M1 MFA 2020–2021, ALGÈBRE
CORRIGÉ DE L'EXAMEN DU 12 JANVIER 2021

PAUL LESCOT

Exercice I

Soit $n \in \mathcal{E}$.

Comme rappelé, chaque diviseur premier p de n est tel que $p-1$ divise $\phi(n) = 42 = 2.3.7$, donc

$$p - 1 \in \{1, 2, 3, 6, 7, 14, 21, 42\},$$

ou

$$p \in \{2, 3, 4, 7, 8, 15, 22, 43\},$$

soit

$$p \in \{2, 3, 7, 43\}.$$

Supposons que 43 divise n ; alors 43^2 ne peut pas diviser n, sans quoi $43.42 = 43.(43-1)$ diviserait $\phi(n) = 42$. On a donc $n = 43m$ avec m non divisible par 43, donc premier avec lui ; il s'ensuit que

$$42 = \phi(n) = \phi(43m) = \phi(43)\phi(m) = 42\phi(m)$$

d'où $\phi(m) = 1$, $m = 1$ ou $m = 2$ et $n = 43$ ou $n = 86$.

Supposons maintenant que 43 ne divise pas n ; alors chaque facteur premier de n appartient à

$$\{2, 3, 7\},$$

et apparaissent huit possibilités :

(1) $n = 1$
(2) $n = 2^\alpha$
(3) $n = 3^\alpha$
(4) $n = 7^\alpha$
(5) $n = 2^\alpha 3^\beta$
(6) $n = 2^\alpha 7^\beta$
(7) $n = 3^\alpha 7^\beta$
(8) $n = 2^\alpha 3^\beta 7^\gamma$

Dans le cas (1), $\phi(n) = 1$: absurde.

Dans le cas (2), $42 = \phi(n) = 2^{\alpha-1}(2-1) = 2^{\alpha-1}$, ce qui est absurde.

Dans le cas (3), $\phi(n) = 3^{\alpha-1}(3-1) = 2.3^{\alpha-1}$ ne saurait être égal à 42.

Dans le cas (4), $42 = \phi(n) = 7^{\alpha-1}(7-1) = 7^{\alpha-1}6$, d'où $\alpha - 1 = 1$, $\alpha = 2$ et $n = 7^2 = 49$.

Dans le cas (5), $\phi(n) = 2^{\alpha-1}(2-1)3^{\beta-1}(3-1)$ n'est pas divisible par 7, en particulier n'est pas égal à 42.

Dans le cas (6), $42 = \phi(n) = 2^{\alpha-1}(2-1).7^{\beta-1}.6$, donc $\alpha = 1$, $\beta = 2$ et $n = 2.7^2 = 98$.

Dans le cas (7), $\phi(n)$ est divisible par $(3-1)(7-1)=12$, donc différent de 42. On élimine de même le cas (8).

En conclusion, il nous reste donc quatre possibilités pour n : 43, 49, 86, 98, lesquelles conviennent effectivement.

On a donc

$$\mathcal{E}=\{43,49,86,98\}.$$

Exercice II

(1) Pour tout $(x,y)\in A^2$, l'on peut écrire

$$\begin{aligned}-x-y+xy+yx &= x^2+y^2+xy+yx\\ &= (x+y)^2\\ &= -(x+y)\\ &= -x-y\end{aligned}$$

d'où $xy+yx=0_A$ et $xy=-yx$.

(2) Pour chaque $x\in A$, on a

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

soit

$$x^2=x$$

et

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

Mais alors, pour tout $(x,y)\in A^2$,

$$xy=-yx=yx$$

et $xy=yx$: A est commutatif.

(3) On vient de voir que, pour chaque $x\in A$, $x^2=x$. Si $x\neq 0_A$, vu que A est un corps, il suit de

$$x.x=x^2=x.1_A$$

que $x=1_A$. On a donc $A=\{0_A,1_A\}$; A est un corps à deux éléments, donc isomorphe à $\dfrac{\mathbf{Z}}{2\mathbf{Z}}$.

