:y:z]\in\mathbb{P}^2_{\mathbb{C}} : y^2z = x^3 - xz^2\}$. The multi-valued function associated with C is $z\mapsto(z^3-z)^{1/2}$. Apart from $z=-1,0,1$, this function has 3 values. So when we cut $\mathbb{C}$, we should cut $[-1,0]$ and $[1,\infty)$. Again take two copies of $\mathbb{C}\cup\{\infty\}-([-1,0]\cup[1,\infty])$, open the cuts and glue them together along the cuts. Thus we get a torus as C. In other words, C in this case is a Riemann surface of genus 1.

Note that in this case, there are 4 exceptional points on C in view of the function $\phi\colon C\to\mathbb{C}\cup\{\infty\}$, which are -1, 0, 1 and ∞. Apart from these 4 points $\#\phi^{-1}(\phi(x))=3$ for each $x\in C$. Note that the restriction $\phi|_{C_0}\colon C_0\to\mathbb{C}$ is $(x,y)\mapsto y$.

The drawing procedure in Example 1.3 is valid for most curves of degree 3, for example $\{(x,y) \in \mathbb{C}^2 : y^2 = x^3 + x^2 + 1\}$. Or more generally $\{(x,y) \in \mathbb{C}^2 : y^2 = x(x-1)(x-\lambda)\}$ for $\lambda \neq 0, 1$. However sometimes we may get "singular points" in the process.

Example 1.4. *Consider*

$$\{(x,y) \in \mathbb{C}^2 : y^2 = x^3 + x^2\}.$$

There are 3 exceptional points: 0, -1 and ∞. However 0 is counted twice. One way to see this is by looking at the tangent space of C at 0.[1] *So when we draw the similar picture for C as above, it is a torus but the point 0 is a "node".*

As Riemann surfaces are not supposed to have singular points, we must solve this problem. Now from which Riemann surface can we obtain C in the easiest way? Note that this torus with node can be obtained by identifying two points on the Riemann sphere. So in fact the Riemann surface associated with this C is of genus 0.

Example 1.5. *Consider*

$$\{(x,y) \in \mathbb{C}^2 : y^2 = x^3\}.$$

This is more similar to the first example $z \mapsto \sqrt{z}$. In a similar way we can draw the picture for C, with 0 being a cusp.

Before moving on, let us see the following example related to Fermat's Last Theorem.

Example 1.6. *Consider*

$$\{(x,y) \in \mathbb{C}^2 : x^n + y^n = 1\}.$$

Its projectification is $C = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{C}} : x^n + y^n - z^n = 0\}$. The associated multi-valued function is $w \mapsto (1-w^n)^{1/n}$. Let $\zeta_1, \ldots, \zeta_n$ be the n-th roots of unity. Apart from $\zeta_1, \ldots, \zeta_n$, this function takes n values. Cut $\mathbb{C} \cup \{\infty\}$ along the $[\zeta_i, \zeta_{i+1}]$ for each odd i from 1 to n (if n is odd, then set $\zeta_{n+1} = \infty$), then we obtain n single-valued holomorphic functions. So we want to glue n copies of

$$(\mathbb{C} \cup \{\infty\}) - \bigcup_{i \text{ odd}} [\zeta_i, \zeta_{i+1}]$$

to obtain C. However the glueing process is rather complicated: one needs to study the local behavior of the function to see how these copies are glued together.

[1] Two directions, defined by $y = x$ and $y = -x$.

2. Lecture 2: Hilbert Nullstellensatz and Singularities of plane curves

2.1. Hilbert Nullstellensatz.

We start the following theorem without proof.

Theorem 2.1. *For $P, Q \in \mathbb{C}[X, Y]$, we have:*

$$\{(x, y) \in \mathbb{C}^2 : P(x, y) = 0\} = \{(x, y) \in \mathbb{C}^2 : Q(x, y) = 0\}$$

if and only if P divides some power of Q and Q divides some power of P; or equivalently, if and only if P and Q have the same irreducible factors.

