Les calculatrices, téléphones, tablettes, ordinateurs, montres connectées et tous appareils électroniques de communication ou de stockage, ainsi que les documents, sont interdits. La qualité de la rédaction sera un facteur important d'appréciation des copies. Il est possible d'utiliser les résultats énoncés dans les questions ou parties précédentes, en veillant toutefois à préciser la référence du résultat utilisé.

L'épreuve comporte deux parties :

— Une première partie, composée d'**exercices**. Les candidats sont invités à consacrer au moins un tiers du temps de l'épreuve de cette partie en cherchant à traiter les quatre exercices numérotés 1, 2, 3 et 4.

— Un problème à traiter **au choix** parmi deux proposés : le Problème 1, plutôt orienté « Algèbre et Géométrie » ou bien le Problème 2, plutôt orienté « Analyse et Probabilités ». **Le candidat devra indiquer clairement sur sa copie le problème qu'il choisit. Seul ce choix sera pris en compte dans l'évaluation.** Au moins la moitié du temps de l'épreuve devrait être consacrée à l'un de ces problèmes.

Le barème tient compte de cette répartition indicative du temps à accorder à chaque partie.

Exercice 1

Soit n un entier naturel non nul. On note $\mathcal{M}_n(\mathbb{C})$ l'algèbre des matrices carrées $n \times n$ à coefficients complexes. Si $M \in \mathcal{M}_n(\mathbb{C})$, on note $\operatorname{Tr} M$ sa trace. On rappelle que la fonction $\operatorname{Tr} : \mathcal{M}_n(\mathbb{C}) \to \mathbb{C}$ est une forme linéaire et que si M et N sont deux matrices de $\mathcal{M}_n(\mathbb{C})$, alors $\operatorname{Tr}(MN) = \operatorname{Tr}(NM)$. Si $M, N \in \mathcal{M}_n(\mathbb{C})$, on note $[M, N] = MN - NM$. On admet (et c'est immédiat) que $[,]$ est bilinéaire sur $\mathcal{M}_n(\mathbb{C})$.

Pour toute matrice $A \in \mathcal{M}_n(\mathbb{C})$, on note ad_A l'endomorphisme de $\mathcal{M}_n(\mathbb{C})$ défini par $\operatorname{ad}_A : M \mapsto [A, M]$. Pour toute matrice inversible P de $\mathcal{M}_n(\mathbb{C})$, on note φ_P l'endomorphisme de $\mathcal{M}_n(\mathbb{C})$ défini par $\varphi_P : M \mapsto PMP^{-1}$. Pour toute matrice $A \in \mathcal{M}_n(\mathbb{C})$, on note $f_A : \mathcal{M}_n(\mathbb{C}) \to \mathbb{C}$ définie par $f_A : M \mapsto \operatorname{Tr}(AM)$.

1. Soient $A \in \mathcal{M}_n(\mathbb{C})$ et $\lambda \in \mathbb{C}$. Que dire de $\operatorname{ad}_{A+\lambda I_n}$?

2. Montrer que l'application $A \mapsto f_A$ est un isomorphisme entre les espaces vectoriels $\mathcal{M}_n(\mathbb{C})$ et $\mathcal{L}(\mathcal{M}_n(\mathbb{C}), \mathbb{C})$.

3. Soit $A, B \in \mathcal{M}_n(\mathbb{C})$. Montrer qu'il existe un unique $C \in \mathcal{M}_n(\mathbb{C})$ telle que

$$f_A \circ \operatorname{ad}_B = f_C$$

et exprimer C en fonction de A et B.

Soit $N \in \mathcal{M}_n(\mathbb{C})$ nilpotente. On souhaite montrer qu'il existe $X \in \mathcal{M}_n(\mathbb{C})$ telle que $[X, N] = N$.

4. Montrer que toute matrice nilpotente de $\mathcal{M}_n(\mathbb{C})$ est de trace nulle.

5. Montrer que $\operatorname{Ker} \operatorname{ad}_N \subset \operatorname{Ker} f_N$.

6. Montrer qu'il existe $\varphi \in \mathcal{L}(\mathcal{M}_n(\mathbb{C}), \mathbb{C})$ telle que $f_N = \varphi \circ \operatorname{ad}_N$.

7. Conclure.

Soient $X, N \in \mathcal{M}_n(\mathbb{C})$ qui vérifient $[X, N] = N$. On se propose de montrer réciproquement qu'alors N est nilpotente.

8. Soit $k \in \mathbb{N}$. Montrer que $[X, N^k] = kN^k$.

9. Conclure.

Exercice 2

Dans tout l'exercice, p est un entier supérieur ou égal à 2. On note $\mathcal{M}_p(\mathbb{C})$ l'ensemble des matrices carrées $p \times p$ et I_p la matrice identité $p \times p$. On note D le disque ouvert complexe de centre 0 et de rayon 1 et $\overline{D}$ le disque fermé de centre 0 et de rayon 1.

Pour toute matrice $M \in \mathcal{M}_p(\mathbb{C})$, on note $\mathrm{Sp}(M)$ le spectre de M, c'est-à-dire l'ensemble de ses valeurs propres. Si λ est une valeur propre de M, on note $m(\lambda)$ la multiplicité de λ en tant que racine du polynôme caractéristique χ_M de M ; on note de plus $E_\lambda(M) = \mathrm{Ker}(M - \lambda I_p)$ l'espace propre associé et $K_\lambda(M) = \mathrm{Ker}(M - \lambda I_p)^{m(\lambda)}$ l'espace caractéristique associé.
On rappelle que $\mathcal{M}_p(\mathbb{C})$ ne possède qu'une seule topologie d'espace normé puisque toutes les normes y sont équivalentes. Cela permet de parler sans ambiguïté de suites bornées et de suites convergentes.

1. Déterminer successivement, en justifiant la réponse, l'ensemble des $z \in \mathbb{C}$ tels que :
   - (i) la suite $(z^n)_{n\in\mathbb{N}}$ est bornée ;
   - (ii) la suite $(z^n)_{n\in\mathbb{N}}$ converge ;
   - (iii) la série $\sum z^n$ converge ;
   - (iv) la suite de terme général $\dfrac{1}{n}\displaystyle\sum_{k=0}^{n-1} z^k$ converge.

2. Soit A, $B \in \mathcal{M}_p(\mathbb{C})$ semblables. Montrer que $(A^n)_{n\in\mathbb{N}}$ converge (resp. est bornée) si et seulement si $(B^n)_{n\in\mathbb{N}}$ converge (resp. est bornée).

3. Soit $N \in \mathcal{M}_p(\mathbb{C})$ nilpotente non nulle. Montrer qu'il existe $x \in \mathrm{Ker}\, N^2 \setminus \mathrm{Ker}\, N$.

Dans les questions 4 à 7, on suppose que $M \in \mathcal{M}_p(\mathbb{C})$ est une matrice admettant une unique valeur propre λ.

4. On suppose dans cette question que la suite $(M^n)_{n\in\mathbb{N}}$ est bornée et que $|\lambda| = 1$. Montrer que $M = \lambda I_p$.

