ALGEBRE[1]

Examen du 02 juin 2005

Corrigé succinct

I.

(1) Dans $\mathbb{Z}/17\mathbb{Z}$ on a

$$x^2 = -\overline{1} \iff x^2 = \overline{16} \iff x^2 = \overline{4}^2 \iff x^2 - \overline{4}^2 = \overline{0} \iff (x-\overline{4})(x+\overline{4}) = \overline{0}.$$

Puisque 17 est premier, $\mathbb{Z}/17\mathbb{Z}$ est un corps, donc est intègre et la dernière égalité est équivalente à $x = \overline{4}$ ou $x = -\overline{4} = \overline{13}$. Donc l'équation admet deux et seulement deux solutions qui sont $\overline{4}$ et $\overline{13}$.

(2) Dans $\mathbb{Z}/7\mathbb{Z}$ on $-\overline{1} = \overline{6}$. Des calculs immédiats donnent

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
x^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$

donc x^2 ne prend jamais la valeur $\overline{6}$ et l'équation n'a pas de solution.

II.

(1) e est évidemment d'ordre 1. Pour σ_1, on remarque que $\sigma_1^2 = (12)(34)(12)(34) = (12)^2(34)^2$ car les cycles de supports disjoints commutent. Enfin on a $(12)^2 = e$ et $(34)^2 = e$ car on sait qu'un cycle de longueur k est d'ordre k (on peut aussi évidemment le vérifier directement par le calcul). Il suit que l'ordre de σ_1 (qui est différent de e) est égal à 2. La même démonstration et le même résultat valent pour σ_2 et σ_3.

(2) Construisons une table. Un calcul très simple conduit à

$\swarrow$	e	σ_1	σ_2	σ_3
e	e	σ_1	σ_2	σ_3
σ_1	σ_1	e	σ_3	σ_2
σ_2	σ_2	σ_3	e	σ_1
σ_3	σ_3	σ_2	σ_1	e

Ce tableau montre que que H (qui est trivialement non vide) est stable pour le produit ($f,g \in H \implies f \cdot g \in H$) et pour l'inverse ($f \in H \implies f^{-1} \in H$), en fait on a toujours $f = f^{-1}$ pour $f \in H$. Ceci montre que H est un sous-groupe. Enfin, la symétrie du tableau assure que H est commutatif.

(3) Soit G un sous-groupe quelconque de H. Le théorème de Lagrange nous dit que le cardinal de G divise le cardinal de H. Il y a alors seulement trois possibilités : $|G| = 1$, $|G| = 2$ et $|G| = 4$. $|G| = 1$ donne $G = \{e\}$ et $|G| = 4$ donne $G = H$. Etudions le cas $|G| = 2$. Si G contient 2 éléments, il est de la forme $G = \{e,x\}$ avec x élément d'ordre 2 donc $G = \{e,\sigma_1\}$ ou $G = \{e,\sigma_2\}$ ou $G = \{e,\sigma_3\}$ donc H a exactement 5 sous-groupes parmi lesquels 3 sont propres.

---

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

(4) (a) Cherchons l'image de $f(1)$ par $f\cdot(12)(34)\cdot f^{-1}$. On a

$$f(1)\overset{f^{-1}}{\to}1\overset{(34)}{\to}1\overset{(12)}{\to}2\overset{f}{\to}f(2)$$

De même on montre que l'image de $f(2)$ est $f(1)$, l'image de $f(3)$ est $f(4)$ et l'image de $f(4)$ est $f(3)$ d'où il suit que $f\cdot(12)(34)\cdot f^{-1}=\big(f(1)f(2)\big)\big(f(3)f(4)\big)$.

(b) Pour montrer que H est un sous-groupe *distingué* de $\mathbf{S}_4$, il suffit de vérifier que pour tout $f\in\mathbf{S}_4$ on a $f\cdot\sigma_i\cdot f^{-1}\in H$ pour $i=1,2,3$. Considérons le cas σ_1. On vient de voir que $f\cdot\sigma_1\cdot f^{-1}=f\cdot(12)(34)\cdot f^{-1}=\big(f(1)f(2)\big)\big(f(3)f(4)\big)$. Mais puisque f est une bijection de $\{1,2,3,4\}$ dans lui-même, l'élément $\big(f(1)f(2)\big)\big(f(3)f(4)\big)$ n'est autre que σ_1 ou σ_2 ou σ_3. (Il peut se présenter sous une forme un peu différente, on peut avoir par exemple $(21)(43)$ qu'il faut savoir reconnaître comme égal à $(12)(34)$.) Il suit que $f\cdot\sigma_1\cdot f^{-1}\in H$. On procède de même pour σ_2 et σ_3. On commence par généraliser le calcul de la question précédente pour obtenir $f\cdot(13)(24)\cdot f^{-1}=\big(f(1)f(3)\big)\big(f(2)f(4)\big)$ et $f\cdot(14)(23)\cdot f^{-1}=\big(f(1)f(4)\big)\big(f(2)f(3)\big)$. Ensuite on applique le même raisonnememtn que précédemment pour s'assurer finalement que $f\cdot\sigma_i\cdot f^{-1}\in H$ $(i=1,2,3)$ et donc que H est un sous-groupe distingué.

(5) L'application définie par $f(e)=(\overline{0},\overline{0})$, $f(\sigma_1)=(\overline{1},\overline{0})$, $f(\sigma_2)=(\overline{0},\overline{1})$ et $f(\sigma_3)=(\overline{1},\overline{1})$ définit un isomorphisme de groupe entre H et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

III.