This theorem implies that the irreducible factors of a polynomial in $\mathbb{C}[X, Y]$ are characterized by the plane algebraic curve associated with it. More precisely, we have

Corollary 2.2. *Assume $P, Q \in \mathbb{C}[X, Y]$ have no repeated factors, i.e. there exists no polynomial of degree ≥ 1 whose square divides P or Q. Then P and Q define the same plane algebraic curve in $\mathbb{C}^2$ if and only if $P(x, y) = \lambda Q(x, y)$ for some $\lambda \in \mathbb{C}^*$.*

2.2. Singularities of plane curves.

Consider a plane affine curve $C_{\text{aff}} = V(P) = \{(x, y) \in \mathbb{C}^2 : P(x, y) = 0\}$. For each point $(a, b) \in C_{\text{aff}}$, by Taylor's expansion we have

$$P(x, y) = (x - a)\frac{\partial P}{\partial x}(a, b) + (y - b)\frac{\partial P}{\partial y}(a, b) + \text{higher terms}.$$

Thus $T_{(a,b)}C_{\text{aff}}$ is the line defined by $(x - a)\frac{\partial P}{\partial x}(a, b) + (y - b)\frac{\partial P}{\partial y}(a, b) = 0$ if one of $\frac{\partial P}{\partial x}(a, b)$ and $\frac{\partial P}{\partial y}(a, b)$ is not zero. However if $\frac{\partial P}{\partial x}(a, b) = \frac{\partial P}{\partial y}(a, b) = 0$, then either $T_{(a,b)}C_{\text{aff}}$ is the union of several different lines[2], or (a, b) is a cusp[3]. Based on this observation we make the following definition.

Definition 2.3. *A point $(a, b) \in C_{\text{aff}}$*

(1) *is a singular point if*

$$\frac{\partial P}{\partial x}(a, b) = \frac{\partial P}{\partial y}(a, b) = 0.$$

(2) *has multiplicity m if m is the smallest integer such that*

$$\frac{\partial^m P}{\partial x^i \partial y^j}(a, b) \neq 0$$

for some i, j with $i + j = m$. Denote by $m_P(C_{\text{aff}})$ the multiplicity of C_{aff} at $P = (a, b)$.

(3) *is a node (or ordinary double point) if it has multiplicity 2 and*

$$\left(\frac{\partial^2 P}{\partial x \partial y}\right)^2 \neq \left(\frac{\partial^2 P}{\partial x^2}\right)\left(\frac{\partial^2 P}{\partial y^2}\right)$$

at (a, b).

The geometric meaning of nodes is that $T_{(a,b)}C_{\text{aff}}$ is the union of two simple lines.

We have similar definitions for plane projective curves

$$C = V(P) = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{C}} : P(x, y, z) = 0\}.$$

[2] For example $C = \{(x, y) \in \mathbb{C}^2 : y^2 = x^3 - x^2\}$ at $(0, 0)$.

[3] For example $C = \{(x, y) \in \mathbb{C}^2 : y^2 = x^3\}$ at $(0, 0)$.

It can be computed that $T_{[a:b:c]}C$ is the projective line defined by

$$x\frac{\partial P}{\partial x}(a,b,c) + y\frac{\partial P}{\partial y}(a,b,c) + z\frac{\partial P}{\partial z}(a,b,c) = 0$$

if not all three partial derivatives are 0.

Definition 2.4. *A point $[a : b : c] \in C$ is a singular point if*

$$\frac{\partial P}{\partial x}(a,b,c) = \frac{\partial P}{\partial y}(a,b,c) = \frac{\partial P}{\partial z}(a,b,c) = 0.$$

The curve C is said to be smooth if it has no singular points.

We can define multiplicities and nodes as for plane affine curves. But one can also use known information to treat this by covering $\mathbb{P}^2_{\mathbb{C}}$ by three pieces of affine charts to obtain three plane affine curves and by the following lemma.

