ALGEBRE[1]

Corrigé de l'examen du 2 septembre 2004

durée : 2 heures

I

On considère les polynômes P_1,P_2 et P_3 dans $\mathbb{Z}/2\mathbb{Z}[X]$ définis par

$$P_1 = X^5 - \bar{1}X - \bar{1}, \quad P_2 = X^3 + X^2 + \bar{1} \quad \text{et} \quad P_3 = X^2 + X + \bar{1}.$$

Montrer que $P_1 = P_2 \cdot P_3$.

Solution. On a en utilisant $\bar{1} + \bar{1} = \bar{0}$,

$$\begin{aligned} P_2 \cdot P_3 &= (X^3 + X^2 + \bar{1}) \cdot (X^2 + X + \bar{1}) \\ &= X^5 + (\bar{1} + \bar{1})X^4 + (\bar{1} + \bar{1})X^3 + (\bar{1} + \bar{1})X^2 + \bar{1}X + \bar{1} \\ &= X^5 + \bar{1}X + \bar{1} \end{aligned}$$

C'est le résultat demandé car, dans $\mathbb{Z}/2\mathbb{Z}$, $\bar{1} = -\bar{1}$.

□

II

A – a) On considère l'application ϕ définie pour $a \in \mathbb{Z}/4\mathbb{Z}$ par $\phi(a) = \bar{2} \cdot a$. Calculer les images des quatre éléments de $\mathbb{Z}/4\mathbb{Z}$. L'application Φ est-elle un endomorphisme du groupe $(\mathbb{Z}/4\mathbb{Z},+)$? un automorphisme ?

Solution. On a $\phi(\bar{0}) = \bar{2} \cdot \bar{0} = \bar{0}$, $\phi(\bar{1}) = \bar{2} \cdot \bar{1} = \bar{2}$, $\phi(\bar{2}) = \bar{2} \cdot \bar{2} = \bar{4} = \bar{4}$, $\phi(\bar{3}) = \bar{2} \cdot \bar{3} = \bar{6} = \bar{2}$. En utilisant la distributivité de $\cdot$ par rapport à $+$ dans l'anneau $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ on obtient $\phi(a + b) = \bar{2} \cdot a + b = \bar{2} \cdot a + \bar{2} \cdot b$ qui montre que ϕ est un morphisme. Ce n'est pas un automorphisme car il n'est pas injectif $(\phi(\bar{0}) = \phi(\bar{2}) = \bar{0})$.

□

b) Déterminer tous les automorphismes de $(\mathbb{Z}/4\mathbb{Z},+)$.

Solution. Soit ψ un morphisme quelconque de $(\mathbb{Z}/4\mathbb{Z},+)$. On a nécessairement $\psi(\bar{0}) = 0$ (car l'image du neutre est égale au neutre) puis $\psi(\bar{2}) = \psi(\bar{1} + \bar{1}) = \psi(\bar{1}) + \psi(\bar{1})$ et $\psi(\bar{3}) = \psi(\bar{1} + \bar{1} + \bar{1}) = \psi(\bar{1}) + \psi(\bar{1}) + \psi(\bar{1})$. Cela signifie qu'un morphisme ψ est complètement connu dès que l'on connaît l'image de $\bar{1}$ par ψ. Il y a quatre possibilités.

- $\psi(\bar{1}) = \bar{0} \implies \psi = cte = \bar{0}$ et n'est donc pas un auto.
- $\psi(\bar{1}) = \bar{1} \implies \psi =$ Identité qui un auto.
- $\psi(\bar{1}) = \bar{2} \implies \psi = \phi$ et l'on a vu que ϕ n'est pas un auto.
- $\psi(\bar{1}) = \bar{3} \implies \psi(\bar{2}) = \bar{3} + \bar{3} = \bar{2}$ et $\psi(\bar{3}) = \bar{3} + \bar{3} + \bar{3} = \bar{1}$ et ψ est bien un auto.

