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 une relation $1+3i = 0$. Autrement dit, $\overline{R} = R/I$, où I est un idéal engendré par $1+3i$.

1. Montrer que $i = 3$ dans $\overline{R}$.
   $-i(1+3i)+i = 3$
2. En déduire que $10 = 0$ dans $\overline{R}$.
   $0 = (1+3i) = 1+3.3 = 10 \bmod 1+3i$
3. Montrer qu'il existe un unique homomorphisme d'anneaux
$$\phi : \mathbb{Z} \to \overline{R}.$$
   Unicité : Un morphisme d'anneau envoie 1 sur 1. Ainsi, on définit $\phi(1) = 1$ et donc $\forall k \in \mathbb{N}, \phi(k) = \phi(1+..+1) = \phi(1)+..+\phi(1)$ k fois, et $\forall k \in \mathbb{Z}, 0 = \phi(k-k) = \phi(k)+\phi(-k)$. Pour l'existence, on prend les relations préalablement définies pour $\phi(k)$ et on vérifie trivialement les axiomes de morphisme d'anneau.
4. Calculer les images de $0, 1, 2, \ldots, 10$ par ϕ.
   D'après la question précédente, pour $0 \leq k \leq 9$,$\phi(k) = k$ et $\phi(10) = 10 = 0$.
5. Montrer que ϕ est surjectif.
   Soit $y \in \overline{R}$.$y = a+ib = a+3b = k$ avec $0 \leq k \leq 9$. résultat de la division euclidienne de $a+3b$ par 10. La question précédente montre donc la surjectivité.
6. Quel est le noyau de ϕ?
   On a $10 \in \ker\phi$ d'après ce qui précède. Or $\ker\phi$ est un idéal principal car $\mathbb{Z}$ est euclidien (donc principal). On a $\ker\phi = (a)$ avec a diviseur de 10. D'après ce qui précède $a = 10$ car $\phi(2) = 2$ et $\phi(5) = 5$. Il reste à montrer que 2 et 5 sont non nuls. Si $2 = 0$ il existe $\lambda \in \mathbb{Z}[i]$ tel que $2+\lambda(1+3i) = 0$ d'où $4 = 10|\lambda|^2$, exclu. Si $5 = 0$ on trouve de même $5 = 2|\lambda|^2$, impossible également.
7. Conclure.
   On utilise le théorème de factorisation. On obtient un morphisme injectif $\overline{\phi} : \mathbb{Z}/\ker\phi = \mathbb{Z}/10\mathbb{Z} \to \overline{R}$ qui fait commuter le diagramme avec la projection canonique. Le morphisme ϕ étant surjectif, $\overline{\phi}$ l'est aussi par commutation de diagramme. On obtient un isomorphisme entre $\mathbb{Z}/10\mathbb{Z}$ et $\overline{R}$.

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 $R \equiv R(\lambda) \quad [X-\lambda]$.
   Soit $\lambda \in \mathbb{C}^*$ et R dans $\mathbb{C}[X]$. On effectue la division euclidienne de R par $X-\lambda$ et obtient l'existence de Q et L, tels que $R(X) = Q(X)(X-\lambda)+L(X)$ $\deg(L) = 0$ donc $L \in \mathbb{C}$. En évaluant en λ on trouve $R \equiv R(\lambda) \quad [X-\lambda]$.
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 $A \equiv B + e(X-\lambda)^n \quad [(X-\lambda)^{n+1}]$.

$A \equiv B \quad [(X-\lambda)^n]$ équivaut à : il existe $K \in \mathbb{C}[X]$ tel que $A - B = K.(X-\lambda)^n$ On effectue la division euclidienne $K = Q.(X-\lambda) + e$, $e \in \mathbb{C}$, $Q \in \mathbb{C}[X]$. Ainsi, il existe $e \in \mathbb{C}$ tel que $A - B = (Q.(X-\lambda)+e).(X-\lambda)^n = e(X-\lambda)^n \quad [(X-\lambda)^{n+1}]$.

La réciproque est évidente.

3. Montrer qu'il existe $R \in \mathbb{C}[X]$ tel que $R(X)^2 X \equiv 1 \quad [X-\lambda]$.

On utilise la première question : $R(X)^2 X \equiv R(\lambda)^2 \lambda \equiv 1 \quad [X-\lambda]$. Il suffit donc de construire un polynôme R (de degré 0) tel que R est une racine carré sur $\mathbb{C}$ de $\frac{1}{\lambda}$.

