I. The Land of Algebraic Geometry

I.1. Complex Tori as Elliptic Curves

Recall I.1.1

A complex torus is $\mathbb{C}/\Lambda$ where Λ is a lattice with $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$. Goal is to relate this to a cubic curve.

A meromorphic function is a holomorphic map $f : \mathbb{C}/\Lambda \to \widehat{\mathbb{C}}$. Put another way, this is a meromorphic Λ-periodic map $\mathbb{C} \to \mathbb{C}$ (or holomorphic $\mathbb{C} \to \widehat{\mathbb{C}}$).

The Weierstrass $\wp_\Lambda$ function is given by

$$\wp_\Lambda(z) \coloneqq \frac{1}{z^2} + \sum_{\omega\in\Lambda}{}' \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

, where $z \in \mathbb{C} \setminus \Lambda$ and $\sum'$ means to exclude $\frac{1}{0}$.

The summand is $\sim \frac{z}{\omega^3}$, which can be used to show $\wp_\Lambda(z)$ converges absolutely and uniformly on all compact subsets away from Λ. Thus $\wp_\Lambda$ is holomorphic at all points $\mathbb{C} \setminus \Lambda$.

We can of course compute for $z \in \mathbb{C} \setminus \Lambda$ that

$$\wp'_\Lambda(z) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-w)^3}.$$

It is clear that $\wp'_\Lambda(z)$ is in fact Λ-periodic.

Exercise I.1.2 (1.4.2)

Show that $\wp_\Lambda(z)$ must in fact be periodic.

Fact: The field of all meromorphic functions on $\mathbb{C}/\Lambda$ is given by $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$ (that is rational expressions in $\wp_\Lambda, \wp'_\Lambda$).

Recall I.1.3

We have the Eisenstein series

$$G_k(\tau) \coloneqq \sum_{c,d\in\mathbb{Z}}{}' \frac{1}{(c\tau+d)^k},$$

which is sum of reciprocals of k-th powers over a lattice $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$.

This can generalize to a function of a lattice

$$G_k(\Lambda) \coloneqq \sum_{\omega\in\Lambda}{}' \frac{1}{\omega^k}.$$

Usually we will take $k > 2$ to guarantee good convergence properties. Also if k is odd $G_k(\Lambda) \equiv 0$, so we'll restrict to k even.

There is then an identity for every $m \in \mathbb{C}^\times$,

$$G_k(m\Lambda) = m^{-k}G_k(\Lambda).$$

Theorem I.1.1 (1.4.1)

The Laurent expansion of $\wp_\Lambda$ at $z = 0$ (i.e., on a tiny punctured disk about $z = 0$) is given by

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{n=2 \\ n \text{ even}}}^{\infty} (n+1)G_{n+2}(\Lambda)z^n.$$

Furthermore, we have the following relation

$$(\wp'_\Lambda(z))^2 = 4(\wp_\Lambda(z))^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda),$$

where $g_2(\Lambda) := 60G_4(\Lambda)$ and $g_3(\Lambda) := 140G_6(\Lambda)$.

Proof. For the first piece, recall

$$\wp_\Lambda(z) = \frac{1}{z^2} + {\sum_{\omega\in\Lambda}}' \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

We see that

$$\begin{aligned}\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right) \\ &= \frac{1}{\omega^2}\left(\left(1 + \frac{z}{\omega} + \frac{z^2}{\omega^2} + \cdots\right)^2 - 1\right),\end{aligned}$$

since $z/\omega < 1$ for z sufficiently small and $\omega \in \Lambda$ nonzero (here using that Λ is discrete). In fact, upon simplifying, we see that

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^n}.$$

We now have that

$$\begin{aligned}\wp_\Lambda(z) &= \frac{1}{z^2} + {\sum_{\omega\in\Lambda}}' \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}. \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}\left({\sum_{\omega\in\Lambda}}' \frac{1}{\omega^{n+2}}\right)(n+1)z^n,\end{aligned}$$

which is exactly what we want.

For the second part, we write

$$\begin{aligned}\wp_\Lambda(z) &= \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + O(z^6) \\ \wp'_\Lambda(z) &= -\frac{2}{z^3} + 6G_4(\Lambda)z + 20G_6(\Lambda)z^3 + O(z^5).\end{aligned}$$

Both $(\wp'_\Lambda(z))^2$ and $4(\wp_\Lambda(z))^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda)$ look like

$$\frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda) + O(z^2).$$

Thus the difference of these two is a holomorphic function with value 0 at 0. Furthermore it is Λ-periodic, so by complex analysis (i.e., Liousville's theorem) it must be constant.

Proposition I.1.2

The cubic equation

$$4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

has distinct roots. This is equivalent to $g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0$ (the discriminant), and equivalently this means the curve $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ is nonsingular.

Proof. In 1.4.1, not difficult to prove (just compute with an explicit lattice). 

