Lemme de Selberg

Ce devoir étudie des propriétés des sous-groupes de $\mathrm{GL}_d(\mathbb{C})$.

À une exception près, tous les groupes du devoir sont notés multiplicativement.

Dans tout l'exercice, Sp désigne le spectre **complexe** d'une matrice de $\mathrm{M}_d(\mathbb{C})$, y compris quand on étudie des matrices à coefficients entiers ou rationnels.

Étant donné un morphisme d'anneaux commutatifs $\varphi : \mathrm{R}_1 \to \mathrm{R}_2$ et un entier $d \geq 1$, on notera

- $\mathrm{M}_d(\varphi) : \mathrm{M}_d(\mathrm{R}_1) \to \mathrm{M}_d(\mathrm{R}_2)$ l'application obtenue en appliquant φ coefficient par coefficient ; on pourra utiliser sans démonstration qu'il s'agit d'un morphisme d'anneaux ;
- $\varphi_* : \mathrm{GL}_d(\mathrm{R}_1) \to \mathrm{GL}_d(\mathrm{R}_2)$ le morphisme de groupes induit, défini à la question 2.

Partie I. Un peu de théorie des groupes

Groupes linéaires

Soit R un sous-anneau de $\mathbb{C}$. On ne demande pas de vérifier que $\mathrm{M}_d(\mathrm{R})$ est un sous-anneau de $\mathrm{M}_d(\mathbb{C})$. On note $\mathrm{GL}_d(\mathrm{R}) = \left\{\mathrm{A} \in \mathrm{M}_d(\mathrm{R}) \,\middle|\, \exists \mathrm{B} \in \mathrm{M}_d(\mathrm{R}) : \mathrm{AB} = \mathrm{I}_d = \mathrm{BA}\right\}$ le groupe des inversibles de $\mathrm{M}_d(\mathrm{R})$ et $\mathrm{R}^\times$ le groupe des inversibles de R.

1. (a) Montrer que $\mathrm{GL}_d(\mathrm{R}) = \left\{\mathrm{A} \in \mathrm{M}_d(\mathrm{R}) \,\middle|\, \mathrm{A} \in \mathrm{GL}_d(\mathbb{C}) \text{ et } \mathrm{A}^{-1} \in \mathrm{M}_d(\mathrm{R})\right\}$.
   (b) En déduire que $\mathrm{GL}_d(\mathrm{R}) = \left\{\mathrm{A} \in \mathrm{M}_d(\mathrm{R}) \,\middle|\, \det \mathrm{A} \in \mathrm{R}^\times\right\}$.
   (c) En déduire une description de $\mathrm{GL}_d(\mathbb{Z})$.
2. Soit $\mathrm{R}_1, \mathrm{R}_2$ deux anneaux commutatifs et $\varphi : \mathrm{R}_1 \to \mathrm{R}_2$ un morphisme d'anneaux.
   Montrer que le morphisme d'anneaux $\mathrm{M}_d(\varphi) : \mathrm{M}_d(\mathrm{R}_1) \to \mathrm{M}_d(\mathrm{R}_2)$ défini dans le préambule induit un morphisme de groupes $\varphi_* : \mathrm{GL}_d(\mathrm{R}_1) \to \mathrm{GL}_d(\mathrm{R}_2)$.

Sous-groupes d'indice fini

Soit G un groupe.

- Étant donné $\mathrm{T} \subseteq \mathrm{G}$ et un élément $g \in \mathrm{G}$, on définit $g\mathrm{T} = \left\{gt \,\middle|\, t \in \mathrm{T}\right\}$ et $\mathrm{T}g$ de manière symétrique.
- Un sous-groupe H de G est dit *d'indice fini* s'il existe $g_1, \ldots, g_r \in \mathrm{G}$ tels que $\mathrm{G} = g_1\mathrm{H} \cup \cdots \cup g_r\mathrm{H}$.

