Licence (L3) *Année 2015/2016*

ALGÈBRE

Exercices sur les anneaux

A. CHAMBERT-LOIR

EXERCICE 1

Soit A un anneau et soit S une partie de A.

1 Démontrer que le centralisateur $Z_S(A)$ de S dans A (pour la structure de monoïde multiplicatif) est un sous-anneau de A.

2 En déduire que le centre de A est un sous-anneau de A.

EXERCICE 2

Soit A le sous-anneau de $\mathbf{C}$ engendré par $\sqrt{2}$.

1 Démontrer que pour tout élément a de A, il existe un unique couple (u,v) d'entiers relatifs tels que $a = u + v\sqrt{2}$.

2 Démontrer que le monoïde des endomorphismes de A possède deux éléments, l'identité et l'application donnée par $u + v\sqrt{2} \mapsto u - v\sqrt{2}$.

3 Pour $a = u + v\sqrt{2}$, on pose $N(a) = u^2 - 2v^2$. Démontrer que $N\colon A \to \mathbf{Z}$ est un homomorphisme de monoïdes multiplicatifs.

4 Démontrer que a est inversible dans A si et seulement si $N(a) \in \{\pm 1\}$.

5 Soit a un élément inversible de A. On suppose que $1 < a < 3$; démontrer alors que $a = 1 + \sqrt{2}$. Dans le cas général, démontrer qu'il existe un unique entier $n \in \mathbf{Z}$ tel que $|a| = (1+\sqrt{2})^n$. En déduire que le groupe $A^\times$ est isomorphe à $\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})$.

EXERCICE 3

Soit A le sous-anneau de $\mathbf{C}$ engendré par $\sqrt[3]{2}$.

1 Démontrer que pour tout $a \in A$, il existe un unique triple $(u,v,w) \in \mathbf{Z}^3$ tel que $a = u + v\sqrt[3]{2} + w\sqrt[3]{4}$.

2 Démontrer que l'endomorphisme identique est l'unique endomorphisme de A.

EXERCICE 4

1 Soit A le sous-anneau de $\mathbf{C}$ engendré par i (où $i^2 = -1$) (« entiers de Gauß »).

2 Démontrer que pour tout élément a de A, il existe un unique couple (u,v) d'entiers relatifs tels que $a = u + iv$.

3 Démontrer que le monoïde des endomorphismes de A possède deux éléments, l'identité et la conjugaison complexe.

4 Pour $a = u + iv \in A$, on pose $N(a) = u^2 + v^2 = |a|^2$. Démontrer que $N\colon A \to \mathbf{N}$ est un homomorphisme de monoïdes multiplicatifs.

5 Démontrer que a est inversible dans A si et seulement si $a \in \{\pm 1, \pm i\}$. En déduire que le groupe $A^\times$ est isomorphe à $\mathbf{Z}/4\mathbf{Z}$.

EXERCICE 5

Soit K un corps, soit V un K-espace vectoriel de dimension n, soit $A = \mathrm{End}_K(V)$ l'anneau des endomorphismes de V et soit $u \in A$.

1 Déterminer $\mathrm{Z}_u(A)$ lorsque u est diagonalisable.

2 déterminer $\mathrm{Z}_u(A)$ lorsque le polynôme minimal de u est égal à T^n.

3 Démontrer que le centre de A est l'ensemble des endomorphismes de la forme $v \mapsto \lambda v$, pour $\lambda \in K$.

EXERCICE 6

Soit A un anneau. Soit a un élément de a tel que $a^2 = a$ (on dit que a est idempotent).

1 On pose $A_a = aAa$; Démontrer que l'addition et la multiplication de A font de A_a un anneau. Est-ce un sous-anneau de A ?

2 Démontrer que $1-a$ est idempotent et construire un isomorphisme de l'anneau A sur l'anneau produit $A_a \times A_{1-a}$.

EXERCICE 7

Soit A un anneau.

1 Soit $a \in A$ un élément nilpotent. Démontrer que $1+a$ est inversible dans A et calculer son inverse.

2 Soit a, b des éléments de A ; on suppose que a est inversible, b nilpotent, et que $ab = ba$. Démontrer que $a+b$ est inversible.

