université de BORDEAUX

Institut de Mathématiques de Bordeaux

THÈSE

présentée pour obtenir le grade de

Docteur de l'Université de Bordeaux

École Doctorale Mathématiques et Informatique

Spécialité Mathématiques Pures

par **Alexandre Bailleul**

Étude de la répartition des automorphismes de Frobenius dans les groupes de Galois

Sous la direction de : **Florent Jouve**

Présentée et soutenue publiquement le 27 novembre 2020.

Membres du jury

Philippe Cassou-Noguès	Professeur émérite, Université de Bordeaux, IMB	Examinateur
Daniel Fiorilli	Chargé de recherche, Université Paris-Saclay, LMO	Examinateur
Florent Jouve	Professeur, Université de Bordeaux, IMB	Directeur
Emmanuel Kowalski	Professeur, ETH Zürich	Rapporteur
Youness Lamzouri	Professeur, Université de Lorraine, IECL	Président
Nathan Ng	Professeur, University of Lethbridge	Rapporteur
Olivier Ramaré	Directeur de recherche, Aix-Marseille Université, I2M	Examinateur

Titre : Étude de la répartition des automorphismes de Frobenius dans les groupes de Galois

Résumé : Dans cette thèse, on s'intéresse à divers aspects de la théorie des courses de nombres premiers, initiée par Rubinstein et Sarnak en 1994. Dans le premier chapitre, on revient sur la méthode de Rubinstein et Sarnak, on fait un tour d'horizon de prolongements de leurs travaux, et on développe leur méthode dans un cadre général, en cherchant à s'affranchir le plus possible des hypothèses de travail de ceux-ci concernant l'indépendance linéaire des parties imaginaires des zéros non triviaux des fonctions L de Dirichlet. Dans le deuxième chapitre, on s'intéresse à la généralisation des problèmes de courses de nombres premiers au contexte de la répartition des automorphismes de Frobenius dans les groupes de Galois d'extensions de corps de nombres. Dans la lignée de travaux récents de Fiorilli et Jouve, on met en évidence l'influence que des zéros en $1/2$ de certaines fonctions L d'Artin peuvent avoir sur de telles courses. Dans le troisième et dernier chapitre, on s'intéresse à la transposition des questions précédentes aux extensions de corps de fonctions en une variable sur les corps finis, et on montre un nouveau théorème central limite pour des extensions superelliptiques.

Mots-clés : Courses de nombres premiers, Automorphismes de Frobenius, Fonctions L d'Artin, Biais de Tchebychev

---

Title : On the distribution of Frobenius automorphisms in Galois groups

Abstract : In this thesis, we are interested in multiple aspects of the theory of prime number races, initiated by Rubinstein and Sarnak in 1994. In the first chapter, we explain Rubinstein and Sarnak's method, we give an overview of extensions of their work, and we develop their method in a general setting, with the goal of weakening as much as possible their working hypothesis about the linear independence of the imaginary parts of non-trivial zeros of Dirichlet L-functions. In the second chapter, we are interested in the generalisation of problems of prime number races in the context of the distribution of Frobenius automorphisms in Galois groups of number field extensions. Following recent work of Fiorilli and Jouve, we highlight the influence that the vanishing at $1/2$ of some Artin L-functions can have on such races. In the third and final chapter, we are interested in the same kind of questions as before in the context of extensions of function fields in one variable over finite fields, and we prove a new central limit theorem for superelliptic extensions.

Keywords : Prime number races, Frobenius automorphisms, Artin L-functions, Chebyshev's bias

À la mémoire de mon père,
Pascal Bailleul

Remerciements

Mes remerciements vont en premier lieu à mon directeur de thèse, Florent Jouve, pour m'avoir fait découvrir des mathématiques fascinantes depuis mon stage de M2, pour sa disponibilité, pour son soutien constant, pour son implication jusqu'à la fin et au-delà du processus de thèse, et aussi pour son humanité dans un milieu qui en manque parfois.

Je remercie Emmanuel Kowalski et Nathan Ng d'avoir accepté de lire mes travaux et de rapporter cette thèse. Je remercie également Philippe Cassou-Noguès, Daniel Fiorilli, Youness Lamzouri et Olivier Ramaré de me faire l'honneur de participer à mon jury de thèse.

Pour des discussions mathématiques qui m'ont aidé dans ma recherche, je remercie Lucile Devin, ma grande sœur de thèse, et à nouveau Daniel Fiorilli. Le point de départ de mes premiers travaux a été une note écrite par Philippe Cassou-Noguès sur les spécificités des extensions quaternioniennes de corps de nombres, qu'il en soit remercié ici.

Je remercie toutes les institutions qui m'ont accueilli depuis le début de mes études, dans l'ordre chronologique l'ENS Rennes, l'Université de Bordeaux et l'ENS de Lyon, ainsi que leurs personnels qui ont pu m'aider de près ou de loin. Merci notamment à Cyril Mauvillain d'avoir toléré mes emprunts en (trop) grand nombre à la bibliothèque de l'IMB et pour avoir toujours été disponible pour dénicher les références les plus obscures. Merci à Muriel Hachemi, Ida Sirben et Catherine Vrit d'avoir répondu à mes nombreuses questions naïves concernant ma grande passion qu'est l'administration. Merci à Sylvain Allemand et Sandrine Layrisse pour leur aide dans l'organisation de la soutenance en visio.

Je dois remercier tous mes professeurs de mathématiques qui m'ont tant appris et qui m'ont permis d'arriver où j'en suis aujourd'hui. Un remerciement particulier pour Pierre-Marie Princiaux, mon professeur de MPSI, pour m'avoir appris la rigueur mais également montré que l'on peut (et que l'on doit !) s'émerveiller devant la beauté des mathématiques. Merci à Patrick Dehornoy pour une parenthèse de théorie des ensembles passionnante pendant quelques mois en parallèle de la thèse.

Merci à mes étudiants qui m'ont fait réaliser qu'il ne suffit pas de se contenter d'accumuler du savoir mais qu'il était tout autant, voire plus enrichissant de le transmettre. Merci à eux sans qui je n'aurais pas su que Cayley était un mathématicien britannique du XIX$^{\text{ème}}$ siècle ou qu'on pouvait trouver les racines du polynôme nul en posant Δ. Merci également à Guilhem de ne pas avoir fui en voyant la proposition de stage que je lui faisais.

Merci à Ératosthène pour son crible qui permet de combler 20 minutes d'exposé. Merci à Riemann pour son hypothèse. Merci à Hadamard et de la Vallée-Poussin pour avoir démontré un théorème plutôt intéressant. Merci aux éditions Calvage & Mounet pour leurs livres. Merci au forum les-mathematiques.net, je sais maintenant que de grands pouvoirs impliquent de grandes responsabilités. Enfin, merci sci-hub (#Valou) et n'oublions pas libgen.

J'en viens maintenant à mes amis, rencontrés à Bordeaux, ou bien avant. Merci à Charles pour les souvenirs très studieux (ou pas) de prépa et pour les discours de motivation.

Merci à mes amis de Rennes, la *Team KL*. Même si nos chemins ont pour la plupart divergé, je sais que je pourrai continuer à compter sur vous à l'avenir. Merci à Baptiste d'avoir toujours été un si bon ami en toute circonstance. Merci aussi pour les soirées passées sur TF2 (même si au fond tu es un W+M1 tu t'en sors bien). Merci à Yann pour la double vie agrégatif/McDoloc pendant une année, pour les soirées de g@ming, et pour le soutien moral pendant les périodes difficiles. Merci à Paul pour les fajitatouilles et les Carrés Frais$^{\text{TM}}$. Merci aussi pour les discussions sur les « Frobenius » (*Hihihi, tu dis ça parce que c'est dans le titre de la thèse*). Merci également pour ton soutien lors des moments difficiles. Merci à Adrien d'être la meilleure des racles que l'on puisse imaginer (toute sensation est agréable, surtout celle de « rater » un DS avec 20/20). Merci aussi pour la leçon sur la classification des yaois. Merci à Manon pour les souvenirs de la commuz' (*You make my wiiiiish come true*) et ceux du Brésil (*Este lugar é muito bom !*). Merci à Marine pour les références Disney que je n'ai jamais eues. Merci à Corentin pour les jeux de mots qui font passer les conférences plus vites. Merci à Cléééémeeeent Viiiince de ne toujours pas connaître mon prénom au bout de sept ans.

