Lecture 17

Recall. last time we defined, for $\Lambda \subset \mathbb{C}$, rank 2 abelian gp.

$$\wp(z) = z^{-2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left((z-\lambda)^{-2} - \lambda^{-2} \right)$$ Weierstrass' $\wp$-function.

and showed that this series converges uniformly and hence defines a meromorphic function $\wp : \mathbb{C} \dashrightarrow \mathbb{C}$ which is doubly-periodic with period lattice Λ. $\wp$ has double pole at each $\lambda \in \Lambda$.

Hence, by the fundamental theorem for elliptic functions.

$\forall \alpha \in \mathbb{C}$, $\wp(z) = \alpha$ has exactly 2 solutions modulo Λ.

§1. Differential equation for $\wp(z)$.

Consider the Taylor series expansion of $\wp(z) - z^{-2}$ near 0. It is an even function, vanishing at 0, so

$$\wp(z) - z^{-2} = c_2 z^2 + c_4 z^4 + \dots$$

where

$$c_{2n} = \frac{1}{(2n)!} \frac{d^{2n}}{dz^{2n}} \left(\sum_{\lambda \in \Lambda \setminus \{0\}} (z-\lambda)^{-2} - \lambda^{-2} \right) \Bigg|_{z=0}$$

$$= (2n+1) \sum_{\lambda \in \Lambda \setminus \{0\}} \lambda^{-2n-2}$$

$$\Rightarrow \quad \wp(z) = z^{-2} + c_2 z^2 + c_4 z^4 + \cdots$$

$$\wp'(z) = -2 z^{-3} + 2 c_2 z + 4 c_4 z^3 + \cdots$$

So, $\wp'(z)^2 = 4 z^{-6} - 8 c_2 z^{-2} - 16 c_4 + \cdots$ (here, $\cdots$ contains terms vanishing at 0)

$$\wp(z)^3 = z^{-6} + 3 c_2 z^{-2} + 3 c_4 + \cdots$$

$$\Rightarrow \quad \wp'(z)^2 - 4\wp(z)^3 = -20 c_2 z^{-2} - 28 c_4 + \cdots$$

So, $\wp'(z)^2 - 4\wp(z)^3 + 20 c_2 \wp(z) + 28 c_4$ vanishes at 0, in particular it is holomorphic and doubly-periodic, hence a constant $= 0$.

$$\boxed{\wp'(z)^2 = 4\wp(z)^3 - g_2 \wp(z) - g_3}$$ where

$$g_2 = 20 c_2 = 60 \sum_{\lambda \in \Lambda^\circ} \lambda^{-4} \qquad g_3 = 28 c_4 = 140 \sum_{\lambda \in \Lambda^\circ} \lambda^{-6}.$$

Exercise - Show that $c_{2n} = (2n+1) \sum_{\lambda \in \Lambda^\circ} \lambda^{-2n-2}$ $(n \geq 3)$ can be written in terms of g_2 and g_3. e.g.,

$$c_6 = \frac{g_2^2}{2^4 \cdot 3 \cdot 5^2} \qquad c_8 = \frac{3 g_2 g_3}{2^4 \cdot 5 \cdot 7 \cdot 11} \qquad \cdots$$

§2. Addition rule for $\wp$-function.

If $u+v+w=0 \pmod{\Lambda}$ then
$$\det\begin{bmatrix} \wp(u) & \wp'(u) & 1 \\ \wp(v) & \wp'(v) & 1 \\ \wp(w) & \wp'(w) & 1 \end{bmatrix} = 0.$$

i.e. $(\wp(u), \wp'(u)) \ldots$ are collinear.

Proof. Assume $(\wp(u), \wp'(u)) \neq (\wp(v), \wp'(v))$

Let A, B be such that
$$\wp'(u) = A\,\wp(u) + B$$
$$\wp'(v) = A\,\wp(v) + B$$

$\Big($ so, $A = \dfrac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}$ and $B = \wp'(u) - \wp(u)\cdot\left(\dfrac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\right)$
$$= \frac{-\wp'(u)\,\wp(v) + \wp(u)\,\wp'(v)}{\wp(u) - \wp(v)}\Big)$$

$\Rightarrow$ $\wp'(z) - A\,\wp(z) - B$, as a doubly-periodic fn. of z has at least 2 solns. namely u and v. But it has order 3 pole at 0, so, it must have 3 solutions which add up to 0 $\pmod{\Lambda}$. That is, $z = -u-v$ also solves $\wp'(z) - A\,\wp(z) - B = 0$. The theorem is proved. $\square$

Cor. $$\wp(x+y) = \frac{1}{4}\left(\frac{\wp'(x)-\wp'(y)}{\wp(x)-\wp(y)}\right)^2 - \wp(x) - \wp(y).$$

$$\wp(2x) = \frac{1}{4}\left(\frac{\wp''(x)}{\wp'(x)}\right)^2 - 2\wp(x).$$

Proof of the first identity: (second left as an exercise).