3 Soit a, b des éléments nilpotents de A qui commutent. Démontrer que $a+b$ est nilpotent.

4 Donner des exemples qui montrent que dans les deux questions précédentes, on ne peut pas omettre l'hypothèse que a et b commutent.

EXERCICE 8

Soit A un anneau, soit a et b des éléments de A.

1 On suppose que ab est nilpotent. Démontrer que ba est nilpotent. En déduire une formule reliant les inverses de $1-ab$ et de $1-ba$.

2 On suppose que $1-ab$ est inversible dans A. Démontrer que $1-ba$ est inversible.

EXERCICE 9

Soit A un anneau commutatif. Soit $f = a_0 + a_1 T + \cdots + a_n T^n \in A[T]$.

1 Démontrer que f est nilpotent dans l'anneau $A[T]$ si et seulement si, pour tout i, a_i est nilpotent dans A.

2 On suppose que a_0 est inversible et que $a_1, \ldots, a_n$ sont nilpotents dans A ; démontrer que f est inversible dans A.

3 Inversement, on suppose que f est inversible dans $A[T]$ et soit $g = b_0 + \cdots + b_m T^m$ son inverse ; démontrer par récurrence sur k que $a_n^{k+1} b_{m-k} = 0$. En déduire que a_0 est inversible et que $a_1, \ldots, a_n$ sont nilpotents.

4 On suppose que f n'est pas simplifiable. Soit $g \in A[T]$ un polynôme non nul de degré minimal tel que $fg = 0$; démontrer que $a_k g = 0$ pour tout entier k. En déduire qu'il existe un élément non nul $a \in A$ tel que $af = 0$.

EXERCICE 10

Soit K un corps, soit V un K-espace vectoriel de dimension finie et soit A l'anneau $\mathrm{End}_K(V)$ des endomorphismes de V.

1 Soit W un sous-espace vectoriel de V. Démontrer que $N_W = \{u \in A ; W \subset \mathrm{Ker}(u)\}$ est un idéal à gauche de A.

2 Inversement, si I est un idéal à gauche de A, démontrer qu'il existe un unique sous-espace vectoriel W de V tel que $I = N_W$.

3 Soit W un sous-espace vectoriel de V. Démontrer que $I_W = \{u \in A ; \Im(u) \subset W$ est un idéal à droite de A.

4 Inversement, si J est un idéal à droite de A, démontrer qu'il existe un unique sous-espace vectoriel W de V tel que $J = I_W$.

5 Soit I un idéal bilatère de A. Démontrer que $I = \{0\}$ ou $I = A$.

EXERCICE 11

Soit A un anneau et soit I un idéal à droite de A.

1 Démontrer que l'idéal à gauche engendré par I est un idéal bilatère.

2 Soit J l'ensemble des éléments $a \in A$ tels que $xa = 0$ pour tout $x \in I$. Démontrer que J est un idéal bilatère de A.

EXERCICE 12

Soit A un anneau commutatif, soit I et J des idéaux tels que $I + J = A$. Démontrer que $I^n + J^n = A$ pour tout entier $n \geqslant 1$.

EXERCICE 13

Soit A un anneau et soit I l'idéal bilatère de A engendré par les éléments de la forme $xy - yx$, pour $x, y \in A$.

1 Démontrer que l'anneau A/I est commutatif.

2 Soit J un idéal bilatère de A tel que l'anneau A/J soit commutatif. Démontrer que $I \subset J$.

EXERCICE 14

Soit A un anneau commutatif et soit S une partie multiplicative de A. Soit A_S l'anneau des fractions de A à dénominateurs dans S et soit $j : A \to A_S$ l'homomorphisme canonique.

1 Démontrer que le noyau de j est l'ensemble des éléments $a \in A$ tels qu'il existe $s \in S$ tel que $as = 0$.

2 En déduire que j est injectif si et seulement si tout élément de S est simplifiable.

3 Soit $a \in A$. Démontrer que $j(a)$ est inversible dans A_S si et seulement s'il existe $b \in A$ tel que $ab \in S$.

4 Soit S' l'ensemble des éléments $a \in A$ tels qu'il existe $b \in A$ de sorte que $ab \in S$. Démontrer que S' est l'ensemble des éléments $a \in A$ tels que $j(a)$ soit inversible dans A_S.

