UNIVERSITÉ PARIS SUD
FACULTÉ DES SCIENCES D'ORSAY

MATHEMATIQUES ORSAY

UNIVERSITÉ PARIS-SUD

Faculté des sciences d'Orsay

École doctorale de mathématiques Hadamard (ED 574)

Laboratoire de mathématique d'Orsay (UMR 8628 CNRS)

Mémoire présenté pour l'obtention du

Diplôme d'habilitation à diriger les recherches

Discipline : Mathématiques

par

Florent Jouve

Étude de propriétés génériques dans des familles de graphes, de groupes arithmétiques, et de courbes elliptiques.

Rapporteurs :
ÉTIENNE FOUVRY
PHILIPPE MICHEL
ZEEV RUDNICK

Date de soutenance : 10 décembre 2015

Composition du jury :
JEAN-BENOÎT BOST
RÉGIS DE LA BRETÈCHE
EMMANUEL BREUILLARD
ÉTIENNE FOUVRY
EMMANUEL KOWALSKI
EMMANUEL PEYRE

Remerciements

Je remercie Frédéric Paulin pour ses conseils avisés sur le déroulement du processus allant de l'écriture du mémoire d'habilitation jusqu'à la soutenance. Je remercie également Valérie Lavigne et Martine Thouvenot pour leur aide précieuse à diverses étapes de ce processus.

Étienne Fouvry, Philippe Michel, et Zeev Rudnick ont accepté d'écrire un rapport sur mon dossier d'habilitation. Ils ont toute ma reconnaissance pour avoir consenti à s'acquitter de cette tâche. Je remercie les membres du jury Jean-Benoît Bost, Régis de la Bretèche, Emmanuel Breuillard, Étienne Fouvry, Emmanuel Kowalski et Emmanuel Peyre pour l'intérêt qu'ils ont manifesté à l'égard des travaux dont ce mémoire fait état et pour leur participation active à la soutenance.

Les articles présentés dans le texte qui suit ont été écrits en commun avec d'autres mathématiciens. L'échange des idées, l'élaboration des résultats au fur et à mesure des discussions, aspects d'importance bien connue dans le travail d'un chercheur, furent particulièrement cruciaux dans l'évolution de mes centres d'intérêts, dans ma conception de ce qu'est l'activité mathématique et dans la lente prise de recul sur les objets d'étude qui m'occupent quotidiennement. À tous ces titres, je remercie vivement mes coauteurs : Byungchul Cha, Daniel Fiorilli, Étienne Fouvry, Emmanuel Kowalski, Fernando Rodriguez Villegas, Jean-Sébastien Sereni et David Zywina. Depuis la fin de ma thèse j'ai bénéficié, parfois en tant qu'orateur et souvent en tant qu'auditeur, de l'atmosphère détendue et stimulante des « Rencontres de théorie analytique des nombres » qui se tiennent régulièrement à l'IHP. Pour l'impact bénéfique indéniable de cette manifestation sur les jeunes chercheurs et pour tout le profit que jai pu personnellement tiré de ces rencontres, je remercie Régis de la Bretèche.

Je voudrais également témoigner ma reconnaissance aux nombreux étudiants côtoyés à Orsay depuis mon arrivée en 2009 et qui, insensibles aux arguments approximatifs, m'ont poussé à mieux comprendre (je devrais dire, à réellement comprendre) de nombreux énoncés ou raisonnements que j'avais jusqu'alors la conviction de parfaitement maîtriser.

Je dois enfin des remerciements particuliers à trois personnes. À Olivier Fouquet d'abord, qui est responsable d'au moins 50% de l'excellente ambiance qui règne dans le bureau que nous partageons depuis notre arrivée simultanée à Orsay. À Emmanuel Kowalski ensuite, qui, malgré le nombre croissant d'années écoulées depuis ma thèse (on pourra s'affranchir du décompte exact), continue à répondre patiemment à mes questions. À Étienne Fouvry enfin ; ses constants encouragements, ses intuitions mathématiques redoutables et ses non moins redoutables traits d'humour ont grandement participé à l'avancement de mon travail et au plaisir que j'éprouve à aller travailler au bâtiment 425 du campus d'Orsay.

Liste des travaux

- *Prime number races for elliptic curves over function fields*, prépublication, avec B. Cha, et D. Fiorilli.
- *Independence of the zeros of elliptic curve L-functions over function fields*, prépublication, avec B. Cha et D. Fiorilli.
- *Sieving in graphs and explicit bounds for non-typical elements*, prépublication, avec J-S. Sereni.
- *On the bilinear structure associated to bezoutians*, avec F. Rodriguez Villegas, J. Algebra 400 (2014), 161–184.
- *A positive density of fundamental discriminants with large regulator*, avec É. Fouvry, Pacific J. Math. 262 (2013), no 1, 81–107.
- *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, avec E. Kowalski et D. Zywina, Israel J. Math. 193 (2013), no. 1, 263–307.
- *Size of regulators and consecutive square-free numbers*, avec É. Fouvry, Math. Z. 273 (2013), no. 3-4, 869–882.
- *Fundamental solutions to Pell equation with prescribed size*, avec É. Fouvry, Proc. of the Steklov Institute of Math., (2012), Vol. 276, no. 1, pp 40–50
- *The large sieve and random walks on left cosets of arithmetic groups*, Comment. Math. Helv. 85 (2010), 647–704.
- *Maximal Galois group of L-functions of elliptic curves*, Int. Math. Res. Not. (2009), no 19, 3557–3594.
- *An explicit integral polynomial whose splitting field has Galois group $W(E_8)$*, avec E. Kowalski et D. Zywina, J. Théor. Nombres Bordeaux, 20 (2008), no 3, 761–782.
- *The geometry of the third moment of exponential sums* J. Théor. Nombres Bordeaux, 20 (2008), no 3, 733–760.

Table des matières

Introduction

Ce mémoire a pour objectif de présenter les travaux [1]–[6]. Une motivation commune pour les résultats que ces articles contiennent est d'essayer de démontrer un énoncé *quantitatif*, ou comportant des aspects *effectifs*, confirmant l'intuition suivant laquelle une propriété que l'on pense typique testée sur des objets de nature arithmétique, algébrique, ou combinatoire, est effectivement satisfaite fréquemment.

Les questions de ce type ne manquent pas. Citons quelques exemples bien connus provenant de l'arithmétique : si l'on prend un entier naturel au hasard, quelle est la probabilité qu'il soit premier ? Sans facteur carré ? Somme de deux carrés ? Somme de quatre carrés ? Si l'on prend un polynôme unitaire de degré fixé et à coefficients entiers au hasard, est-il typiquement irréductible ? Quel est le groupe de Galois typique de son corps de décomposition sur $\mathbf{Q}$? Ou, pour citer un exemple tout à fait d'actualité : si l'on prend une courbe elliptique sur $\mathbf{Q}$ au hasard, quel doit être, typiquement, son rang ?

Dans le chapitre 2, on s'intéresse au comportement galoisien typique du polynôme caractéristique d'un élément au hasard d'un groupe arithmétique. On y explique aussi que l'on peut répondre de manière effective au problème de Galois inverse pour le groupe de Weyl $W(\mathbf{E}_8)$ sur $\mathbf{Q}$. Dans le chapitre 4 on se demande si un graphe aléatoire contient génériquement une sous-structure fixée, ou si une coloration aléatoire d'un tel graphe admet en général une sous-structure monochromatique prescrite. Dans le chapitre 5, on adapte aux courbes elliptiques sur les corps de fonctions la question, posée par Chebyshev, de savoir si les tranches initiales d'entiers contiennent plus de nombres premiers congrus à 3 modulo 4 qu'à 1 modulo 4. On explique que cette question est étroitement liée à une propriété d'indépendance linéaire de zéros de fonctions L, et l'on présente un résultat quantitatif montrant que cette propriété est générique dans certaines familles de courbes elliptiques bien choisies.

Dans tous ces travaux se pose la question de savoir comment produire un élément sur lequel tester une propriété que l'on pense être fréquemment satisfaite. On doit à chaque fois préciser ce que l'on entend par élément « au hasard ». Dans le cas d'une structure finie, on retrouve l'idée d'un résultat *en moyenne*. Dans les chapitres 2 et 4, on a en revanche à faire à des ensembles infinis, et on adopte alors le point de vue des marches aléatoires pour produire des éléments au hasard. Comment produire alors *une estimation* pour le nombre (ou la probabilité d'apparition) des éléments rares ? C'est le crible qui nous permet de répondre à cette question. *Via* le recours à des résultats profonds (suivant le contexte : l'hypothèse de Riemann sur les corps finis, ou la propriété (T) de Kazhdan, dans sa version affaiblie due à Lubotzky), la « version locale » de la propriété testée, qui donne lieu à des calculs de

densité dans des structures finies, peut être « remontée » quantitativement en une propriété des objets globaux initiaux.

Outre le recours nécessaire aux résultats profonds mentionnés ci-dessus, de sérieuses difficultés dans le calcul de densités locales apparaissent et ouvrent parfois le champ à des questionnements indépendants. Ainsi, le chapitre 3 traite de constructions explicites d'espaces bilinéaires permettant la résolution de questions propres aux aspects locaux du crible apparaissant notamment dans le chapitre 5. Ces espaces bilinéaires, qui trouvent leur origine dans des travaux de Bézout, ont leur intérêt propre et présentent notamment des liens remarquables avec les groupes hypergéométriques de Beukers et Heckman.

Les divers cadres d'étude que l'on présente font intervenir des méthodes trés variées. Les questions posées et l'approche générale relèvent de la théorie analytique des nombres, mais figurent aussi en bonne place les conjectures de Weil, l'analyse harmonique sur les groupes arithmétiques, les propriétés des familles de graphes expanseurs, les méthodes de transfert de formes bilinéaires non dégénérées, et quelques propriétés élémentaires des chaînes de Markov. Nous espérons que transparaît dans les pages qui suivent, toute la joie que nous avons eue à travailler avec un tel mélange de belles théories mathématiques.

Chapitre 1

Le grand crible non-abélien

Les méthodes de crible apparaissent en théorie des nombres au début du vingtième siècle sous l'impulsion de V. Brun et de son crible combinatoire mis au point pour étudier les nombres premiers jumeaux. Des variantes de l'approche originale de Brun se sont ensuite développées. La version du crible qui est au coeur de ce mémoire trouve sa source dans les travaux de Linnik (datant des années 1940) sur la taille du plus petit non-résidu quadratique modulo p (en fonction du nombre premier p). La variante de Linnik est maintenant connue sous le nom de *grand crible* du fait que, pour chaque premier p utilisé pour cribler, c'est une proportion constante de classes modulo p que l'on décide de ne pas garder (on comprend facilement, dans le cas de l'étude du plus petit non-résidu quadratique modulo p, que cette proportion est moralement $1/2$).

Le grand crible a connu de nombreuses évolutions et raffinements dans la seconde moitié du vingtième siècle (grâce notamment à Montgomery [M], Brüdern–Fouvry [BF], Fouvry–Michel [FM],...), mais jusqu'au début des années 2000 un point commun essentiel à ses diverses formes est son caractère *abélien*. Précisément les applications permettant de passer de la question "globale" posée à sa variante "locale" (plus propice à une approche combinatoire) sont du type $A \to A_p$, où A peut être l'anneau $\mathbf{Z}$, l'anneau d'entiers $\mathbf{Z}_K$ d'un corps de nombres K, ou, plus généralement encore, un produit cartésien de tels anneaux, et A_p est l'anneau $\mathbf{Z}/p\mathbf{Z}$, ou le corps résiduel en un idéal premier p de $\mathbf{Z}_K$, ou un produit cartésien de tels objets.

L'approche axiomatique de Kowalski, initiée dans [K3] et poursuivie dans un très vaste degré de généralité dans [K4], marque une rupture dans le sens où elle présente le grand crible comme un *principe*, a priori détaché de ses potentielles applications arithmétiques (mais que l'on peut rapprocher par certains aspects de [M]). En particulier, l'axiomatisation (ainsi que de nombreuses applications obtenues depuis) de ce principe fait apparaître pour la première fois des objets *non-abéliens*, i.e. les applications de « réduction » utilisées sont de simples applications ensemblistes surjectives $Y \to Y_p$, où aucune structure n'est a priori nécessaire sur Y, ou Y_p (et où l'on n'exige pas non plus que l'ensemble de ces applications soit indexé par un sous-ensemble de nombres premiers).

1.1 L'axiomatique du grand crible

Rappelons plus en détail le cadre d'étude de [K4]. On appelle *cadre de crible*, un triplet $(Y, \Lambda, (\rho_\ell \colon Y \to Y_\ell))$, où Y est un ensemble quelconque, Λ est un ensemble indexant les applications surjectives ρ_ℓ, et où l'on suppose que les Y_ℓ sont des ensembles finis. On appelle *ensemble à cribler* associé à $(Y, \Lambda, (\rho_\ell \colon Y \to Y_\ell))$, un triplet (X, μ, F), où (X, μ) est un espace mesuré et $F \colon X \to Y$ est une application rendant les applications composées $\rho_\ell \circ F \colon X \to Y_\ell$ mesurables (i.e. les ensembles $\{x \in X \colon \rho_\ell(F(x)) = y\}$ sont mesurables pour tout $\ell \in \Lambda$ et tout $y \in Y_\ell$). Enfin on suppose donné un sous-ensemble *fini* $\mathcal{L}^* \subseteq \Lambda$ appelé *support premier de crible* et une famille $\Theta = (\Theta_\ell)$, indexée par Λ, où pour chaque ℓ on a $\Theta_\ell \subseteq Y_\ell$. Les ensembles dont on espère pouvoir estimer (ou tout du moins, majorer) la mesure, sont les *ensembles criblés* :

$$S(X, \Theta, \mathcal{L}^*) := \{x \in X \colon \rho_\ell(F(x)) \notin \Theta_\ell,\ \forall \ell \in \mathcal{L}^*\}\,. \tag{1.1.1}$$

On a en tête le cas classique où le cadre de crible est $(\mathbf{Z}, \{ \text{ nombres premiers } \}, \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z})$, et l'ensemble à cribler associé est de la forme

$$(\{n \in \mathbf{Z} \colon M < n \leqslant M + N\},\ \text{mesure de comptage}\ ,\ \text{identité}\ )$$

L'ensemble criblé obtenu prend la forme traditionnelle

$$\{n \in \mathbf{Z} \colon M < n \leqslant M + N,\ n \,(\mathrm{mod}\, p) \notin \Theta_p,\ \forall p \in \mathcal{L}^*\}\,,$$

où $\mathcal{L}^*$ est un ensemble de nombres premiers, et où Θ_p est un ensemble de classes modulo p pour tout p. Il est aisé d'étendre ce cas classique en dimension supérieure. Les ensembles criblés obtenus sont alors de la forme :

$$\{(n_1, \dots, n_r) \in \mathbf{Z}^r \colon M_i < n_i \leqslant M_i + N_i,\ (n_1 \,(\mathrm{mod}\, p), \dots, n_1 \,(\mathrm{mod}\, p)) \notin \Theta_p,\ \forall p \in \mathcal{L}^*\}\,,$$

où l'on a fixé des entiers $M_i \in \mathbf{Z}$ et $N_i \in \mathbf{N}_{>0}$, des ensembles $\Theta_p \in (\mathbf{Z}/p\mathbf{Z})^r$, et où le cadre de crible et l'ensemble à cribler associé sont les généralisations évidentes de ceux donnés ci-dessus. Déjà ce cadre multidimensionnel classique permet, *via* la présentation axiomatique du grand crible donnée par Kowalski, de redémontrer simplement (cf [K4, Th. 4.2]) le théorème de Gallagher.

Théorème 1.1.1 (Gallagher, 1973)**.** *Soit $r \geqslant 1$ un entier. Pour tout $N \in \mathbf{N}_{\geqslant 1}$, soit $E_r(N)$ l'ensemble des polynômes $T^r + a_{r-1}T^{r-1} + \cdots + a_1 T + a_0$ de $\mathbf{Z}[T]$ tels que $|a_i| \leqslant N$ pour tout i, et dont le groupe de Galois du corps de décomposition sur $\mathbf{Q}$ est d'ordre $< r!$. Alors*

$$|E_r(N)| \ll r^3 (2N+1)^{r-1/2} \log N\,,$$

pour $N \geqslant 2$, et avec une constante implicite absolue.

Ce théorème a longtemps constitué la meilleure majoration connue pour $|E_r(N)|$ (pour des améliorations récentes [1], voir [Z, Prop. 1.5] où Zywina parvient à faire disparaître le facteur log, et [D2], où l'exposant $r-1/2$ est amélioré en $r-(2-\sqrt{2}-\varepsilon)$), peut être vu à la fois comme un point de départ, et comme une incarnation simple de l'intuition qui sous-tend les travaux [3] et [4] que le présent mémoire a pour objet de présenter. L'idée est ici qu'un polynôme « pris au hasard », à coefficients rationnels est irréductible avec grande probabilité, ou, mieux encore, en notant r le degré du polynôme, son corps de décomposition sur $\mathbf{Q}$ doit avoir un groupe de Galois isomorphe à $\mathfrak{S}_r$, avec grande probabilité. Parmi les cadres naturels où des familles de polynômes à coefficients rationnels (ou plus généralement, à coefficients dans un corps de nombres) apparaissent, mentionnons les polynômes caractéristiques de matrices à coefficients rationnels, ou les polynômes caractéristiques de Frobenius géométriques agissant sur la cohomologie ℓ-adique d'une variété. Ces deux familles correspondent à deux des exemples les plus importants traités dans [2], [3] et [4].

Toutes les estimations non triviales que ces travaux contiennent ont pour point de départ commun une majoration a priori de la mesure de (1.1.1). On appelle cette majoration théorique *inégalité de grand crible* (cf [K4, Prop.2.3]). La puissance de la méthode y transparaît *via* un phénomène de séparation de variables. Dans les notations ci-dessus, cette inégalité peut s'écrire sous la forme succinte :

$$\mu(S(X,\Theta,\mathcal{L}^*)) \leqslant \Delta H^{-1}\,, \tag{1.1.2}$$

où Δ est une constante (appelée *constante de grand crible*) indépendante de la famille Θ, et H est une constante indépendante de X. L'aspect « principe local-global » de la méthode ici décrite s'incarne par le fait que H est de nature combinatoire et rassemble les informations locales (i.e. modulo chaque $\ell \in \mathcal{L}^*$), alors que Δ est de nature « harmonique » et mesure la possibilité d'induire une information globale quantitative à partir de son analogue local.

Pour définir H et Δ, il faut d'abord fixer une mesure de densité ν_ℓ sur Y_ℓ, pour tout $\ell \in \Lambda$. On considère ensuite l'espace $L^2(Y_\ell,\nu_\ell)$ des fonctions sur Y_ℓ à valeurs complexes muni du produit scalaire :

$$\langle f,g\rangle = \sum_{x\in Y_\ell} f(x)\overline{g(x)}\nu_\ell(x)\,,$$

relativement auquel on fixe une base orthonormée $\mathcal{B}_\ell$ (contenant la fonction constante égale à 1) de cet espace. Avec ces notations, la définition de H est la suivante :

$$H := \sum_{\ell\in\mathcal{L}^*} \frac{\nu_\ell(\Theta_\ell)}{\nu_\ell(Y_\ell\setminus\Theta_\ell)}\,.$$

En pratique, une situation agréable dans laquelle appliquer ce formalisme de crible est celle où $Y=G$ est un groupe et les applications surjectives $Y\to Y_\ell$ sont des morphismes surjectifs vers des groupes finis $G_\ell := Y_\ell$ (cf [K5, Chap. 3]). En raffinant un peu plus le choix de Y_ℓ (il est commode de remplacer G_ℓ par l'ensemble de ses classes de conjugaison $G_\ell^\sharp$), on voit

1. Très récemment, Rivin annonce dans [R3] avoir obtenu une borne supérieure du type $\ll_r N^{r-1}\log^{f(r)} N$, où f est une fonction à croissance polynomiale en r explicitement calculable.

immédiatement un choix naturel pour les densités ν_ℓ et les bases orthonormées $\mathcal{B}_\ell$. En effet, si ν_ℓ est la densité naturelle associant $\#C/\#G_\ell$ à une classe de conjugaison quelconque C de G_ℓ, alors on peut prendre pour $\mathcal{B}_\ell$ les caractères d'un système de représentants (contenant la représentation triviale) pour les classes d'isomorphisme de représentations irréductibles de G_ℓ. Pour tout choix d'ensemble $\Theta_\ell \subseteq G_\ell$ invariant par conjugaison, on a alors la minoration

$$H \geqslant \sum_{\ell \in \mathcal{L}^*} \frac{\#\Theta_\ell}{\#G_\ell}\,. \tag{1.1.3}$$

La terminologie *grand* crible sous-entend que les ensembles Θ_ℓ sont en proportion essentiellement constante (lorsque ℓ varie) dans G_ℓ. En d'autres termes, on espère en pratique pouvoir montrer

$$H \gg |\mathcal{L}^*|\,. \tag{1.1.4}$$

Dans [6], on choisit pour Y_ℓ l'ensemble des éléments d'un groupe abélien fini, ce qui constitue un cas trivial de crible de conjugaison. Dans [4] et [2] l'ensemble Y_ℓ est l'ensemble des classes de conjugaison d'une certaine classe à gauche αG_ℓ^g relativement à un sous groupe $G_\ell^g \trianglelefteq G_\ell$ tel que le quotient G_ℓ/G_ℓ^g est abélien.

Il est plus délicat de définir précisément ce qu'est la constante Δ. Nous renvoyons à [K5, Prop. 2.3] où Δ est définie comme étant la norme d'une certaine application linéaire. Par dualité, on peut aussi voir Δ comme la norme d'une application bilinéaire ([K5, Lem. 2.8]). Ce second point de vue est commode pour obtenir une majoration a priori de Δ faisant intervenir certaines généralisations de sommes exponentielles. D'après [K5, Prop. 2.9], on a :

$$\Delta \leqslant \max_{\ell \in \mathcal{L}^*} \max_{\varphi \in \mathcal{B}_\ell \setminus \{1\}} \sum_{\ell' \in \mathcal{L}^*} \sum_{\varphi' \in \mathcal{B}_{\ell'} \setminus \{1\}} |W(\varphi, \varphi')|\,,$$

où

$$W(\varphi, \varphi') = \int_X \varphi \circ \rho_\ell(F_x)\overline{\varphi' \circ \rho_{\ell'}(F_x)}\,\mathrm{d}\mu(x)\,. \tag{1.1.5}$$

En pratique, la partie la plus délicate dans l'application du grand crible est la majoration des « sommes » individuelles $W(\varphi, \varphi')$. Pour être non triviales, ces majorations requièrent l'utilisation de propriétés remarquables des cadres de crible $(Y, \Lambda, Y \to Y_\ell)$. Dans [4], cette propriété est la propriété (τ) de Lubotzky, utilisée dans la généralité démontrée par Clozel dans [C5]. Dans [2], c'est l'hypothèse de Riemann sur les corps finis de Deligne qui intervient.

Notons que la propriété (τ) de Lubotzky a fait l'objet de nombreux travaux récents dans le cadre de l'étude du phénomène d'expansion dans les groupes linéaires (phénomène qui a également été baptisé « approximation super-forte »). Ces travaux profonds, cités sans être directement utilisés dans [4], constituent l'un des ingrédients qui a permis à Lubotzky et Rosenzweig de généraliser, dans [LR], les énoncés de [4].

Dans tous les cas mentionnés ci-dessus, c'est une propriété d'*écart spectral* qui permet la majoration efficace (c'est-à-dire, avec une uniformité suffisante en les divers paramètres intervenants) des sommes $W(\varphi, \varphi')$. Partant de ce constat, une idée séduisante est d'essayer de s'abstraire autant que possible des cadres algébriques de [2] ou [4] pour travailler dans

une situation où seule demeure la propriété d'écart spectral uniforme requise. C'est là un des points de départ de l'article [6] où l'on développe un grand crible pour les graphes. Dans ce cadre c'est le principe selon lequel les graphes au hasard font de bons graphes expanseurs qui permet la majoration des quantités $W(\varphi, \varphi')$.

