Centrale Maths 2 MP 2004 — Corrigé

Ce corrigé est proposé par Céline Chevalier (ENS Cachan) ; il a été relu par Jean Starynkévitch (ENS Cachan) et David Lecomte (Université de Stanford).

L'objectif de ce problème assez long est de présenter quelques-unes des propriétés des réseaux de $\mathbb{C}$ (sous-ensembles de $\mathbb{C}$ de la forme $\mathbb{Z}\alpha + \mathbb{Z}\beta$, où (α, β) est une base de $\mathbb{C}$ sur $\mathbb{R}$) et d'étudier l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan, dit de Poincaré, constitué des nombres complexes dont la partie imaginaire est strictement positive. Ceci joue un rôle très important dans la théorie des « courbes elliptiques », qui sont un outil fondamental en théorie des nombres. Les parties sont liées entre elles et s'enchaînent bien, quitte à admettre au besoin des résultats des parties précédentes.

- La première partie est consacrée à l'étude de $\mathscr{M}_2(\mathbb{Z})$ et plus particulièrement $\mathrm{SL}_2(\mathbb{Z})$ et $\mathrm{GL}_2(\mathbb{Z})$, dont on montre différentes caractérisations. Elle traite globalement de calcul matriciel et de diagonalisation.
- Les deux parties suivantes établissent tous les résultats de base sur les réseaux, qui seront réutilisés par la suite. La troisième partie considère plus particulièrement les similitudes directes laissant stable un réseau.
- Dans la dernière partie, on établit le lien entre toutes les précédentes en démontrant des propriétés de l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur les réseaux.

En conclusion, ce problème contient quelques questions difficiles, mais il est assez original et constitue une bonne introduction à une théorie importante en mathématiques.

Indications

Partie I

I.B.2 Utiliser la formule donnant l'inverse de la matrice A en fonction de son déterminant et de sa comatrice.

I.C.2 Faire la différence entre la relation reliant c et d et une relation équivalente avec c et d connus. Utiliser ensuite le théorème de Gauss.

I.C.4 Penser au théorème de Bézout.

I.D.1 Calculer les polynômes caractéristiques des différentes matrices.

I.E.1 Le polynôme $\mathrm{X}^2 - 1$ annule A. Que peut-on en déduire ?

I.F.1 Considérer le polynôme $\mathrm{X}^2 + 1$, annulateur de A, et se rappeler de la forme générale du polynôme caractéristique d'une matrice 2×2.

I.F.2 Utiliser les relations connues sur la trace et le déterminant de A.

I.G.1 Si $\mathrm{U} = \mathrm{PVP}^{-1} \in \mathrm{GL}_2(\mathbb{C})$, écrire $\mathrm{P} = \mathrm{A} + \mathrm{iB}$ avec A et B deux matrices réelles. En déduire que le polynôme $\mathrm{D}(\mathrm{X}) = \det(\mathrm{A} + \mathrm{XB})$ n'est pas identiquement nul et qu'il existe donc un réel x tel que $\mathrm{D}(x) \neq 0$. Conclure.

I.G.2 Utiliser la question précédente.

Partie II

II.A.1 Montrer qu'un réseau est un groupe additif.

II.B.1 Exprimer ${\omega_1}'$ et ${\omega_2}'$ dans la base $\mathscr{B}$.

II.B.2 Montrer le résultat par double inclusion en exprimant la condition pour que $\omega_1, \omega_2 \in \mathscr{B}'$.

II.C Utiliser les résultats démontrés dans la première partie.

II.D Utiliser la question II.B.

Partie III

III.A.2 Utiliser la question II.B.

III.B.4 Montrer que $\mathrm{S}(\Lambda_{\mathscr{B}}) = \mathrm{S}(\Lambda_\tau)$.

III.B.5 Montrer que $\mathrm{S}(\Lambda_\tau) \subset \Lambda_\tau$.

III.C.1 Considérer un élément $z \in \mathrm{S}(\Lambda_\tau) \smallsetminus \mathbb{Z}$ et exprimer que $z\tau,\ z \in \Lambda_\tau$.

III.C.2.a Montrer que $u\tau \in \mathrm{S}(\Lambda_\tau)$.

III.C.2.b Montrer que $\mathrm{S}(\Lambda_\tau) = \Lambda_\tau$.

Partie IV

IV.A.1 Utiliser le résultat de la question II.A.3.

IV.A.4 Si $\Phi(\mathrm{A}) = \mathrm{id}_{\mathscr{H}}$, en particulier $\Phi(\mathrm{A})$ fixe i et $1 + \mathrm{i}$. Qu'en déduit-on sur les coefficients de A ?

IV.A.5.a Combiner les questions IV.A.2 et IV.A.4.

IV.B.2 Injecter l'image de z par s dans l'équation de la question IV.B.1.

IV.C.1 Si $z = x + \mathrm{i}\beta$ est un point de la droite $\mathscr{D}$, alors il existe $\theta \in \left]-\pi/2\,;\pi/2\right[$ tel que $x = \beta\tan\theta$. Simplifier alors l'expression de $s(z)$ à l'aide de formules de trigonométrie. Reconnaître une figure géométrique simple.

IV.C.2 Si $\alpha > 0$ et $z = \alpha + \mathrm{i}y$ est un point de la droite $\mathscr{D}_+$, il existe $\theta \in \left]\,0\,;\pi/2\,\right[$ tel que $y = \alpha \tan\theta$. Utiliser à nouveau la trigonométrie pour simplifier l'expression de $s(z)$.