Lemma 2.5. *Let $[a : b : c] \in C$. If $c \neq 0$, then $[a : b : c]$ is a non-singular point of C if and only if $(\frac{a}{c}, \frac{b}{c})$ is a non-singular point of the affine curve*

$$C_0 = \{(x, y) \in \mathbb{C}^2 : P(x, y, 1) = 0\}.$$

Similar results for the cases $a \neq 0$ and $b \neq 0$.

Moreover, the intersection of $\mathbb{C}^2$, identified with $\{[x : y : z] \in \mathbb{P}^2_{\mathbb{C}} : z \neq 0\}$, and the projective tangent line $T_{[a:b:c]}C \subseteq \mathbb{P}^2_{\mathbb{C}}$ is the tangent line $T_{(a/c,b/c)}C_0 \subseteq \mathbb{C}^2$.

Proof. Assume $m = \deg P$. Differentiating the identity $P(\lambda x, \lambda y, \lambda z) = \lambda^m P(x, y, z)$ with respect to λ and setting $\lambda = 1$, we obtain the following *Euler's relation*

$$x\frac{\partial P}{\partial x}(x,y,z) + y\frac{\partial P}{\partial y}(x,y,z) + z\frac{\partial P}{\partial z}(x,y,z) = mP(x,y,z).$$

The point $(\frac{a}{c}, \frac{b}{c})$ is a singular point of C_0 if and only if

$$P(\frac{a}{c}, \frac{b}{c}, 1) = 0 = \frac{\partial P}{\partial x}(\frac{a}{c}, \frac{b}{c}, 1) = \frac{\partial P}{\partial y}(\frac{a}{c}, \frac{b}{c}, 1).$$

Since $P(x, y, z)$ and its partial derivatives are homogeneous and $c \neq 0$, this holds true if and only if

$$P(a,b,c) = 0 = \frac{\partial P}{\partial x}(a,b,c) = \frac{\partial P}{\partial y}(a,b,c).$$

By Euler's relation above, this is equivalent to

$$P(a,b,c) = 0 = \frac{\partial P}{\partial x}(a,b,c) = \frac{\partial P}{\partial y}(a,b,c) = \frac{\partial P}{\partial z}(a,b,c),$$

and hence equivalent to $[a : b : c]$ being a singular point of C.

For the "moreover" part, the intersection of $\mathbb{C}^2$ (identified with $\{[x : y : z] \in \mathbb{P}^2_{\mathbb{C}} : z \neq 0\}$) and the projective tangent line

$$x\frac{\partial P}{\partial x}(a,b,c) + y\frac{\partial P}{\partial y}(a,b,c) + z\frac{\partial P}{\partial z}(a,b,c) = 0$$

is the line in $\mathbb{C}^2$ defined by

$$x\frac{\partial P}{\partial x}(a,b,c) + y\frac{\partial P}{\partial y}(a,b,c) + \frac{\partial P}{\partial z}(a,b,c) = 0.$$

Since all these partial derivatives are homogeneous of degree $m-1$, Euler's relation implies that this is precisely

$$(x-\frac{a}{c})\frac{\partial P}{\partial x}(\frac{a}{c},\frac{b}{c},1)+(y-\frac{b}{c})\frac{\partial P}{\partial y}(\frac{a}{c},\frac{b}{c},1)=0,$$

which is $T_{(a/c,b/c)}C_0 \subseteq \mathbb{P}^2_{\mathbb{C}}$. □

Example 2.6. *Consider the curve C of degree 3 defined by*

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

One can check that C is smooth if and only if $\lambda \neq 0, 1$. If $\lambda = 0$, then $[0:0:1]$ is a node. If $\lambda = 1$, then $[1:0:1]$ is a node.

Example 2.7. *Let us look at the following example. Let $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ be distinct numbers ($n \geq 4$). Consider the projective curve*

$$C = \{[x:y:z] \in \mathbb{P}^2_{\mathbb{C}} : y^2z^{n-2} = (x-\alpha_1 z)\cdots(x-\alpha_n z)\}.$$

Then $P(x,y,z) = y^2z^{n-2} - (x-\alpha_1 z)\cdots(x-\alpha_n z)$.

