Travaux Dirigés – Exercices. Série I

Semaine I. 17/09/07 – 21/09/07

A– Groupes abéliens, anneaux d'endomorphismes.

Soit $(G, +)$ un groupe abélien, noté additivement. On appelle endomorphisme de G un homomorphisme de groupes $G \to G$. On note $End(G)$ l'ensemble des endomorphismes de G.

1. Montrer que $End(G)$ est muni de deux lois $+$, donnée par $(\phi_1 + \phi_2)(g) = \phi_1(g) + \phi_2(g)$ (ϕ_1, $\phi_2 \in End(G)$, $g \in G$), et $\circ$, qui est la composition des applications. Montrer que $(End(G), +, \circ)$ est un anneau. [Pointer le ou les endroit(s) où la commutativité de la loi sur G est utile.]
2. Montrer que l'anneau $End(\mathbb{Z})$ est isomorphe à $\mathbb{Z}$.
3. Quel est l'anneau des endomorphismes du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$?
4. Déterminer l'anneau $(End(\mathbb{Z}^n), +, \circ)$. Vérifier qu'il existe beaucoup d'endomorphismes nilpotents sur le groupe additif $\mathbb{Z}^2$. En déduire que les groupes additifs $\mathbb{Z}$ et $\mathbb{Z}^2$ ne sont pas isomorphes.
5. Donner au moins trois autres raisons qui montrent que les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$ ne sont pas isomorphes.
6. Soit $(A, +, \cdot)$ un anneau. En particulier $(A, +)$ est un groupe abélien. Pour $a \in A$, notons m_a l'application $A \to A$ qui à x associe $a \cdot x$. Montrer que m_a est un endomorphisme du groupe abélien $(A, +)$, puis que l'application $a \mapsto m_a$ est un homomorphisme d'anneaux de A dans $End(A)$. Montrer que cet homomorphisme est injectif, puis que $End(A)$ possède un sous-anneau isomorphe à A. Donner un exemple où ce sous-anneau est distinct de $End(A)$. Réaliser l'anneau $\mathbb{Z}[i]$ des entiers de Gauss et l'anneau $\mathbb{Z}[j]$ comme sous-anneaux de $M(2, \mathbb{Z})$.

B– Groupe des inversibles d'un anneau.

1. Vérifier que l'ensemble des éléments inversibles d'un anneau $(A, +, \cdot)$ unitaire a une structure naturelle de groupe multiplicatif. Ce groupe sera noté $(A^\star, \cdot)$, ou simplement $A^\star$.
2. Quel est le groupe des inversibles de $End(G)$, lorsque G est un groupe abélien ? Examiner les cas où G est le groupe $(\mathbb{Z}, +)$, $(\mathbb{Z}^2, +)$ ou $(\mathbb{Z}/n\mathbb{Z}, +)$.
3. Quel est le groupe des inversibles de l'anneau $(M(n, \mathbb{K}), +, \cdot)$ des matrices carrées d'ordre n, à coefficients dans le corps commutatif $\mathbb{K}$? Examiner le cas où $n = 1$.
4. Déterminer le cardinal du groupe des automorphismes du groupe additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
5. Quel est le groupe des inversibles de l'anneau $\mathcal{D}$ des nombres réels décimaux ? Idem pour les anneaux $\mathbb{Z}[X]$, $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$.
6. Quel est le groupe des inversibles de l'anneau de Boole $(\mathcal{P}(E), \Delta, \cap)$ des parties de l'ensemble E ? (On rappelle que $X\Delta Y = (X \cup Y)\backslash(X \cap Y)$ et que cette loi est associative.)

C– Le groupe additif $\mathbb{Z}/n\mathbb{Z}$.

1. Calculer le nombre de sous-groupes du groupe additif $\mathbb{Z}/1001\mathbb{Z}$.

2. Dessiner le graphe du treillis des sous-groupes du groupe additif $\mathbb{Z}/20\mathbb{Z}$.
3. Montrer (de deux manières) que le nombre de sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ est impair si, et seulement si, l'entier n est un carré.
4. Quel est le nombre de sous-groupes minimaux du groupe additif $\mathbb{Z}/n\mathbb{Z}$? Idem pour les sous-groupes maximaux.
5. Déterminer les automorphismes d'ordre deux du groupe additif $\mathbb{Z}/n\mathbb{Z}$. En déduire que l'indicateur d'Euler $\varphi(n)$ de l'entier n est (presque) toujours pair. Retrouver cela par un argument élementaire en restant dans $\mathbb{N}$.

