EPFL Automne 2025
Algebre Lineaire Avancee, MATH-110

Série 6

Vous etes fortement encourages a essayer de resoudre (eventuellement a plusieurs) l'exercice ($\star$) et a rendre votre solution (eventuellement a plusieurs) avant le vendredi de la semaine suivante celle ou la serie a ete postee. Il faudra transmettre votre solution sur moodle, sous forme de fichier pdf (eventuellement tape en LaTeX) en suivant le lien a cet effet dans la semaine de la serie.

1 Calculs dans les anneaux

Exercice 1. Soit $(A, +, .)$ un anneau commutatif et $a, c \in A$, on dit que a divise c et on le note

$$a|c$$

si il existe $b \in A$ tel que

$$c = a.b.$$

On dit egalement que a est un diviseur de b.

1. Montrer que la relation de divisibilite est reflexive et transitive.
2. Montrer que tout element du groupe des unites $A^\times$ est un diviseur de tout element de A.
3. Quels sont les diviseurs de 0_A ? de 1_A ?

Exercice 2. Soit A un anneau commutatif. Soit l'ensemble

$$M_2(A) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a, b, c, d \in A\}$$

des matrices 2×2 a coefficients dans A. On muni cet ensemble des lois d'addition et de multiplication des matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix},\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

est un anneau d'element nul la matrice nulle et d'unite la matrice identite

$$0_{2,A} = \begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix},\ \mathrm{Id}_2 = \begin{pmatrix} 1_A & 0_A \\ 0_A & 1_A \end{pmatrix}.$$

1. Montrer que les ensembles des matrices scalaires

$$A.\mathrm{Id}_2 = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},\ a \in A\} \subset M_2(A),$$

des matrices diagonales

$$\mathrm{Diag}_2(A) = \{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix},\ a, d \in A\} \subset M_2(A),$$

des matrices triangulaires superieures

$$B_2(A) = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix},\ a, b, d \in A\} \subset M_2(A),$$

et des matrices triangulaires inferieures

$$B_{-,2}(A) = \{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix},\ a, c, d \in A\} \subset M_2(A)$$

sont des sous-anneaux.

2. Montrer que si A possede au moins deux elements distincts alors $M_2(A)$ n'est pas commutatif : pour cela on montrera que $B_2(A)$ n'est pas commutatif.

Exercice 3. Soit $(A, +, ., 0_A, 1_A)$ un anneau . On a dit qu'un element $a \in A$ est inversible a gauche (resp. a droite) si il existe $b \in A$ (resp. $c \in A$) tel que

$$b.a = 1_A \ (resp.\ a.c = 1_A).$$

On dit que b est un inverse a gauche (resp. c est un inverse a droite)

1. On suppose que a est inversible a gauche ET inversible a droite (avec des inverses a gauche et a droite notes respectivement b et c). Montrer qu'alors

$$b = c$$

de sorte que a est inversible au sens du cours (les inverses a droite et a gauche etant les memes). On a alors vu que l'inverse est uniquement defini.

2. On va maintenant donner un exemple d'un anneau possedant un element inversible a gauche mais qui n'est pas inversible a droite. Soit $\mathcal{F}(\mathbb{Z}, \mathbb{Z})$ l'ensemble des fonctions (toutes les fonctions, par seulement les morphismes de groupes) de $\mathbb{Z}$ sur $\mathbb{Z}$. Alors avec l'addition et la *composition* des fonctions, on obtient un anneau

$$(\mathcal{F}(\mathbb{Z}, \mathbb{Z}), +, \circ, \underline{0}, \mathrm{Id}_{\mathbb{Z}})$$

Remarque. Dans cet exercice la "multiplication" est la composition des fonctions... pas la multiplication sur les fonctions induite par la multiplication dans l'anneau d'arrivee $\mathbb{Z}$.
En particulier l'anneau etudie ici est non commutatif.

(a) On considere la fonction de doublement

$$D : \begin{array}{ccc} \mathbb{Z} & \mapsto & \mathbb{Z} \\ n & \mapsto & D(n) = 2n \end{array}.$$

Soit $[\bullet] : \mathbb{R} \mapsto \mathbb{Z}$ la fonction partie entiere ($[x]$ est le plus grand entier inferieur ou egal a x). Montrer que la fonction

$$H := [\frac{\bullet}{2}] : n \in \mathbb{Z} \mapsto [\frac{n}{2}] \in \mathbb{Z}$$

est un inverse a gauche de D.

