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.
On a $2 = -\sqrt{-2}^2$ et $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$. Par ailleurs, $\sqrt{-2}$ et $1 + \sqrt{-2}$ sont premiers car de normes premières donc $2 \cdot 3 = -\sqrt{-2}(1+\sqrt{-2}) \cdot \sqrt{-2}(1-\sqrt{2}) = (2-\sqrt{-2}) \cdot (2+\sqrt{-2})$ donc les deux factorisations induisent des décompositions en facteurs premiers de 6 identiques.
2. Soit $\varphi \colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ une isogénie. Montrer que φ est surjective.
On note $\pi \colon \mathbb{C} \to \mathbb{C}/\Lambda$ et $\pi' \colon \mathbb{C} \to \mathbb{C}/\Lambda'$ les projections canoniques et $\alpha \colon \mathbb{C} \to \mathbb{C}$ la représentation analytique de φ. Par définition de la représentation analytique on a $\varphi \circ \pi = \pi' \circ \alpha$. On propose deux méthodes.

   Méthode 1 : Soit $\pi'(z') \in X'$. On a $\varphi\left(\pi\left(\frac{z'}{\alpha}\right)\right) = \pi'\left(\alpha \cdot \frac{z'}{\alpha}\right) = \pi'(z')$.

   Méthode 2 : D'après la relation $\varphi \circ \pi = \pi' \circ \alpha$, puisque π' est surjective et α bijective alors $\varphi \circ \pi$ est surjective ce qui implique 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 ?
On a $-7 = 1 \mod 4$ donc l'ordre maximal est $\mathscr{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$.
2. Montrer que $R \subseteq \mathrm{End}(X)$. Expliquez pourquoi cela nous permet de considérer $\mathfrak{a}$ comme un R-idéal.
On a R est engendré par 1 et $\sqrt{-7}$ et $1 \cdot \mathfrak{a} = \mathfrak{a}$ et
$$\sqrt{-7} \cdot 2 = 2\sqrt{-7} = -2 + 2(1 + \sqrt{-7}) \in \mathfrak{a}$$
$$\sqrt{-7} \cdot (1 + \sqrt{-7}) = \sqrt{-7} - 7 = -4 \cdot 2 + (1 + \sqrt{-7}) \in \mathfrak{a}.$$
3. Montrer qu'on a l'égalité de R-idéaux $\mathfrak{a}\overline{\mathfrak{a}} = \langle 4, 2 + 2\sqrt{-7} \rangle$.
$$\begin{aligned}
\mathfrak{a}\overline{\mathfrak{a}} &= \langle 2, 1 + \sqrt{-7} \rangle \cdot \langle 2, 1 - \sqrt{-7} \rangle \\
&= \langle 4, 2 \cdot (1 + \sqrt{-7}), 2 \cdot (1 - \sqrt{-7}), 1 + 7 \rangle \\
&= \langle 4, 2 + 2\sqrt{-7}, 2 \cdot (1 - \sqrt{-7}) + 2 \cdot (1 - \sqrt{-7}) \rangle \\
&= \langle 4, 2 + 2\sqrt{-7}, 4 \rangle \\
&= \langle 4, 2 + 2\sqrt{-7} \rangle
\end{aligned}$$
4. En déduire que $\mathfrak{a}$ n'est pas un R-idéal inversible.
On a $2|2, 2|4$ et $4|2 \cdot N(1 + \sqrt{-7}) = 16$ donc $N(\mathfrak{a}\overline{\mathfrak{a}}) = 4 \times 2 = 8$. Or $\mathfrak{a}$ est de norme 2 donc si $\mathfrak{a}$ était inversible on aurait $\mathfrak{a}\overline{\mathfrak{a}} = 2R$ de norme 4.