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

$$S(X)^2 X \equiv 1 \quad [(X-\lambda)^{n+1}].$$

On suppose que $R \in \mathbb{C}[X]$ avec $R(X)^2 X \equiv 1 \quad [(X-\lambda)^n]$

On souhaite trouver $c \in \mathbb{C}$ tel que $S(X) = R(X) - c(X-\lambda)^n$ vérifie

$$S(X)^2 X \equiv 1 \quad [(X-\lambda)^{n+1}] \ .$$

Ainsi,

$$(R(X) - c(X-\lambda)^n)^2 X \equiv 1 \quad [(X-\lambda)^{n+1}] \ .$$

$$(R(X)^2 X - 2cR(X)X(X-\lambda)^n + c^2 X(X-\lambda)^2 n) \equiv 1 \quad [(X-\lambda)^{n+1}] \ .$$

Comme $n \geq 1$, $(X-\lambda)^2 n) \equiv 0 \quad [(X-\lambda)^{n+1}]$. De part l'avant dernière question $R(X)^2 X = 1 + e(X-\lambda)^n \quad [(X-\lambda)^{n+1}]$. Il vient :

$$(e - 2cR(X)X)(X-\lambda)^n \equiv 0 \quad [(X-\lambda)^{n+1}] \ .$$

$$(e - 2cR(X)X) \equiv 0 \quad [(X-\lambda)] \ .$$

Il suffit donc de prendre $c = \frac{e}{2R(\lambda)\lambda}$, si $R(\lambda)\lambda$ est non nul, $c = 0$ sinon.

5. En déduire que, pour tout n, il existe $R \in \mathbb{C}[X]$ tel que $R(X)^2 X \equiv 1 \quad [(X-\lambda)^n]$.

On procède par récurrence. L'initialisation est prouvée par le 3. L'hérédité par la question précédente.

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 $Q(X)^2 X \equiv 1 \quad [P]$.

Sur $\mathbb{C}$ (algébriquement clos), P se factorise en produit $\prod_i (X-\lambda_i)^{v_i}$. De plus, aucun des λ_i n'est nul d'après l'hypothèse sur P. D'après le théorème des restes chinois, on a un isomorphisme ψ entre $\mathbb{C}[X]/(P)$ et le produit d'anneau $\mathbb{C}[X]/((X-\lambda_i)_i^v)$. Or, sur chacun de ces anneaux d'après ce qui précèdent il existe Q_i tel que $Q_i(X)^2 X = 1$. Il vient que $\psi^{-1}(Q_1, \dots)^2 X = \psi^{-1}(1) = 1$ dans $\mathbb{C}[X]/(P)$.

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 $M^2 = A^{-1}$.

Soit P polynôme minimal de A. $P(0) \neq 0$, sinon $P(X) = XN(X)$ et $AN(A) = 0$, il vient que l'image de $N(A)$ (non nulle par minimalité de P est dans le noyau de A, absurde si A inversible. En utilisant le travail précédent, il existe $Q \in^C C$ tel que $Q(X)^2 X \equiv 1 \quad P$ D'où, $Q(A)^2 A = I$, et donc $Q(A)^2 A^{-1}$.

8. Même question avec $M^2 = A$.

Il suffit de prendre M^{-1} dans la question précédente.