Merci à mes amis de Bordeaux. Grâce à vous ma vie bordelaise a été trépidante et inoubliable ! Merci à Corentin, mon frère de thèse, de musique et d'effractions. S'il y avait un saxophoniste dans Metallica tu serais comme lui, en mieux conservé ! Merci à Marc'Antò le plateformiste pour les discussions de maths qui m'ont fait perdre de nombreux après-midi, pour l'hébergement quand mon chauffe-eau avait décidé d'exploser et pour la peur persistante de mettre les pieds en Corse. Merci à Thomas de m'avoir fait découvrir que les gens de Lyon n'étaient pas comme les autres, pour ta maîtrise des réseaux sociaux (#LambdaFood) et pour avoir réussi à me convaincre d'aller au HFC (il y aura pas de deuxième fois). Merci à Lara d'être la *poubelle* de l'IMB. Si un jour tu as mal à *la* bide à cause de *la rédige*, il faut aller prendre l'*ayr*. Merci à nouveau à Baptiste qui, je l'espère, arrivera un jour à résoudre son IDP (peut-être une fulgurance au Porge ?). Merci aussi pour les Motus. Merci à Antonin d'avoir prouvé qu'on peut avoir la motivation pour passer (et obtenir) l'agreg deux fois : cet exploit restera dans les annales ! Merci à Petit Paul de m'avoir montré comment plier sa salade en 4, *ouais gros c'est la puissance !* Merci à Antoine, la « force tranquille » de l'IMB, de m'avoir révélé tes subtiles techniques de négociation avec le rectorat. Merci à Robin de m'avoir fait découvrir une facette de Nounours qui m'était inconnue, *ho hohoho !* Merci à Adrien de m'avoir prouvé qu'il existe vraiment des gens qui comprennent quelque chose à la cohomologie. Merci à Jean pour l'aide dans la gestion de Lambda. Je dois avouer que ta prononciation de Größencharakter et de Jugendtraum m'a toujours impressionné. Merci à Anne-Edgar de m'avoir attendu pour grimper le mont Puget et pour avoir prouvé qu'il est possible de faire des démonstrations au milieu d'un repas. Merci à Jonathan de m'avoir

fait découvrir le juteux filon des corrections de concours. Merci à Nico pour la technique du permis, j'espère ne pas avoir à l'appliquer un jour. Merci à Niko de m'avoir fait découvrir une nouvelle facette (?) de la langue française. Merci à Sami qui n'est pas à Bordeaux ce midi. En parlant de midi, merci à Vassilis de les avoir systématiquement retardés. Face à cette attitude, je n'ai qu'une question à te poser : ποιος είναι ο σκοπός της ζωής σας ? Thanks to Dimitris for his many advices on pursuing a mathematical carrer. In the future, just remember to remove your glasses before jumping into a pool. Merci à Elsa pour cette dernière impression, dommage d'avoir fui Lyon à cause de moi. Merci à Yiye pour les souvenirs de Chine. Merci à Roxane de ne pas avoir peur de choisir les (bonnes !) musiques en soirée, là au moins le service client était à la hauteur. Merci à Aurore pour les leçons sur les glissements sémantiques dans la langue française. Merci à Manon et Guigui pour les conseils d'œnologie. Merci à Chloé pour tes streams d'Isaac, la prochaine fois tu sauras que King Baby avec Litchi c'est pas une bonne idée ! Merci à l'Alcala, au Twist'n'Crêpes (alias le Blue Covfefe) et au Yu de nous avoir offert des alternatives au Haut-Carré. Enfin, merci à Nicolas Hublot de s'être toujours assuré que les normes européennes sont respectées, grâce à lui c'était un vrai régal tous les midis.

Je remercie la fanfare Los Teoporos, qui m'a permis de faire de nombreuses rencontres, de voyager, de passer sur France 3 et accessoirement de faire de la musique. Merci à nouveau à Coco de m'avoir invité dans la fanfare, et d'être toujours motivé à jouer les plus gros saucissons. Merci à Eunyde qui, à défaut de garder le rythme, garde toujours le sourire et le transmet de manière contagieuse. Merci à Guimouv' pour sa positivité imperturbable et les révisions sur les noms de peuples européens. Merci à Ophèlie de m'avoir fait découvrir la vraie définition du courage : celle de jouer des doubles croches sans bouger les poignets. Merci à Jojo de m'avoir si bien accueilli et d'avoir toujours été un rayon de soleil. Merci à Maxence pour ses interprétations épiques de Fanchon. Merci à CQ pour les mails de la semaine, même si j'en ai quand même écrit quelques-uns. Merci à Jiraf pour les parties du 7ème Continent, on arrivera peut-être à en finir une un jour. Merci à Polo pour les bombardements et le café, *en tout bien tout honneur !* Merci à Étienne pour les plats et les roues libres. La prochaine fois on essaiera d'aller jusqu'au bout du marathon Star Wars. Merci à Quentin pour les memes de qualité supérieure et la défense éternelle du BK. Merci à Hortense de préserver l'esprit de Michael Jackson. Merci à Gamin de m'avoir montré qu'on pouvait râler sans complexe. Merci à Georgette pour les cocktails kamikazes. Merci à François pour tes conversations, j'ai pas tout compris mais c'était sympa quand même. Merci à Molmol pour tes chorégraphies. Merci à Emma pour ta crédulité (*Vous vous foutez de moi là, non ?*). Merci à Nico pour le local de répète, l'accent du sud et les solos. Merci à tous les fanfarons qui font de cette fanfare ce qu'elle est.

Merci à ma famille, en particulier mes parents Catherine et Pascal, et ma sœur Marie, qui malgré la distance m'ont toujours soutenu et apporté leur aide quand j'en avais besoin.

Enfin, merci à Léa pour m'avoir apporté sûrement bien plus que ce qu'elle imagine, et pour avoir fait de moi qui je suis aujourd'hui. Ta présence a été indispensable pour moi ces dernières années. Chaque jour durant la thèse a été bien plus agréable grâce à toi, et celle-ci n'existerait probablement pas sans toi. Pour tout ce que l'on a vécu ensemble, merci.

Table des matières

Introduction **1**

Notations **4**

1 La méthode de Rubinstein et Sarnak **6**
1.1 Courses de nombres premiers 7
1.1.1 Le problème 7
1.1.2 Formule explicite 8
1.1.3 Distribution limite 9
1.1.4 Existence de la densité 10
1.1.5 Vue d'ensemble des résultats de Rubinstein et Sarnak 12
1.2 Prolongement des travaux de Rubinstein et Sarnak 13
1.2.1 Comportement asymptotique du biais 14
1.2.2 Course entre carrés et non carrés 14
1.2.3 Affaiblissement de GSH 15
1.2.4 Influence de zéros hors de la droite critique 16
1.2.5 Courses entre entiers ayant k facteurs premiers 17
1.2.6 Courses à plus de deux participants 18
1.3 Courses de polynômes irréductibles 19
1.3.1 Arithmétique dans $\mathbb{F}_q[T]$ 19
1.3.2 Généralisation des travaux de Rubinstein et Sarnak par Cha 22
1.3.3 Violation de l'hypothèse GSH_M 26
1.4 Théorèmes de Kronecker-Weyl explicites et applications aux courses de nombres premiers 28
1.4.1 Explicit Kronecker-Weyl theorems 33
1.4.2 Applications 52

2 Biais de Tchebychev dans les corps de nombres **63**
2.1 Fonctions L d'Artin et théorème de Chebotarev 64
2.1.1 Automorphismes de Frobenius 64
2.1.2 Théorie des représentations 67
2.1.3 Fonctions L d'Artin 69
2.1.4 Théorème de Chebotarev 74
2.2 Courses d'idéaux premiers dans les corps de nombres 76
2.2.1 Formule explicite 76
2.2.2 Discussion de l'hypothèse d'indépendance linéaire 78

2.2.3 Évolution du biais de Tchebychev en familles 79
2.2.4 Root numbers et zéros en 1/2 81
2.3 Biais de Tchebychev dans les groupes de Galois diédraux et de quaternions généralisés 82
2.3.1 Chebotarev biases in Galois groups of number fields 85
2.3.2 Recollection on ramification and on dihedral and quaternion groups of 2-power order 93
2.3.3 Extensions of $\mathbb{Q}$ of group $\mathbb{H}_8$: horizontal Chebotarev biases 100
2.3.4 Chebyshev's bias in towers 104

3 Biais de Tchebychev dans les corps de fonctions 122
3.1 Arithmétique des corps de fonctions 122
3.1.1 Définitions 122
3.1.2 Genre d'un corps de fonctions 124
3.1.3 Théorie de la ramification dans les extensions galoisiennes de corps de fonctions 125
3.1.4 Fonctions L d'Artin et théorème de Chebotarev 126
3.2 Courses de diviseurs premiers dans des extensions géométriques de corps de fonctions 128
3.2.1 Les résultats de Cha et Im 129
3.2.2 En l'absence d'indépendance linéaire 130
3.3 Un théorème central limite 131
3.4 Perspectives 136

Bibliographie 138

Introduction

L'étude de la répartition des nombres premiers est un sujet central de la théorie analytique des nombres qui a pris son essor lors du XIX$^{\text{ème}}$ siècle avec notamment les travaux de Dirichlet, Tchebychev, et Riemann, et qui continue de susciter beaucoup de travaux de recherche. La problématique centrale de cette thèse est celle de la répartition des automorphismes de Frobenius dans les groupes de Galois d'extensions de corps globaux, qui constitue un prolongement naturel des questions de répartition des nombres premiers.

Plus précisément, on s'intéresse ici aux disparités dans la répartition de ces automorphismes de Frobenius. De puissants théorèmes tels que le théorème des nombres premiers en progressions arithmétiques montrent que certaines fonctions de comptage de nombres premiers, ou d'autres quantités possédant un intérêt arithmétique, possèdent le même terme principal dans leurs développements asymptotiques. Il est notoire que les termes suivants sont beaucoup plus difficiles à étudier : à l'aide de formules explicites, on montre que ces quantités s'expriment à l'aide de termes oscillants qui font intervenir les zéros de certaines fonctions analytiques, appelées fonctions L. La taille maximale de ces termes secondaires est prédite, et dans certains cas démontrée, par l'hypothèse de Riemann, qui traite des parties réelles des zéros de ces fonctions L. La comparaison de ces termes secondaires entre eux fait, elle, intervenir des informations sur les parties imaginaires de ces mêmes zéros.