(b) Montrer que D n'admet pas d'inverse a droite : il n'existe pas de $H' : \mathbb{Z} \mapsto \mathbb{Z}$ telle que

$$D \circ H' = \mathrm{Id}_{\mathbb{Z}}.$$

Exercice 4 (Formule du binome)**.** Soit $(A, +, .)$ un anneau pas forcement commutatif, $x, y \in A$ et $n \geqslant 1$ un entier.

1. Montrer que si x et y COMMUTENT pour la multiplication de A (ie $x.y = y.x$) on a la formule du binome de Newton :

$$(x+y)^n = (x+y).\cdots.(x+y)\ _{n \text{ fois}} = \sum_{k=0}^{n} C_n^k.x^k.y^{n-k}.$$

On rappelle que pour $0 \leqslant k \leqslant n$, $C_n^k \geqslant 1$ est le nombre de sous-ensembles de cardinal k dans un ensemble de cardinal n et pour tout $m \in \mathbb{N}$ et $x \in A$ on note

$$m.x = x + \cdots + x \ (m \text{ fois}).$$

2. On suppose que $A = \mathbb{Z}/p\mathbb{Z}$ pour p un nombre premier ($\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est alors un corps mais on ne l'utilisera pas). Montrer que

$$\forall x, y \in \mathbb{Z}/p\mathbb{Z},\ (x+y)^p = x^p + y^p.$$

Ainsi l'application "elevation a la puissance p" est un endomorphisme du groupe $(\mathbb{Z}/p\mathbb{Z}, +)$! Pour la preuve on utilisera la formule des coefficients du binome obtenue par denombrement

$$C_p^k = \frac{p!}{k!(p-k)!}$$

avec

$$n! = n.(n-1).\cdots.1,\ n \geqslant 1,\ 0! = 1.$$

pour montrer que

$$\forall\ 1 \leqslant k \leqslant p-1,\ p | C_p^k.$$

3. Montrer (Petit Thm de Fermat) que pour tout $x \in \mathbb{Z}/p\mathbb{Z}$ on a $x^p = x$. Pour cela on pourra ecrire $x = n \,(\mathrm{mod}\, p)$ avec $1 \leqslant n \leqslant p$ et

$$n \,(\mathrm{mod}\, p) = (n-1) \,(\mathrm{mod}\, p) + 1 \,(\mathrm{mod}\, p)$$

et on procedera par recurrence en utilisant la question precedente.
Alternatiement on ecrira directement

$$n \,(\mathrm{mod}\, p) = 1 \,(\mathrm{mod}\, p) + \cdots + 1 \,(\mathrm{mod}\, p) \ (n \text{ fois})$$

et on utilisera la question precedente.

2 Anneau quotient dans un anneau commutatif

Dans cette series d'exercice on discute la notion de quotient d'un anneau par un ideal (bilatere si A n'est pas commutatif). Cet exercice est largement corrige a la fin du chapitre sur les anneaux. On vous demande donc (d'essayer de) ne pas regarder la solution en particlier pour l'exercice 8.

Soit $(A, +, \cdot)$ un anneau qu'on suppose commutatif pour commencer et soit $I \subset A$ un ideal. Soit $a \in A$, la classe de congruence de a modulo I est le sous-ensemble

$$a \,(\mathrm{mod}\, I) := a + I = \{a + i,\ i \in I\} \subset A.$$

On note ce sous-ensemble

$$a \,(\mathrm{mod}\, I) := a + I.$$

Soient $a, a' \in A$; si on a

$$a \,(\mathrm{mod}\, I) = a' \,(\mathrm{mod}\, I),$$

on dit que a est *congru* a a' modulo I et on note cette relation

$$a \equiv a' \,(\mathrm{mod}\, I).$$

L'ensemble des classes de congruences modulo I

$$A/I = \{a \,(\mathrm{mod}\, I) = a + I,\ a \in a\}$$

est un sous-ensemble de l'ensemble $\mathscr{P}(A)$ des parties de A. On va munir A/I d'une structure d'anneau de sorte que l'application (evidement surjective)

$$\pi_I : a \in A \mapsto a \,(\mathrm{mod}\, I) = a + I \in A/I$$

soit un morphisme d'anneaux.

Exercice 5. On reprend les notations ci-dessus.