Let us look at the affine chart $\{[x:y:z] \in \mathbb{P}^2_{\mathbb{C}} : z \neq 0\}$, and the plane affine curve $C_0 = \{(x,y) \in \mathbb{C}^2 : P(x,y,1) = 0\}$ thus obtained. Then

$$\frac{\partial P(x,y,1)}{\partial x} = -\sum_{i=1}^{n}\prod_{j\neq i}(x-\alpha_j), \ \frac{\partial P(x,y,1)}{\partial y} = 2y.$$

It is then easy to check that C_0 has no singular points.

On the other hand, one can compute $C - C_0 = \{[0:1:0]\}$. To see whether this point is singular, we consider the affine chart $\{[x:y:z] \in \mathbb{P}^2_{\mathbb{C}} : y \neq 0\}$, and the plane affine curve $C_1 = \{(x,z) \in \mathbb{C}^2 : P(x,1,z) = 0\}$ thus obtained. In this chart $[0:1:0]$ becomes the origin $(0,0)$, and

$$\frac{\partial P(x,1,z)}{\partial x}(0,0) = \frac{\partial P(x,1,z)}{\partial z}(0,0) = 0.$$

Hence $[0:1:0]$ is a singular point of C (of multiplicity $n-2$).

Example 2.7 gives a good explanation why we need projective curves instead of affine curves: although the affine curve C_0 is smooth, its projectification C is NOT. When computing the genus, we need to study the singular points, which is $\{\infty\}$ for these curves. Worse, they are not nodes.

3. Lecture 3: Analytic theory of elliptic curves, I

3.1. **Revision on complex analysis.** Let us recall some basic facts in complex analysis. A function $f\colon U \to \mathbb{C}$ on an open subset $U \subseteq \mathbb{C}$ is called *holomorphic* if its derivative

$$f'(a) := \lim_{z \to a} \frac{f(z) - f(a)}{z - a}$$

exists at every $a \in U$. A function f is holomorphic on an open disc $\{z \in \mathbb{C} : |z - a| < r\}$ if and only if it can be expressed as a convergent power series

$$f(z) = \sum_{n \geq 0} c_n (z - a)^n.$$

A function $f\colon U \to \mathbb{C} \cup \{\infty\}$ is called *meromorphic* if its restriction to $U \setminus f^{-1}(\infty)$ is holomorphic and f can be expressed as $f(z) = g(z)/(z - a)^m$ near each $a \in f^{-1}(\infty)$ for some $m > 0$ and some $g(z)$ holomorphic in an open neighborhood of a with $g(a) \neq 0$. Thus near $a \in f^{-1}(\infty)$, we can express $f(z)$ as a Laurent series

$$f(z) = \sum_{n \geq -m} c_n (z - a)^n$$

with $c_{-m} \neq 0$. We call each $a \in f^{-1}(\infty)$ a *pole* of f, and call m the *order* of the pole. The *residue* of f at a, denoted by $\mathrm{Res}_a(f)$, is defined to be c_{-1}.

Theorem 3.1 (Cauchy's residue theorem). *Let γ be a contour in $\mathbb{C}$. Let f be a memomorphic function inside and on γ with no poles on γ. Let $a_1, \ldots, a_r$ be the poles of f inside γ. Then*

$$\int_\gamma f(z) dz = \pm 2\pi i \sum_{j=1}^{r} \mathrm{Res}_{a_j}(f).$$

A partial converse is the following theorem.

Theorem 3.2 (Morera's theorem). *Let $f\colon U \to \mathbb{C}$ be a continuous function on an open subset U of $\mathbb{C}$. If*

$$\int_\gamma f(z) dz = 0$$

for all closed piecewise-smooth paths γ in convex open subsets of U, then f is holomorphic on U.

The following theorem is useful for constructing holomorphic and memomorphic functions.