1.2 Le cas du crible de conjugaison

Fixons un cadre de crible $(Y, \Lambda, (Y \to Y_\ell))$ et un ensemble à cribler associé (X, μ, F). Comme on l'a déjà mentionné, il est commode de travailler dans le cas où $Y = G$ est un groupe et où, pour chaque $\ell \in \Lambda$, l'ensemble $Y_\ell =: G_\ell^\sharp$ est l'ensemble des classes de conjugaison d'un groupe fini image d'un homomorphisme $G \to G_\ell$. Les applications ρ_ℓ sont alors les composées

$$G \to G_\ell \to G_\ell^\sharp,$$

où la seconde flèche associe à chaque $x \in G_\ell$ sa classe de conjugaison. Dans ce cas, la théorie des caractères des groupes finis fournit un choix naturel pour la base orthonormée $\mathcal{B}_\ell$ intervenant dans la définiton et l'estimation des constantes Δ et H de (1.1.2). Ce cadre particulier de crible est appelé *crible de conjugaison* dans [K5, Chap. 3] ; c'est celui que l'on applique dans les articles [2], [4], et [6]. Dans [6], la situation est plus simple encore puisque le groupe G est abélien. Les bases $\mathcal{B}_\ell$ sont donc constituées de caractères de degré 1 et l'expression (1.1.5) pour $W(\varphi, \varphi')$ en est alors grandement simplifiée. Dans [2] en revanche, le cadre de crible est un peu plus général : les ensembles Y_ℓ sont encore des réunions de classes de conjugaison de groupes finis G_ℓ, mais on se contente de demander que Y_ℓ soit l'ensemble des classes de conjugaison d'une classe à gauche de G_ℓ relativement à un sous-groupe distingué fixé G_ℓ^g contenant le sous-groupe dérivé de G_ℓ. C'est le *crible pour les classes à gauche* initié dans [K3], dont l'axiomatique est décrite dans [K5, Chap. 3], et dont divers raffinements font l'objet de [J2].

A défaut de disposer d'un cadre de crible de conjugaison pour un groupe ayant de bonnes propriétés, on combine, dans [4], un crible de conjugaison pour les classes à gauche et les propriétés générales des chaînes de Markov. On reviendra sur ce point dans les sections du présent mémoire consacrées à l'article [4].

On conclut ce chapitre par la description d'un grand crible visant à étudier les propriétés typiques d'un « objet » arithmétique « aléatoire ». Ce cadre d'étude est exposé en détails dans [K4, chap. 6 et 7] et est utilisé dans [J2]. Comme on l'a sous-entendu plus haut, c'est aussi cette approche probabiliste qui est adoptée dans [4] et [6].

1.3 Grand crible probabiliste

On fixe un cadre de crible $(Y, \Lambda, (Y \to Y_\ell))$ et un espace probabilisé $(\Omega, \Sigma, \boldsymbol{P})$. La donnée d'une variable aléatoire fixée $X \colon \Omega \to Y$ permet de voir $(\Omega, \boldsymbol{P}, X)$ comme un ensemble à cribler associé à $(Y, \Lambda, (Y \to Y_\ell))$. Si $\mathcal{L}^*$ est un support premier de crible et si, pour chaque

$\ell \in \Lambda$, on fixe $\Theta_\ell \subseteq Y_\ell$, alors la mesure de l'ensemble $S(\Omega, (\Theta_\ell)_{\ell\in\Lambda}, \mathcal{L}^*)$, défini par (1.1.1), est

$$\boldsymbol{P}(\rho_\ell(X) \notin \Theta_\ell,\, \forall \ell \in \mathcal{L}^*)\,,$$

en adoptant les notations probabilistes standard où l'argument $\omega \in \Omega$ est omis. Le langage probabiliste permet aussi de récrire chaque somme $W(\varphi, \varphi')$ (donnée par (1.1.5)) comme l'espérance d'une variable aléatoire :

$$W(\varphi, \varphi') = \boldsymbol{E}\left(\varphi \circ \rho_\ell(X)\overline{\varphi' \circ \rho_{\ell'}(X)}\right)\,.$$

Le langage probabiliste est commode pour étudier les propriétés que l'on espère typiques pour des éléments de structures arithmétiques qui donnent naturellement lieu à un ou plusieurs espaces probabilisés possibles. Pour un exemple simple où la variable aléatoire X est l'aboutissement d'une marche aléatoire sur $\mathbf{Z}$, on renvoie à [K4, Cor. 6.2], qui constitue un analogue probabiliste du théorème de Brun–Titchmarsh. Dans le chapitre qui suit, on prendra également pour X l'aboutissement d'une marche aléatoire, mais cette fois dans le cas non-abélien, où ce sont les points $\mathbf{Q}$-rationnels de groupes algébriques linéaires dont on étudie les propriétés typiques.

Chapitre 2

Théorie de Galois probabiliste pour les groupes arithmétiques

L'expression « théorie de Galois probabiliste » est ici à comprendre dans le sens suivant : étant donné un polynôme à coefficients entiers (ou plus généralement à coeffcients dans l'anneau des entiers $\mathbf{Z}_K$ d'un corps de nombres K fixé) dont on suppose ou non qu'il sataisfait à un certain nombre de propriétés de symétrie, quel est typiquement le groupe de Galois de son corps de décomposition sur $\mathbf{Q}$ (ou sur K si l'on s'intéresse à des polynômes à coefficients dans $\mathbf{Z}_K$) ?

Le théorème 1.1.1, dû à Gallagher, est un des exemples les plus naturels de résultat relevant de la théorie de Galois probabiliste. Le modèle probabiliste est dans ce cas très simple. La mesure dont il provient correspond à la hauteur naturelle des polynômes à coefficients entiers. Puisque l'on n'impose, dans l'énoncé du théorème 1.1.1, aucune propriété de symétrie particulière, l'ensemble des polynômes unitaires de degré $r \geqslant 1$ à coefficients entiers est en bijection avec $\mathbf{Z}^r$. La preuve de Gallagher utilise alors une méthode de grand crible sur $\mathbf{Z}^r$. L'absence de condition de symétrie laisse penser que le groupe de Galois du corps de décomposition d'un polynôme de $\mathbf{Z}[X]$ unitaire de degré r est typiquement isomorphe à $\mathfrak{S}_r$. Le théorème de Gallagher donne une information quantitative confirmant cette intuition.

Qu'en est-il maintenant si l'on restreint davantage l'ensemble de polynômes considérés ? Les sous-groupes arithmétiques de groupes de matrices à coefficients dans un corps de nombres K fournissent des familles naturelles de polynômes satisfaisant à certaines propriétés de symétrie : il suffit de considérer le polynôme caractéristique de chaque élément du groupe.

Exemple 2.0.1. Fixons des entiers naturels $n, m, g \geqslant 1$, avec n et m de parité contraire, et considérons $G = \mathrm{SO}(n, m)(\mathbf{Z})$ (où l'on a fixé au préalable une forme quadratique sur $\mathbf{Q}$ de signature (n, m)) ou $G = \mathrm{Sp}(2g, \mathbf{Z})$, alors le polynôme caractéristique χ_M d'un élément $M \in G$ satisfait à l'équation fonctionnelle

$$\det(-M)T^{\deg \chi_M}\chi_M\left(\frac{1}{T}\right) = \chi_M(T)\,,$$

traduisant le fait que l'ensemble des valeurs propres de M est globalement stable par inversion. On note que dans le cas où $G = \mathrm{SO}(n,m)(\mathbf{Z})$, on a $\chi_M(1) = 0$, i.e. χ_M se factorise par $T-1$.

Dans les deux cas, si l'on note k_M le corps de décomposition de χ_M sur $\mathbf{Q}$, et en définissant $2r_M := \deg \chi_M = 2g$ (resp. $2r_M := \deg \chi_M - 1 = n+m-1$) si $G = \mathrm{Sp}(2g,\mathbf{Z})$ (resp. si $G = \mathrm{SO}(n,m)(\mathbf{Z})$), alors le groupe $\mathrm{Gal}(k_M/\mathbf{Q})$ est d'ordre au plus $2^{r_M} r_M!$. Plus précisément, $\mathrm{Gal}(k_M/\mathbf{Q})$ est isomorphe à un sous-groupe du groupe des permutations de l'ensemble $\{-r_M,\dots,-1,1,\dots,r_M\}$ formé des éléments de $\mathfrak{S}_{2r_M}$ agissant sur les paires $\{-i,i\}$, $1 \leqslant i \leqslant r_M$. Ce groupe, noté W_{2r_M}, est le groupe de Weyl commun aux systèmes de racines B_{r_M} et C_{r_M}.

L'exemple que nous venons de donner illustre en réalité un principe général qui fait l'objet d'une étude systématique dans [4]. Ce principe est le suivant : si K est un corps de nombres et g est un élément K-rationnel « au hasard » dans un groupe algébrique $\mathbf{G}/K$ réductif, connexe, scindé et muni d'une représentation fidèle $\rho\colon G \to \mathrm{GL}_m$, alors le groupe de Galois du corps de décomposition de $\det(T-\rho(g))$ sur K est isomorphe au groupe de Weyl de $\mathbf{G}$ avec grande probabilité. Le cas particulier du groupe spécial linéaire et du groupe symplectique est traité, indépendamment, dans [K4] et [R2], quant au cas du groupe orthogonal pour une forme bilinéaire indéfinie, il fait l'objet de [J2]. L'article [3], antérieur à [4], donne une incarnation explicte de ce principe dans le cas où $\mathbf{G}$ est une forme scindée de $\mathbf{E}_8/\mathbf{Q}$. On y calcule un élément explicite de $\mathbf{E}_8(\mathbf{Z})$ obtenu comme aboutissement d'une marche aléatoire (à 16 pas !) dont on calcule, par un recours au logiciel `magma`, le polynôme caractéristique. On montre alors que le groupe de Galois du corps de décomposition de ce polynôme sur $\mathbf{Q}$ est isomorphe au groupe de Weyl $W(\mathbf{E}_8)$, donnant ainsi une solution explicite au problème de Galois inverse sur $\mathbf{Q}$ pour le groupe $W(\mathbf{E}_8)$. *Via* une approche semblable combinée à l'utilisation des réseaux de Mordell–Weil, Shioda a ensuite produit dans [S3] d'autres polynômes entiers (de même degré que celui apparaissant explicitement dans [3]) satisfaisant la même propriété (voir aussi [VAZ] où l'on retrouve l'utilisation des réseaux de Mordell–Weil).

Dans ce chapitre, on présente les articles [3] et [4]. On expliquera d'abord le cadre général de travail de [4], puis on verra [3] comme un cas particulier contenant divers aspects explicites. Insistons sur le fait que cette présentation se fait dans l'ordre inverse de la chronologie des résultats obtenus.

2.1 Éléments rationnels aléatoires de groupes algébriques et corps de décomposition de tores

Le cadre de travail de [3] et [4] est le suivant. Soit k un corps de nombres et $\mathbf{Z}_k$ son anneau d'entiers. Soit $\mathbf{G}/k$ un groupe algébrique linéaire connexe. Il est toujours possible de voir $\mathbf{G}$ comme un groupe de matrices *via* une représentation fidèle fixée $\rho\colon \mathbf{G} \to \mathrm{GL}(m)$, définie sur k. On se donne par ailleurs un sous-groupe Γ de $\mathbf{G}(k)$, dont on suppose qu'il est

Zariski-dense dans $\mathbf{G}$ et *arithmétique*[1], i.e. $\rho(\Gamma)$ est commensurable à $\rho(\mathbf{G}(k)) \cap \mathrm{GL}(m, \mathbf{Z}_k)$.

Pour chaque $g \in \Gamma$, on considère le polynôme caractéristique $\det(T - \rho(g)) \in k[T]$ et l'on note k_g son corps de décomposition sur k. On cherche à décrire, pour un g pris « au hasard » le groupe $\mathrm{Gal}(k_g/k)$.

2.1.1 La marche aléatoire

Pour produire des éléments $g \in \Gamma$ aléatoires, on fixe un espace probabilisé $(\Omega, \Sigma, \boldsymbol{P})$ et une partie génératrice finie (rappelons que Γ est un sous-groupe arithmétique de $\mathbf{G}(k)$) S de Γ dont on suppose qu'il est symétrique (i.e. $s^{-1} \in S$ dès que $s \in S$). Soit $(p_s)_{s \in S}$ une suite réelle finie vérifiant

$$p_s > 0\,,\ p_s = p_{s^{-1}}\ (s \in S)\,, \qquad \sum_{s \in S} p_s = 1\,.$$

Les éléments $g \in \Gamma$ auxquels on s'intéresse sont les aboutissements, après un nombre de pas arbitrairement grand, d'une marche aléatoire $(X_k)_{k \geqslant 0}$. Les pas de la marche aléatoire forment la suite de variables aléatoires indépendantes $(\xi_k)_{k \geqslant 1}$ de loi commune

$$\boldsymbol{P}(\xi_k = s) = \boldsymbol{P}(\xi_k = s^{-1}) = p_s = p_{s^{-1}}\,.$$

La marche aléatoire (X_k) est alors définie comme suit :

$$\begin{cases} X_0 = g_0\,, \\ X_{k+1} = X_k \xi_{k+1},\ k \geqslant 1\,, \end{cases} \tag{2.1.1}$$

où $g_0 \in \Gamma$ est fixé, par exemple $g_0 = \mathrm{Id}$. (Plus généralement, on peut choisir g_0 comme étant un élément aléatoire d'une partie finie fixée $T \subseteq \Gamma$.) La partie génératrice S étant finie, le choix le plus naturel pour la suite (p_s) est sans doute $p_s := |S|^{-1}$, pour tout $s \in S$.

Il est commode de traduire la marche aléatoire (X_k) en termes combinatoires. Le graphe de Cayley X dont les sommets sont les éléments de Γ et tel que (v_1, v_2) est une arête si et seulement si $v_2 = v_1 s$, pour un $s \in S$, est un graphe connexe et non-orienté par hypothèse sur S. La suite (X_k) peut être vue comme une marche aléatoire sur les sommets de X. L'intérêt de ce point de vue apparaît lorsque, appliquant la majoration du grand crible (1.1.2), ce sont les propriétés d'expansion d'une famille de graphes de Cayley construite à partir de X qui permettront de borner efficacement Δ.

Le crible utilisé dans [4] est le grand crible de conjugaison dans sa version probabiliste décrite dans la section 1.3. Précisément, la situation idéale est du type suivant : on choisit comme cadre de crible $(\Gamma, \Lambda, (\Gamma \to \Gamma_\lambda^\sharp))$, où Λ est l'ensemble des idéaux premiers (à un nombre fini d'exceptions près) $\lambda \subseteq \mathbf{Z}_k$, et, pour chaque $\lambda \in \Lambda$, le groupe Γ_ℓ est fini et coïncide avec le groupe des points $\mathbf{F}_\lambda$-rationnels du groupe algébrique $\mathbf{G}/\mathbf{F}_\lambda$. (Le corps fini $\mathbf{F}_\lambda$ est le corps résiduel correspondant à l'idéal premier λ.)

1. Cette hypothèse n'est en fait pas nécessaire. Comme suggéré dans [4, Rem. 5.10] et démontré dans [LR], il est suffisant de supposer que Γ est un sous-groupe de type fini de $\mathbf{G}(\mathbf{Z}_k)$ Zariski-dense dans $\mathbf{G}$.

La contrainte majeure dans ce « cadre idéal » est l'égalité $\Gamma_\lambda = \mathbf{G}(\mathbf{F}_\lambda)$. En d'autres termes on demande que l'image de Γ par réduction modulo λ soit maximale, dans le sens où elle coïncide avec le groupe de *tous* les points $\mathbf{F}_\lambda$-rationnels de $\mathbf{G}/\mathbf{F}_\lambda$. Puisque l'on suppose Γ Zariski-dense dans $\mathbf{G}$, cette contrainte est satisfaite si $\mathbf{G}$ est *simplement connexe*. Il s'agit là d'une conséquence du théorème d'approximation forte de Nori, Matthews–Vaserstein–Weisfeiler, et Weisfeiler (voir [4, preuve de la prop. 5.2], pour des références précises). Dans [4], on veut s'affranchir de cette hypothèse ; il est donc nécessaire de procéder à une étape de réduction permettant de se ramener du cas général au cas où $\mathbf{G}/k$ est simplement connexe.

Une fois cette étape de réduction opérée, on dispose, pour chaque entier $n \geqslant 0$ d'un ensemble à cribler, $(\Omega, \boldsymbol{P}, X_n)$. Pour tout choix d'une famille d'ensembles criblants $(\Theta_\lambda)_{\lambda\in\Lambda}$, et moyennant de bonnes estimations sur les constantes Δ et H apparaissant dans (1.1.2), on peut alors majorer la probabilité

$$\boldsymbol{P}(\rho_\ell(X_n) \notin \Theta_\lambda,\, \forall \lambda \in \mathcal{L}^*)\,,$$

où $\mathcal{L}^*$ est une partie finie fixée de Λ. Il faut ensuite chioisir la famille (Θ_λ) de sorte à ce qu'elle nous renseigne sur le groupe de Galois $\mathrm{Gal}(k_{X_n}/k)$ du corps de décomposition de $\det(T - X_n)$ sur k. Plus précisément on commence par déterminer *a priori* quel est le groupe de Galois maximal $\Pi(\mathbf{G})$ auquel $\mathrm{Gal}(k_{X_n}/k)$ peut être isomorphe. Le choix des ensembles Θ_λ permet ensuite de détecter les classes de conjugasion de $\Pi(\mathbf{G})$ qui intersectent non trivialement $\mathrm{Gal}(k_{X_n}/k)$.

2.1.2 Corps de décomposition de tores et de polynômes caractéristiques

Soit k un corps parfait, $\mathbf{G}/k$ un groupe réductif, et soit $\mathbf{T}$ un tore maximal de $\mathbf{G}$ défini sur k. On note $\bar{k}$ une clôture algébrique de k et $X(\mathbf{T})$ le groupe des caractères de $\mathbf{T}$ c'est-à-dire le groupe des $\bar{k}$-morphismes $\alpha\colon \mathbf{T}_{\bar{k}} \to \mathbf{G}_{m,\bar{k}}$. Ce groupe est muni d'une action de $\mathrm{Gal}(\bar{k}/k)$. Précisément, on a un morphisme de groupes

$$\varphi_{\mathbf{T}}\colon\ \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(X(\mathbf{T}))\,, \qquad \sigma \mapsto (\alpha \mapsto \sigma\cdot\alpha)\,,$$

où $\sigma\cdot\alpha$ est défini de manière unique par

$$(\sigma\cdot\alpha)\,(\sigma(t)) = \sigma(\alpha(t))\,, (t \in \mathbf{T}(\bar{k}))\,.$$

À la donnée $(\mathbf{G}, \mathbf{T})$ est naturellement associé un groupe *fini* : le groupe de Weyl $W(\mathbf{G}, \mathbf{T})$. Il s'agit du groupe des points $\bar{k}$-rationnels du quotient $N_{\mathbf{G}}(\mathbf{T})/Z_{\mathbf{G}}(\mathbf{T})$ où $N_{\mathbf{G}}(\mathbf{T})$ (resp. $Z_{\mathbf{G}}(\mathbf{T})$) désigne le normalisateur (resp. le centralisateur) de $\mathbf{T}$ dans $\mathbf{G}$. Le groupe $W(\mathbf{G}, \mathbf{T})$ agit fidèlement sur $X(\mathbf{T})$ *via* l'homomorphisme :

$$W(\mathbf{G}, \mathbf{T}) \to \mathrm{Aut}(X(\mathbf{T}))\,, \qquad w \mapsto \left(\alpha \mapsto \left(\alpha^w\colon t \mapsto \alpha(ntn^{-1})\right)\right), (t \in \mathbf{T}(\bar{k}))\,,$$

où n désigne un représentant de w dans $N(\mathbf{G}, \mathbf{T})$. On peut donc identifier $W(\mathbf{G}, \mathbf{T})$ à un sous-groupe de $\mathrm{Aut}(X(\mathbf{T}))$. La proposition suivante, qui est une compilation de [4, Prop.

2.1, Lem. 2.2], définit le groupe $\Pi(\mathbf{G},\mathbf{T})$ qui joue un rôle central dans la détermination des groupes de Galois étudiés, et énonce des propriétés d'indépendance relativement au choix du tore $\mathbf{T}$.

Proposition 2.1.1. *En conservant les notations ci-dessus, soit* $\Pi(\mathbf{G},\mathbf{T})$ *le sous-groupe de* $\mathrm{Aut}(X(\mathbf{T}))$ *engendré par* $W(\mathbf{G},\mathbf{T})$ *et* $\varphi_{\mathbf{T}}(\mathrm{Gal}(\bar{k}/k))$. *On a les propriétés suivantes.*

(i) le groupe $W(\mathbf{G},\mathbf{T})$ *est distingué dans* $\Pi(\mathbf{G},\mathbf{T})$,

(ii) à isomorphisme près, les groupes $W(\mathbf{G},\mathbf{T})$ *et* $\Pi(\mathbf{G},\mathbf{T})$ *sont indépendants du choix d'un tore maximal* $\mathbf{T}$ *de* $\mathbf{G}$ *défini sur* k,

(iii) soit $k_{\mathbf{T}} \supseteq k$ *le corps de décomposition de* $\mathbf{T}$ *i.e. la plus petite extension de* k *telle que* $\mathrm{Gal}(\bar{k}/k_{\mathbf{T}})$ *agisse trivialement sur* $X(\mathbf{T})$ via $\varphi_{\mathbf{T}}$. *On définit le* corps de décomposition de $\mathbf{G}$ *:*

$$k_{\mathbf{G}} := \bigcap_{\mathbf{T}\ \textit{tore maximal de}\ \mathbf{G}} k_{\mathbf{T}}\,.$$

On a $\varphi_{\mathbf{T}}(\mathrm{Gal}(\bar{k}/k_{\mathbf{G}})) \subseteq W(\mathbf{G},\mathbf{T})$.

Le point *(ii)* de la proposition permet de considérer les groupes abstraits $W(\mathbf{G})$ et $\Pi(\mathbf{G})$, lorsque l'utilisation d'un tore nécessaire à la définition de ces groupes n'est pas requise.

On décrit maintenant le lien entre les corps de décomposition de tores et les corps de décomposition de polynômes caractéristiques d'éléments de $\mathbf{G}(k)$. Fixons tout d'abord une représentation fidèle $\rho\colon \mathbf{G} \to \mathrm{GL}(m)$ définie sur k. Étant donné $g \in \mathbf{G}(k)$, on note k_g le corps de décomposition du polynôme caractéristique $\det(T-\rho(g))$ sur k. Si l'élément g est semisimple et régulier, on peut (par la définition même de la propriété de régularité) lui associer un tore maximal privilégié $\mathbf{T}_g$ de $\mathbf{G}$: c'est l'unique tore maximal de $\mathbf{G}$ contenant g. On a alors, suivant la théorie développée au début de §2.1.2, un homomorphisme

$$\varphi_{\mathbf{T}_g}\colon\ \mathrm{Gal}(\bar{k}/k) \to \Pi(\mathbf{G})\,.$$

On peut établir le lien suivant entre les extensions k_g et $k_{\mathbf{T}_g}$ de k (voir [4, Lem. 2.4]).

Lemme 2.1.2. *Supposons que le groupe* $\mathbf{G}/k$ *est réductif. Alors :*

(i) pour tout $g \in \mathbf{G}(k)$, *le groupe* $\mathrm{Gal}(k_g/k)$ *est isomorphe à un sous-quotient de* $\Pi(\mathbf{G})$, *et, si* $k_{\mathbf{G}}k_g$ *désigne le compositum de* k_g *et* $k_{\mathbf{G}}$ *dans* $\bar{k}$, *le groupe* $\mathrm{Gal}(k_gk_{\mathbf{G}}/k_{\mathbf{G}})$ *est isomorphe à un sous-quotient de* $W(\mathbf{G})$,

(ii) il existe une sous-variété fermée $Y \subsetneq \mathbf{G}$ *stable par conjugasion par* $\mathbf{G}$, *et telle que pour tout* $g \in \mathbf{G}(k) \setminus Y(k)$, *l'élément* g *est régulier semisimple et* $k_{\mathbf{T}_g} = k_g$.

On remarque en particulier que si l'on suppose $\mathbf{G}/k$ scindé, le groupe de Galois maximal attendu pour l'extension k_g/k est le groupe de Weyl $W(\mathbf{G})$.

La proposition 2.1.1 et le lemme 2.1.2 permettent d'une part d'identifier clairement le « groupe de Galois maximal attendu » pour le corps de décomposition de polynômes caractéristiques d'éléments de $\mathbf{G}(k)$, et d'autre part de donner un sens algébrique naturel à ces polynômes. Ces liens sont importants pour mener à bien la partie « locale » du crible, c'est-à-dire pour identifier clairement comment choisir les ensembles criblants Θ_λ, et pour minorer la constante H de (1.1.2).

2.2 Densités locales et équirépartition

Dans [3] et [4], la méthode permettant de s'assurer que le groupe de Galois considéré est aussi gros que possible repose sur les faits standard suivants déjà utilisés par exemple dans [G1], [K4, Chap. 7], ou [J2].