This is a cubic equation coming from a lattice on $\mathbb{C}$. This is our relation to elliptic curves! It gives us a map

$$\begin{aligned} \mathbb{C} \setminus \Lambda &\to \left\{(x,y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)\right\} \\ z &\mapsto (\wp_\Lambda(z), \wp'_\Lambda(z)). \end{aligned}$$

If we mod out by the lattice, this is a bijection (this is a simple computation). How does this compare to the torus $\mathbb{C}/\Lambda$? Well we're missing a point! By mapping Λ/Λ to some point at ∞, we get a bijection

$$\mathbb{C}/\Lambda \to \text{an "elliptic curve" } E_\Lambda.$$

We should see how the group law on the torus translates to E_Λ! We'll say zero is the point at ∞ as $\mathcal{O}_{E_\Lambda}$.

Then in fact "colinear points sum to zero" (this is not obvious but it is a computation). Namely if $z_1, z_2, z_3 \in E_\Lambda$ lie on the same line then $z_1 + z_2 + z_3 = \mathcal{O}$. When $z_1 = z_2$, we should take a line tangent to z_1! It turns out that $P = (x, y)$ gives $-P = (x, -y)$.

We actually have every elliptic curve $y^2 = 4x^3 - a_2x - a_3$ where $a_2^3 - 27a_3^2 \neq 0$ comes from a lattice. One can actually very explicitly write it down!

How should we consider isomorphisms of elliptic curves? Well consider $m \in \mathbb{C}^\times$, then

$$(x, y) \mapsto (m^{-2}x, m^{-3}y)$$

maps

$$\{y^2 = 4x^3 - a_2x - a_3\} \xrightarrow{\sim} \{y^2 = 4x^3 - m^{-4}a_2x - m^{-6}a_3\}.$$

This map comes from an isomorphism of tori, namely $z + \Lambda \mapsto mz + m\Lambda$.

Corollary I.1.3

The discriminant function $\Delta : \mathcal{H} \to \mathbb{C}$, which we recall is

$$\Delta(\tau) = (g_2(\tau))^3 - 27(g_2(\tau))^2$$

is in fact never zero.

Proof. Up to some multiple, $\Delta(\tau)$ is in fact the discriminant of an elliptic curve E_{Λ_τ} (which is nonsingular). 

I.2. **Elliptic curves as algebraic curves**

This is section 7.1 in the book. Let k be a field of characteristic 0 and let $\overline{k}$ be the algebraic closure.

Definition I.2.1

A Weierstrass equation over k is

$$y^2 = 4x^3 - a_2x - a_3$$

for $a_2, a_3 \in k$. The discriminant is $\Delta = a_2^3 - 27a_3^2 \in k$. If $\Delta \neq 0$, then we define the j-invariant to be $j = \frac{1728a_2^3}{\Delta} \in k$. We call

$$E(x, y) = y^2 - 4x^3 + a_2x + a_3.$$

Definition I.2.2

If we have a Weierstrass equation with $\Delta \neq 0$, we say E is nonsingular and we call

$$\mathcal{E} = \{(x, y) \in \overline{k}^2 \mid E(x, y) = 0\} \cup \{\infty\},$$

an elliptic curve over k, which we can think of as a variety which is a subset of the projective plane $\mathbb{P}^2(\overline{k})$.

If L/k is any extension we write $\mathcal{E}(L)$ for $\mathcal{E} \cap \mathbb{P}^2(L^2)$.

Let L/k be Galois and $\mathcal{E}/k$ to be an elliptic curve over k. Furthermore let $\sigma \in \mathrm{Gal}(L/k)$, and for $x \in L$ write $x^\sigma := \sigma(x)$. Then since $E(x, y) \in k[x, y]$ we have

$$E(x^\sigma, y^\sigma) = E(x, y)^\sigma$$

for $x, y \in L$. Thus there is a group action $\mathrm{Gal}(L/k)$ on $\mathcal{E}(L)$.

This actually can give you representations of a Galois group for certain curves/points on those curves. There is a group law on $\mathcal{E}$ where $P + Q + R = \mathcal{O}_\mathcal{E}$ if and only if $P, Q, R \in \mathcal{E}$ are colinear (over k). This also gives a group structure on $\mathcal{E}(L)$ for any $k \subseteq L \subseteq \overline{k}$. Namely we can just write down an equation for the point $P + Q$ and it's an equation over k.

Thus $\mathrm{Gal}(L/k)$ is acting on a group! It acts in a nice way, $\sigma \in \mathrm{Gal}(L/k)$ gives a group homomorphism $\mathcal{E}(L) \to \mathcal{E}(L)$, since the equation for $P + Q$ is an equation over k (and hence is carried over nicely by σ).

Theorem I.2.1 (Bezout's Theorem)

If C_1, C_2 are two curves in x, y of degree d_1, d_2 then they meet in d_1d_2 points in $\mathbb{P}^2(\overline{k})$, where we count with multiplicity.

Suppose $k = \mathbb{Q}$, so $\mathcal{E}/\mathbb{Q}$ is an elliptic curve. What can we say about the structure of $\mathcal{E}(\mathbb{Q})$. This is an abelian group. But what is it? It turns out $\mathcal{E}(\mathbb{Q})$ is finitely generated, and this result is called Mordell's Theorem. It is quite difficult to prove

Author's Note: I may include notes about the Mordell-Weil Theorem as an appendix from a UVA (Ono's) REU mini-course

The rank of $\mathcal{E}(\mathbb{Q})$ is often called the rank of an elliptic curve.