5 Démontrer qu'il existe un unique homomorphisme d'anneaux de A_S dans $A_{S'}$ qui applique $a/1$ sur $a/1$, pour tout $a \in A$. Démontrer que cet homomorphisme est un isomorphisme.

EXERCICE 15

Soit A un anneau commutatif, soit s un élément de A et soit $S = \{1, s, s^2, \ldots\}$ l'ensemble des puissances de s. Soit A_s l'anneau des fractions de A à dénominateurs dans S ; on le considère comme une A-algèbre au moyen de l'homomorphisme canonique $j\colon A \to A_s$.

1 Démontrer qu'il existe un unique homomorphisme de A-algèbres $f\colon A[T] \to A_s$ qui applique T sur $1/s$.

2 Démontrer que f est surjectif et que son noyau contient $1 - sT$.

3 Démontrer que l'image de s dans l'anneau quotient $A[T]/(1 - sT)$ est inversible.

4 Soit $\varphi\colon A[T]/(1 - sT) \to A_s$ l'homomorphisme déduit de f par passage au quotient. Démontrer que φ est un isomorphisme.

EXERCICE 16

Soit A un anneau. On dit qu'un idéal à gauche I de A est maximal si $I \neq A$ et si pour tout idéal à gauche J de A tel que $I \subset J$, on a $J = I$ ou $J = A$.

1 Démontrer que tout idéal à gauche I de A qui est distinct de A est contenu dans un idéal à gauche maximal.

2 Soit R l'intersection de la famille des idéaux à gauche maximaux de A (« radical de Jacobson » de A). Démontrer qu'un élément a de A appartient à R si et seulement si $1 - xa$ est inversible à gauche, pour tout $x \in A$.

3 Démontrer que R est un idéal bilatère de A.

4 Soit a un élément de A. On suppose que l'image de a dans A/R est inversible ; démontrer que a est inversible.

5 Soit J un idéal à gauche de A tel que $1 + x$ est inversible, pour tout $x \in J$. Démontrer que $J \subset R$.

EXERCICE 17

1 Soit A l'anneau $\mathscr{C}(\mathbf{R};\mathbf{R})$ des fonctions continues de $\mathbf{R}$ dans $\mathbf{R}$. Démontrer que l'ensemble des fonctions à support compact est un idéal de A qui n'est pas contenu dans un idéal de la forme $M_x = \{f\,;\, f(x) = 0\}$, pour $x \in X$.

2 Soit $f_1, \ldots, f_n \in M_0$; démontrer que $\inf(|f_1|, \ldots, |f_n|)^{1/2}$ n'appartient pas à l'idéal engendré par les f_i. En déduire que dans l'anneau A, l'idéal M_0 n'est pas de type fini.

3 Soit B l'anneau des fonctions continues sur le disque unité de $\mathbf{C}$ dont la restriction au disque ouvert est holomorphe. Soit I un idéal de B ; démontrer qu'il existe un polynôme $P \in \mathbf{C}[T]$ dont toutes les racines sont de module $\leqslant 1$ tel que $I = (P)$. En déduire que les idéaux maximaux de B sont les idéaux $(z-a)$, pour $a \in \mathbf{C}$ de module $\leqslant 1$.

EXERCICE 18

Soit A un anneau non nul.

1 On suppose que A possède un seul idéal à gauche maximal M. Démontrer que $A - M$ est l'ensemble $A^\times$ des éléments inversibles de A.

2 On suppose inversement que $M = A - A^\times$ est un sous-groupe du groupe additif de A. Démontrer que M est un idéal bilatère de A, et est l'unique idéal à gauche maximal de A.

EXERCICE 19

Soit A un anneau commutatif possédant un seul idéal maximal. Soit I et J des idéaux de A et soit a un élément simplifiable de A tels que $IJ = (a)$.

