Examen

Problème 1

Soit $(\Omega, \Sigma, \mathbf{P})$ un espace probabilisé. Soit G un groupe abélien et $(N_i)_{i\in\mathbf{N}_{>0}}$ une famille de sous-groupes d'indice fini de G. Pour chaque i, on note n_i l'indice de N_i dans G et $\rho_i : G \to G/N_i$ la surjection canonique. Comme en cours, on note $\rho_{i,j} = \rho_i \times \rho_j$ et $\rho_{i,i} = \rho_i$ pour des indices distincts $i, j \in \mathbf{N}_{>0}$. On fixe une partie $S \subseteq G$ **génératrice** et symétrique (i.e. $s \in S$ si et seulement si $s^{-1} \in S$). Pour chaque $i \in \mathbf{N}_{>0}$ on note $S_i := \rho_i(S)$. On considère une marche aléatoire (X_k) sur G construite *via* S : les pas ξ_k, $k \geqslant 1$, sont des variables aléatoires indépendantes toutes de même loi donnée par

$$\forall k \geqslant 1,\, \forall s \in S,\, \mathbf{P}(\xi_k = s) = \mathbf{P}(\xi_k = s^{-1}) = p_s\,,$$

où $(p_s)_{s\in S}$ est une suite de réels de $]0,1]$ telle que $\sum_{s\in S} p_s = 1$. La marche aléataoire (X_k) est alors définie par

$$X_0 = 1\,, \qquad X_{k+1} = X_k\xi_{k+1}\,,\ k \geqslant 0\,.$$

On fait les hypothèses suivantes :

(H1) pour tout $i, j \in \mathbf{N}_{>0}$ on a $\rho_{i,j}(S) = S_i \times S_j$, si $i \neq j$.

(H2) pour tout $k \geqslant 1$, pour tout $i \in \mathbf{N}_{>0}$ et pour tout $t \in S_i$, on a

$$\mathbf{P}(\rho_i(\xi_k) = t) = \frac{1}{\#S_i}\,.$$

(H3) pour tout $k \geqslant 1$ pour tout couple (i, j) d'indices positifs distincts et pour tout $(t_i, t_j) \in G/N_i \times G/N_j$, les évènements "$\rho_i(\xi_k) = t_i$" et "$\rho_j(\xi_k) = t_j$" sont indépendants.

(H4) pour tout $i \in \mathbf{N}_{>0}$, notons $\mathcal{F}_i := \{f\colon G/N_i \to \mathbf{C}\}$, et $\mathcal{A}_i$ l'endomorphisme de $\mathcal{F}_i$ défini pour $f \in \mathcal{F}_i$ et $g \in G/N_i$ par $\mathcal{A}_i(f)(g) := (1/\#S_i)\sum_{t\in S_i} f(g \cdot t)$. On suppose qu'il existe $\gamma > 0$ tel que pour tout $i \in \mathbf{N}_{>0}$ les valeurs propres de $\mathcal{A}_i$ vérifient soit $\lambda = 1$ soit $|\lambda| < 1 - \gamma$.

1. Pour tout $i \in \mathbf{N}_{>0}$ donner une base de $\mathcal{F}_i$ formée de vecteurs propres de $\mathcal{A}_i$.

2. Fixons $k \geqslant 1$. Soit φ_i (resp. φ_j) une fonction de la base de $\mathcal{F}_i$ (resp. $\mathcal{F}_j$) explicitée à la question précédente. Établir une majoration de

$$|\mathbf{E}([\varphi_i, \overline{\varphi_j}]\rho_{i,j}(X_k))|\,,$$

analogue à celle obtenue en cours dans l'étude de marches aléatoires sur $SL(n, \mathbf{Z})$. (On reprend ici la notation du cours $[\phi, \psi]$ pour désigner le produit tensoriel des fonctions ϕ et ψ).

