Université Claude Bernard - Lyon 1 Semestre de printemps 2022-2023

Anneaux et Corps - L3 Durée : 1h15

Devoir numéro 1

Les exercices 2 et 3 constituent un problème, vous pouvez (et devez) réutiliser les résultats des exercices précédents.

Exercice 1 (Questions de cours)**.**

1. Rappelez le théorème de factorisation pour un anneau euclidien.
2. Donner la définition d'anneau euclidien.
3. Soit A un anneau et $a \in A$, montrer que si (a) est maximal, pour tout $q \in A$ tel que $a \nmid q$ il existe $(u, v) \in A^2$ tel que $au + qv = 1$.

Exercice 2 (Anneaux euclidiens et presque euclidien)**.**

1. Montrer que, si A est un anneau euclidien, il existe $x \in A$ non inversible, tel que la restriction à $A^* \cup \{0\}$ de la projection canonique $\pi : A \to A/(x)$ est surjective. *On pourra considérer un x qui minimise la norme euclidienne.*

   Correction : (Cas du corps, x=0) Soit $x \in A$ non inversible qui minimise $\nu(x)$ (existe si on n'est pas sur un corps). Soit $z \in A/(x)$, il existe $y \in A$ tel que $\pi(y) = z$. Alors, la division euclidienne par x donne l'existence de $(q, r) \in A^2$ vérifiant $y = qx + r$ avec $0 \leq \nu(r) < \nu(x)$. L'élément r est donc inversible et $\pi(r) = \pi(y)$.

2. On dit que A est *presque euclidien* s'il est intègre et s'il existe une fonction $N : A \to \mathbb{Z}$ telle que $\forall (a, b) \in A \times (A - \{0\})$, il existe $(q, r) \in A^2$ tels que :

   — $N(x) < N(2x)$ $\forall x \in A$

   — $r = 0$ ou $N(r) < N(b)$.

   — $a = bq + r$ ou $2a = bq + r$.

   Montrer que, si A est presque euclidien et (2) est maximal dans A alors A est principal.

   Correction :((Même preuve que euclidien implique principal) Soit I un idéal de A, on considère un élément $x \in I$ non nul qui minimise N. Soit $y \in I$, on utilise la presque division euclidienne de y par x, pour avoir l'existence de (q, r) tel que :

   — $r = 0$ ou $N(r) < N(b)$.

   — $y = bx + r$ ou $2y = bx + r$.

   Or, $y - bx$ et $2y - bx$ sont dans I. Donc r est dans I et par minimalité $N(x)$, on a $r = 0$ et ainsi, $y = bx$ ou $2y = bx$.

   Si $y = bx$, c'est fini.

   Si $2y = bx$, et $2 \nmid b$ (sinon cela est également fini) (2) étant maximal, il existe $(u, v) \in A$ tel que $2u + bv = 1$. En multipliant par x, $2xu + 2vy = x$ et donc 2 divise x. En appelant $x' = 2xu + 2vy$, on a x' appartient à I avec $N(x') < N(x)$. Ce qui contredit la minimalité de x.

Exercice 3. (Propriétés de $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$)
On pose $A := \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ et $\alpha = \frac{1+i\sqrt{19}}{2}$.