— Si k est un corps de nombres d'anneau d'entiers $\mathbf{Z}_k$ et si l'on fixe un idéal premier $\mathfrak{p}$ de $\mathbf{Z}_k$ (de corps résiduel associé $\mathbf{F}_\mathfrak{p}$) et un polynôme unitaire $P \in \mathbf{Z}_k[T]$ de discriminant non divisible par $\mathfrak{p}$, alors, en supposant que P mod $\mathfrak{p}$ se factorise sur $\mathbf{F}_\mathfrak{p}[T]$ en le produit de n_1 facteurs linéaires, n_2 facteurs quadratiques irréductibles, et plus généralement n_i facteurs irréductibles de degré i, on déduit que le groupe de Galois du corps de décomposition de P sur k, vu comme groupe de permutation de ses racines dans $\mathbf{C}$, contient un élément produit disjoint de n_1 points fixes, n_2 transpositions, et plus généralement n_i cycles de longueur i.

— Si G est un groupe fini et si H est un sous-groupe strict de G alors il existe une classe de conjugaison de G disjointe de H.

Ces principes dictent un choix naturel d'ensembles criblants (Θ_λ). Avec les mêmes notations que dans §2.1.1, fixons un corps de nombres k et supposons $\mathbf{G}/k$ scindé (cette hypothèse n'est pas nécessaire, mais facilite l'exposition). Pour chaque $\lambda \in \Lambda$, l'ensemble Θ_λ est une partie stable par conjugaison de Γ_λ qui correspond à une unique classe de conjugaison de $W(\mathbf{G})$ (en vertu des résultats énoncés dans §2.1.2). Pour rendre rigoureux ce choix naturel d'ensemble criblant, on a recours à la construction (déjà présente, par exemple, dans des travaux de Carter et Fulman cités dans [4]) d'une certaine application envoyant naturellement, dans le cas d'un groupe $\mathbf{G}$ connexe, scindé, semisimple sur un corps fini $\mathbf{F}_q$, un élément $\mathbf{F}_q$-rationnel régulier semisimple sur une classe de conjugaison canonique de $W(\mathbf{G})$.

Plus précisément, fixons un tel groupe $\mathbf{G}/\mathbf{F}_q$. L'application que l'on vient de mentionner est la suivante :

$$\theta\colon \mathbf{G}(\mathbf{F}_q)_{sr} \to W(\mathbf{G})^\sharp, \qquad g \mapsto \varphi_{\mathbf{T}_g}(\mathrm{Frob}_q)^\sharp, \tag{2.2.1}$$

où l'on adopte les notations de §2.1.2, et où Frob_q désigne l'application $x \mapsto x^q$ et l'indice sr signifie que l'on se restreint aux éléments semisimples réguliers. Dans [4], on établit le résultat d'équirépartition suivant (voir [4, Prop. 4.1]) pour les valeurs prises par la fonction θ en les points $\mathbf{F}_q$-rationnels semisimples réguliers de $\mathbf{G}$.

Proposition 2.2.1. *Pour tout $C \in W(\mathbf{G})^\sharp$, on a*

$$\frac{|\{g \in \mathbf{G}(\mathbf{F}_q)_{sr}\colon \theta(g) = C\}|}{|\mathbf{G}(\mathbf{F}_q)|} = \frac{|C|}{|W(\mathbf{G})|}\left(1 + O(q^{-1})\right),$$

avec une constante implicite ne dépendant que de $\mathbf{G}$ (plus précisément, la constante implicite ne dépend que de la classe d'isomorphisme de la donnée radicielle de $\mathbf{G}$).

L'existence et les propriétés d'équirépartition de la fonction θ étant établies, on peut se placer de nouveau dans le cadre d'étude où k est un corps de nombres et $\mathbf{G}/k$ est un groupe linéaire connexe semisimple scindé. A l'exception d'un nombre fini d'idéaux premiers $\lambda \subseteq \mathbf{Z}_k$

on définit les ensembles criblants :

$$\Theta_\lambda := \{g \in \mathbf{G}(\mathbf{F}_\lambda)_{sr} \colon \theta_\lambda(g) = C\}\,,$$

où C est une classe de conjugaison fixée de $W(\mathbf{G})$, et où θ_λ n'est autre que l'application θ, définie par (2.2.1), relativement au groupe $\mathbf{G}/\mathbf{F}_\lambda$.

Pour ce choix d'ensemble criblant, la proposition 2.2.1 permet d'obtenir un minorant satisfaisant pour la constante H apparaissant dans (1.1.2), à partir de la minoration *a priori* (1.1.3). Cela signifie en pratique que la minoration (1.1.4) est valide. Pour un choix évident de support premier de crible $\mathcal{L}^*$, on a par exemple

$$H \gg |\{\lambda \in \Lambda \colon \lambda \text{ idéal premier de } \mathbf{Z}_k \text{ tel que } \mathrm{N}(\lambda) \leqslant L\}|$$

où $L \geqslant 1$ est un réel fixé. Puisque Λ est l'ensemble des idéaux premiers de $\mathbf{Z}_k$, à un nombre fini d'exceptions près, on déduit alors pour L assez grand

$$H \gg \frac{L}{\log L}\,. \tag{2.2.2}$$

2.3 Énoncé du résultat général et éléments de preuve

On conserve les notations de §2.1 et §2.2. Une combinaison d'arguments de réduction et de la méthode de grand crible dont on a décrit les préparatifs aux paragraphes §2.1 et §2.2 permet de démontrer le résultat suivant ([4, Th. 6.1]).

Théorème 2.3.1. *Soit k un corps de nombres et soit $\mathbf{G}/k$ un groupe algébrique linéaire connexe. Soit $R_u(\mathbf{G})$ le radical unipotent de $\mathbf{G}$, i.e. le sous-groupe unipotent connexe distingué maximal de $\mathbf{G}$. Si le groupe $\mathbf{G}$ n'est pas réductif (i.e. si $R_u(\mathbf{G})$ n'est pas trivial), on définit $k_{\mathbf{G}} := k_{\mathbf{G}/R_u(\mathbf{G})}$, $W(\mathbf{G}) := W(\mathbf{G}/R_u(\mathbf{G}))$, et $\Pi(\mathbf{G}) := \Pi(\mathbf{G}/R_u(\mathbf{G}))$, dans les notations de §2.1 et §2.2.*

(i) On a

$$\lim_{n\to\infty} \boldsymbol{P}\left(\mathrm{Gal}(k_{X_n}/k) \simeq \Pi(\mathbf{G})\right) = 1\,.$$

(ii) Si $\mathbf{G}$ est semisimple, alors il existe une constante $c > 1$ telle que

$$\boldsymbol{P}\left(\mathrm{Gal}(k_{X_n}/k) \simeq \Pi(\mathbf{G})\right) = 1 + O(c^{-n})\,,$$

pour tout $n \geqslant 1$.

(iii) Il existe une constante $c > 1$ telle que

$$\boldsymbol{P}\left(\mathrm{Gal}(k_{\mathbf{G}}k_{X_n}/k_{\mathbf{G}}) \simeq W(\mathbf{G})\right) = 1 + O(c^{-n})\,,$$

pour tout $n \geqslant 1$.

Les constantes c apparaissant ainsi que les constantes implicites ne dépendent que du groupe $\mathbf{G}$, de la partie génératrice S de Γ, et de la distribution des pas ξ_n de la marche aléatoire (X_n).

On décrit dans le reste de cette section les étapes principales de la preuve de ce théorème.

2.3.1 Étapes de réduction

Pour pouvoir appliquer la proposition 2.2.1, il nous faut tout d'abord contrôler la probabilité que l'aboutissement X_n de la marche aléatoire après n pas ne soit pas un élément semisimple régulier de $\mathbf{G}$. C'est une nouvelle fois le crible qui permet ce contrôle (comme mentionné dans [4, Rem. 6.3], on pourrait en fait se contenter de cribler en n'utilisant qu'un seul idéal premier bien choisi de $\mathbf{Z}_k$). Plus généralement, on utilise le lemme 2.1.2 combiné avec [4, Lem. 6.2] affirmant que si $Y \subsetneq \mathbf{G}$ est une sous-variété fermée stable par conjugaison dans $\mathbf{G}$ alors

$$\boldsymbol{P}(X_n \in Y(k)) = \begin{cases} o(1), \text{ lorsque } n \to \infty\,, \\ O(c^{-n})\,, \text{ si } \mathbf{G} \text{ est semismple}\,, \end{cases} \tag{2.3.1}$$

où l'uniformité sur la constante $c > 1$ et la constante implicite sont les mêmes que dans l'énoncé du théorème 2.3.1. C'est dans cette première étape que se fait la distinction entre le cas réductif non semisimple et le cas semisimple. Le fait que l'on n'obtienne qu'une information qualitative dans le point (i) du théorème 2.3.1 en est la conséquence.

Sans perte de généralité on peut supposer que $\mathbf{G}/k$ est réductif. En effet, on dispose d'un morphisme quotient $\pi\colon \mathbf{G}' := \mathbf{G} \to \mathbf{G}/R_u(\mathbf{G})$ entre groupes définis sur k. Le groupe $\mathbf{G}'$ est réductif et l'application π permet de considérer la marche aléatoire $(\pi(X_n))$ sur $\pi(\Gamma)$. Le fait qu'il suffise d'étudier cette nouvelle marche aléatoire provient du fait que $k_{X_n} = k_{\pi(X_n)}$ (voir [4, Lem. 2.3]).

Par un argument analogue, la spécificité du cas semisimple explicitée par (2.3.1) est essentiellement la seule par rapport au cas où l'on suppose simplement $\mathbf{G}$ réductif. En effet si $\mathbf{G}$ est réductif et si l'on note $R(\mathbf{G})$ son radical (i.e. la composante neutre de son sous-groupe distingué résoluble maximal), alors le groupe $\mathbf{G}'' := \mathbf{G}/R(\mathbf{G})$ est semisimple et l'on a un morphisme quotient $\pi'\colon \mathbf{G} \to \mathbf{G}''$. Au lieu de la marche aléatoire (X_n), on considère alors (X_n''), où $X_n'' := \pi'(X_n)$. C'est une marche aléatoire sur $\Gamma'' := \pi'(\Gamma)$ définie en utilisant $S'' := \pi'(S)$. On peut en outre montrer que $k_{X_n''} \subseteq k_{X_n}$ (voir [4, Lem. 6.5]). Si K est une extension finie de k contenant à la fois $k_{\mathbf{G}}$ et $k_{\mathbf{G}''}$ (voir la proposition 2.1.1(iii)) on a alors l'inégalité

$$\boldsymbol{P}\left(\mathrm{Gal}(Kk_{X_n''}/K) \simeq W(\mathbf{G}'')\right) \leqslant \boldsymbol{P}\left(\mathrm{Gal}(Kk_{X_n}/K) \simeq W(\mathbf{G})\right)\,,$$

ce qui suffit à se restreindre au cas semisimple.

La dernière étape de réduction est plus délicate. Comme on l'a déjà mentionné, elle nécessite le recours d'une part au théorème d'approximation forte, et d'autre part aux propriétés des chaînes de Markov.

Si $\mathbf{G}/k$ est un groupe alébrique linéaire semisimple connexe, on peut considŕer son revêtement simplement connexe $\varphi\colon \mathbf{G}^{sc} \to \mathbf{G}$. Le groupe $\mathbf{G}^{sc}$ et le morphisme φ sont définis sur k, et le groupe

$$\Gamma^{sc} := \varphi\left(\varphi^{-1}(\Gamma) \cap \mathbf{G}^{sc}(k)\right)$$

est d'indice fini dans Γ. Les étapes successives de la marche aléatoire (X_n) se répartissent donc dans les classes à gauche (en nombre fini) de Γ relativement à Γ^{sc}. Par extraction de sous-suites, on obtient donc une marche aléatoire sur chaque classe à gauche, i.e. sur

chaque élément de $\Gamma^{sc}\backslash\Gamma$. Dans [4, Lemmes 5.4 et 5.6], on donne les arguments probabilistes nécessaires pour justifier une forme d'équirépartition de la marche aléatoire initiale dans les divers éléments de $\Gamma^{sc}\backslash\Gamma$.

Le sous-groupe arithmétique Γ^{sc} de $\mathbf{G}$ (en fait tout élément de $\Gamma^{sc}\backslash\Gamma$) a les propriétés requises pour appliquer la méthode de grand crible décrite dans le chapitre 1. Dans [4, Prop. 5.2], on énonce la conséquence suivante du théorème d'approximation forte pour le groupe Γ^{sc}. Pour tout $\lambda \in \Lambda$, en dehors d'un ensemble R fini d'exceptions, l'application φ induit l'homomorphisme

$$\varphi_\lambda \colon \mathbf{G}^{sc}(\mathbf{F}_\lambda) \to \mathbf{G}(\mathbf{F}_\lambda)\,,$$

et l'on a simultanément un morphisme bien défini

$$\pi_\lambda \colon \Gamma \to \mathbf{G}(\mathbf{F}_\lambda)\,;$$

on note $\Gamma_\lambda^{sc} := \pi_\lambda(\Gamma^{sc})$. Le théorème d'approximation forte affirme que pour des idéaux premiers distincts $\lambda, \lambda' \in \Lambda \setminus R$, le morphisme

$$\pi_\lambda \times \pi_{\lambda'} \colon \Gamma^{sc} \to \Gamma_\lambda^{sc} \times \Gamma_{\lambda'}^{sc} \tag{2.3.2}$$

est surjectif.

Ces diverses étapes de réduction conduisent à un cadre favorable au crible. L'inégalité (1.1.2) peut être appliquée. La minoration de H étant expliquée dans §2.2, il reste à décrire la méthode permettant de majorer Δ.

2.3.2 Majoration de la constante de grand crible

La majoration de la constante de grand crible Δ repose sur des propriétés d'analyse harmonique staisfaites par le groupe arithmétique Γ^{sc} déjà exploitées dans les cas particulier $\mathbf{G} = \mathrm{SL}_n, \mathrm{Sp}_{2g}$, ou $\mathrm{O}(m,n)$ dans [K4] et [J2]. Il s'agit d'une propriété *d'écart spectral* appelée propriété (τ), dont la définition est attribuée à Lubotzky, et qui constitue un affaiblissement de la célèbre propriété (T) de Kazhdan. Rappelons en l'énoncé précis.

Définition 2.3.2 (Propriété (τ))**.** Soit G un groupe topologique et $(N_i)_{i\in I}$ une famille, indexée par un ensemble I, de sous-groupes distingués d'indice fini dans G. On dit que le groupe G a la propriété (τ) relativement à la famille (N_i) s'il existe une partie finie $K \subseteq G$ et $\varepsilon > 0$ tels que pour toute représentation unitaire continue et irréductible $\rho \colon G \to \mathcal{U}(\mathcal{H})$ (le groupe d'arrivée est le groupe unitaire d'un espace de Hilbert $\mathcal{H}$) sans vecteur invariant et satisfaisant $\ker\rho \subseteq N_i$, pour un certain $i \in I$, on a

$$\max_{s\in K} \|\rho(s)v - v\| > \varepsilon\|v\|\,,$$

pour tout $v \in \mathcal{H}$.

Dans [4, Prop. 5.5], on exploite le fait, conséquence d'un résultat de Clozel [C5], que Γ^{sc} satisfait à la propriété (τ) relativement aux sous-groupes de congruence $\ker \pi_{\lambda,\lambda'}$ (dans les notations de §2.3.1) où $\pi_{\lambda,\lambda'} = \pi_\lambda$, si $\lambda = \lambda'$ et $\pi_{\lambda,\lambda'} = \pi_\lambda \times \pi_{\lambda'}$ sinon. *Via* des arguments explicités dans [K4, Prop. 7.2] ou [J2, Prop. 5], on montre dans [4, Prop. 5.5] que la constante de grand crible Δ apparaissant dans (1.1.2) satisfait la majoration

$$\Delta(X_n, \mathcal{L}^*) \leqslant 1 + L^A \mathrm{e}^{-cn}\,, \tag{2.3.3}$$

où $L \geqslant 1$ est fixé et $\mathcal{L}^*$ est consitué, à un ensemble fini près, des idéaux premiers de $\mathbf{Z}_k$ de norme $\leqslant L$. Les constantes $c > 0$ et $A \geqslant 0$ ne dépendent que de k, Γ et de la distribution des pas de la marche aléatoire sur Γ^{sc} induite par (X_n). La preuve du théorème 2.3.1 se déduit alors des étapes de réduction de §2.3.1, et de (1.1.2) où l'on combine (2.2.2) et (2.3.3). (La majoration pour Δ et la minoration pour H dictent le choix optimal pour L, qui doit être choisi de l'ordre de $\exp(cn/A)$.)

Remarques. La constante c apparaissant dans (2.3.3) peut être donnée explicitement en fonction de la constante ε provenant de la propriété (τ) pour Γ^{sc}. On peut en fait montrer que tout ensemble générateur de Γ^{sc} constitue un ensemble S possible dans la définition 2.3.2.

Les années récentes ont vu le développement rapide d'outils de combinatoire additive qui ont permis de généraliser les travaux de Clozel [C5]. Mentionnons le point de départ [H] et le point culminant [GV] de ces progrès remarquables dans la compréhension des phénomènes de croissance et d'expansion dans les groupes (voir [4, Rem. 5.10] pour davantage de références sur le sujet). Le théorème principal de [GV] donne notamment une condition nécessaire et suffisante sur $\mathbf{G}$ pour qu'un sous-groupe Zariski-dense de type fini dans $\mathbf{G}$ ait la propriété (τ) relativement à ses sous-groupes de congruence. Le recours à ce résultat profond rend en fait possible la généralisation du théorème 2.3.1 au cas où l'on suppose simplement Γ Zariski-dense dans $\mathbf{G}$. C'est là l'un des points de départ de l'article [LR] qui généralise également [4] par d'autres aspects. Tout d'abord, Lubotzky et Rosenzweig ne supposent pas $\mathbf{G}$ connexe. Ils montrent, que dans le cas non-connexe, la situation peut être très différente de ce qu'annonce le théorème 2.3.1, et ont recours pour cela a une notion modifiée de groupe de Weyl introduite par Mohrdieck. Par ailleurs, leur résultat (voir [LR, Th. 1.1]) s'applique à tout corps k de type fini sur $\mathbf{Q}$ (et pas seulement aux corps de nombres).

Mentionnons enfin qu'il est naturel de poser la question analogue à celle à laquelle le théorème 2.3.1 répond, pour une notion archimédienne « d'élément aléatoire » : on compte la proportion de « bons » éléments dans une boule de centre l'identité et de rayon R (relativement à une norme matricielle fixée sur $\mathrm{GL}_m(\mathbf{C})$), puis on cherche à étudier cette proportion lorsque $R \to \infty$. Cette question est résolue par Gorodnik–Nevo ([GN]) *via* le recours à des arguments de théorie ergodique. Le résultat qu'ils obtiennent est analogue au théorème 2.3.1.

2.4 Aspects explicites dans le cas d'une forme scindée de $\mathbf{E}_8/\mathbf{Q}$

On reprend les idées de §2.1.1 et §2.1.2 dans le cas concret suivant. On choisit pour $\mathbf{G}$ le goupe $\mathbf{E}_8/\mathbf{Q}$, forme scindée du groupe de type $\mathbf{E}_8$. Il s'agit d'un groupe simple sur $\mathbf{Q}$ de

rang 8 et de dimension 248. La représentation fidèle ρ choisie est la représentation adjointe

$$\mathrm{Ad}\colon \mathbf{E}_8 \to \mathrm{GL}(\mathfrak{e}_8)\,, \qquad g \mapsto T_e(h \mapsto ghg^{-1})$$

où $\mathfrak{e}_8$ est l'algèbre de Lie du groupe $\mathbf{E}_8$, et T_e est l'opérateur de différentiation en l'identité. Le groupe arithmétique Γ que l'on choisit est le groupe des points entiers $\mathbf{E}_8(\mathbf{Z})$.

Le point (*iii*) du théorème 2.3.1 prédit que le corps de décomposition k_g du polynôme $\det(T - \mathrm{Ad}(g))$, où g est un élément aléatoire $g \in \mathbf{E}_8(\mathbf{Z})$, doit satisfaire $\mathrm{Gal}(k_g/\mathbf{Q}) \simeq W(\mathbf{E}_8)$ avec grande probabilité. Cette approche paraît donc pouvoir fournir un exemple explicite d'extension des rationnels répondant au problème de Galois inverse pour le groupe $W(\mathbf{E}_8)$. C'est l'aspect *explicite* qui constitue ici la nouveauté, et l'on a recours, dans [3], au logiciel `magma` pour l'essentiel des calculs. La taille du groupe $W(\mathbf{E}_8)$ explique pourquoi cette question est restée longtemps ouverte, alors que Shioda avait déjà traité dans [S2] le cas de $W(\mathbf{E}_6)$ et $W(\mathbf{E}_7)$. Le groupe $W(\mathbf{E}_8)$ est d'ordre $696\,729\,600 = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$ et ses facteurs de Jordan–Hölder sont $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}$, et le groupe des points $\mathbf{F}_2$-rationnels du groupe algébrique scindé de type D_4 (de dimension 28). Si $g \in \mathbf{E}_8(\mathbf{Z})$ est un élément semisimple, alors pour tout choix de tore maximal $\mathbf{T} \subseteq \mathbf{E}_8$ contenant g, on a

$$\det(T - \mathrm{Ad}(g)) = (T-1)^8 \prod_{\alpha \in R(\mathbf{T},\mathbf{E}_8)} (T - \alpha(g))\,,$$

où $R(\mathbf{T}, \mathbf{E}_8)$ est l'ensemble des racines de $\mathbf{E}_8$ relativement à $\mathbf{T}$. Le polynôme fournissant un candidat à la résolution du problème posé est le quotient $\det(T - \mathrm{Ad}(g))/(T - 1^8)$, qui est de degré $240 = |R(\mathbf{T}, \mathbf{E}_8)|$.

Pour produire un élément g de $\mathbf{E}_8(\mathbf{Z})$, on procède de manière analogue à ce qui est décrit dans §2.1. On choisit une partie génératrice S symétrique que l'on utilise pour construire une marche aléatoire « courte » sur $\mathbf{E}_8(\mathbf{Q})$ (i.e. on s'arrête dès que l'aboutissement de la marche fournit un élément qui répond à la question). La partie S choisie dans [3] est le système des générateurs de Steinberg. Il s'agit du système de 16 « générateurs algébriques » implanté dans `magma`. Ce système correspond à un choix de 8 racines simples $\alpha_1, \ldots, \alpha_8$ chacune associée à l'un des 8 sous-groupes unipotents U_{α_i}, et aux générateurs $-\alpha_i$ des sous-groupes unipotents associés à l'opposé des α_i (voir [3, Rem. 2.5 et §3] et les références indiquées dans *loc. cit.*). A partir de l'ensemble $S := \{x_1, \ldots, x_{16}\}$ obtenu, on considère l'élément

$$g = x_1 \cdots x_{16}\,,$$

et le polynôme $P_g := \det(T - \mathrm{Ad}(g))/(T-1)^8$. Le calcul explicite de $\mathrm{Ad}(g)$ et de P_g par `magma` montre que $\mathrm{Ad}(g)$ est une matrice à coefficients entiers et que par conséquent $P_g \in \mathbf{Z}[T]$.

Le résultat principal de [3] est le suivant.

Théorème 2.4.1. *Le corps de décomposition k_g du polynôme P_g (donné explicitement dans* [3, Append. B]*) sur $\mathbf{Q}$ vérifie* $\mathrm{Gal}(k_g/\mathbf{Q}) \simeq W(\mathbf{E}_8)$.

Donnons quelques informations sur le polynôme P_g. Il s'agit par construction d'un polynôme réciproque (i.e. $T^{\deg P_g} P_g(1/T) = P_g$) de degré 240. L'ordre de grandeur de son discriminant est 10^{14952}. On renvoie à [3, p. 768] pour des données numériques plus précises.

D'après la proposition 2.1.1 et le lemme 2.1.2, le groupe $\mathrm{Gal}(k_g/\mathbf{Q})$ s'injecte dans $W(\mathbf{E}_8)$. La méthode permettant de démontrer que $\mathrm{Gal}(k_g/\mathbf{Q})$ est isomorphe au groupe $W(\mathbf{E}_8)$ tout entier suit les deux principes rappelés au début de §2.2. On déduit les informations suivantes sur le groupe $\mathrm{Gal}(k_g/\mathbf{Q})$ vu comme sous-groupe de $\mathfrak{S}_{240}$.

— modulo 7, le polynôme P_g est produit de 2 irréductibles distincts de degré 4 et de 29 irréductibles distincts de degré 8, donc $\mathrm{Gal}(k_g/\mathbf{Q})$ contient un élément du type

$$g_8 := c_1^{(4)} c_2^{(4)} c_3^{(8)} \cdots c_{31}^{(8)} ,$$

où les $c_i^{(\ell)}$ sont des ℓ-cycles à supports disjoints,

— modulo 11, le polynôme P_g est produit de 16 irréductibles distincts de degré 15, donc $\mathrm{Gal}(k_g/\mathbf{Q})$ contient un élément du type

$$g_{15} := d_1^{(15)} \cdots d_{16}^{(15)} ,$$

où les $d_j^{(\ell)}$ sont des ℓ-cycles à supports disjoints.

