M1 MA 2021–2022, ALGÈBRE
CORRIGÉ DE L'EXAMEN DU MERCREDI 12 JANVIER 2022

PAUL LESCOT

Exercice I

(1) Si $f : A \to B$ est un morphisme d'anneaux, on doit avoir, pour chaque entier $k \geq 1$:

$$\begin{aligned} f(\bar{k}) &= f(\underbrace{\bar{1} + ... + \bar{1}}_{k \text{ termes}}) \\ &= f(\underbrace{1_A + ... + 1_A}_{k \text{ termes}}) \\ &= \underbrace{f(1_A) + ... + f(1_A)}_{k \text{ termes}} \\ &= kf(1_A) \\ &= kf(\bar{1}). \end{aligned}$$

L'égalité ci–dessus est évidente pour $k = 0$, et elle est exacte pour $-k$ si elle l'est pour k ; on a donc

$$(\forall k \in \mathbf{Z})\ f(\bar{k}) = kf(\bar{1}).$$

Le morphisme f est donc déterminé par $f(\bar{1})$. De plus on doit avoir

$$f(\bar{1}) = f(\bar{1}^2) = (f(\bar{1}))^2,$$

c'est–à–dire que $f(\bar{1}) \in B$ est idempotent.

Réciproquement, si $e \in B$ est idempotent, l'application

$$\begin{array}{rccc} f & : & \dfrac{\mathbf{Z}}{84\mathbf{Z}} & \to & \dfrac{\mathbf{Z}}{21\mathbf{Z}} \\ & & \bar{k} & \mapsto & ke \end{array}$$

est bien définie et un morphisme d'anneaux. Par exemple, pour tout $(k, l) \in \mathbf{Z}^2$:

$$\begin{aligned} f(\bar{k}\bar{l}) &= f(\overline{kl}) \\ &= kle \\ &= kle^2 \\ &= (ke)(le) \\ &= f(\bar{k})f(\bar{l}). \end{aligned}$$

Les morphismes d'anneaux de A dans B correspondent donc bijectivement aux idempotents de B. Or ces derniers sont au nombre de quatre :

$\tilde{0}$, $\tilde{1}$, $\tilde{7}$ et $\tilde{15}$. On peut le voir par examen direct des 21 éléments de B ; on peut aussi utiliser l'isomorphisme d'anneaux

$$\frac{\mathbf{Z}}{21\mathbf{Z}} \simeq \frac{\mathbf{Z}}{3\mathbf{Z}} \times \frac{\mathbf{Z}}{7\mathbf{Z}}$$

donné par le Théorème des Restes Chinois. En effet, dans un corps K, les seuls idempotents sont 0_K et 1_K. Un élément $\tilde{n}$ de $\dfrac{\mathbf{Z}}{21\mathbf{Z}}$ est idempotent si et seulement si chaque composante de son image dans $\dfrac{\mathbf{Z}}{3\mathbf{Z}} \times \dfrac{\mathbf{Z}}{7\mathbf{Z}}$ l'est, c'est à dire si et seulement si n est congru à 0 ou 1 modulo 3 et congru à 0 ou 1 modulo 7. On obtient donc quatre possibilités :

$$n \equiv 0[3] \text{ et } n \equiv 0[7]$$

$$n \equiv 0[3] \text{ et } n \equiv 1[7],$$

$$n \equiv 1[3] \text{ et } n \equiv 0[7],$$

$$n \equiv 1[3] \text{ et } n \equiv 1[7],$$

équivalant respectivement à

$$n \equiv 0\,[21],$$

$$n \equiv 15\,[21],$$

$$n \equiv 7\,[21],$$

et

$$n \equiv 1\,[21].$$

Les morphismes recherchés sont donc

$$\bar{k} \mapsto \tilde{0},$$

$$\bar{k} \mapsto 15\tilde{k},$$

$$\bar{k} \mapsto 7\tilde{k}$$

et

$$\bar{k} \mapsto \tilde{k}.$$

(2) Un morphisme ψ d'anneaux unitaires de A dans B doit vérifier

$$\psi(\bar{1}) = \psi(1_A) = 1_B = \tilde{1}.$$

D'après (1), on a donc

$$(\forall k \in \mathbf{Z})\ \psi(\bar{k}) = \tilde{k}.$$

Réciproquement, ce ψ convient.

Exercice II

Soit $n \in \mathcal{E}$, et soit p un diviseur premier de n ; alors $p-1 \mid \phi(n) = 78$, d'où

$$p - 1 \in \{1, 2, 3, 6, 13, 26, 39, 78\}$$

et

$$p \in \{2, 3, 4, 7, 14, 27, 40, 79\}.$$

p étant premier, on a nécessairement

$$p \in \{2, 3, 7, 79\}.$$

Supposons que 79 ne divise pas n ; alors les facteurs premiers de $\phi(n)$ figurent parmi 2, 3, 7 et ceux de $2-1=1$, $3-1=2$ et $7-1=6$; en particulier $13 \in \{2, 3, 7\}$, une contradiction. Donc 79 divise n ; mais 79^2 ne divise pas n, sans quoi $79.78 = 79(79-1)$ diviserait $\phi(n) = 78$. On a donc $n = 79m$ avec $79 \nmid m$; mais alors m et 79 sont premiers entre eux, donc

$$78 = \phi(n) = \phi(79m) = \phi(79)\phi(m) = 78\phi(m),$$

donc $\phi(m) = 1$, $m \in \{1, 2\}$ et $n = 79m \in \{79, 158\}$.

