Université Claude Bernard Lyon 1 — Anneaux et Corps - L3
Semestre de printemps 2023-2024

Examen 1 – Durée 75 min – le mardi 5 mars 2024

Les documents, les téléphones et les calculatrices ne sont pas autorisés.
La notation tiendra compte du soin apporté à la rédaction des réponses.
BIEN INDIQUER SON NUMÉRO DE GROUPE DE TD SUR LA COPIE (A,B ou Z)
L'énoncé comporte quatre exercices.

Exercice 1. Un réseau de $\mathbb{C}$.
Soit $j = e^{\frac{2i\pi}{3}} \in \mathbb{C}$ tel que $1 + j + j^2 = 0$. Posons

$$\mathbb{Z}[j] = \{a + jb \ : \ a, b \in \mathbb{Z}\}.$$

1. Montrer que $\mathbb{Z}[j]$ est un sous anneau de $\mathbb{C}$.
   Contient $0 = 0 + 0j$ et $1 = 1 + 0j$. Stable par $+$: évident. Stable par $\times$ car

$$(a + jb)(c + jd) = ac - (1 + j)bd + j(bc + ad) = (ac - bd) + (bc - bd + ad)j \in \mathbb{Z}[j].$$

2. Soit $|\ |$ le module complexe. Soit $z = a + jb \in \mathbb{Z}[j]$ (avec a et b dans $\mathbb{Z}$).
   Montrer que
$$|z|^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2.$$
   Calcul immédiat.
3. Déterminer l'ensemble $\mathbb{Z}[j]^\times$ des éléments inversibles de $\mathbb{Z}[j]$.
   Soit $z = a + bj$ inversible. Alors $z\bar{z}$ est inversible dans $\mathbb{Z}$. Donc avec la question précédente $\left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2 = \pm 1$. En particulier $3b^2 \leq 4$ donc $b = 0$ ou ± 1. Pour chacune de ces 3 valeurs ou trouve a. On obtient
$$\mathbb{Z}[j]^\times \subset \{\pm 1, \pm j, \pm \bar{j}\}.$$
   Pour chacun de ces 6 éléments on trouve facilement un inverse grâce aux relations $1 + j + j^2 = 1 + \bar{j} + \bar{j}^2 = 0$ et $j^2 = \bar{j}$:
$$1 = 1^2 = (-1)^2 = j.\bar{j} = -j.(-\bar{j}).$$
4. Montrer que $\mathbb{Z}[j]$ est euclidien pour le stathme $|\ |^2$. *On écrit $z_1/z_2 = x + jy$. Il existe a et b dans $\mathbb{Z}$ tels que $2|x - a| \leq 1$ et $2|y - b| \leq 1$. Posons $q = a + jb$ et $r = z_1 - q * z_2$. Grâce au calcul de la question 2, on montre que $|r|^2 \leq \frac{12}{16}\frac{1}{|z_2|^2}$. Ce qui conclut.*

Exercice 2. Polynômes.

1. Soit $S = X^4 + 5X^2 - 8X + 9$. Pour tout nombre premier p, on notera S_p le réduit modulo p de S dans $\mathbb{Z}/p\mathbb{Z}[X]$
   (a) Décomposer en facteurs irréductible S_2 dans $\mathbb{Z}/2\mathbb{Z}[X]$. *On a $S_2 = (X^2 + X + 1)^2$ et $X^2 + X + 1$ est irréductible car de degré 2 sans racine.*
   (b) Décomposer en facteurs irréductible S_3 dans $\mathbb{Z}/3\mathbb{Z}[X]$.
   On a $S_3 = X(X^3 - X + 1)$ et $X^3 - X + 1$ est irréductible car de degré 3 sans racine (vérification des 3 valaure $0, \pm 1$).
   (c) En déduire que S est irréductible dans $\mathbb{Q}[x]$.
   D'après Gauss, il sufficit de montrer que S est irréductible dans $\mathbb{Z}[X]$. Supposons $S = AB$ avec A et B non constants dans $\mathbb{Z}[X]$. Alors A et B (quitte à prendre $-A$ et $-B$) sont unitaires. Alors, en réduisant modulo 2, on obtient $\deg(A) = \deg(B) = 2$. En réduisant modulo 3, on obtient $\{\deg(A), \deg(B)\} = \{1, 3\}$. Contradiction.

2. Soient
$$P = X^4 + 2X^3 + 5X^2 + 4X + 4 \quad \text{et} \quad Q = X^3 - 2X^2 - X - 6$$
deux polynômes de $\mathbb{Q}[X]$.
   (a) Calculer le PGCD de P et Q. *On a $P-(X+4)Q = 14(X^2+X+2)$ et $Q = (X-3).(X^2+X+2)$. L'algo d'Euclide donne alors $A \wedge B = X^2 + X + 2$.*
   (b) Trouver une relation de Bézout pour ces deux polynômes. *On a vu que*
$$\frac{1}{14}P - \frac{X+4}{14} = X^2 + X + 2.$$
   (c) Donner la décomposition en facteurs irreductibles de P et Q dans $\mathbb{Q}[X]$. *Tout d'abord X^2+X+2 est irréductible car de degré 2 et sans racine dans $\mathbb{Q}$ (et même dans $\mathbb{R}$ car $\Delta = -7$).*
   Donc $Q = (X-3).(X^2+X+2)$ est la décomposition en irréductible de Q.
   En divisant P par X^2+X+2, on constate que $P = (X^2+X+2)^2$.