Let A, B be as in the theorem above, so that

$\wp'(z) - A\wp(z) - B = 0$ has 3 solns. x, y and $-x-y$.

$$\Rightarrow \quad \wp'(z)^2 - (A\wp(z)+B)^2$$
$$= 4\wp(z)^3 - A^2\wp(z)^2 - (2AB+g_2)\wp(z) - (B^2+g_3) = 0$$

has 3 roots: $\wp(x)$, $\wp(y)$, $\wp(x+y)$.

$$\Rightarrow \quad \wp(x+y) + \wp(x) + \wp(y) = \frac{1}{4}A^2$$

(sum of roots = $(-1)\cdot$ coeff of subleading term for monic poly. $T^3 - \frac{A^2}{4}T^2 - \cdots = 0$)

□

§3. Corollary - addition rule for elliptic curves.

Weierstrass' $\wp$-function defines a map

$$\begin{aligned} \mathbb{C} &\longrightarrow \{\text{Zero locus of } ZY^2 = 4X^3 - g_2XZ^2 - g_3Z^3\}/\mathbb{C}^\times \subseteq \mathbb{P}^2 \\ (\mathrm{mod}\,\Lambda)\quad 0 \neq z &\longmapsto (\wp(z), \wp'(z), 1) \\ 0 &\longmapsto (0, 1, 0) \end{aligned}$$

and hence identifies

$$\mathbb{C}/\Lambda \longleftrightarrow \text{Elliptic curve in } \mathbb{P}^2$$

smooth alg. curve of deg. 3 in 3 variables.

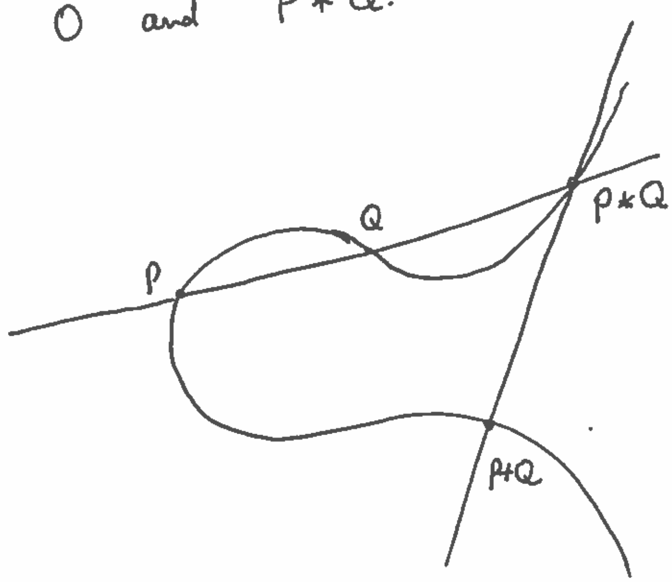
The group operation on $\mathbb{C}/\Lambda$ (addition) carried over to elliptic curves, say C, has the following geometric interpretation (from Thm §2 above). Let $O = (0,1,0)$ "pt. at ∞".

Given P, Q on C; let ℓ be the line joining P and Q (or tangent to C at P, if $P = Q$)

As C has degree 3, $\ell \cap C = \{P, Q, \underbrace{P * Q}_{\text{another point on } C}\}$.

Let ℓ_∞ be the line joining O and $P * Q$.

$P + Q$ is the point of intersection of ℓ_∞ and C, other than O and $P * Q$.