Il y a donc en tout deux automorphismes : l'identité (notée I) et la quatrième application ci-dessus que l'on notera par la suite θ.

□

1. Licence de mathématiques (2-ième année), *Université Paul Sabatier (Toulouse III)*. Année scolaire 2003-2004

B – Dresser la table du groupe $((\mathbb{Z}/5\mathbb{Z})^*,\cdot)$.
(On rappelle que dans un anneau $(A,+,\cdot)$, A^* désigne l'ensemble des éléments inversibles pour la multiplication $\cdot$.)

Solution. Puisque 5 est un nombre premier $(\mathbb{Z}/5\mathbb{Z},+,\cdot)$ est un corps; tous les éléments non nuls sont donc inversibles et $(\mathbb{Z}/5\mathbb{Z})^* = \{\bar{1},\bar{2},\bar{3},\bar{4}\}$.

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

□

C – Montrer que $(\mathbb{Z}/5\mathbb{Z})^* \simeq \mathbb{Z}/4\mathbb{Z}$.

Solution. $(\mathbb{Z}/5\mathbb{Z})^*$ est cyclique d'ordre 4. En effet

$$(\mathbb{Z}/5\mathbb{Z})^* = \{\bar{2}^0,\bar{2}^1,\bar{2}^2,\bar{2}^3\} = \{\bar{1};\bar{2},\bar{4},\bar{3}\}.$$

D'après un théorème du cours tout groupe cyclique d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

□

D – Déterminer tous les isomorphismes de $(\mathbb{Z}/4\mathbb{Z},+)$ sur $((\mathbb{Z}/5\mathbb{Z})^*,\cdot)$.

Solution. L'application f définie par $f(n\bar{1}) = \bar{2}^n$ pour $n = 1,2,3,4$ définit un isomorphisme de $(\mathbb{Z}/4\mathbb{Z},+)$ sur $(\mathbb{Z}/5\mathbb{Z})^*,\cdot)$. Supposons que g soit un autre isomorphisme. Alors $f^{-1}\circ g$ est un automorphisme de $(\mathbb{Z}/4\mathbb{Z},+)$. Or nous avons vu dans la question A) b) qu'il existe seulement deux tels automorphismes : I et θ. Il suit que $f^{-1}\circ g = I$ ou $f^{-1}\circ g = \theta$ et $g = f$ ou $g = f\circ\theta$. Il y a donc deux isomorphismes de $(\mathbb{Z}/4\mathbb{Z},+)$ sur $(\mathbb{Z}/5\mathbb{Z})^*,\cdot)$.

□

III

On considère l'ensemble $\mathbb{D}$ formé des nombres décimaux. De manière précise

$$\mathbb{D} = \left\{ \frac{m}{10^n} \,:\, m \in \mathbb{Z}\,, n \in \mathbb{N} \right\}$$

Par exemple $x = -5{,}5674 \in \mathbb{D}$ car $x = \frac{-55674}{10^4}$.

A – Montrer que $\mathbb{D}$ est un sous-anneau (unitaire) de $(\mathbb{Q},+,\cdot)$.

Solution. $\mathbb{D}$ est un sous-ensemble non vide de $\mathbb{Q}$ (contenant $\mathbb{Z}$). De plus

$$\frac{m}{10^n} - \frac{m'}{10^{n'}} = \frac{m10^{n'} - m'10^n}{10^{n+n'}} \in \mathbb{D} \quad \text{et} \quad \frac{m}{10^n}\cdot\frac{m'}{10^{n'}} \in \mathbb{D}$$

d'où il résulte que $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$. C'est un sous-anneau unitaire d'unité $1 = \frac{1}{10^0}$.

□

B – Montrer que pour tous α et β dans $\mathbb{Z}$ on a $2^\alpha\cdot 5^\beta \in \mathbb{D}$.