Exercice 3. Éléments non-inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$**.** Soit $n \in \mathbb{N}$. On dit que n est primaire lorsqu'il existe un nombre premier p et $\alpha \in \mathbb{N}^*$ tel que $n = p^\alpha$. Soit $n \in \mathbb{N}$ tel que $n > 1$ et n ne soit pas primaire.

1. Établir qu'il existe deux entiers, que l'on notera k et l, tels que $n = kl$, $1 < k < l$ et $k \wedge l = 1$. (On pourra utiliser la décomposition en produit de facteur premiers de n.)
2. Montrer alors que $(k+l) \wedge n = 1$.
3. Établir également que : $\overline{k}$ et $\overline{l}$ ne sont pas inversibles dans $\mathbb{Z}/n\mathbb{Z}$.
4. Conclure que l'ensemble des éléments non-inversibles de $\mathbb{Z}/n\mathbb{Z}$ ne forme pas de sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exercice 4. Anneau des séries formelles.
Considérons l'ensemble des séries formelles
$$\mathbb{R}[[X]] := \left\{ \sum_{n\geq 0} a_k X^k \mid a_k \in \mathbb{R} \right\}.$$
L'ensemble $\mathbb{R}[[X]]$ est muni de l'addition terme à terme et de la multiplication donnée par le produit de Cauchy :
$$\left(\sum_{k\geq 0} a_k X^k\right)\left(\sum_{k\geq 0} b_k X^k\right) = \sum_{n\geq 0}\left(\sum_{i=0}^{n} a_i b_{n-i}\right) X^n.$$
On admetra qu'alors $\mathbb{R}[[X]]$ est un anneau.
Dans la suite $P = \sum_{n\geq 0} a_k X^k$.

1. Montrer que $1 - X$ est inversible dans $\mathbb{R}[[X]]$ en exibant son inverse. *Posons $Q = \sum_{k\geq 0} X^k$. On a*
$$Q.(1-X) = \sum_{k\geq 0} X^k - \sum_{k\geq 0} X^{k+1} = 1.$$
2. Soit $P \in \mathbb{R}[[X]]$ tel que $a_0 = 0$. Montrer que $1 - P$ est inversible. *Même démonstration avec $Q = \sum_{k\geq 0} P^k$.*
3. Montrer que P est inversible si et seulement si $a_0 \neq 0$. *Si $a_0 \neq 0$, on écrit $P = a_0 P_1$. Alors P_1 est inversible par la question précédente. Donc P l'est.*
   Réciproquement, si $PQ = 1$, en regardant le coefficient de X^0, on obtient $a_0 b_0 = 1$. Donc $a_0 \neq 0$.
4. Pour $P \in \mathbb{R}[[X]]$ non nul, on pose $v(P) = \min\{k : a_k \neq 0\}$.
   (a) Soit $P \in \mathbb{R}[[X]]$ et $v \in \mathbb{N}$. Montrer que $v(P) = v$ si et seumement s'il existe $P_1 \in \mathbb{R}[[X]]$ inversible tel que $P = X^v P_1$. *Si $v(P) = v$, $P = \sum_{k\geq v} a_k X^k = X^v \sum_{k\geq v} a_k X^{k-v}$. Le coefficient constant de $P_1 = \sum_{k\geq v} a_k X^{k-v}$ est non nul. £Il est donc inversible.*
   Réciproquement, si $P_1 = \sum_{k\geq v} a_k X^k$ avec $a_0 \neq 0$ alors le premier terme non nul de $X^v P_1$ est $a_0 X^v$. Donc $v(P) = v$.

(b) En déduire que, pour tout $(P, Q) \in \mathbb{R}[[X]]^2$, $v(PQ) = v(P) + v(Q)$.
On écrit $P = X^{v(P)} P_1$ et $Q = X^{v(Q)} Q_1$ comme ci-dessus. Alors $PQ = X^{v(P)+v(Q)} P_1 Q_1$. Comme $P_1 Q_1$ est inversible, on peut conclure.

(c) Montrer que, pour tout $(P, Q) \in \mathbb{R}[[X]]^2$, $v(P + Q) \geq \min(v(P), v(Q))$.
C'est évident.
Donner un exemple pour lequel l'inégalité est stricte.
On peut prendre $P = 1 + X$ et $Q = -1 + X$. Alors $v(P) = v(Q) = 0$ et $v(P + Q) = 1$.

5. Montrer que l'ensemble des éléments non inversibles de $\mathbb{R}[[X]]$ forme un idéal maximal $\mathfrak{M}$ de $\mathbb{R}[[X]]$.
6. Montrer que $\mathfrak{M}$ est principal.
7. Montrer que tout idéal de $\mathbb{R}[[X]]$ est principal.
8. Montrer que $\mathbb{R}[[X]]$ est un anneau euclidien pour le stathme v.