5. Montrer que la suite $(M^n)_{n\in\mathbb{N}}$ converge vers 0 si et seulement si $\lambda \in D$.

6. À quelle condition nécessaire et suffisante la suite $(M^n)_{n\in\mathbb{N}}$ est-elle bornée ?

7. À quelle condition nécessaire et suffisante la suite $(M^n)_{n\in\mathbb{N}}$ converge-t-elle ?

On revient au cas général. Soit $M \in \mathcal{M}_p(\mathbb{C})$.

8. Caractériser à l'aide des $m(\lambda)$ et des $E_\lambda(M)$ les matrices $M \in \mathcal{M}_p(\mathbb{C})$ telles que la suite $(M^n)_{n\in\mathbb{N}}$ soit bornée.

9. Soit $A \in \mathcal{M}_p(\mathbb{C})$ telle que la suite $(A^n)_{n\in\mathbb{N}}$ soit bornée. On pose

$$B_n = \frac{1}{n+1}\sum_{k=0}^{n} A^k.$$

   - (a) Montrer que $(B_n)_{n\in\mathbb{N}}$ admet une valeur d'adhérence B. Montrer que $AB = BA = B$ et que B est un projecteur.
   - (b) Montrer que $\mathrm{Ker}\, B = \mathrm{Im}(I_p - A)$ et que $\mathrm{Im}\, B = \mathrm{Ker}(I_p - A)$.
   - (c) Montrer que $(B_n)_{n\in\mathbb{N}}$ converge.

10. Déterminer les matrices $M \in \mathcal{M}_p(\mathbb{C})$ telles que la suite $\left(\dfrac{1}{n}\displaystyle\sum_{k=0}^{n-1} M^k\right)_{n\in\mathbb{N}^*}$ converge.

11. Déterminer les matrices $M \in \mathcal{M}_p(\mathbb{C})$ telles que la série $\sum M^n$ converge.

Exercice 3

Dans cet exercice, les variables aléatoires sont définies sur un même espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ et à valeurs dans $\mathbb{N}$. La *distance en variation totale* entre deux variables aléatoires X et Y est définie par

$$d(X,Y) = \sup_{A \in \mathcal{P}(\mathbb{N})} \Big| \mathbb{P}(X \in A) - \mathbb{P}(Y \in A) \Big|,$$

où $\mathcal{P}(\mathbb{N})$ désigne l'ensemble des parties de $\mathbb{N}$.

I. Propriétés de la distance en variation totale

1. (a) Soit X et Y deux variables aléatoires (définies sur Ω et à valeurs dans $\mathbb{N}$).
Pour $A \in \mathcal{P}(\mathbb{N})$, montrer que $\mathbb{P}(X \in A) \leqslant \mathbb{P}(Y \in A) + \mathbb{P}(X \neq Y)$. En déduire que

$$d(X,Y) \leqslant \mathbb{P}(X \neq Y).$$

(b) Soit $n \in \mathbb{N}^*$ et $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ des variables aléatoires à valeurs dans $\mathbb{N}$. Montrer

$$d\Big(\sum_{i=1}^{n} X_i, \sum_{i=1}^{n} Y_i\Big) \leqslant \sum_{i=1}^{n} \mathbb{P}(X_i \neq Y_i).$$

2. Montrer que $d(X,Y) = \dfrac{1}{2} \displaystyle\sum_{k \in \mathbb{N}} \big|\mathbb{P}(X = k) - \mathbb{P}(Y = k)\big|$.

II. Rappels sur les variables aléatoires de Poisson

Soit Y une variable aléatoire de Poisson de paramètre $\lambda \geqslant 0$.
On rappelle que Y est à valeurs dans $\mathbb{N}$ et que, pour pour tout $k \in \mathbb{N}$, $\mathbb{P}(Y = k) = e^{-\lambda} \dfrac{\lambda^k}{k!}$.

3. Calculer l'espérance et la variance de Y.

4. Soit Y' une variable aléatoire de Poisson de paramètre λ' telle que Y et Y' soient indépendantes. Montrer que $Y + Y'$ est une variable aléatoire de Poisson de paramètre $\lambda + \lambda'$.

III. Couplage Bernoulli-Poisson

Soit $p \in [0,1]$ et soit (X,Y) un couple de variables aléatoires à valeurs dans $\mathbb{N}$ définies sur Ω.
On dit que (X,Y) est un *p-couple adapté de Bernoulli-Poisson* si

$$\mathbb{P}(X = 0, Y = k) = \begin{cases} 1-p & \text{si } k = 0 \\ 0 & \text{si } k \geqslant 1 \end{cases} \quad \text{et} \quad \mathbb{P}(X = 1, Y = k) = \begin{cases} e^{-p} - (1-p) & \text{si } k = 0 \\ e^{-p}\dfrac{p^k}{k!} & \text{si } k \geqslant 1 \end{cases}$$

On suppose dans cette partie que (X,Y) est un p-couple adapté de Bernoulli-Poisson.

5. Montrer que les formules précédentes définissent une loi de probabilité pour (X,Y), que X est une variable de Bernoulli de paramètre p et que Y est une variable de Poisson de paramètre p.

6. Montrer que $d(X,Y) = p(1 - e^{-p})$.

IV. Inégalité de Le Cam

On suppose que $X_1, \ldots, X_n$ sont des variables aléatoires de Bernoulli sur Ω indépendantes, et on note $p_i = \mathbb{E}(X_i)$. On suppose données des variables aléatoires de Poisson indépendantes $Y_1, \ldots, Y_n$ sur Ω telles que, pour tout i, (X_i, Y_i) soit un p_i-couple adapté de Bernoulli-Poisson. On note

$$X = \sum_{i=1}^{n} X_i \qquad Y = \sum_{i=1}^{n} Y_i \qquad \lambda = \sum_{i=1}^{n} p_i$$

7. Montrer $d(X,Y) \leqslant \displaystyle\sum_{i=1}^{n} p_i(1 - e^{-p_i})$.

8. En déduire l'inégalité de Le Cam : $\displaystyle\sum_{k=0}^{\infty} \Big| P(X = k) - e^{-\lambda}\frac{\lambda^k}{k!} \Big| \leqslant 2 \sum_{i=1}^{n} p_i^2$.

Exercice 4

Soit G l'ensemble des fonctions $f : \mathbb{R} \to \mathbb{R}$ continues et strictement croissantes telles que pour tout $x \in \mathbb{R}$, $f(x+1) = f(x) + 1$.

I. Le groupe des homéomorphismes croissants de $\mathbb{R}$

1. Soit $f \in G$. Déterminer les limites en $\pm\infty$ de f.

2. Montrer que $(G, \circ)$ est un groupe.

3. Soit $f \in G$. Que dire de la périodicité de $x \mapsto f(x) - x$? En déduire que les fonctions $f \in G$ sont uniformément continues.

4. Quelles sont les fonctions $f \in G$ affines ? convexes ? polynomiales ?

5. Donner un exemple de fonction $f \in G$ qui n'est pas lipschitzienne.

II. Nombre de translation

6. Montrer que pour tous $x, y \in \mathbb{R}$, l'écart en valeur absolue entre $f(x) - x$ et $f(y) - y$ est inférieur ou égal à 1.