Theorem 3.3. *Let $(f_n\colon U \to \mathbb{C})_{n\geq 1}$ be a sequence of holomorphic functions on an open subset U of $\mathbb{C}$ converging uniformly to a function $f\colon U \to \mathbb{C}$. Then f is holomorphic on U, and the derivatives f_n' converge uniformly to f' on U.*

Corollary 3.4 (Weierstrass's M-test). *Let $(f_n\colon U \to \mathbb{C})_{n\geq 1}$ be a sequence of holomorphic functions on an open subset U of $\mathbb{C}$. Assume there exist positive real number M_n such that the series $\sum_{n\geq 1} M_n$ converges and that $|f_n(z)| \leq M_n$ for all $z \in U$. Then the series*

$$\sum_{n \geq 1} f_n(z)$$

converges uniformly on U to a holomorphic function $f(z)$ such that

$$f'(z) = \sum_{n\geq 1} f_n'(z).$$

Theorem 3.5 (Liouville's theorem)**.** *Any bounded holomorphic function on $\mathbb{C}$ is constant.*

3.2. **Weierstrass $\wp$-function.** Let ω_1 and ω_2 be non-zero complex numbers such that $\omega_2/\omega_1 \notin \mathbb{R}$. Set

$$\Lambda := \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subseteq \mathbb{C}.$$

Then Λ is a lattice in $\mathbb{C}$.

Proposition 3.6. *The series*

$$z^{-2} + \sum_{\omega\in\Lambda\setminus\{0\}} ((z-\omega)^{-2} - \omega^{-2})$$

converges to a meromorphic function on $\mathbb{C}$, which we denote by $\wp(z)$. Its derivative is

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

Before moving on to the proof, let us make the following definition.

Definition 3.7. *The function $\wp(z)$ constructed in Proposition 3.6 is called the* ***Weierstrass $\wp$-function*** *associated with Λ.*

The proof of the following elementary lemma is left as an exercise.

Lemma 3.8. *There exists a real number $\delta > 0$ such that $|x\omega_1 + y\omega_2| \geq \delta\sqrt{x^2+y^2}$ for all real numbers x and y.*

Proof of Proposition 3.6. For each $R > 0$, set

$$\Lambda_R := \{\omega \in \Lambda : |\omega| \leq 2R\}.$$

Then Λ_R is a finite set. Moreover, if $\omega \in \Lambda \setminus \Lambda_R$ and $|z| \leq R$, then $|z| \leq |\omega|/2$ and hence

$$\begin{aligned} |(z-\omega)^{-2} - \omega^{-2}| &= |z(2\omega - z)(z-\omega)^{-2}\omega^{-2}| \\ &\leq (5R|\omega|/2)4|\omega|^{-4} \\ &= 10R/|\omega|^3 \\ &\leq 10R\delta^{-3}(n^2+m^2)^{-3/2}, \end{aligned}$$

where the last inequality follows from Lemm 3.8 (in the last term we write $\omega = n\omega_1 + m\omega_2$). Notice that

$$\sum_{(n,m)\neq(0,0} (n^2+m^2)^{-3/2} = \sum_{k\geq 1} \sum_{\max\{|n|,|m|\}=k} (n^2+m^2)^{-3/2} \leq 8\sum_{k\geq 1} k^{-2} < \infty.$$

Hence by Weierstrass's M-test (Corollary 3.4), the series

$$\sum_{\omega\in\Lambda\setminus\Lambda_R} ((z-\omega)^{-2} - \omega^{-2})$$

converges absolutely uniformly on the disc $\{z \in \mathbb{C} : |z| \leq R\}$ to a holomorphic function $f(z)$ such that $f'(z) = \sum_{\omega\in\Lambda\setminus\Lambda_R} -2(z-\omega)^{-3}$. As this is true for any $R > 0$, we can conclude for the proposition. □

The following property of $\wp$ is important.