3. Soit H un sous-groupe d'indice fini de G. Montrer qu'il existe $g_1, \ldots, g_r \in \mathrm{G}$ tels que $\mathrm{G} = \mathrm{H}g_1 \cup \cdots \cup \mathrm{H}g_r$.
4. Soit K, H deux sous-groupes de G tels que $\mathrm{K} \subseteq \mathrm{H}$. Montrer que si K est d'indice fini, alors H aussi.
5. Soit F un groupe fini et $f : \mathrm{G} \to \mathrm{F}$ un morphisme de groupes. Montrer que $\ker f$ est un sous-groupe d'indice fini de G.

6. Soit H un sous-groupe d'indice fini de G. On va montrer qu'il existe un groupe fini F et un morphisme de groupes $f : G \to F$ tel que $\ker f \subseteq H$.
   (a) Montrer que l'ensemble $X = \{gH \mid g \in G\}$ est fini.
   (b) Soit $g \in G$. Montrer que, pour tout $T \in X$, $gT \in X$ et que $gH = H \Leftrightarrow g \in H$.
   (c) On note $\mathfrak{S}(X)$ le groupe des permutations de l'ensemble X et $\mathrm{Stab}(H) = \{\sigma \in \mathfrak{S}(X) \mid \sigma(H) = H\}$. Construire un morphisme de groupes $f : G \to \mathfrak{S}(X)$ tel que $f^{-1}[\mathrm{Stab}\, H] = H$.
   (d) Conclure.

Groupes virtuellement sans torsion

- Un groupe G est dit *sans torsion* si, à part son élément neutre, tous ses éléments sont d'ordre infini, c'est-à-dire si $\forall g \in G, (\exists k \in \mathbb{N}^* : g^k = 1) \Rightarrow g = 1$.
- Un groupe G est dit *virtuellement sans torsion* si G possède un sous-groupe d'indice fini sans torsion.

7. Montrer que le groupe symétrique $\mathfrak{S}(1854)$ est virtuellement sans torsion.
8. Montrer que le groupe multiplicatif $\mathbb{Q}^*$ est virtuellement sans torsion.
9. Soit G un groupe virtuellement sans torsion. Montrer qu'il existe $N \in \mathbb{N}$ tel que tous les éléments d'ordre fini de G sont d'ordre $\leq N$.
10. Soit $d \geq 2$. On va montrer que $\mathrm{GL}_d(\mathbb{Q})$ n'est pas virtuellement sans torsion. Soit F un groupe fini et $f : \mathrm{GL}_d(\mathbb{Q}) \to F$ un morphisme de groupes.
    (a) Montrer que tout morphisme de groupes $(\mathbb{Q}, +) \to F$ est trivial (c'est-à-dire constant).
    (b) Soit $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Écrire la matrice $M = \begin{pmatrix} J & 0 \\ 0 & I_{d-2} \end{pmatrix} \in \mathrm{GL}_d(\mathbb{Q})$ comme un produit de transvections.
    (c) En déduire que $M \in \ker f$ et conclure la démonstration.

Le but de ce problème est de montrer le résultat suivant.

> **Lemme de Selberg (1960).** Soit G un sous-groupe de $\mathrm{GL}_d(\mathbb{C})$ engendré par un nombre fini d'éléments. Alors G est virtuellement sans torsion.

Partie II. Un argument omniprésent

Soit $A \in \mathrm{GL}_d(\mathbb{C})$ un élément d'ordre $m \in \mathbb{N}^*$.

11. Montrer que A est diagonalisable sur $\mathbb{C}$ et que $\mathrm{Sp}(A) \subseteq \mathbb{U}_m$.
12. Montrer que $|\mathrm{tr}\, A| \leq d$ et que si $\mathrm{tr}\, A = d$, alors $A = I_d$.

Partie III. Lemme de Selberg pour $\mathrm{GL}_d(\mathbb{Z})$

Soit $p \geq 3$ un nombre premier impair. On note $\pi : \mathbb{Z} \to \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ le morphisme d'anneaux donné par la réduction modulo p, ce qui fournit un morphisme de groupes $\pi_* : \mathrm{GL}_d(\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{F}_p)$.