D– Quelques petits groupes et les treillis de leurs sous-groupes.

1. Dessiner le graphe du treillis des sous-groupes du groupe additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
2. Préciser combien d'"individus" habitent à chaque étage de ce treillis. Montrer plus généralement que pour qu'un élément figure à l'endroit où apparaît un sous-groupe, il faut et il suffit que ce sous-groupe soit cyclique. Que peut-on dire d'un groupe fini G qui ne possède qu'un seul sous-groupe maximal ?
3. Traiter de même le cas du groupe cyclique $\mathbb{Z}/20\mathbb{Z}$ et celui, plus délicat, du groupe $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.
4. En déduire, en recençant les "habitants" du treillis des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$, que

$$n = \sum_{d|n} \varphi(d).$$

5. Déterminer les sous-groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ du groupe des isométries du plan affine euclidien. Vérifier qu'ils sont en correspondance avec les systèmes d'axes orthogonaux.
6. *En déduire* le graphe des sous-groupes du groupe $\mathcal{D}_4$ des isométries "du" carré. Déterminer *alors* le groupe des automorphismes intérieurs de ce groupe.
7. Dessiner le graphe du treillis des sous-groupes du groupe quaternionique $\mathbb{H}_8$, et celui du groupe abélien élémentaire $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. On pourra pour ce dernier repérer ce groupe dans la géométrie de l'espace affine euclidien de dimension 3.

E– Algèbres de groupes.

Soit G un groupe, et $\mathbb{K}$ un corps commutatif. On note $\mathbb{K}[G]$ l'ensemble des applications $f : G \to \mathbb{K}$ telles que $\{g \in G, f(g) \neq 0\}$ soit fini. Il est alors commode de noter $\sum_{g\in G} f(g)[g]$ l'élément f. En particulier, l'application qui vaut 1 en l'élément $g \in G$ et 0 en tout $h \in G$, $h \neq g$, est notée $1[g]$, ou plus simplement $[g]$.

1. Montrer que les lois $+$ et $\cdot$ données par $(f_1 + f_2)(g) = f_1(g) + f_2(g)$ et $(f_1 \cdot f_2)(g) = \sum_{h\in G} f_1(h)f_2(gh^{-1})$ font de $(\mathbb{K}[G], +, \cdot)$ un anneau, et même une $\mathbb{K}$-algèbre.
2. Montrer que si $g \in G$, $[g]$ est inversible dans $\mathbb{K}[G]$, puis que l'application $G \to \mathbb{K}[G]^*$ qui à g associe $[g]$ est un homomorphisme de groupes.
3. Quand $\mathbb{K}[G]$ est-elle une $\mathbb{K}$-algèbre de dimension finie ?
4. Quand est-elle commutative ?
5. Vérifier que si le groupe G est fini et non réduit à un élément, $\mathbb{K}[G]$ a des diviseurs de 0. [On poura penser à $(1 - g)(1 + g + \cdots + g^{d-1})$.]
6. Montrer que l'application $\mathbb{K}[G] \to \mathbb{K}$ qui à $\sum_{g\in G} f(g)[g]$ associe $\sum_{g\in G} f(g)$ est un homomorphisme d'anneaux. On l'appelle l'*homomorphisme d'augmentation*. Son noyau I_G s'appelle l'*idéal d'augmentation* (de l'algèbre $\mathbb{K}[G]$).

7. Déterminer l'algèbre $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$ associée au groupe additif $\mathbb{Z}/n\mathbb{Z}$ et au corps $\mathbb{C}$ des nombres complexes. Quel en est l'idéal d'augmentation ?
8. Soit ζ une racine primitive n-ème de l'unité dans $\mathbb{C}$. Montrer que l'application $\mathbb{Q}[\mathbb{Z}/n\mathbb{Z}] \to \mathbb{C}$ qui à $\sum_{i=0}^{n-1} a_i[\bar{i}]$ associe $\sum_{i=0}^{n-1} a_i\zeta^i$ est un homorphisme d'anneaux. Est-elle injective ?
9. Montrer que l'algèbre $\mathbb{K}[\mathbb{Z}]$ est isomorphe à l'algèbre de polynômes $\mathbb{K}[X]$.
10. Déterminer les classes de conjugaison des éléments du groupe symétrique $\mathfrak{S}_3$. Déterminer l'algèbre $\mathbb{C}[\mathfrak{S}_3]$, ainsi que son idéal d'augmentation. Montrer en particulier qu'elle est isomorphe à l'algèbre produit $\mathbb{C}\oplus\mathbb{C}\oplus M(2,\mathbb{C})$. (On pourra à cet effet faire opérer linéairement le groupe symétrique $\mathfrak{S}_3$ sur l'hyperplan
$$H_0 = \{(z_1, z_2, z_3) \in \mathbb{C}^3, z_1 + z_2 + z_3 = 0\}.)$$
11. Dessiner le treillis des sous-groupes du groupe alterné $\mathfrak{A}_4$, à la lumière de la géométrie du tétraèdre régulier. Déterminer les classes de conjugaison des éléments de ce groupe. Déterminer l'algèbre $\mathbb{C}[\mathfrak{A}_4]$.

