

Théorème :  $\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda(z), \wp'_\Lambda(z))$

c'est-à-dire toute fonction elliptique est de la forme

$$f = \frac{P(\wp_\Lambda, \wp'_\Lambda)}{Q(\wp_\Lambda, \wp'_\Lambda)} \quad \text{pour } P, Q \in \mathbb{C}[X, Y] \\ Q \neq 0$$

Démonstration : Soit  $f \in \mathbb{C}(\Lambda)$ . Il suffit de démontrer le théorème pour  $f$  paire.

En effet,

$$f(z) = \underbrace{\frac{f(z) + f(-z)}{2}}_{\text{elliptique paire}} + \underbrace{\frac{f(z) - f(-z)}{2}}_{\text{elliptique impaire}}$$

et si  $f$  est impaire, alors  $\wp' f$  est paire.

Pour  $f$  paire,  $\text{ord}_x(f) = \text{ord}_{-x}(f)$  et

si  $2x \in \Lambda$ , alors  $\text{ord}_x(f)$  est pair.

(En effet,  $f(z) = f(-z)$  implique

$$f^{(i)}(z) = (-1)^i f^{(i)}(-z).$$

⑥

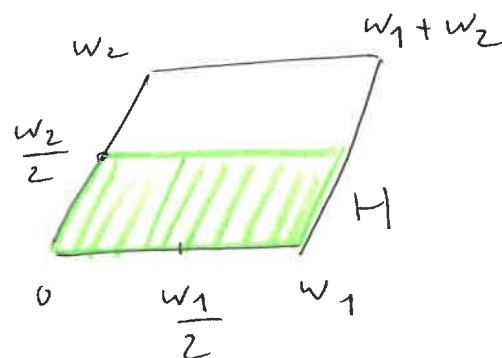
Si  $2x \in \Lambda$ , alors

$$f^{(i)}(x) = (-1)^i f^{(i)}(\underbrace{-x}_{x-2x}) = (-1)^i f^{(i)}(x),$$

donc  $f^{(i)}(x) = 0$  pour  $i$  impair

Soit  $D$  un domaine fondamental et  $H$  comme dans le dessin.

Considérons la fonction



$$g(z) = \prod_{w \in H \setminus \{0\}} (\wp_{\Lambda}(z) - \wp_{\Lambda}(w))^{n_w}$$

$$\text{où } n_w = \begin{cases} \text{ord}_w(f) & \text{si } 2w \notin \Lambda \\ \frac{1}{2} \text{ord}_w(f) & \text{si } 2w \in \Lambda \end{cases}$$

les fonctions  $f$  et  $g$  satisfont

$$\text{ord}_w(f) = \text{ord}_w(g) \quad \text{pour tout } w \in H \setminus \{0\}$$

puisque  $\wp_{\Lambda}(z) - \wp_{\Lambda}(w)$  a des zéros  $\left| \begin{array}{l} \text{double } 2w \in \Lambda \\ \text{simple } 2w \notin \Lambda \end{array} \right.$  en  $w$  et  $-w$  et une pôle double en 0.

En utilisant la relation  $\sum_{w \in D} \text{ord}_w(f) = 0$

on en déduit que c'est aussi vrai à l'origine:

$$\text{ord}_0(f) = \text{ord}_0(g)$$

Il s'ensuit que

$\frac{f(z)}{g(z)}$  est elliptique holomorphe,

donc constante, c'est-à-dire

$$f \in \mathbb{C}(\mathcal{P}_\Lambda(z))$$

□

### ③ PLONGEMENT PROJECTIF

Calculons les coefficients de la fonction  $\mathcal{P}_\Lambda(z)$  autour de  $z=0$ . Pour  $|z| < |w|$  avec  $w \neq 0$ , on a:

$$\begin{aligned} \frac{1}{(z-w)^2} - \frac{1}{w^2} &= \frac{1}{w^2} \left[ \frac{1}{\left(1 - \frac{z}{w}\right)^2} - 1 \right] \\ &= \left[ \sum_{n=1}^{\infty} (n+1) \left(\frac{z}{w}\right)^n \right] \cdot \frac{1}{w^2} \end{aligned}$$

en utilisant l'identité  $\frac{1}{(1-t)^2} = \sum_{n=1}^{\infty} n t^{n-1}$ .

on obtient alors:

$$\begin{aligned}
 j_{\Lambda}'(z) &= \frac{1}{z^2} + \sum_{n=1}^{\infty} \left( \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{n+1}{w^{n+2}} \right) z^n \\
 &= \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}
 \end{aligned}$$

car les séries d'Eisenstein sont nulles si l'exposant est impair.