En 1853, Tchebychev observe numériquement qu'il semble y avoir plus de nombres premiers congrus à 3 modulo 4 que de nombres premiers congrus à 1 modulo 4 dans les intervalles de la forme $[2, x]$. Cette observation ne fut justifiée rigoureusement qu'en 1994 quand Rubinstein et Sarnak développèrent une nouvelle méthode, basée sur l'analyse harmonique, pour étudier ce phénomène, naturellement appelé biais de Tchebychev. Une hypothèse cruciale d'indépendance linéaire sur $\mathbb{Q}$ des parties imaginaires de zéros de fonctions L est au cœur de la méthode de Rubinstein et Sarnak, qui a été revisitée plusieurs fois depuis. La nature arithmétique des zéros des fonctions L reste aujourd'hui très mystérieuse, et de tels résultats d'indépendance linéaire semblent pour le moment hors de portée. En l'absence de résultats sur le sujet, mais en ayant l'intime conviction de leur véracité en raison de la nature transcendante des fonctions concernées, on énoncera à de nombreuses reprises des résultats supposant de telles hypothèses.

Dans cette thèse, en plus de contributions originales, on donne un tour d'horizon, non exhaustif, de résultats portant plus généralement sur les « courses de nombres premiers », qui concernent, bien évidemment, les nombres premiers, mais aussi les polynômes irréductibles sur les corps finis, les idéaux premiers des anneaux d'entiers de corps de nombres et également les diviseurs premiers des corps de fonctions en une variable sur les corps finis.

Cette thèse est organisée de la manière suivante. Dans le premier chapitre, on détaille la méthode développée par Rubinstein et Sarnak dans l'article [RS94] pour étudier les courses de

nombres premiers, puis on discute de divers prolongements et généralisations de ces travaux. On a ensuite reproduit l'article original [Bai20] dont le but est d'énoncer des résultats dans l'esprit de l'article de Rubinstein et Sarnak dans la plus grande généralité, avec pour objectif d'affaiblir au maximum les hypothèses usuelles d'indépendance linéaire. Dans le deuxième chapitre, on transpose les questions de courses de nombres premiers au contexte de la répartition des automorphismes de Frobenius dans les groupes de Galois d'extensions de corps de nombres. Pour ce faire, on introduit les outils nécessaires pour aboutir au théorème de Chebotarev, généralisation du théorème des nombres premiers à ce contexte. On parle ensuite des travaux de Ng ([Ng00]) et de Fiorilli-Jouve ([FJ20a]) concernant le phénomène de biais de Tchebychev pour les courses d'idéaux premiers. Enfin on a reproduit l'article original [Bai19] dans lequel on met notamment en évidence l'influence très importante que peut avoir la présence de zéros en $1/2$ de certaines fonctions L sur le biais de Tchebychev. Dans le troisième et dernier chapitre, on effectue le même travail pour la transposition des questions de courses de nombres premiers au contexte de la répartition des automorphismes de Frobenius dans les groupes de Galois d'extensions de corps de fonctions (en une variable sur un corps fini). On obtient un nouveau résultat du type théorème central limite pour certaines familles de telles extensions. Le chapitre se termine sur quelques pistes de recherches à venir.

Notations

La notation $A := B$ signifie que la quantité A est définie par la formule B. Le cardinal de l'ensemble E sera noté $\#E$ et parfois $|E|$. Le symbole log désigne le logarithme népérien. Les notations $f = O(g)$ et $f \ll g$ sont synonymes et veulent dire qu'il existe une constante $C > 0$ telles que pour tout x dans le domaine considéré on ait $|f(x)| \leq Cg(x)$. Quand la constante C dépend d'un ou plusieurs paramètres, la dépendance sera notée en indice des symboles $\ll$ et O. La notation $f(x) \asymp g(x)$ signifie que $f(x) \ll g(x)$ et $g(x) \ll f(x)$, avec les mêmes précisions de dépendance par rapport à des paramètres si nécessaire.

Sauf mention explicite du contraire, la lettre p dans une indexation signifie que celle-ci se fait sur un ensemble de nombres premiers. Le PGCD des entiers a et b est noté (a, b). L'indicatrice d'Euler de l'entier q est $\varphi(q) := \#\{n \in \mathbb{N} \mid 1 \leq n \leq q, (n, q) = 1\}$. Si $x \geq 2$, $\pi(x) := \#\{p \leq x\}$ et si a et q sont des entiers, on note $\pi(x; q, a) := \#\{p \leq x \mid p \equiv a \bmod q\}$ le nombre de nombres premiers inférieurs à x congrus à a modulo q. Le groupe des classes d'entiers inversibles modulo q est noté $(\mathbb{Z}/q\mathbb{Z})^\times$. On note X_q l'ensemble des caractères de Dirichlet modulo q, c'est-à-dire l'ensemble des morphismes $(\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$, prolongés par 0 à $\mathbb{Z}/q\mathbb{Z}$ puis relevés en des fonctions $\mathbb{Z} \longrightarrow \mathbb{C}$. On note X_q^* l'ensemble des caractères de Dirichlet primitifs modulo q, c'est-à-dire qui ne peuvent être induits par des caractères de Dirichlet modulo d avec d divisant strictement q.

Pour $x > 1$, la quantité $\mathrm{Li}(x)$ désigne le logarithme intégral

$$\int_2^x \frac{\mathrm{d}t}{\log t}.$$

Si K est un corps de nombres, son anneau des entiers, c'est-à-dire l'ensemble des entiers algébriques éléments de K (ou encore la clôture intégrale de $\mathbb{Z}$ dans K) est noté $\mathcal{O}_K$.

Chapitre 1

La méthode de Rubinstein et Sarnak

Il est connu depuis Dirichlet que si $q \geq 2$ et a est un entier premier avec q, alors il existe une infinité de nombres premiers $p \equiv a \bmod q$, autrement dit que $\pi(x;q,a) \underset{x\to+\infty}{\longrightarrow} +\infty$. À la fin du XIX$^{\text{ème}}$ siècle de la Vallée Poussin parvint à adapter sa démonstration du théorème des nombres premiers pour démontrer le théorème des nombres premiers en progressions arithmétiques : sous les mêmes hypothèses sur a et q, on a

$$\pi(x;q,a) \underset{x\to+\infty}{\sim} \frac{1}{\varphi(q)} \operatorname{Li}(x).$$

D'après le théorème des nombres premiers, il est équivalent de dire que

$$\frac{\pi(x;q,a)}{\pi(x)} \underset{x\to+\infty}{\longrightarrow} \frac{1}{\varphi(q)}.$$

Autrement dit, il y a équirépartition uniforme des classes $p \bmod q$ dans les $\varphi(q)$ classes inversibles modulo q.

Il est ensuite naturel, ayant fixé deux entiers a et b premiers avec q, de chercher à comparer plus finement les quantités $\pi(x;q,a)$ et $\pi(x;q,b)$. Par exemple, il avait été observé par Tchebychev dans une lettre de 1853 [Tch53] que $\pi(x;4,3) > \pi(x;4,1)$ pour les premiers milliers de valeurs de x. Bien que l'inégalité en question et son opposée ne persistent pas indéfiniment (Littlewood a montré que $\pi(x;4,3) - \pi(x;4,1) = \Omega_{\pm}\left(x^{1/2}\frac{\log\log\log x}{\log x}\right)$ [Lit14]), il existe un phénomène sous-jacent, appelé le *biais de Tchebychev*, expliquant la prépondérance visible des nombres premiers congrus à 3 modulo 4 par rapport aux nombres premiers congrus à 1 modulo 4. Dans leur article *Chebyshev's bias* [RS94], Rubinstein et Sarnak développent une nouvelle méthode permettant d'expliquer ce phénomène, et plus généralement d'étudier la question suivante : soient $q, D \geq 2$ et $a_1, \ldots, a_D$ des entiers premiers avec q, les inégalités $\pi(x;q,a_1) > \cdots > \pi(x;q,a_D)$ ont-elles lieu « souvent » ? On parle alors de courses de nombres premiers, ou de courses de Shanks-Rényi, en imaginant une « course » entre les D équipes constituées des nombres premiers $p \equiv a_i \bmod q$, et on se pose alors la question de savoir si une certaine configuration se produit souvent, du moins plus fréquemment que d'autres.

Le point de départ de la méthode de Rubinstein et Sarnak est l'utilisation de *formules explicites* permettant de relier la répartition des nombres premiers dans les progressions modulo q à la répartition des zéros des fonctions L de Dirichlet modulo q, étape classique depuis le célèbre mémoire de Riemann [Rie59] sur les nombres premiers. En étudiant les

phénomènes oscillatoires sous-jacents à ces formules explicites, et en particulier à l'aide du théorème de Kronecker-Weyl en analyse harmonique, il est alors possible de montrer que les restes dans le théorème des nombres premiers en progressions arithmétiques possèdent une distribution logarithmique limite. Une hypothèse d'indépendance linéaire portant sur les parties imaginaires positives des fonctions L de Dirichlet modulo q permet d'étudier plus en détails cette distribution limite.

Dans ce chapitre, on commence par détailler la méthode de Rubinstein et Sarnak, qui constitue le point de départ de nos travaux. Ensuite on s'intéresse à quelques prolongements de leurs travaux (notamment des affaiblissements d'hypothèses et la transposition des questions de courses de nombres premiers pour les polynômes irréductibles sur les corps finis). La dernière partie du chapitre reprend une partie des résultats de l'article original *Explicit Kronecker-Weyl theorems and applications to prime number races* [Bai20].

1.1 Courses de nombres premiers

Dans cette section, $q \geq 2$ est un entier et $a_1, \dots, a_D$ sont des entiers deux à deux distincts premiers avec q.