3. Montrer qu'il existe une constante $\eta > 0$ telle que si l'on fixe pour tout $i \in \mathbf{N}_{>0}$ un ensemble $\Omega_i \in G/N_i$ alors pour tout $k \geqslant 1$ et pour tout $L > 0$ fixé on a

$$\mathbf{P}\left(\rho_i(x_k) \notin \Omega_i,\, \forall i \in \{L, \dots, 2L\}\right) \leqslant \left(1 + L(\max_{L \leqslant i \leqslant 2L} n_i)\exp(-\eta k)\right)\left(\sum_{i=L}^{2L} \frac{\#\Omega_i}{n_i}\right)^{-1}$$

où l'on donnera explicitement une valeur possible de la constante η en fonction uniquement de γ.

Problème 2

Qu'obtient-on si l'on applique le crible probabiliste développé en cours pour $SL(n, \mathbf{Z})$, $n \geqslant 3$, pour montrer que la trace d'une matrice au hasard (au sens de la marche aléatoire redéfinie dans le problème 1) de $SL(n, \mathbf{Z})$ est, avec faible probabilité, somme de deux carrés d'entiers ? (En d'autres termes, on remplace la propriété étudiée en cours "$\det(T - g) \in \mathbf{Z}[T]$ est irréductible" par "$\mathrm{Tr}(g)$ n'est pas somme de deux carrés", où g désigne un élément "au hasard" de $SL(n, \mathbf{Z})$.)

Problème 3

Soit $g \geqslant 2$ un entier. On note W_{2g} le sous-groupe de $\mathfrak{S}_{2g}$ (vu comme groupe des permutations de $\{-g, \dots -1, 1, \dots g\}$) constitué des permutations agissant sur les paires $\{-i, i\}$, $1 \leqslant i \leqslant g$. Soit $P \in \mathbf{Q}[X]$ un polynôme de degré $2g$ dont on suppose que le groupe de Galois G du corps de décomposition (sur $\mathbf{Q}$) est isomorphe à W_{2g}. Notons $M = \{\alpha_{-g}, \dots, \alpha_{-1}, \alpha_1 \dots, \alpha_g\}$ l'ensemble des racines complexes de P. On suppose que l'on a $\alpha_{-i}\alpha_i = q_0$ pour tout $i \in \{1, \dots g\}$ et pour un entier $q_0 \in \mathbf{N}_{>0}$ indépendant de i. On peut voir G comme un groupe de permutations de M.

1. Montrer que G agit transitivement sur M et justifier que les racines de P sont deux à deux distinctes.

2. On considère l'action diagonale de G sur $M \times M$. Montrer qu'il y a trois orbites pour cette action :

$$\Delta = \{(\alpha_i, \alpha_i) \colon i \in \{-g, \dots, -1, 1, \dots g\}\},\ \Delta_c = \{(\alpha_i, \alpha_{-i}) \colon i \in \{-g, \dots, -1, 1, \dots, g\}\}$$
$$O = \{(\alpha_i, \alpha_j) \colon i \neq j, i \neq -j\}.$$

3. On note $F(M)$ le $\mathbf{Q}$-espace vectoriel de base les symboles f_α, $\alpha \in M$. L'action par permutation de G sur M fait de $F(M)$ une $\mathbf{Q}$-représentation de G. En utilisant le fait que le caractère de cette représentation est à valeurs réelles, montrer que $F(M)$ se décompose en la somme directe de trois représentations irréductibles :

$$\mathbf{1} := \Big\{\lambda\big(\sum_{\alpha \in M} f_\alpha\big) \mid \lambda \in \mathbf{Q}\Big\},$$
$$G(M) := \Big\{\sum_{i \in \{-g, \dots g\} \setminus \{0\}} \lambda_{\alpha_i} f_{\alpha_i} \mid \lambda_{\alpha_i} - \lambda_{\alpha_{-i}} = 0 \text{ pour } 1 \leqslant i \leqslant g \text{ et } \sum_{i \in \{-g, \dots g\} \setminus \{0\}} \lambda_{\alpha_i} = 0\Big\},$$
$$H(M) := \Big\{\sum_{i \in \{-g, \dots g\} \setminus \{0\}} \lambda_{\alpha_i} f_{\alpha_i} \mid \lambda_{\alpha_i} + \lambda_{\alpha_{-i}} = 0 \text{ pour } 1 \leqslant i \leqslant g\Big\}.$$