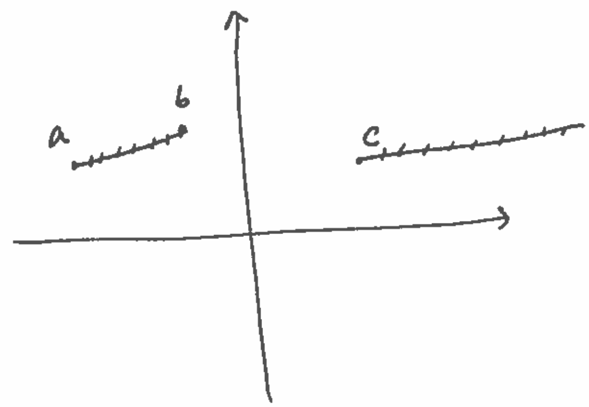
§4. Remark on Riemann Surface construction.

Let $y^2 = f(x)$ where $f(x) = (x-a)(x-b)(x-c)$
a, b, c distinct

For $z_0 \in \mathbb{C} \setminus \{a,b,c\}$, we can solve for y in 2 different ways

$$y \in (z-z_0)^{1/2}\, \mathbb{C}[[z-z_0]]$$

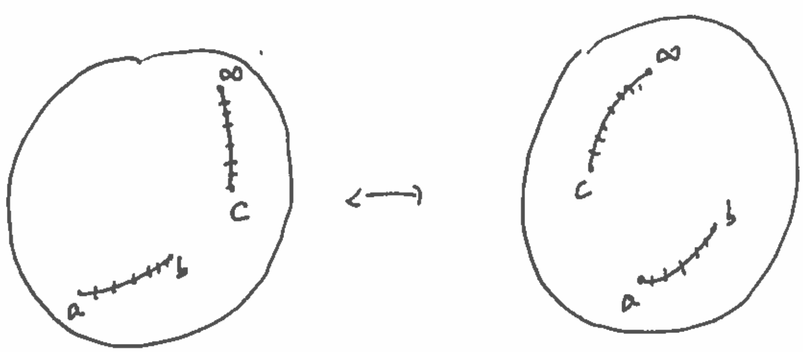
s.t. $y^2 = f(z)$ for all z near z_0.



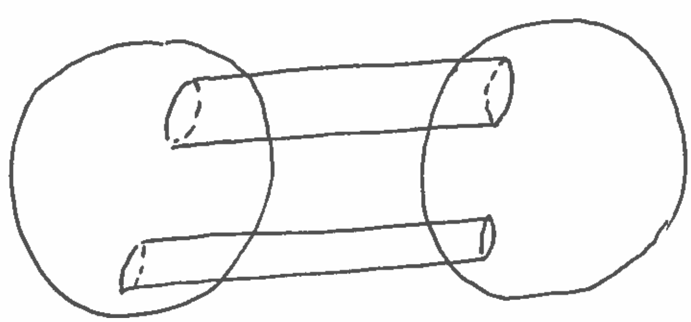
Cut for log - determines a single-valued $\sqrt{f(x)}$

Let Σ be the Riemann surface associated to this germ., near z_0.

Geometrically Σ is obtained by gluing 2 copies of the cut sphere



=



=

§5. Let us pick a system of generators $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$

As $\wp'(z)$ is Λ-periodic and odd, we get, for any $\lambda \in \mathbb{C}$ s.t. $2\lambda \in \Lambda$:

$$\wp'(\lambda) = \wp'(-\lambda+2\lambda) = \wp'(-\lambda)$$
$$= -\wp'(\lambda)$$

$$\Rightarrow \wp'(\lambda) = 0.$$

Hence $\wp'(z) = 0$ at $z = \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$. (These are all the zeroes of $\wp'$, since its degree is 3)

<u>Lemma</u> - $e_1 = \wp\left(\frac{\omega_1}{2}\right)$, $e_2 = \wp\left(\frac{\omega_2}{2}\right)$, $e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$

are distinct roots of $4T^3 - g_2 T - g_3 = 0$.

<u>Proof</u> - It only remains to see that e_1, e_2, e_3 are distinct.

Assume, for the sake of a contradiction, that $e_1 = e_2$.

Then $f(z) = \wp(z) - e_1 = 0$ has 2 distinct roots at $\frac{\omega_1}{2}, \frac{\omega_2}{2}$ each of order ≥ 2 since $f'\left(\frac{\omega_1}{2}\right) = f'\left(\frac{\omega_2}{2}\right) = 0$. This contradicts that f has degree 2. □

§6. Discriminant $\Delta = g_2^3 - 27 g_3^2 \neq 0$ by Lemma above.

<u>Ex.</u> Verify that $g_2^3 - 27 g_3^2 = (e_1-e_2)^2 (e_2-e_3)^2 (e_1-e_3)^2$.