On choisit désormais et jusqu'à la fin de cette partie une fonction $f \in G$ et $x_0 \in \mathbb{R}$.
On pose $F(n) = f^n(x_0) - x_0$, où f^n désigne $f \circ f \circ \cdots \circ f$ (n fois).

7. Montrer que pour tous $n, p \in \mathbb{N}$, on a

$$|F(n+p) - F(n) - F(p)| \leqslant 1.$$

8. En déduire que pour tous $n, k \in \mathbb{N}^*$, on a $\left| \dfrac{F(kn)}{kn} - \dfrac{F(n)}{n} \right| \leqslant \dfrac{1}{n}$.

9. En déduire que la suite $(F(n)/n)_{n \in \mathbb{N}^*}$ est de Cauchy. On note τ_{x_0} sa limite.

10. Montrer que si $x, y \in \mathbb{R}$ sont tels que $|x - y| \leqslant k$ où $k \in \mathbb{N}$, alors $|f^n(x) - f^n(y)| \leqslant k$ pour tout $n \in \mathbb{N}$. En déduire que τ_{x_0} ne dépend pas de x_0.

Le réel $\tau_{x_0} = \tau$ s'appelle le nombre de translation de f. On le notera aussi $\tau(f)$.

11. Montrer que pour tout $x \in \mathbb{R}$ et tout $n \in \mathbb{N}$,

$$-1 \leqslant f^n(x) - x - n\tau \leqslant 1. \tag{1}$$

III. Quelques propriétés du nombre de translation

12. Soit $\lambda \in \mathbb{R}$ et $T_\lambda : \mathbb{R} \to \mathbb{R}$ la fonction définie par $T_\lambda(x) = x + \lambda$. Montrer que $T_\lambda \in G$ et déterminer son nombre de translation.

13. Soit $f \in G$ et $k \in \mathbb{N}$. Montrer que $\tau(f^k) = k\tau(f)$.

14. (a) On note $\|.\|_\infty$ la norme uniforme sur les fonctions bornées de $\mathbb{R}$ dans $\mathbb{R}$. Montrer que l'application $d : G \times G \to \mathbb{R}^+$ définie par $d(f, g) = \|f - g\|_\infty$ est une distance sur G.

(b) Montrer que si $(f_n)_{n \in \mathbb{N}}$ et $(g_n)_{n \in \mathbb{N}}$ sont deux suites dans l'espace métrique G convergeant respectivement vers f et g dans G, alors $(f_n \circ g_n)_{n \in \mathbb{N}}$ converge vers $f \circ g$.

(c) Montrer que $\tau : G \to \mathbb{R}$ est continue pour cette distance.

IV. Nombre de rotation et points fixes

Pour tout $x \in \mathbb{R}$, on note $\lfloor x \rfloor$ la partie entière de x et $\{x\} = x - \lfloor x \rfloor$ sa partie fractionnaire. On note $\mathbb{U}$ l'ensemble des nombres complexes de module 1. Pour tout $f \in G$ et tout $\theta \in \mathbb{R}$, on pose

$$\widehat{f}(e^{i2\pi\theta}) = e^{i2\pi f(\theta)} \qquad \text{et} \qquad \rho(\widehat{f}) = \tau(f) - \lfloor \tau(f) \rfloor = \{\tau(f)\}\,.$$

Le réel $\rho(\widehat{f})$ s'appelle le nombre de rotation de $\widehat{f}$.

Soit $f \in G$.

15. Montrer que $\widehat{f}$ est une bijection de $\mathbb{U}$ sur lui-même. *(On vérifiera que $\widehat{f}$ est bien définie.)*

16. Soit $g \in G$. Montrer que $\widehat{f} = \widehat{g}$ si et seulement si il existe $p \in \mathbb{Z}$ tel que $f - g = p$.
En particulier, si $\widehat{f} = \widehat{g}$, alors $\rho(\widehat{f}) = \rho(\widehat{g})$, et donc le nombre de rotation de $\widehat{f}$ est bien défini.

17. Soit $\alpha \in \mathbb{R}$ et $r_\alpha : \mathbb{U} \to \mathbb{U}$ la rotation définie par $z \mapsto e^{i2\pi\alpha} z$. Montrer qu'il existe $h \in G$ telle que $\widehat{h} = r_\alpha$ et déterminer le nombre de rotation associé.

18. On suppose que $\widehat{f}$ n'admet pas de point fixe.

(a) Montrer que l'image de $x \mapsto f(x) - x$ est un segment $[a, b]$ inclus dans un intervalle $]k, k+1[$ où $k \in \mathbb{Z}$.

(b) Avec les notations de la question précédente, montrer que pour tout $n \in \mathbb{N}^*$ et tout $x \in \mathbb{R}$,

$$na \leqslant f^n(x) - x \leqslant nb.$$

19. Montrer que $\widehat{f}$ admet un point fixe si et seulement si $\rho(\widehat{f}) = 0$.

20. L'orbite du point $z \in \mathbb{U}$ sous $\widehat{f}$ est l'ensemble $\{\widehat{f}^k(z) \mid k \in \mathbb{Z}\}$. Montrer que $\widehat{f}$ admet une orbite finie si et seulement si $\rho(\widehat{f}) \in \mathbb{Q}$.

Problème d'algèbre – le lemme de Selberg

Lorsque p est un nombre premier, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps à p éléments. Tous les anneaux de ce problème sont des anneaux unitaires, c'est-à-dire que A contient un élément neutre pour le produit généralement noté 1_A. On rappelle que si A est un anneau commutatif intègre, alors A est un sous-anneau de son corps de fractions. Les corps seront toujours des corps commutatifs.
Si k est un corps et $X_1, ..., X_n$ des indéterminées, on note $k(X_1, \dots, X_n)$ le corps des fractions de l'anneau commutatif intègre $k[X_1, \dots, X_n]$. Ses éléments sont les fractions rationnelles $\dfrac{P(X_1, \dots, X_n)}{Q(X_1, \dots, X_n)}$ où $P, Q \in k[X_1, \dots, X_n]$ avec Q non nul.
Si A est un anneau commutatif, on désigne par $\mathcal{M}_n(A)$ l'ensemble des matrices carrées $n \times n$ à coefficient dans l'anneau A. Si $\alpha \in A$, on dispose alors du morphisme d'anneau $\mathbb{Z}[X] \to A$ donné par $P \mapsto P(\alpha)$. On note $\mathbb{Z}[\alpha]$ son image ; c'est un sous-anneau de A.

Un élément γ d'un groupe G est de torsion s'il est d'ordre fini, c'est-à-dire qu'il existe $m \in \mathbb{N}^*$ tel que $\gamma^m = e$ où e est l'élément neutre de G. Un groupe G est de torsion si tous ses éléments sont de torsion ; il est sans torsion si le seul élément de torsion est e. Un groupe G est de type fini s'il est engendré par une partie finie de G.

Dans tout ce problème, k est un corps commutatif et n est un entier naturel supérieur ou égal à 2.

L'objectif du problème est de démontrer le résultat suivant, dû à Atle Selberg (1960).

Lemme de Selberg *Soit k un corps de caractéristique nulle et Γ un sous-groupe de type fini de $\mathrm{GL}_n(k)$. Alors Γ contient un sous-groupe d'indice fini et distingué sans torsion.*

I Le groupe $\mathrm{GL}_n(A)$

Soit A un anneau commutatif intègre et soit K_A son corps des fractions.