4. On note $\langle M \rangle$ le $\mathbf{Z}$-module multiplicatif engendré par M (i.e. l'ensemble des produits $\prod_\alpha \alpha^{n_\alpha}$ indexés par M, où les n_α sont des entiers). On considère l'application $\mathbf{Q}$-linéaire

$$\Phi \colon F(M) \to \langle M \rangle \otimes \mathbf{Q}, \qquad f_\alpha \mapsto \alpha.$$

Justifier que $\ker \Phi$ peut être vu comme une représentation $\mathbf{Q}$-linéaire de G.

5. Montrer que $G(M) \subseteq \ker \Phi$.

6. Montrer que $\mathbf{1} \subseteq \ker \Phi$ si et seulement si $q_0 = 1$. Déduire la décomposition de $\ker \Phi$ en somme directe de représentations irréductibles.

7. Soit $f \in \mathbf{Z}[X]$ un polynôme de degré $2g$ sans facteur carré et soit p un premier ne divisant pas le discriminant de f. On fixe une puissance *paire* q de p et pour tout $t \in \mathbf{F}_q$ tel que $f(t) \neq 0$ on considère le modèle projectif lisse C_t de la courbe affine donnée par

$$y^2 = f(x)(x-t)\,.$$

On note $P_t \in \mathbf{Z}[T]$ le numérateur de la fonction zêta de $C_t/\mathbf{F}_q$.

(a) Montrer, à partir du travail fait en cours, l'existence d'une constante γ ne dépendant que de g (et qu'on donnera explicitement) telle que l'on ait l'estimation non triviale

$$|\{t \in \mathbf{F}_q \colon f(t) \neq 0 \text{ et la somme des inverses des racines de } P_t \text{ est nulle}\}| \ll q^{1-\gamma^{-1}} \log q\,,$$

où la constante implicite ne dépend que de g.

(b) Fixons $t \in \mathbf{F}_q$ satisfaisant $f(t) \neq 0$. Soit M_t l'ensemble des inverses des zéros de P_t. On appelle *relation multiplicative* dans M_t toute relation du type

$$\prod_{\alpha \in M_t} (\alpha/\sqrt{q})^{n_\alpha} = 1$$

où $n_\alpha \in \mathbf{Z}$. Donner une borne supérieure du type apparaissant dans la question précédente pour le nombre de $t \in \mathbf{F}_q$ tels que $f(t) \neq 0$ et tel que M_t présente une relation multiplicative ne provenant pas de l'équation fonctionnelle :

$$q^g T^{2g} P_t(1/qT) = P_t(T)\,.$$

Problème 4

Soit A un anneau vérifiant $\mathbf{Z} \subseteq A \subseteq \mathbf{Q}$ et $n \geqslant 3$ un entier. On fixe un élément $d \in A^\times$ (i.e. d est un inversible de A) et l'on considère

$$Y_d := \{M \in GL(n, A) \colon \det(M) = d\}\,.$$

Expliquez comment adapter le crible probabiliste pour $SL(n, \mathbf{Z})$ étudié en cours à l'étude de l'irréductibilité sur $\mathbf{Q}$ du polynôme caractéristique d'une matrice aléatoire de Y_d. On ne demande pas de donner les détails de l'adaptation, mais de dégager clairement une stratégie de preuve en mettant l'accent sur les différences avec le cas traité en cours, et en expliquant quels résultats supplémentaires (ou quelles hypothèses sur A) sont nécessaires.