Université Claude Bernard Lyon 1 — Anneaux et Corps
Semestre de printemps 2022-23 — Licence 3

Contrôle Terminal 2 – Durée 120 min – mardi 23 mai 2023

Les documents, les téléphones et les calculatrices ne sont pas autorisés.
La notation tiendra compte du soin apporté à la rédaction des réponses.
Les **réponses mal justifiées** ne permettront pas d'obtenir tous les points.
L'énoncé comporte 2 exercices.

Exercice 1. Structure d'un anneau quotient.

Dans cet exercice on veut montrer que l'anneau $\mathbb{Z}[i]/(1+3i)$ est isomorphe à l'anneau $\mathbb{Z}/10\mathbb{Z}$.
Soit $R = \mathbb{Z}[i]$ l'anneau des entiers de Gauss, et $\overline{R}$ l'anneau quotient de R par la relation $1+3i=0$. Autrement dit, $\overline{R} = R/I$, où I est l'idéal engendré par $1+3i$.

1. Montrer que $i = 3$ dans $\overline{R}$.
2. En déduire que $10 = 0$ dans $\overline{R}$.
3. Montrer qu'il existe un unique homomorphisme d'anneaux
$$\phi : \mathbb{Z} \to \overline{R}.$$
4. Calculer les images de $0, 1, 2, \dots, 10$ par ϕ.
5. Montrer que ϕ est surjectif.
6. Quel est le noyau de ϕ?
7. Conclure.

Exercice 2. Racines carrés modulo P.
On considère des quotients de l'anneau $\mathbb{C}[X]$ des polynômes à coefficients complexes.

1. Fixons $\lambda \in \mathbb{C}^*$. Soit R dans $\mathbb{C}[X]$. Justifier que $R \equiv R(\lambda) \quad [X-\lambda]$.
2. Soit A et B dans $\mathbb{C}[X]$ et $n \in \mathbb{N}^*$. Montrer que les assertions suivantes sont équivalentes :
   (a) $A \equiv B \quad [(X-\lambda)^n]$;
   (b) $\exists e \in \mathbb{C}$ tel que $A \equiv B + e(X-\lambda)^n \quad [(X-\lambda)^{n+1}]$.
3. Montrer qu'il existe $R \in \mathbb{C}[X]$ tel que $R(X)^2 X \equiv 1 \quad [X-\lambda]$.
4. Soit $n \in \mathbb{N}^*$ et $R \in \mathbb{C}[X]$ tel que $R(X)^2 X \equiv 1 \quad [(X-\lambda)^n]$. Montrer qu'il existe $c \in \mathbb{C}$ tel que $S(X) = R(X) - c(X-\lambda)^n$ vérifie
$$S(X)^2 X \equiv 1 \quad [(X-\lambda)^{n+1}].$$
5. En déduire que, pour tout n, il existe $R \in \mathbb{C}[X]$ tel que $R(X)^2 X \equiv 1 \quad [(X-\lambda)^n]$.
6. Soit $P \in \mathbb{C}[X]$ tel que $P(0) \neq 0$. A l'aide du théorème des restes chinois, montrer qu'il existe $Q \in \mathbb{C}[X]$ tel que $Q(X)^2 X \equiv 1 \quad [P]$.
7. Soit $A \in \mathrm{GL}_n(\mathbb{C})$. Déduire de la question précédente qu'il existe $M \in \mathrm{GL}_n(\mathbb{C})$ telle que $M^2 = A^{-1}$.
8. Même question avec $M^2 = A$.

Exercice 3. On se place dans l'anneau $A = \mathbb{F}_3[X]$ des polynômes à coefficients dans le corps fini à 3 éléments. Soit $P(X) = X^8 + 1$. Le but de cet exercice est de factoriser P.

1. Exiber un polynôme irréductible de degré 2 dans A.
2. Montrer que les deux polynômes $X^4 \pm X^2 - 1$ n'ont pas de racine dans $\mathbb{F}_9$.
3. En déduire qu'ils sont irréductibles dans A.

4. Montrer que P est sans facteur carré.
5. En déduire, à l'aide du théorème des restes chinois, qu'il existe un isomorphisme

$$\psi : A/(P) \to \prod_{i=1}^{s} K_i,$$

   où s est un entier naturel et les K_i sont des corps, extensions finies de $\mathbb{F}_3$.
6. On considère l'application

$$\begin{array}{rccc} \varphi : & A/(P) & \longrightarrow & A/(P) \\ & y & \longmapsto & y^3 - y. \end{array}$$

   Montrer que φ est $\mathbb{F}_3$-linéaire et donner un élément T de son noyau, non multiple de 1.
7. On note $\psi(X^6 + X^2) = (T_1, \ldots, T_s)$. Montrer que $T_i \in \mathbb{F}_3$, pout tout $i = 1, \ldots, s$.
8. En déduire que $P = \prod_{\alpha \in \mathbb{F}_3} \mathrm{pgcd}(P, X^6 + X^2 - \alpha)$.
9. Déduire de la formule précédente que $P(X) = (X^4 - X^2 - 1)(X^4 + X^2 - 1)$.