13. Soit $A \in \ker \pi_*$, que l'on suppose d'ordre fini.
    (a) Montrer que la matrice $B := \dfrac{A - I_d}{p}$ appartient à $M_d(\mathbb{Z})$.
    (b) Montrer que B est semblable (sur $\mathbb{C}$) à une matrice diagonale dont tous les coefficients sont de module strictement inférieur à 1 et en déduire $B^n \xrightarrow[n\to+\infty]{} 0$, puis $B = 0$.
14. Montrer le **lemme de Minkowski** : le noyau $\ker(\pi_*)$ est un sous-groupe de $\mathrm{GL}_d(\mathbb{Z})$ sans torsion.
15. En déduire que tout sous-groupe de $\mathrm{GL}_d(\mathbb{Z})$ est virtuellement sans torsion.

Partie IV. Entiers algébriques

On note $\mathbb{Z}[X]_{\text{unit}}$ l'ensemble des polynômes unitaires à coefficients entiers (ce qui exclut le polynôme nul) et on définit l'ensemble

$$\mathcal{O} = \left\{ z \in \mathbb{C} \,\middle|\, \exists P \in \mathbb{Z}[X]_{\text{unit}} \,:\, P(z) = 0 \right\}$$

des *entiers algébriques*.

16. $\mathbb{Z}$ **est intégralement clos.** Montrer que $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$.
Indication. Dans le sens non trivial, mettre $z \in \mathbb{Q}$ sous forme d'une fraction irréductible, et réécrire la condition d'annulation de $P(z)$ en « chassant les dénominateurs ».
17. Montrer $\mathcal{O} = \bigcup_{d \in \mathbb{N}^*} \bigcup_{A \in M_d(\mathbb{Z})} \mathrm{Sp}(A)$.
18. Soit $u \in \mathscr{L}\big(M_{d,\delta}(\mathbb{C})\big)$ un endomorphisme tel que $\forall A \in M_{d,\delta}(\mathbb{Z}), u(A) \in M_{d,\delta}(\mathbb{Z})$. Montrer que $\mathrm{Sp}(u) \subseteq \mathcal{O}$.
Indication. On pourra montrer que, dans la base canonique, la matrice de u est à coefficients entiers.
19. Soit $A \in M_d(\mathbb{C})$ et $B \in M_\delta(\mathbb{C})$. Vérifier rapidement que les applications

$$\mathrm{Syl}_{A,B} : \begin{cases} M_{d,\delta}(\mathbb{C}) \to M_{d,\delta}(\mathbb{C}) \\ M \mapsto AM - MB \end{cases} \qquad \text{et} \qquad \mathrm{Frob}_{A,B} : \begin{cases} M_{d,\delta}(\mathbb{C}) \to M_{d,\delta}(\mathbb{C}) \\ M \mapsto AMB \end{cases}$$

sont des endomorphismes de $M_{d,\delta}(\mathbb{C})$ et montrer les inclusions

$$\left\{ \alpha - \beta \,\middle|\, \alpha \in \mathrm{Sp}(A), \beta \in \mathrm{Sp}(B) \right\} \subseteq \mathrm{Sp}(\mathrm{Syl}_{A,B}) \qquad \text{et} \qquad \left\{ \alpha\beta \,\middle|\, \alpha \in \mathrm{Sp}(A), \beta \in \mathrm{Sp}(B) \right\} \subseteq \mathrm{Sp}(\mathrm{Frob}_{A,B}).$$

20. Déduire de ce qui précède que $\mathcal{O}$ est un sous-anneau de $\mathbb{C}$.

Partie V. Lemme de Selberg pour $\mathrm{GL}_d(\mathbb{Q})$

Soit Γ un sous-groupe de $\mathrm{GL}_d(\mathbb{Q})$ engendré par un nombre fini de matrices $U_1, \dots, U_r \in \mathrm{GL}_d(\mathbb{Q})$.

Étant donné $s \in \mathbb{N}^*$, on note $\mathbb{Z}[1/s] = \left\{ \dfrac{a}{s^n} \,\middle|\, a \in \mathbb{Z}, n \in \mathbb{N} \right\}$. Il s'agit d'un sous-anneau de $\mathbb{Q}$ (on ne demande pas de le vérifier).

21. On fixe $s \in \mathbb{N}^*$ tel que $\forall j \in [\![1, r]\!], sU_j^{\pm 1} \in M_d(\mathbb{Z})$.
Montrer que Γ est un sous-groupe de $\mathrm{GL}_d(\mathbb{Z}[1/s])$.

