Master 1 Mathématiques et Applications : Algèbre
Corrigé de l'examen du 16 janvier 2018

Paul Lescot

Exercice I

1. Il suffit de montrer que chaque élément non nul de A est inversible. Soit donc $a \in A$, $a \neq 0_A$. Considérons l'application

$$\begin{array}{rcl} \phi & : & A \to A \\ & & x \mapsto ax. \end{array}$$

Si l'on a $\phi(x) = \phi(y)$, alors $ax = ay$ d'où

$$a(x-y) = ax - ay = ax - ax = 0_A \ ;$$

vu que A est intègre et que $a \neq 0_A$, il suit que $a = 0_A$ ou $x - y = 0_A$, soit $x = y$. Nous avons établi l'injectivité de ϕ

Mais ϕ est une application de l'ensemble fini A dans lui–même ; elle est donc surjective. En particulier, il existe $b \in A$ tel que $1_A = \phi(b) = ab$. Mais alors $ba = ab = 1_A$: a est inversible.

2.

3. Si $\theta^{-1}(y) = \emptyset$, le résultat est évident. Dans le cas contraire, fixons un $u \in \theta^{-1}(y)$; alors

$$au = \theta(u) = y.$$

Soit maintenant $z \in \theta^{-1}(y)$; de $az = \theta(z) = y$ suit que $az = au$ donc (comme en 1.) $a(z-u) = 0_A$. Vu que $a \neq 0_A$, $z - u$ est soit nul soit un diviseur de 0, c'est–à–dire que

$$z - u \in \mathcal{D}(A) \cup \{0_A\}.$$

Il y a donc au plus $|\mathcal{D}(A) \cup \{0_A\}| = 1 + |\mathcal{D}(A)|$ possibilités pour z, d'où le résultat.

4. On peut écrire

$$b\theta(x) = b(ax) = (ab)x = 0_A x = 0_A.$$

Vu que $b \neq 0_A$, $\theta(x)$ est soit nul soit un diviseur de 0, C.Q.F.D. .

5. Soit $C = \theta(A) := \{\theta(x) | x \in A\}$; il résulte de 4. que $C \subseteq \mathcal{D}(A) \cup \{0_A\}$, d'où

$$|C| \leq |\mathcal{D}(A) \cup \{0_A\}| = 1 + |\mathcal{D}(A)|.$$

Mais

$$\begin{aligned} |A| &= \sum_{y\in C} |\theta^{-1}(y)| \\ &\leq \sum_{y\in C} (1+|\mathcal{D}(A))| \text{ (d'après 3.)} \\ &= (1+|\mathcal{D}(A)|)|C| \\ &\leq (1+|\mathcal{D}(A)|)^2. \end{aligned}$$

On a donc $1+|\mathcal{D}(A)| \geq \sqrt{|A|}$, d'où le résultat voulu.

6. Soit $A = \dfrac{\mathbf{Z}}{p^2\mathbf{Z}}$; on a bien $|A| = p^2$.

   Soit alors $x = \overline{n}$ un élément de $\dfrac{\mathbf{Z}}{p^2\mathbf{Z}}$.

   Si p ne divise pas n alors x est inversible, donc ni nul ni diviseur de 0.

   Si p divise n, p^2 divise pn et $\overline{p}x = \overline{pn} = \overline{pn} = \overline{0} = 0_A$; vu que $\overline{p} \neq 0_A$, x est soit nul soit un diviseur de 0.

   Les diviseurs de 0 sont donc exactement les $\overline{n}$ pour $n \in \{0, ..., p^2-1\}$ divisible par p mais non par p^2 ; ces n sont les pm pour $1 \leq m \leq p-1$. On a donc bien $|\mathcal{D}(A)| = p-1 = \sqrt{|A|}-1$.

Exercice II

Que 1. entraîne 2. a été vu en cours.

Réciproquemant, supposons A principal, soit $a \in A \setminus \{0_A\}$, et considérons l'idéal I de B engendré par a et x :

$$I = aB + xB$$

(comme il est usuel, on identifie les éléments de A et les polynômes de degré 0).

Par hypothèse il existe un polynôme $P(x) \in A[x] = B$ tel que $I = P(x)B$. Vu que $a = a.1_A + x.0_A \in B$, $P(x)$ divise $a \neq 0_A$; en particulier $P(x)$ est de degré 0, donc égal à une constante $c \in A \setminus \{0_A\}$.

