ALGEBRE[1]

Epreuve de septembre 2005

INDICATIONS DE CORRECTIONS

Ce document donnent simplement des éléments de réponses SANS les accompagner des détails de calculs ou de demonstrations NECESSAIRES.

EXERCICE

$(\mathbb{Z}/9\mathbb{Z})^\star = \{\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8}\}$. Le tableau suivant donne les inverses.

x	x^{-1}
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{7}$
$\overline{5}$	$\overline{2}$
$\overline{7}$	$\overline{4}$
$\overline{8}$	$\overline{8}$

Le groupe $(\mathbb{Z}/9\mathbb{Z})^\star$ est cyclique engendré par $\overline{2}$. En effet, $\overline{1} = \overline{2}^0, \overline{2} = \overline{2}^1, \overline{4} = \overline{2}^2, \overline{5} = \overline{32} = \overline{2}^5, \overline{7} = \overline{16} = \overline{2}^4, \overline{8} = \overline{2}^3$ de sorte que $(\mathbb{Z}/9\mathbb{Z})^\star = \{\overline{2}^k \,:\, k = 0,\dots,5\}$.

PROBLÈME

I —

(1) $(f_{\alpha,\beta} \circ f_{\alpha',\beta'})(z) = f_{\alpha,\beta}(\alpha' z + \beta') = \alpha(\alpha' z + \beta') + \beta = f_{\alpha\alpha',\alpha\beta'+\beta}(z)$.

(2) $f^{-1}_{\alpha,\beta} = f_{1/\alpha,-\beta/\alpha}$.

(3) La loi $\circ$ sur G n'est pas commutative (contrexemple : $f_{2,0} \circ f_{3,1} = f_{6,2}$ mais $f_{3,1} \circ f_{2,0} = f_{6,1}$.)

II —

(1) On remarque que $H_\mathbb{Z} = \{f_{1,n} \,:\, n \in \mathbb{Z}\}$. Ensuite, d'après une question précédente, $f_{1,n} \circ f_{1,m} = f_{1,n+m} \in H_\mathbb{Z}$ et $f^{-1}_{1,n} = f_{1,-n} \in H_\mathbb{Z}$ donc $H_\mathbb{Z}$ est bien un sous-groupe de G. On montre que l'application $\phi : n \in \mathbb{Z} \to f_{1,n} \in H_\mathbb{Z}$ est bien définie et est un isomorphisme de groupe. La fait que ϕ soit un morphisme provient de la relation $f_{1,n} \circ f_{1,m} = f_{1,n+m}$ qui dit $\phi(n+m) = \phi(n) \circ \phi(m)$. Attention, les groupes étant de cardinal infini, il faut ensuite montrer *à la fois* l'injectivité ($n \in \ker\phi \implies f_{1,n} = Id \implies n = 0$) et la surjectivité ($f_{1,n}$ a n pour antécédent).

(2) Il suffit de prendre $H_T = \{f_{1,\beta} \,:\, \beta \in T\}$. On montre que c'est un sous-groupe et qu'il est isomorphe à T en procédant comme dans la question précédente.

III —

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

(1) Il suffit de prendre $H_L = \{f_{\alpha,0} : \alpha \in L\}$. On montre comme précédemment, en utilisant les relations $f_{\alpha,0} \circ f_{\alpha',0} = f_{\alpha\cdot\alpha',0}$ et $f_{\alpha,0}^{-1} = f_{\alpha^{-1},0}$ que H_L est un sous-groupe et l'isomorphisme ϕ est défini par $\phi : \alpha \in L \to f_{\alpha,0} \in H_L$. Là encore, il faut établir à la fois l'injectivité et la surjectivité.

On a

$$f_{a,b}^{-1} \circ f_{\alpha,0} \circ f_{a,b} = f_{a,b}^{-1} \circ f_{\alpha a,\alpha b} = f_{\alpha,\alpha b/a-b/a}.$$

Donc pour que $f_{a,b}^{-1} \circ f_{\alpha,0} \circ f_{a,b} \in H_L$ pour tous a,b il est nécessaire que $\alpha = 1$. Cela montre que H_L n'est pas distingué à moins que L soit réduit à l'élément neutre i.e. $L = \{1\}$.

(2) Il suffit de prendre $H_{\mathbf{U}_n}$ où $\mathbf{U}_n$ le groupe des racines n-ième de l'unité.