1.1.1 Le problème

Définition 1.1. *On note*

$$\mathcal{P}_{q;a_1,\dots,a_D} := \{x \geq 2 \mid \pi(x;q,a_1) > \cdots > \pi(x;q,a_D)\}.$$

L'objectif est de mesurer « la taille » de $\mathcal{P}_{q;a_1,\dots,a_D}$. Pour ce faire, il semble naturel d'étudier la densité naturelle

$$d(q;a_1,\dots,a_D) := \lim_{X\to+\infty} \frac{1}{X}\int_2^X \mathbf{1}_{\mathcal{P}_{q;a_1,\dots,a_D}}(t)\,\mathrm{d}t,$$

si elle existe. Cependant, cette notion de densité n'est pas bien adaptée à ce problème. Ainsi, Kaczorowski a montré dans [Kac95] sous l'hypothèse de Riemann pour la fonction L de Dirichlet associée au caractère non trivial χ_4 modulo 4 que $\underline{d}(4;3,1) < \overline{d}(4;3,1)$, où les barres désignent les limites inférieures et supérieures de la quantité ci-dessus, contredisant une conjecture de Knapowski et Turán dans [KT62] prédisant que $d(4;3,1) = 1$. La bonne notion de densité à considérer est la suivante.

Définition 1.2. *Soit A un borélien de $\mathbb{R}^+$. On dit que A admet une* ***densité logarithmique*** *lorsque la limite suivante existe :*

$$\delta(A) := \lim_{X\to+\infty} \frac{1}{\log X}\int_0^X \mathbf{1}_A(t)\frac{\mathrm{d}t}{t} = \lim_{X\to+\infty} \frac{1}{X}\int_0^X \mathbf{1}_A(e^t)\,\mathrm{d}t.$$

Remarque 1.3. Les densités considérées ici et dans la suite ne dépendent pas des « premières valeurs » des ensembles considérés, il n'y a donc aucune différence à considérer les intégrales partant de 0 ou de n'importe quel autre nombre réel (traditionnellement on préfère partir de 2, le plus petit nombre premier).

1.1.2 Formule explicite

Pour comparer les différentes quantités $\pi(x;q,a_i)$, Rubinstein et Sarnak les renormalisent en soustrayant le terme principal de l'équivalent donné par le théorème des nombres premiers en progressions arithmétiques. Ceux-ci introduisent alors les quantités

$$E(x,q,a_i) := \frac{\log x}{\sqrt{x}}(\varphi(q)\pi(x;q,a_i) - \pi(x))$$

pour $1 \leq i \leq D$, et

$$E_{q;a_1,\dots,a_D}(x) := (E(x,q,a_1),\dots,E(x,q,a_D)).$$

Il est clair que la densité logarithmique de $\mathcal{P}_{q;a_1,\dots,a_D}$ sera alors la densité logarithmique de l'ensemble

$$\{x \geq 2 \mid E(x,q,a_1) > \cdots > E(x,q,a_D)\}.$$

L'intérêt d'introduire les quantités $E(x,q,a_i)$ est qu'elles englobent exactement le comportement oscillatoire des termes d'erreur dans le théorème des nombres premiers dans les progressions arithmétiques $a_i + q\mathbb{Z}$, comme le montre la *formule explicite* suivante.

Proposition 1.4. *Supposons* GRH *pour les fonctions L de Dirichlet modulo q. Alors pour tout $x \geq 2$ et pour tout a premier avec q, on a*

$$E(x,q,a) = -c(q,a) - \sum_{\chi \neq \chi_0} \overline{\chi(a)} \sum_{\gamma_\chi} \frac{x^{i\gamma_\chi}}{\frac{1}{2} + i\gamma_\chi} + O\left(\frac{1}{\log x}\right),$$

où la sommation en γ_χ porte sur les parties imaginaires des zéros non triviaux de $L(s,\chi)$ et où $c(q,a) = -1 + \sum_{\substack{b^2 \equiv a \bmod q \\ 0 \leq b \leq q-1}} 1$.

Remarques 1.5.

i) Pour établir une telle formule, on commence par établir une formule explicite analogue pour la quantité $\varphi(q)\psi(x;q,a) - \psi(x)$, où $\psi(x) = \sum_{p^k \leq x} \log p$ et $\psi(x;q,a) = \sum_{\substack{p^k \leq x \\ p \equiv a \bmod q}} \log p$ sont les fonctions de Tchebychev usuelles, avant de procéder à une sommation partielle. La convergence de la série indexée par γ_χ est à comprendre au sens de la convergence des sommes symétriques $\lim_{T \to +\infty} \sum_{|\gamma_\chi| \leq T} \frac{x^{i\gamma_\chi}}{\frac{1}{2}+i\gamma_\chi}$. On insiste sur le fait que la série n'est pas absolument convergente (voir [Dav00, p.80]).

ii) Le fait que les termes oscillants dans la somme ci-dessus soient de la forme $x^{i\gamma_\chi}$ et non pas $e^{i\gamma_\chi}$ justifie que l'on va par la suite étudier $E(e^x,q,a)$ au lieu de $E(x,q,a)$, et donc justifie l'utilisation de la notion de densité logarithmique au lieu de celle de densité naturelle.

iii) La division par $\sqrt{x}$ provient de l'hypothèse de Riemann : la formule explicite pour $\varphi(q)\psi(x;q,a) - \psi(x)$ fait intervenir des termes de la forme x^ρ, avec ρ zéro de $L(s,\chi)$. Sous GRH, ρ est de la forme $\frac{1}{2} + i\gamma_\chi$ et donc $x^\rho = \sqrt{x}x^{i\gamma_\chi}$. Si l'on ne suppose pas l'hypothèse de Riemann, on peut, à la place de diviser par $\sqrt{x}$, diviser par x^{β_q}, où β_q est la borne supérieure des parties réelles des zéros des $L(s,\chi), \chi \neq \chi_0$. C'est ce qui est fait dans [Dev19] et dans [FJ20a] dans les énoncés où les auteurs ne supposent pas l'hypothèse de Riemann.

iv) Le terme constant $-c(q,a)$ est la source du biais de Tchebychev. En effet, on verra plus loin que la « valeur moyenne » de $E(x,q,a)$ est $-c(q,a)$, de sorte que si a et un carré modulo q et b n'est pas un carré modulo q, alors $\pi(x;q,a) - \pi(x;q,b)$ est « en moyenne » négatif.

1.1.3 Distribution limite

On définit maintenant la notion de distribution logarithmique limite, qui permettra ensuite de montrer l'existence de certaines densités logarithmiques.

Définition 1.6. *Soit $E : \mathbb{R}^+ \longrightarrow \mathbb{R}^D$ une fonction borélienne. On dit que E admet une **distribution logarithmique limite** s'il existe une mesure borélienne μ sur $\mathbb{R}^D$ telle que pour toute fonction continue bornée $f : \mathbb{R}^D \longrightarrow \mathbb{R}$, on ait*

$$\lim_{X\to+\infty} \frac{1}{X}\int_0^X f(E(e^t))\mathrm{d}t = \int_{\mathbb{R}^D} f(x)\,\mathrm{d}\mu(x).$$

Le théorème crucial pour établir l'existence d'une telle distribution limite pour la fonction $E_{q;a_1,\dots,a_D}$ est le suivant.

Théorème 1.7 (Kronecker-Weyl)**.** *Soient $\theta_1,\dots,\theta_r$ des nombres réels. Alors le sous-groupe*

$$\Gamma = \left\{\left(e^{i\theta_1 t},\dots,e^{i\theta_r t}\right) \mid t\in\mathbb{R}\right\}$$

de $\mathbb{T}^r := \{(z_1,\dots,z_r)\in\mathbb{C}^r \mid |z_1| = \cdots = |z_r| = 1\}$ est équiréparti dans un sous-tore de $\mathbb{T}^r$. Autrement dit, il existe un sous-groupe fermé H de $\mathbb{T}^r$ tel que pour toute fonction continue $f : \mathbb{T}^r \longrightarrow \mathbb{C}$ on ait

$$\lim_{X\to+\infty} \frac{1}{X}\int_0^X f\left(e^{i\theta_1 t},\dots,e^{i\theta_r t}\right)\,\mathrm{d}t = \int_H f(z)\,\mathrm{d}\mu(z)$$

où μ est la mesure de Haar normalisée de H. De plus, H est de dimension (en tant que sous-variété complexe de $\mathbb{T}^r$) la dimension de $\mathrm{Vect}_{\mathbb{Q}}(\theta_1,\dots,\theta_r)$. En particulier, si $\theta_1,\dots,\theta_r$ sont linéairement indépendants sur $\mathbb{Q}$ alors $H = \mathbb{T}^r$.

On reviendra plus en détails sur ce théorème, sa démonstration et ses applications dans la Section 1.4.

En notant

$$E^{(T)}(x,q,a) := -c(q,a) - \sum_{\chi\neq\chi_0} \overline{\chi(a)} \sum_{|\gamma_\chi|\leq T} \frac{x^{i\gamma_\chi}}{\frac{1}{2}+i\gamma_\chi}$$

pour $T \geq 1$, Rubinstein et Sarnak appliquent le théorème de Kronecker-Weyl à la famille finie $\{\gamma_\chi \mid \chi\neq\chi_0, 0\leq\gamma_\chi\leq T\}$ pour établir l'existence d'une distribution limite $\mu^{(T)}_{q;a_1,\dots,a_D}$ pour la fonction vectorielle $x\mapsto(E^{(T)}(x,q,a_1),\dots,E^{(T)}(x,q,a_D))$. Ils établissent ensuite que

$$\frac{1}{X}\int_2^X \left|E(e^x,q,a) - E^{(T)}(e^x,q,a)\right|^2 \mathrm{d}x \underset{\mathbb{T}\to+\infty}{\longrightarrow} 0,$$

ce qui leur permet de montrer que la famille de mesures $\{\mu^{(T)}_{q;a_1,\dots,a_D} \mid T \geq 1\}$ converge en loi vers une mesure $\mu_{q;a_1,\dots,a_D}$ qui se trouve être la distribution logarithmique limite de $E_{q;a_1,\dots,a_D}$.

