Examen

Mercredi 15 mai 2024 - Durée 2h
Documents interdits - Calculettes interdites

Les 4 exercices sont indépendants.

Exercice 1. — Répondre aux questions en justifiant sa réponse.

1. Existe-t-il un corps de cardinal 36 ?
2. La classe de 2 dans le groupe multiplicatif $(\mathbf{Z}/13\mathbf{Z})^*$ est un générateur ?
3. L'ensemble des solutions du système $\begin{cases} x & \equiv & 3 \pmod 8 \\ x & \equiv & 7 \pmod{12} \end{cases}$ est $x \equiv 43 \pmod{48}$?

Exercice 2. —
Soit p un nombre premier et $\alpha = i\sqrt{p} \in \mathbf{C}$. On note $\mathbf{Z}[\alpha]$ le sous-anneau de $\mathbf{C}$ engendré par α.

1. Montrer que $\mathbf{Z}[\alpha] = \mathbf{Z} + \alpha\mathbf{Z} = \{a + b\alpha \mid a, b \in \mathbf{Z}\}$.
2. Montrer que l'application $\Psi : \begin{array}{ccc} \mathbf{Z}\times\mathbf{Z} & \to & \mathbf{Z}[\alpha] \\ (x\,,\,y) & \mapsto & x + y\alpha \end{array}$ est un isomorphisme de groupe.
3. Montrer que $\alpha\mathbf{Z}[\alpha] = p\mathbf{Z} + \alpha\mathbf{Z} = \{a + b\alpha \mid a, b \in \mathbf{Z}, a \equiv 0 \pmod p\}$.
4. En déduire que α est un élément premier de $\mathbf{Z}[\alpha]$.

Exercice 3. — Cardinal de l'anneau $\mathbf{Z}[i]/(a+ib)$, où $(a,b) = 1$
$\mathbf{Z}[i] = \{x + iy \mid x, y \in \mathbf{Z}\}$ désigne le sous-anneau de $\mathbf{C}$ engendré par i. On désigne par a, b deux entiers premiers entre eux, et on considère l'idéal $(a + ib) = (a + ib)\mathbf{Z}[i]$ de $\mathbf{Z}[i]$. On note Φ l'unique morphisme d'anneaux de $\mathbf{Z}$ vers $\mathbf{Z}[i]/(a + ib)$.

1. Soit $x, y \in \mathbf{Z}$, tels que $m = (a + ib)\cdot(x + iy) \in \mathbf{Z}$.
   (a) Montrer que $ax - by = m$ et $ay + bx = 0$.
   (b) Montrer que $\{(x, y) \in \mathbf{Z}^2 \mid ay + bx = 0\} = \{\lambda(-a, b), \lambda \in \mathbf{Z}\}$.
   (c) En déduire que $\ker\Phi = (a^2 + b^2)\mathbf{Z}$.
2. Soit $u, v, t \in \mathbf{Z}$, tels que $i = t + (a + ib)(v + iu)$.
   (a) Montrer que $bu - av = t$ et $au + bv = 1$.
   (b) En déduire qu'il existe $t_0 \in \mathbf{Z}$, tel que $\Phi(t_0) \equiv i \pmod{(a + ib)}$.
   (c) En déduire un isomorphisme d'anneaux entre $\mathbf{Z}[i]/(a + ib)$ et $\mathbf{Z}/(a^2 + b^2)\mathbf{Z}$.
3. Montrer que $\mathrm{Card}\big(\mathbf{Z}[i]/(a + ib)\big) = a^2 + b^2$.
4. Montrer que $a + ib$ divise $x + iy$ dans $\mathbf{Z}[i]$ si et seulement si $a^2 + b^2$ divise $x + t_0y$ dans $\mathbf{Z}$.
   Indication : on pourra considérer $\Psi : x + iy \to \Phi(x + t_0y)$.

Exercice 4. — Soit K un corps commutatif et $P = X^6 + X^4 + X^2 + 1 \in K[X]$.

1. Montrer que P divise $X^8 - 1 \in K[X]$.
2. On suppose ici $K = \mathbf{Q}$.
   (a) Montrer que $P = (1 + X^2)(1 + X^4) \in \mathbf{Z}[X]$
   (b) Quelle est la factorisation de P en produit ce polynômes irréductibles dans $\mathbf{Q}[X]$?
3. On suppose ici que $K = \mathbf{Z}/17\mathbf{Z}$.
   (a) Montrer que les racines de P sont dans K et sont toutes des carrés de K^*.
   (b) Déterminer les racines de P dans K.
4. On suppose ici que $K = \mathbf{Z}/3\mathbf{Z}$.
   (a) Montrer que $(P, X^3 - X) = 1$.
   (b) En déduire que P se factorise en produit de polynômes irréductibles de degré 2.
   (c) Factoriser P en produit de polynômes irréductibles dans $K[X]$.