1. Montrer que $(\mathcal{M}_n(A), +, \times)$ est un sous-anneau de $(\mathcal{M}_n(K_A), +, \times)$.
On note $G = \mathrm{GL}_n(A)$ son groupe des inversibles.

2. Soient A et B deux anneaux commutatifs et $\varphi : A \to B$ un morphisme d'anneaux. On définit $\widetilde{\varphi} : \mathcal{M}_n(A) \to \mathcal{M}_n(B)$ de la manière suivante : si $M \in \mathcal{M}_n(A)$, en notant $[M]_{i,j}$ le coefficient matriciel d'indice (i, j) de M, alors $[\widetilde{\varphi}(M)]_{i,j} = \varphi([M]_{i,j})$.
Montrer que $\widetilde{\varphi}$ est un morphisme d'anneaux unitaires. Montrer que sa restriction à $\mathrm{GL}_n(A)$ est un morphisme de groupe de $\mathrm{GL}_n(A)$ dans $\mathrm{GL}_n(B)$.

3. Soit $M \in \mathcal{M}_n(\mathbb{Z})$. Montrer $M \in \mathrm{GL}_n(\mathbb{Z})$ si et seulement si $\det M = \pm 1$.

II Sous-groupes d'indice fini

Soit G un groupe et H un sous-groupe de G, et l'on écrira $H < G$. Si $x \in G$, on note $xH = \{xh \mid h \in H\}$.

4. On considère la relation binaire $\sim$ sur G définie par $x \sim y$ si et seulement si $x^{-1}y \in H$. Montrer que $\sim$ est une relation d'équivalence et que les classes d'équivalences sont les xH où x parcourt G.
On note G/H l'ensemble des classes d'équivalence.

Définition *Soit H un sous-groupe du groupe G. Le groupe H est d'indice fini dans G si G/H est fini.*

5. Soit $f : G \to H$ un morphisme de groupe où H est fini. Montrer que $\operatorname{Ker} f$ est un sous-groupe d'indice fini de G et distingué.

III Le lemme de Selberg pour $\mathrm{GL}_n(\mathbb{Z})$

Dans cette partie, on démontre de deux manières un cas particulier du lemme de Selberg. La première est élémentaire, mais c'est la deuxième qui se généralisera à tout corps de caractéristique nulle.

Soit G le sous-groupe $\mathrm{GL}_n(\mathbb{Z})$ de $\mathrm{GL}_n(\mathbb{Q})$ et Γ un sous-groupe de G (pas forcément de type fini). On souhaite démontrer que Γ contient un sous-groupe d'indice fini distingué sans torsion.

III.1 Une première méthode

On fixe ici $p = 3$. D'après la question 2, on dispose du morphisme de réduction $f : \mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{F}_p)$ induit par le morphisme d'anneau $\mathbb{Z} \to \mathbb{F}_p$ de réduction modulo p. Soit G_0 son noyau. On choisit $\gamma \in G_0$ de torsion, c'est-à-dire qu'il existe $m \in \mathbb{N}^*$ tel que $\gamma^m = I_n$.

6. Montrer que γ est diagonalisable dans $\mathcal{M}_n(\mathbb{C})$. Que dire de ses valeurs propres ?
7. Montrer que $A = \dfrac{1}{3}(\gamma - I_n)$ est une matrice de $\mathcal{M}_n(\mathbb{Z})$.
8. Montrer que la suite $(A^k)_{k\in\mathbb{N}}$ converge vers 0.
9. En déduire que $A = 0$.
10. Montrer que Γ admet un sous-groupe d'indice fini sans torsion.

III.2 Une deuxième méthode

On fixe un nombre premier p strictement supérieur à $2n$. D'après la question 2, le morphisme de réduction modulo p induit un morphisme de groupe $f_0 : \Gamma \to \mathrm{GL}_n(\mathbb{F}_p)$. Soit Γ_0 le noyau de ce morphisme. On choisit $\gamma \in \Gamma_0$ de torsion, c'est-à-dire qu'il existe $m \in \mathbb{N}^*$ tel que $\gamma^m = I_n$.

11. Montrer que $|\operatorname{Tr}\gamma| \leqslant n$. *On pourra utiliser la question 6.*
12. Montrer que $\operatorname{Tr}\gamma \equiv n \mod p$ puis que $\operatorname{Tr}\gamma = n$.
13. Montrer que Γ_0 est un sous-groupe distingué d'indice fini sans torsion de Γ.

IV Entiers algébriques

Soit A un anneau commutatif intègre. On dit que $x \in A$ est un entier algébrique si x est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$.
On rappelle que si $P \in \mathbb{Z}[X_1, X_2, ..., X_n]$ est un polynôme symétrique en les indéterminées $X_1, ..., X_n$, alors il existe un polynôme $Q \in \mathbb{Z}[X_1, X_2, ..., X_n]$ tel que $P = Q(\sigma_1, \sigma_2, ..., \sigma_n)$ où les σ_k sont les polynômes symétriques élémentaires en les X_i, à savoir

$$\sigma_k = \sigma_k(X_1, ..., X_n) = \sum_{I \subset [\![1,n]\!],\ |I|=k} \prod_{i\in I} X_i.$$

On note $\mathfrak{S}_n$ ou S_n le groupe symétrique des permutations de $[\![1, n]\!]$.
On note E l'ensemble des entiers algébriques de A. On se propose de montrer dans les questions 14 à 17 que E est un anneau. Soient $\alpha_1, \alpha_2 \in E$ distincts.

14. Montrer qu'il existe un $P \in \mathbb{Z}[X]$ unitaire dont α_1 et α_2 sont racines. On fixe un tel P.

15. Soit K un corps de décomposition de P.
Il existe donc $\alpha_3, \dots, \alpha_n \in K$ tels que $P = (X - \alpha_1) \cdots (X - \alpha_n)$.
Soit g un polynôme de $\mathbb{Z}[X_1, X_2, ..., X_n]$ et $h(X) = \prod_{s \in \mathfrak{S}_n} (X - g(\alpha_{s(1)}, ..., \alpha_{s(n)}))$.
Montrer que les coefficients de h sont dans $\mathbb{Z}$.

16. En considérant $g(X_1, ..., X_n) = X_1 - X_2$, montrer que $\alpha_1 - \alpha_2$ est un entier algébrique de A.

17. Montrer que E est un sous-anneau de A. *On pourra adapter la question précédente en modifiant judicieusement g.*

18. Quels sont les entiers algébriques de $\mathbb{Q}$?

19. Soient $X_1, ...X_r$ des indéterminées. Quel est l'anneau des entiers de $\mathbb{Q}(X_1, ..., X_r)$?

V Le lemme de Selberg pour $k = \mathbb{Q}$

On note $k = \mathbb{Q}$ et $G = \mathrm{GL}_n(k)$. Soit Γ un sous-groupe de type fini de G.

20. Montrer qu'il existe un entier $s \in \mathbb{N}^*$ tel que Γ est un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}[1/s])$. On note désormais A l'anneau $\mathbb{Z}[1/s]$.