Remarque 1.8. Le fait que $\frac{1}{X}\int_2^X \left|E(e^x,q,a) - E^{(T)}(e^x,q,a)\right|^2 \mathrm{d}x \underset{\mathbb{T}\to+\infty}{\longrightarrow} 0$ signifie que le reste $E(e^x,q,a)$ dans le théorème des nombres premiers dans la progression arithmétique $a+q\mathbb{Z}$ est B^2-presque périodique au sens de Besicovitch ([Bes55]). Il se trouve que de nombreux termes d'erreur de la théorie analytique des nombres sont de cette nature, comme observé dans [ANS14].

1.1.4 Existence de la densité

On souhaite désormais établir l'existence de la quantité

$$\lim_{X\to+\infty} \frac{1}{X}\int_2^X \mathbf{1}_{E(e^t,q,a_1)>\cdots>E(e^t,q,a_D)}\,\mathrm{d}t,$$

autrement dit, on veut être capable de remplacer les fonctions continues bornées f de la Définition 1.6 par l'indicatrice de l'ensemble $\{(x_1,\dots,x_D)\in\mathbb{R}^D \mid x_1>\cdots>x_D\}$. Pour ce faire, on peut utiliser un argument standard d'approximation de fonction indicatrice par des fonctions lipschitziennes. Cependant, un passage à la limite lors de cet argument révèle qu'il est nécessaire de savoir que la mesure $\mu_{q;a_1,\dots,a_D}$ assigne une masse nulle aux hyperplans de la forme $\{(x_1,\dots,x_D)\in\mathbb{R}^D \mid x_j = x_{j+1}\}$ avec $1\leq j\leq D-1$. C'est par exemple le cas si cette mesure est absolument continue par rapport à la mesure de Lebesgue.

On voit donc qu'une compréhension de la régularité de la mesure $\mu_{q;a_1,\dots,a_D}$ est nécessaire pour poursuivre cette étude. Pour obtenir plus d'informations sur cette mesure, Rubinstein et Sarnak introduisent l'hypothèse suivante.

Conjecture 1.9 (GSH : Grand Simplicity Hypothesis)**.** *Le multi-ensemble*

$$\{\gamma\geq 0 \mid \exists q\in\mathbb{Z}, \exists\chi\in X_q^*, \exists\beta\in]0,1[, L(\beta+i\gamma,\chi)=0\}$$

est linéairement indépendant sur $\mathbb{Q}$*.*

Remarques 1.10.

i) L'hypothèse serait la même en considérant les parties imaginaires positives des zéros non triviaux des $L(s,\chi)$ avec χ non nécessairement primitif. En effet, si χ^* est le caractère primitif induisant χ, on a $L(s,\chi)=L(s,\chi^*)P(s)$ où $P(s)$ est un produit eulérien fini n'ayant que des zéros de partie réelle nulle.

ii) On parle de multi-ensemble car on compte les zéros des $L(s,\chi)$ avec multiplicité. L'hypothèse GSH implique donc que tous les zéros des fonctions L de Dirichlet modulo q sont simples.

iii) L'hypothèse GSH implique en particulier l'inexistence de zéros réels dans $]0,1[$ pour les fonctions L de Dirichlet, donc en particulier l'inexistence de zéro de Siegel et la conjecture de Chowla sur la non annulation en $1/2$ de ces fonctions.

iv) Dans tout ce qui suit, il suffirait de supposer l'indépendance linéaire des parties imaginaires positives des zéros non triviaux des fonctions L de Dirichlet modulo q pour établir des résultats à q fixé.

Sous l'hypothèse GSH, le théorème de Kronecker-Weyl implique que, pour tout $T \geq 1$, l'ensemble $\{e^{i\gamma_\chi t} \mid \chi \neq \chi_0, 0 < \gamma_\chi \leq T, t \in \mathbb{R}\}$ est équiréparti dans $\mathbb{T}^{N_T}$, où $N_T = \#\{\gamma_\chi \mid \chi \neq \chi_0, 0 < \gamma_\chi \leq T\}$. Cela permet de calculer la fonction caractéristique $\hat{\mu}^{(T)}_{q;a_1,\dots,a_D}$ de la mesure $\mu^{(T)}_{q;a_1,\dots,a_D}$: pour tout $\xi \in \mathbb{R}^D$,

$$\hat{\mu}^{(T)}_{q;a_1,\dots,a_D}(\xi) = \exp\left(-i\sum_{j=1}^{D} c(q,a_j)\xi_j\right) \times \prod_{\chi\neq\chi_0} \prod_{0<\gamma_\chi\leq T} J_0\left(\frac{2\left|\sum_{j=1}^{D}\chi(a_j)\xi_j\right|}{\sqrt{\frac{1}{4}+\gamma_\chi^2}}\right),$$

où J_0 est la fonction de Bessel de première espèce

$$J_0(z) = \sum_{n=0}^{+\infty} \frac{(-1)^n z^{2n}}{2^{2n}(n!)^2}.$$

L'apparition de la fonction de Bessel ici est naturelle, car celle-ci n'est rien d'autre que la fonction caractéristique de la partie réelle d'une variable aléatoire uniforme sur le cercle unité, et le théorème de Kronecker-Weyl permet grossièrement de traiter chaque terme $\overline{\chi(a_i)}\frac{e^{i\gamma_\chi t}}{\frac{1}{2}+i\gamma_\chi} + \chi(a_i)\frac{e^{-i\gamma_\chi t}}{\frac{1}{2}-i\gamma_\chi}$ de la formule explicite pour $E^{(T)}(e^t, q, a_i)$ comme la partie réelle d'une variable aléatoire uniforme sur le cercle de rayon $\frac{|\chi(a_i)|}{\sqrt{\frac{1}{4}+\gamma_\chi^2}}$. Notons que cette formule donne une nouvelle démonstration, conditionnelle, de la convergence en loi de la famille de mesures $\{\mu^{(T)}_{q;a_1,\dots,a_D} \mid T \geq 1\}$, via le théorème de Lévy. En effet, on a évidemment $J_0(t) = 1 - \frac{t^2}{4} + O(t^4)$ au voisinage de 0, et comme la série $\sum_{\gamma_\chi} \frac{1}{\frac{1}{4}+\gamma_\chi^2}$ converge (d'après la théorie générale des fonctions entières d'ordre 1, ou encore d'après les estimées classiques sur le nombre de zéros de $L(s,\chi)$ dans un rectangle donné *cf.* [MV07, Theorem 10.17]), le produit ci-dessus converge quand T tend vers l'infini. Toujours d'après le théorème de Lévy, on en déduit donc la formule suivante pour la fonction caractéristique de $\mu_{q;a_1,\dots,a_D}$.

Théorème 1.11 ([RS94])**.** *Supposons* GRH *pour les fonctions L de Dirichlet modulo q et* GSH*. On a*

$$\hat{\mu}_{q;a_1,\dots,a_D}(\xi) = \exp\left(-i\sum_{j=1}^{D} c(q,a_j)\xi_j\right) \times \prod_{\chi\neq\chi_0} \prod_{\gamma_\chi>0} J_0\left(\frac{2\left|\sum_{j=1}^{D}\chi(a_j)\xi_j\right|}{\sqrt{\frac{1}{4}+\gamma_\chi^2}}\right)$$

pour tout $\xi \in \mathbb{R}^D$.

Cette formule a plusieurs conséquences importantes. Tout d'abord, on lit immédiatement que la valeur moyenne $\int_{\mathbb{R}^D} X \,\mathrm{d}\mu_{q;a_1,\dots,a_D}(X)$ vaut $(-c(q,a_1),\dots,-c(q,a_D))$ ce qui justifie l'affirmation précédente du fait que la valeur moyenne de $E(x,q,a_i)$ est $-c(q,a_i)$.

Ensuite, si $D < \varphi(q)$, on peut montrer que $\hat{\mu}_{q;a_1,\dots,a_D}(\xi)$ décroît rapidement en l'infini, ce qui implique que $\mu_{q;a_1,\dots,a_D}$ admet une densité par rapport à la mesure de Lebesgue, qui est en fait une fonction analytique. Comme dit précédemment, cela implique l'existence de $\delta(\mathcal{P}_{q;a_1,\dots,a_D})$ qui n'est autre que $\mu_{q;a_1,\dots,a_D}(\{(x_1,\dots,x_D) \in \mathbb{R}^D \mid x_1 > \cdots > x_D\})$.

Dans le cas où $D = \varphi(q)$, il est clair par définition que pour tout $x \geq 2$, $E_{q;a_1,\dots,a_D}(x) \in (1,\dots,1)^\perp$, ce qui implique facilement que $\hat{\mu}_{q;a_1,\dots,a_D}(\xi)$ est $(1,\dots,1)$-périodique. Le même raisonnement que ci-dessus montre que $\mu_{q;a_1,\dots,a_D}$ admet une densité par rapport à la mesure

de Lebesgue de l'hyperplan $(1,\dots,1)^\perp$, mesure qui n'assigne pas de masse aux sous-espaces $\{(x_1,\dots,x_D)\in\mathbb{R}^D \mid x_j = x_{j+1}\}\cap(1,\dots,1)^\perp$. On peut alors comme précédemment conclure que $\delta(\mathcal{P}_{q;a_1,\dots,a_D})$ existe.