1 Démontrer qu'il existe $x \in I$ et $y \in J$ tels que $xy = a$.

2 Démontrer que x et y sont simplifiables.

3 Démontrer que $I = (x)$ et $J = (y)$.

EXERCICE 20

Soit A un anneau commutatif intègre et soit $j\colon A - \{0\} \to \mathbf{N}$ une application. On suppose que pour tous $a, b \in A$ tels que $b \neq 0$, il existe $q, r \in A$ tels que $a = bq + r$ et $r = 0$ ou $j(r) < j(b)$.
Soit $j'\colon A - \{0\} \to \mathbf{N}$ l'application définie par $j'(a) = \inf\{j(ax)\,;\, x \in A - \{0\}\}$. Démontrer que j' est un stathme euclidien sur A.

EXERCICE 21

Soit A un anneau commutatif intègre et soit j un stathme euclidien sur A.

1 Soit $a \in A - \{0\}$ un élément non nul, non inversible, pour lequel $j(a)$ soit minimal. Démontrer que pour tout élément $b \in A - (a)$, il existe un élément inversible $u \in A^\times$ et $v \in A$ tel que $1 = ub + va$.

2 On suppose que $A^\times$ est fini. Démontrer qu'il existe un idéal maximal M de A tel que $\mathrm{Card}(A/M) \leqslant \mathrm{Card}(A^\times) + 1$.

EXERCICE 22

Soit A le sous-anneau de $\mathbf{C}$ engendré par i (anneau des entiers de Gauß).

1 Pour tout $z \in \mathbf{C}$, démontrer qu'il existe $a \in A$ tel que $|a - z|^2 < 1/4$.

2 Démontrer que l'application $N\colon z \mapsto |z|^2$ est un stathme euclidien sur A.

3 Soit $a \in A$ tel que $N(a)$ soit un nombre premier ; démontrer que a est irréductible.

4 Pour tout nombre premier p, démontrer que l'anneau $A/(p)$ est isomorphe à l'anneau $(\mathbf{Z}/p\mathbf{Z})[T]/(T^2+1)$. En déduire que p est irréductible dans A si et seulement si $p \equiv 3 \pmod 4$.

5 Soit p un nombre premier tel que $p \equiv 1 \pmod 4$. Démontrer qu'il existe $u, v \in \mathbf{Z}$ tels que $u^2 + v^2 = p$ (théorème de Fermat sur les sommes de deux carrés).

EXERCICE 23

Soit $f\colon A \to B$ un homomorphisme d'anneaux commutatifs, soit S une partie multiplicative de A et soit T une partie multiplicative de B telle que $f(S) \subset T$. Démontrer qu'il existe un unique homomorphisme d'anneaux $\varphi\colon A_S \to B_T$ qui applique $a/1$ sur $f(a)/1$ pour tout $a \in A$.

EXERCICE 24

Soit A un anneau commutatif, soit S une partie multiplicative de A et soit $j\colon A \to A_S$ l'homomorphisme canonique de A dans l'anneau des fractions de A à dénominateurs dans S.

1 Soit I un idéal de A ; on note I_S l'idéal de A_S engendré par $j(I)$. Démontrer que I_S est l'ensemble des fractions a/s, pour $a \in I$ et $s \in S$.

2 Démontrer que $I_S = A_S$ si et seulement si $S \cap I \neq \emptyset$.

3 Soit J un idéal de A_S et soit $I = j^{-1}(J)$. Démontrer que l'on a $I_S = J$.

4 Soit $f\colon A \to A/I$ l'homomorphisme canonique, soit $T = f(S)$ et soit $k\colon A/I \to (A/I)_T$ l'homomorphisme canonique de A/I dans l'anneau des fractions de A/I à dénominateurs dans T. Démontrer qu'il existe un unique homomorphisme d'anneaux $\varphi\colon (A/I)_T \to A_S/I_S$ qui applique $f(a)/1$ sur la classe de $a/1$ modulo I_S. Démontrer que φ est un isomorphisme.

EXERCICE 25

Soit A un anneau commutatif, soit S un partie multiplicative de A et soit $j\colon A \to A_S$ l'homomorphisme canonique de A dans l'anneau des fractions de A à dénominateurs dans S.