Par inspection (ici aussi, on a recours au logiciel `magma`), on vérifie qu'aucun sous-groupe maximal de $W(\mathbf{E}_8)$, vu comme sous-groupe de $\mathfrak{S}_{240}$, ne contient simultanément une classe de conjugasion déterminée par la décomposition de g_8 et une classe de conjugasion déterminée par la décomposition de g_{15}. Plus précisément, l'unique sous-groupe d'indice 2 de $W(\mathbf{E}_8)$ est le noyau de l'homomorphisme ε de signature. Comme $\varepsilon(g_8) = (-1)^{31} = -1$, on a $\mathrm{Gal}(k_g/\mathbf{Q}) \not\subset \ker \varepsilon$. Quant aux autres sous-groupes maximaux de $W(\mathbf{E}_8)$, aucun d'entre eux ne contient d'élément de type g_{15}.

Le recours à l'outil informatique peut sembler excessif dans la démarche ci-dessus, si l'on souhaite pouvoir garantir l'exactitude du théorème 2.4.1. Dans [3, Append. A], on explique comment il est en principe possible d'obtenir le polynôme P_g et de montrer que le groupe de Galois de $k_g/\mathbf{Q}$ est isomorphe à $W(\mathbf{E}_8)$ uniquement par raisonnement déductif et sans recours à un logiciel de calcul formel. Notons enfin que [3, §4] contient les prémices de la méthode de crible utilisée dans [4]. On montre en effet, à partir de l'extension $k_g/\mathbf{Q}$, que l'on peut construire une infinité d'extensions des rationnels deux à deux linéairement disjointes dont le groupe de Galois sur $\mathbf{Q}$ est isomorphe à $W(\mathbf{E}_8)$ (voir [3, Prop. 4.1]). Un point crucial de la preuve utilise le fait suivant : si $\mathbf{E}_8/\mathbf{Z}$ est un modèle du groupe de Chevalley scindé $\mathbf{E}_8$ défini sur $\mathbf{Z}$, alors le morphisme de réduction produit

$$\mathbf{E}_8(\mathbf{Z}) \to \mathbf{E}_8(\mathbf{F}_7) \times \mathbf{E}_8(\mathbf{F}_{11}) ,$$

est surjectif. La généralisation de ce type de propriété (i.e. la disjonction linéaire du cadre de crible) dans [4], joue un rôle essentiel dans l'application du grand crible, comme on l'a expliqué au §2.3.1.

2.5 Questions ouvertes

Le théorème 2.3.1 appelle plusieurs questions qui, à notre connaissance, sont pour l'instant encore ouvertes. Dans cette section, on suppose pour simplifier que $\mathbf{G}/k$ est semisimple scindé

et l'on reprend les notations de la section 2.1. Tout d'abord, l'application du lemme de Borel–Cantelli combiné au théorème 2.3.1 montre qu'il n'y a qu'un nombre fini d'entiers n tels que $\mathrm{Gal}(k_{X_n}/k)$ n'est pas isomorphe au groupe de Weyl $W(\mathbf{G})$. Dans [4, §7], on pose la question de la distribution des variables aléatoires

$$\tau := \min\{n \geqslant 1 :\ \mathrm{Gal}(k_{X_n}/k) \simeq W(\mathbf{G})\}\,,$$
$$\tau^* := \max\{n \geqslant 1 :\ \mathrm{Gal}(k_{X_n}/k) \not\simeq W(\mathbf{G})\}\,.$$

Les méthodes de [4] ne semblent pas en mesure d'apporter des réponses à ces questions.

Dans le même ordre d'idées, le grand crible, s'il constitue un outil efficace pour détecter des classes de conjugaison dans un groupe de Galois, semble inopérant pour *exclure* des classes de conjugaison. On a en tête la question de l'existence et de la fréquence d'apparition d'un sous-groupe strict donné de $W(\mathbf{G})$ comme groupe de Galois $\mathrm{Gal}(k_{X_n}/k)$. Une autre question qui se pose naturellement et qui semble difficile consiste à aller au-delà de la propriété de généricité que constitue le théorème 2.3.1, et de demander [2] s'il existe dans Γ un « gros » sous-groupe dont *tous* les éléments g non triviaux vérifient $\mathrm{Gal}(k_g/k) \simeq W(\mathbf{G})$.

Là encore le grand crible n'est pas un outil suffisant pour pouvoir répondre puisqu'il ne parvient pas à exclure l'apparition d'un élément « rare » dans la suite (X_n).

2. Cette question nous a été posée par E. Breuillard.

Chapitre 3

Formes bilinéaires de Bézout

Dans §2.2, on a donné un énoncé général (proposition 2.2.1), permettant de résoudre la question de l'estimation de densités locales conduisant à une minoration de la constante H de l'inégalité de grand crible (1.1.2). Dans le cas du groupe SL_n ou Sp_{2g}, de telles estimations étaient déjà présentes dans [K4, Append. B] (voir aussi [J2], où l'on traite le cas du groupe $\mathrm{O}(m,n)$). Dans ces premiers exemples, l'approche adoptée est plus élémentaire et, en un sens, plus explicite, que dans la preuve de la proposition 2.2.1.

Explicitons cette approche sur l'exemple suivant. On se place dans le cadre du crible de conjugaison décrit en 1.2. Pour $n \geqslant 3$, on pose $Y = \mathrm{SL}_n(\mathbf{Z})$, $\Lambda = \{\text{nombres premiers}\}$, et $\rho_\ell \colon \mathrm{SL}_n(\mathbf{Z}) \to \mathrm{SL}_n(\mathbf{F}_\ell) \to \mathrm{SL}_n(\mathbf{F}_\ell)^\sharp$, pour tout $\ell \in \Lambda$. On cherche à démontrer que l'irréductibilité de $\det(T-g) \in \mathbf{Z}[T]$ est une propriété typique des éléments $g \in \mathrm{SL}_n(\mathbf{Z})$. Les ensembles criblants que l'on choisit sont les

$$\Theta_\ell := \{g \in \mathrm{SL}_n(\mathbf{F}_\ell) \colon \det(T-g) \text{ est irréductible sur } \mathbf{F}_\ell\}\,.$$

Pour minorer convenablement H, on doit montrer une inégalité du type

$$\frac{|\Theta_\ell|}{|\mathrm{SL}_n(\mathbf{F}_\ell)|} \gg 1\,,$$

avec une constante implicite indépendante de ℓ (voir (1.1.3)).

La stratégie employée dans [K4, Append. B], [J2, §2] (et déjà présente dans [C3, §3]), et de compter d'abord les polynômes de $\mathbf{F}_\ell[T]$ *candidats* (dans l'exemple ci-dessus, cela signifie simplement que le degré doit être égal à n et que le coefficient constant du polynôme doit être $(-1)^n$), puis, pour chaque polynôme candidat, de dénombrer les matrices dont il est polynôme caractéristique. La seconde étape est le calcul du nombre d'éléments dans une réunion de classes de conjugaison de $\mathrm{SL}_n(\mathbf{F}_\ell)$. Cette résolution en deux étapes sous-entend le fait suivant : pour chaque polynôme f candidat, il existe un élément du groupe considéré ($\mathrm{SL}_n(\mathbf{F}_\ell)$ dans notre exemple) dont f est le polynôme caractéristique.

Cette assertion est trivialement vraie pour $\mathrm{SL}_n(\mathbf{F}_\ell)$ par un simple recours à la matrice compagnon du polynôme f. La propriété est aussi vérifiée pour le groupe $\mathrm{Sp}_{2g}(\mathbf{F}_\ell)$ (Chavdarov a recours, dans [C3, Lem. 3.4], à l'isogénie de Lang, et utilise de manière cruciale le fait

que le groupe algébrique $\mathrm{Sp}_{2g}/\mathbf{F}_\ell$ est simplement connexe). En revanche, dès que l'on passe au groupe orthogonal, cette propriété est en général mise en défaut.

Exemple 3.0.1. On reprend l'exemple donné au début de [J2, §2.3] (on renvoie à cet article pour le détail de l'argument). Soit $f(T) := T^2 + T + 1 \in \mathbf{F}_5[T]$, et considérons $\mathbf{F}_5^2$ comme un $\mathbf{F}_5$-espace vectoriel muni de la forme scindée $\Psi((x,y)) = x^2 + y^2$. Alors il n'y a pas d'isométrie de $(\mathbf{F}_5^2, \Psi)$ dont le polynôme caractéristique est f.

Dans ce chapitre on présente les résultats de [5]. Un des objectifs de l'article est de donner une construction simple et explicite d'isométries (relativement à une forme bilinéaire non-dégénérée) de polynôme caractéristique prescrit. L'exemple ci-dessus montre déjà que si l'on se place sur un corps fini, on ne pourra pas en général prescrire simultanément le polynôme caractéristique et la classe du discriminant modulo les carrés du corps fini en question. Dans le cas où la forme est symétrique on peut également choisir de prescrire la norme spinorielle, et dans le cas général, (mais sur un corps algébriquement clos seulement) la forme de Jordan de l'isométrie. Dans [5], on répond à ces diverses questions et l'on fait une analyse détaillée des formes bilinéaires entrant en jeu.

3.1 Matrice de Bézout classique

Le procédé général étudié provient de la théorie des noeuds (voir les références de [5]) et porte le nom de *transfert*. Soit k un corps et A une k-algèbre de dimension finie. On fixe un élément $\alpha \in A$, dont on suppose qu'il engendre A sur k, i.e. $A = k[\alpha]$, et une application k-linéaire

$$t\colon A \to k\,,$$

telle que l'application k-bilinéaire définie sur A par $(x,y) \mapsto t(xy)$ est non-dégénérée. L'application t est le transfert mentionné ci-dessus. Il produit une forme k-bilinéaire non-dégénérée sur A à partir de la forme A-bilinéaire $(x,y) \mapsto xy$.

Dans [5], on appelle *algèbre monogène de Frobenius* un triplet (A, α, t) vérifiant les conditions ci-dessus. On a la notion suivante d'isomorphisme pour les algèbres monogènes de Frobenius : on dit que (A,α,t) et (A',α',t') sont des algèbres monogènes de Frobenius isomorphes s'il existe un isomorphisme de k-algèbres $\varphi\colon A \simeq A'$ tel que $\alpha' = \varphi(\alpha)$ et $t' = t \circ \varphi^{-1}$.

On note aussi que le groupe des unités $A^\times$ de A agit naturellement sur les transferts $t\colon A \to k$ *via*

$$a \cdot t\colon A \to k\,, \qquad x \mapsto t(ax)\,.$$

Le premier résultat de [5] donne une paramétrisation simple des classes d'isomorphie d'algèbres monogènes de Frobenius ([5, Th. 2.1]) par une certaine classe de fractions rationnelles.

Théorème 3.1.1. *Pour tout $d \geqslant 1$, l'application*

$$(A,\alpha,t) \mapsto w(T) := \sum_{\ell \geqslant 0} t(\alpha^\ell) T^{-\ell-1} \in k[[T^{-1}]]\,,$$

établit une bijection entre les classes d'isomorphismes de k-algèbres monogènes de Frobenius (A, α, t) de dimension d et les fractions rationnelles de degré d nulles en l'infini et qui admettent un développement en série formelle dans $k[[T^{-1}]]$.

La preuve est élémentaire et repose sur des manipulations sur les séries formelles. On déduit la conséquence suivante. Si l'on fixe un polynôme $q \in k[T]$ de degré $\geqslant 1$, il existe une application linéaire $t\colon k[T]/(q) \to k$ telle que $(k[T]/(q), T \bmod q, t)$ est une algèbre monogène de Frobenius. Il suffit de considérer l'algèbre monogène de Fronenius associée à $w = 1/q$. Illustrons le théorème en reprenant [5, §2.1].

Exemple 3.1.2. (i) Fixons $q \in k[T]$ irréductible et séparable. L'algèbre $A := k[T]/(q)$ est alors une extension du corps k et la forme $(x, y) \mapsto \mathrm{Tr}_{A/k}(xy)$ est non-dégénérée. Ainsi $(A, T \bmod q, \mathrm{Tr}_{A/k})$ est une algèbre monogène de Frobenius. La fraction rationnelle qui lui est associée par le théorème 3.1.1 est $w := (\mathrm{d}q/\mathrm{d}T)/q$.

(ii) Soit $A := k[T]/(T^d)$ pour un entier $d \geqslant 1$. A la fraction rationnelle $1/T^d$ correspond l'algèbre monogène de Frobenius $(A, T \bmod T^d, t)$ où t est défini par

$$t(T^i \bmod T^d) = 0\,, (0 \leqslant i \leqslant d-2)\,, \qquad t(T^{d-1} \bmod T^d) = 1\,.$$

Explicitons maintenant le lien entre les algèbres monogènes de Frobenius et la construction classique de Bézout associant à un couple de polynômes de degré d une matrice de taille $d \times d$ dont le déterminant est égal au résultant de p et q.

Définition 3.1.3 (Matrice de Bézout)**.** Soit k un corps et $p, q \in k[T]$. Notons $d = \max(p, q)$. La *matrice de Bézout* $B(p, q)$ de (p, q) est la matrice $(b_{i,j}) \in \mathcal{M}_d(k)$ dont les coefficients sont donnés par

$$\frac{p(x)q(y) - p(y)q(x)}{x - y} = \sum_{i,j=1}^{d} b_{i,j} x^{i-1} y^{j-1}\,.$$

Soit maintenant (A, α, t) une algèbre monogène de Frobenius de dimension $d \geqslant 1$. Fixons une k-base $(e_1, \ldots, e_d)$ de A et notons $(e_i^{\#})$ la base duale de (e_i) relativement à $(x, y) \mapsto t(xy)$, i.e.

$$\langle e_i, e_j^{\#} \rangle := t(e_i e_j^{\#}) = \delta_{i,j}\,(i, j = 1, \ldots d)\,.$$

Le noyau reproduisant (ou élément de Casimir)

$$C := \sum_{i=1}^{d} e_i \otimes e_i^{\#} \in A \otimes A$$

peut encore s'écrire $C = \sum_{i,j=1}^{d} \langle e_i^{\#}, e_j^{\#} \rangle e_i \otimes e_j$. En adoptant la notation $e_i = \alpha^{i-1}$, $b_{i,j}^{\#} = \langle e_i^{\#}, e_j^{\#} \rangle$ pour $1 \leqslant i, j \leqslant d$, et en représentant les éléments de $A \otimes A$ par des polynômes de $k[x, y]$ de degré au plus $d-1$ en chaque variable, on voit finalement que

$$C = \sum_{i,j=1}^{d} b_{i,j}^{\#} x^{i-1} y^{j-1}\,.$$

On établit alors le lien annoncé ([5, Th. 2.7]) :

Théorème 3.1.4. *Soit $B^{\#}$ la matrice de terme général $b^{\#}_{i,j}$ et soit p/q une forme irréductible, avec q unitaire, de la fraction rationnelle w associée à la classe d'isomorphie de (A, α, t) par le théorème 3.1.1. Alors*

$$B^{\#} = B(q, r)\,,$$

où $r \in k[T]$ est de degré au plus d et vérifie $rp \equiv 1 (\mathrm{mod}\, q)$.

La structure bilinéaire qui fait l'objet de [5] est une version tordue de la construction ci-dessus. Nous présentons maintenant cette variante qui nous a été inspirée par des travaux de Hamada–Anderson.

3.2 Matrice de Bézout tordue

Soit k un corps et $d \geqslant 1$ un entier. Dans la suite de ce chapitre on suppose que $\mathrm{car}\, k \neq 2$. Soit $a = a_0 + a_1 T + a_2 T^2 + \cdots \in k[[T]]$, on définit $M(a)$ comme étant la matrice de l'endomorphisme de $k[T]/(T^d)$ correspondant à la multiplication par a, et relativement à la base $1, T, \ldots, T^{d-1}$, i.e.

$$M(a) = \begin{pmatrix} a_0 & 0 & & 0 \\ a_1 & a_0 & & \\ \vdots & & \ddots & 0 \\ a_{d-1} & \cdots & \cdots & a_0 \end{pmatrix}.$$

L'application $a \mapsto M(a)$ définit un morphisme de k-algèbres de $k[[T]]$ vers $\mathcal{M}_d(k)$.

Définition 3.2.1 (Matrice de Bézout tordue)**.** Soit $w = p/q \in k(T)$ une fraction rationnelle écrite sous forme irréductible et ne s'annulant pas en $0, \infty$ (en particulier $\deg q \geqslant \deg p$). On note

$$w(T) = w_0 + w_1 T + \cdots\,, \qquad w(T) = w_0^* + w_1^* T^{-1} + \cdots\,,$$

les développements en série formelle de w en 0 et ∞ respectivement. Soit $d = \deg(w) := \max\{\deg p, \deg q\}$. La *matrice de Bézout tordue* associée à w est

$$B^*(w) = {}^t M(T^{d-\deg p} w^*) - M(w) = \begin{pmatrix} w_0^* - w_0 & w_1^* & \cdots & w_{d-1}^* \\ -w_1 & w_0^* - w_0 & w_1^* & w_{d-2}^* \\ \vdots & \ddots & \ddots & w_1^* \\ -w_{d-1} & \cdots & -w_1 & w_0^* - w_0 \end{pmatrix}.$$

Il est également possible de définir la matrice de Bézout tordue par une construction proche de celle donnée dans §3.1 dans le cadre des algèbres monogènes de Frobenius. Considérons tout d'abord l'anneau $R = k[T, T^{-1}]$ et soit $t\colon R \to t$ l'application associant à un polynôme de Laurent son coefficient constant. On peut représenter le dual de cet espace $\mathrm{Hom}(R, k)$ par des séries de Laurent généralisées :

$$\omega := \sum_{n \in \mathbf{Z}} \omega(T^n) T^{-n}\,.$$

On peut munir $\mathrm{Hom}(R,k)$ d'une structure de R-module en utilisant la loi habituelle de multiplicatin des séries. On a alors, pour $u \in R$,

$$\omega(u) = t(u \cdot \omega)\,.$$

Si l'on écrit

$$\omega := \sum_{n\geqslant 0} w_n^* T^n - \sum_{n\geqslant 0} w_n T^{-n}\,,$$

c'est-à-dire

$$\omega(T^n) = \begin{cases} -w_n & n > 0 \\ w_0^* - w_0 & n = 0\,. \\ w_{-n}^* & n < 0 \end{cases} \tag{3.2.1}$$

on peut alors définir la matrice de Bézout tordue associée à $\sum_{i\geqslant 0} w_i T^i = \sum_{j\geqslant 0} w_j^* T^{-j}$ comme la matrice de terme général $\omega(T^{i-j})$, pour $i,j = 0,1,\ldots,d-1$.

La proposition suivante rend plus évident encore le lien avec la construction classique de Bézout (voir [5, Prop. 3.1 et Rem. 3.2]).

Proposition 3.2.2. *En adoptant les notations de la définition 3.2.1, soient q_0 et q_d le coeffcient constant et le coefficient dominant de q, respectivement. On a alors*

$$q_0^d q_d^{\deg p} \det B^*(w) = (-1)^{d-\deg p}\mathrm{Res}(p,q)\,,$$

où $\mathrm{Res}(p,q)$ désigne le résultant de p et q.

De plus si $d = \deg p$, alors la matrice

$$B^*(p,q) := {}^tM(q^*)B^*(w)M(q)$$

a pour terme général le coefficient de $x^{i-1}y^{j-1}$ du polynôme

$$\frac{p(x)q^*(y) - q(x)p^*(y)}{xy-1}\,,$$

où l'on note $f^*(T) = T^{\deg f} f(1/T)$ pour tout $f \in k[t]$. On a alors la formule

$$\det B^*(p,q) = \mathrm{Res}(p,q)\,.$$

Tout comme la matrice de Bézout classique, la matrice de Bézout tordue est un outil efficace permettant de calculer le résultant de deux polynômes. Cependant, la structure qui lui est associée est bien plus riche. Dans la section suivante, on décrit les propriétés de la structure bilinéaire sous-jacente à $B^*(w)$.

3.3 Structure bilinéaire et isométries d'invariants prescrits

Reprenons les notations de §3.2. En particulier $w = p/q$ est une fraction rationnelle (écrite sous forme irréductible) ne s'annulant pas en 0 et ∞, et par conséquent $d := \deg w = \deg q$. On considère le k-espace vectoriel $V := R/(q^*)$. La forme linéaire ω définie par (3.2.1) s'annule sur l'idéal (q^*) (voir [5, §3.3]), et induit donc une forme linéaire sur V.

Dans la suite on travaille sous les hypothèses supplémentaires

$$w(\infty) = 1\,, \qquad w(T^{-1}) = -\varepsilon w(T)\,,$$

où $\varepsilon = \pm 1$. Sous cette hypothèse, on a nécessairement $p^* = \varepsilon_p p$ et $q^* = \varepsilon_q q$, avec $\varepsilon_p, \varepsilon_q \in \{\pm 1\}$ et $\varepsilon_p \varepsilon_q = \varepsilon$ (notons que l'on ne peut pas avoir $\varepsilon_p = \varepsilon_q = -1$ car on suppose $(p, q) = 1$). On a la forme simplifiée

$$B^*(w) = \begin{pmatrix} \varepsilon + 1 & w_1^* & \cdots & w_{d-1}^* \\ \varepsilon w_1^* & \varepsilon + 1 & \cdots & w_{d-2}^* \\ \vdots & \vdots & \vdots & \vdots \\ \varepsilon w_{d-1}^* & \varepsilon w_{d-2}^* & \cdots & \varepsilon + 1 \end{pmatrix}. \tag{3.3.1}$$

La matrice ci-dessus est ε-symétrique, i.e. ${}^t B^*(w) = \varepsilon B^*(w)$, et définit donc une forme bilinéaire symétrique ou antisymétrique suivant le signe ε. Cette forme est non-dégénérée dès que p et q sont premiers entre eux, d'après la proposition 3.2.2.

On note que la forme bilinéaire donnée par (3.3.1), provient, tout comme dans le cas classique, d'un transfert. On va voir, en explicitant le transfert en question, que l'on obtient sans plus d'effort une isométrie de V de polynôme caractéristique q. L'anneau $R = k[T, T^{-1}]$ est muni de l'involution $\iota\colon T \mapsto T^{-1}$, qui passe au quotient par (q^*). On obtient ainsi une involution de V que l'on note encore ι. La matrice $B^*(w)$ donnée par (3.3.1) n'est autre que la matrice de Gram, écrite dans la base $1, T, \ldots, T^{d-1}$, de la forme bilinéaire

$$\Psi(u, v) = t(uv^\iota \cdot w) = \omega(uv^\iota)\,,$$

où ω est défini par (3.2.1). Concrètement, la forme bilinéaire Ψ est définie par

$$\Psi(T^i, T^j) = \omega(T^{i-j})\ (i, j \in \mathbf{Z})\,.$$

La forme bilinéaire Ψ est ε-symétrique et, d'après la formule ci-dessus, la multiplication par T induit une isométrie γ de (V, Ψ) de polynôme caractéristique $\pm q$ (le générateur unitaire de $(q) = (q^*)$). En observant les coefficients de $B^*(w)$ dans la formule (3.3.1), on voit que la classe v_0 de 1 dans $V = R/(q^*)$ vérifie $\Psi(v_0, v_0) = 1 + \varepsilon$. En outre $(v_0, \gamma(v_0), \gamma^2(v_0), \ldots)$ engendre l'espace V. Ces propriétés caractérisent les k-espaces vectoriels de dimension finie munis d'une forme bilináire ε-symétrique non dégénérée. Pour énoncer précisément ce résultat, on considère l'isométrie σ_{v_0} associée à v_0 définie par

$$\sigma_{v_0}(v) = v - \Psi(v_0, v)v_0\,, (v \in V)\,.$$

On a alors la caractérisation suivante des espaces munis d'une forme bilinéaire provenant d'une matrice de Bézout tordue (voir [5, Th. 3.3]). Il s'agit d'un analogue du théorème de classification 3.1.1, où l'ingrédient nouveau apparaissant est l'involution ι de l'anneau $k[T, T^{-1}]$.

Théorème 3.3.1. *Soit (V, Ψ) un k-espace vectoriel de dimension finie muni d'une forme bilinéaire Ψ, non dégénérée et ε-symétrique. Supposons qu'il existe une isométrie γ de cet espace et un vecteur $v_0 \in V$ tel que*

(i) $\Psi(v_0, v_0) = 1 + \varepsilon$,

(ii) la famille $(v_0, \gamma(v_0), \gamma^2(v_0), \ldots)$ est génératrice dans V.