5. Montrer que $\mathrm{End}(X) = \mathscr{O}_K$.
   Puisque $\mathfrak{a}$ n'est pas inversible dans R il est inversible dans un sur-ordre $R_\mathfrak{a} = (\mathfrak{a}\colon \mathfrak{a})$ de R. Or l'unique sur-ordre de R est $\mathscr{O}_K$. On en déduit que
   $$\mathrm{End}(X) = (\mathfrak{a}\colon \mathfrak{a}) = \mathscr{O}_K.$$

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 $\mathscr{O}_K$?
   L'ordre maximal est $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ car $-19 = 1 \mod 4$. Le conducteur de R dans $\mathscr{O}_K$ est 2.
2. Quelle est la norme de $\mathfrak{a}$?
   Sa norme est 4×1 car $4 | N(-1+\sqrt{-19})$.
3. Montrer que $\mathfrak{a}\overline{\mathfrak{a}} = \langle 4\rangle$.
   On a
   $$\begin{aligned}\mathfrak{a}\overline{\mathfrak{a}} &= \left\langle 16, 4(1+\sqrt{-19}), 4(1-\sqrt{-19}), 20\right\rangle\\ &= \left\langle 16, 4(1+\sqrt{-19}) + 4(1-\sqrt{-19}), 4(1-\sqrt{-19}), 20\right\rangle\\ &= \left\langle 16, 8, 4(1-\sqrt{-19}), 20\right\rangle\\ &= \left\langle 4, 4(1-\sqrt{-19}), 20\right\rangle \text{ car } \mathrm{pgcd}(8,20) = 4 \in \mathfrak{a}\overline{\mathfrak{a}}\\ &= \langle 4\rangle\end{aligned}$$
4. L'idéal $\mathfrak{a}$ est-il inversible ?
   Oui il est inversible d'inverse $\mathfrak{a}^{-1} = \frac{1}{4}\overline{\mathfrak{a}}$.
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 $\mathfrak{a}' = 2\mathscr{O}_K$.
   On a $\omega = 2\omega' - 1$ donc $\mathfrak{a}' = 4\mathscr{O}_K + (-2+2\omega')\mathscr{O}_K = 4\mathscr{O}_K + (2+2\omega')\mathscr{O}_K$. Par ailleurs, $(2+2\omega')\cdot(1+\overline{\omega'}) = 2 \cdot N(1+\omega') = 14$ donc $\mathfrak{a}'$ contient 4 et 14 donc $\mathrm{pgcd}(4,14) = 2$ donc $\mathfrak{a}' = 2\mathscr{O}_K$.
   (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. $R \subseteq \mathscr{O}_K$,
   $[\mathscr{O}_K\colon R] = 2$ donc c'est une isogénie de degré 2
   ii. $\mathfrak{a} \subseteq R$,
   $[R\colon \mathfrak{a}] = N(\mathfrak{a}) = 4$
   iii. $\mathfrak{a} \subseteq \mathscr{O}_K$,
   Il s'agit de la composée des deux isogénies précédentes donc son degré est $2 \times 4 = 8$.
   iv. $\mathfrak{a}' \subseteq \mathscr{O}_K$,
   La norme de $\mathfrak{a}'$ dans $\mathscr{O}_K$ est 4 donc c'est une isogénie de degré 4.
   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.
Une telle courbe devrait avoir pour trace $a = 5 + 1 - 7 = -1$. Le discriminant de l'ordre engendré par son endomorphisme de Frobenius est alors de discriminant $\Delta = a^2 - 4 \cdot 5 = -19$. Il s'agit du discriminant de l'ordre maximal R. Une courbe à CM par R a pour trace $\pm a = \pm 1$. Une telle courbe a pour j-invariant une racine de $H_R \mod 5 = X + 1$, i.e. $j = -1$ et on a bien $-1 \neq 0$ et $-1 \neq 1728 = 3$. On considère la courbe
$$E\colon y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j} = x^3 + \frac{-3}{-1}x + \frac{-2}{-1} = x^3 + 3x + 2$$
de j-invariant -1. Cette courbe a soit 7 soit $q+1+(-1) = 5$ points. On compte le nombre de points de E sachant que les carrés non nuls de $\mathbb{F}_5$ sont ± 1 :

x	x^3+3x+2	
0	2	
1	1	$\to$ 2 points
-1	-2	
2	1	$\to$ 2 points
-2	-2.	

La courbe E a donc $2+2$ points affines plus le neutre à l'infini soit 5 points. Ses tordues quadratiques ont donc 7 points. On considère $2 \in \mathbb{F}_5$ un non-carré et

$$\widetilde{E}\colon y^2 = x^3 + 2^2 \cdot 3x + 2^3 \cdot 2 = x^3 + 2x + 1$$

qui a 7 points rationnels (inutile de le vérifier).