Proposition 3.9. *For all $z \in \mathbb{C}$ and all $\zeta \in \Lambda$, we have*

$$\wp(-z) = \wp(z) = \wp(z + \zeta).$$

Proof. We have

$$\wp(-z) = z^{-2} + \sum_{\omega\in\Lambda\setminus\{0\}} ((z+\omega)^{-2} - \omega^{-2}) = z^{-2} + \sum_{-\omega\in\Lambda\setminus\{0\}} ((z-(-\omega))^{-2} - (-\omega)^{-2}) = \wp(z)$$

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

We have

$$\wp'(z+\zeta) = -2\sum_{\omega\in\Lambda}(z+\zeta-\omega)^{-3} = -2\sum_{\zeta-\omega\in\Lambda}(z+\zeta-\omega)^{-3} = \wp'(z)$$

for all $z \in \mathbb{C}$. Hence the function $\wp(z+\zeta) - \wp(z)$, as a function in z, is constant. In particular

$$\wp(z+\zeta) - \wp(z) = \wp(\zeta/2) - \wp(-\zeta/2) = 0$$

for all $z \in \mathbb{C}$. We are done. □

Definition 3.10. *A function $f : \mathbb{C} \to \mathbb{C}$ is called **doubly periodic** with period lattice Λ if $f(z+\zeta) = f(z)$ for all $z \in \mathbb{C}$ and all $\zeta \in \Lambda$.*

An example of doubly periodic function is $\wp$.

Lemma 3.11. *Any holomorphic doubly periodic function f on $\mathbb{C}$ is constant.*

Proof. The function f is bounded on the compact set $\Delta := \{s\omega_1 + t\omega_2 : s, t \in [0,1]\}$. Double periodicity then implies that f is bounded on $\mathbb{C}$. Hence f is constant by Liouville's theorem (Theorem 3.5). □

We will use this lemma to prove the following theorem.

Theorem 3.12. *Set $g_2 = g_2(\Lambda) = 60\sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-4}$ and $g_3 = g_3(\Lambda) = 140\sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-6}$. Then*

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

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

Proof. The function

$$\wp(z) - z^{-2} = \sum_{\omega\in\Lambda\setminus\{0\}} ((z-\omega)^{-2} - \omega^{-2})$$

vanishes at 0 and is holomorphic near 0. Moreover $\wp(-z) - (-z)^{-2} = \wp(z) - z^2$, so the Taylor expansion of this function at 0 has only even powers of z. Hence

$$\wp(z) = z^{-2} + \lambda z^2 + \mu z^4 + z^6 h(z)$$

for some holomorphic function $h(z)$ near 0. Thus

$$\wp'(z) = -2z^{-3} + 2\lambda z + 4\mu z^3 + 6z^5 h(z) + z^6 h'(z).$$

Moreover since 2λ and 24μ are the second and fourth derivatives at 0 of the function $\sum_{\omega\in\Lambda\setminus\{0\}}((z-\omega)^{-2} - \omega^{-2})$, we can compute $g_2 = 20\lambda$ and $g_3 = 28\mu$.

Consider the function

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

Then the above formulae imply $k(0) = 0$ and that k is holomorphic near 0. Next $k(z)$ is holomorphic on $\mathbb{C} \setminus \Lambda$ because both $\wp(z)$ and $\wp'(z)$ are. But $k(z)$ is also holomorphic near each $\zeta \in \Lambda$ because k is holomorphic near 0, $\wp(z+\zeta) = \wp(z)$ and $\wp'(z+\zeta) = \wp'(z)$ for all $z \in \mathbb{C}$ and $\zeta \in \Lambda$. So $k(z)$ is a holomorphic doubly periodic function on $\mathbb{C}$. Hence $k(z) = k(0) = 0$ for all $z \in \mathbb{C}$. We are done. □

4. Lecture 4: Analytic theory of elliptic curves, II

We use the same conventions and notations as in the last lecture.

4.1. **Weierstrass $\wp$-function continued.**

Last time we have seen that $\wp$ and $\wp'$ satisfying an algebraic equation. Today we start by showing that all solutions of this algebraic equation are values of $\wp$ and $\wp'$.