Réciproquement ces nombres conviennent, d'où

$$\mathcal{E} = \{79, 158\}.$$

On pouvait également procéder par force brute, en considérant une par une les seize possibilités pour l'ensemble des facteurs premiers de n : $n = 2^a$, $n = 2^a 3^b 79^c$, etc. .

Exercice III

(1) De $x^2 = 0_A$ suit que $-x = x^3 = x.x^2 = x.0_A = 0_A$ et donc $x = 0_A$.

(2) En appliquant l'hypothèse à x^2, on obtient

$$(x^2)^3 = -x^2,$$

soit

$$x^6 = -x^2.$$

Mais

$$x^6 = (x^3)^2 = (-x)^2 = x^2$$

d'où

$$x^2 = x^6 = -x^2$$

et le résultat.

(3) Tout d'abord, on a, pour chaque $x \in A$:

$$x^4 = x.x^3 = x.(-x) = -x^2 = x^2$$

(on a utilisé (2)) d'où

$$\begin{aligned}(y^2x + y^2xy^2)^2 &= y^2xy^2x + y^2xy^2xy^2 + y^2xy^4x + y^2xy^4xy^2 \\ &= y^2xy^2x - y^2xy^2xy^2 - y^2xy^2x + y^2xy^2xy^2 \\ &= 0_A,\end{aligned}$$

d'où, d'après (1), $y^2x + y^2xy^2 = 0_A$.

On voit de façon similaire que

$$xy^2 + y^2xy^2 = 0_A.$$

(4) D'après (3), on a, pour chaque $x \in A$:

$$xy^2 = -y^2xy^2 = y^2x,$$

d'où $y^2 \in Z(A)$.

(5) On a

$$-xy = (xy)^3 = xyxyxy = x(yx)^2y.$$

(6) Soit $(x, y) \in A^2$; on a

$$\begin{aligned} -xy &= x(yx)^2y \\ &\quad \text{(d'après (5))} \\ &= (yx)^2xy \\ &\quad \text{(d'après (4))} \\ &= yxyx^2y \\ &= yxx^2yy \\ &\quad \text{(d'après (4))} \\ &= yx^3y^2 \\ &= -yx^3y^2 \\ &\quad \text{(d'après (2))} \\ &= -yy^2x^3 \\ &= -y^3x^3 \\ &= -(-y)(-x) \\ &= -yx, \end{aligned}$$

d'où $xy = yx$: A est commutatif.

Exercice IV

(1) Soit

$$B := \{\begin{bmatrix} a & \bar{0} \\ \bar{0} & b \end{bmatrix} | (a, b) \in (\frac{\mathbf{Z}}{19\mathbf{Z}})^2\}.$$

On a

$$1_A = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix} \in B.$$

Si

$$x = \begin{bmatrix} a & \bar{0} \\ \bar{0} & b \end{bmatrix} \in B$$

et

$$y = \begin{bmatrix} c & \bar{0} \\ \bar{0} & d \end{bmatrix} \in B,$$

alors

$$x - y = \begin{bmatrix} a-c & \bar{0} \\ \bar{0} & b-d \end{bmatrix} \in B$$

et

$$xy = \begin{bmatrix} ac & \bar{0} \\ \bar{0} & bd \end{bmatrix} \in B.$$

Donc B est un sous–anneau unitaire de A ; il est clair que

$$|B| = 19^2 = 361.$$

Soient

$$x = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix} \in B$$

et

$$y = \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix} \in B.$$

Alors $x \neq 0_B$, $y \neq 0_B$ et $xy = 0_B$: B n'est pas intègre.

Une construction similaire est possible en remplaçant 19 par n'importe quel nombre premier.

(2) Soit

$$C := \{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} | (a,b) \in (\frac{\mathbf{Z}}{19\mathbf{Z}})^2 \}.$$

On a

$$1_A = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix} \in C.$$

Si

$$x = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in C$$

et

$$y = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \in C,$$

alors

$$x - y = \begin{bmatrix} a-c & b-d \\ -(b-d) & a-c \end{bmatrix} \in C$$

et

$$xy = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \in C.$$

Donc C est un sous–anneau unitaire de A ; il est clair que

$$|C| = 19^2 = 361.$$

Pour montrer que C est un corps, il suffit d'établir que chaque élément non nul de C est inversible dans C.

Soit donc

$$x = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in C,$$

$x \neq 0_C$.

Alors $a \neq \bar{0}$ ou $b \neq \bar{0}$; supposons par exemple $a \neq \bar{0}$. Vu que $-\bar{1}$ n'est pas un carré dans $\frac{\mathbf{Z}}{19\mathbf{Z}}$ (car $19 \equiv 3[4]$; cf. p. 15 des notes), on a $-\bar{1} \neq (\frac{b}{a})^2$, d'où $a^2 + b^2 \neq \bar{0}$.

Soit alors

$$y = \begin{bmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix}.$$

Alors $y \in C$ et un calcul simple permet d'établir que

$$xy = yx = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix} = 1_C :$$

x est inversible. Donc C est un corps.

Une construction similaire est possible en remplaçant 19 par n'importe quel nombre premier de la forme $4n + 3$.