1 Soit P un idéal premier de A tel que $P \cap S = \emptyset$. Démontrer que P_S est un idéal premier de A_S.

2 Soit Q un idéal premier de A_S. Démontrer que $P = j^{-1}(Q)$ est l'unique idéal premier de A tel que $P_S = Q$.

3 On suppose que $S = A - P$, où P est un idéal premier de A. Démontrer que tout idéal de A_P qui est distinct de A_P est contenu dans P_P. En déduire que l'anneau A_P possède un unique idéal maximal.

EXERCICE 26

Soit A un anneau intègre et soit K son corps des fractions. Soit $f = a_n T^n + \cdots + a_0$ un polynôme à coefficients dans A en une indéterminée T.

1 Soit P un idéal premier de A tel que $a_0, \ldots, a_{n-1} \in P$, $a_n \notin P$ et $a_0 \notin P^2$. Démontrer qu'il n'existe pas de polynômes non constants $g, h \in A[T]$ tels que $f = gh$.

On suppose dans la suite que A est un anneau factoriel qu'il existe un un élément irréductible p de A tel que p divise $a_0, \ldots, a_{n-1}$, et p^2 ne divise pas a_0.

2 On suppose de plus que f est de contenu 1. Démontrer que le polynôme f est irréductible dans $A[T]$.

3 Démontrer que le polynôme f est irréductible dans $K[T]$. (« Critère d'Eisenstein ».)

4 Démontrer que pour tout nombre premier p, le polynôme $T^{p-1} + \cdots + T + 1$ est irréductible dans $\mathbf{Q}[T]$. (Faire d'abord une substitution $T = U + 1$.)

5 Soit K un corps. Démontrer que pour tout polynôme $f \in K[X]$ qui n'est pas un carré, le polynôme $Y^2 - f(X)$ est irréductible dans $K[X, Y]$.

EXERCICE 27

Pour tout entier $n \geqslant 1$, soit $\Phi_n \in \mathbf{C}[T]$ le polynôme unitaire dont les racines sont simples, égales aux racines primitives n-ième de l'unité (« polynôme cyclotomique »).

1 Démontrer que pour tout entier $n \geqslant 1$, on a $\prod_{d|n} \Phi_d = T^n - 1$.

2 Calculer Φ_1. Calculer Φ_p si p est un nombre premier.

3 Démontrer par récurrence sur n que $\Phi_n \in \mathbf{Z}[T]$ pour tout entier $n \geqslant 1$.

EXERCICE 28

Soit n un entier $\geqslant 1$. Le but de l'exercice est de démontrer que le polynôme cyclotomique Φ_n est irréductible dans $\mathbf{Q}[T]$.

1 Soit a une racine primitive n-ième de l'unité et soit $P \in \mathbf{Q}[T]$ un polynôme unitaire de degré minimal tel que $P(a) = 0$. Démontrer que $P \in \mathbf{Z}[T]$ et que P divise Φ_n dans $\mathbf{Z}[T]$.

2 Soit p un nombre premier qui ne divise pas n. Démontrer que a^p est une racine primitive p-ième de l'unité.

3 Démontrer que le polynôme $P(T^p) - P(T)^p$ appartient à $p\mathbf{Z}[T]$. En déduire qu'il existe $b \in \mathbf{Z}[a]$ tel que $P(a^p) = pb$.

4 On suppose que $b \neq 0$. Démontrer qu'il existe un polynôme $Q \in \mathbf{Z}[T]$ tel que $T^n - 1 = PQ$ et $Q(a^p) = 0$. En dérivant $T^n - 1$, démontrer que $n \in \mathbf{Z}[a]$ puis en déduire une contradiction.

5 Démontrer que $P(z) = 0$ pour toute racine primitive n-ième de l'unité et en déduire que $P = \Phi_n$.

6 Démontrer que pour tout entier $n \geqslant 1$, le polynôme Φ_n est irréductible dans $\mathbf{Q}[T]$.

EXERCICE 29

Soit A un anneau commutatif. On dit qu'une application $D\colon A \to A$ est une dérivation sur A si c'est un morphisme de groupes additifs et si, pour tout $a, b \in A$, on a $D(ab) = aD(b) + bD(a)$. Soit D une dérivation sur A.

