

TD2 TANC - Tores et courbes elliptiques complexes

Exercice 1. On pose $\Lambda = \mathbb{Z} + i\pi\mathbb{Z} \subseteq \mathbb{C}$ et $X = \mathbb{C}/\Lambda$. Montrer que $\text{End}(X) = \mathbb{Z}$.

Exercice 2. On considère $\Lambda = \mathbb{Z}[\omega] \subseteq \mathbb{C}$ avec $\omega = \frac{1+\sqrt{-3}}{2}$.

1. Montrer que $g_2(\Lambda) = 0$ (on pourra considérer $g_2(\omega\Lambda)$).
2. Montrer que $\mathbb{C}/\Lambda \simeq E(\mathbb{C})$ avec $E: y^2 = 4x^3 - g_3(\Lambda)$.
3. Quel est le j -invariant de E ?
4. Montrer que E est isomorphe à la courbe elliptique $^1 y^2 = x^3 + 1$.

Exercice 3 (Degré des isogénies et isogénies contragrédientes). Soit $X = \mathbb{C}/\Lambda$ et $X' = \mathbb{C}/\Lambda'$ des tores complexes. Soit $\alpha: X \rightarrow X'$ une isogénie qu'on identifie avec sa représentation analytique.

1. Montrer que $\deg[n]_X = n^2$.
2. Soit $X'' = \mathbb{C}/\Lambda''$ un autre tore complexe et $\beta: X' \rightarrow X''$ une isogénie. Montrer que $\deg(\beta \circ \alpha) = \deg(\beta) \deg(\alpha)$.
3. On pose $n = \deg(\alpha) = [\Lambda': \alpha\Lambda]$.
 - (a) Justifier que pour tout $\lambda' \in \Lambda'$ on a $n\lambda' \in \alpha\Lambda$.
 - (b) En déduire que pour toute isogénie $\alpha: X \rightarrow X'$ de degré n il existe une isogénie $\hat{\alpha} = \frac{n}{\alpha}: X' \rightarrow X$ appelée isogénie contragrédiente de α telle que

$$\hat{\alpha} \circ \alpha = [n]_X \text{ et } \alpha \circ \hat{\alpha} = [n]_{X'}.$$

- (c) (Un exemple). On considère $\Lambda = \mathbb{Z}[2i] \subseteq \mathbb{C}$ et $\Lambda' = \mathbb{Z}[i]$.
 - i. Déterminer $\text{End}(X)$ et $\text{End}(X')$.
 - ii. Quel est le degré de l'isogénie donnée par la représentation rationnelle $\iota: \mathbb{Z}[2i] \hookrightarrow \mathbb{Z}[i]$?
 - iii. Quelle est son isogénie contragrédiente ?

Exercice 4. On pose $R = \mathbb{Z}[\sqrt{-11}]$, $\omega = \sqrt{-11}$ et $\mathfrak{a} = \langle 3, 1 + \sqrt{-11} \rangle$. On dit que deux isogénies $\iota_1: \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda'_1$ et $\iota_2: \mathbb{C}/\Lambda_2 \rightarrow \mathbb{C}/\Lambda'_2$ sont isomorphes s'il existe des isomorphismes α et $\alpha' \in \mathbb{C}$ telles que

$$\begin{array}{ccc} \mathbb{C}/\Lambda_1 & \xrightarrow{\iota_1} & \mathbb{C}/\Lambda'_1 \\ \alpha \downarrow & & \downarrow \alpha' \\ \mathbb{C}/\Lambda_2 & \xrightarrow{\iota_2} & \mathbb{C}/\Lambda'_2. \end{array}$$

1. (a) L'ordre R est-il maximal ? Quel est son discriminant ? Quel est son conducteur ?
- (b) L'idéal $\mathfrak{a}$ est-il principal ? Est-il inversible ?
2. On identifie R à un sous anneau de $\mathbb{C}$ et on considère R et $\mathfrak{a}$ comme des réseaux de $\mathbb{C}$. On pose $\iota_{\mathfrak{a}}: \mathbb{C}/\mathfrak{a} \rightarrow \mathbb{C}/R$ l'isogénie engendrée par l'inclusion $\mathfrak{a} \hookrightarrow R$.
 - (a) Quelle est sa représentation analytique ?
 - (b) Quel est le degré de $\iota_{\mathfrak{a}}$?
 - (c) Les courbes elliptiques complexes $E_{\mathfrak{a}}$ et E_R sont-elles isomorphes ?
3. On pose $\mathfrak{b} = \bar{\mathfrak{a}}$.
 - (a) Montrer que $\mathfrak{a}$ et $\mathfrak{b}$ n'ont pas la même classe dans $\text{Cl}(R)$ (on pourra montrer que $\mathfrak{a}^2 = \langle 9, 4 + \sqrt{-11} \rangle$ et justifier qu'il n'est pas principal).
 - (b) On considère $\iota_{\mathfrak{b}}$ l'isogénie définie de la même façon que $\iota_{\mathfrak{a}}$. Les isogénies $\iota_{\mathfrak{a}}$ et $\iota_{\mathfrak{b}}$ sont elles isomorphes ?