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

1. Exhiber un polynôme irréductible de degré 2 dans A.
   Le polynôme X^2+1 est irréductible car il n'a pas de racine sur $\mathbb{F}_3$.
2. Montrer que les deux polynômes $X^4 \pm X^2 - 1$ n'ont pas de racine dans $\mathbb{F}_9$.
   On construit donc $\mathbb{F}_9$ comme le quotient $\mathbb{F}_3[X]/(X^2+1)$. Le corps $\mathbb{F}_9 = \mathbb{F}_3[i]$ avec $i^2 = -1$. Le nombre $\alpha = a + ib$ ($(a,b) \in \mathbb{F}_3^2$) est racine de $X^4 + X^2 + 1$ est racine si et seulement si
   $$(a+ib)^4 + (a+ib)^2 + 1 = 0$$
   .
   Cela revient à $(a+ib)(a-ib) + (a^2 + 2iab - b^2) + 1 = a^2 + 1 + 2iab = 0$. Nécessairement, $a^2+1 = 0$, ce qui est impossible.
   On fait de même avec $X^4 - X^2 - 1$, et on obtient que $X^4 \pm X^2 - 1$ n'ont pas de racine dans $\mathbb{F}_9$.
3. En déduire qu'ils sont irréductibles dans A.
   Supposons ces polynômes F non irréductibles. Soit, il se factorise par un polynôme de degré 1 (Impossible car pas de racine dans $\mathbb{F}_3$). Soit il se factorise par un polynôme de degré 2 irréductible Q. Alors il existe R de degré 2 tel que $F = QR$. Ainsi, α la classe de X dans $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(Q)$ est racine de F. Or cela est exclu d'après la question précédente. Les polynômes sont irréductibles.
4. Montrer que P est sans facteur carré.
   On calcule $P'(X) = 8X^7$ qui est premier avec P (Bézout). Ainsi, P n'a pas de 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 $\mathbb{F}_3$.
   Le polynôme P par factorialité de l'anneau des polynômes s'écrit $\prod_{i=1}^{s} P_i$ avec P_i irréductibles sans carré (valuation =1) d'après la question précédente.
   [Théorème des restes chinois]
   On construit la surjection canonique $\tilde{\psi} := \prod_i \psi_i : A \to \prod_i A/(P_i)$. Le noyau de $\tilde{\psi}$ est engendré par par un polynôme par principalité de A qui doit être divisé par tous les P_i. Ainsi, $\ker\tilde{\psi} = (P)$ et le théorème de factorisation donne l'existence de ψ.
   De plus, P_i étant irréductible, $A/(P_i)$ est une extension finie du corps $\mathbb{F}_3$.
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.
   Montrons que $y \mapsto y^3$ sur A est linéaire (l'application est trivialement définie puisque $A/(P)$ est un anneau). L'anneau A est de caractéristique 3. Ainsi, soient $(y_1, y_2) \in A^2$ et $\lambda \in \mathbb{F}_3$, $(y_1 + \lambda y_2)^3 = y_1^3 + 3\lambda y_2 y_1^2 + 3\lambda^2 y_2^2 y_1 + + \lambda^3 y_1 = y_1^3 + \lambda^3 y_2^3 = y_1^3 + \lambda y_2^3$. La propriété d'être linéaire passe trivialement au quotient.
7. On note $\psi(X^6 + X^2) = (T_1, \ldots, T_s)$. Montrer que $T_i \in \mathbb{F}_3$, pour tout $i = 1, \ldots, s$.
   On pose $\psi(X^6 + X^2) = (T_1, \ldots, T_s)$. Alors, on a $\psi(\varphi(X^6 + X^2)) = (T_1^3 - T_1, \ldots, T_s^3 - T_s)$. Or $\varphi(X^6 + X^2) = X^{18} + X^6 - X^6 - X^2 = X^{16+2} - X^2 = 0$. Donc pour tout $T_i \in K_i$, $T_i^3 - T_i$. Ce sont les racines du polynôme de degré 3 $Y^3 - Y$ qui a pour seules racines les éléments de $\mathbb{F}_3$ sur K_i. On obtient $T_i \in \mathbb{F}_3$.
8. En déduire que $P = \prod_{\alpha \in \mathbb{F}_3} \operatorname{pgcd}(P, X^6 + X^2 - \alpha)$.
   On voit que $\prod_{\alpha \in \mathbb{F}_3} \operatorname{pgcd}(P, X^6 + X^2 - \alpha)$ divise P, puisque chaque terme du produit est un diviseur de P et ces diviseurs sont premiers entre eux d'après Bézout. En effet,
   $$(X^6 + X^2 - \alpha) - (X^6 + X^2 - \alpha') = (\alpha' - \alpha)$$

inversible si non nul.
Enfin, P divise le produit puisque tout ses facteurs irréductibles P_i le divisent. En effet, $\psi(X^6 + X^2) = T_i \in \mathbb{F}_3 \subset A/(P_i)$ et donc pour $\alpha = T_i$, $X^6 + X^2 - \alpha$ est divisible par P_i.

9. Déduire de la formule précédente que $P(X) = (X^4 - X^2 - 1)(X^4 + X^2 - 1)$.
On pourrait simplement effectuer le calcul ;)
Sinon il faut calculer le pgcd de P et (X^6+X^2-1) par l'algorithme d'Euclide qui donne X^4+X^2-1.