1 Démontrer que pour tout $a \in A$ et tout $n \in \mathbf{N}$, on a $D(a^n) = na^{n-1}D(a)$. Si a est inversible, démontrer cette relation pour $n \in \mathbf{Z}$.

2 Soit B l'ensemble des éléments $a \in A$ tels que $D(a) = 0$. Démontrer que B est un sous-anneau de A.

3 Soit ε la classe de T dans l'anneau quotient $A[T]/(T^2)$. Démontrer que l'application $f\colon A \to A[T]/(T^2)$ définie par $f(a) = a + D(a)\varepsilon$ est un homomorphisme de A-algèbres.

4 Soit K un anneau commutatif ; on suppose que $A = K[T]$. Démontrer qu'il existe une unique dérivation D sur A qui applique T sur 1 et tout polynôme constant sur 0.

EXERCICE 30

Soit A un anneau et soit $f \in A[T]$.

1 Soit I un idéal de A tel que $I^2 = 0$, soit $a \in A$ et $b \in I$. Démontrer que $f(a+b) = f(a) + bf'(a)$. On suppose que $f(a) \in I$ et que $f'(a)$ est inversible modulo I. Démontrer qu'il existe un unique élément $a' \in A$ tel que $a' \equiv a \pmod{I}$ et $f(a') = 0$.

2 Soit I un idéal de A. On suppose qu'il existe un entier $m \geqslant 1$ tel que $I^m = 0$. Soit $a \in A$ tel que $f(a) \in I$ et tel que $f'(a)$ soit inversible modulo I. Démontrer qu'il existe un unique élément $a' \in A$ tel que $a' \equiv a \pmod{I}$ et $f(a') = 0$.

3 Trouver tous les éléments $a \in \mathbf{Z}/125\mathbf{Z}$ tels que $a^2 = -1$.

EXERCICE 31

Soit A un anneau.

1 Soit $a \in A^\times$ et $b \in B$; démontrer qu'il existe un automorphisme φ de la A-algèbre $A[T]$, et un seul, tel que $\varphi(T) = aT + b$.

2 Soit φ un automorphisme de la A-algèbre $A[T]$. Démontrer qu'il existe un unique couple (a, b), où $a \in A^\times$ et $b \in A$, tels que $f = \varphi(T) - aT - b$ soit divisible par T^2.

3 Soit $f \in A$ tel que $f - T$ soit nilpotent. Démontrer qu'il existe un automorphisme φ de $A[T]$, et un seul, tel que $\varphi(T) = f$.

EXERCICE 32

Soit $A = \mathbf{Z}[i\sqrt{5}]$ le sous-anneau de $\mathbf{C}$ engendré par $i\sqrt{5}$.

1 Démontrer que tout élément de A s'écrit de manière unique sous la forme $a + ib\sqrt{5}$, pour $a, b \in \mathbf{Z}$.

2 Démontrer que $A^\times = \{\pm 1\}$.

3 Démontrer que $2, 3, 1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles dans A.

4 Démontrer que A n'est pas un anneau factoriel.

EXERCICE 33 (Nullstellensatz combinatoire [?])

Soit K un corps commutatif, soit n un entier $\geqslant 1$, et soit $f \in K[T_1,\dots,T_n]$. Pour $i \in \{1,\dots,n\}$, soit A_i une partie de K et soit $g_i = \prod_{a\in A_i} (T_i - a)$.

1 On suppose que f s'annule en tout point de $A_1 \times \cdots \times A_n$. On suppose que $\mathrm{Card}(A_i) > \deg_{T_i}(f)$ pour tout i, alors $f = 0$. (Traiter d'abord le cas $n = 1$ puis raisonner par récurrence sur n.)

2 On suppose encore que f s'annule en tout point de $A_1 \times \cdots \times A_n$. Démontrer qu'il existe des polynômes $h_1,\dots,h_n \in K[T_1,\dots,T_n]$ tels que $f = \sum_{i=1}^{n} g_i h_i$ et $\deg(g_i) + \deg(h_i) \leqslant \deg(f)$ pour tout i.