Alors l'espace (V, Ψ) est isométrique à $(R/(q), B^*(w))$ où $w = p/q$, et q (resp. p) est le polynôme caractéristique de γ (resp. de $\gamma\sigma_{v_0}$).

Dans le cas où $k = \mathbf{C}$, le théorème 3.3.1 établit un lien remarquable entre la structure associée à la matrice de Bézout tordue et les groupes hypergéométriques au sens de [BH]. On explique dans [5, §3.5] que le sous-groupe $\langle \gamma, \sigma \rangle$ de $\mathrm{GL}(V)$ est un groupe hypergéométrique fixant une unique (à multiplication par un scalaire près) forme bilinéaire non dégénérée sur V. Cette forme bilinéaire se trouve donc être donnée par la matrice de Bézout tordue $B^*(w)$.

A l'aide de la forme bilinéaire associée à la matrice de Bézout tordue, on peut répondre, de manière explicite, à la question posée au début de ce chapitre (voir [5, Th. 4.1]). Etant donné un polynôme $q \in k[T]$ réciproque (i.e. satisfaisant $q^*(T) = q(T)$), existe-t-il un k-espace vectoriel V muni d'une forme bilinéaire ε-symétrique (où $\varepsilon = \pm 1$ est fixé) non dégénérée Ψ et une isométrie γ de (V, Ψ) telle que $f(T) = \det(T - \gamma)$?

Théorème 3.3.2 (Isométries de polynôme caractéristique fixé)**.** *Soit $q \in k[T]$ un polynôme réciproque de degré $d \geqslant 1$. Alors*

(i) il existe un k-espace vectoriel (V, Ψ) muni d'une forme bilinéaire symétrique Ψ non dégénérée et une isométrie γ de (V, Ψ) de polynôme caractéristique q.

(ii) si l'on suppose d pair, il existe un k-espace vectoriel (V, Ψ) muni d'une forme bilinéaire antisymétrique Ψ non dégénérée et une isométrie γ de (V, Ψ) de polynôme caractéristique q.

Il s'agit là de résultats bien connus, et l'on renvoie à [5] pour diverses références, notamment à des articles relevant de la théorie des noeuds. La nouveauté dans [5] consiste en l'utilisation de la matrice de Bézout tordue, fournissant une preuve constructive particulièrement simple du théorème 3.3.2. Pour le point (ii), notamment, il suffit de poser $p(T) := q(T) + T^m$, où $m := d/2$ pour obtenir un polynôme symétrique et premier à q (comme on vérifie immédiatement par le calcul de $\mathrm{Res}(p, q)$). La matrice de Bézout tordue $B^*(p/q)$ fournit alors la structure antisymétrique non dégénérée recherchée.

Pour (i), une difficulté supplémentaire apparaît si jamais le polynôme q s'annule en ± 1. En effet le polynôme p cherché pour construire $w := p/q$ doit être premier à q et antiréciproque. Ces conditions peuvent ne pas être compatibles. On résout le problème en remplaçant q par

le quotient de q dans la division par son facteur unitaire de plus grand degré dont les seules racines sont ± 1.

Il est naturel de poser la question de l'existence d'isométries dont on fixe d'autres invariants que le polynôme caractéristique. *Via* la forme bilinéaire associée à la matrice de Bézout tordue, on donne une nouvelle preuve de la caractérisation des isométries d'espaces bilinéaires non dégénérés sur un corps algébriquement clos par sa forme de Jordan (voir [5, Th. 7.5]).

Dans le cas d'une forme bilinéaire symétrique sur un corps quelconque, [5, Cor. 5.3] répond à la question de l'existence d'isométries de polynôme caractéristique *et* de norme spinorielle prescrits. Il s'agit là d'un problème qui apparaît dans le crible de conjugison décrit en §1.2 appliqué à une classe à gauche donné du groupe orthogonal $\mathrm{O}(m,n)(\mathbf{Z})$ (relativement à une forme indéfinie de signature (m,n)) par rapport à son groupe dérivé $\Omega(n,m)(\mathbf{Z})$. Ce sous-groupe est en effet le noyau conjoint du déterminant et de la norme spinorielle. On rappelle qu'étant donné un vecteur v non isotrope dans (V,Ψ) et une réflexion r_v laissant fixe l'orthogonal de $\langle v\rangle$, la *norme spinorielle* de r_v est

$$\mathrm{N}_{\mathrm{spin}}(r_v) = \Psi(v,v) \in k^\times/(k^\times)^2\,.$$

On montre que cette formule permet de définir un morphisme $\mathrm{O}(V,\Psi) \to k^\times/(k^\times)^2$. L'énoncé de [5, Cor. 5.3] est alors le suivant.

Proposition 3.3.3. *Soit $q \in k[t]$ un polynôme unitaire réciproque de degré $d \geqslant 1$ se factorisant sous la forme*

$$q(T) = (T-1)^{v_+}(T+1)^{v_-}\mathcal{Q}_0(T)\,, \qquad \mathcal{Q}_0 \in k[T],\ \mathcal{Q}_0(\pm 1) \neq 0\,.$$

On a alors les résultats suivants.

1. *Si $v_- > 0$, alors il existe un k-espace bilinéaire symétrique non dégénéré de dimension d et une isométrie γ de cet espace de polynôme caractéristique q et de norme spinorielle arbitraire. C'est en particulier le cas si d est impair.*
2. *Si $v_- = 0$ et si γ est une isométrie de polynôme caractéristique q alors $\mathrm{N}_{\mathrm{spin}}(\gamma) = \mathcal{Q}_0(-1)$, modulo les carrés non nuls de k. C'est en particulier le cas si q est séparable et d est pair.*

Par rapport au théorème 3.3.2, l'ingrédient supplémentaire dans la preuve de la proposition est une formule due à Zassenhaus pour la norme spinorielle d'une isométrie de déterminant 1 n'ayant pas -1 pour valeur propre. Cette formule est à rapprocher du lien entre discriminant d'un k espace quadratique (V,Ψ) non dégénéré de dimension $d = 2m$ et discriminant du polynôme caractéristique q d'une isométrie de cet espace :

$$\mathrm{disc}(V,\Psi) = \mathrm{disc}\, q = (-1)^m q(1)q(-1)\,, \tag{3.3.2}$$

modulo les carrés non nuls de k (voir [5, §6]). Cette formule explique notamment le phénomène décrit dans l'exemple 3.0.1.

3.4 Prolongements et « non-réseaux » Zariski-denses

La construction de la matrice de Bézout et de la matrice de Bézout tordue telle qu'on l'a décrite, donne des espaces vectoriels munis de formes bilinéaires aux propriétés remarquables. Les arguments développés laissent penser qu'il est pour l'essentiel possible de reproduire ces constructions sur un anneau. Dans [5, §3.6], on donne quelques exemples explicites de matrices de Bézout tordues construites sur $\mathbf{Z}$. Précisément, les polynômes p et q sont à coefficients entiers ; la matrice de Bézout $B^*(p,q)$ est donc elle aussi à coefficients entiers, ce qui permet de définir trivialement un $\mathbf{Z}$-module bilinéaire (non dégénéré si $(p,q)=1$). La question plus générale de l'énumération des réseaux stables par la forme quadratique $B^*(p,q)$ semble accessible via une étude des facteurs communs des réductions des polynômes p et q modulo un nombre premier quelconque ℓ.

Dans la cas où la forme bilinéaire de Bézout est symétrique et hyperbolique (i.e. de signature $(n-1,1)$, où $\max(\deg p, \deg q) = n$), des travaux récents de Fuchs–Meiri–Sarnak [FMS] montrent la pertinence de cette généralisation au cas où la base est un anneau. Dans *loc. cit.*, ils construisent des familles de groupes hypergéométriques qui sont d'indice infini dans le groupe des points entiers de leur adhérence de Zariski [1] (dans le groupe GL_n ambiant). Ces groupes particuliers ont suscité ces dernières années un fort intérêt en conjonction avec les progrès rapides de la compréhension des phénomènes de croissance et d'expansion (progrès mentionnés dans le chapitre 2). La construction de familles de tels groupes est en général délicate, mais Fuchs–Meiri–Sarnak parviennent à donner des exemples de telles familles en étudiant des groupes hypergéométriques (au sens de Beukers–Heckman) sur $\mathbf{Z}$. Dans la discussion suivant l'énoncé du théorème 3.3.1, on a évoqué la remarque faite dans [5] expliquant que ces groupes hypergéométriques coïncident avec les groupes d'isométries pour certaines structures de Bézout tordues. Ces liens ont pour l'instant été peu exploités mais peuvent sans doute permettre la mise en lumière d'aspects explicites intéressants dans la construction de groupes hypergéométriques d'indice infini dans le groupe des points entiers de leur adhérence de Zariski.

1. Le titre de la section est une suggestion de traduction pour la terminologie anglo-saxonne devenue standard pour désigner ces groupes : « thin groups ».

Chapitre 4

Un crible pour les graphes

Dans la section 2.3.2, on a vu l'importance du recours à une propriété de séparation de valeurs propres (la propriété (τ)), pour étudier *via* le grand crible, le groupe de Galois typique du polynôme caractéristique d'un élément d'un groupe arithmétique donné. Cette propriété d'analyse harmonique admet une traduction en termes d'expansion de graphes de Cayley. Par exemple, l'assertion selon laquelle $\mathrm{SL}_2(\mathbf{Z})$ possède la propriété (τ) relativement à ses sous-groupes de congruence

$$\ker\left(\pi_d\colon \mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/d\mathbf{Z})\right)$$

(conséquence du célèbre théorème de Selberg sur les valeurs propres du Laplacien hyperbolique agissant sur les fonctions de carré intégrable sur $\Gamma(d)\backslash\mathbf{H}$, $d \geqslant 1$), équivaut au fait que, si l'on fixe une partie génératrice symétrique S de $\mathrm{SL}_2(\mathbf{Z})$, la famille de graphes de Cayley $X(\mathrm{SL}_2(\mathbf{Z}/d\mathbf{Z}), \pi_d(S))$, indexée par les entiers $d \geqslant 2$ sans facteur carré, forme une famille de graphes expanseurs. Soit $\varepsilon > 0$; rappelons que si $G = (V, E)$ est un graphe fini non orienté d'ensemble de sommets V et d'ensemble d'arêtes E, on dit que G est un graphe *ε-expanseur* si

$$h(G) := \min_{\substack{A \subseteq V \\ 1 \leqslant |A| \leqslant |V|}} \frac{|\partial A|}{|A|} \geqslant \varepsilon\,,$$

où l'on définit $\partial A := \{(a, b) \in E\colon a \in A,\, b \in V \setminus A\}$. La notion de graphes expanseurs a émergé dans les années 70 avec le développement de la théorie des télécommunications. Une question cruciale et naturelle est celle de la construction explicite d'une *famille* d'expanseurs i.e. une suite de graphes $(G_n) = ((V_n, E_n))$ connexes telle que, pour un certain entier $d \geqslant 1$ et un certain $\varepsilon > 0$,

— chaque G_n est d-régulier,
— $|G_n| \to \infty$ lorsque $n \to \infty$,
— chaque G_n est ε-expanseur.

Le lien entre expansion et écart spectral est donné par l'inégalité suivante. Soit $d \in \mathbf{N}_{\geqslant 1}$ et soit G un graphe connexe d-régulier. On note $(1/d)\mathrm{Adj}(G)$ l'opérateur d'adjacence normalisé de G. Il s'agit d'un opérateur autoadjoint dont on peut ordonner les valeurs propres :

$$1 = \mu_0 > \mu_1 \geqslant \mu_2 \geqslant \cdots \geqslant \mu_{n-1} \geqslant -1\,,$$

où $n = |V|$. On a alors (voir par exemple [DSV, Th. 1.2.3])

$$\frac{d}{2}(1-\mu_1) \leqslant h(G) \leqslant d\sqrt{2(1-\mu_1)}\,.$$

Ce lien entre combinatoire des graphes et analyse harmonique conduit à la question suivante. Est-il possible d'obtenir une majoration pour la constante de grand crible Δ (voir (1.1.2)) dans un cadre où seule est requise la propriété d'expansion d'une famille de graphes associée au problème ? Quelles seraient alors les applications possibles ? Ces questions constituent le point de départ de [6], qui fait un premier pas dans la réduction du grand crible exposé dans le chapitre 1 à son coeur combinatoire. Dans *loc. cit.*, les objets « globaux » considérés sont des graphes. Ceux-ci sont tout de même munis d'une structure de groupe abélien, de sorte que l'on peut facilement leur associer une famille de graphes de Cayley dont les sommets correspondent à une famille de quotients du groupe de départ. L'objectif de [6] est d'étudier les propriétés typiques d'un sous-graphe aléatoire d'un graphe donné. L'idée principale est d'exploiter le fait qu'un graphe de Cayley aléatoire (en un sens que l'on va préciser) est un bon expanseur dès qu'il possède un grand nombre d'arêtes. Cette propriété va permettre la majoration de Δ *via* une estimation de sommes exponentielles analogues à (1.1.5).

4.1 Expansion de graphes de Cayley aléatoires et grand crible

La propriété d'expansion utilisée dans [6] est une conséquence d'un résultat d'Alon–Roichman, dont nous énonçons maintenant une version raffinée due à Christofides–Markström (voir les références dans *loc. cit.*). Il est commode, pour énoncer ce résultat, d'utiliser une notion d'expansion directement liée aux propriétés spectrales des graphes concernés : *l'écart spectral* d'un graphe d-régulier connexe G est

$$\gamma(G) := \min\{1-|\lambda| : |\lambda| \neq 1,\ \lambda \text{ valeur propre de } (1/d)\mathrm{Adj}(G)\}\,.$$

Soit G un groupe abélien et soit $\Lambda \subseteq \mathbf{N}$ un ensemble fixé d'indices. On suppose donnée une famille de sous-groupes $(H_\ell)_{\ell\in\Lambda}$ d'indice fini $n_\ell := [G : H_\ell]$. On note $\rho_\ell \colon G \to G/H_\ell$ la surjection canonique.

Le cadre de crible dans lequel on veut se placer est le crible probabiliste de §1.3. On note que, puisque G est abélien, le triplet $(G, \Lambda, \rho_\ell \colon G \to G/H_\ell)$ est trivialement un cadre de crible de conjugaison. Fixons donc un espace probabilisé $(\Omega, \Sigma, \boldsymbol{P})$. On fixe par ailleurs un réel $\delta \in]0, 1/2]$ et l'on note

$$\psi(\delta) := 2((2-\delta)\log(2-\delta) + \delta\log\delta)^{-1}\,.$$

Pour $\ell \in \Lambda$, on note

$$\kappa(b, \ell; \delta) := \lceil \psi(\delta)(\log n_\ell + b_\ell + \log 2\rceil\,,$$

où $b := (b_\ell)_{\ell\in\Lambda}$ est une suite de $\mathbf{R}_{>0}$ fixée. Pour $\ell \in \Lambda$ et $i \in \{1, \dots, \kappa(b, \ell; \delta)\}$ on considère une variable aléatoire s_i à valeurs dans G/H_ℓ et de distribution uniforme. On suppose que

les s_i sont deux à deux indépendantes et l'on s'intéresse aux propriétés d'expansion de la famille de graphes de Cayley $X_\ell := X(G/H_\ell, \{s_i\} \cup \{s_i^{-1}\})$ où, dans la réunion d'ensembles définissant les arêtes, $1 \leqslant i \leqslant \kappa(b, \ell; \delta)$. On a alors

Théorème 4.1.1 (Alon–Roichman, Christofides–Markström)**.** *Pour tout $\ell \in \Lambda$ la probabilité que $\gamma(X_\ell) < \delta$ est au plus* $\exp(-b_\ell)$.

Hormis ce résultat crucial dans la majoration de la constante de grand crible Δ, d'autres difficultés se posent dans ce cadre plus combinatoire. Elles sont liées au fait que l'on fait peu d'hypothèses de structure. En particulier la propriété de disjonction linéaire (i.e. la surjectivité des morphismes produit $\rho_\ell \times \rho_{\ell'}$, pour $\ell \neq \ell'$), qui en (2.3.2) provient du théorème d'approximatin forte, n'est pas garantie. De même, il n'est pas clair que le graphe de Cayley produit sur $G/H_\ell \times G/H_{\ell'}$ et dont les arêtes sont défnies de façon évidente à partir de celles de X_ℓ et $X_{\ell'}$, soit δ-expanseur sous la seule hypothèse que X_ℓ et $X_{\ell'}$ le sont.

Donnons maintenant les hypothèses et l'énoncé de la contribution théorique principale de [6]. On conserve les notations ci-dessus et l'on souhaite définir une marche aléatoire sur G comme en (2.1.1). Dans les applications on prendra pour G diverses collections de graphes munies d'une loi de groupe. La marche aléatoire va donc produire un graphe « au hasard » dans la collection considérée. Il nous faut définir l'analogue de l'ensemble S utilisé dans le cas (2.1.1). Pour pouvoir appliquer le théorème 4.1.1, l'idée est de reconstruire cet ensemble par relèvement puis recollement des ensembles

$$S_\ell(b, \delta) := \{s_i \colon 1 \leqslant i \leqslant \kappa(b, \ell; \delta)\} \cup \{s_i^{-1} \colon 1 \leqslant i \leqslant \kappa(b, \ell; \delta)\}\,.$$

Cet aspect combinatoire induit des complications absentes dans la cadre du crible probabiliste pour les groupes arithmétiques du chapitre 2. Il faut notamment faire un choix de relèvement dans G pour les $s_i \in G/H_\ell$. Dans [6, §1.2], on définit la notion de *suite locale admissible* pour résoudre cette question. Il s'agit d'une suite $(R_\ell)_{\ell\in\Lambda}$ (associée à la famille $(H_\ell)_{\ell\in\Lambda}$) où chaque R_ℓ est un système de représentants de G/H_ℓ vérifiant :

— $\bigcap_{\ell\in\Lambda} R_\ell = \{1\}$,

— si $\ell, \ell' \in \Lambda$ et $\ell \neq \ell'$, alors $R_\ell \subseteq H_{\ell'}$.

On montre alors ([6, Lem. 1.6]) que s'il existe une suite locale admissible relative à H_ℓ, alors elle est unique. Si l'on fixe $\ell \in \Lambda$ et $1 \leqslant i \leqslant \kappa(b, \ell; \delta)$, et sous l'hypothèse de l'existence d'une suite locale admissible relative à (H_ℓ), on note alors $\tilde{s}_i^{(\ell)}$ l'unique relèvement de s_i qui est élément de R_ℓ, et on définit

$$\tilde{S}_\ell(b, \delta) := \left\{\tilde{s}_1^{(\ell)}, \cdots, \tilde{s}_{\kappa(b_\ell,\ell;\delta)}^{(\ell)}\right\} \cup \left\{(\tilde{s}_1^{(\ell)})^{-1}, \cdots, (\tilde{s}_{\kappa(b_\ell,\ell;\delta)}^{(\ell)})^{-1}\right\}\,.$$

On peut maintenant définir la « partie génératrice » suivante :

$$S(b, \delta) := \prod_{\ell\in\Lambda}{}' \left(\{1\} \cup \tilde{S}_\ell(b_\ell, \delta)\right)\,, \tag{4.1.1}$$

notation signifiant que, à un nombre fini d'exceptions près, le ℓ-ème facteur du membre de droite vaut 1.

On peut maintenant considérer la marche aléatoire $(X_k)_{k\geqslant 0}$ sur G, définie par (2.1.1) avec le choix $S := S(b,\delta)$. Cela sous-entend la donnée d'une suite (p_s) de $\mathbf{R}_{>0}$ indexée par $S(b,\delta)$ définissant la distribution des pas de la marche aléatoire. Ici encore, le fait que l'on remplace le recours à la propriété (τ) relativement à (H_ℓ) par la propriété combinatoire plus faible que constitue le théorème 4.1.1, impose une restriction supplémentaire sur la suite (p_s). Il s'agit de la condition $(\star)$ précédent l'énoncé de [6, Prop. 1.8] et signifiant que la distribution des pas de la marche aléatoire doit être une généralisation de la distribution uniforme (que l'on pourrait considérer si $S(b,\delta)$ est fini). Précisément, fixons un entier $L \geqslant 1$ et le support de crible $\mathcal{L}^* := \Lambda \cap [1,L]$. On suppose que pour tout $\ell, \ell' \in \Lambda_L$ et tout $(s',t') \in S_\ell(b,\delta) \times S_{\ell'}(b,\delta)$, on a

$$\sum_{\substack{s\in S(b,\delta)\\ \rho_{\ell,\ell'}(s)=(s',t')}} p_s \geqslant \frac{1}{\kappa(b_L,L,\delta)}\,. \qquad (\star)$$

Avec ces notations et sous ces hypothèses, on démontre alors le résultat suivant (voir [6, Prop. 1.8]), qui peut être vu comme un analogue combinatoire de [K4, Prop. 3.5] ou [J2, Prop. 6].

Proposition 4.1.2 (Grand crible pour les graphes)**.** — *Soit*

$$C_0 := \sup_{L\in\mathbf{N}_{>0}} \max_{\substack{\ell\neq\ell'\in\Lambda\\ L\leqslant\ell,\ell'\leqslant 2L}} \frac{\#S_\ell(b,\delta)}{\#S_{\ell'}(b,\delta)}\,, \qquad \kappa_N := \kappa(b_N,N,\delta),\ (N\in\mathbf{N}_{>0})\,,$$

et supposons que l'hypothèse $(\star)$ soit vérifiée. Alors pour tout choix d'ensemble criblant $\Theta_\ell \subseteq G/H_\ell$, il existe $\nu > 0$ tel que pour tout $k \geqslant 1$,

$$\boldsymbol{P}(\rho_\ell(X_k)\notin\Theta_\ell,\ \forall \ell\in\Lambda_L) \leqslant \boldsymbol{P}(C_0=\infty) + \sum_{\ell\in\Lambda_L}\exp(-b_\ell) + \left(1+\left(\sum_{\ell\in\Lambda_L} n_\ell\right)(1-\kappa_{2L}^{-2}\nu)^k\right)\left(\sum_{\ell\in\Lambda_L}\frac{\#\Theta_\ell}{n_\ell}\right)^{-1},$$

où $L \geqslant 1$ est un entier fixé, et la constante ν ne dépend que de C_0, de l'ensemble $S(b,\delta)$, et de la distribution des pas de la marche aléatoire (i.e. de la suite (p_s)).

Dans les travaux antérieurs cités [K4, Prop. 3.5] ou [J2, Prop. 6], les quantités $\boldsymbol{P}(C_0 = \infty)$ et $\sum_{\ell\in\Lambda_L}\exp(-b_\ell)$ n'ont pas d'analogue. La seconde quantité est liée à l'application du théorème 4.1.1, alors que la première provient de la difficulté, déjà mentionnée, de la construction d'un graphe de Cayley expanseur « produit » à partir de deux graphes de Cayley expanseurs. (Ainsi posée, la question est triviale : précisément on souhaite que l'écart spectral pour le graphe de Cayley produit soit de l'ordre de celui des deux graphes initiaux, et ce uniformément sur la famille de graphes considérée.) Dans le cas où G est abélien, on a une description simple des valeurs propres de $\mathrm{Adj}(X(G,S))$ en termes des caractères de G, ce qui permet une résolution partielle mais suffisante de la question (voir [6, Lem. 1.3]).

Le fait que l'on puisse majorer efficacement $\boldsymbol{P}(C_0 = \infty)$ est une conséquence de principes de concentration assurant que les ensembles $S_\ell(b,\delta)$ sont deux à deux de taille comparable

avec grande probabilité. Ces principes prennent différentes formes suivant que $n_\ell \geqslant \kappa_\ell$ ou non. Ils font l'objet de [6, Lem. 1.4]. Enfin, le troisième terme du membre de droite dans l'inégalité de la proposition 4.1.2 est le résultat de l'adaptation de la preuve [K4, Prop. 3.5] dans le cas favorable où l'expansion des graphes de Cayley quotient est garantie et où l'on a $C_0 < \infty$. On note l'apparition du facteur « parasite » $(1 - \kappa_{2L}\nu)^k$ qui, dans les applications, explique pourquoi l'on ne parvient pas à obtenir une décroissance exponentielle de la probabilité des évènements rares considérés.

4.2 Applications combinatoires

Décrivons maintenant certaines des applications de la proposition 4.1.2 que l'on obtient dans [6, §2–4].