1. Attention l'isomorphisme est sur $\mathbb{C}$ il n'y a pas de raison pour que $g_3(\Lambda) \in \mathbb{Q}$.

Exercice 5. Soit $X = \mathbb{C}/\Lambda$ un tore complexe à multiplication complexe par un ordre quadratique $R = \text{End}(X) = \{\alpha \in \mathbb{C}, \alpha\Lambda \subseteq \Lambda\}$ dans un corps quadratique K . On pose $\tau \in \mathcal{H}$ tel que $\Lambda \simeq \Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$. On pose

$$\text{Ell}_{\mathbb{C}}(R) = \{E \text{ courbe elliptique sur } \mathbb{C} / \text{End}(E) \simeq R\} / \simeq$$

l'ensemble des classes d'isomorphisme de courbes elliptiques sur $\mathbb{C}$ à multiplication complexe par R .

1. Montrer que $\tau \in K$.
2. En déduire qu'il existe $u \in R$ tel que $u\Lambda_\tau$ est un idéal $\mathfrak{a}$ de R .
3. Montrer que $\mathfrak{a}$ est un idéal inversible (on pourra considérer l'anneau des endomorphismes de $\mathfrak{a} \subseteq \mathbb{C}$ en tant que réseau).
4. Soit $\Lambda' \subseteq \mathbb{C}$ et $X' = \mathbb{C}/\Lambda'$ tel que $\Lambda' \simeq \mathfrak{a}'$ un idéal inversible de R . Montrer que $X \simeq X'$ si et seulement si $\mathfrak{a}$ et $\mathfrak{a}'$ ont la même classe dans $\text{Cl}(R)$.
5. En déduire que $\#\text{Ell}_{\mathbb{C}}(R) = \#\text{Cl}(R) = h(R)$.

Exercice 6 (Anneau d'endomorphisme d'une courbe elliptique sur $\mathbb{C}$). Soit $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subseteq \mathbb{C}$ et $X = \mathbb{C}/\Lambda$ le tore complexe correspondant. On veut montrer que $R = \text{End}(X) = \{\alpha \in \mathbb{C} / \alpha\Lambda \subseteq \Lambda\}$ est soit $\mathbb{Z}$ soit un ordre quadratique. Considérons $\alpha \in \text{End}(X)$ et $j, k, m, n \in \mathbb{Z}$ tels que $\alpha\omega_1 = j\omega_1 + k\omega_2$ et $\alpha\omega_2 = m\omega_1 + n\omega_2$.

1. On pose $M = \begin{pmatrix} \alpha - j & -k \\ -m & \alpha - n \end{pmatrix} \in M_2(\mathbb{C})$. Montrer que $\det(M) = 0$.
2. En déduire que $X^2 - (j+n)X + jn - km \in \mathbb{Z}[X]$ annule α et donc que α est un entier algébrique.
3. En déduire que $R \cap \mathbb{R} = \mathbb{Z}$.
4. Montrer que si $\alpha \notin \mathbb{Z}$ alors α est dans un ordre dans un corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{d})$.
5. Soit $\beta \in R \setminus \mathbb{Z}$ un autre élément. D'après ce qui précède β est aussi dans un ordre quadratique imaginaire dans un corps $\mathbb{Q}(\sqrt{d'})$.
 - (a) Soit $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}, \beta \in \mathbb{Q}(\sqrt{d'}) \setminus \mathbb{Q}$ avec d et d' des entiers sans facteur carré. Supposons que $\alpha + \beta$ de degré ≤ 2 . Montrer qu'alors $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ (on pourra se ramener au cas $\alpha = \sqrt{d}$ et $\beta = \sqrt{d'}$ puis déduire d'une relation de degré 2 en $\alpha + \beta$ que $\sqrt{d} \in \mathbb{Q}(\sqrt{d'})$ par exemple).
 - (b) Conclure.

Exercice 7 (La multiplication complexe est transmissible). On pose $X = \mathbb{C}/\Lambda$ et $X' = \mathbb{C}/\Lambda'$ deux tores complexes et $R = \mathbb{Z}[\omega]$ un ordre quadratique imaginaire et on suppose qu'il existe une isogénie $\alpha: X \rightarrow X'$ de degré $f \geq 1$ entre les deux. Soit $S = \mathbb{Z}[f\omega]$.

1. Montrer que si X est à CM par R alors $S \subseteq \text{End}(X')$.
2. Montrer que si X' est à CM par R alors $S \subseteq \text{End}(X)$ (on pourra penser à (ré)utiliser l'isogénie contragrédiente).
3. Montrer qu'on a pas forcément $\text{End}(X) = \text{End}(X')$ (cf. question 3.c de l'Exercice 3).

Exercice 8. On admet que $\overline{\mathbb{Q}}$ est dénombrable. Justifier que les courbes elliptiques complexes à CM sont « rares » parmi l'ensemble des courbes elliptiques complexes.