EPFL Automne 2020
Algebre Lineaire Avancee, MATH-110

Série 5

Tous les exercices seront corriges. La correction sera postee sur le moodle apres 2 semaines.

Vous etes fortement encourages a essayer de resoudre (eventuellement a plusieurs) l'exercice ($\star$) et a rendre votre solution (eventuellement a plusieurs) avant le dimanche 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.

Exercice 1. 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).

Exercice 2. Soit $q \geqslant 2$ un entier on rappelle que la relation de congruence modulo q

$$m \equiv n \pmod{q} \Longleftrightarrow q | m - n$$

est une relation d'equivalence. On note $\mathbb{Z}/q\mathbb{Z}$ l'ensemble des classes (d'equivalences pour cette relation) de congruences modulo q : si $n \in \mathbb{Z}$ on note $n \pmod{q} = n + q.\mathbb{Z}$ la classe de congruence correspondante (l'ensemble des $m \in \mathbb{Z}$ tels que $q|m-n$). Ainsi

$$\mathbb{Z}/q\mathbb{Z} = \{0 \pmod{q}, 1 \pmod{q}, \cdots, q - 1 \pmod{q}\}.$$

On definit sur $\mathbb{Z}/q\mathbb{Z}$ une structure d'anneau commutatif en posant :

$$a \pmod{q} + b \pmod{q} := a + b \pmod{q},\ a \pmod{q}.b \pmod{q} := a.b \pmod{q}.$$

1. Montrer que ces lois sont bien definies : que si $a \pmod q = a' \pmod q$, $b \pmod q = b' \pmod q$ alors

$$a' \pmod q + b' \pmod q = a \pmod q + b \pmod q,$$

$$a' \pmod q . b' \pmod q = a \pmod q . b \pmod q$$

2. Verifier que ces lois font de $(\mathbb{Z}/q\mathbb{Z}, +, .)$ un anneau commutatif d'element neutre $0 \pmod q = q.\mathbb{Z}$ et d'unite $1 \pmod q = 1 + q\mathbb{Z}$.
3. Montrer que l'application (de reduction modulo q)

$$\bullet \pmod q : n \in \mathbb{Z} \mapsto n \pmod q \in \mathbb{Z}/q\mathbb{Z}$$

est un morphisme d'anneau. Par quel autre nom appelle-t-on ce morphisme ?

4. Montrer que si $q = 4, 6$ alors $(\mathbb{Z}/q\mathbb{Z}, +, .)$ n'est pas integre en trouvant tous les $a \pmod q, b \pmod q \neq 0 \pmod q$ et qui verifient

$$a \pmod q . b \pmod q = 0 \pmod q.$$

Montrer que plus generalement que si q est compose $(\mathbb{Z}/q\mathbb{Z}, +, .)$ n'est pas integre.

5. Montrer que reciproquement, si q est premier, $(\mathbb{Z}/q\mathbb{Z}, +, .)$ est integre.

Exercice 3. ($\star$) Dans cet exercice on va demontrer le lemme vu en cours :

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

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

(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 (utiliser que A est integre) qu'il existe un entier $k \geqslant 1$ tel que $a^k - 1_A = 0_A$.
3. Conclure.

Exercice 4. Soit K un corps de caracteristique positive p et $\mathrm{frob}_p : K \mapsto K$ le Frobenius donne par

$$\mathrm{frob}_p(x) = x^p.$$

Soit

$$\mathbb{F}_p = \mathbb{Z}.1_K = \{n_K = n.1_K,\ n \in \mathbb{Z}\}$$

le sous-corps premier de K

1. Montrer que pour tout $x \in \mathbb{F}_p$, on a

$$x^p = x.$$

   On pourra commencer par montrer cela par pour les x de la forme $x = n_K$ avec $n \in \mathbb{N}$.

0.1 L'anneau des polynomes a coefficients dans un anneau commutatif

Soit A un anneau commutatif non nul. Dans le prochain exercice, on va donner une construction algebrique de $A[X]$, l'anneau des polynomes en une variable a coefficients dans un anneau A : un tel polynome est une expression formelle

$$P(X) = a_0 + a_1.X + a_2.X^2 + \cdots + a_d.X^d,\ a_0, a_1, \cdots, a_d \in A.$$

On peut additonner deux polynomes en posant pour

$$Q(X) = b_0 + b_1.X + b_2.X^2 + \cdots + b_d.X^d,\ b_0, b_1, \cdots, b_d \in A.$$

$$(P + Q)(X) := (a_0 + b_0) + (a_1 + b_1).X + \cdots + (a_d + b_d).X^d$$

et les multiplier en posant

$$P.Q(X) = \sum_{n=0}^{2d} c_n X^n$$

avec

$$c_n = \sum_{i+j=n} a_i.b_j.$$

Cette derniere formule est obtenue en decomposant le produit

$$P.Q(X) = (a_0 + a_1.X + a_2.X^2 + \cdots + a_d.X^d).(b_0 + b_1.X + b_2.X^2 + \cdots + b_d.X^d)$$

en somme de $(d + 1)^2$ termes (par associativite), en ecrivant par commutativite que

$$a_i.X^i.b_j.X^j = a_i.b_j.X^{i+j}$$

et en regroupant ensemble les monomes de meme degre...

Voici une construction de $A[X]$ ou l'on ne parle pas d'"expression formelle".

Exercice 5. Soit
$$A^{\mathbb{N}} = \{\mathbf{a} = (a_n)_{n\geqslant 0}, a_n \in A\}$$
l'ensemble des suites a valeurs dans A (si on prefere $A^{\mathbb{N}} = \mathcal{F}(\mathbb{N}; A)$ est l'ensemble des applications de $\mathbb{N}$ a valeurs dans A).