(i) Soit $\mathcal{G}$ le graphe dont l'ensemble des sommets est $\mathbf{Z}^2$ et où deux sommets (a, b) et (c, d) sont voisins si $|a-c|+|b-d| = 1$. Notons G l'ensemble des sous-graphes couvrant de $\mathcal{G}$. La différence symétrique appliquée aux ensembles d'arêtes permet de définir une loi de groupe abélien sur G. Soit $\Lambda := \mathbf{N}_{\geqslant 1}$; pour chaque $\ell \in \Lambda$, on note $\mathcal{C}_\ell$ un carré de taille 3×3 dans $\mathbf{Z}^2$ vu comme un graphe dont les sommets sont les points de $\mathbf{Z}^2$ renfermés par le carré, et dont les arêtes sont celles de $\mathcal{G}$ qui sont intérieures au carré ou qui constituent les côtés gauche et inférieur du carré. On choisit et on ordonne les $\mathcal{C}_\ell$ de sorte à ce qu'ils constituent une partition de $\mathcal{G}$. Pour chaque $\ell \in \Lambda$, on pose $H_\ell := \mathcal{G} \cap \mathcal{C}_\ell$. On s'intéresse, pour un sous-graphe au hasard H de $\mathcal{G}$ (i.e. un élément au hasard de G) à la propriété $\mathcal{P}$ suivante : H contient un sous-graphe donné (pour fixer les idées on prend pour sous-structure prescrite, un 4-cycle).

(ii) Soit $\mathcal{G} = (\mathbf{N}, E)$ le graphe complet infini dénombrable. Fixons un entier $c \geqslant 3$ et notons $\mathcal{C}$ l'ensemble des fonctions $f\colon E \to \mathbf{Z}/c\mathbf{Z}$ muni de la structure de groupe induite par celle de $\mathbf{Z}/c\mathbf{Z}$. On choisit $\Lambda = \mathbf{N}$ et une partition $(I_\ell)_{\ell\in\Lambda}$ de Λ, où chaque I_ℓ est fini. Pour $\ell \in \Lambda$, on note E_ℓ l'ensemble des arêtes de $\mathcal{G}$ dont les extrémités sont dans I_ℓ et l'on définit C_ℓ comme étant l'ensemble des $f \in \mathcal{C}$ nulles en dehors de E_ℓ. La collection de sous-groupes d'indice fini (H_ℓ) de G que l'on fixe est

$$H_\ell := \{f \in \mathcal{C}\colon f_{|E_\ell} \equiv 0\}\,.$$

La propriété $\mathcal{P}$ que l'on souhaite détecter pour une coloration au hasard $f \in \mathcal{C}$ est la présence d'un triangle monochromatique comme sous-graphe de $\mathcal{G}$.

(iii) Soit G l'ensemble des parties de $\mathcal{G} := \mathbf{Z} \setminus \{0\}$. La différence symétrique Δ munit G d'une loi de groupe abélien. Posons $\Lambda := \mathbf{N}_{\geqslant 1}$, et $I_\ell := \{-\ell, \ell\}$, $C_\ell := \{\text{sous-ensembles de } I_\ell\}$ pour chaque $\ell \in \Lambda$. La suite (H_ℓ) que l'on choisit est donnée, pour $\ell \in \Lambda$, par

$$H_\ell := \{A \subseteq \mathbf{Z} \setminus \{0\}\colon A \cap I_\ell = \emptyset\}\,.$$

Dans ce cas, la propriété $\mathcal{P}$ testée pour une partie aléatoire A de $\mathbf{Z}\setminus\{0\}$, est l'existence d'une sous-partie de A dont la somme des éléments est nulle.

Par des arguments élémentaires, on étudierait facilement la propriété $\mathcal{P}$ dans chacun des cas (i)–(iii) ci-dessus en utilisant la notion naturelle de probabilité discrète sur une partie finie bien choisie $\mathcal{H}$ de $\mathcal{G}$. Dans [6], la question que l'on pose est différente et plus délicate, puisque la notion « d'élément au hasard » correspond à la marche aléatoire (2.1.1) définie en utilisant l'ensemble $S := S(b, \delta)$, et puisque l'on ne fait aucune hypothèse de finitude sur la structure sous-jacente.

Les résultats que l'on obtient (voir [6, Th. 2.2, Th. 3.3, Th. 3.4]) sont les suivants.

Théorème 4.2.1. *En conservant les notations ci-dessus, on a, dans les cas* (i)–(iii)*,*

1. *(C_ℓ) est une suite locale admissible de G relativement à (H_ℓ),*
2. *soit (X_k) la marche aléatoire sur G définie par (2.1.1) en utilisant l'ensemble $S(b, \delta)$ (voir (4.1.1)), avec $\tilde{S}_\ell(b, \delta) \subseteq C_\ell$ pour chaque $\ell \in \Lambda$. On suppose l'hypothèse $(\star)$ satisfaite et l'on fixe $\varepsilon > 0$. Alors il existe une constante C_ε telle que pour tout $k \geqslant 1$,*

$$\boldsymbol{P}(X_k \text{ ne satisfait pas } \mathcal{P}) \leqslant C_\varepsilon k^{-1/2+\varepsilon}.$$

La constante C_ε ne dépend que de ε, C_0, de $S(b, \delta)$ et de la suite (p_s) dans les cas (i) *et* (iii)*. Dans le cas* (ii)*, la constante C_ε ne dépend que de ces quatre paramètres et de c.*

Outre le recours à la proposition 4.1.2, la preuve requiert l'évaluation des quantités $\sum_{\ell \in \Lambda_L} \#\Theta_\ell / n_\ell$, où les Θ_ℓ forment une famille d'ensembles criblants permettant de détecter la propriété $\mathcal{P}$ dans chacun des cas (i)–(iii). Ces calculs sont aisés et correspondent à l'approche intuitive déjà mentionnée plus haut, puisqu'ils relèvent de dénombrements dans des structures finies simples.

L'application (i) peut être vue comme un « cas test » qui a motivé l'adaptation du grand crible probabiliste de §1.3 aux graphes. Les applications (ii) et (iii) sont plus proches de sujets centraux en théorie extrêmale des graphes. Ils peuvent par exemple être vus comme des approches effectives de la théorie de Ramsey [R1], dont la philiosophie générale prédit l'existence de sous-structures ordonnées dans toute structure combinatoire suffisamment grande. Dans [6, §3 et 4], on démontre des résultats généralisant les cas (ii) et (iii) du théorème 4.2.1, et l'on discute les liens avec les versions originales et généralisées au cas de structures infinies du théorème de Ramsey.

4.3 Perspectives pour l'étude des propriétés algébriques des polynômes de graphes

La théorie des graphes regorge de fonctions polynomiales dont l'évaluation peut par exemple permettre le comptage de certaines structures ou de tester certaines propriétés. Les propriétés algébriques de ces polynômes sont en général méconnues, et la combinaison du grand crible pour les graphes présenté dans ce chapitre et de l'étude du groupe de Galois générique de polynômes caractéristiques aléatoires dont le chapitre 2 fait l'objet, peut constituer une stratégie possible pour attaquer ces questions.

Plus précisément, intéressons nous à un cas simple de polynôme de $\mathbf{Z}[T]$ associé à un graphe G donné et contenant beaucoup d'informations combinatoires sur G : son *polynôme chromatique*. Il s'agit du polynôme χ_G tel que, pour tout $n \geqslant 1$, l'évaluation de χ_G en n donne le nombre de colorations des sommets sans voisins deux à deux de même couleur utilisant au plus n couleurs. Le fait qu'un tel polynôme existe est élémentaire, tout comme le fait que $\chi_G(n) = 0$ si n est strictement inférieur au nombre chromatique de G. Dans [C1], Cameron pose la question des propriétés algébriques de la « partie intéressante » de χ_G (i.e. du quotient que l'on note χ_G^{prim} de χ_G par le produit des facteurs linéaires $T - i$ où i parcourt l'ensemble des entiers $\geqslant 1$ et strictement inférieurs au nombre chromatique de G). Certaines propriétés des racines complexes de χ_G^{prim} sont connues (par exemple Sokal montre que, lorsque G varie, ces racines forment une partie dense de $\mathbf{C}$) ; cependant les questions « inverses » consistant à savoir si, par exemple, un entier algébrique donné est racine d'un polynôme χ_G^{prim} pour un certain G, sont largement ouvertes.

Dans la droite ligne du type de résultat exposé dans le chapitre 2, Cameron énonce également dans [C1] la conjecture suivante

Conjecture 4.3.1 ("Cameron's wild speculation")**.** *Il existe un espace probabilisé (à définir), tel que pour presque tout graphe fini non orienté connexe G, le groupe de Galois du corps de décomposition de χ_G^{prim} sur $\mathbf{Q}$ est isomorphe à $\mathfrak{S}_{r(G)}$, où $r(G) := \deg \chi_G^{\text{prim}}$.*

Peu de résultats partiels en direction de cette conjecture sont connus. Mentionnons tout de même le résultat principal de [MdMN] affirmant que le polynôme de Tutte (il s'agit d'un polynôme de $\mathbf{Z}[X, Y]$ dont une spécialisation redonne le polynôme chromatique) d'un matroïde connexe est irréductible. Dans [BCM], les auteurs étudient des questions de maximalité du groupe de Galois pour des généralisations multivariées du polynôme de Tutte. Le théorème d'irréductibilité de Hilbert et d'autre méthodes de spécialisation jouent un rôle crucial dans *loc. cit.* ; la transposition de ces techniques au cas du polynôme chromatique semblent donc sans espoir. La conjecture 4.3.1 reste par conséquent largement inexplorée et les méthodes de grand crible dans des variantes combinatoires encore à définir semblent constituer une approche intéressante.

Chapitre 5

Indépendance de zéros de fonctions L et courses de nombres premiers sur les corps de fonctions

Dans ce chapitre final, on présente les travaux [1] et [2] dont l'objet est d'étudier un analogue géométrique du phénomène appelé *bias de Chebyshev* relatif, dans sa version originale, aux nombres premiers. Dans une lettre datée de 1853 [C4], Chebyshev énonce la propriété frappante suivante : pour « la plupart » des réels $x \geqslant 2$ on a l'inégalité

$$\pi(x,4,1) < \pi(x,4,3)\,,$$

où si q est un entier $\geqslant 1$ et a est un entier inversible modulo q, on note $\pi(x,q,a) := \#\{p \leqslant x\colon p \equiv a \,(\mathrm{mod}\, q)\}$. Cet énoncé n'est rigoureux que si l'on définit précisément ce que l'on entend par « la plupart ». Plus généralement, fixons un entier $q \geqslant 1$ et des classes inversibles $a_1, \ldots, a_r$ modulo q. On note

$$P(q; a_1, \ldots, a_r) := \{x \geqslant 2\colon \pi(x,q,a_1) < \pi(x,q,a_2) < \cdots < \pi(x,q,a_r)\}\,.$$

Rubinstein et Sarnak font l'étude systématique, dans [RS], de généralisations de questions issues de l'assertion de Chebyshev. Ils répondent aux questions suivantes : l'ensemble $P(q; a_1, \ldots, a_r)$ est-il non vide ? S'il est non vide, peut-on le mesurer, et quelle est sa mesure ?

Wintner avait déjà montré dans les années 1940, que la bonne notion de mesure pour les questions de biais de Chebyshev, est la densité logarithmique définie, pour $P \subseteq \mathbf{R}$ par

$$\overline{\delta}(P) := \limsup_{x\to\infty} \frac{1}{\log x} \int_{[2,x]\cap P} \frac{\mathrm{d}t}{t}\,, \qquad \underline{\delta}(P) := \liminf_{x\to\infty} \frac{1}{\log x} \int_{[2,x]\cap P} \frac{\mathrm{d}t}{t}\,,$$

et, si $\overline{\delta}(P)$ et $\underline{\delta}(P)$ existent et coïncident, alors $\delta(P)$ est leur valeur commune.

Les résultats théoriques et numériques obtenus par Rubinstein et Sarnak sont conditionnels à l'Hypothèse de Riemann pour les fonctions L des caractères de Dirichlet primitifs modulo q ; beaucoup de ces résultats sont aussi conditionnels à l'énoncé suivant (appelé Grand Simplicity Hypothesis dans *loc. cit.*, et plus couramment LI (pour Linear Independence) dans la littérature).

Conjecture 5.0.1 (LI). *La famille*

$$\{\gamma \geqslant 0 \colon L(1/2 + i\gamma, \chi) = 0,\ \chi \text{ caractère de Dirichlet primitif modulo } q\}$$

vue comme multi-ensemble de nombres réels, est libre sur $\mathbf{Q}$.

Cette assertion semble hautement hypothétique. Mentionnons par exemple que l'on ne sait pas si l'espace vectoriel engendré par l'ensemble des parties imaginaires γ ci-dessus est de dimension > 1 sur $\mathbf{Q}$. Par ailleurs cette conjecture implique trivialement la non annulation en $1/2$ de $L(s, \chi)$ et la simplicité des zéros critiques de $L(s, \chi)$.

La question du bias de Chebyshev, dans sa forme originale, peut être vue comme la comparaison du comportement asymptotique de la distribution des nombres premiers dans les progressions arithmétiques (question à laquelle le théorème des nombres premiers dans les progressions arithmétiques répond complètement) par rapport à la distribution des « tranches initiales » des nombres premiers dans les progressions arithmétiques. On peut définir des analogues de cette comparaison, dès que l'on dispose d'une suite indexée par les nombres premiers dont on connait le comportement asymptotique [1]. Ainsi, la résolution de la conjecture de Sato–Tate ([CHT], [HSBT]) suggère de définir le problème de biais de Chebyshev suivant. Soit $E/\mathbf{Q}$ une courbe elliptique ; pour p un premier de bonne réduction, on adopte la notation standard $a_p(E) := \#E(\mathbf{F}_p) - (p+1)$, où $E(\mathbf{F}_p)$ désigne le nombre de points $\mathbf{F}_p$-rationnels de la réduction de E modulo p. Mazur suggère dans [M] d'étudier la fonction

$$T(t) = \#\{p \leqslant t \colon p \text{ de bonne réduction}, a_p > 0\} - \#\{p \leqslant t \colon p \text{ de bonne réduction}, a_p < 0\}\,;$$

ce qui constitue un analogue clair au problème initial de Chebyshev. Dans [S1], Sarnak donne un cadre natruel d'étude pour la question de Mazur et met en évidence le rôle joué par les zéros des fonctions L des puissances symétriques de E. Là encore, l'approche est conditionnelle à une hypothèse de Riemann et à une hypothèse d'indépendance linéaire des zéros pour ces fonctions L.

Sarnak remarque également que, contrairement à la fonction T, le signe de la fonction sommatoire des $a_p(E)/\sqrt{p}$ peut être étudié à partir de la seule fonction $L(E, s)$, sans recours aux puissance symétriques supérieures. Fiorilli poursuit dans [F] le travail initié par Sarnak et pose la question de l'existence de courbes ellitpiques sur $\mathbf{Q}$ donnant lieu à un biais de Chebyshev « extrême » (i.e. proche de 1). Conditionnellement à une hypothèse de Riemann et à une hypothèse de multiplictité bornée pour les zéros non réels de $L(E, s)$ (hypothèse BM de [F]), Fiorilli montre qu'un tel biais apparaît à condition que le rang analytique de la courbe elliptique E soit significativement plus grand que $\sqrt{\log N_E}$, où N_E désigne le conducteur de E.

Dans [1], on transpose le cadre d'étude proposé par Sarnak aux courbes elliptiques sur un corps de fonctions sur un corps fini $\mathbf{F}_q$. En supposant que les courbes elliptiques considérées ne sont pas isotriviales, les fonctions L apparaissant sont des polynômes, et l'hypothèse de

1. Dans la terminologie anglo-saxonne, on parle souvent de *prime number races* pour désigner la question du bias de Chebyshev et ses généralisations, ce qui explique l'intitulé du chapitre.

Riemann est un résultat inconditionnel conséquence des travaux de Grothendieck, Deligne, et leurs collaborateurs. La question de l'indépendance linéaire des zéros de ces fonctions L, peut également, dans une certaine mesure, être traité inconditionnellement. C'est l'objet de [2]. Pour ce point précis, on aura une nouvelle fois recours à la méthode de grand crible du chapitre 1. Plus précisément on utilise dans [2] une généralisation du crible pour les morphismes de Frobenius initié dans [K3] (voir aussi [K4, Chap. 8]). Notons que l'étude du bias de Chebyshev classique (comme exposé dans [RS]) a été adapté aux corps de fonctions par Cha dans [C2].

Les deux sections qui suivent présentent respectivement les travaux de [1] et [2].

5.1 Biais de Chebyshev pour les courbes elliptiques sur les corps de fonctions

Soit $\mathbf{F}_q$ un corps fini de caractéristique $\geqslant 5$ et soit $C/\mathbf{F}_q$ une courbe projective lisse et géométriqement irréductible. Soit $K = \mathbf{F}_q(C)$ le corps de fonctions de C et soit E/K une courbe elliptique d'invariant j non constant. Pour v une place de K de bonne réduction pour E, on note a_v la trace du Frobenius en v, dont on sait qu'elle vérifie la borne de Hasse :

$$|a_v| \leqslant 2q^{\deg v/2}\,,$$

de sorte que l'on peut écrire $a_v = 2q^{\deg v/2}\cos(\theta_v)$, pour un unique $\theta_v \in [0,\pi]$. On s'intéresse dans [1] à la fonction sommatoire

$$T_E(X) := -\frac{X}{q^{X/2}} \sum_{\substack{\deg v \leqslant X \\ v \text{ bon}}} 2\cos(\theta_v) \quad (X \geqslant 1)\,; \tag{5.1.1}$$

analogue [2] de la fonction sommatoire dont Sarnak propose l'étude dans [S1]. Pour comprendre le signe de la fonction $T_E(X)$, on définit les densités

$$\overline{\delta}(E) := \limsup_{M\to\infty} \frac{1}{M} \sum_{\substack{X\leqslant M \\ T_E(X)>0}} 1\,, \qquad \underline{\delta}(E) := \liminf_{M\to\infty} \frac{1}{M} \sum_{\substack{X\leqslant M \\ T_E(X)>0}} 1\,,$$

et l'on note $\delta(E)$ la valeur commune à $\overline{\delta}(E)$ et $\underline{\delta}(E)$ si ces quantités coïncident.

Par ailleurs, l'hypothèse selon laquelle l'invariant j de E/K est non constant assure, d'après le théorème de pureté de Deligne [D1, §3.2.3], que la fonction L de E/K (voir [2, §1.2] pour des rappels sur la définition et les propriétés désormais classiques de $L(E/K,T)$, et plus généralement de $L(\mathrm{Sym}^n E/K,T)$) :

$$L(E/K,T) = \prod_{i=1}^{N_{E/K}} (1 - q\mathrm{e}^{i\theta_j}T) \in 1 + T\mathbf{Z}[T]\,,$$

2. Notons que le facteur de normalisation $X/q^{X/2}$ provient de l'analogue du théorème des nombres premiers dans l'anneau de fonctions régulières $\mathbf{F}_q[C]$.

où $N_{E/K}$ est donné explicitement en fonction du genre de C et du degré du conducteur d'Artin de E/K, et $\theta_j \in [0, 2\pi[$ pour tout j.

Notre objectif dans [1] est d'une part de décrire le cas « générique », i.e. d'étudier l'existence et le comportement typique de $\delta(E)$ pour une courbe elliptique au hasard E/K, et d'autre part de considérer une famille particulière de courbes elliptiques E/K pour laquelle la fonction $L(E/K, T)$ peut être calculée explicitement. Dans le premier cas, on s'attend à ce que E/K vérifie un analogue de la propriété LI. Dans le second cas, on se concentre sur la famille de courbes elliptiques de Ulmer (voir [U]) pour laquelle la propriété LI n'est clairement pas satisfaite. On démontre des comportements très variés pour la fonction $\delta(E)$ attachée aux courbes de cette famille. En particulier, les résultats de [S1] et [F] pour les corps de nombres ne permettent pas en général de prédire la situation sur les corps de fonctions.

5.1.1 Un théorème central limite dans le cas générique

Précisons quel est le bon analogue de la propriété LI définie dans la conjecture 5.0.1.

Définition 5.1.1 (LI pour $L(E/K, T)$)**.** On conserve les notations et hypothèses ci-dessus et l'on note $\gamma_j := qe^{i\theta_j}$, pour $j = 1, \ldots, N_{E/K}$, les inverses des zéros de $L(E/K, T)$. Soit $\varepsilon(E/K) = \pm 1$ le signe de l'équation fonctionnelle pour $L(E/K, T)$ dont on rappelle la forme (voir par exemple [2, Th. 1.1], et les références qui y sont mentionnées) :

$$L(E/K, T) = \varepsilon(E/K)(qT)^{N_{E/K}} L(E/K, 1/(q^2T)). \tag{5.1.2}$$

On définit l'ensemble des *zéros imposés* de E/K comme étant :

$$\mathrm{FZ}(E/K) := \begin{cases} \{\varepsilon(E/K)q\} & \text{si } N_{E/K} \text{ est impair,} \\ \{q, -q\} & \text{si } N_{E/K} \text{ est pair et } \epsilon(E/K) = -1, \\ \{\} & \text{sinon.} \end{cases} \tag{5.1.3}$$

Quitte à renuméroter, soit $\{\theta_1, ..., \theta_k\}$ le multi-ensemble des arguments des γ_j se trouvant dans $[0, \pi]$ et qui ne correspondent pas à un zéro imposé de E/K. On dit que E/K vérifie la propriété *d'indépendance linéaire* (LI) si le multi-ensemble

$$\left\{\theta_j/\pi \colon 0 < \theta_j \leq \pi,\, j \in \{1, \ldots k\}\right\} \cup \{1\}$$

forme une partie libre sur $\mathbb{Q}$.

Dans cette définition, l'idée sous-jacente est simple. Dire que E/K satisfait LI, sous-entend que l'on ignore toute relation multiplicative triviale entre les zéros de $L(E/K, T)$, notamment celles provenant de la conjugaison complexe et les zéros imposés $\gamma = \pm q$, de même que le zéro $\gamma = q$ provenant de l'annulation de $L(E/K, T)$ au point central, et donnant alors lieu à un rang analytique strictement positif pour E/K. Ces restrictions sont analogues au fait que l'on suppose la partie imaginaire des zéros critiques positive dans la conjecture 5.0.1.

Dans [2] on montre qu'en moyenne dans des familles bien choisies, une propriété plus forte que LI est vraie. Commençons par énoncer [1, Th. 1.2] qui donne l'espérance et la variance de la variable aléatoire attachée à la distribution limite de la fonction $T_E(X)$, ainsi qu'un théorème central limite si la condition LI est satisfaite. Rappelons que l'on dit qu'une fonction $S\colon \mathbf{N}_{\geqslant 1} \to \mathbf{R}$ admet une *distribution limite* s'il existe une mesure borélienne μ sur $\mathbf{R}$ telle que pour toute fonction continue lipschitzienne bornée $f\colon \mathbf{R} \to \mathbf{R}$, on a

$$\lim_{M\to\infty} \frac{1}{M} \sum_{X=1}^{M} f\left(S(X)\right) = \int_{\mathbb{R}} f(t)\mathrm{d}\mu(t). \tag{5.1.4}$$

Théorème 5.1.2. *En conservant les notations ci-dessus, on a :*

(i) La fonction $T_E(X)$ admet une distribution limite. Soit X_E la variable aléatoire associée. Son espérance et sa variance sont respectivement donnés par

$$\mathbb{E}[X_E] = \frac{\sqrt{q}}{\sqrt{q}-1}\left(\mathrm{rang}(E/K) - \frac{1}{2}\right),$$

et

$$\mathbb{V}[X_E] = \frac{1}{4}\left(\frac{\sqrt{q}}{\sqrt{q}+1}\right)^2 + \sum_{\theta_j\neq 0}^{*} \frac{m(\theta_j)^2}{|1-q^{-1/2}\mathrm{e}^{-i\theta_j}|^2},$$

où $m(\theta_j)$ est la multiplicité de θ_j, et la sommation $(\sum^*)$ porte sur les $\theta_j \neq 0$ comptés sans multiplicité.

(ii) Soit $\{E/K\}$ une famille de courbes elliptiques de conducteur non borné, dont tous les éléments satisfont LI dans le sens de la définition 5.1.1, et telle que $\mathrm{rang}(E/K) = o(\sqrt{N_{E/K}})$ lorsque $N_{E/K} \to \infty$. Alors la variable aléatoire

$$\sqrt{\frac{q-1}{q}} X_E/\sqrt{N_{E/K}}$$

converge en loi vers la distribution gaussienne centrée réduite lorsque $N_{E/K} \to \infty$. Par conséquent $\delta(E) \to \frac{1}{2}$ lorsque $N_{E/K} \to \infty$.