Enfin, la même méthode que ci-dessus montre que la quantité $E(x,q,a)-E(x,q,b)$ admet également une distribution logarithmique limite, symétrique par rapport à sa moyenne $c(q,b)-c(q,a)$ (car la fonction J_0 est paire), ce qui a pour conséquence que

$$\delta(\mathcal{P}_{q;a,b})\begin{cases} < \frac{1}{2} \text{ si } a\equiv\square \bmod q \text{ et } b\not\equiv\square \bmod q \\ = \frac{1}{2} \text{ si } a,b\equiv\square \bmod q \text{ ou si } a,b\not\equiv\square \bmod q \\ > \frac{1}{2} \text{ si } a\not\equiv\square \bmod q \text{ et } b\equiv\square \bmod q, \end{cases}$$

où l'on a noté $c\equiv\square \bmod q$ si c est un carré modulo q et $c\not\equiv\square \bmod q$ si c n'est pas un carré modulo q. Ce résultat justifie l'existence du biais de Tchebychev. En effet, 1 étant un carré modulo 4 et 3 n'étant pas un carré modulo 4, on obtient (en supposant GRH et GSH) que $\delta(\mathcal{P}_{4;1,3})<\frac{1}{2}$.

1.1.5 Vue d'ensemble des résultats de Rubinstein et Sarnak

On rassemble dans le prochain énoncé une partie des résultats de Rubinstein et Sarnak sur ce problème des courses de nombres premiers.

Théorème 1.12 (Rubinstein, Sarnak, [RS94])**.** *Supposons* GRH *pour les fonctions L de Dirichlet modulo q. Alors la fonction $E_{q;a_1,\dots,a_D}$ admet une distribution logarithmique limite. Si on suppose de plus* GSH*, alors $\delta(\mathcal{P}_{q;a_1,\dots,a_D})$ existe et vérifie $0<\delta(\mathcal{P}_{q;a_1,\dots,a_D})<1$. De plus, en supposant* GRH *pour toutes les fonctions L de Dirichlet, on a*

$$\max_{b_1,\dots,b_D\in(\mathbb{Z}/q\mathbb{Z})^\times}\left|\delta(\mathcal{P}_{q;b_1,\dots,b_D})-\frac{1}{D!}\right| \underset{q\to+\infty}{\longrightarrow} 0.$$

Remarques 1.13.

i) Le dernier point du théorème précédent dit que tout biais dans des courses de nombres premiers modulo q disparaît uniformément lorsque q tend vers l'infini. C'est un phénomène de type « théorème central limite » qui reviendra à plusieurs reprises dans cette thèse. Notons de plus que ce résultat suppose le nombre de participants D fixé.

ii) Rubinstein et Sarnak déterminent également à quelle condition la densité de $\mu_{q;a_1,\dots,a_D}$ est invariante par permutation des variables : ça ne se produit qu'en présence de deux participants qui sont simultanément des carrés ou des non carrés modulo q, et en présence de trois participants qui sont liés par les relations $a_2=\rho a_1, a_3=\rho a_2$ où ρ est une racine cubique de 1 dans $(\mathbb{Z}/q\mathbb{Z})^\times$.

Rubinstein et Sarnak s'intéressent également au biais entre la répartition des nombres premiers qui sont des carrés modulo q et la répartition de ceux qui ne sont pas des carrés modulo q, dans le cas où $q=4, q=p^\alpha$ ou $q=2p^\alpha$, c'est-à-dire les cas où il y a autant de carrés que de non carrés dans $(\mathbb{Z}/q\mathbb{Z})^\times$. Autrement dit, avec la même méthode que ci-dessus, ceux-ci étudient la distribution logarithmique limite de la quantité

$$E_{q;NR,R}(x)=\frac{\log x}{\sqrt{x}}(\pi_{NR}(x,q)-\pi_R(x,q)),$$

où

$$\pi_R(x,q) := \sum_{\substack{p\leq x \\ \exists x\in\mathbb{Z}, x^2\equiv p \bmod q}} 1$$

et

$$\pi_{NR}(x,q) := \pi(x) - \pi_R(x,q).$$

Sous GRH pour les fonctions L de Dirichlet, ils établissent comme ci-dessus l'existence de cette distribution limite $\mu_{q;NR,R}$, et obtiennent également une minoration de $\mu_{q;NR,R}([\lambda,+\infty[)$ et de $\mu_{q;NR,R}(]-\infty,-\lambda])$ pour tout $\lambda > 0$ assez grand. Ceci implique notamment que $\underline{\delta}(\mathcal{P}_{q;NR,R}) > 0$ et $\overline{\delta}(\mathcal{P}_{q;NR,R}) < 1$, où

$$\mathcal{P}_{q;NR,R} := \{x \geq 2 \mid \pi_{NR}(x,q) > \pi_R(x,q)\}$$

(un argument de symétrie par rapport à la moyenne 1 de $\mu_{q;N,R}$ montre en fait directement que $\underline{\delta}(\mathcal{P}_{q;NR,R}) > \frac{1}{2}$). Dans le cas où $q = 4$, on a évidemment $\pi_{NR}(x,4) = \pi(x;4,3)$ et $\pi_R(x,4) = \pi(x;4,1)$ donc on retrouve en particulier le célèbre résultat de Littlewood sur l'existence d'une infinité de changements de signe de $\pi(x;4,3) - \pi(x;4,1)$. Le phénomène d'atténuation du biais est également présent dans ce contexte : sous GRH et GSH, on a

$$\delta(\mathcal{P}_{q;NR,R}) \underset{q\to+\infty, q=p^\alpha \text{ ou } q=2p^\alpha}{\longrightarrow} \frac{1}{2}.$$

Pour finir, la formule donnant la fonction caractéristique de $\mu_{q;a_1,\dots,a_D}$ et de $\mu_{q;NR,R}$ sous GRH et GSH permet à Rubinstein et Sarnak de calculer les valeurs numériques de certaines densités (conditionnellement à ces hypothèses). Par exemple, ils calculent

$$\delta(\mathcal{P}_{4;3,1}) \approx 0,9959\dots$$

et

$$\delta(\mathcal{P}_{3;2,1)} \approx 0,9990\dots,$$

tandis que

$$\delta(\mathcal{P}_{\mathrm{Li},\pi}) \approx 0,99999973,$$

où

$$\mathcal{P}_{\mathrm{Li},\pi} := \{x \geq 2 \mid \mathrm{Li}(x) > \pi(x)\}.$$

1.2 Prolongement des travaux de Rubinstein et Sarnak

Les travaux de Rubinstein et Sarnak présentés dans la section précédente amènent naturellement à plusieurs types de prolongements. Dans cette section très bibliographique, on recense plusieurs travaux qui motivent certains des résultats de cette thèse. On omet pour l'instant les généralisations « non abéliennes » dûes à Ng dans [Ng00] et Cha-Im dans [CI11], dans le contexte des corps de nombres et des corps de fonctions sur les corps finis. Ces généralisations seront traitées dans les Chapitre 2 et 3 respectivement.

1.2.1 Comportement asymptotique du biais

Dans [FM13], Fiorilli et Martin obtiennent un développement asymptotique, conditionnel à GRH et GSH, pour $\delta(\mathcal{P}_{q;a,b})$, qui fournit l'estimation suivante.

Théorème 1.14 (Fiorilli-Martin, [FM13])**.** *Supposons* GRH *et* GSH*. Alors pour tout $q \geq 2$ et tout $a, b \in (\mathbb{Z}/q\mathbb{Z})^\times$ tels que a soit un non carré et b soit un carré modulo q, on a*

$$\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2} + \frac{\rho(q)}{\sqrt{2\pi V(q;a,b)}} + O\left(\frac{\rho(q)^3}{V(q;a,b)^{3/2}}\right)$$

où $\rho(q)$ désigne le nombre de racines carrées de n'importe quel carré de $(\mathbb{Z}/q\mathbb{Z})^\times$ et

$$V(q;a,b) := \sum_{\chi \neq \chi_0} |\chi(a) - \chi(b)|^2 \sum_{\gamma_\chi} \frac{1}{\frac{1}{4} + \gamma_\chi^2} \underset{q \to +\infty}{\sim} 2\varphi(q) \log q.$$

Remarque 1.15. La quantité $\rho(q)$ est $O_\varepsilon(q^\varepsilon)$ pour tout $\varepsilon > 0$.

À l'aide d'estimations précises sur la variance $V(q;a,b)$, Fiorilli et Martin établissent la liste des courses de nombres premiers à deux participants exhibant le biais le plus extrême, plus précisément telles que $\delta(\mathcal{P}_{q;a,b}) > 9/10$. Ainsi la course de nombres premiers à deux participants la plus biaisée est celle entre les classes 5 et 1 modulo 24 : on a $\delta(\mathcal{P}_{24;5,1}) \approx 0.999988\ldots$. Remarquons au passage que l'on a toujours $\delta(\mathcal{P}_{q;a_1,a_2,\ldots,a_D}) \leq \delta(\mathcal{P}_{q;a_1,a_2})$ de sorte qu'il s'agit véritablement de la course de nombres premiers en progressions arithmétiques la plus biaisée.

1.2.2 Course entre carrés et non carrés

En ce qui concerne la course « N contre R » entre les non carrés et les carrés modulo q, Fiorilli montre notamment dans [Fio14] que l'atténuation du biais observée par Rubinstein et Sarnak ne tient plus lorsque l'on travaille avec des modules q arbitraires. Pour que la course soit équilibrée, on compare les fonctions de comptages renormalisées en fonction du nombre de carrés dans $\mathbb{Z}/q\mathbb{Z}$: on note $\delta(q; NR, R)$ la densité logarithmique de l'ensemble des $x \geq 2$ tels que

$$\frac{\rho(q)}{\varphi(q)} \#\{p \leq x \mid \exists a \in \mathbb{Z}, x^2 \equiv p\} < \frac{1}{\varphi(q)\left(1 - \frac{1}{\rho(q)}\right)} \#\{p \leq x \mid \forall a \in \mathbb{Z}, x^2 \not\equiv p\}.$$

En particulier, Fiorilli produit des courses à biais extrême (c'est-à-dire tels que $\delta(\mathcal{P}_{q;N,R})$ soit arbitrairement proche de 1) en choisissant des modules q hautement composés. Il montre même plus précisément le résultat suivant.