Proposition: Pour tout  $z \in \mathbb{C} \setminus \Lambda$ , on a

$$j_{\Lambda}'(z)^2 = 4 j_{\Lambda}(z)^3 - \underbrace{60 G_4(\Lambda)}_{g_2} j_{\Lambda}(z) - \underbrace{140 G_6(\Lambda)}_{g_3}$$

Démonstration: c'est un calcul autour de  $z=0$ , on utilise les développements

$$j(z) = \frac{1}{z^2} + 3 G_4 z^2 + \dots$$

$$j(z)^3 = \frac{1}{z^6} + \frac{9 G_4}{z^2} + 15 G_6 + \dots$$

$$j'(z)^2 = \frac{4}{z^6} - 24 \frac{G_4}{z^2} - 80 G_6 + \dots$$

On voit ainsi si que

$$j_{\Lambda}'(z)^2 - 4j_{\Lambda}(z)^3 + 60g_4(\Lambda)j_{\Lambda}(z) + 140g_6(\Lambda) = O(z^2)$$

C'est donc une fonction elliptique holomorphe, donc constante, donc nulle car elle s'annule en  $z=0$ .  $\square$

on a ainsi obtenu une application holomorphe

$$\begin{aligned} \mathbb{C} \setminus \Lambda &\longrightarrow \{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2x - g_3\} \\ z &\longmapsto (j_{\Lambda}(z), j_{\Lambda}'(z)) \end{aligned}$$

et cette application s'étend en une application holomorphe

$$\begin{aligned} \mathbb{C} &\longrightarrow \{[x:y:z] \in \mathbb{P}^2(\mathbb{C}) \mid y^2z = 4x^3 - g_2xz^2 - g_3z^3\} \\ z &\longmapsto \begin{cases} [j_{\Lambda}(z) : j_{\Lambda}'(z) : 1] & \text{si } z \notin \Lambda \\ [0 : 1 : 0] & \text{si } z \in \Lambda \end{cases} \end{aligned}$$

Proposition: le polynôme  $f(x) = 4x^3 - g_2x - g_3$  a trois racines distinctes. En particulier,

$$\Delta(\Lambda) = g_2^3 - 27g_3^2 \neq 0$$

Démonstration. Soient  $w_1, w_2$  et  $w_3 = w_1 + w_2$ .

Comme  $\wp'$  est impaire,

$$\wp'\left(\frac{w_i}{2}\right) = -\wp'\left(-\frac{w_i}{2}\right) = -\wp'\left(\frac{w_i}{2}\right)$$

invariance par  
translation par  $w_i$

on a donc  $\wp'\left(\frac{w_i}{2}\right) = 0$  et de la  
relation  $y^2 = 4x^3 - g_2x - g_3$  on déduit  
que les racines de  $f(x)$  sont les points

$$e_i = \wp\left(\frac{w_i}{2}\right)$$

La fonction  $\wp(z) - \wp\left(\frac{w_i}{2}\right)$  est elliptique  
paire et a un pôle d'ordre 0, donc  
elle a 2 zéros. Comme  $\frac{w_i}{2}$  est déjà un  
zéro double, c'est le seul, d'où  $e_i \neq e_j$   
pour  $i \neq j$  □

Proposition. L'application

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\varphi} & E \subset \mathbb{P}^2(\mathbb{C}) \\ z & \longmapsto & [\wp(z) : \wp'(z) : 1] \end{array}$$

est une biholomorphisme.

Démonstration: Comme  $\varphi$  est une fonction holomorphe entre surfaces de Riemann compactes, il suffit de voir que  $\varphi$  est bijective.

(1) Injectivité: Soient  $z_1, z_2 \in \mathbb{C} \setminus \Lambda$  avec  $\varphi(z_1) = \varphi(z_2)$ , c'est-à-dire  $\wp(z_1) = \wp(z_2)$  et  $\wp'(z_1) = \wp'(z_2)$ .

• Si  $2z_1 \notin \Lambda$ , la fonction  $\wp(z) - \wp(z_1)$  s'annule en  $z_1, -z_1, z_2$ , donc

$$z_2 \equiv \pm z_1 \pmod{\Lambda}$$

car il n'y a que 2 zéros. Mais si  $z_2$  étant congrue à  $-z_1$  modulo  $\Lambda$  on aurait

$$\wp'(z_1) = \wp'(z_2) = \wp'(-z_1) = -\wp'(z_1),$$

donc  $\wp'(z_1) = 0$ , ce qui implique  $2z_1 \in \Lambda$ .

On en déduit  $z_2 \equiv z_1 \pmod{\Lambda}$ .

• Si  $2z_1 \in \Lambda$ , alors  $\wp(z) - \wp(z_1)$  a un zéro double en  $z_1$  et donc  $z_2 \equiv z_1 \pmod{\Lambda}$ .