21. Soit p premier strictement supérieur à s et $2n$. Montrer que le morphisme de réduction modulo p de $\mathbb{Z}$ dans $\mathbb{F}_p$ se prolonge en un morphisme d'anneaux surjectif de A dans $\mathbb{F}_p$ et que ce morphisme induit un morphisme de groupes de Γ dans $\mathrm{GL}_n(\mathbb{F}_p)$.

On fixe désormais ce p et on note Γ_0 son noyau.

22. Soit $\gamma \in \Gamma_0$ de torsion ; on note $m \in \mathbb{N}^*$ tel que $\gamma^m = I_n$. Montrer que $\mathrm{Tr}\,\gamma$ est un entier algébrique. En déduire comme en III.2 que $\gamma = I_n$.

23. En déduire le lemme de Selberg pour $k = \mathbb{Q}$.

VI Structure des extensions de corps de type fini

Si k est un sous-corps du corps K, on dit que K est une extension du corps k ; on parle alors de l'extension K/k. Dans ce cas, le corps K est une k-algèbre commutative. Le degré de l'extension K/k est la dimension de K comme k-espace vectoriel. Lorsque ce degré est fini, on le note $[K : k]$.
On rappelle que si L/K et K/k sont deux extensions de degrés finis, alors $[L : K][K : k] = [L : k]$ (théorème de multiplicativité des degrés).

Soit K/k une extension de corps. Si $u_1, ..., u_r$ sont des éléments de K, on note $k(u_1, ..., u_r)$ le plus petit sous-corps de K contenant k et tous les u_j. Les éléments de $k(u_1, ..., u_r)$ sont les $\dfrac{P(u_1, ..., u_r)}{Q(u_1, ..., u_r)}$ où $P, Q \in k[X_1, ..., X_r]$ tels que $Q(u_1, ..., u_r)$ soit non nul.

Soit K/k une extension de corps et $u_1, ..., u_r$ dans K. On dit que la famille $(u_1, ..., u_r)$ est algébriquement liée sur k s'il existe un polynôme non nul $P \in k[X_1, ..., X_r]$ tel que $P(u_1, ..., u_r) = 0$, et qu'elle est algébriquement libre sinon. Lorsque $(u_1, ..., u_r)$ est algébriquement libre sur k, on dit que l'extension $k(u_1, ..., u_r)/k$ est purement transcendante.
Le but de cette partie est de prouver le résultat suivant :

Lemme *Soit k un corps et L une extension de k. On suppose qu'il existe $a_1, ..., a_r \in L$ tels que $L = k(a_1, ..., a_r)$. Alors il existe un sous-corps K de L contenant k tel que l'extension K/k est purement transcendante et l'extension L/K est finie.*

Soit L un corps et k un sous-corps de L. On suppose qu'il existe $a_1, ..., a_r \in L$ tels que $L = k(a_1, ..., a_r)$. On dit alors que L est une extension de type fini de k.

24. Montrer qu'il existe une partie une partie $I \subset [\![1, r]\!]$ telle que $(a_i)_{i\in I}$ est algébriquement libre de cardinal maximal.

Quitte à renuméroter les a_i, on supposera dans la suite que $(a_1, ..., a_s)$ est algébriquement libre de cardinal maximal.

25. Montrer que $k(a_1, ..., a_s)$ est isomorphe en tant que corps à $k(X_1, ..., X_s)$

26. Soit $L = k(a_1, ..., a_r)$ et $K = k(a_1, ..., a_s)$. Montrer que l'extension L/K est de degré fini.

VII Le lemme de Selberg

Soit $G = \mathrm{GL}_n(k)$ où k est un corps de caractéristique nulle.
On suppose dans les questions 27 à 33 qu'il existe $r \in \mathbb{N}^*$ tel que $k = \mathbb{Q}(X_1, ...X_r)$ et que Γ est un sous-groupe de type fini de G.

27. Montrer qu'il existe $s = s(X_1, ..., X_r) \in \mathbb{Z}[X_1, ..., X_r]$ non nul tel que $\Gamma < \mathrm{GL}_n(A)$ où $A = \mathbb{Z}[X_1, ..., X_r, 1/s]$.

28. Justifier qu'il existe un nombre premier $p > 2n$ tel que $s \not\equiv 0 \mod p$.

29. Soit $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. Montrer qu'il existe $(\alpha_1, ..., \alpha_r) \in (\overline{\mathbb{F}}_p)^r$ tel que $s(\alpha_1, ..., \alpha_r) \neq 0$. On fixe une telle famille et on note $K = \mathbb{F}_p(\alpha_1, ..., \alpha_r)$. *On pourra raisonner par récurrence sur r.*

30. Montrer que $K = \mathbb{F}_p(\alpha_1, ..., \alpha_r)$ est un corps fini.

31. Montrer l'existence d'un morphisme d'anneaux $\varphi : A = \mathbb{Z}[X_1, ..., X_r, 1/s] \to K$ qui envoie X_i sur α_i pour tout i entre 1 et r.

On dispose donc d'un morphisme de réduction $f : \mathrm{GL}_n(A) \to \mathrm{GL}_n(K)$ induit par φ.

32. Soit Γ_0 le noyau de la restriction de f à Γ et $\gamma \in \Gamma_0$ d'ordre $m \in \mathbb{N}^*$. Montrer que $\mathrm{Tr}\,\gamma$ est un entier et que $|\mathrm{Tr}\,\gamma| \leqslant n$. *On pourra remarquer que γ est diagonalisable dans $\mathcal{M}_n(\mathbb{C}(X_1, ..., X_r))$ et que $\mathrm{Tr}\,\gamma$ est un entier algébrique.*

33. Montrer que Γ_0 est un sous-groupe d'indice fini sans torsion de Γ.

On revient au cas général. Soit k un corps de caractéristique nulle et Γ un sous-groupe de type fini de $\mathrm{GL}_n(k)$.

34. Montrer qu'il existe un nombre fini d'éléments $a_1, ..., a_r \in k$ tel que $\Gamma \subset \mathrm{GL}_n(\mathbb{Q}(a_1, ..., a_r))$.

On peut donc supposer que k est de la forme $\mathbb{Q}(a_1, ..., a_r)$. D'après la partie VI, il existe un sous-corps k_0 de k tel que k_0 est une extension transcendante pure de $\mathbb{Q}$ et k une extension de degré fini de k_0. On note d le degré de l'extension k/k_0.

35. Soit H un sous-groupe de $\mathrm{GL}_n(k)$. Montrer que H est isomorphe à un sous-groupe de $\mathrm{GL}_{nd}(k_0)$. *On pourra remarquer que si K/k est une extension de corps, et en notant $\mathcal{L}_k(K^n)$ les endomorphismes k-linéaires de K^n, alors $\mathcal{L}_K(K^n)$ est un sous-anneau de $\mathcal{L}_k(K^n)$.*

36. En déduire le lemme de Selberg.

37. **Une application**. Soit k un corps de caractéristique nulle et Γ un sous-groupe de torsion et de type fini de $\mathrm{GL}_n(k)$. Montrer que Γ est fini. (Théorème de Burnside.)

Problème d'analyse

Ce problème traite diverses questions d'analyse réelle et complexe (parties I à III) qui se rattachent aux formes modulaires (partie IV) avant d'aboutir à un résultat sur un certain réseau de $\mathbb{R}^8$.

