Examen terminal TANC (durée 2h)

Lors de cette épreuve tous les documents sont autorisés (cours, TD, corrigés des TD, livres etc). Tous les appareils électroniques sont cependant interdits et doivent être éteints (téléphone, ordinateur, calculatrice etc). Tous les résultats énoncés dans le cours (exercices inclus) et dans les TDs peuvent être utilisés librement. L'exercice 1 est à rédiger sur une feuille indépendante du reste de la composition.

Le barème indiqué est donné à titre indicatif et est susceptible de changer.

Exercice 1 (3 points)**.** Soit $I = \langle X^2Y - 1, XY^2 - X \rangle \subset \mathbb{C}[X, Y]$.

1. Calculer une base de Gröbner minimale réduite de I pour l'ordre lexicographique avec $X > Y$.
2. Donner une base du $\mathbb{C}$-espace vectoriel $\mathbb{C}[X, Y]/I$.
3. Est ce que la classe $\overline{1 + X} = (1 + X) + I$ de $1 + X$ dans l'anneau quotient $\mathbb{C}[X, Y]/I$ est inversible ?

Exercice 2 (2 points)**.** Les questions 1 et 2 de cet exercice sont indépendantes.

1. Les factorisations
$$6 = 2 \cdot 3 = (2 + \sqrt{-2}) \cdot (2 - \sqrt{-2})$$
contredisent-elles le fait que $\mathbb{Z}[\sqrt{-2}]$ est factoriel (car principal) ? Expliquez.
2. Soit $\varphi \colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ une isogénie. Montrer que φ est surjective.

Exercice 3 (4,5 points)**.** On pose $\mathfrak{a} = 2\mathbb{Z} + (1 + \sqrt{-7})\mathbb{Z} \subseteq \mathbb{C}, X = \mathbb{C}/\mathfrak{a}$ ainsi que $K = \mathbb{Q}\left(\sqrt{-7}\right)$ et $R = \mathbb{Z}[\sqrt{-7}]$.

1. Quel est l'ordre maximal $\mathscr{O}_K$ de K ?
2. Montrer que $R \subseteq \mathrm{End}(X)$. Expliquez pourquoi cela nous permet de considérer $\mathfrak{a}$ comme un R-idéal.
3. Montrer qu'on a l'égalité de R-idéaux $\mathfrak{a}\overline{\mathfrak{a}} = \left\langle 4, 2 + 2\sqrt{-7} \right\rangle$.
4. En déduire que $\mathfrak{a}$ n'est pas un R-idéal inversible.
5. Montrer que $\mathrm{End}(X) = \mathscr{O}_K$.

Exercice 4 (7 points)**.** On considère $R = \mathbb{Z}[\omega]$ avec $\omega = \sqrt{-19}$ et $K = \mathbb{Q}\left(\sqrt{-19}\right)$. On pose $\mathfrak{a} = \left\langle 4, -1 + \sqrt{-19} \right\rangle$ un idéal de R.

1. Quel est l'ordre maximal $\mathscr{O}_K = \mathbb{Z}[\omega']$? Quel est le conducteur de R dans $\mathscr{O}_K$?
2. Quelle est la norme de $\mathfrak{a}$?
3. Montrer que $\mathfrak{a}\overline{\mathfrak{a}} = \langle 4 \rangle$.
4. L'idéal $\mathfrak{a}$ est-il inversible ?
5. On pose $\mathfrak{a}' = \mathfrak{a}\mathscr{O}_K = 4\mathscr{O}_K + (-1 + \sqrt{-19})\mathscr{O}_K$, l'idéal de $\mathscr{O}_K$ engendré par les générateurs de $\mathfrak{a}$.
   (a) Montrer que $\mathfrak{a}' = 2\mathscr{O}_K$.
   (b) Quels sont les degrés des trois isogénies $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ avec $\Lambda \subseteq \Lambda'$ pour $\Lambda \subseteq \Lambda'$ les inclusions suivantes :
      i. $R \subseteq \mathscr{O}_K$,
      ii. $\mathfrak{a} \subseteq R$,
      iii. $\mathfrak{a} \subseteq \mathscr{O}_K$,
      iv. $\mathfrak{a}' \subseteq \mathscr{O}_K$,

      Justifiez vos réponses.

Exercice 5 (4,5 points)**.** Déterminer une courbe E définie sur $\mathbb{F}_5$ avec $N = 7$ points rationnels **en appliquant la méthode CM**. On pose $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ et on donne

$$H_R(X) = X + 884736 \in \mathbb{Z}[X]$$

le polynôme de classes de Hilbert correspondant.