We start by the following observation. Let f be a meromorphic function. Then f'/f is meromorphic on $\mathbb{C}$, and all poles of f'/f are simple (*i.e.* multiplicity 1). Moreover, the poles of f'/f are precisely

- the poles of f (say of multiplicity m), where the residue of f'/f is $-m$;
- the zeros of f (say of multiplicity m), where the residue of f'/f is m.

Thus Cauchy's residue theorem implies the follows: If $\gamma \subseteq \mathbb{C}$ is a contour not passing through any zero or pole of f, then

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}dz = Z - P \tag{4.1}$$

with Z and P the numbers of zeros and poles of f inside γ, counted with multiplicity.

Proposition 4.1. *We have $\wp(\mathbb{C}\backslash\Lambda) = \mathbb{C}$. Moreover, $\wp(z) = \wp(w)$ if and only if $w \in \Lambda \pm z$.*

Proof. Let $c \in \mathbb{C}$, and define $f(z) = \wp(z) - c$. Then f is a meromorphic function on $\mathbb{C}$. Take γ to be the boundary of the parallelogram

$$\Delta(a) = \{a + s\omega_1 + t\omega_2 : s, t, \in [0, 1]\}$$

where a is chosen such that γ does not pass through any zeros or poles of f. In particular, there is exactly one lattice point $\zeta \in \Lambda$ inside γ. The double periodicity of f yields

$$\int_\gamma \frac{f'(z)}{f(z)}dz = 0$$

since the integrals along opposite sides of $\Delta(a)$ cancel out. Hence $Z = P$ with the notations from (4.1). But f has poles of multiplicity 2 at all lattice points (as $\wp$) and no other poles. So $Z = 2$, and hence there exists some $w_0 \in \Delta(a)$ such that $f(w_0) = 0$. Hence $\wp(w_0) = c$. Since c is arbitrary, we get that $\wp(\mathbb{C} \setminus \Lambda) = \mathbb{C}$.

Since $\wp$ is even and doubly periodic, we have

$$\wp(z) = \wp(w_0) = c \quad \text{for all } z \in \Lambda \pm w_0.$$

Conversely assume $w_1 \in (\Lambda - \omega_0) \cap \Delta(a)$ such that $\wp(w_1) = \wp(w_0) = c$. If $w_0 \neq w_1$, then there are no other zeros because $Z = 2$. If $w_0 = w_1$, then we wish to show that w_0 is a zero of multiplicity 2, *i.e.* $f'(w_0) = 0$, or equivalently $\wp'(w_0) = 0$. Now $w_0 = w_1$ implies $\Lambda + w_0 = \Lambda - w_0$. Since $\wp'(z)$ is an odd doubly periodic function, we have

$$\wp'(w_0) = -\wp'(-w_0) = -\wp'(w_0).$$

Hence we are done. □

4.2. Algebraic curve of degree 3 associated with Λ.

Definition 4.2. *Let $E_\Lambda \subseteq \mathbb{P}^2_{\mathbb{C}}$ be the projective curve defined by the polynomial*

$$Q_\Lambda := Y^2Z - (4X^3 - g_2XZ^2 - g_3Z^3)$$

where $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$.

Proposition 4.3. *Let*

$$\alpha = \wp(\omega_1/2),\ \beta = \wp(\omega_2/2),\ \gamma = \wp((\omega_1+\omega_2)/2).$$

Then they are distinct complex numbers, and the polynomial Q_Λ from Definition 4.2 equals

$$Y^2Z - 4(X-\alpha Z)(X-\beta Z)(X-\gamma Z).$$

As a consequence, the cubic curve E_Λ from Definition 4.2 is smooth.

Proof. By the second part of Proposition 4.1, α, β and γ are distinct.