Théorème 1.16 (Fiorilli, [Fio14])**.** *Supposons* GRH *et* GSH*. Alors*

$$\overline{\{\delta(q; NR, R) \mid q \geq 2\}} = \left[\frac{1}{2}, 1\right].$$

De l'autre côté, Fiorilli montre que la situation de biais extrême est exceptionnelle, au sens où pour tout $\varepsilon > 0$, le nombre de modules $q \leq x$ tels que $\delta(q; NR, R) > 1 - \varepsilon$ est $o(x)$ quand x tend vers l'infini.

1.2.3 Affaiblissement de GSH

Un autre type de prolongement des travaux de Rubinstein et Sarnak concerne les tentatives d'affaiblissement de l'hypothèse GSH d'indépendance linéaire utilisées par ceux-ci.

Dans [MN20], Martin et Ng cherchent des conditions plus faibles sur les zéros des fonctions L de Dirichlet modulo q afin d'établir l'existence et la stricte positivité de la densité $\delta(\mathcal{P}_{q;a_1,\dots,a_D})$. Ils posent la définition suivante, sur laquelle nous reviendrons.

Définition 1.17. *Soit $q \geq 2$ et $a_1, \dots, a_D$ des entiers premiers avec q. On dit que la course entre (les nombres premiers congrus à) $a_1, \dots, a_D$ est **faiblement inclusive** lorsque pour toute permutation σ de $\{1, \dots, D\}$, la densité logarithmique $\delta(\mathcal{P}_{q;a_{\sigma(1)},\dots,a_{\sigma(D)}})$ existe. On dit de plus qu'elle est **inclusive** lorsque $\delta(\mathcal{P}_{q;a_{\sigma(1)},\dots,a_{\sigma(D)}}) > 0$ pour toute telle permutation σ.*

Les résultats de Rubinstein et Sarnak montrent donc qu'en supposant GRH et GSH, toute course de nombres premiers est inclusive, en particulier faiblement inclusive. Dans l'optique d'affaiblir l'hypothèse GSH, Martin et Ng introduisent la notion de *zéro auto-suffisant* (« self-sufficient zero »).

Définition 1.18. *Soit $q \geq 2$. Posons $\beta_q := \sup\{\beta \in]0,1[\mid \exists \chi \in X_q, \exists \gamma \in \mathbb{R}, L(\beta+i\gamma, \chi) = 0\}$. Pour tout caractère de Dirichlet χ modulo q, notons $\Gamma(\chi) := \{\gamma \geq 0 \mid L(\beta_q + i\gamma, \chi) = 0\}$. On dit que $\gamma \in \Gamma(\chi)$ est **auto-suffisant** lorsque γ est $\mathbb{Q}$-linéairement indépendant de $\bigcup_{\chi' \in X_q} \Gamma(\chi') \setminus \{\gamma\}$. Pour tout caractère de Dirichlet χ modulo q, notons $\Gamma^S(\chi) := \{\gamma \in \Gamma(\chi) \mid \gamma$ est auto-suffisant$\}$.*

Remarques 1.19.

i) On utilisera souvent l'appellation abusive « zéro » concernant le réel γ lorsque c'est $\beta + i\gamma$ qui est un zéro d'une fonction L de Dirichlet.

ii) Dans [MN20], l'ensemble $\Gamma(\chi)$ ne concerne que les zéros de partie réelle $\frac{1}{2}$ car les auteurs supposent GRH pour les fonctions L de Dirichlet modulo q. Comme la notion de zéros auto-suffisants a été généralisée en l'absence de l'hypothèse de Riemann dans [Dev19], on donne directement la définition ci-dessus.

De tels zéros, s'ils existent, permettent de traiter les termes $e^{i\gamma x}$ dans les formules explicites pour les fonctions de comptage de nombres premiers comme des variables aléatoires uniformes sur le cercle unité qui sont indépendantes des autres termes. En conséquence, la fonction caractéristique $\hat{\mu}_{q;a_1,\dots,a_D}$ admet un certain nombre de facteurs de la forme $J_0\left(\frac{2\left|\sum_{\chi \neq \chi_0} \chi(a_j)\xi_j\right|}{\sqrt{\frac{1}{4}+\gamma^2}}\right)$, dont la petitesse à l'infini peut impliquer certains types de régularité pour la mesure $\mu_{q;a_1,\dots,a_D}$ (absence d'atomes, existence d'une densité, régularité de la densité).

Théorème 1.20 (Martin-Ng, [MN20])**.** *Soit $q \geq 2$ et a et b des entiers premiers avec q. Supposons GRH pour les fonctions L de Dirichlet modulo q. Si $\#\bigcup_{\substack{\chi \in X_q \\ \chi(a) \neq \chi(b)}} \Gamma^S(\chi) \geq 3$ alors la course entre a et b est faiblement inclusive (autrement dit $\delta(\mathcal{P}_{q;a,b})$ existe). Si de plus la somme $\sum_{\substack{\chi \in X_q \\ \chi(a) \neq \chi(b)}} \sum_{\gamma \in \Gamma^S(\chi)} \frac{1}{\gamma}$ diverge, alors la course entre a et b est inclusive (autrement dit on a $0 < \delta(\mathcal{P}_{q;a,b}) < 1$).*

Les hypothèses de l'énoncé ci-dessus constituent une grande amélioration par rapport à l'hypothèse GSH de Rubinstein et Sarnak (qui revient à supposer que tous les zéros non triviaux des fonctions L de Dirichlet modulo q sont auto-suffisants). Ainsi, même une proportion négligeable de zéros vérifiant une hypothèse particulière d'indépendance linéaire sur $\mathbb{Q}$ suffit à impliquer l'inclusivité faible, et même l'inclusivité d'une course de nombres premiers à deux participants. En effet, le nombre de zéros des fonctions L de Dirichlet modulo q de parties imaginaires entre 0 et T est équivalent à $\frac{\varphi(q)}{2\pi}T\log(qT)$ ([MV07, Theorem 10.17]), et en présence de seulement $Tg(T)$ zéros auto-suffisants (correspondant à des caractères $\chi \in X_q$ séparant a et b au sens où $\chi(a) \neq \chi(b)$) inférieurs à T, avec $g(T) \underset{T\to+\infty}{\longrightarrow} +\infty$ et $g(T) = o(\log T)$, la dernière hypothèse du théorème ci-dessus est bien vérifiée.

Pour les courses à plus de participants, Martin et Ng obtiennent le résultat suivant, dans le même esprit que le précédent.

Théorème 1.21 (Martin-Ng, [MN20])**.** *Soit $q \geq 2$. Supposons* GRH *pour les fonctions L de Dirichlet modulo q. Si pour tout $\chi \in X_q \setminus \{\chi_0\}$, on a $\#\Gamma^S(\chi) \geq 2\varphi(q)+1$ alors toute course de nombres premiers modulo q est faiblement inclusive. Si de plus on a $\sum_{\gamma\in\Gamma^S(\chi)} \frac{1}{\gamma} = +\infty$ pour tout $\chi \in X_q \setminus \{\chi_0\}$ alors toute course de nombres premiers modulo q est inclusive.*

Par la suite, Devin est parvenue à affaiblir encore les hypothèses de Martin et Ng pour des courses à deux participants, associées à une classe large de fonctions L, appelées fonctions L analytiques, inspirée de [IK04, Chapitre 5]. On citera simplement pour illustrer la variété des applications possibles de ses résultats que ses énoncés peuvent par exemple s'appliquer à la répartition des angles des nombres premiers de Gauss (dans $\mathbb{Z}[i]$), voir [Dev19, Theorem 3.7]. Pour une autre approche générale, cette fois-ci concernant l'existence d'une distribution limite de fonctions B^1-presque périodiques, on cite [ANS14], dans lequel les auteurs montrent en particulier que beaucoup de restes dans des estimations classiques de théorie analytique des nombres sont de cette nature. Dans notre contexte de courses de nombres premiers, on peut extraire de l'article [Dev19] les deux énoncés suivants.

Théorème 1.22 (Devin, [Dev19])**.** *Soit $q \geq 2$ entier et a et b des entiers premiers avec q.*

i) S'il existe $\chi \in X_q$ tel que $\chi(a) \neq \chi(b)$ et $\Gamma^S(\chi) \neq \emptyset$ alors la course entre a et b est faiblement inclusive.

ii) S'il existe $\varepsilon > 0$ tel que pour tout T suffisamment grand, il existe $\chi \in X_q$ vérifiant $\chi(a) \neq \chi(b)$ et $\gamma \in \Gamma(\chi)\cap]0, T^{1/2-\varepsilon}[$ qui est $\mathbb{Q}$-linéairement indépendant de $\Gamma_q\cap]T^{1/2-\varepsilon}, T[$, alors la course entre a et b est faiblement inclusive.

On notera que ces énoncés ne nécessitent pas l'hypothèse de Riemann.