La partie I établit le produit eulérien de $\sin(\pi x)$ et le développement eulérien de $\dfrac{\cos(\pi z)}{\sin(\pi z)}$.

La partie II utilise séries de Fourier et transformation de Fourier en vue de la formule de Poisson.

La partie III porte sur une série d'Eisenstein, en vue de la partie IV sur les formes modulaires et de la partie V de conclusion.

Rappels et notations

On rappelle deux résultats d'analyse complexe.

— **Stabilité de l'holomorphie par convergence uniforme :** Si $\sum_{n\in\mathbb{N}} f_n$ est une série de fonctions holomorphes sur un ouvert Ω de $\mathbb{C}$, et si cette série converge uniformément sur tout compact de Ω, alors la somme S de cette série est une fonction holomorphe sur Ω.

— **Principe du prolongement analytique :** Si f et g sont deux fonctions holomorphes sur un ouvert connexe Ω qui coïncident sur une partie A de Ω possédant un point d'accumulation, alors $f = g$.

Pour la partie II, on rappelle les résultats suvants.

— Pour toute fonction f de $\mathbb{R}$ dans $\mathbb{C}$ de classe $\mathscr{C}^\infty$ et 1-périodique, on considère ses coefficients de Fourier, donnés par

$$\forall n \in \mathbb{Z}, \qquad c_n(f) = \int_0^1 f(x)e^{-2i\pi nx}\,\mathrm{d}x,$$

et on admet que f est somme, normalement convergente, de sa série de Fourier :

$$\forall x \in \mathbb{R}, \qquad f(x) = \sum_{n\in\mathbb{Z}} c_n(f)e^{2i\pi nx}.$$

— On dit qu'une fonction f de $\mathbb{R}$ dans $\mathbb{C}$ est de la classe de Schwartz si elle est de classe $\mathscr{C}^\infty$ et si pour tous p, $k \in \mathbb{N}$, la fonction $x \mapsto x^p f^{(k)}(x)$ est bornée.

— Si f est une fonction de la classe de Schwartz, sa transformée de Fourier est la fonction $\widehat{f}$ donnée par

$$\forall \xi \in \mathbb{R}, \qquad \widehat{f}(\xi) = \int_{\mathbb{R}} f(x)e^{-2i\pi\xi x}\,\mathrm{d}x.$$

Pour la partie IV, on donne les notations suivantes.

— Le demi-plan de Poincaré, noté $\mathcal{H}$, est l'ensemble des nombres complexes de partie imaginaire strictement positive : $\mathcal{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$.

— On note $\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$.

Enfin pour la partie V, on rappelle qu'un réseau de $\mathbb{R}^d$ est un ensemble Γ de la forme $\mathbb{Z}u_1 + \mathbb{Z}u_2 + \cdots \mathbb{Z}u_d$, où $(u_1, \ldots, u_d)$ est une base de $\mathbb{R}^d$ considéré comme $\mathbb{R}$-espace vectoriel. On dit alors que $(u_1, \ldots, u_d)$ est une $\mathbb{Z}$-base de Γ.

I Un produit eulérien

Pour tout $n \in \mathbb{N}$ et tout $c \in \mathbb{R}$, soit

$$I_n(c) = \int_0^{\pi/2} (\cos t)^n \cos(ct)\,\mathrm{d}t.$$

1. Soit $c \in \mathbb{R}$. Calculer $I_0(c)$.

2. Montrer que pour tout entier n supérieur ou égal à 2 et tout réel c,

$$cI_n(c) = n \int_0^{\pi/2} (\cos(t))^{n-1} \sin(t) \sin(ct)\,\mathrm{d}t$$

et en déduire que $\left(n^2 - c^2\right) I_n(c) = \left(n^2 - n\right) I_{n-2}(c)$.

3. Montrer que pour tout $(k, x) \in \mathbb{N}^* \times \mathbb{R}$, $\qquad \left(1 - \dfrac{x^2}{k^2}\right) \dfrac{I_{2k}(2x)}{I_{2k}(0)} = \dfrac{I_{2k-2}(2x)}{I_{2k-2}(0)}$.

4. En déduire que pour tout entier n supérieur ou égal à 1 et tout réel $x \in \left]0, \dfrac{1}{2}\right[$,

$$\frac{\sin(\pi x)}{\pi x} = \left[\prod_{k=1}^{n} \left(1 - \frac{x^2}{k^2}\right)\right] \frac{I_{2n}(2x)}{I_{2n}(0)}.$$

5. Montrer que pour tout $(x, t) \in \left[0, \dfrac{1}{2}\right] \times \left[0, \dfrac{\pi}{2}\right]$, $\qquad \cos(2xt) \geqslant (\cos t)^2$.

6. Prouver que pour tout $(n, x) \in \mathbb{N}^* \times \left[0, \dfrac{1}{2}\right]$, $I_{2n}(0) \geqslant I_{2n}(2x) \geqslant I_{2n+2}(0)$ puis que

$$1 \geqslant \frac{I_{2n}(2x)}{I_{2n}(0)} \geqslant \frac{2n+1}{2n+2}.$$

7. En déduire que pour tout réel $x \in \left]0, \dfrac{1}{2}\right[$,

$$\ln \sin(\pi x) = \ln(\pi x) + \sum_{k=1}^{+\infty} \ln\left(1 - \frac{x^2}{k^2}\right).$$

8. Montrer que pour tout $z \in \left]0, \dfrac{1}{2}\right[$, $\quad \pi \dfrac{\cos(\pi z)}{\sin(\pi z)} = \dfrac{1}{z} + \displaystyle\sum_{n=1}^{+\infty} \left(\dfrac{1}{z-n} + \dfrac{1}{z+n}\right)$.

9. On pose pour tout $z \in \mathbb{C}$,

$$\cos(\pi z) = \frac{e^{i\pi z} + e^{-i\pi z}}{2} \text{ et } \sin(\pi z) = \frac{e^{i\pi z} - e^{-i\pi z}}{2i}.$$

Prouver que la fonction $z \mapsto \dfrac{\cos(\pi z)}{\sin(\pi z)}$ est définie et holomorphe sur $\mathbb{C} \setminus \mathbb{Z}$.

10. Montrer finalement que l'égalité de la question 8 est valable pour tout $z \in \mathbb{C} \setminus \mathbb{Z}$.

II Formule de Poisson

On admet que toute fonction f de classe $\mathscr{C}^\infty$ et 1-périodique est somme de sa série de Fourier :

$$\forall x \in \mathbb{R}, \qquad f(x) = \sum_{n\in\mathbb{Z}} c_n(f) e^{2i\pi n x},$$

où pour tout $n \in \mathbb{Z}, c_n(f) = \displaystyle\int_0^1 f(x) e^{-2i\pi n x}\,\mathrm{d}x$.
On rappelle qu'une fonction f de $\mathbb{R}$ dans $\mathbb{C}$ est de la classe de Schwartz lorsque qu'elle est de classe $\mathscr{C}^\infty$ et que pour tous $p, k \in \mathbb{N}$, la fonction $x \mapsto x^p f^{(k)}(x)$ est bornée.
On suppose que la fonction f de $\mathbb{R}$ dans $\mathbb{C}$ est de la classe de Schwartz. On note $\widehat{f}$ sa transformée de Fourier donnée par

$$\forall \xi \in \mathbb{R}, \qquad \widehat{f}(\xi) = \int_{\mathbb{R}} f(x) e^{-2i\pi\xi x}\,\mathrm{d}x.$$

11. Montrer que $\widehat{f}$ est une fonction de la classe de Schwartz.

On définit la fonction F par

$$\forall x \in \mathbb{R}, \qquad F(x) = \sum_{n\in\mathbb{Z}} f(x+n).$$

12. (a) Montrer que la fonction F est bien définie et de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$ et qu'elle est 1-périodique.