(1) (a) On a 3 possibilités pour chaque coefficient. Il y a donc au total 3^4 éléments dans A soit 81 éléments.

(b) Posant $M=\begin{pmatrix}\overline{1}&\overline{1}\\ \overline{1}&\overline{1}\end{pmatrix}$ on a

$$M^2=\begin{pmatrix}\overline{2}&\overline{2}\\ \overline{2}&\overline{2}\end{pmatrix}\quad\text{et}\quad M^3=\begin{pmatrix}\overline{4}&\overline{4}\\ \overline{4}&\overline{4}\end{pmatrix}=\begin{pmatrix}\overline{1}&\overline{1}\\ \overline{1}&\overline{1}\end{pmatrix}=M.$$

Supposons que $M\in A^\star$, c'est-à-dire que M^{-1} existe. De $M^3=M$ on tire $M^3\cdot M^{-1}=M\cdot M^{-1}$ d'où $M^2=1_A$ mais M^2 calculé ci-dessus est différent de $1_4=\begin{pmatrix}\overline{1}&\overline{0}\\ \overline{0}&\overline{1}\end{pmatrix}$. De la contradiction on déduit que M n'est pas inversible.

(c) $M^3=M\iff M^3-M=0_A\iff M(M^2-1_A)=0_A$ mais $M\neq 0_A$ et $M^2-1_A=\begin{pmatrix}\overline{1}&\overline{2}\\ \overline{2}&\overline{1}\end{pmatrix}\neq 0_A$. Un produit d'éléments non nuls peut donc être nul et cela montre que A n'est pas intègre.

(2) On considère B le sous-ensemble de A formé des matrices de la forme $\begin{pmatrix}a&b\\ -b&a\end{pmatrix}$ avec a,b quelconques dans $\mathbb{Z}/3\mathbb{Z}$.

(a) B est trivialement non vide $(0_A\in B)$. Si

$$M=\begin{pmatrix}a&b\\ -b&a\end{pmatrix}\in B\quad\text{et}\quad M'=\begin{pmatrix}a'&b'\\ -b'&a'\end{pmatrix}\in B$$

on a

$$M-M'=\begin{pmatrix}a=a'&b+b'\\ -(b+b')&a+a'\end{pmatrix}\in A\,\text{et}\,M\cdot M'=\begin{pmatrix}a\cdot a'-b\cdot b'&a\cdot b'+b\cdot a'\\ -(a\cdot b'+b\cdot a')&a\cdot a'-b\cdot b'\end{pmatrix}\in B$$

et ceci montre que B est un sous-anneau de $(A, +, \cdot)$.

(b) B contient $9 = 3^2$ éléments : 3 possibilités pour a combinées avec 3 possibilités pour b. La liste des 9 éléments est :
$0_A = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix}$, $\begin{pmatrix} \overline{0} & \overline{1} \\ \overline{2} & \overline{0} \end{pmatrix}$, $\begin{pmatrix} \overline{0} & \overline{2} \\ \overline{1} & \overline{0} \end{pmatrix}$, $1_A = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$, $\begin{pmatrix} \overline{1} & \overline{2} \\ \overline{1} & \overline{1} \end{pmatrix}$, $\begin{pmatrix} \overline{1} & \overline{1} \\ \overline{2} & \overline{1} \end{pmatrix}$, $\begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{2} \end{pmatrix}$, $\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{2} & \overline{2} \end{pmatrix}$, $\begin{pmatrix} \overline{2} & \overline{2} \\ \overline{1} & \overline{2} \end{pmatrix}$.

(c) Le seul élément non inversible du corps $\mathbb{Z}/3\mathbb{Z}$ est $\overline{0}$. Donc on doit résoudre $a^2 + b^2 = \overline{0}$. Dans le tableau suivant on prend a et b comme entrée et on met $a^2 + b^2$ comme résultat :

a^2+b^2	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\leftarrow a$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{1}$	
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{2}$	
$\overline{2}$	$\overline{1}$	$\overline{2}$	$\overline{2}$	
$\uparrow$				
b				

.

Le tableau montre que la seule possibilité pour $a^2 + b^2 = 0$ est $a = 0$ et $b = 0$.

(d)
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a^2+b^2 & \overline{0} \\ \overline{0} & a^2+b^2 \end{pmatrix}.$$

(e) Si $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ est un élément non nul de B, on a $(a,b) \neq (\overline{0},\overline{0})$ donc, d'après la question précédente, $a^2 + b^2$ est inversible, donc $(a^2 + b^2)^{-1}$ existe et on peut former la matrice
$$M' = \begin{pmatrix} (a^2+b^2)^{-1}a & (a^2+b^2)^{-1}b \\ -(a^2+b^2)^{-1}b & (a^2+b^2)^{-1}a \end{pmatrix}.$$
On vérifie que $M \cdot M' = M' \cdot M = 1_A$ donc M est inversible d'inverse M' donc tout élément non nul de B est inversible cela signifie que B est un corps.

(f) B contient 9 éléments donc la seule possibilité est $B \simeq \mathbb{Z}/9\mathbb{Z}$ mais ceci est impossible car B est un corps et $\mathbb{Z}/9\mathbb{Z}$ ne l'est pas (par exemple, si $f : B \to \mathbb{Z}/9\mathbb{Z}$ isomorphisme existait on aurait $\overline{0} = \overline{3}^2 \implies (f^{-1}(3))^2 = 0_A$ avec $f^{-1}(3) \neq 0_A$ puisque f bijective et cela contredirait le fait que B est intègre donc que B est un corps).

FIN