1. Montrer que A est un anneau intègre dont les éléments sont $\{x + y\alpha, (x, y) \in \mathbb{Z}^2\}$.
   Correction : Il suffit de montrer que c'est un sous-anneau de l'anneau intègre $\mathbb{C}$.
2. Montrer que A est isomorphe à $\mathbb{Z}[X]/(X^2 - X + 5)$?
   Correction : On définit le morphisme (d'évaluation) d'anneau (clairement surjectif) :
   $\eta : \mathbb{Z}[X] \to \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$,
   $$\eta(P) = P(\alpha) \ .$$
   D'après le théorème de factorisation on obtient un isomorphisme
   $$\hat{\eta} : \mathbb{Z}[X]/\ker(\eta) \to \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$$
   .
   On montre que $\ker(\eta) = (X^2 - X + 5)$. Soit $Q \in \ker \eta$, le reste de la division euclidienne de Q par $X^2 - X + 5$ est un polynôme de degré au plus 1. Il est aussi annulateur de α. Or cela est impossible car α n'est pas un nombre rationnel.
3. Quel est la signature de la forme quadratique sur $\mathbb{R}^2$ définie par $q(a, b) = a^2 + ab + 5b^2$.
4. Quels sont les inversibles de A ?
   Correction : Soit z inversible. Alors, il existe $z' \in A$ tel que $zz' = 1$. La norme de $|z|^2|z'|^2 = |zz'|^2 = 1$. Or $|z|^2$ est entier, donc égal à 1. Si $z = a + b\alpha$, alors $|z|^2 = a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{19}{4}b^2$, or $\frac{19}{4}b^2 > 1$ si $b \neq 0$. Donc z inversible implique $b = 0$ et donc $a = \pm 1$.
   Les inversibles de A sont ± 1.
5. Nous allons en déduire que A n'est pas euclidien.
   (a) Supposons que A est euclidien. Montrer que l'élément x de l'exercice 2 1) fait de $A/(x)$ un corps. Quel est-il ?
   Correction : On utilise la question 1 de l'exercice 2 et ses notations. On suppose par l'absurde que A est euclidien. Alors, il existe x non inversible tel que $A/(x)$ est l'image de la restriction de π à $A^* \cup \{0\}$. On a montrer que $A^* \cup \{0\}$ est l'ensemble $\{-1, 0, 1\}$, L'image de celui-ci par π (qui est $A/(x)$) est soit le corps à 3 éléments, soit le corps à 2 éléments.
   (b) Monter que $X^2 - X + 5$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.
   Correction (il n'a pas de racines)
   (c) En déduire que A n'est pas euclidien.
   Correction : On considère β l'image de α par le morphisme π de l'exercice 2.1. Cet élément annule le polynôme $X^2 - X + 5$. C'est impossible car $A/(x)$ est $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$.
6. Nous allons montrer que A est toutefois principal.
   (a) Montrer que $\mathbb{Z}[X]/(2, X^2 - X + 5)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}[X]/(X^5 - X + 5)$.
   (b) En déduire que l'idéal (2) est maximal.
   Correction : (Une preuve très rapide revient à (re)questionner $\mathbb{Z}[X]/(X^2 - X + 5)$ par l'idéal (2), l'irréductibilité de $X^2 - X + 5$ sur $\mathbb{Z}/2\mathbb{Z}$ termine la preuve). Sinon, on cherche à montrer que $A/(2)$ est un corps, et que pour $z \in A$ non nul, il existe $(u, v) \in A^2$, tel que $2u + zv = 1$.

On pose $z = (a+b\alpha)$, $u = (a'+b'\alpha)$ et $v = (a''+b''\alpha)$. On obtient alors un système d'équation dont les variables sont entières.

$$aa' - 5bb' = 1 - 2a''$$

$$ba' + (a-b)b' = -2b''$$

Cette équation sur (a', b') présente une solution sur $\mathbb{Z}_2$ car le déterminant est $a^2 + ab + 5b^2$ non nul si $2 \nmid z$. Nous prenons : $a' = a + b$ et $b' = -b$. Les conditions sur la parités implique qu'il existe (a'', b'') qui conviennent.

(c) Montrer que

$$\forall (a,b) \in [0, \frac{1}{2}] \times [0, \frac{1}{3}], |a + b\alpha|^2 < 1 \ .$$

(d) Montrer que A est principal en utilisant l'exercice 2.

Correction : (Même idée que pour les entiers de Gauss)

Nous allons montrer que A est presque euclidien et comme (2) est maximal, A sera principal.

On prouve l'indication : Soit $(a,b) \in \mathbb{R}^2$Si $(|a|, |b|) \in [0, \frac{1}{2}] \times [0, \frac{1}{3}]$,

$$|a + b\alpha|^2 = a^2 + ab + 5b^2 \leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} \ .$$

Soit $(y, x) \in A^2$, sur $\mathbb{C}$, on calcule $z = \frac{y}{x} = a + \alpha b$ et nous allons montrer que z ou $2z$ est à une norme inférieure stricte à 1 de A. En effet, soit $n = \lfloor a \rfloor + \alpha \lfloor b \rfloor \in A$, on aura alors $y = xn + r$ ou $2y = 2xn + r$ avec $|r| < |x|$.

— Si $l = a' + \alpha b'$ vérifie $0 \leq b' \leq \frac{1}{3}$ alors d'après le lemme $|l| < 1$ ou $|l - 1| < 1$.

— Si $l = a' + \alpha b'$ vérifie $\frac{2}{3} \leq b' \leq 1$ alors d'après le lemme $|l - \alpha| < 1$ ou $|l - (1 + \alpha)| < 1$.

— Si $l = a' + \alpha b'$ vérifie $\frac{1}{3} \leq b' \leq \frac{2}{3}$ alors d'après le lemme $|2l - \alpha| < 1$ ou $|2l - (1 + \alpha)| < 1$ d'après le cas précédent.