Feuille d'exercices n° 4

Exercice 1. Dans cet exercice on revient sur les notions d'ordre et sur la multiplication complexe des courbes elliptiques. Soit $K/\mathbb{Q}$ un corps de nombres. On dit qu'un sous-anneau $A \subset K$ est un ordre si c'est un $\mathbb{Z}$-module de type fini et que $K = \mathrm{Frac}(A)$. Un réseau est un sous-$\mathbb{Z}$-module de type fini $M \subset K$ tel que $M \otimes_{\mathbb{Z}} \mathbb{Q} = K$.

1. Soit $M \subset K$ un réseau. Montrer que $\{\alpha \in K \mid \alpha \cdot M = M\}$ est un ordre O_M de K.
2. Soient M, $M' \subset K$ deux réseaux tels qu'il existe $x \in K^*$ tel que $M' = x \cdot M$. Monter que $O_{M'} = O_M$.
3. Montrer que pour tout ordre $A \subset K$ il existe un réseau $M \subset K$ tel que $A = O_M$.
4. Montrer que l'ensemble des ordres de K ordonné pour la relation d'inclusion admet un unique élément maximal, qui est l'anneau $\mathcal{O}_K$ des entiers algébriques de K.
5. Soit $A \subset K$ un ordre. Est-ce un anneau de Dedekind ?
6. Montrer que $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Q}(\sqrt{d})$ est un ordre pour tout $d \in \mathbb{Z}$. Quand est-il égal maximal ?
7. Soit désormais $K/\mathbb{Q}$ un corps quadratique imaginaire et $A \subset K$ un ordre. Montrer qu'il existe $f \in \mathcal{O}_K$ tel que $A = \mathbb{Z} + f \cdot \mathcal{O}_K$. On appelle f le conducteur de l'ordre. On a $f = 1$ si et seulement si l'ordre est maximal.
8. Soit $A \subset K$ un ordre d'un corps quadratique imaginaire. Construire une courbe elliptique E sur $\mathbb{C}$ telle que $\mathrm{End}(E) = A$.
9. Donner des équations explicites de cette courbe elliptique lorsque $K = \mathbb{Q}(i)$ et $A = \mathbb{Z} + 2i\mathbb{Z}$.

Exercice 2 Dans cet exercice, on s'intéresse aux endomorphismes des courbes elliptiques sur les corps finis. On voit apparaître une courbe elliptique supersingulière. Soit k un corps contenant une racine primitive 4-ième de 1 notée I. Soit E la courbe elliptique sur k d'équation $y^2 = x^3 - x$.

1. Vérifier que $[i]_E : (x, y) \mapsto (-x, Iy)$ est un endomorphisme de E.
2. En déduire l'existence d'un morphisme d'anneau $[\bullet]_E : \mathbb{Z}[i] \to \mathrm{End}(E)$.
3. Montrer que $[\bullet]_E$ est injectif et que $[\alpha]_E$ est une isogénie pour tout $\alpha \neq 0$.
4. Soit p premier tel que $p \equiv 3$ modulo 4. Notons désormais $k = \mathbb{Z}[i]/p \cdot \mathbb{Z}[i]$. Rappeler la structure de k. On notera $I \in k$ la classe de i.
5. Notons $\phi_p : E \to E$ le morphisme $(x, y) \mapsto (x^p, y^p)$. Vérifier que $\phi_p \circ [i]_E = [-i]_E \circ \phi_p$.

6. Est-ce que l'anneau $\mathrm{End}(E)$ est commutatif ?

7. Admettons que $\phi_p^2 = [-p]_E$. Notons A l'anneau non commutatif défini par générateur et relation
$$A \;=\; \mathbb{Z} < I, J > / \left(I^2 = -1,\; J^2 = -p,\; IJ = -JI \right)$$
Construire un morphisme d'anneaux $A \to \mathrm{End}(E)$.

8. Prouver que ce morphisme est injectif.