Solution. Puisque $\mathbb{D}$ est un sous-anneau, il suffit de montrer que $2^\alpha \in \mathbb{D}$ et $5^\beta \in \mathbb{D}$. Lorsque α et β sont positifs c'est évident. Regardons les cas négatifs. Si $\alpha = -n$ avec $n > 0$ alors $2^\alpha = \frac{1}{2^n} = \frac{5^n}{10^n} \in \mathbb{D}$ et si $\beta = -n$ avec $n > 0$ alors $5^\beta = \frac{1}{5^n} = \frac{2^n}{10^n} \in \mathbb{D}$. Nous appelerons S l'ensemble des éléments de la forme $2^\alpha \cdot 5^\beta$ avec α et β entiers relatifs.

□

C – a) Les éléments suivants sont-ils inversibles (pour $\cdot$) : $\frac{3}{10}$, $\frac{1}{10}$, $\frac{2}{5^2}$?

Solution. Supposons que $\frac{3}{10}$ soit inversible d'inverse $\frac{m}{10^n}$. On a alors $\frac{3}{10} \cdot \frac{m}{10^n} = 1 \implies \frac{3m}{10^{n+1}} = 1 \implies 3m = 10^{n+1} \implies 3|10$ ce qui est impossible. Donc $3/10$ n'est pas inversible. $\frac{1}{10}$ est évidemment inversible d'inverse 10. De même $\frac{2}{5^2} = 2^1 5^{-2}$ est inversible d'inverse $2^{-1}5^2 \in \mathbb{D}$.

□

b) Déterminer l'ensemble $\mathbb{D}^*$ formé de tous les éléments inversibles de $\mathbb{D}$.

Solution. Supposons que $x = \frac{m}{10^n}$ soit inversible. Appelons x' son inverse et notons $x' = \frac{m'}{10^{n'}}$. L'égalité $x \cdot x' = 1$ donne $mm' = 10^{n+n'} = 2^{n+n'}5^{n+n'}$. Il suit que les seuls nombres premiers qui divisent m sont 2 et 5 (et 1) de sorte que $m = 2^u 5^v$ et $x = \frac{2^u 5^v}{10^n} = 2^\alpha 5^\beta$ avec $\alpha,\beta \in \mathbb{Z}$. Nous avons ainsi montré que $\mathbb{D}^* \subset S$ (l'ensemble S a été défini ci-dessus). Nous avons l'inclusion réciproque car si $x = 2^\alpha 5^\beta$ alors x est inversible d'inverse $2^{-\alpha}5^{-\beta}$. On a donc $\mathbb{D}^* = S$.

□

D – On rappelle que si a est un élément d'un anneau commutatif A, (a) désigne l'idéal principal engendré par a c'est-à-dire $(a) = \{ta : t \in A\}$. Soient x,$y \in \mathbb{D}$. A quelle(s) condition(s) a-t-on $(x) = (y)$?

Solution. Puisque $(x) = (y)$ on a $x \in (y)$ et $y \in (x)$ d'où $x = ty$ et $y = t'x$. Il suit $x = (tt')x$ d'où $tt' = 1$ donc t est inversible d'inverse t'. Donc une condition nécessaire pour que $(x) = (y)$ est que x et y soient égaux à la multiplication par un inversible près. Cette condition est aussi suffisante. En effet si $x = ty$ avec t inversible alors $y \in (x)$ car $y = t^{-1}x$ et $y \in (x)$ implique $(y) \subset (x)$ puis, comme $ty = x$ donne directement $(x) \subset (y)$, on en déduit $(x) = (y)$.

□

E – On note $(\frac{6}{5},\frac{9}{2})$ l'ensemble défini par

$$\left(\frac{6}{5},\frac{9}{2}\right) =_{def} \left\{ t\frac{6}{5} + t'\frac{9}{2} \ : \ t,t' \in A \right\}.$$

a) Montrer que $(\frac{6}{5},\frac{9}{2})$ est un idéal de $\mathbb{D}$.