(2) Surjectivité: Soit  $(x, y) \in E$ . La fonction elliptique  $P(z) - x$  n'est pas constante, donc elle a un zéro, disons en  $z = a$ , donc  $x = P(a)$  et  $y^2 = P'(a)^2$ . Autant à remplacer  $a$  par  $-a$  si nécessaire, on obtient  $(x, y) = (P(a), P'(a))$   $\square$

Remarque: Dans le langage de la géométrie algébrique, on a vu que la courbe projective d'équation

$$y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3$$

est lisse. En effet,

$$f(x, y, z) = y^2 z - 4x^3 + g_2 x z^2 + g_3 z^3$$

satisfait

$$\frac{\partial f}{\partial x} = -12x^2 + g_2 z^2$$

$$\frac{\partial f}{\partial y} = 2yz$$

$$\frac{\partial f}{\partial z} = y^2 + 2g_2 xz + 3g_3 z^2$$



et les points singuliers seraient donc les  $[x:y:1]$  tels que  $4x^3 - g_2x - g_3$  a une racine double.

### Théorème d'uniformisation

Soient  $a, b \in \mathbb{C}$  tels que  $a^3 - 27b^2 \neq 0$ .  
Alors il existe un réseau  $\Lambda \subseteq \mathbb{C}$  avec

$$a = g_2(\Lambda) \quad b = g_3(\Lambda).$$

Autrement dit, toutes les surfaces de Riemann  $E \subset \mathbb{P}^2(\mathbb{C})$  d'équation

$$y^2z = 4x^3 - axz^2 - bz^3$$

sont isomorphes à  $\mathbb{C}/\Lambda$  pour un réseau  $\Lambda \subseteq \mathbb{C}$ .

Remarque: L'application

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow E \\ z &\longmapsto [y(z) : y'(z) : 1] \end{aligned}$$

admet pour inverse l'application

$$\begin{aligned} E &\longrightarrow \mathbb{C}/\Lambda \\ p &\longmapsto \int_p^0 \frac{dx}{y} \quad \text{le point } [0:1:0] \end{aligned}$$

qui est bien définie car l'intégrale dépend du choix de chemin entre 0 et P par les périodes

$$\int_{\gamma_1} \frac{dx}{y} = w_1 \quad \text{et} \quad \int_{\gamma_2} \frac{dx}{y} = w_2$$



À comparer avec: l'inverse de l'application

$$\begin{aligned} \mathbb{C}/2\pi i \mathbb{Z} &\longrightarrow \mathbb{C}^\times \\ z &\longmapsto \exp(z) \end{aligned}$$

est l'application  $\mathbb{C}^\times \longrightarrow \mathbb{C}/2\pi i \mathbb{Z}$ ,  
 $P \longmapsto \int_1^P \frac{dt}{t}$

qui est bien définie car  $\int_{|t|=1} \frac{dt}{t} = 2\pi i$ .

Définition. on appelle courbe elliptique complexe la surface de Riemann

$$\begin{aligned} \mathbb{C}/\Lambda &\simeq E \subset \mathbb{P}^2(\mathbb{C}) \\ y^2 z &= 4x^3 - g_2 x z^2 - g_3 z^3 \end{aligned}$$

## ④ MORPHISMES DE COURBES ELLIPTIQUES COMPLEXES

Soient  $\Lambda_1, \Lambda_2 \subseteq \mathbb{C}$  des réseaux. Soit  $\alpha \in \mathbb{C}$ .  
Si  $\alpha \Lambda_1 \subseteq \Lambda_2$ , alors la multiplication  
par  $\alpha$  est un morphisme de groupes holomorphe

$$\begin{aligned} f_\alpha: \mathbb{C}/\Lambda_1 &\longrightarrow \mathbb{C}/\Lambda_2 \\ z &\longmapsto \alpha z \bmod \Lambda_2 \end{aligned}$$

qui envoie 0 sur 0. Ce sont les seuls!

Théorème. Il y a une bijection

$$\begin{aligned} \{\alpha \in \mathbb{C} \mid \alpha \Lambda_1 \subseteq \Lambda_2\} &\longrightarrow \left\{ \begin{array}{l} \text{applications holomor-} \\ \text{phes } f: \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2 \\ \text{avec } f(0) = 0 \end{array} \right\} \\ \alpha &\longmapsto f_\alpha \end{aligned}$$

En particulier, une application holomorphe  
 $f: \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2$  telle que  $f(0) = 0$  est un  
morphisme de groupes.

Démonstration:

(1) Injectivité: Si  $f_\alpha = f_\beta$ , alors  $\alpha z \equiv \beta z$   
modulo  $\Lambda$  pour tout  $z \in \mathbb{C}$ . Alors la multi-

plication par  $\alpha - \beta$  envoie  $\mathbb{C}$  (anneau) sur  $\Lambda$  (discret), donc c'est l'application nulle.  
On trouve ainsi  $\alpha = \beta$ .

