EPFL Automne 2022
Algebre Lineaire Avancee, MATH-110

Série 5

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 $(A, +, \times, 0_A, 1_A)$ un ensemble muni de structures additionelles :

— $(A, +, \times, 0_A)$ est un groupe (pas necessairement commutatif).

— La loi de composition $\times : A \times A \mapsto A$ est associative (mais pas forcement commutative) et admet 1_A comme element neutre (a droite et a gauche).

— La loi $\times$ est distributive par rapport a $+$: pour tout $a, x, y \in A$, on a

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

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

1. Montrer que 0 est absorbant :

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

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

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

et conclure.

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 si $x.y = y.x$) 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

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

Remarque. On n'en a pas besoin mais on rappelle la formule des coefficients du binome obtenue par denombrement

$$C_n^k = \frac{n!}{k!(n-k)!}$$

avec

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

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

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

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

$$a \pmod{I} := a + I = \{a + i,\ i \in I\} \subset A.$$

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

$$a \pmod{I} = a' \pmod{I}$$

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

$$a \equiv a' \pmod{I}.$$

Exercice 4. On reprend les notations ci-dessus.

1. Montrer l'equivalence

$$a \equiv a' \pmod I \iff a - a' \in I \iff a - a' \equiv 0_A \pmod I.$$

2. Montrer que la relation de congruence modulo I, $a \equiv a' \pmod I$ est une relation d'equivalence sur A dont les classes d'equivalences sont precisement les classes de congruence $a \pmod I$, $a \in A$ et que $a \pmod I$ est l'unique classe d'equivalence de cette relation contenant a.

L'ensemble des classes de congruences modulo I (c'est un sous-ensemble de $\mathscr{P}(A)$) est note

$$A/I := \{a \pmod I = a + I,\ a \in A\}$$

On peut/veut munir cet ensemble d'une structure d'anneau commutatif qu'on appelle l'*anneau quotient* de A par l'ideal I.

Exercice 5. Soit $(A, +, .)$ un anneau commutatif et $I \subset A$ un ideal et A/I l'ensemble des classes de congruences modulo I.

1. Pour $a, b \in A$, on defini

$$a +_I b := a + b \pmod I,\ a \cdot_I b := a.b \pmod I.$$

   Montrer que ces deux operations determinent des applications bien definies qu'on notera encore

$$+_I, \cdot_I : A/I \times A/I \mapsto A/I;$$

   c'est a dire que si $a \pmod I = a' \pmod I$ et $b \pmod I = b' \pmod I$ on a

$$a + b \pmod I = a' + b' \pmod I,\ ab \pmod I = a' \cdot b' \pmod I.$$

2. Montrer que $(A/I, +_I, \cdot_I, 0_A \pmod I, 1_A \pmod I)$ forme un anneau commutatif. (pour verifier que les lois $+_I$ et $._I$ on les bonnes proprietes de commutativite, distributivite, associativite ainsi que les bons elements neutres, on utilisera le fait que dans $\mathbb{Z}$ les lois $+$ et $.$ ont toutes ces proprietes.
3. Montrer que l'application

$$\bullet \pmod I : \begin{array}{ccc} A & \mapsto & A/I \\ a & \mapsto & a \pmod I = a + I \end{array}$$

   est un morphisme d'anneau de noyau

$$\ker(\bullet \pmod I) = I.$$

4. Que vaut l'anneau A/I si $I = A$? si $I = \{0_A\}$.

Exercice 6. Soit A un anneau commutatif non nul et I un ideal. On a vu en cours que si $I \neq A$ est maximal (si $J \neq A$ est un ideal 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
$$I \text{ est premier } \iff A/I \text{ est integre.}$$
3. En deduire qu'un ideal maximal est premier (la reciproque n'est pas vraie en general).

Corps

Exercice 7. Soit K un corps.

1. Soit $I \subset K$ un sous K-module de K (aka encore un ideal de l'anneau K). Montrer que ou bien $I = \{0_K\}$ ou bien $I = K$.
2. Retrouver le fait qu'un morphisme d'anneau $\varphi : K \mapsto A$ est soit nul soit injectif.
3. Soit V un K-module et $\varphi : K \mapsto V$ un morphisme de K-modules. Montrer que φ est soit nul, soit injectif.
4. Montrer qu'un morphisme de K-modules $\ell : V \mapsto K$ est soit nul, soit surjectif.

Remarque 0.1. La premier question dit que le seul ideal strict ($\neq K$) d'un corps K est l'deal nul $\{0_K\}$. Ainsi $\{0_K\}$ est maximal ce qui est coherent avec le fait que le quotient
$$K/\{0_K\} \simeq K$$
est un corps.

Exercice 8. ($\star$) 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'element de A, donnee pour tout entier $n \geqslant 0$ par

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

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

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 $a^k - 1_A = 0_A$.
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 B/I soit fini. Montrer que si I est premier alors I est maximal (cf. Ex. 6).

Exercice 9. Soit K et L des corps 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 $\mathrm{car}(K) = \mathrm{car}(L)$.