1. Montrer les equivalences

$$a \equiv a' \,(\mathrm{mod}\, I) \Longleftrightarrow a - a' \in I \Longleftrightarrow a - a' \equiv 0_A \,(\mathrm{mod}\, I).$$

2. Montrer que la relation de congruence modulo I, $a \equiv a' \,(\mathrm{mod}\, I)$ est une relation d'equivalence sur A dont les classes d'equivalences sont precisement les classes de congruence $a \,(\mathrm{mod}\, I)$ pour $a \in A$ et que $a \,(\mathrm{mod}\, I)$ est la seule classe d'equivalence (pour cette relation) contenant a.
3. Que vaut A/I si $I = A$? si $I = \{0_A\}$?

Exercice 6. On suppose qu'on dispose sur A/I d'une structure d'anneau avec une addition $+_{A/I}$ et une multiplication $\cdot_{A/I}$.

1. Montrer que si

$$\pi_I : a \in A \mapsto a + I \in A/I$$

est un morphisme d'anneaux alors

$$0_{A/I} = I,\ 1_{A/I} = 1_A + I$$

et que pour tout $a, b \in A$

$$\begin{aligned} a \,(\mathrm{mod}\, I) +_{A/I} b \,(\mathrm{mod}\, I) &= a + b \,(\mathrm{mod}\, I), \\ a \,(\mathrm{mod}\, I) \cdot_{A/I} b \,(\mathrm{mod}\, I) &= a \cdot b \,(\mathrm{mod}\, I). \end{aligned} \tag{2.1}$$

Exercice 7. Dans cet exercice on montre que les formules precedentes definissent effectivement une structure d'anneaux.

1. Soient a, a', b, b', montrer que si $a \,(\mathrm{mod}\, I) = a' \,(\mathrm{mod}\, I)$ et $b \,(\mathrm{mod}\, I) = b' \,(\mathrm{mod}\, I)$ alors

$$a + b \,(\mathrm{mod}\, I) = a' + b' \,(\mathrm{mod}\, I),\ a \cdot b \,(\mathrm{mod}\, I) = a' \cdot b' \,(\mathrm{mod}\, I).$$

$$\pi_I : a \in A \mapsto a + I \in A/I$$

est un morphisme d'anneaux alors

$$0_{A/I} = I,\ 1_{A/I} = 1_A + I$$

et que pour tout $a, b \in A$

$$a \,(\mathrm{mod}\, I) +_{A/I} b \,(\mathrm{mod}\, I) = a' + b' \,(\mathrm{mod}\, I),$$

$$a \,(\mathrm{mod}\, I) \cdot_{A/I} b \,(\mathrm{mod}\, I) = a' \cdot b' \,(\mathrm{mod}\, I).$$

2. En deduire que les formules (2.1) definissent des lois de composition internes de $A/I \times A/I$ vers A/I et que $(A/I, +_{A/I}, \cdot_{A/I}, 0_{A/I}, 1_{A/I})$ est bien un anneau : on deduira cela du fait que $(A, +_A, \cdot_A, 0_A, 1_A)$ est un anneau et de la definition (2.1).
3. Montrer que π_I est un morphisme d'anneaux dont le noyau est I.

Exercice 8. ($\star$) Soit A et I comme ci-dessus. Soit $\varphi : A \to B$ un morphisme. On suppose que

$$I \subset \ker \varphi =: K.$$

1. Montrer qu'il existe un unique morphisme d'anneaux

$$\varphi_I : A/I \to B$$

tel que

$$\varphi = \varphi_I \circ \pi_I.$$

Remarquer que cette derniere eqgalite vous donne une formule pour la valeur $\varphi_I(a \,(\mathrm{mod}\, I))$ pour tout $a \in A$; il restera a verifier que cette formule permet effectivement de definir φ_I (a la maniere de la premiere question de l'exercice precedent) et qu'on obtient bien un morphisme d'anneaux. On dit que φ se factorise par π_I.

2. On considere le cas $I = \ker \varphi$. Montrer que

$$\varphi_{\ker \varphi}(A/\ker \varphi) = \varphi(A)$$

et que $\varphi_{\ker \varphi}$ est un isomorphisme d'anneaux $A/\ker \varphi$ sur l'image $\varphi(A) \subset B$, ie.

$$\varphi_{\ker \varphi} : A/\ker \varphi \simeq \varphi(A).$$

L'existence de cet isomorphisme est appele le "theoreme Noyau-Image".
En particulier si B est fini on a

$$|A/\ker \varphi| = |\varphi(A)|.$$

Exercice 9. Etendre les resultats precedents au cas d'un anneau A n'est pas necessairement commutatif quand on suppose que I est un ideal bilatere de A :

$$\forall a, a' \in A,\ a.I.a' \subset I.$$

Bonnes vacances !