1. Definir une addition sur $A^{\mathbb{N}}$ lui donnant une structure de groupe abelien.
2. Pour tout $b \in A$ et $\mathbf{a} = (a_n)_{n\geqslant 0} \in A^{\mathbb{N}}$, on pose
$$b.\mathbf{a} = (b.a_n)_{n\geqslant 0}.$$
Montrer que cela defini sur $A^{\mathbb{N}}$ une structure de A-module.
3. On definit sur $A^{\mathbb{N}}$ le produit suivant : pour $\mathbf{a} = (a_n)_{n\geqslant 0}$ et $\mathbf{b} = (b_n)_{n\geqslant 0}$
$$\mathbf{a} \star \mathbf{b} = (c_n)_{n\geqslant 0}$$
avec
$$c_n := a_0.b_n + a_1.b_{n-1} + \cdots + a_n.b_0 = \sum_{i+j=n} a_i.b_j.$$
Montrer que le produit $\star$ est associatif, commutatif, distributif par rapport a $+$ et trouver deux elements $0_{A^{\mathbb{N}}}$ et $1_{A^{\mathbb{N}}}$ tels que $(A^{\mathbb{N}}, +, \star)$ forme un anneau (et meme une A-algebre avec la multiplication externe $(b, \mathbf{a}) \mapsto b.\mathbf{a}$).
4. Etant donne $\mathbf{a} = (a_n)_n$ une suite, son support $\mathrm{supp}(\mathbf{a})$ est le sous-ensemble des indices n tels que a_n est non-nul :
$$\mathrm{supp}(\mathbf{a}) = \{n \in \mathbb{N},\ a_n \neq 0_A\} \subset \mathbb{N}.$$
Soit
$$A^{\mathbb{N}}_f = \{\mathbf{a} = (a_n)_n,\ \mathrm{supp}(\mathbf{a}) \text{ est un ensemble fini}\} \subset A^{\mathbb{N}}$$
l'ensemble des suites de support fini. Montrer que $A^{\mathbb{N}}_f$ est un sous-A module de $A^{\mathbb{N}}$ et un sous-anneau pour $+$ et $\star$.
5. Soit $\mathbf{a} \in A^{\mathbb{N}}_f$, on definit le degre de $\mathbf{a}$ par
$$\deg(\mathbf{a}) = \max\{n \geqslant 0\ a_n \neq 0\}.$$
Si $\mathbf{a} = \underline{0}_A = (0_A)_{n\geqslant 0}$ dont le support est vide, on pose $\deg(\underline{0}_A) = -\infty$.
6. Montrer que si A est integre, alors pour tout $\mathbf{a}, \mathbf{b} \in A^{\mathbb{N}}_f$
$$\deg(\mathbf{a} \star \mathbf{b}) = \deg(\mathbf{a}) + \deg(\mathbf{b})$$
et en deduire que $A^{\mathbb{N}}_f$ est un anneau integre.

Remarque 0.1. L'anneau $(A_f^{\mathbb{N}}, +, \star)$ fournit une construction algebrique de l'anneau des polynomes $(A[X], +, .)$ en associant a la suite (de support fini) $\mathbf{a} = (a_n)_{n\geqslant 0}$ le polynome

$$P_{\mathbf{a}}(X) = a_0 + a_1.X + \cdots + a_n.X^n + \cdots = \sum_{n=0}^{\infty} a_n X^n$$

(comme le support de $\mathbf{a}$ est fini cette somme est en fait finie puisque les a_n sont nuls pour n assez grand). Le A-module des polynomes de degre $\leqslant d$, $A[X]_{\leqslant d}$ correspond au sous-module des suites $\mathbf{a}$ telles que $\mathrm{supp}(\mathbf{a}) \subset [0, d]$.

L'anneau $(A^{\mathbb{N}}, +, \star)$ des suites dont le support n'est pas forcement fini donne ce qu'on appelle l'anneau des series formelles (pas forcement finies) a coefficients dans A

$$A[[X]] = \{\sum_{n=0}^{\infty} a_n X^n,\ a_n \in A\}.$$

Exercice 6. On considere l'anneau de polynomes a coefficients dans $\mathbb{F}_p$:

$$\mathbb{F}_p[X] = \{P(X) = a_0 + a_1.X + a_2.X^2 + \cdots + a_d.X^d,\ d \geqslant 0, a_0, a_1, \cdots, a_d \in \mathbb{F}_p\}.$$

A un tel polynome on associe la fonction polynomiale $f_P : \mathbb{F}_p \mapsto \mathbb{F}_p$ definie pour $x \in \mathbb{F}_p$ par

$$f_P(x) := a_0 + a_1.x + a_2.x^2 + \cdots + a_d.x^d \in \mathbb{F}_p.$$

On a donc un morphisme d'anneaux (on ne demande pas de le verifier) :

$$P \in \mathbb{F}_p[X] \mapsto f_P \in \mathcal{F}(\mathbb{F}_p; \mathbb{F}_p)$$

de l'anneau des polynomes vers l'anneau des fonctions de $\mathbb{F}_p$ vers $\mathbb{F}_p$ (qui est un anneau pour la somme et le produit des fonctions).

1. Montrer que ce morphisme n'est pas injectif (utiliser l'exercice 4).

Remarque 0.2. Ainsi pour un anneau general, on ne peut PAS identifier un polynome $P \in A[X]$ avec la fonction polynomiale $f_P : A \mapsto A$ qui lui est associe ; d'ou la definition d'un anneau de polynome donnee dans l'exercice 5. En revanche si A est integre et infini l'application $P \mapsto f_P$ est bien injective.