3 Soit $m = (m_1,\dots,m_n) \in \mathbf{N}^n$ tel que le coefficient de T^m dans f soit non nul et tel que $\deg(f) = m_1 + \cdots + m_n$. On suppose que $\mathrm{Card}(A_i) > m_i$ pour tout i. Démontrer qu'il existe $a \in A_1 \times \cdots \times A_n$ tel que $f(a) \neq 0$.

EXERCICE 34

Soit p un nombre premier.

1 Soit C une partie de $\mathbf{Z}/p\mathbf{Z}$, distincte de $\mathbf{Z}/p\mathbf{Z}$, et soit $f_C \in (\mathbf{Z}/p\mathbf{Z})[X,Y]$ le polynôme $\prod_{c\in C} (X + Y - c)$. Soit $m, n \in \mathbf{N}$ tels que $\mathrm{Card}(C) = m + n$. Démontrer que le coefficient de $X^m Y^n$ dans f n'est pas nul.

2 Soit A, B des sous-ensembles non vides de $\mathbf{Z}/p\mathbf{Z}$; on pose $C = A + B$. On suppose que $\mathrm{Card}(A) + \mathrm{Card}(B) > p$; démontrer que $C = \mathbf{Z}/p\mathbf{Z}$.

3 On suppose que $\mathrm{Card}(A) + \mathrm{Card}(B) \leqslant p$. Observer que $f_C(a,b) = 0$ pour tout $(a,b) \in A \times B$. Utiliser le résultat de l'exercice 33 pour démontrer l'*inégalité de Cauchy–Davenport :*

$$\mathrm{Card}(A + B) \geqslant \mathrm{Card}(A) + \mathrm{Card}(B) - 1.$$

EXERCICE 35

Soit p un nombre premier.

1 Soit d un entier $\geqslant 1$. Démontrer qu'il existe un élément d'ordre multiplicatif d dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si d divise $p - 1$.

2 Démontrer que -1 est un carré dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si $p \equiv 1 \pmod 4$ ou $p = 2$.

3 Démontrer que l'équivalence des propriétés suivantes : (i) Le polynôme $T^2 + T + 1$ est réductible dans $(\mathbf{Z}/p\mathbf{Z})[T]$; (ii) -3 est un carré dans $\mathbf{Z}/p\mathbf{Z}$; (iii) $p \equiv 1 \pmod 3$.

EXERCICE 36

1 Soit M un monoïde commutatif vérifiant la propriété $(*)$: pour tout $m \in M$, l'ensemble des couples $(p,q) \in M \times M$ tels que $p + q = m$ est fini. Soit A un anneau commutatif.
Montrer que le produit de convolution définit encore une loi commutative et associative sur A^M. Vérifier qu'alors $(A^M, +, *)$ est une A-algèbre commutative et associative dont $A^{(M)}$ est une sous-algèbre. (« Algèbre large du monoïde M ».)

2 Soit n un entier naturel. Démontrer que le monoïde $M = \mathbf{N}^n$ vérifie la propriété $(*)$.

3 Démontrer qu'une fonction $f \in A^M$ est inversible pour le produit de convolution si et seulement $f(0) \in A^\times$.

4 On suppose que A est un anneau noethérien et que $M = \mathbf{N}$. Démontrer que $(A^{\mathbf{N}}, +, *)$ est un anneau noethérien.

EXERCICE 37

Soit A un anneau.

1 Soit (P_i) une famille totalement ordonnée d'idéaux premiers de A. Démontrer que son intersection $P = \bigcap_i P_i$ est un idéal premier de A.

2 Démontrer que tout idéal premier de A contient un idéal premier minimal.

EXERCICE 38

Soit n un entier naturel. Soit K un corps commutatif. Soit A l'anneau $K[T_1, \ldots, T_n]$ et soit P l'anneau des fonctions de K^n dans K.

1 Pour tout $f \in A$, on note $\varphi(f)$ la fonction de K^n dans K donnée par $a \mapsto f(a)$. Démontrer que l'application $\varphi\colon A \to P$ est un homomorphisme d'anneaux.

2 On suppose que K est un corps infini. Démontrer que l'homomorphisme φ est injectif mais pas surjectif.

3 On suppose que K est un corps fini. Démontrer que l'homomorphisme φ est surjectif mais pas injectif.