Exercice III

(1) I (en tant qu'idéal) et $\mathbf{Z}$ (en tant que sous–anneau) sont des sous–groupes additifs de B, donc $J=I\cap\mathbf{Z}$ en est un ; vu que $J\subset\mathbf{Z}$, J est un sous–groupe additif de $\mathbf{Z}$. Pour $a\in\mathbf{Z}$ et $b\in J$, on a $b\in\mathbf{Z}$ (donc $ab\in\mathbf{Z}$) et $b\in I$ et $a\in B$ (car $\mathbf{Z}\subset B$), donc $ab\in I$ et $ab\in I\cap\mathbf{Z}=J$: J est un idéal de $\mathbf{Z}$.

Vu que I est maximal dans B, $I\neq B$ et $1_B\notin I$; mais $1_B=1$ car $\mathbf{Z}$ est un sous–anneau unitaire de B, donc $1\notin I$, $1\notin J=I\cap\mathbf{Z}$ et $J\neq\mathbf{Z}$.

Soit $(a,b)\in\mathbf{Z}^2$ avec $ab\in J$; alors $(a,b)\in B^2$ et $ab\in I$. Mais I est maximal dans B, donc premier, d'où $a\in I$ ou $b\in I$. Dans le premier cas, $a\in I\cap\mathbf{Z}=J$, et de même, dans le second cas, $b\in I\cap\mathbf{Z}=J$: J est un idéal premier de $\mathbf{Z}$.

(2) On vient de voir que J est un idéal premier de $\mathbf{Z}$; on sait qu'alors $J = \{0\}$ ou $J = p\mathbf{Z}$ pour un (unique) p premier. Le cas $J = \{0\}$ étant exclu par hypothèse, on a le résultat.

(3) I étant un idéal maximal de B, le quotient $\dfrac{B}{I}$ est un corps. On a $p = p.1 \in p\mathbf{Z} = J = I \cap \mathbf{Z}$, d'où $p \in I$. Mais alors, dans $K := \dfrac{B}{I}$:

$$\begin{aligned} p.1_K &= p\overline{1_B} \\ &= p\bar{1} \\ &= \overline{p.1} \\ &= \bar{p} \\ &= \bar{0} \\ &(\quad \text{car } p \in I \ ) \\ &= 0_K : \end{aligned}$$

K est de caractéristique p.

Exercice IV

Notons $\bar{n}$ la classe modulo $3\mathbf{Z}$ de $n \in \mathbf{Z}$.
Soit

$$K := \{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} | (a,b) \in (\frac{\mathbf{Z}}{3\mathbf{Z}})^2\}.$$

Il est visible que $|K| = |\dfrac{\mathbf{Z}}{3\mathbf{Z}}|^2 = 3^2 = 9$, et que K est un sous–groupe additif de $A := \mathcal{M}_2(\dfrac{\mathbf{Z}}{3\mathbf{Z}})$.

Si $(M, M^{'}) \in K^2$, écrivons

$$M = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

et

$$M^{'} = \begin{bmatrix} a^{'} & b^{'} \\ -b^{'} & a^{'} \end{bmatrix}.$$

Alors

$$MM^{'} = \begin{bmatrix} aa^{'} - bb^{'} & ab^{'} + ba^{'} \\ -(ab^{'} + ba^{'}) & aa^{'} - bb^{'} \end{bmatrix} \in K :$$

K est un sous–anneau de A.
Au passage on obtient que

$$(\forall (M, M^{'}) \in K^2) \ MM^{'} = M^{'}M :$$

K est commutatif.
Vu que

$$1_A = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix} = \begin{bmatrix} \bar{1} & \bar{0} \\ -\bar{0} & \bar{1} \end{bmatrix} \in K,$$

K est un sous–anneau commutatif et unitaire de A.

Il suffit donc de montrer que chaque élément non nul k de K est inversible dans K. Soit donc

$$k = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

Par hypothèse a ou b n'est pas nul ; or, dans $\mathbf{F}_3$, le carré de chaque élḿent non nul vaut $\bar{1}$. L'un de a^2 et b^2 vaut donc $\bar{1}$, et l'autre $\bar{0}$ ou $\bar{1}$. Il s'ensuit que $a^2 + b^2 \in \{\bar{1}, \bar{2}\}$; en particulier, $a^2 + b^2 \neq \bar{0}$.

Ecrivons alors

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

Il est facile de voir que $l \in K$ et

$$lk = kl = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix} = 1_A = 1_K.$$