IV — Soit A un sous-ensemble non vide de $\mathbb{C}$. On définit l'ensemble G^A par la condition suivante

$$f \in G^A \iff f(A) = A,$$

Autrement dit $f \in G^A$ si l'image de tout élément de A par f est encore dans A et si tout élément de A est image par f d'un élément de A.

(1) D'abord G^A est non vide car $Id \in G^A$. Si $f,g \in G^A$ alors $g(A) = A \implies f(g(A)) = f(A) = A \implies (f \circ g)(A) = A \implies f \circ g \in G^A$. Ensuite $f(A) = A \implies f^{-1}(f(A)) = f^{-1}(A)$ mais $f^{-1}(f(A)) = A$ d'où $f^{-1} \in G^A$ et G^A est bien un sous-groupe de G.

(2) $g \in G^{f(A)} \implies g(f(A)) = f(A) \implies f^{-1}(g(f(A))) = A \implies f^{-1} \circ g \circ f \in G^A$ d'où $f^{-1} \circ G^{f(A)} \circ f \subset G^A$. On vérifie de la même manière l'inclusion réciproque de sorte que $f^{-1} \circ G^{f(A)} \circ f = G^A$.

(3) $A = \{0\}$. Une application d définie par $g(z) = \alpha z + \beta \in G^A$ ssi $g(0) = 0$ ssi $\beta = 0$ donc $G^A = H_{\mathbb{C}^\star}$. Donc d'après une question précédente G^A est isomorphe à $\mathbb{C}^\star$.

(4) $A = \{0,1\}$. Une application d définie par $g(z) = \alpha z + \beta \in G^A$ ssi ($g(0) = 0$ et $g(1) = 1$) ou ($g(0) = 1$ et $g(1) = 0$). Dans le premier cas on obtient $g = Id$, dans le second $g(z) = -z + 1$. Donc $G^A = \{Id, f_{-1,1}\}$.

(5) Prenons $A = \mathbb{Z}$ et montrons que G^A est isomorphe à $\mathbb{Z}$. Pour cela nous commençons par déterminer G^A. Prenons $g(z) = \alpha z + \beta \in G^A$ avec $\alpha \neq 0$. On a $g(0) \in \mathbb{Z}$ donc $\beta = n \in \mathbb{Z}$. Ensuite quel que soit $r \in \mathbb{Z}$ on a $\alpha r + n \in \mathbb{Z}$ d'ou quel que soit $r \in \mathbb{Z}$, $\alpha.r \in \mathbb{Z}$. la seule possibilité est $\alpha \in \mathbb{Z}^\star$. Donc $g(z) = mz + n$. Comme $g(\mathbb{Z}) = \mathbb{Z}$, quel que soit r, l'élément $n + r$ a un antécédent dans $\mathbb{Z}$, autrement dit il existe q tel que $mq + n = n + r$ ou $mq = r$ donc quel que soit $r \in \mathbb{Z}$, m divise r. Cela force $m = 1$. Finalement g est de la forme $g(z) = z + n$ i.e. $g \in H_{\mathbb{Z}}$ d'où $G^A \subset H_{\mathbb{Z}}$. On montre facilement l'inclusion réciproque. D'ou finalement $G^A = H_{\mathbb{Z}}$ et d'après une question précédente, il suit que G^A est isomorphe à $\mathbb{Z}$.

(6) $A = \mathbf{U}$ où $\mathbf{U}$ désigne l'ensemble des nombres complexes de module 1. On remarque que g définie par $g(z) = \alpha z + \beta$ est la composée de $g_\alpha = z \to \alpha z$ et de la translation $t_\beta : z \to z + \beta$, $f = t_\beta \circ g_\alpha$. Or g_α envoie le cercle unité $\mathbf{U}$ sur le cercle de centre 0 et de rayon $|\alpha|$ tandis que la translation t_β envoie le cercle de rayon $|\alpha|$ et centre 0 sur le cercle de même rayon et de centre β. Au total g envoie $\mathbf{U}$ sur le cercle de centre β et de rayon $|\alpha|$. Pour que ce cercle d'arrivée coïncide avec $\mathbf{U}$ il faut donc que $\beta = 0$ et $|\alpha| = 1$. Il suit que $G^A \subset H_{\mathbf{U}}$. On verifie facilement l'inclusion réciproque donc $G^A = H_{\mathbf{U}}$ et d'après une question précédente, on en déduit que G^A est isomorphe à $\mathbf{U}$.

FIN