On fixe jusqu'à la fin de cette section un nombre premier p vérifiant $p > 2d$ et $p > s$.

22. Montrer qu'il existe un unique morphisme d'anneaux $\pi : \mathbb{Z}[1/s] \to \mathbb{F}_p$ prolongeant le morphisme $\tilde{\pi} : \mathbb{Z} \to \mathbb{F}_p$ de réduction modulo p.
23. On va montrer que le noyau $\ker \pi_*$ du morphisme de groupes $\pi_* : \mathrm{GL}_d(\mathbb{Z}[1/s]) \to \mathrm{GL}_d(\mathbb{F}_p)$ est sans torsion.
    (a) Soit $A \in \ker \pi_*$ et $m \in \mathbb{N}^*$ tel que $A^m = I_d$.
    Montrer que $\mathrm{tr}\, A \in \mathcal{O}$ et en déduire $\mathrm{tr}\, A \in \mathbb{Z}$.
    (b) En raisonnant modulo p, montrer que $\mathrm{tr}\, A = d$ et conclure.
24. Montrer que Γ est virtuellement sans torsion.

Partie VI. Lemme de Selberg pour $\mathrm{GL}_d(\mathbb{C})$

Un peu comme dans la partie précédente, on montre sans difficulté que tout sous-groupe de $\mathrm{GL}_d(\mathbb{C})$ engendré par un nombre fini d'éléments est en fait un sous-groupe d'un groupe linéaire $\mathrm{GL}_d(\mathrm{R})$, où R est un sous-anneau de $\mathbb{C}$ engendré[1] par un nombre fini de nombres complexes.

On va directement montrer que $\mathrm{GL}_d(\mathrm{R})$ est virtuellement sans torsion, ce qui conclut.

On admet le résultat suivant, qui n'est pas si difficile mais demande un peu de théorie des anneaux et des corps.

> **Résultat admis**. Soit R un sous-anneau de $\mathbb{C}$ engendré par un nombre fini d'éléments. Alors il existe un corps fini K et un morphisme d'anneaux $\mathrm{R} \to \mathrm{K}$.

On peut donc fixer K un corps fini, dont on notera p la caractéristique, et $\varphi : \mathrm{R} \to \mathrm{K}$ un morphisme d'anneaux.

25. Soit $\mathrm{A} \in \ker \varphi*$ et $m \in \mathbb{N}^*$ tel que $\mathrm{A}^m = \mathrm{I}_d$. On suppose que p ne divise pas m.
    (a) On note $\mathrm{S} = \sum_{k=0}^{m-1} \mathrm{A}^k \in \mathrm{M}_d(\mathrm{R})$. Calculer $\mathrm{M}_d(\varphi)(\mathrm{S})$ et en déduire que $\mathrm{S} \in \mathrm{GL}_d(\mathbb{C})$.
    (b) En calculant $(\mathrm{A} - \mathrm{I}_d)\mathrm{S}$, montrer que $\mathrm{A} = \mathrm{I}_d$.
26. Montrer que tout élément de $\ker \varphi_*$ est soit d'ordre infini, soit d'ordre une puissance de p.
27. En appliquant le résultat admis à $\mathrm{R}[1/p] = \left\{ \frac{a}{p^n} \,\middle|\, a \in \mathrm{R}, n \in \mathbb{N} \right\}$, montrer qu'il existe un corps fini L de caractéristique $\ell \neq p$ et un morphisme d'anneaux $\psi : \mathrm{R} \to \mathrm{L}$.
28. Montrer que $\mathrm{GL}_d(\mathrm{R})$ est virtuellement sans torsion.

1. Par définition, un sous-anneau R de C est engendré par $z_1, \dots, z_r$ s'il est le plus petit sous-anneau de $\mathbb{C}$ contenant ces éléments. Cet anneau est souvent noté $\mathbb{Z}[z_1, \dots, z_r]$ car il s'agit de l'ensemble des valeurs $\mathrm{P}(z_1, \dots, z_r)$ des polynômes entiers en r variables.