Correction du Contrôle Continu du 21/10/25
"Algèbre 1 - HAX708X"

Questions isolées

a. On rappelle qu'un polynôme $P = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X] - \{0\}$ est dit *primitif* si $\mathrm{pgcd}(a_0, \ldots, a_n) = 1$. Montrer que le produit de deux polynômes primitifs est un polynôme primitif.

Voir le cours.

b. Dans l'anneau euclidien $\mathbb{Z}[i]$:

(1) Effectuer la division euclidienne de $8 + 5i$ par $2 + 3i$.

On a
$$\frac{8+5i}{2+3i} = \frac{(8+5i)(2-3i)}{13} = \tfrac{31}{13} - \tfrac{14}{13}i = 2 - i + \tfrac{5}{13} - \tfrac{1}{13}i,$$
donc $8 + 5i = (2-i)(2+3i) + 1 + i$ avec $|1+i| < |2+3i|$.

(2) Calculer le pgcd de $8 + 5i$ par $2 + 3i$.

D'après le calcul précédent, on voit que $pgcd(8+5i, 2+3i) = pgcd(2+3i, 1+i)$. D'autre part, la division euclidienne de $2+3i$ par $1+i$, $2+3i = 2(1+i)+i$, montre que $pgcd(2+3i, 1+i) = i$ et i est un inversible de $\mathbb{Z}[i]$. Conclusion : $pgcd(8+5i, 2+3i) = 1$.

c. On considère l'anneau de polynômes $\mathbb{Z}/5\mathbb{Z}[X]$, ainsi que le quotient $\mathbb{K} := \mathbb{Z}/5\mathbb{Z}[X]/(X^2+X+1)$. Montrer que $\mathbb{K}$ est un corps. Quel est son cardinal ?

Le polynôme $X^2 + X + 1$ n'admet pas de racine sur le corps $\mathbb{Z}/5\mathbb{Z}$. Cela implique que $X^2 + X + 1$ est irréductible dans $\mathbb{Z}/5\mathbb{Z}[X]$, et donc que le quotient $\mathbb{K} := \mathbb{Z}/5\mathbb{Z}[X]/(X^2+X+1)$ est un corps, contenant $\mathbb{Z}/5\mathbb{Z}$ comme sous-corps. La famille $\{\bar{1}, \bar{X}\}$ est une base de $\mathbb{K}$, vu comme $\mathbb{Z}/5\mathbb{Z}$-espace vectoriel. Cela montre que $\mathbb{K} \simeq (\mathbb{Z}/5\mathbb{Z})^2$: ainsi le cardinal de $\mathbb{K}$ est 25.

d. Décrire tous les morphismes de groupes $\varphi : \mathbb{Z}/80\mathbb{Z} \to \mathbb{Z}/50\mathbb{Z}$.

Comme $\bar{1}$ engendre le groupe $\mathbb{Z}/80\mathbb{Z}$, le morphisme φ est entièrement déterminé par $\varphi(\bar{1})$. Soit $\alpha \in \{0, \ldots, 49\}$ tel que $\varphi(\bar{1}) = \alpha \bmod 50$. On a
$$0 \bmod 50 = \varphi(\overline{80}) = 80\alpha \bmod 50.$$
Cela implique que 5 divise α, c'est à dire $\alpha = 5\beta$ avec $\beta \in \{0, \ldots, 9\}$. Maintenant, pour tout $\beta \in \{0, \ldots, 9\}$, on vérifie que l'application $\varphi_\beta : \mathbb{Z}/80\mathbb{Z} \to \mathbb{Z}/50\mathbb{Z}$, $\bar{k} \mapsto 5k\beta \bmod 50$, est bien définie, et est un morphisme de groupe.

e. Est-ce que $\mathbb{Z}[X]$ possède un idéal qui n'est pas un $\mathbb{Z}[X]$-module libre ?