Solution. $(\frac{6}{5},\frac{9}{2})$ est un ensemble non vide (il contient 0) et on vérifie immédiatement que x_1,$x_2 \in (\frac{6}{5},\frac{9}{2})$ entraînent $x_1 - x_2 \in (\frac{6}{5},\frac{9}{2})$. Il reste seulement à montrer que $x_1 \in \mathbb{D}$ et $x_2 \in (\frac{6}{5},\frac{9}{2})$ entraînent $x_1 \cdot x_2 \in (\frac{6}{5},\frac{9}{2})$. On a $x_2 = t_2\frac{6}{5} + t'_2\frac{9}{2}$. Par conséquent

$$\begin{aligned} x_1 \cdot x_2 &= x_1 \cdot \left(t_2\tfrac{6}{5} + t'_2\tfrac{9}{2}\right) \\ &= (x_1t_2)\tfrac{6}{5} + (x_1t'_2)\tfrac{9}{2} = \square\tfrac{6}{5} + \triangle\tfrac{9}{2} \in (\tfrac{6}{5},\tfrac{9}{2}). \end{aligned}$$

Cela conclut la démonstartion que $(\frac{6}{5},\frac{9}{2})$ est un idéal.

□

b) Trouver z tel que $(\frac{6}{5},\frac{9}{2}) = (z)$

Solution. On a $t\frac{6}{5} + t'\frac{9}{2} = (t\frac{2}{5} + t'\frac{3}{2}) \cdot 3$. Or $(t\frac{2}{5} + t'\frac{3}{2}) \in \mathbb{D}$ dès que t,$t' \in \mathbb{D}$ donc $(\frac{6}{5},\frac{9}{2}) \subset (3)$. Ensuite, de l'identité $3 = -6 + 9$ qu'on écrit $3 = (-5)\frac{6}{5} + 2\frac{9}{2}$ on tire $3 \in (\frac{6}{5},\frac{9}{2})$ qui donne $(3) \subset (\frac{6}{5},\frac{9}{2})$. On conclut $(\frac{6}{5},\frac{9}{2}) = (3)$.

□

F – Montrer plus généralement que tous les idéaux de I sont principaux autrement dit que $\mathbb{D}$ est un anneau principal.

Solution. On donnera une démonstration très voisine de celle employée dans le cours pour démontrer que $\mathbb{Z}$ est un anneau principal. Soit I un idéal de $\mathbb{D}$. Si $I = \{0\}$ alors $I = (0)$ et I est trivialement un idéal principal. Nous supposerons que $I \neq \{0\}$. Dans ce cas I possède un élément non nul et puisque $x \in I \implies -x \in I$ il contient un élément non nul strictement positif. En outre si $x = m/10^n \in I$ alors, I étant un idéal, on a aussi $10^n \cdot x = m \in I$. On en déduit que I contient un élément entier strictement positif, autrement dit $I \cap \mathbb{N}^\star \neq \emptyset$. On peut alors considérer $p =_{def} \inf\{m \in I \cap \mathbb{N}^\star\}$. Puisque $p \in I$ on $(p) \subset I$, on va montrer la réciproque. Soit $y \in I$ alors $y = \frac{s}{10^n}$ avec $s \in \mathbb{Z}$. Effectuant la division euclidienne de s par p, on obtient $s = kp + R$ avec $r \in \{0,1,\ldots,p-1\}$ d'où $y = \frac{s}{10^n} = \frac{k}{10^n}p + \frac{r}{10^n}$. Puisque y et $\frac{k}{10^n}p$ appartiennent à l'idéal I, il suit que $\frac{r}{10^n} \in I$ et donc aussi $10^n \cdot \frac{r}{10^n} = r \in I$. Or r est plus petit que p et p est le plus petit entier positif dans I. La seule possibilité est que $r = 0$ qui donne en revenant à l'expression de y, $y = \frac{k}{10^n}p \in I$ d'où $I \subset (p)$. On conclut $I = (p)$ et I est donc un idéal principal.

□

FIN