F– Le centre d'un anneau.

Soit A un anneau. On appelle *centre* de A l'ensemble $\{a \in A, xa = ax (x \in A)\}$.

1. Montrer que c'est un sous-anneau de A.
2. Soit E un espace vectoriel sur un corps $\mathbb{K}$. Montrer que les éléments du centre de $End(E)$ est constitué des homothéties. (C'est un exercice classique d'algèbre linéaire : on se ramène à montrer que si u est dans le centre de A tout élément x de E est vecteur propre de u ; ce dernier point peut être établi par l'absurde, en effet si x et $u(x)$ ne sont pas colinéaires, on peut considérer $v \in A$ tel que $v(x) = x$ et $v(u(x)) = x$.)
3. En déduire un anneau non commutatif dont le centre est $\{0, 1\}$.
4. Quel est le centre de l'algèbre $\mathbb{C}[\mathfrak{S}_3]$?

G– L'algèbre des polynômes en une matrice.

Soit A une matrice carrée $n \times n$ à coefficients dans le corps commutatif $\mathbb{K}$. Pour $P(X) = a_0 + a_1X + \cdots + a_kX^k$, on pose $P(A) = a_0 + a_1A + \cdots + a_kA^k \in M_n(\mathbb{K})$.

1. Montrer que l'application $P \mapsto P(A)$ est un homomorphisme d'anneaux. Montrer que son image $\mathbb{K}[A]$ est une $\mathbb{K}$-algèbre commutative. Quelle est sa dimension comme $\mathbb{K}$-espace vectoriel ?
2. Quel est le groupe des éléments inversibles de $\mathbb{K}[A]$?
3. Quels en sont les idéaux maximaux ?
4. Déterminer les différentes algèbres qui apparaissent dans le cas des matrices d'ordre deux à coefficients dans $\mathbb{C}$ ou $\mathbb{R}$.
5. Donner une condition nécessaire et suffisante pour que l'algèbre $\mathbb{C}[A]$ soit réduite (c'est-à-dire sans éléments nilpotents non nuls).
6. Énoncer une condition nécessaire et suffisante pour que l'algèbre $\mathbb{K}[A]$ coïncide avec le commutant $\mathfrak{z}(A) = \{M \in M(n, \mathbb{K}), AM = MA\}$ de la matrice A.
7. Deviner, sans en donner une démonstration, l'algèbre des matrices qui commutent avec toutes les matrices qui commutent avec A.

H– Entiers quadratiques.

Soit d un entier qui n'est pas un carré. Soit $\sqrt{d}$ une racine carrée de d dans $\mathbf{C}$. Considérons
$$\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d}, a \in \mathbf{Z}, b \in \mathbf{Z}\}.$$

1. Montrer que c'est un sous-anneau de $\mathbf{C}$.
2. Lorsque $d<0$, déterminer $\mathbf{Z}[\sqrt{d}]^*$.
3. Lorsque $d<0$ et $d\equiv 1 \pmod 4$, montrer que $\mathbf{Z}[(1+\sqrt{d})/2]=\{(a+b\sqrt{d})/2, a\in\mathbf{Z}, b\in\mathbf{Z}, a\equiv b \pmod 2\}$ est un sous-anneau de $\mathbf{C}$ et déterminer ses éléments inversibles.

I– Entiers 10-adiques.

