EPFL Automne 2024
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 mercredi de la semaine suivante. Il faudra transmettre votre solution sur moodle, sous forme d'un fichier pdf unique (eventuellement tape en LaTeX) en suivant le lien a cet effet dans la semaine de la serie.

Calculs dans les anneaux

Exercice 1. Soit $(A, +, \cdot, 0_A, 1_A)$ un ensemble muni de structures additionelles :

- $(A, +, 0_A)$ est un groupe (pas necessairement commutatif).
- La loi de composition $\bullet \cdot \bullet : A \times A \mapsto A$ est associative (mais pas forcement commutative) et admet 1_A comme element neutre (a droite et a gauche).
- La loi $\bullet \cdot \bullet$ est distributive par rapport a $+$: pour tout $a, x, y \in A$, on a

$$a \cdot (x + y) = a \cdot x + a \cdot y, \ (x + y) \cdot a = x \cdot a + y \cdot a.$$

On va montrer que $(A, +, 0_A)$ est commutatif (et donc que $(A, +, \cdot, 0_A, 1_A)$ est un anneau.

On notera 0 et 1 pour 0_A et 1_A et on note $-a$ pour l'inverse de a dans le groupe $(A, +, 0_A)$.

1. Montrer que 0_A est absorbant :

$$\forall x \in A, \ 0_A.x = x.0_A = 0_A.$$

2. Montrer que $(-1) \cdot x = -x$.
3. Soient $x, y \in A$. Calculer de deux manieres $-(x + y)$ et en deduire que

$$(-x) + (-y) = (-y) + (-x)$$

et conclure que $+$ est bien commutative.

Exercice 2 (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

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

   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

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

Exercice 3. Soient $(A, +_A, .A)$ et $(B, +_B, .B)$ deux anneaux commutatifs. On considere l'anneau produit

$$A \times B = \{(a, b),\ a \in A,\ b \in B\}$$

muni de l'addition et de la multiplication coordonee par coordonnee

$$(a,b) + (a',b') = (a +_A a', b +_B b'),\ (a,b).(a',b') = (a._A a', b._B b')$$

avec comme neutre et unite $0_{A\times B} = (0_A, 0_B),\ 1_{A\times B} = (1_A, 1_B)$.

1. Montrer que si A et B ne sont pas des anneaux nuls alors $A \times B$ n'est pas un anneau integre (meme si A et B sont integres).

Anneau quotient dans un anneau commutatif

Soit $(A, +, \cdot)$ un anneau commutatif et $I \subset A$ un ideal. Soit $a \in A$, on rappelle que la classe de congruence de a modulo I est le sous-ensemble

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

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

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

Exercice 4. 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 l'unique classe d'equivalence de cette relation contenant a.
   On rappelle que l'ensemble des classes de congruences modulo I est note

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

3. Que vaut A/I si $I = A$? si $I = \{0_A\}$?

On rappelle que A/I est muni d'une structure d'anneau commutatif $(A/I, +_I, \cdot_I, 0_I, 1_I)$ qu'on appelle *anneau quotient* de A par l'ideal I et dont les lois sont

$$a \,(\mathrm{mod}\, I) +_I b \,(\mathrm{mod}\, I) = a + b \,(\mathrm{mod}\, I)$$

$$a \,(\mathrm{mod}\, I) \cdot_I b \,(\mathrm{mod}\, I) = a \cdot b \,(\mathrm{mod}\, I)$$

de sorte que l'application

$$\bullet \,(\mathrm{mod}\, I) : \begin{array}{ccc} A & \mapsto & A/I \\ a & \mapsto & a \,(\mathrm{mod}\, I) = a + I \end{array}$$

est un morphisme d'anneaux surjectif de noyau

$$\ker(\bullet \,(\mathrm{mod}\, I)) = I.$$

Exercice 5. Soit A un anneau commutatif non nul et I un ideal. On a vu en cours que si $I \neq A$ est maximal parmi les ideaux stricts de A (si $J \neq A$ est un ideal strict de A tel que $I \subset J$ alors $I = J$) alors l'anneau quotient A/I est un corps.

1. Montrer que reciproquement, si A/I est un corps alors I est maximal. Pour cela on pourra considerer un ideal $J \supset I$ et montrer que si $J \neq I$, il existe $a \in J$ et $b \in A$ tel que $a.b \equiv 1_A \pmod{I}$ (utiliser que A/I est un corps) ; on en deduira que $1_A \in J$ avant de conclure que $J = A$.
2. Un ideal $I \neq A$ est dit premier si il verifie la condition suivante

$$\forall a, b \in A,\ a.b \in I \Longrightarrow a \in I \text{ ou bien } b \in I.$$

   Montrer que

$$I \text{ est premier } \iff A/I \text{ est un anneau integre.}$$

3. En deduire qu'un ideal maximal est premier (la reciproque n'est pas vraie en general).

Corps

Exercice 6. ($\star$) Dans cet exercice on va demontrer le resultat suivant :

Lemme. *Soit A un anneau non-nul commutatif, integre et FINI alors A est un corps (tout element non-nul de A est inversible).*

Soit donc $a \in A - \{0_A\}$ non-nul, on veut montrer que a admet un inverse dans A.

Pour cela on considere la suite d'elements $(a_n)_{n \geqslant 0}$ de A, donnee pour tout entier $n \geqslant 0$ par

$$a_n := a^n = a.a.\cdots.a \ (n \text{ fois})$$

(avec $a_0 = a^0 = 1_A$).

1. Montrer qu'il existe deux entiers $0 \leqslant m < n$ tels que $a^n = a^m$.
2. En deduire qu'il existe un entier $k \geqslant 1$ tel que $a^k - 1_A = 0_A$ (on factorisera l'egalite $a^n - a^m = 0_A$)
3. Conclure la preuve du Lemme.
4. Soit B un anneau commutatif non nul et $I \neq B$ un ideal strict tel que l'anneau quotient $A = B/I$ soit fini. Montrer que si I est premier alors I est maximal (cf. Ex. 5).

Exercice 7. Soit K et L des corps de caracteristique $\mathrm{car}(K)$ et $\mathrm{car}(L)$ et

$$\varphi : K \mapsto L$$

un morphisme d'anneaux non nul ($\varphi \neq \underline{0}_L$). Pour $n \in \mathbb{Z}$ on note

$$n_K := \mathrm{Can}_K(n) = n.1_K \text{ (resp. } n_L := \mathrm{Can}_L(n) = n.1_K)$$

l'image de n par les morphismes canoniques respectifs.

1. Montrer que pour tout $n \in \mathbb{Z}$, $\varphi(n_K) = n_L$.
2. En deduire que necessairement $\mathrm{car}(K) = \mathrm{car}(L)$.