(b) Montrer que la série de Fourier de F est donnée par :

$$F(x) = \sum_{k\in\mathbb{Z}} \widehat{f}(k) e^{2i\pi k x}.$$

(c) En déduire

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{k\in\mathbb{Z}} \widehat{f}(k).$$

13. Soit $a > 0$ et soit $f_a : \mathbb{R} \to \mathbb{C}$ définie par

$$f_a(x) = e^{-a\pi x^2}.$$

(a) Montrer que la fonction f_a est de la classe de Schwartz.

(b) Montrer que, pour tout $\xi \in \mathbb{R}$, $\widehat{f_1}'(\xi) = -2\pi\xi \widehat{f_1}(\xi)$.

(c) On admet que $\displaystyle\int_{\mathbb{R}} f_1(x)\,\mathrm{d}x = 1$. Montrer que

$$\forall \xi \in \mathbb{R}, \qquad \widehat{f_1}(\xi) = e^{-\pi\xi^2}.$$

(d) En déduire, pour $a > 0$, l'expression explicite de la transformée de Fourier de f_a :

$$\forall \xi \in \mathbb{R}, \qquad \widehat{f_a}(\xi) = \frac{1}{\sqrt{a}} \exp\left(-\frac{\pi\xi^2}{a}\right).$$

14. Pour $a > 0$, montrer que pour tout $x \in \mathbb{R}$,

$$\sum_{n\in\mathbb{Z}} e^{-a\pi(x+n)^2} = \frac{1}{\sqrt{a}} \sum_{k\in\mathbb{Z}} e^{-\pi k^2/a}\, e^{2i\pi k x}$$

$$\sum_{n\in\mathbb{Z}} e^{-a\pi n^2} = \frac{1}{\sqrt{a}} \sum_{k\in\mathbb{Z}} e^{-\pi k^2/a}$$

III Une série d'Eisenstein

15. Montrer l'existence d'un réel $K > 0$ tel que pour tout $c \in \mathbb{N}^*$,

$$\sum_{d=1}^{+\infty} \frac{1}{\max(c^4, d^4)} \leqslant \frac{K}{c^3}.$$

16. Soit $z \in \mathcal{H}$. On note $x = \mathrm{Re}(z)$ et $y = \mathrm{Im}(z)$. Montrer que pour tout $(c, d) \in \mathbb{Z}^2$,

$$\begin{cases} \text{Si } c \neq 0, & \dfrac{1}{|cz+d|} \leqslant \dfrac{1}{|c|y}. \\ \text{Si } d \neq 0, & \dfrac{1}{|cz+d|} \leqslant \dfrac{\sqrt{x^2+y^2}}{|d|y}. \end{cases}$$

17. Soit $\mathcal{K}$ un compact inclus dans $\mathcal{H}$. Montrer qu'il existe un réel $M > 0$ tel que

$$\forall z \in \mathcal{K},\ \forall (c,d) \in \mathbb{Z}^2 \setminus \{(0,0)\}, \qquad \frac{1}{|cz+d|^4} \leqslant \frac{M}{\max\{c^4, d^4\}}.$$

18. En déduire que pour tout $z \in \mathcal{H}$, la famille $\left(\dfrac{1}{(cz+d)^4}\right)_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}}$ est sommable.

On note $G : z \in \mathcal{H} \mapsto \displaystyle\sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{1}{(cz+d)^4}$ sa somme.

19. Montrer que pour tout $z \in \mathcal{H}$, $\qquad G(z+1) = G(z)$ et $G\left(-\dfrac{1}{z}\right) = z^4 G(z)$.

20. Montrer que pour tout $z \in \mathcal{H}$, $\quad G(z) = 2\zeta(4) + 2\displaystyle\sum_{c=1}^{+\infty}\sum_{d\in\mathbb{Z}} \frac{1}{(cz+d)^4}$, où $\zeta(4) = \displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^4}$, puis montrer que G est holomorphe sur $\mathcal{H}$.

21. Pour tout $z \in \mathbb{C}$, on pose $q(z) = e^{2i\pi z}$.

(a) Montrer que, si $z \in \mathcal{H}$, alors $|q(z)| < 1$ et

$$i\pi - 2i\pi \sum_{d=0}^{+\infty} q(z)^d = \pi \frac{\cos(\pi z)}{\sin(\pi z)} = \frac{1}{z} + \sum_{n=1}^{+\infty} \left(\frac{1}{z-n} + \frac{1}{z+n}\right).$$

(b) En remarquant que $q'(z) = 2i\pi q(z)$, montrer que, pour tout $z \in \mathcal{H}$,

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^4} = \frac{8\pi^4}{3} \sum_{d=1}^{+\infty} d^3\, q(z)^d.$$

(c) Montrer finalement que pour tout $z \in \mathcal{H}$,

$$G(z) = \frac{\pi^4}{45}\Big(1 + 240 \sum_{n=1}^{+\infty} \sigma_3(n)\, q(z)^n\Big),$$

où, pour tout $n \in \mathbb{N}^*, \sigma_3(n) = \displaystyle\sum_{d|n} d^3$ est la somme des cubes des diviseurs positifs de n.

On pourra utiliser l'égalité de la question 20 et la relation $\zeta(4) = \dfrac{\pi^4}{90}$.

IV Les formes modulaires

Le demi-plan de Poincaré $\mathcal{H}$ et $\mathrm{SL}_2(\mathbb{Z})$ sont définis dans les rappels. On admet que $\mathrm{SL}_2(\mathbb{Z})$ est le sous-groupe de $(\mathrm{GL}_2(\mathbb{R}), \times)$ engendré par $\{S_0, T_0\}$ où $S_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $T_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Pour tout $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et tout $z \in \mathcal{H}$, on note

$$g \cdot z = \frac{az+b}{cz+d} \in \mathbb{C} \qquad \text{et} \qquad \rho(g) : z \in \mathcal{H} \mapsto g \cdot z \in \mathcal{H}.$$

22. (a) Soient $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et $z \in \mathcal{H}$. Montrer que $\mathrm{Im}(g \cdot z) = \dfrac{\mathrm{Im}(z)}{|cz+d|^2}$.

(b) Montrer que ρ définit une action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{H}$, c'est-à-dire que

— $\forall (g, z) \in \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H}, \qquad \rho(g)(z) \in \mathcal{H}$,

— $\rho(I_2) = \mathrm{Id}_{\mathcal{H}}$,

— $\forall g, g' \in \mathrm{SL}_2(\mathbb{Z}), \quad \rho(g \times g') = \rho(g) \circ \rho(g')$.