Considérons l'ensemble $\mathbf{Z}_{10}$ des suites à valeurs dans $\{0,1,2,...,9\}$. On note $\sum_{i=0}^{\infty} a_i 10^i$ la suite $(a_i)_{i\geq 0}$. On munit $\mathbf{Z}_{10}$ d'une loi $+$ donnée par $\sum_{i=0}^{\infty} a_i 10^i + \sum_{i=0}^{\infty} b_i 10^i = \sum_{i=0}^{\infty} c_i 10^i$ avec $c_i = a_i + b_i - 10 r_{i+1} + r_i$, où $r_i \in \{0,1\}$ et $r_0 = 0$. (L'addition est l'addition habituelle des nombres en écriture décimale, mais portant sur une infinité de décimales, la quantité r_i étant l'éventuelle retenue.) On le munit aussi d'une loi $\times$ donnée par $(\sum_{i=0}^{\infty} a_i 10^i)(\sum_{i=0}^{\infty} b_i 10^i) = \sum_{i=0}^{\infty} c_i 10^i$ avec $c_i = \sum_{j=0}^{i} a_j b_{i-j} + r_i - 10 r_{i+1}$, où r_i est un entier ≥ 0 et $r_0 = 0$. (C'est la multiplication habituelle avec le système des retenues.)

Les éléments de $\mathbf{Z}_{10}$ s'appellent les *entiers 10-adiques*. On peut y penser comme à des nombres dont les développements décimaux sont infinis à gauche.

1. Montrer que $(\mathbf{Z}_{10},+)$ est un groupe abélien, puis que $(\mathbf{Z}_{10},+,\times)$ est un anneau commutatif.
2. Montrer qu'on a un homomorphisme injectif d'anneaux $\mathbf{Z}\to\mathbf{Z}_{10}$. Est-il surjectif ? Quelle est l'image de -1 ? On identifie maintenant $\mathbf{Z}$ à un sous-anneau de $\mathbf{Z}_{10}$.
3. Montrer que $\sum_{i=0}^{\infty} a_i 10^i$ est inversible dans $\mathbf{Z}_{10}$ si, et seulement si, $a_0\in\{1,3,7,9\}$. Quel est l'inverse de 3 dans $\mathbf{Z}_{10}$? Montrer si a et b sont deux entiers avec a premier à 10, l'équation $ax=b$ admet une solution x dans $\mathbf{Z}_{10}$.
4. Montrer que les idéaux principaux engendrés par 2 et 5 respectivement sont maximaux. Quels sont les corps quotients ?
5. Considérons la suite $(u_k)_{k\geq 0}$ (resp. $(u_k)_{k\geq 0}$) donnée par la récurrence suivante $u_0=1$ (resp. $v_0=1$) et $u_{k+1}=2^{u_k-1}+u_k$ (resp. $v_{k+1}=4.2^{v_k-1}+v_k$). Montrer que $5^{u_{k+1}}\equiv 5^{u_k} \pmod{2^{u_k}}$ (resp. $2^{v_{k+1}}\equiv 2^{v_k} \pmod{5^{v_k}}$), puis que $5^{u_{k+1}}\equiv 5^{u_k} \pmod{10^{u_k}}$ (resp. $2^{v_{k+1}}\equiv 2^{v_k} \pmod{10^{v_k}}$). Notons U_i (resp. V_i) le i-ème chiffre de 5^{u_k} (resp. 2^{v_k} lorsque k est un entier quelconque tel que $u_k>i$ (resp. $v_k>i$). Posons $U=\sum_{i=0}^{\infty} U_i 10^i$ et $V=\sum_{i=0}^{\infty} V_i 10^i$. Montrer que U (resp. V) est divisible par toute puissance de 5 (resp. de 2).
6. L'anneau $\mathbf{Z}_{10}$ est-il intègre ? (Considérer le produit UV.)
7. Soit n un entier ≥ 0. Montrer que l'application $\phi_n:\mathbf{Z}_{10}\to\mathbf{Z}/10^n\mathbf{Z}$ qui à $\sum_{i=0}^{\infty} a_i 10^i$ associe la classe de $\sum_{i=0}^{n-1} a_i 10^i$ modulo 10^n est un homomorphisme surjectif d'anneaux. Montrer que $a\in\mathbf{Z}_{10}$ est nul si, et seulement si, pour tout $n\geq 0$, on a $\phi_n(a)=0$.
8. Montrer que $\mathbf{Z}_{10}^*$ possède un élément d'ordre 4.

J– Inversible à gauche, inversible à droite On se donne un élément a d'un anneau A vérifiant d'une part $ab=1$, pour $b\in A$, et d'autre part $ax=0$ pour un nombre fini seulement d'éléments $x\in A$. Montrer que $a\in A^\star$.