Mais alors, du fait que $x = a.0_A + 1_A.x \in B$, $c = P(x)$ divise x : $x = cS(x)$ pour un certain $S(x) \in B$. Mais alors, en évaluant au point $x = 1_A$, il vient que

$$1_A = cS(1_A).$$

Vu que $c = c.1_A \in cB = I$, il existe $T(x) \in B$ et $U(x) \in B$ tels que

$$c = aT(x) + xU(x).$$

En évaluant cette fois au point 0_A il vient que

$$c = aT(0_A) + 0_A U(0_A) = aT(0_A).$$

Soit alors $d := T(0_A)S(1_A) \in A$; on voit que

$$da = ad = aT(0_A)S(1_A) = (aT(0_A))S(1_A) = cS(1_A) = 1_A,$$

et a est inversible.

Donc tout élément non nul de A est inversible : A est un corps, soit 1..

Remarque 0.1 *Cet argument avait été vu en cours dans le cas particulier $A = \mathbf{Z}$ et $a = 2$ ... .*

Exercice III

1. Par hypothèse on a

$$\begin{aligned} x+x &= (x+x)^2 \\ &= (x+x)(x+x) \\ &= x^2+x^2+x^2+x^2 \\ &= x+x+x+x. \end{aligned}$$

   Il s'ensuit bien que $x+x=0_A$.

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

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

   d'où $xy+yx=0_A$. Mais, en vertu de 1., on a $xy+xy=0_A$, d'où $xy+yx=xy+xy$ et $yx=xy$: A est commutatif.

3. Vérifions une par une les propriétes caractéristiques d'une relation d'ordre.

   Soit $x\in A$; alors $xx=x^2=x$ donc $x\leq x$: $\leq$ est **réflexive**.

   Soit $(x,y)\in A^2$ avec $x\leq y$ et $y\leq x$; alors $xy=x$ et $yx=y$, d'où

$$x=xy=yx=y$$

   et $x=y$: $\leq$ est antisymétrique .

   Soit $(x,y,z)\in A^3$ avec $x\leq y$ et $y\leq z$; alors $xy=x$ et $yz=y$. Il apparaît que

$$xz=(xy)z=x(yz)=xy=x,$$

   soit $x\leq z$: $\leq$ est **transitive** .

4. Supposons qu'il n'y ait pas d'élément maximal dans A, et soit $m_0\in A$ (par exemple $m_0=0_A$). Vu que m_0 n'est pas maximal, il existe $m_1\neq m_0$ tel que $m_0\leq m_1$, donc $m_0<m_1$. De même, m_1 n'étant pas maximal, il existe $m_2\in A$ tel que $m_1<m_2$. En continuant ce processus on construit une suite infinie d'éléments de A strictement croissante (pour $\leq$) ; en particulier, A est infini : absurde !

   Remarque 0.2 *Cet argument établit plus généralement que, pour toute relation d'ordre sur un ensemble fini non vide admet au moins un élément maximal, et d'ailleurs aussi au moins un élément minimal.*

   Soit donc e un élément de A maximal pour $\leq$; alors, pour chaque $x\in A$:

$$\begin{aligned} e(x+e-ex) &= ex+e^2-ex \\ &= ex+e-ex \\ &= e \end{aligned}$$

soit $e \leq e + x - ex$; de la maximalité de e suit maintenant que $e = e + x - ex$, soit $ex = x$. Mais alors

$$(\forall x \in A)\ xe = ex = x$$

et e est l'unité de A.

5. Soit E un ensemble ; on a vu en cours que $B := \mathcal{P}(E)$, muni de la différence symétrique pour addition et de l'intersection pour multiplication, était un anneau commutatif.

   Prenons E infini (par exemple $E = \mathbf{N}$), et soit $A = \mathcal{P}_f(E)$ l'ensemble des parties **finies** de E ; il est visible que A est un sous–anneau de B. De plus, pour chaque $x \in A$ on a

   $$x^2 = x.x = x \cap x = x,$$

   donc l'anneau A vérifie (**).

   Supposons A unitaire, et soit I son unité ; alors I est une partie de E.

   Pour $x \in E$, posons $C = \{x\} \in \mathcal{P}_f(E) = A$; alors $C.I = C$, soit $C \cap I = C$, d'où $\{x\} = C \subset I$ et $x \in I$. On a donc $E \subset I$, donc $E = I \in A = \mathcal{P}_f(E)$ et E est fini, une contradiction.

   A n'est donc pas unitaire.

.