Déterminer de plus $\rho(S_0)$ et $\rho(T_0)$.

23. Soit $z \in \mathcal{H}$ et $\Omega_z = \{\rho(g)(z) \mid g \in \mathrm{SL}_2(\mathbb{Z})\}$ l'orbite de z sous l'action de $\mathrm{SL}_2(\mathbb{Z})$. On cherche ici à montrer qu'il existe un élément dans $\Omega_z \cap \mathscr{D}$ où

$$\mathscr{D} = \{z \in \mathcal{H} \mid |z| \geqslant 1, |\mathrm{Re}(z)| \leqslant 1/2\}.$$

On pourra dessiner $\mathscr{D}$ et constater que tous ses éléments ont une partie imaginaire supérieure ou égale à $\sqrt{3}/2$.

(a) Montrer que l'ensemble $\Big\{(c, d) \in \mathbb{Z}^2 \mid |cz+d| \leqslant 1\Big\}$ est non vide et de cardinal fini.

(b) En déduire que l'ensemble $\{\mathrm{Im}\,(z') \mid z' \in \Omega_z\}$ admet un maximum, que l'on notera $\mathrm{Im}\,(z_0)$, où $z_0 \in \Omega_z$. Montrer de plus que l'on peut supposer que $-1/2 \leqslant \mathrm{Re}\,(z_0) \leqslant 1/2$.

(c) Conclure en montrant que $|z_0| \geqslant 1$.

24. Soit $h : \mathcal{H} \to \mathbb{C}$ une fonction holomorphe, qui vérifie

$$\begin{cases} \forall (g, z) \in \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H}, & h(g \cdot z) = h(z), \\ \exists M > 0,\ \forall (x, y) \in \mathbb{R} \times [1, +\infty[, & |h(x+iy)| \leqslant M e^{-2\pi y}. \end{cases}$$

(a) Montrer que $|h|$ admet un maximum sur $\mathscr{D}$.

(b) En conclure que h est constante sur $\mathcal{H}$.

25. Soit $f : \mathcal{H} \to \mathbb{C}$ une fonction holomorphe vérifiant $\forall z \in \mathcal{H}, f(z+1) = f(z)$.

(a) Justifier l'égalité suivante pour tout $z = x + iy \in \mathcal{H}$,

$$f(z) = \sum_{n \in \mathbb{Z}} a_n(y) e^{2i\pi nz}, \text{ où } \forall n \in \mathbb{Z}, a_n(y) = \int_0^1 f(t+iy) e^{-2i\pi n(t+iy)}\,\mathrm{d}t.$$

(b) Montrer que pour tout $y > 0$ et tout $n \in \mathbb{Z}, a_n(y) = a_n(1)$.

On note désormais $a_n = a_n(1)$.

26. Pour toute fonction $f : \mathcal{H} \to \mathbb{C}$ holomorphe vérifiant $\forall z \in \mathcal{H}, f(z+1) = f(z)$, il existe donc une suite $(a_n)_{n\in\mathbb{Z}} \in \mathbb{C}^{\mathbb{Z}}$ telle que pour tout $z \in \mathcal{H}, f(z) = \sum_{n\in\mathbb{Z}} a_n e^{2i\pi nz}$.

f est dite holomorphe à l'infini lorsque pour tout $n \in \mathbb{N}^*, a_{-n} = 0$.
Lorsque de plus $a_0 = 0$, on dit que l'infini est un zéro de f d'ordre p, où $p = \min\{k \in \mathbb{N} \mid a_k \neq 0\}$.
On admet l'existence d'une fonction $\Delta : \mathcal{H} \to \mathbb{C}$ holomorphe et vérifiant :

— $\forall z \in \mathcal{H}, \qquad \Delta(z+1) = \Delta(z) \quad$ et $\quad \Delta\left(-\frac{1}{z}\right) = z^{12}\Delta(z)$,
— $\forall z \in \mathcal{H}, \qquad \Delta(z) \neq 0$,
— Δ admet un zéro d'ordre 1 en l'infini.

(a) Soit $\theta : \mathcal{H} \to \mathbb{C}$ une fonction holomorphe vérifiant

$$\forall z \in \mathcal{H}, \qquad \theta(z+1) = \theta(z) \quad \text{et} \quad \theta\left(-\frac{1}{z}\right) = z^4\theta(z),$$

et dont l'infini est un zéro.
Montrer que la fonction $h : z \in \mathcal{H} \mapsto \dfrac{\theta(z)^3}{\Delta(z)} \in \mathbb{C}$ est holomorphe, qu'elle vérifie

$$\forall (g, z) \in \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H}, h(g \cdot z) = h(z)$$

et qu'elle admet un zéro à l'infini d'ordre $p \geqslant 1$.

(b) En déduire que θ est la fonction nulle.

(c) Montrer enfin que l'espace des fonctions $\theta : \mathcal{H} \to \mathbb{C}$ holomorphes vérifiant

$$\forall z \in \mathcal{H}, \qquad \theta(z+1) = \theta(z) \text{ et } \theta\left(-\frac{1}{z}\right) = z^4\theta(z)$$

et qui sont de plus holomorphes à l'infini est l'ensemble des fonctions colinéaires à G.

V Conclusion

Soit $\Gamma = \{x \in \mathbb{Z}^8 \mid x_1 + \cdots + x_8 \equiv 0 \pmod 2\} \cup \{x \in (\mathbb{Z} + \frac{1}{2})^8 \mid x_1 + \cdots + x_8 \equiv 0 \pmod 2\}$.

On vérifie que Γ est un réseau de $\mathbb{R}^8$ et qu'il admet la $\mathbb{Z}$-base $(u_1, \ldots, u_8)$ donnée par

$$u_i = e_i - e_{i+1} \quad \text{pour } 1 \leqslant i \leqslant 7 \quad \text{et} \quad u_8 = \tfrac{1}{2}(e_1 + \ldots + e_8),$$

où $(e_1, \ldots, e_8)$ est la base canonique de $\mathbb{R}^8$.
On vérifie de plus que $\det(u_1, \ldots, u_8) = 1$ et que, pour tout $x \in \Gamma$, $\|x\|^2$ est un entier pair.
(Dans cette partie, $\|.\|$ désigne la norme euclidienne canonique sur $\mathbb{R}^8$.)

Dans ces conditions, on peut, en généralisant les méthodes de la partie II, démontrer que

$$\forall t \in \left]0, +\infty\right[, \qquad \sum_{k\in\Gamma} e^{-\pi t\|k\|^2} = t^{-4} \sum_{k\in\Gamma} e^{-\pi\|k\|^2/t}.$$

Pour tout $n \in \mathbb{N}$, on note $r(n)$ le nombre d'éléments x de Γ tels que $\|x\|^2 = 2n$.
Pour $z \in \mathcal{H}$, on pose $\theta(z) = \sum_{n\in\mathbb{N}} r(n)e^{2i\pi nz}$.

27. Montrer que la fonction θ est définie et holomorphe sur $\mathcal{H}$ et qu'elle vérifie les conditions de la question 26c.

28. En déduire que $r(n) = 240\sigma_3(n)$ pour tout $n \in \mathbb{N}^*$.