Devoir de Mathématiques n°14

Kévin Polisano
MPSI 1

Lundi 10 Mars 2008

Problème 1

Énoncé :

On considère l'équation du second degré :

$$z^2 - bz + c = 0 \quad (1)$$

avec $(b,c) \in \mathbb{Z}^2$ et $b^2 - 4c < 0$; α étant une des racines de cette équation.

On note Z_α l'ensemble des nombres complexes $z = p + q\alpha$ où $(p,q) \in \mathbb{Z}^2$.
On note Q_α l'ensemble des nombres complexes $w = v + u\alpha$ où $(u,v) \in \mathbb{Q}^2$.

1) Montrons que $(Z_\alpha, +, .)$ est un sous anneau de $(\mathbb{C}, +, .)$.

On a clairement $Z_\alpha \subset \mathbb{C}$ et Z_α contient 1, neutre de $\mathbb{C}$ par .

• Soit $(z, z') \in Z_\alpha^2$ on a :

$$z - z' = p + q\alpha - p' - q'\alpha = (p - p') + (q - q')\alpha$$

Les termes $(p - p')$ et $(q - q')$ sont des entiers relatifs donc :

$$z - z' \in Z_\alpha$$

• On a également :

$$z.z' = (p + q\alpha).(p' + q'\alpha) = pp' + (pq' + qp')\alpha + qq'\alpha^2$$

Or d'après (1) : $\alpha^2 = b\alpha - c$ d'où :

$$z.z' = (pp' - cqq') + (pq' + qp' + bqq')\alpha \in Z_\alpha$$

Par conséquent $(Z_\alpha, +, .)$ est un anneau.

Supposons alors $(p,q) \neq (0,0)$ et montrons que $(p', q') = (0,0)$ c'est-à-dire que $(Z_\alpha, +, .)$ est intègre.

On écrit α sous forme algébrique $\alpha = a + ib, (a,b) \in \mathbb{R}^{2\star}$ et on voit alors que :

$$z.z' = 0 \Leftrightarrow \begin{cases} pp' - cqq' = 0 \\ qp' + (bq+p)q' = 0 \end{cases}$$

On a alors un système de deux équations à inconnues (p', q'), par substitution de p' dans la deuxième ligne on obtient :

$$q'\left(\frac{cq^2}{p} + bq + p\right) = 0$$

Imaginons un instant que $q' \neq 0$ alors puisqu'on travaille avec des entiers on aurait :

$$p^2 + bpq + cq^2 = 0$$

Ainsi si on recherchait p qui existe et est non nul il viendrait :

$$\Delta = b^2q^2 - 4cq^2 = q^2(b^2 - 4c) < 0$$

Ce qui est absurde donc $q' = 0$ et par suite $p' = 0$.

On en déduit que $(Z_\alpha, +, .)$ est un anneau intègre.

De même Z_β est un anneau intègre où β est la seconde racine de (1).

2) Soit f l'application de Z_α dans $\mathbb{Z}$ définie par :

$$f(p + q\alpha) = p^2 + bqp + cq^2$$

On a vu à la question précédente que pour $x \in Z_\alpha$ non nul soit $(p,q) \neq (0,0)$ on a :

$$p^2 + bqp + cq^2 > 0 \Rightarrow f(x) \neq 0$$

Donc par contraposition on a :

$$f(x) = 0 \Rightarrow x = 0$$

Par ailleurs il est clair que si $x = 0$ on a $(p,q) = (0,0)$ et donc $f(x) = 0$ d'où :

$$x = 0 \Rightarrow f(x) = 0$$

On a montré la première assertion :

$$\boxed{f(x) = 0 \Leftrightarrow x = 0 \quad (i)}$$

En prenant $x = p + q\alpha$ et $y = p' + q'\alpha$ on a montré que :

$$xy = (pp' - cqq') + (pq' + qp' + bqq')\alpha$$

En appliquant f il vient :

$$f(xy) = (pp' - cqq')^2 + b(pp' - cqq')(pq' + qp' + bqq') + c(pq' + qp' + bqq')^2$$