(2) Surjectivité: soit  $f: \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2$   
une fonction holomorphe avec  $f(0) = 0$ . On  
applique la propriété de relèvement

$$\begin{array}{ccc}
 \text{relèvement} & \begin{array}{ccc} X' & x'_0 \\ \downarrow p & \downarrow & \\ Y & \xrightarrow{h} & X \\ y_0 \mapsto & x_0 \end{array} & \begin{array}{l} \text{se relève en } Y \rightarrow X' \\ y \mapsto x'_0 \end{array}
 \end{array}$$

si et seulement si

$$h_*(\pi_1(Y, y_0)) \subset p_*(\pi_1(X', x'_0))$$

(c'est donc toujours le cas si  $Y$  est simplement connexe). On obtient l'existence de

$$\begin{array}{ccc}
 \mathbb{C} & \xrightarrow{\tilde{f}} & \mathbb{C} \\
 \downarrow & & \downarrow \text{relèvement} \\
 \mathbb{C}/\Lambda_1 & \xrightarrow{f} & \mathbb{C}/\Lambda_2
 \end{array}$$

$\tilde{f}(0) = 0$

On a  $\tilde{f}(z+w) \equiv \tilde{f}(z) \pmod{\Lambda_2}$  pour tout  $w \in \Lambda_1$ , donc  $\tilde{f}(z+w) - \tilde{f}(z)$  est constante, donc  $\tilde{f}'(z+w) = \tilde{f}'(z)$ . Ainsi,  $\tilde{f}'$  est elliptique

holomorphe, donc on s'attend. Ceci implique  $\tilde{f}(z) = \alpha z + \gamma$  pour  $\alpha, \gamma \in \mathbb{C}$  et comme  $\tilde{f}(0) = 0$ , on trouve  $\tilde{f}(z) = \alpha z$ . La condition  $\tilde{f}(\Lambda_1) \subset \Lambda_2$  donne  $\alpha \Lambda_1 \subset \Lambda_2$   $\square$

Proposition. Soit  $\mathbb{C}/\Lambda$  une courbe elliptique complexe. Alors  $\text{End}(\mathbb{C}/\Lambda)$  est

(a) soit égal à  $\mathbb{Z}$

(b) soit égal à un ordre dans un corps quadratique imaginaire. Plus précisément, si  $\text{End}(\mathbb{C}/\Lambda) \neq \mathbb{Z}$  et  $\Lambda = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ , alors  $z = \frac{w_1}{w_2}$  est quadratique imaginaire et  $\text{End}(\mathbb{C}/\Lambda) \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$ . On dit alors que  $\mathbb{C}/\Lambda$  a multiplication complexe.

Démonstration. Soit  $\Lambda = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ . Alors

$\mathbb{C}/\Lambda$  est isomorphe à  $\mathbb{C}/\underline{\mathbb{Z} \oplus \mathbb{Z}z} = \Lambda_2$  et

$$\text{End}(\mathbb{C}/\Lambda) \cong \{ \alpha \in \mathbb{C} \mid \alpha \Lambda_2 \subset \Lambda_2 \} \supseteq \mathbb{Z}$$

La condition  $\alpha \Lambda_2 \subset \Lambda_2$  équivaut à l'existence d'entiers  $a, b, c, d \in \mathbb{Z}$  avec

$$\alpha \cdot 1 = a + bz$$

$$\alpha \cdot z = c + dz$$

Si  $\alpha \notin \mathbb{Z}$ , alors  $b \neq 0$  et  $z = \frac{\alpha - a}{b}$ , d'où

$$\alpha \left( \frac{\alpha - a}{b} \right) = c + dz$$

$$\Rightarrow \alpha^2 - (a+d)\alpha + ad - bc = 0$$

ce qui implique que  $\text{End}(\mathbb{C}/\Lambda)$  est une extension intègre de  $\mathbb{Z}$ .

Par ailleurs, si  $\alpha \notin \mathbb{Z}$ , on écrit

$$z = \frac{\alpha z}{\alpha} = \frac{c + dz}{a + bz}$$

et on trouve que  $bz^2 + (a-d)z - c = 0$ .

Comme  $z$  n'est pas réel,  $K = \mathbb{Q}(z)$  est un corps quadratique imaginaire.

Enfin,  $\text{End}(\mathbb{C}/\Lambda) \subseteq \mathbb{Z}[z]$  et donc

$$\uparrow$$

$$\alpha = a + bz$$

$\text{End}(\mathbb{C}/\Lambda) \otimes_{\mathbb{Z}} \mathbb{Q} = K$  pour des raisons de  
division

□

Exemple: La courbe elliptique complexe

$\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}i$  a multiplication complexe  
car le réseau  $\mathbb{Z} \oplus \mathbb{Z}i$  est stable par  
multiplication par  $i$ .