

Licence – Mathématiques
Algèbre 2

COURS À DISTANCE – DM1

Exercice 1. Soit $(G, +)$ un groupe commutatif. On note $\text{End}(G)$ l'ensemble des endomorphismes de G sur lequel on définit la loi $+$ par $f + g : \begin{cases} G & \rightarrow & G \\ x & \mapsto & f(x) + g(x) \end{cases}$.

Étant donné que G est un groupe, on parle ici d'endomorphismes de groupe.

1. Montrer que $(\text{End}(G), +, \circ)$ est un anneau unitaire.

La loi $+$ sur $\text{End}(G)$ est associative et commutative car la loi $+$ sur G l'est. La fonction constante égale au neutre 0_G de G est un endomorphisme de G qui est un élément neutre pour la loi $+$. Si $f \in \text{End}(G)$, alors le morphisme g défini par $g(x) = -f(x)$ pour tout $x \in G$ est l'inverse de f . Ainsi tout élément de $\text{End}(G)$ admet un inverse, et $(\text{End}(G), +)$ est un groupe abélien.

La loi de composition est clairement associative. Pour la distributivité, on remarque que

$$f \circ (g + h)(x) = f(g(x) + h(x)) = f(g(x)) + f(h(x)) = f \circ g(x) + f \circ h(x)$$

où la deuxième égalité est due au fait que f est un morphisme de groupe ; donc $f \circ (g+h) = f \circ g + f \circ h$. De même,

$$(f + g) \circ h(x) = (f + g)(h(x)) = f(h(x)) + g(h(x)) = f \circ h(x) + g \circ h(x)$$

implique $(f + g) \circ h = f \circ h + g \circ h$. Finalement, $(\text{End}(G), +, \circ)$ est un anneau. Il est unitaire d'unité le morphisme identité.

2. Déterminer l'ensemble des inversibles de $\text{End}(G)$.

Pour $f \in \text{End}(G)$, f est inversible s'il existe $g \in \text{End}(G)$ tel que $f \circ g = g \circ f = \text{Id}_G$, c'est-à-dire si f est bijectif et que son inverse est aussi un morphisme. Or l'inverse d'un morphisme bijectif est toujours un morphisme. Donc $(\text{End}(G))^\times = \text{Aut}(G)$.

3. On prend $G = \mathbb{R}^2$. L'anneau $\text{End}(G)$ est-il commutatif ? Est-il intègre ?

Les applications

$$f : \begin{cases} \mathbb{R}^2 & \rightarrow & \mathbb{R}^2 \\ (x, y) & \mapsto & (x, 0) \end{cases} \quad \text{et} \quad g : \begin{cases} \mathbb{R}^2 & \rightarrow & \mathbb{R}^2 \\ (x, y) & \mapsto & (y, 0) \end{cases}$$

sont des endomorphismes de $\mathbb{R}^2$. On a $f \circ g = g$ et $g \circ f = 0$. Ainsi $f \circ g \neq g \circ f$, donc $\text{End}(\mathbb{R}^2)$ n'est pas commutatif, et $g \circ f = 0$ avec $f \neq 0$ et $g \neq 0$, donc $\text{End}(\mathbb{R}^2)$ n'est pas intègre.

4. Même question avec $G = \mathbb{Z}$.

Soit $f \in \text{End}(\mathbb{Z})$. Notons $n = f(1)$. Comme f est un morphisme, pour tout $k \in \mathbb{Z}$, on a $f(k) = f(k.1) = k.f(1) = k.n$. Donc $\text{End}(\mathbb{Z})$ est l'ensemble des applications μ_n définies par $\mu_n(k) = kn$ avec $n \in \mathbb{Z}$. Notons que μ_n est le morphisme trivial —le neutre de $\text{End}(\mathbb{Z})$ — si et seulement si $n = 0$.

Pour $m, n \in \mathbb{Z}$, on a $\mu_n \mu_m = \mu_m \mu_n = \mu_{mn}$. Donc $\text{End}(\mathbb{Z})$ est commutatif. De plus, si $\mu_n \mu_m = 0$, alors $\mu_{nm} = 0$ implique $nm = 0$, donc soit $n = 0$ et $\mu_n = 0$, soit $m = 0$ et $\mu_m = 0$. Donc $\text{End}(\mathbb{Z})$ est intègre.

Exercice 2.

1. Déterminer les diviseurs de zéro de l'anneau $\mathbb{Z}/63\mathbb{Z}$.

Notons déjà que la décomposition de 63 en produit de facteurs premiers est $63 = 3 \times 3 \times 7$.

Si $k \in \mathbb{Z}$ est divisible par 3, alors $k = 3\ell$ avec $\ell \in \mathbb{Z}$ et on a $\overline{21k} = \overline{63\ell} = \overline{0}$; or $\overline{21} \neq \overline{0}$, donc $\overline{k}$ est un diviseur de zéro. Si $k \in \mathbb{Z}$ est divisible par 7, on raisonne de la même façon, en remplaçant 21 par 9, pour conclure que $\overline{k}$ est un diviseur de zéro.

Soit maintenant $k \in \mathbb{Z}$ qui n'est divisible ni par 3 ni par 7. Alors k est premier à 63, donc il existe des entiers u et v tels que $uk + 63v = 1$. On en déduit que $\overline{uk} = \overline{1}$, donc que $\overline{k}$ est inversible dans $\mathbb{Z}/63\mathbb{Z}$. Or un élément inversible ne peut pas être un diviseur de zéro.

Finalement, les diviseurs de zéro dans $\mathbb{Z}/63\mathbb{Z}$ sont les classes des entiers divisibles par 3 ou 7 (l'énumération n'est pas demandée, mais la voici à titre indicatif : $\overline{0}, \overline{3}, \overline{6}, \overline{7}, \overline{9}, \overline{12}, \overline{14}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}, \overline{28}, \overline{30}, \overline{33}, \overline{35}, \overline{36}, \overline{39}, \overline{42}, \overline{45}, \overline{48}, \overline{49}, \overline{51}, \overline{54}, \overline{56}, \overline{57}, \overline{60}$).

2. Un élément a d'un anneau est nilpotent s'il existe un entier $k > 0$ tel que $a^k = 0$. Déterminer les éléments nilpotents de $\mathbb{Z}/63\mathbb{Z}$.

Soit $a \in \mathbb{Z}$. En utilisant la décomposition en facteurs premiers de a , on peut écrire $a = 3^\alpha 7^\beta b$ avec $\alpha, \beta, b \in \mathbb{Z}$ et b premier à 3 et 7. Alors, pour $k \in \mathbb{Z}$, $a^k = 3^{k\alpha} 7^{k\beta} b^k$. Ainsi, a^k est divisible par 63 si et seulement si $k\alpha \geq 2$ et $k\beta \geq 1$. C'est vrai pour un certain k si et seulement si $\alpha > 0$ et $\beta > 0$, c'est-à-dire si 21 divise a . Ainsi les éléments nilpotents de $\mathbb{Z}/63\mathbb{Z}$ sont les classes des entiers divisibles par 21, à savoir $\overline{0}, \overline{21}$ et $\overline{42}$.