Dans [1], on démontre une version plus forte de ce résultat. Une généralisation du point (i) fait l'objet de [1, Cor. 2.7] : on peut remplacer, dans la définition de T_E, la fonction cos par une fonction $V\colon [0,\pi] \to \mathbf{R}$ « suffisamment régulière » (i.e. orthogonale à 1 pour le produit scalaire usuel de $L^2([0,\pi])$ et satisfaisant une condition de décroissance, voir [1, Prop. 2.6]). On montre que la fonction $T_V(X)$ obtenue vérifie encore une assertion du type 5.1.2(i).

Pour ce qui est du point (ii), on en établit une forme plus précise en donnant une borne pour la vitesse de convergence de la variable aléatoire considérée vers la gaussienne centrée réduite. Il s'agit de [1, Th. 4.5] (voir aussi [1, Cor. 4.6] pour une version de la dernière assertion de (ii) avec un terme d'erreur explicite).

La preuve du théorème 5.1.2 et de ses généralisations utilise principalement deux ingrédients. D'abord on a recours à des techniques probabilistes (version discrète du théorème de Kronecker–Weyl, inégalité de Berry–Esseen,...). Tout comme dans le cas classique [RS], l'hypothèse LI

est cruciale pour calculer explicitement la fonction caractéristique de la variable aléatoire X_E (voir [1, (60)]). Par ailleurs on établit une formule explicite ([1, Th. 2.1]), reliant une sommation sur les places v de K à une sommation sur les zéros des fonctions L de puissances symétriques $L(\mathrm{Sym}^n E/K, T)$.

5.1.2 Étude de la famille de Ulmer

Dans [U], Ulmer construit des courbes elliptiques de grand rang sur un corps de fonctions. Il considère notamment la famille :

$$E_d \colon y^2 + xy = x^3 - t^d \,,$$

sur le corps de fonctions rationnel $\mathbf{F}_q(t)$. Le paramètre $d \geqslant 1$ et la caractéristique p doivent satisfaire $d \mid p^n+1$, pour un certain $n \geqslant 1$. Outre le cas générique décrit par le théorème 5.1.2, on s'intéresse dans [1] au comportement de la fonction $T_E(X)$ définie par (5.1.1) dans le cas où $E = E_d$ (on notera alors, pour simplifier, $T_d(X) := T_{E_d}(X)$). On montre en particulier que divers choix de paramètres conduisent à des valeurs très variées pour $\underline{\overline{\delta}}(E_d)$. Notre approche repose sur le calcul explicite de la fonction T_d qui est rendu possible par la connaissance précise de la fonction $L(E_d/\mathbf{F}_q(t), T)$ et par la formule explicite [1, Th. 2.1] déjà mentionnée et sa conséquence [1, Cor. 2.8]. Des travaux de Ulmer, on déduit en effet facilement le résultat suivant (voir [1, Prop. 3.1]).

Proposition 5.1.3 (Calcul de $L(E_d/\mathbf{F}_q(t), T)$)**.** *Sous les hypothèses ci-dessus, on a*

$$L(E_d/\mathbf{F}_q(t), T) = (1 - qT)^{\varepsilon_d} \prod_{\substack{e \mid d \\ e \nmid 6}} \left(1 - (qT)^{o_e(q)}\right)^{\phi(e)/o_e(q)} \,,$$

où la fonction ϕ est l'indicatrice d'Euler et $o_e(q)$ est l'ordre (multiplicatif) de q dans $(\mathbf{Z}/e\mathbf{Z})^*$. De plus, ε_d est défini comme suit :

$$\varepsilon_d := \begin{cases} 0 & \text{si } 2 \nmid d \text{ ou } 4 \nmid q-1 \\ 1 & \text{si } 2 \mid d \text{ et } 4 \mid q-1 \end{cases} + \begin{cases} 0 & \text{si } 3 \nmid d \\ 1 & \text{si } 3 \mid d \text{ et } 3 \nmid q-1 \\ 2 & \text{si } 3 \mid d \text{ et } 3 \mid q-1 \end{cases} .$$

En particulier le rang de $E_d/\mathbb{F}_q(t)$ est donné par :

$$\mathrm{rang}(E/\mathbf{F}_q(t)) = \varepsilon_d + \sum_{\substack{e \mid d \\ e \nmid 6}} \frac{\phi(e)}{o_e(q)} \,.$$

Les résultats sur les comportements divers de $\underline{\overline{\delta}}(E_d)$ font l'objet de [1, Th. 1.5, Th. 1.7, Th. 1.8]. Citons les deux premeirs.

Théorème 5.1.4 (Exemples de biais extrêmes)**.** *Pour la famille $\{E_d/\mathbb{F}_q(t)\}$, les cas suivants se produisent.*

(i) *Supposons $q \geqslant 3$, et supposons que*
— *soit d est divisible par 2 et $q \equiv 1 \bmod 4$,*
— *soit d est divisible par 3.*
Alors on a $T_d(X) > 0$ pour X assez grand, et en particulier $\underline{\delta}(E_d) = \overline{\delta}(E_d) = 1$.

(ii) *Si $q = p^k$ avec p assez grand et $d = p^n + 1$ pour un certain $1 \leqslant n \leqslant \mathrm{e}^{q^{\frac{1}{2}}/2}$ satisfaisant $n \equiv 0 \bmod k$, alors $T_d(X) > 0$ pour X assez grand, et en particulier $\underline{\delta}(E_d) = \overline{\delta}(E_d) = 1$.*

(iii) *Soit $\varepsilon > 0$. Il existe des nombres premiers $d \geqslant 3$ et p tels que p est une racine primitive modulo d, et tels que si l'on pose $q := p^{\frac{d-1}{2}+1}$, alors la courbe elliptique associée E_d est de rang analytique 1 (resp. 2) si $(d-1)/2$ est pair (resp. impair). De plus*

$$0 < \underline{\delta}(E_d) \leqslant \overline{\delta}(E_d) < \varepsilon\,.$$

Notons qu'une conséquence des travaux de Rubinstein et Sarnak permet de démontrer que l'on a toujours $\delta(E) < 1$ (si cette densité existe), pour une courbe elliptique sur $\mathbf{Q}$. De ce point de vue, les assertions (i) et (ii) sont donc surprenantes. Outre les arguments déjà mentionnés, la preuve de (iii) utilise un théorème de Goldfeld ([G]) assurant qu'il y a une proportion positive de couples de premiers (d, p) tels que p est une racine primitive modulo d. Revenant à la comparaison avec les corps de nombres, notons que pour une courbe elliptique $E/\mathbf{Q}$, Sarnak démontre dans [S1] sous une hypothèse de Riemann et une hypothèse d'indépendance des zéros pour $L(E, s)$, que l'on doit avoir $\delta(E) > 1/2$ dès que le rang analytique de E est au moins 1. Là encore, le point (iii) met en évidence un contraste marqué entre le cas des corps de nombres et celui des corps de fonctions.

Théorème 5.1.5 (Exemples d'absence de biais)**.** *Soit $p \equiv 3 \bmod 4$ et soit $d \geqslant 5$ un diviseur de $p^2 + 1$. On pose $q := p^{4k+1}$ pour un entier $k \geqslant 1$. Alors le rang analytique de E_d vaut $(d-1)/4$ ou $(d-2)/4$ suivant que d est congru à 1 ou 2 modulo 4. De plus :*

$$\underline{\delta}(E_d) = \overline{\delta}(E_d) = \frac{1}{2}\,.$$

La dernière partie de la proposition 5.1.3 donne, sous les hypothèses du théorème ci-dessus, $\mathrm{rang}(E/\mathbf{F}_q(t)) \geqslant (p^2-1)/4$, quantité significativement plus grande que la racine carrée du conducteur $N_{E_d/K}$ qui est de l'ordre de p (voir [U, §10.2]). Dans cette situation, les travaux de Fiorilli [F] montrent que, sur les corps de nombres, on doit alors s'attendre à avoir $\overline{\delta}(E_d)$ proche de 1, pour peu que l'hypothèse BM de *loc. cit.* soit satisfaite. Tout analogue de cette condition est cependant fortement mis en défaut par $L(E_d/\mathbf{F}_q(t), T)$, comme on peut le voir directement grâce à la formule de la proposition 5.1.3.

Enfin dans le cas d'une courbe elliptique $E/\mathbf{Q}$, Sarnak montre dans [S1] que, conditionnellement à une hypothèse de Riemann et une hypothèse d'indépendance linéaire des zéros pour $L(E, s)$, on a toujours $\delta(E) \neq 1/2$.

Les deux théorèmes ci-dessus montrent que $1/2$ et 1 sont des valeurs possibles pour la fonction δ et qu'il existe des valeurs de $\underline{\delta}(E_d)$ arbitrairement proches de 0. On peut obtenir

plus d'informations sur les valeurs possibles pour $\underline{\delta}(E_d)$ et $\overline{\delta}(E_d)$. Tout d'abord [1, Cor. 3.3] permet de montrer que l'on a toujours $\underline{\delta}(E_d) \neq 0$. Par ailleurs, [1, Th. 1.8] affirme que tout rationnel de la forme $1/(2m)$, $m \geqslant 1$, est arbitrairement proche d'une valeur de $\underline{\delta}(E_d)$ pour un certain choix de paramètres. Ces derniers résultats sont obtenus *via* des considérations sur la périodicité de la « partie principale » (voir [1, (44)]) du développement asymptotique de $T_d(X)$.

Les particularités de la fonction $T_d(X)$ et des densités associées proviennent pour une part importante du fait que les courbes elliptiques de la famille d'Ulmer $(E_d/\mathbf{F}_q(t))$ ne satisfont pas LI. On revient maintenant au cas que l'on a appelé générique et on décrit les travaux de [2] portant sur l'étude de LI dans deux familles algébro-géométriques de courbes elliptiques.

5.2 Indépendance linéaire dans des familles de tordues quadratiques et de pullbacks

Au-delà de la propriété LI de la définition 5.1.1, on cherche à étudier les relations de dépendance linéaire éventuelles entre les racines de $L(\mathrm{Sym}^n E/K, T)$ pour n prenant un nombre fini de valeurs entières. La résolution de ce problème n'est pas strictement requise dans l'étude de $T_E(X)$ (où seule la fonction $L(E/K, T)$ joue un rôle), mais il s'agit en revanche d'une étape importante si l'on souhaite aborder l'analogue sur les corps de fonctions de la question posée par Mazur dans [M] et mentionnée au début de ce chapitre (voir aussi §5.3).

C'est à cette question plus générale que l'on apporte des réponses dans [2]. Commençons par définir les objets algébriques permettant de détecter la présence (ou l'absence) de relations de dépendance linéaire. On utilise une approche initiée par Girstmair [G2] et appliquée par Kowalski dans [K5] pour l'étude de l'indépedance linéaire des zéros de numérateurs de fonctions zêtas de courbes sur un corps fini. L'idée est de se ramener à une question de théorie des représentations linéaires d'un groupe de Galois fini.

5.2.1 Indépendance de zéros et action galoisienne

Soit $k \geqslant 1$ un entier et soit $P_1, \ldots, P_k$ des polynômes à coefficients rationnels. Pour chaque i, notons K_i le corps de décomposition de $P_i/\mathbf{Q}$ et $G_i := \mathrm{Gal}(K_i/\mathbf{Q})$. Si l'on note M_i l'ensemble des racines complexes de P_i, on peut voir G_i comme un sous-groupe du groupe des permutations de M_i. On suppose que les extensions $K_i/\mathbf{Q}$ sont deux à deux linéairement disjointes, de sorte que le corps de décompositon de $P := P_1 \cdots P_k$ sur $\mathbf{Q}$ a un groupe de Galois G isomorphe à $G_1 \times \cdots \times G_k$. On note enfin M la réunion (nécessairement disjointe) des M_i, $1 \leqslant i \leqslant k$, et $F(M)$ le G-module correspondant à l'action par permutation de G sur M. On s'intéresse à la propriété *d'indépendance multiplicative* des zéros du polynôme P. On note $\langle M \rangle$ le $\mathbf{Z}$-module multiplicatif engrendré par M et $\langle M \rangle_{\mathbf{Q}} := \langle M \rangle \otimes_{\mathbf{Z}} \mathbf{Q}$, le $\mathbf{Q}$-espace vectoriel obtenu par extension des scalaires. L'action de G sur M induit une action linéaire

de G sur $\langle M\rangle_{\mathbf{Q}}$ et une application linéaire G-équivariante

$$r\colon F(M)\to\langle M\rangle_{\mathbf{Q}}\,,$$

dont le noyau est le G-module $\mathrm{Rel}_{\mathbf{Q}}(M):=\mathrm{Rel}(M)\otimes_{\mathbf{Z}}\mathbf{Q}$, où

$$\mathrm{Rel}(M):=\{(n_\alpha)\in\mathbf{Z}^M\colon\ \prod_{\alpha\in M}\alpha^{n_\alpha}=1\}\,.$$

Notre objet d'étude dans [2] est le G-module des *relations multiplicatives* $\mathrm{Rel}(M)$. Pour décrire ce G-module, l'approche consiste en la décomposition explicite de $F(M)$ en somme directe de G-modules simples, puis en l'identification de ceux d'entre eux dont la somme constitue $\mathrm{Rel}_{\mathbf{Q}}(M)$. On doit d'abord décrire le groupe G, dans le cadre qui nous intéresse, i.e. lorsque chaque P_i correspond à $L(\mathrm{Sym}^{n_i}E/K,T)$, pour une certaine courbe elliptique E/K et un certain entier $n_i\geqslant 1$.

Fixons une courbe elliptique E/K, où les notations et les hypothèses sont les mêmes qu'au début de §5.1. Soit $m\geqslant 1$ un entier. Dans [2, Th. 1.1], on rappelle l'équation fonctionnelle satisfaite par la fonction L de la m-ème puissance symétrique de E :

$$L(\mathrm{Sym}^m E/K,T)=\varepsilon_m(E/K)\cdot(q^{(m+1)/2}T)^{\nu_m}\cdot L(\mathrm{Sym}^m E/K,1/(q^{m+1}T))\,,\tag{5.2.1}$$

où $\nu_m:=\deg L(\mathrm{Sym}^m E/K,T)$ et $\varepsilon_m(E/K)=\pm 1$. On rappelle également la conséquence suivante du théorème de pureté de Deligne :

$$L(\mathrm{Sym}^m E/K,T)=\prod_{j=1}^{\nu_m}(1-\gamma_{m,j}T),\tag{5.2.2}$$

où chaque $\gamma_{m,j}$ est un entier algébrique de valeur absolue $q^{(m+1)/2}$. (Précisément on fixe un nombre premier $\ell\neq p$ et pour tout choix de plongement $\iota\colon\overline{\mathbf{Q}_\ell}\to\mathbf{C}$, on a $|\iota(\gamma_{m,j})|=q^{(m+1)/2}$.) L'équation fonctionnelle (5.2.1) peut imposer les zéros rationnels $\pm 1/q$ au polynôme (5.2.2) (dans le cas $m=1$, ce fait justifie l'introduction de l'ensemble $\mathrm{FZ}(E/K)$ défini par (5.1.3) à partir de (5.1.2)). Ces zéros constituent évidemment une obstruction à la propriété d'indépendance linéaire que l'on étudie. On exclut donc de notre étude ces zéros imposés en considérant une version réduite des fonctions L de puissances symétriques. En notant

$$L_u(\mathrm{Sym}^m E/K,T):=L(\mathrm{Sym}^m E/K,T/q^{(m+1)/2})\,,$$

(qui est un polynôme réciproque ou antiréciproque au sens de §3.3) on définit :

$$L_{\mathrm{red}}(\mathrm{Sym}^m E/K,T)=\begin{cases}L_u(\mathrm{Sym}^m E/K,T)/(1+\varepsilon_m(E/K)T)\,,\text{ si }\nu_m\text{ est impair}\,,\\ L_u(\mathrm{Sym}^m E/K,T)/(1-T^2)\,,\text{ si }\nu_m\text{ est pair et }\varepsilon_m(E/K)=-1\,,\\ L_u(\mathrm{Sym}^m E/K,T)\,,\text{ sinon}\,.\end{cases}$$

On note que le degré $\nu_{m,\mathrm{red}}$ de ce polynôme réduit est pair. Pour chaque m, les relations auxquelles on s'intéresse sont de la forme

$$\prod_{j=1}^{\nu_{m,\mathrm{red}}}\mathrm{e}^{in_j\theta_{m,j}}=1\,,\qquad n_j\in\mathbf{Z}\,,$$

et si le poynôme étudié est le produit des $L(\mathrm{Sym}^m E/K,T)$, pour $1\leqslant m\leqslant k$, on considèrera plus généralement le $\mathbf{Z}$-module multiplicatif :

$$\mathrm{Rel}\left((\gamma_{m,j})_{\substack{1\leqslant j\leqslant \nu_{m,\mathrm{red}}\\ 1\leqslant m\leqslant k}}\right)=\left\{(n_{m,j})_{\substack{1\leqslant j\leqslant \nu_{m,\mathrm{red}}\\ 1\leqslant m\leqslant k}}\colon n_{m,j}\in\mathbf{Z}\text{ et }\prod_{m=1}^{k}\left(\prod_{j=1}^{\nu_{m,\mathrm{red}}}\mathrm{e}^{in_{m,j}\theta_{m,j}}\right)=1\right\}.$$

Outre les zéros imposés, on déduit de (5.2.1) d'autres relations que l'on nomme *triviales*. Elles proviennent de la stabilité de l'ensemble des zéros de chaque $L_{\mathrm{red}}(\mathrm{Sym}^m E/K,T)$ par conjugasion (ou, ce qui revient au même, par inversion). Pour un polynôme donné (disons pour $L(E/K,T)$), la propriété LI (voir la définition 5.1.1) est une conséquence de la trivialité du $\mathbf{Z}$-module multiplicatif des relations, i.e. du fait que le $\mathbf{Z}$-module des relations est exclusivement constitué des relations triviales (voir [1, preuve du Th. 1.3]). On a donc réduit la question au problème de la coïncidence « générique » entre $\mathrm{Rel}((\gamma_{m,j}))$ et son sous-module de relations triviales. On a vu que ces deux modules galoisiens sont des sous-mdules de $F((\gamma_{m,j}))$. Dans le cas où le groupe de Galois du corps de décomposition sur $\mathbf{Q}$ de $\prod_{1\leqslant m\leqslant k}L(\mathrm{Sym}^m E/K,T)$ est « maximal », on peut donner la décomposition de $F((\gamma_{m,j})$ en une somme de modules simples.

La notion de « maximalité » du groupe de Galois est à rapprocher de la proposition 2.1.1. Les familles de courbes elliptiques que l'on va présenter dans la section suivante sont des familles algébriques dont la monodromie ℓ-adique géométrique est un sous-groupe d'un groupe symplectique ou d'un groupe orthogonal. De ce fait, et en accord avec ce qu'affirme la proposition 2.1.1, les groupes de Galois à étudier se plongeront dans la groupe de Weyl d'un système de racines de type B_n (ou, cela revient au même, C_n) ou D_n, pour un certain $n\geqslant 1$. On a rappelé dans l'exemple 1.1.5 quel était le groupe de Weyl W_{2n} commun aux systèmes de racines de type B_n et C_n. Le groupe de Weyl W_{2n}^+ du système de racines D_n peut être vu comme un sous-groupe de W_{2n} de la manière suivante (voir [2, §3.2] pour plus de détails). Si l'on note $\mathfrak{S}_{2n}$ le groupe des permutations de l'ensemble $\{-n,\dots,-1,1,\dots,n\}$, alors $W_{2n}\subseteq\mathfrak{S}_{2n}$ est le sous-groupe des permutations agissant sur les paires $\{-i,i\}$, $1\leqslant i\leqslant n$. On dit que $\sigma\in W_{2n}$ présente un *changement de signes* s'il existe $1\leqslant i,j\leqslant n$ tels que $\sigma(i)=-j$ et (nécessairement) $\sigma(-i)=j$. Cette définition donne lieu à un homomorphisme

$$\mathrm{sgn}\colon W_{2n}\to\{\pm 1\},\qquad \sigma\mapsto(-1)^{\#\{\text{changements de signes de }\sigma\}}.$$

On a alors

$$W_{2n}^+:=\ker\mathrm{sgn}. \tag{5.2.3}$$

Le sous-groupe W_{2n}^+ est d'indice 2 dans W_n mais, pour $n\geqslant 3$, la représentation par permutation sur $\{-n,\dots,-1,1,\dots,n\}$ se décompose en la même somme de G-modules simples que G soit le groupe W_{2n} tout entier ou le sous-groupe W_{2n}^+. Ce fait est sous-entendu dans la proposition suivante qui réduit la question de l'indépendance multiplicative des zéros à celle de la coïncidence du groupe de Galois avec l'un des groupes W_{2n} ou W_{2n}^+

Proposition 5.2.1. *On reprend les notations du début de §5.2.1 et l'on suppose que chaque polynôme P_i est réciproque ou antirécirpoque. Supposons que pour chque $1\leqslant i\leqslant k$, le*

groupe de Galois du corps de décomposition de P_i sur $\mathbf{Q}$ est isomorphe au groupe $\mathcal{W} := \mathcal{W}_i \in \{W_{2g_i}, W_{2g_i}^+\}$, pour un certain entier $g_i \geqslant 3$. Le groupe $\mathcal{W}_1 \times \cdots \times \mathcal{W}_k$ agit sur M, donnant lieu au $\mathcal{W}$-module $F(M)$. Alors le sous-module des relations multiplicatives dans M se décompose comme suit

$$\mathrm{Rel}_{\mathbf{Q}}(M) = \bigoplus_{1 \leqslant i \leqslant k} \mathrm{Rel}_{\mathbf{Q}}(M_i)\,,$$

et, pour chaque i, le $\mathcal{W}_i$-module $\mathrm{Rel}_{\mathbf{Q}}(M_i)$ coïncide avec le sous-$\mathcal{W}_i$-module des relations multiplicatives triviales.

Cette proposition est la conséquence de résultats plus précis ([2, Lem. 3.1, Cor. 3.3, Prop. 3.4]) donnant la décomposition explicite en $\mathcal{W}$-modules simples de $F(M)$ d'une part et de $\mathrm{Rel}_{\mathbf{Q}}(M)$ d'autre part. Ces résultats utilisent de manière cruciale la structure des groupes W_{2n} et W_{2n}^+. Pour le groupe W_{2n} seul, ces résultats ont déjà été prouvés et utilisés dans [K5]. Le passage au groupe W_{2n}^+ que l'on doit opérer dans [2] peut être vu comme une généralisation des résultats de *loc. cit.*.

5.2.2 Deux familles de courbes elliptiques

Maintenant ramenés à une question de maximalité du groupe de Galois du corps de décomposition sur $\mathbf{Q}$ d'un produit fini (indexé par m) de $L(\mathrm{Sym}^m E/K, T)$, on peut appliquer la stratégie initiée dans [K3], puis adaptée dans [J1], pour obtenir des résultats en moyenne sur des familles de courbes elliptiques ayant grande monodromie ℓ-adique. Dans [2], on s'intéresse à deux familles en particulier. La première des deux a déjà été considérée dans [J1] mais seulement dans l'optique de l'étude de $L(E/K, T)$, sans mention du cas des puissances symétriques supérieures.

Une famille de tordues quadratiques

Fixons une courbe elliptique E/K d'invariant j non constant. Dans [K1], Katz définit et étudie une famille de courbes elliptiques construites à partir de E/K. Donnons une description succinte de cette construction dans le cas $C = \mathbf{P}^1$. Il nous faut tout d'abord supposer que le lieu $\mathcal{M}$ de réduction multiplicative de E/K n'est pas vide, et fixer $m \in \mathbf{F}_q[t]$ s'annulant en au moins un point de $\mathcal{M}$ (il s'agit là d'une hypothèse technique permettant d'assurer la propriété de grande monodromie dont bénéficie la famille étudiée). Si E est donnée par une équation de Weierstrass $y^2 = x^3 + ax + b$, $a, b \in \mathbf{F}_q[t]$, alors pour tout $f \in K^\times$ l'equation

$$y^2 = x^3 + f^2 ax + f^3 b\,,$$

donne un modèle de Weierstrass pour une courbe elliptique E_f/K. On dit que E_f est une *tordue quadratique* de E si f n'est pas un carré dans K. La variété de paramètres choisie par Katz pour construire des tordues quadratiques E_f de E est la suivante : pour chaque $d \geqslant 1$ fixé, on note $\mathcal{F}_d$ la variété affine de dimension $d+1$ dont les points $\mathbf{F}$-rationnels sont, pour chaque extension finie fixée $\mathbf{F}/\mathbf{F}_q$:

$$\mathcal{F}_d(\mathbf{F}) = \{f \in \mathbf{F}[t] \colon f \text{ sans facteur carré, } \deg f = d,\ \mathrm{pgcd}(f, m) = 1\}\,.$$

Une des observations cruciales faites par Katz est que, pour $f \in \mathcal{F}_d(\mathbf{F}_{q^n})$ le degré de $L(E_f/K,T)$ dépend de d et q, mais pas de n, de sorte que, dans une perspective de crible, n est un paramètre qui peut tendre vers l'infini. Enonçons le résultat principal [2, Th. 2.3] que l'on démontre pour cette famille.