L'idéal $I \subset \mathbb{Z}[X]$ engendré par 2 et X, n'est pas principal. Ainsi, I n'est pas un $\mathbb{Z}[X]$-module libre.

Exercice 1

(1) Déterminer la torsion du groupe abélien $\mathbb{R}/\mathbb{Z}$.

Pour tout $x \in \mathbb{R}$, la classe $x \bmod \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ est de torsion si et seulement si il existe $k \geq 1$ tel que $kx \bmod \mathbb{Z} = 0 \bmod \mathbb{Z}$. Cette condition est équivalente au fait que $x \in \mathbb{Q}$. Ainsi, la torsion du groupe abélien $\mathbb{R}/\mathbb{Z}$ est $\mathbb{Q}/\mathbb{Z}$.

(2) Montrer que, $\forall n \geq 1$, il existe un unique sous-groupe cyclique de $\mathbb{R}/\mathbb{Z}$ d'ordre n.

Si $H \subset \mathbb{R}/\mathbb{Z}$ est un sous-groupe de cardinal n, alors H est contenu dans

$$H_n := \{y \in \mathbb{R}/\mathbb{Z}, ny = 0\}.$$

Maintenant, il suffit de voir que H_n est le sous-groupe cyclique de $\mathbb{R}/\mathbb{Z}$ d'ordre n, engendré par $\frac{1}{n} \bmod \mathbb{Z}$.

Exercice 2

Soit $\alpha = \frac{1}{2}\left(1 + i\sqrt{19}\right)$. On note $\mathbb{Z}[\alpha]$ le sous-anneau de $\mathbb{C}$ engendré par 1 et α.

(1) Déterminer un polynôme de degré 2 à coefficients entiers qui annule α. En déduire que tous les éléments de $\mathbb{Z}[\alpha]$ sont de la forme $x + y\alpha$, $x, y \in \mathbb{Z}$.

On vérifie que $\alpha^2 - \alpha + 5 = 0$. Comme $X^2 - X + 5$ est un polynôme unitaire de $\mathbb{Z}[X]$, pour tout $P \in \mathbb{Z}[X]$, il existe $Q, R \in \mathbb{Z}[X]$, avec $\deg(P) \leq 1$, tels que $P(X) = Q(X)(X^2 - X + 5) + R(X)$. Ainsi $P(\alpha)$ est égal à $R(\alpha) = x + y\alpha$ avec $x, y \in \mathbb{Z}$.

(2) Montrer qu'il n'existe pas de morphisme d'anneaux $\mathbb{Z}[\alpha] \to \mathbb{Z}/3\mathbb{Z}$.

Si $\varphi : \mathbb{Z}[\alpha] \to \mathbb{Z}/3\mathbb{Z}$ un morphisme d'anneau, alors $\varphi(\alpha)$ est une racine du polynôme $X^2 - X + 5$ dans $\mathbb{Z}/3\mathbb{Z}$, ce qui est impossible.

(3) Montrer que l'idéal engendré par 2 est maximal dans $\mathbb{Z}[\alpha]$.

Comme l'anneau $\mathbb{Z}[\alpha]$ est isomorphe au quotient $\mathbb{Z}[X]/(X^2 - X + 5)$, on voit que

$$\mathbb{Z}[\alpha]/(2) \simeq \mathbb{Z}[X]/(2, X^2 - X + 5) \simeq \mathbb{Z}/2\mathbb{Z}[X]/(X^2 - X + 5).$$

Dans l'anneau $\mathbb{Z}/2\mathbb{Z}[X]$, le polynôme $X^2 - X + 5 = X^2 + X + 1$ est irréductible car il n'admet pas de racines dans $\mathbb{Z}/2\mathbb{Z}$. On a donc montré que le quotient $\mathbb{Z}[\alpha]/(2)$ est un corps : l'idéal engendré par 2 est maximal dans $\mathbb{Z}[\alpha]$.