Et par ailleurs :

$$f(x)f(y) = (p^2 + bpq + cq^2)(p'^2 + bp'q' + cq'^2)$$

On vérifie alors aisément par soustraction que :

$$\boxed{\forall (x,y) \in Z_\alpha^2, f(xy) = f(x)f(y) \quad (ii)}$$

3) Soit G_α l'ensemble des éléments de Z_α qui sont inversibles dans Z_α.

a) On a montré dans le cours que les éléments inversibles d'un anneau forment un groupe noté $U(Z_\alpha)$. En effet la loi . est une lci associative dans $U(Z_\alpha)$ car elle l'est dans Z_α, on a $1 \in U(Z_\alpha)$ qui est son propre neutre et chaque élément x de $U(Z_\alpha)$ possède un symétrique x^{-1} dans $U(Z_\alpha)$ également puisque son symétrique est x.

b) Si x est inversible alors puisque $f(1) = 1$ par morphisme de f :

$$f(x.x^{-1}) = f(x)f(x^{-1}) \Rightarrow f(1) = f(x)f(x^{-1}) \Rightarrow f(x)f(x^{-1}) = 1$$

Puisque l'on est dans $\mathbb{Z}$ et que les images par f sont strictements positives alors :

$$x \text{ inversible} \Rightarrow f(x) = 1$$

La condition $f(x) = 1$ est donc nécessaire.

Supposons qu'un nombre quelconque x' vérifie $x.x' = 1$ d'après la question 4) :

$$\begin{cases} p' = -\frac{q}{p^2+bpq+cq^2} \\ q' = \frac{bq+p}{p^2+bpq+cq^2} \end{cases}$$

Ainsi si $f(x) = 1$ on a :

$$\boxed{\begin{cases} p' = -q \\ q' = bq + p \end{cases}}$$

Réciproquement un tel x' convient, c'est l'inverse de x donc $f(x) = 1$ est une condition suffisante.

On en déduit que l'image de G_α par f est :

$$\boxed{f(G_\alpha) = \{1\}}$$

c) Soit $x = p + q\alpha \in G_\alpha$ on a :

$$f(x) = f(p + q\alpha) = p^2 + bpq + cq^2 = 1 \Rightarrow p^2 + bpq + (cq^2 - 1) = 0$$

On a une équation en p de discriminant :

$$\Delta = b^2q^2 - 4(cq^2 - 1) \geq 0$$

puisque x est inversible p et q existent. D'où la condition :

$$\boxed{q^2(4c - b^2) \leq 4}$$

d) On suppose dans cette question $b=-1$ et $c=1$ soit l'équation :

$$z^2+z+1=0$$

vérifiée par j et j^2.

On a avec ces hypothèses :

$$f(p+q\alpha)=p^2-pq+q^2 \quad \text{et} \quad 3q^2 \leq 4$$

Ainsi on a trois choix pour q : -1, 0 et 1. On cherche les éléments inversibles :

- Si $q=-1$ alors $f(p+q\alpha)=p^2+p+1=1$ car inversible donc $p=0$ ou $p=-1$ conviennent.

- Si $q=0$ alors $f(p+q\alpha)=p^2=1$ donc $p=1$ ou $p=-1$ conviennent.

- Si $q=1$ alors $f(p+q\alpha)=p^2-p+1=1$ donc $p=0$ ou $p=1$ conviennent.

Donc l'ensemble des éléments inversibles est :

$$\boxed{G_\alpha=\{-\alpha,-1-\alpha,1,-1,\alpha,1+\alpha\}}$$

4) Montrons que $(Q_\alpha,+,.)$ est un sous-corps de $(\mathbb{C},+,.)$.

Cet ensemble est non vide, il faut montrer que tous les éléments de $Q_\alpha^\star$ sont inversibles par .

Soit $(w,w')\in Q_\alpha$ tels que $w.w'=1$ on a d'après la première question le système :

$$\begin{cases} vv'-cuu'-1=0 \\ uv'+(bu+v)u'=0 \end{cases}$$

On obtient les solutions :

$$\boxed{\begin{cases} u'=-\frac{u}{v^2+vbu+cu^2} \\ v'=\frac{bu+v}{v^2+vbu+cu^2} \end{cases}}$$

qui existent, sont rationnels et uniques puisqu'on a démontrer que le dénominateur est strictement positif.

On vérifie que l'élément $w'=u'+\alpha v'$ convient et donc tous les éléments sont inversibles.