We have

$$\wp'(\omega_1/2) = \wp'(\omega_1/2 - \omega_1) = \wp'(-\omega_1/2) = -\wp'(\omega_1/2).$$

So $\wp'(\omega_1/2) = 0$. Thus

$$4\alpha^3 - g_2\alpha - g_3 = \wp'(\omega_1/2)^2 = 0.$$

So α is a root of the polynomial $4x^3 - g_2x - g_3$. Similarly, β and γ are roots of $4x^3 - g_2x - g_3$. So

$$4x^3 - g_2x - g_3 = 4(x-\alpha)(x-\beta)(x-\gamma)$$

since α, β, and γ are distinct. We are done. □

Now we view $\mathbb{C}/\Lambda$ as a torus. Then we have the following map by Theorem 3.12.

$$\begin{array}{rccl} u\colon & \mathbb{C}/\Lambda & \to & E_\Lambda \subseteq \mathbb{P}^2_{\mathbb{C}} \\ & \Lambda + z & \mapsto & \begin{cases} [\wp(z) : \wp'(z) : 1] \text{ if } z \notin \Lambda \\ [0:1:0] \text{ if } z \in \Lambda. \end{cases} \end{array} \tag{4.2}$$

Proposition 4.4. *The map u is a homeomorphism.*

Proof. We need to show that u is a bijection, and that both u and u^{-1} are continuous.

Injectivity: Assume $z, w \in \mathbb{C} \setminus \Lambda$ such that $u(z) = u(w)$. Then $\wp(z) = \wp(w)$, and hence $z \in \Lambda \pm w$ by Proposition 4.1. Suppose $z \in \Lambda - w$. Then since $\wp'$ is odd doubly periodic, we have $\wp'(z) = -\wp'(w)$. But $u(z) = u(w)$ and hence $\wp'(z) = \wp'(w)$. So we have $\wp'(z) = \wp'(w) = 0$. But then $\wp(w)$ equals $\wp(\omega_1/2)$, $\wp(\omega_2/2)$, or $\wp((\omega_1+\omega_2)/2)$ by the proof of Proposition 4.3. So $w \in \frac{1}{2}\Lambda$ again by Proposition 4.1, and therefore $\Lambda + w = \Lambda - w$. Thus $z \in \Lambda + w$ always holds true. We have established the injectivity of u.

Surjectivity: Let $[a:b:c] \in E_\Lambda$. If $c = 0$ then we must have $[a:b:c] = [0:1:0]$ and hence is in the image of u by definition. From now on we may assume $c = 1$. By the first part of Proposition 4.1, $\wp(z) = a$ for some $z \in \mathbb{C}$. Hence

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 = 4a^3 - g_2a - g_3 = b^2,$$

and so $\wp'(z) = \pm b$. Thus $[a:b:1]$ is either $u(\Lambda + z)$ or $u(\Lambda - z)$. We have established the surjectivity of u.

Continuity: Since $\wp$ and $\wp'$ are holomorphic on $\mathbb{C} \setminus \Lambda$, we know that u is continuous outside $\Lambda + 0$. Near 0 we can write

$$\wp(z) = g(z)/z^2 \quad \text{and} \quad \wp'(z) = h(z)/z^3$$

for some holomorphic functions $g(z)$ and $h(z)$ near 0 such that $g(0) \neq 0$ and $h(0) \neq 0$; this is because $\wp$ has pole at 0 of multiplicity 2 and $\wp'$ has pole at 0 of multiplicity 3. Thus in a neighborhood V of 0, we have

$$u(\Lambda + z) = [\wp(z) : \wp'(z) : 1] = [zg(z) : h(z) : z^3]$$

for each $z \in V \setminus \{0\}$, and thus $u(\Lambda + z) \to [0 : 1 : 0]$ as $z \to 0$. Hence u is continuous at $\Lambda + 0$. This establishes the continuity of u.

Now we can conclude that u is a homeomorphism by the following fact in topology: any continuous bijection from a compact space to a Hausdorff space is a homeomorphism. □

The actual goal is to prove the following theorem.

Theorem 4.5. *The map u is bi-holomorphic.*

Compared with Proposition 4.4, Theorem 4.5 furthermore says that both u and u^{-1} are holomorphic.