Se ramener à ce cas si $\alpha < 0$.

IV.E.1 Poser
$$\forall g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{G} \qquad f(g) = |c\tau + d|$$
et
$$\alpha = \mathrm{Inf}\,\big\{ f(g) \mid g \in \mathrm{G} \big\}$$

Si $\beta > \alpha$, alors par définition $\mathrm{I}_\beta = \big\{ g \in \mathrm{G} \mid f(g) < \beta \big\}$ n'est pas vide. Montrer, par un argument de comptage, que f ne prend qu'un nombre fini de valeurs sur I_β. En déduire qu'elle atteint son minimum sur cet ensemble. Conclure à l'aide de la question II.A.3.

IV.E.3 La transformation t ne modifie pas la partie imaginaire d'un nombre complexe, si bien que
$$\forall g \in \mathrm{G} \qquad \mathrm{Im}\; g\big(t^m(\tau')\big) \leqslant \mathrm{Im}\; t^m(\tau')$$

Utiliser cette propriété dans le cas particulier où $g = s$.

IV.F Soient $g \in \Gamma$ et τ un point intérieur à $\mathscr{F}$. D'après la question IV.E, on peut amener $g(\tau)$ dans $\mathscr{F}$ à l'aide d'une transformation de G. Conclure à l'aide du résultat admis par l'énoncé.

I. Matrices carrées d'ordre 2 à coefficients entiers

I.A Montrons que l'ensemble $\mathscr{M}_2(\mathbb{Z})$ est un sous-anneau de $\mathscr{M}_2(\mathbb{R})$.

- L'élément neutre de $\mathscr{M}_2(\mathbb{R})$ est I_2 et se trouve dans $\mathscr{M}_2(\mathbb{Z})$.
- Si A et B sont deux matrices à coefficients entiers, la matrice $\mathrm{A} - \mathrm{B}$ s'obtient en procédant, coordonnée par coordonnée, à la soustraction des coefficients de B aux coefficients de A. Puisque $\mathbb{Z}$ est un groupe additif, $\mathrm{A} - \mathrm{B}$ est aussi à coefficients entiers.
- À nouveau, soient A et B dans $\mathscr{M}_2(\mathbb{Z})$. On sait que les coefficients de AB s'obtiennent par somme de produits des coefficients de A et B. Comme $\mathbb{Z}$ est un anneau, AB est aussi à coefficients entiers.

Ces trois propriétés montrent que $\mathscr{M}_2(\mathbb{Z})$ est un sous-anneau de $\mathscr{M}_2(\mathbb{R})$; en particulier

$$\boxed{\mathscr{M}_2(\mathbb{Z}) \text{ est un anneau.}}$$

> Il est très souvent plus simple, comme ici, de montrer qu'un ensemble est un sous-anneau d'un autre ensemble que l'on sait être un anneau, plutôt que d'essayer de démontrer directement que c'est un anneau. Il en va de même pour les groupes, corps, algèbres, etc.

I.B.1 Démontrons que $\mathrm{GL}_2(\mathbb{Z})$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

- Si A est inversible dans $\mathscr{M}_2(\mathbb{Z})$, il existe B dans $\mathscr{M}_2(\mathbb{Z})$ telle que

$$\mathrm{AB} = \mathrm{BA} = \mathrm{I}_2$$

Puisque le produit dans $\mathscr{M}_2(\mathbb{Z})$ est induit par le produit matriciel dans $\mathscr{M}_2(\mathbb{R})$, on en déduit d'une part que A est une matrice inversible dans $\mathscr{M}_2(\mathbb{R})$ et d'autre part que l'inverse de A dans $\mathrm{GL}_2(\mathbb{Z})$ n'est autre que l'inverse de A au sens du produit matriciel dans $\mathrm{GL}_2(\mathbb{R})$. Il est de plus à coefficients entiers.

> Cette dernière constatation est importante car on peut parler maintenant sans ambiguïté de l'inverse A^{-1} de A, sans avoir à préciser s'il s'agit d'inverse au sens de $\mathscr{M}_2(\mathbb{Z})$ ou de $\mathscr{M}_2(\mathbb{R})$.

En particulier, $$\mathrm{GL}_2(\mathbb{Z}) \subset \mathrm{GL}_2(\mathbb{R})$$

- I_2 est dans $\mathrm{GL}_2(\mathbb{Z})$ puisqu'il s'agit de l'élément neutre de $\mathscr{M}_2(\mathbb{Z})$ pour la multiplication.
- Soient A et B dans $\mathrm{GL}_2(\mathbb{Z})$. Alors A^{-1} et B^{-1} sont aussi dans $\mathscr{M}_2(\mathbb{Z})$ comme on l'a vu plus haut. Puisque cet ensemble est un anneau, d'après la question I.A, il vient

$$\mathrm{AB}^{-1} \in \mathscr{M}_2(\mathbb{Z}) \qquad \text{et} \qquad \mathrm{BA}^{-1} \in \mathscr{M}_2(\mathbb{Z})$$

Finalement, $$\mathrm{I}_2 = (\mathrm{AB}^{-1})(\mathrm{BA}^{-1}) = (\mathrm{BA}^{-1})(\mathrm{AB}^{-1})$$

ce qui montre que AB^{-1} se trouve dans $\mathrm{GL}_2(\mathbb{Z})$.

Ces trois propriétés assurent que $\mathrm{GL}_2(\mathbb{Z})$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ et

$$\boxed{\mathrm{GL}_2(\mathbb{Z}) \text{ est un groupe multiplicatif.}}$$