Problème 2

Énoncé :

Soit E un $\mathbb{R}$-ev, F un sev de E et G un groupe fini d'automorphismes linéaires de E.

Le sev F est stable par les éléments de G. La composée $u \circ v$ sera notée uv. $\text{Card}(G) = m$

A tout élément $u \in \mathcal{L}(E)$ on associe :

$$u^+ = \frac{1}{m} \sum_{g \in G} g^{-1} u g$$

1) On a $u \in \mathcal{L}(E)$ et $g \in GL(E)$ donc par composition d'endomorphisme $g^{-1}ug \in \mathcal{L}(E)$ puis par addition :

$$u^+ = \frac{1}{m} \sum_{g \in G} g^{-1} u g \in \mathcal{L}(E)$$

On a donc que u^+ est un endomorphisme de E, montrons qu'il commute avec tout $h \in G$:

Les termes de la somme dans u^+h sont de la forme :

$$g^{-1}ugh = hh^{-1}g^{-1}ugh = h(gh)^{-1}u(gh) = hf^{-1}uf$$

(en ayant posé $f = gh$) qui sont donc en bijection avec les termes de la somme dans hu^+ par la translation $g \mapsto hg$ d'où :

$$\forall h \in G, u^+h = hu^+$$

2) Calculons

$$(u^+)^+ = \frac{1}{m} \sum_{h \in G} h^{-1} \left(\frac{1}{m} \sum_{g \in G} g^{-1} u g \right) h = \frac{1}{m^2} \sum_{h \in G} \sum_{g \in G} h^{-1} g^{-1} u g h$$

par distribution du produit de composition par rapport à l'addition. Que l'on réécrit :

$$(u^+)^+ = \frac{1}{m^2} \sum_{h \in G} \sum_{g \in G} (gh)^{-1} u (gh)$$

Or l'application $x \mapsto xh$ est une bijection de G donc quand g parcourt G, gh le parcourt également. Soit en posant $f = gh$ on a :

$$\sum_{g \in G} (gh)^{-1} u (gh) = \sum_{f \in G} f^{-1} u f = m.u^+$$

D'où en mettant $m.u^+$ en facteur :

$$(u^+)^+ = \frac{1}{m^2}.m.u^+ \sum_{h \in G} 1 = u^+$$

3) Soit p un projecteur de E dont l'image est F.

• g est un automorphisme donc $\forall x \in E, g(x) \in E$ et comme $p(E) = F$ on a $pg(x) \in F$ et par stabilité il vient $g^{-1}pg(x) \in F$, par suite $p^+(x) = \frac{1}{m}\sum_{g \in G} g^{-1}pg \in F$ d'où :

$$p^+(E) \subset F$$

• p est un projecteur sur $p(E) = F$ donc $p|_F = \mathrm{id}_F$, et alors $\forall y \in F, pg(y) = g(y)$ d'où :

$$p^+(y) = \frac{1}{m}\sum_{g \in G} g^{-1}pg(y) = y$$

Ce qui prouve que :

$$p^+(F) = F$$

Ces deux points montre que l'image de p^+ est F.

4) A la question précédente on a établit que $\forall y \in F, g^{-1}pg(y) = y$.

Or puisque $h \in G$ on a

$$\forall x \in E, h(x) \in E \Rightarrow ph(x) \in F \Rightarrow h^{-1}ph(x) \in F$$

Par conséquent :

$$\forall x \in E, g^{-1}pgh^{-1}ph(x) = h^{-1}ph(x)$$

5) p est un projecteur de E donc par définition un endomorphisme de E soit $p \in \mathcal{L}(E)$.

Et on a démontré à la question 2 qu'alors $(p^+)^+ = p^+$ donc p^+ est un projecteur.

6) Pour montrer que le noyau de p^+ est stable par tout élément g de G :

Il faut que si $x \in Ker(p^+)$ alors $g(x) \in Ker(p^+)$ autrement dit si $p^+(x) = 0$ alors $p^+(g(x)) = 0$.

On utilise le fait que $\forall g \in G, u^+g = gu^+$ donc en particulier $p^+(g(x)) = g(p^+(x))$ d'où

$$p^+(g(x)) = g(0) = 0$$

car g est linéaire.