ARITHMÉTIQUE DES COURBES ELLIPTIQUES
FEUILLE DE TD 1

Exercice 1. Soit $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ le demi-plan de Poincaré. Pour toute matrice dans $\mathrm{SL}_2(\mathbb{R})$, posons

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

(1) Démontrer que cette formule définit une action transitive de $\mathrm{SL}_2(\mathbb{R})$ sur $\mathbb{H}$.

(2) Soit $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Démontrer que si $\tau' = \frac{a\tau+b}{c\tau+d}$, alors les réseaux $\mathbb{Z} \oplus \mathbb{Z}\tau$ et $\mathbb{Z} \oplus \mathbb{Z}\tau'$ sont homothétiques. En déduire que l'application

$$\begin{aligned} \mathbb{H}/\,\mathrm{SL}_2(\mathbb{Z}) &\longrightarrow \{\text{réseaux dans } \mathbb{C}\}/\mathbb{C}^\times \\ [\tau] &\longmapsto [\mathbb{Z} \oplus \mathbb{Z}\tau] \end{aligned}$$

est bien définie.

(3) Démontrer qu'elle est bijective.

Exercice 2. Soient $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ un réseau et $\mathbb{C}/\Lambda$ la courbe elliptique associée.

(1) Démontrer que $\mathbb{C}/\Lambda$ est isomorphe à $\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau$ avec $\tau = \omega_1/\omega_2$.

(2) Démontrer que les endomorphismes de $\mathbb{C}/\Lambda$ forment une extension intègre de $\mathbb{Z}$, c'est-à-dire un anneau contenant $\mathbb{Z}$ dont tous les éléments sont des racines de polynômes unitaires à coefficients entiers.

(3) Démontrer que si $\mathrm{End}(\mathbb{C}/\Lambda)$ n'est pas réduit à $\mathbb{Z}$, alors $\mathrm{K} = \mathbb{Q}(\tau)$ est un corps quadratique imaginaire et il y a un isomorphisme $\mathrm{End}(\mathbb{C}/\Lambda) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{K}$. On dit alors que la courbe elliptique $\mathbb{C}/\Lambda$ a *multiplication complexe*.

(4) Donner des exemples de courbes elliptiques à multiplication complexe.

Exercice 3. Soit $\Lambda \subset \mathbb{C}$ un réseau d'invariants g_2 et g_3, et soient $z_1, z_2 \in \mathbb{C} \setminus \Lambda$ des nombres complexes tels que $\wp(z_1) \neq \wp(z_2)$. Soit

$$y = ax + b$$

l'équation de la droite passant par les points $(\wp(z_1), \wp'(z_1))$ et $(\wp(z_2), \wp'(z_2))$.

(1) Démontrer que la fonction $\wp'(z) - a\wp(z) - b$ a trois zéros comptés avec multiplicité.

(2) En déduire que si $2z_1 + z_2$ ou $z_1 + 2z_1$ n'appartiennent pas au réseau, alors cette fonction a un zéro en un point $z_3 \equiv -z_1 - z_2 \bmod \Lambda$.

(3) Démontrer l'égalité

$$4\big(x - \wp(z_1)\big)\big(x - \wp(z_2)\big)\big(x - \wp(z_3)\big) = 4x^3 - g_2x - g_3x - (ax + b)^2.$$

(4) En déduire l'égalité $\wp(z_1) + \wp(z_2) + \wp(z_3) = a^2/4$.

(5) Démontrer l'égalité : pour tous $z_1, z_2 \in \mathbb{C}$,

$$\wp(z_1+z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1)-\wp'(z_2)}{\wp(z_1)-\wp(z_2)}\right)^2.$$

(6) En faisant tendre z_2 vers z_1, en déduire la formule de duplication

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

(7) Soient (x_1, y_1) et (x_2, y_2) deux points distincts sur la courbe algébrique affine

$$\mathrm{C}\colon y^2 = 4x^3 - g_2x - g_3.$$

Démontrer qu'il existe un point (x_3, y_3) dans l'intersection entre C et la droite passant par (x_1, y_1) et (x_2, y_2) de coordonnée

$$x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_1-y_2}{x_1-x_2}\right)^2$$

et comparer avec ce qui précède.

Exercice 4. Soit $\Lambda \subset \mathbb{C}$ un réseau. Notons δ la distance minimale entre deux points distincts de Λ et V le volume d'un domaine fondamental.

(1) Soit A une couronne de rayon intérieur r et d'épaisseur $\delta/2$. Démontrer que $\mathrm{A}\cap\Lambda$ contient au plus $4\pi r/\delta$ points.

(2) Démontrer l'estimée

$$|\{\omega \in \Lambda \mid |\omega| \leq \mathrm{R}\}| = \frac{\pi \mathrm{R}^2}{\mathrm{V}} + \mathrm{O}(\mathrm{R}) \quad \text{lorsque } \mathrm{R} \to +\infty.$$

(3) En déduire qu'il existe une constante c dépendant seulement de Λ tel que

$$|\{\omega \in \Lambda \mid \mathrm{R} \leq |\omega| < \mathrm{R}+1\}| \leq c\mathrm{R} \quad \text{pour tout } \mathrm{R} > 0.$$

Exercice 5 (Examen 2024)**.** Soient ω_1, ω_2 deux nombres complexes avec $\mathrm{Im}(\omega_2/\omega_1) > 0$ et $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ le réseau qu'ils engendrent. Considérons la série

$$\zeta_\Lambda(z) = \frac{1}{z} + \sum_{\omega \in \Lambda\setminus\{0\}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).$$

(1) Démontrer que $\zeta_\Lambda(z)$ converge absolument pour tout $z \in \mathbb{C}\setminus\Lambda$ et définit une fonction méromorphe sur $\mathbb{C}$ ayant des pôles simples de résidu 1 aux points de Λ.

(2) Est-ce que ζ_Λ est une fonction elliptique ?

(3) Démontrer l'égalité $\frac{d}{dz}\zeta_\Lambda = -\wp_\Lambda$, où $\wp_\Lambda$ désigne la fonction de Weierstrass associée à Λ.

(4) Posons $\omega_3 = \omega_1 + \omega_2$. Démontrer que pour $j = 1, 2, 3$, il existe des $\eta_j \in \mathbb{C}$ tels que

$$\zeta_\Lambda(z+\omega_j) = \zeta_\Lambda(z) + \eta_j$$

pour tout $z \in \mathbb{C}\setminus\Lambda$, puis l'égalité $\eta_j = 2\zeta_\Lambda(\omega_j/2)$.

(5) À l'aide du théorème du résidu de Cauchy, démontrer l'égalité

$$\eta_1\omega_2 - \eta_2\omega_1 = 2i\pi.$$