Théorème 5.2.2 (Indépendance des zéros générique pour les tordues quadratiques)**.** *On conserve les notations et les hypothèses du début de cette section. Si $f \in \mathcal{F}_d(\mathbf{F}_{q^n})$, alors on note ν_m le degré (ne dépendant que de q et $\deg f = d$) de $L(\mathrm{Sym}^m E_f/K,T)$, la fonction L de la m-ème puissance symétrique de la tordue quadratique E_f de E sur K. On note comme précédemment $(\gamma_{m,j}(f))_{1\leqslant j\leqslant \nu_m}$ la suite finie des inverses des racines de $L(\mathrm{Sym}^m E_f/K,T)$ dans $\mathbf{C}$ ordonnée de sorte à ce qu'apparaissent d'abord les racines correspondantes du polynôme réduit $L_{\mathrm{red}}(\mathrm{Sym}^m E/K,T)$. Soit $k \geqslant 1$ un entier. Alors pour tout p supérieur à une constante ne dépendant que de d et k, et pour tout puissance assez grande $q := p^n$ (précisément n est plus grand qu'une constante ne dépendant que de $\overline{\mathcal{F}_d} := \mathcal{F}_d \times \overline{\mathbf{F}_p}$) et pour tout d plus grand qu'une constante absolue :*

$$\#\left\{f \in \mathcal{F}_d(\mathbf{F}_q)\colon \mathrm{Rel}\left((\gamma_{2m-1,j}(f))_{\substack{1\leqslant j\leqslant \nu_{2m-1,\mathrm{red}}\\ 1\leqslant m\leqslant k}}\right) \text{ n'est pas réduit aux relations triviales}\right\}$$
$$\ll q^{d+1-\gamma^{-1}}\log q\,,$$

où l'on peut prendre $2\gamma = 4 + 7\sum_{m=1}^{k}\nu_{2m-1}(\nu_{2m-1}-1)$ et avec une constante absolue ne dépendant que de d et k.

Notons que l'énoncé exclut les puissances symétriques paires de la fonction L de E_f. La raison en est claire : la fonction L de ces puissances symétriques coïncide avec celle de la même puissance symétrique de la courbe elliptique de base E/K (voir [2, Lem. 5.2]). Comme on l'a déjà mentionné, le théorème 5.2.2 est une généralisation du théorème principal de [J1], où l'on considère seulement la fonction $L(E_f/K,T)$ pour f parcourant une sous-famille à un paramètre de $\mathcal{F}_d$.

La combinaison du théorème 5.2.2 et du théorème 5.1.2 permet d'énoncer un résultat de dissipation générique du biais de Chebyshev pour la fonction T_E, lorsque E parcourt la famille de tordues quadratiques indexée par $\mathcal{F}_d(\mathbf{F}_q)$. Il s'agit de [1, Th. 1.3], et ce type de résultat est la motivation principale des travaux [1] et [2].

Théorème 5.2.3. *On conserve les notations et les hypothèses ci-dessus. Il existe une constante absolue c telle que la proportion de paramètres $f \in \mathcal{F}_d(\mathbf{F}_{q^n})$ pour lesquels $\delta(E_f)$ existe et satisfait l'inégalité*

$$\left|\delta(E_f) - \frac{1}{2}\right| \leqslant \frac{c}{\sqrt{d}}$$

est au moins égale à $1 - O_{d,E/\mathbf{F}_q(C)}(n\log q/q^{nc_E d^{-2}})$, où la constante $c_E > 0$ ne dépend que de la courbe elliptique de base E.

Décrivons maintenant la seconde famille de courbes elliptiques étudiée dans [2].

Une famille de pullbacks

De nouveau, on exploite une construction de Katz (voir [K2, §7.3]) : fixons une courbe elliptique $E/\mathbf{F}_q(t)$ d'invariant j non constant, et supposons que E est donnée par l'équation de Weierstrass

$$E\colon y^2 + a_1(t)y + a_3(t)xy = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)\,,$$

où les a_i sont éléments du corps de fonctions rationnel $\mathbf{F}_q(t)$. En conservant les notations du début de §5.1, fixons une fonction $f \in K = \mathbf{F}_q(C)$, et considérons la courbe obtenue en substituant f à t dans l'équation de Weierstrass ci-dessus :

$$E^f\colon y^2 + a_1(f)y + a_3(f)xy = x^3 + a_2(f)x^2 + a_4(f)x + a_6(f)\,.$$

Katz montre dans *loc. cit.* que la courbe elliptique E^f/K ainsi définie vérifie pour tout $n \geqslant 1$,

$$L(\mathrm{Sym}^n E/\mathbf{F}_q(t), T) \mid L(\mathrm{Sym}^n E^f/\mathbf{F}_q(C), T)\,, \tag{5.2.4}$$

où la relation de divisibilité est à voir dans $\mathbf{Q}[T]$. Cette propriété anéantit tout espoir de montrer un résultat d'indépendance linéaire pour les zéros des polynômes $L(\mathrm{Sym}^n E^f/\mathbf{F}_q(C), T)$, lorsque f varie. En revanche, on peut poser la question de l'indépendance des zéros des polynômes $L^{\mathrm{new}}(\mathrm{Sym}^n E^f/\mathbf{F}_q(C), T)$ (qui sont, par définition, les quotients dans la division correspondant à la relation ci-dessus) lorsque f varie. Pour définir l'espace de paramètres auquel f appartient, on fixe un diviseur D de C de degré $\geqslant 2g+3$, où g désigne le genre de la courbe C. Soit S le lieu de mauvaise réduction de E ; on note $U_{D,S}$ l'ouvert dense de l'espace linéaire de Riemann–Roch $\mathcal{L}(D)$ dont les $\overline{\mathbf{F}_q}$-points sont les $f \in \mathcal{L}(D)/\overline{\mathbf{F}_q}$ dont le diviseur des pôles est D et qui sont finis étales au-dessus de S. Le résultat principal que l'on obtient pour cette famille est le suivant (voir [2, Th. 2.4]).

Théorème 5.2.4 (Indépendance des zéros générique pour les pullbacks)**.** *On conserve les notations et les hypothèses ci-dessus. Soit $n \geqslant 1$ et soit $f \in U_{D,S}(\mathbf{F}_{q^n})$. On note $(\gamma_{m,j}(f)^{\mathrm{new}})_{1\leqslant j\leqslant \nu_m}$ l'ensemble des inverses de zéros de $L^{\mathrm{new}}(\mathrm{Sym}^n E^f/\mathbf{F}_{q^n}(C), T)$ (en tant qu'élément de $\mathbf{Q}[T]$ dont le degré ν_m ne dépend que de D et q). Soit $k \geqslant 1$ un entier fixé. Alors, pour tout p supérieur à une constante ne dépendant que de $\deg D$ et k, pour toute puissance assez grande $q := p^r$ (précisément r doit être plus grand qu'une constante ne dépendant que de D), et pour tout D de degré supérieur à une constante absolue, on a*

$$\#\left\{ f \in U_{D,S}(\mathbf{F}_q) : \mathrm{Rel}\left((\gamma_{m,j}(f)^{\mathrm{new}})_{\substack{1\leqslant j\leqslant \nu_{m,\mathrm{red}} \\ 1\leqslant m\leqslant k}} \right) \text{ n'est pas réduit aux relations triviales} \right\}$$
$$\ll q^{\ell(D)-\gamma^{-1}} \log q\,,$$

où l'on peut prendre

$$2\gamma = 4 + 7\sum_{j=1}^{k} h(j), \qquad h(j) := \begin{cases} \nu_j(\nu_j - 1) & \text{si } j \text{ est impair}, \\ \nu_j(\nu_j + 1) & \text{si } j \text{ est pair}, \end{cases}$$

et où la constante implicite ne dépend que de D et k.

Eléments de preuve des théorèmes 5.2.2 et 5.2.4

D'après la proposition 5.2.1, il suffit, pour montrer les théorèmes 5.2.2 et 5.2.4 de prouver des inégalités analogues à celles constituant ces deux énoncés mais où le membre de gauche est remplacé par l'ensemble des paramètres à coordonnées dans $\mathbf{F}_q$ tels que le groupe de Galois du corps de décomposition du produit de fonctions L de puissances symétriques de la courbe indexée par ce paramètre est un sous-groupe strict du groupe maximal de type $\mathcal{W}$ apparaissant (voir l'énoncé de la proposition 5.2.1). La structure de la démonstration de ces résultats repose sur le crible pour les morphismes de Frobenius défini dans [K3] (voir aussi [K4, Chap. 8] et les premières utilisations pour l'étude de $L(E/K,T)$ dans [J1]). Il s'agit d'un crible de conjugaison pour les classes à gauche (voir §1.2). Si $U/\mathbf{F}_q$ désigne la variété (affine, lisse, et géométriquement connexe) de paramètres ($\mathcal{F}_d$ ou $U_{D,S}$ suivant le cas) et si $\bar{\eta}$ est un point générique géométrique de U, on dispose de la suite exacte courte

$$1 \to \pi_1(\overline{U},\bar{\eta}) \to \pi_1(U,\bar{\eta}) \to \hat{\mathbf{Z}} \to 1\,, \tag{5.2.5}$$

où $\pi_1(U,\bar{\eta})$ (resp. $\pi_1(\overline{U},\bar{\eta})$) est le groupe fondamental étale arithmétique (resp. géométrique) de U, et où l'on note d (pour degré) le morphisme quotient. Chacune des deux familles présentées peut être vue comme l'ensemble des fibres au-dessus de $U(\mathbf{F}_q)$ d'un certain morphisme $\pi\colon \mathcal{E} \to U$. Associé à cette famille et à un nombre premier $\ell \neq p$ Katz associe un faisceau ℓ-adique lisse sur U (ou, de manière équivalente, une représentation ℓ-adique continue $\tilde{\rho}_\ell$ de $\pi_1(U,\bar{\eta})$) dont le polynôme caractéristique du Frobenius (géométrique) sur la fibre en f coïncide avec la fonction L que l'on étudie. Le cadre de crible utilisé dans [K3] est alors $(d^{-1}(-1)^\sharp, \{\ell \neq p\}, (\rho_\ell)_\ell)$, où chaque ρ_ℓ est la réduction modulo ℓ de $\tilde{\rho}_\ell$. Quant à l'ensemble à cribler, c'est $(U(\mathbf{F}_q), \text{mesure de comptage}, x \to \mathrm{Frob}_x)$.

Le point crucial pour le crible est de connaitre précisément l'image des représentations ρ_ℓ de monodromie modulo ℓ. Pour ce point, Kowalski utilise dans [K3] un théorème de Yu. Dans [J1], on invoque un théorème de Hall [H]. Ces deux résultats assurent la maximalité du groupe de monodromie modulo ℓ relatif à certaines familles (dans le cas de [H], il s'agit de la famille de tordues quadratiques d'espace de paramètres $\mathcal{F}_d$), avec des aspects d'uniformité remarquables. Pour les familles plus générales considérées dans [2], les généralisations des théorèmes de Hall et Yu sont imparfaites : on commence par invoquer des résultats de grande monodromie ℓ-adique de Katz ([K1, Th. 7.6.7] et [K2, Th. 7.3.14, 7.3.16]), puis, au prix d'une perte d'uniformité dans la dépendance en les paramètres, on déduit les résultats de grande monodromie modulo ℓ voulus pour ℓ parcourant l'ensemble des nombres premiers à un nombre fini d'exceptions près (voir [2, §5.2] ; c'est cet ensemble d'exceptions qui peut dépendre de chacun des paramètres intervenant).

Dans [2] d'autres difficultés doivent également être surmontées. Mentionnons par exemple que, dans le cas d'une puissance symétrique impaire, les groupes de monodromie ℓ-adique apparaissant en appliquant les résultats de Katz sont des groupes orthogonaux. Par réduction modulo ℓ, on ne peut garantir que le groupe fini obtenu soit le groupe orthogonal (sur le corps fini $\mathbf{F}_\ell$) tout entier. On peut seulement affirmer que ce groupe fini contient le groupe dérivé du groupe orthogonal en question (voir [2, Prop. 5.5]). Géométriquement, cela impose

que l'on modifie le cadre de crible : au lieu de (5.2.5), il faut utiliser une suite exacte faisant intervenir un revêtement étale $\kappa\colon V \to U$ de groupe (abélien) $G(V/U)$:

$$1 \to \pi_1(\overline{V}, \bar{\mu}) \to \pi_1(U, \bar{\eta}) \to G(V/U) \times \hat{\mathbf{Z}} \to 1\,,$$

où $\bar{\mu}$ est un point générique géométrique de V envoyé sur $\bar{\eta}$ par κ (voir [2, (13)]). Cette adaptation nécessaire de (5.2.5) est déjà présente dans [J1]. Un aspect nouveau par rapport à [J1] est la dimension de la variété de paramètres U qui peut être > 1. Ce passage à la dimension supérieure est possible tant que p ne divise pas l'ordre de $\rho_\ell(\pi_1(\overline{V}, \bar{\mu}))$, ce qui assure un bon contrôle de la ramification, puis un bon contrôle du terme d'erreur lorsque l'on invoque l'hypothèse de Riemann sur $V/\mathbf{F}_q$ pour produire l'écart spectral nécessaire pour majorer Δ (voir [2, Th. 4.1 et 4.3]). (L'hypothèse de Riemann sur les corps finis joue de ce point de vue le rôle que joue la propriété (τ) dans le chapitre 2.)

Enfin mentionnons une difficulté technique en lien avec le phénomène propre aux groupes orthogonaux et explicité dans l'exemple 3.0.1. Dans l'étude du produit de fonctions L de puissances symétriques d'une courbe E variant dans les familles décrites ci-dessus, on souhaite montrer que le groupe de Galois typique est un produit du type $\mathcal{W}_1 \times \cdots \times \mathcal{W}_k$, dans les notations de la proposition 5.2.1. Dans l'aspect local de la preuve, il ne suffit pas de choisir des ensembles criblants permettant de détecter que le groupe de Galois typique se surjecte sur chaque $\mathcal{W}_i$. Pour assurer la maximalité du groupe de Galois, il faut aussi montrer que des classes de conjugaison du type $(1, 1, \ldots, 1, c_i, 1, \ldots, 1)$ (où c_i est élément d'une classe de conjugaison fixée de W_i) sont représentées. Cela pose la question de l'existence (si l'on suit l'approche décrite au début du chapitre 3), étant donné un polynôme f réciproque, séparable, scindé, d'une isométrie de polynôme caractéristique f. Une telle isométrie n'existe que si la structure quadratique sous-jacente est la structure scindée, d'après (3.3.2). L'ensemble des nombres premiers par lesquels on crible doit donc être retreint à un sous-ensemble de premiers ℓ tel que la réduction modulo ℓ du groupe orthogonal "global" (dont l'existence est affirmé par les résultats de grande monodromie de Katz) donne un groupe orthogonal scindé sur $\mathbf{F}_\ell$. On renvoie à [2, Lem. 5.7 et 5.8] pour le détail de cet argument et à [2, Lem. 4.5] pour la minoration de l'ensemble criblant correspondant aux classes de conjugaison du type $(1, 1, \ldots, 1, c_i, 1, \ldots, 1)$, dans le cas favorable où la structure quadratique finie est scindée.

5.3 Autres études de biais potentiels

Diverses questions, dans le prolongement des travaux [1] et [2], restent en suspend. On note par exemple que [1] ne contient pas d'énoncé analogue au théorème 5.2.3 pour la famille de pullbacks de §5.2.2. Il nous faudrait pour cela explorer la signification, pour la fonction T_E, de la relation de divisibilité (5.2.4).

Une autre piste encore à explorer est la question de l'analogue sur les corps de fonctions de la course de nombres premiers T définie par Mazur dans [M]. Les travaux de [1] et [2] constituent une étape significative pour aborder cette question. Pour ce problème de biais, il nous faut étudier la fonction T_V, où $V\colon [0, \pi] \to$ est une fonction lisse (vérifiant une condition de décroissance rapide des coefficients de Fourier) quelconque. La différence entre la fonction

T_E et l'analogue de la fonction T de Mazur réside dans le nombre de coefficients de Fourier (relatifs à la base de Chebyshev de $L^2([0,\pi])$) à prendre en compte. Adapter le théorème central limite 5.1.2 à ce cadre, où une infinité de coefficients de Fourier peuvent intervenir (au lieu d'un seul pour la fonction T_E) nécessite de prendre en considération toutes les fonctions $L(\mathrm{Sym}^n E/K, T)$, et pas seulement le cas $n = 1$.

Mentionnons enfin que, dans cette optique, les résultats d'indépendance linéaire fournis par [2] sont imparfaits. La méthode de crible utilisée ne peut en effet traiter que le produit d'un nombre fini de fonctions L de puissances symétriques d'une courbe elliptique donnée. Si l'on veut exploiter ces résultats de crible pour l'étude de l'analogue de la fonction T de Mazur, il nous faudra établir un résultat d'approximation permettant de décrire le phénomène de biais à partir de la seule connaissance d'un nombre fini de coefficients de Fourier pour la fonction indicatrice entrant en jeu.

Bibliographie

[1] Byungchul Cha, Daniel Fiorilli, and Florent Jouve, *Prime number races for elliptic curves over function fields* (2015), submitted, available at www.math.u-psud.fr/~jouve/EllCurvesBias.pdf.

[2] ———, *Independence of the zeros of elliptic curve L-functions over function fields* (2015), submitted, available at www.math.u-psud.fr/~jouve/IndepZeros.pdf.

[3] Florent Jouve, Emmanuel Kowalski, and David Zywina, *An explicit integral polynomial whose splitting field has Galois group $W(E_8)$*, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 761–782.

[4] ———, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, Israel J. Math. **193** (2013), no. 1, 263–307.

[5] Florent Jouve and Fernando Rodriguez Villegas, *On the bilinear structure associated to Bezoutians*, J. Algebra **400** (2014), 161–184.

[6] Florent Jouve and Jean-Sébastien Sereni, *Sieving in graphs and explicit bounds for non-typical elements* (2015), preprint, available at http://www.math.u-psud.fr/~jouve/GraphRandomWalks-v3.pdf.

[BH] Frits Beukers and Gert Heckman, *Monodromy for the hypergeometric function ${}_nF_{n-1}$*, Invent. Math. **95** (1989), no. 2, 325–354.

[BCM] Adam Bohn, Peter J. Cameron, and Peter Müller, *Galois groups of multivariate Tutte polynomials*, J. Algebraic Combin. **36** (2012), no. 2, 223–230.

[BF] Jörg Brüdern and Étienne Fouvry, *Lagrange's four squares theorem with almost prime variables*, J. Reine Angew. Math. **454** (1994), 59–96.

[C1] Peter J. Cameron, *Algebraic properties of chromatic roots*, lecture notes, available at http://www.maths.qmul.ac.uk/~pjc/csgnotes/alchrom1.pdf.

[C2] Byungchul Cha, *Chebyshev's bias in function fields*, Compos. Math. **144** (2008), no. 6, 1351–1374.

[C3] Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180.

[C4] Pafnutiĭ L′vovich Chebyshev, *Lettre de M. le professeur Tchébychev à M. Fuss sur un nouveau théorème relatif aux nombres premiers contenus dans les formes $4n+1$ et $4n+3$*, Bull. Classe Phys. Acad. Imp. Sci. St. Petersburg **11** (1853), 208.

[C5] Laurent Clozel, *Démonstration de la conjecture τ*, Invent. Math. **151** (2003), no. 2, 297–328.

[CHT] Laurent Clozel, Michael Harris, and Richard Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations*, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 1–181.

[DSV] Giuliana Davidoff, Peter Sarnak, and Alain Valette, *Elementary number theory, group theory, and Ramanujan graphs*, London Mathematical Society Student Texts, vol. 55, Cambridge University Press, Cambridge, 2003.

[D1] Pierre Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252.

[D2] Rainer Dietmann, *Probabilistic Galois theory*, Bull. Lond. Math. Soc. **45** (2013), no. 3, 453–462.

[F] Daniel Fiorilli, *Elliptic curves of unbounded rank and Chebyshev's bias*, Int. Math. Res. Not. IMRN **18** (2014), 4997–5024.

[FM] Étienne Fouvry and Philippe Michel, *Sur le changement de signe des sommes de Kloosterman*, Ann. of Math. (2) **165** (2007), no. 3, 675–715.

[FMS] Elena Fuchs, Chen Meiri, and Peter Sarnak, *Hyperbolic monodromy groups for the hypergeometric equation and Cartan involutions*, J. Eur. Math. Soc. (JEMS) **16** (2014), no. 8, 1617–1671.

[G1] Patrick X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 91–101.

[G2] Kurt Girstmair, *Linear dependence of zeros of polynomials and construction of primitive elements*, Manuscripta Math. **39** (1982), no. 1, 81–97.

[GN] Alexander Gorodnik and Amos Nevo, *Splitting fields of elements in arithmetic groups*, Math. Res. Lett. **18** (2011), no. 6, 1281–1288.

[G] Morris Goldfeld, *Artin's conjecture on the average*, Mathematika **15** (1968), 223–226.

[H] Chris Hall, *Big symplectic or orthogonal monodromy modulo l*, Duke Math. J. **141** (2008), no. 1, 179–203.

[HSBT] Michael Harris, Nick Shepherd-Barron, and Richard Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Ann. of Math. (2) **171** (2010), no. 2, 779–813.

[H] Harald A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) **167** (2008), no. 2, 601–623.

[J1] Florent Jouve, *Maximal Galois group of L-functions of elliptic curves*, Int. Math. Res. Not. IMRN **19** (2009), 3557–3594.

[J2] ———, *The large sieve and random walks on left cosets of arithmetic groups*, Comment. Math. Helv. **85** (2010), no. 3, 647–704.

[K1] Nicholas M. Katz, *Twisted L-functions and monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, NJ, 2002.

[K2] ———, *Moments, monodromy, and perversity : a Diophantine perspective*, Annals of Mathematics Studies, vol. 159, Princeton University Press, Princeton, NJ, 2005.

[K3] Emmanuel Kowalski, *The large sieve, monodromy, and zeta functions of algebraic curves.*, Crelle (2006).

[K4] ———, *The large sieve and its applications*, Cambridge Tracts in Mathematics, vol. 175, Cambridge University Press, Cambridge, 2008. Arithmetic geometry, random walks and discrete groups.

[K5] ———, *The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros*, Int. Math. Res. Not. IMRN (2008), Art. ID rnn 091, 57.

[LR] Alexander Lubotzky and Lior Rosenzweig, *The Galois group of random elements of linear groups*, Amer. J. Math. **136** (2014), no. 5, 1347–1383.

[M] Barry Mazur, *Finding meaning in error terms*, Bull. Amer. Math. Soc. (N.S.) **45** (2008), no. 2, 185–228.

[MdMN] Criel Merino, Anna de Mier, and Marc Noy, *Irreducibility of the Tutte polynomial of a connected matroid*, J. Combin. Theory Ser. B **83** (2001), no. 2, 298–304.

[M] Hugh L. Montgomery, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. **84** (1978), no. 4, 547–567.

[R1] Frank P. Ramsey, *On a Problem of Formal Logic*, Proc. London Math. Soc. **S2-30**, no. 1, 264.

[R2] Igor Rivin, *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*, Duke Math. J. **142** (2008), no. 2, 353–379.

[R3] _____, *Galois groups of generic polynomials* (2015), preprint, available at http://arxiv.org/abs/1511.06446.

[RS] Michael Rubinstein and Peter Sarnak, *Chebyshev's bias*, Experiment. Math. **3** (1994), no. 3, 173–197.

[GV] Alireza Salehi Golsefidy and Péter P. Varjú, *Expansion in perfect groups*, Geom. Funct. Anal. **22** (2012), no. 6, 1832–1891.

[S1] Peter Sarnak, *Letter to Barry Mazur on Chebyshev's bias for $\tau(p)$* (2007), available at http://publications.ias.edu/sarnak/.

[S2] Tetsuji Shioda, *Theory of Mordell-Weil lattices*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, pp. 473–489.

[S3] _____, *Some explicit integral polynomials with Galois group $W(E_8)$*, Proc. Japan Acad. Ser. A Math. Sci. **85** (2009), no. 8, 118–121.

[U] Douglas Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) **155** (2002), no. 1, 295–315.

[VAZ] Anthony Várilly-Alvarado and David Zywina, *Arithmetic E_8 lattices with maximal Galois action*, LMS J. Comput. Math. **12** (2009), 144–165.

[Z] David Zywina, *Hilbert's irreducibility theorem and the larger sieve* (2010), prépublication, available at http://arxiv.org/abs/1011.6465.