1.2.4 Influence de zéros hors de la droite critique

Dans l'autre sens, Ford-Konyagin puis Ford-Konyagin-Lamzouri montrent dans une série de trois articles ([FK02], [FK03], [FLK13]) que certaines configurations particulières de zéros de fonctions L de Dirichlet hors de la droite critique impliquent des comportements pathologiques pour certaines courses de nombres premiers. Ainsi, ceux-ci construisent, en supposant l'existence de certaines configurations de zéros, des courses de nombres premiers modulo de nombreux entiers q telles que :

i) Il existe a_1, a_2, a_3 deux à deux distincts et premiers avec q tels que $\pi(x;q,a_1) > \pi(x;q,a_2) > \pi(x;q,a_3)$ ne se produit jamais pour x suffisamment grand.
ii) Il existe $x_0 \geq 2$ tel que pour tout $x \geq x_0$, il existe $a, b \in (\mathbb{Z}/q\mathbb{Z})^\times$ tel que $\pi(x;q,a) \geq \pi(x;q,1)$ et $\pi(x;q,b) \leq \pi(x;q,1)$.
iii) Pour tout $2 \leq D \leq \varphi(q)$ et $a_1, \dots, a_D$ deux à deux distincts et premiers avec q, le nombre de permutations σ de $\{1, \dots, D\}$ telles que l'inégalité $\pi(x;q,a_1) > \cdots > \pi(x;q,a_D)$ se produit pour des x arbitrairement grands est inférieur ou égal à $r(r-1)$.
iv) Il existe a et b distincts et premiers avec q tels que $d(\mathcal{P}_{q;a,b}) = 0$.

Remarques 1.23.
i) Certaines des configurations de Ford et Konyagin pour *i)* ci-dessus satisfont GSH, on voit donc que l'hypothèse GSH seule n'implique pas les résultats de Rubinstein et Sarnak.
ii) Kaczorowski a montré ([Kac93]) la négation du point *ii)* ci-dessus en supposant GRH pour les fonctions L de Dirichlet modulo q.
iii) Le point *iv)* ci-dessus fait intervenir une densité naturelle, et en particulier la densité logarithmique sous-jacente est également nulle. Ce point *iv)* est en fait plus difficile à établir que le point *i)* car il est connu inconditionnellement que $\mathcal{P}_{q;a,b}$ est non borné pour beaucoup de valeurs de q, a et b.

1.2.5 Courses entre entiers ayant k facteurs premiers

Dans [Men18], Meng généralise le problème des courses de nombres premiers dans les progressions arithmétiques à celui des courses entre entiers dans ces mêmes progressions ayant exactement k facteurs premiers. Il faut bien sûr préciser si l'on compte les facteurs premiers avec multiplicité (avec la fonction arithmétique Ω) ou sans multiplicité (avec la fonction arithmétique ω). Meng traite les deux cas, et obtient (en supposant GRH pour les fonctions L de Dirichlet modulo q ainsi que la simplicité des zéros non triviaux de celles-ci) des formules explicites pour les différences des fonctions de comptage des entiers n vérifiant $\omega(n) = k$ ou $\Omega(n) = k$ dans différentes progressions arithmétiques modulo q. Ces formules explicites lui permettent de poursuivre une analyse similaire à celle de Rubinstein et Sarnak.

Définition 1.24. *Soit $q \geq 2$ et a un entiers premier avec q. Pour tout entier $k \geq 1$ et $x \geq 2$, on pose*

$$\pi_k(x;q,a) := \#\{n \leq x \mid n \equiv a \bmod q, \omega(n) = k\}$$

et

$$N_k(x;q,a) := \#\{n \leq x \mid n \equiv a \bmod q, \Omega(n) = k\}.$$

Théorème 1.25 (Meng, [Men18])**.** *Soit $q \geq 2$ et a, b des entiers premiers avec q. Supposons* GRH *et* GSH *pour les fonctions L de Dirichlet modulo q. Alors pour tout entier $k \geq 1$,*

$$\delta_{\omega_k}(q;a,b) := \lim_{X \to +\infty} \frac{1}{X} \int_2^X \mathbf{1}_{\pi_k(e^t;q,a) > \pi_k(e^t;q,b)} \, \mathrm{d}t$$

et

$$\delta_{\Omega_k}(q;a,b) := \lim_{X \to +\infty} \frac{1}{X} \int_2^X \mathbf{1}_{N_k(e^t;q,a) > N_k(e^t;q,b)} \, \mathrm{d}t$$

existent. De plus, si a et b sont simultanément des carrés ou des non carrés modulo q, alors pour tout $k \geq 1$, $\delta_{\omega_k}(q;a,b) = \delta_{\Omega_k}(q;a,b) = \frac{1}{2}$, tandis que si a est un carré modulo q et b n'est pas un carré modulo q alors on a pour tout $k \geq 1$,

$$1 - \delta_{\Omega_{2k-1}}(q;a,b) < \delta_{\Omega_{2k}}(q;a,b) < \frac{1}{2} < \delta_{\Omega_{2k+1}}(q;a,b) < 1 - \delta_{\Omega_{2k}}(q;a,b),$$

$$\delta_{\omega_k}(q;a,b) < \delta_{\omega_{k+1}}(q;a,b) < \frac{1}{2},$$

$$\delta_{\Omega_{2k}}(q;a,b) = \delta_{\omega_{2k}}(q;a,b)$$

et

$$\delta_{\Omega_{2k-1}}(q;a,b) = 1 - \delta_{\omega_{2k-1}}(q;a,b).$$

Remarques 1.26.

i) Ford et Sneed avaient auparavant étudié le cas $k = 2$ ([FS10]) et mis en évidence l'inversion du sens du biais de Tchebychev par rapport aux courses de nombres premiers.

ii) Plus généralement, les résultats de Meng montrent que le biais de Tchebychev change de sens selon la parité de l'entier k lorsque l'on compte les facteurs premiers avec multiplicités.

iii) Meng obtient également des développements asymptotiques pour les quantités $\delta_{\omega_k}(q;a,b)$ et $\delta_{\Omega_k}(q;a,b)$ en fonction de k, qui impliquent une atténuation du biais de Tchebychev lorsque k tend vers l'infini.

1.2.6 Courses à plus de deux participants

Pour finir cette section, on s'intéresse à des travaux concernant des courses de nombres premiers faisant intervenir au moins trois participants.

Martin-Feuerverger ont donné dans [FM00] les premiers exemples de courses de nombres premiers à trois participants a_1, a_2, a_3 biaisée, c'est-à-dire telles que $\delta(\mathcal{P}_{q;a_1,a_2,a_3}) \neq \frac{1}{6}$, bien que a_1, a_2, a_3 soient simultanément des carrés ou des non carrés modulo q. Dans [Mar02], Martin analyse ce phénomène en associant à chaque caractère de Dirichlet χ modulo q une variable aléatoire $X(\chi)$, de telle sorte que, en supposant toujours GRH et GSH, les $X(\chi)$ sont indépendantes et telles que la distribution (logarithmique) limite de $E(x;q,a)$ soit la loi de $-c(q,a) - \sum_{\chi \neq \chi_0} \overline{\chi(a)} X(\chi)$. L'analyse de Martin révèle qu'un tel biais peut être causé par les différentes tailles des variances des $X(\chi)$, ces tailles étant directement reliées aux conducteurs des caractères de Dirichlet modulo q, ainsi que leurs parités en raison de la formule

$$\mathrm{Var}(X(\chi)) = \log \frac{q_\chi}{\pi} - \gamma - (1 + \chi(-1)) \log 2 - 2\mathfrak{Re} \frac{L'(1,\chi)}{L(1,\chi)},$$

où ici γ désigne la constante d'Euler et $q_\chi \leq q$ est le conducteur de χ. Toujours sous GRH et GSH, Lamzouri ([Lam13]) a par la suite montré que pour tout $D \geq 3$, et pour tout q suffisamment grand en fonction de D, il existe une course de nombres premiers modulo q à D participants qui est biaisée, bien que tous les participants soient simultanément des carrés (ou des non carrés).

On a vu plus haut avec les travaux de Fiorilli et Martin que la dissipation du biais dans une course de nombres premiers à deux participants modulo q était contrôlée par la

quantité $\frac{\rho(q)}{\sqrt{2\pi V(q;a,b)}}$, qui se trouve être de l'ordre $\frac{1}{q^{1/2+o(1)}}$ quand $q \to +\infty$. Dans [Lam13], Lamzouri montre que l'atténuation du biais est beaucoup plus lente dans une course à $D \geq 3$ participants : on a

$$\max_{a_1,\dots,a_D \in (\mathbb{Z}/q\mathbb{Z})^\times} \left|\delta(\mathcal{P}_{q;a_1,\dots,a_D}) - \frac{1}{D!}\right| \asymp_D \frac{1}{\log q}.$$

Lorsque le nombre de participants D tend vers l'infini avec q, Lamzouri parvient à établir dans [Lam12] que la quantité

$$\max_{a_1,\dots,a_D \in (\mathbb{Z}/q\mathbb{Z})^\times} \left|\delta(\mathcal{P}_{q;a_1,\dots,a_D}) - \frac{1}{D!}\right|$$

tend vers 0 tant que $D = o(\sqrt{\log q})$. Des travaux ultérieurs du même auteur, avec Harper ([HL18]) puis Ford-Harper ([FHL19]), améliorent la condition sur D, et montrent que la transition entre la dissipation uniforme du biais et l'existence de courses fortement biaisées se produit en présence de $(\log q)^{1+o(1)}$ participants.

À la suite de [Dev19], Devin cherche à affaiblir les hypothèses d'indépendance linéaire garantissant l'existence de la densité logarithmique associée à une course de nombres premiers à un nombre arbitraire de participants. Dans [Dev20], celle-ci dégage une hypothèse (déjà présente dans [Dev19, Theorem 2.2], mais qui ne concernait que des courses à deux participants) de séparation des zéros de la forme suivante :

$$\mathrm{Vect}_{\mathbb{Q}}(\bigcup_{\chi \neq \chi_0} \Gamma(\chi)) = \mathrm{Vect}_{\mathbb{Q}}(\gamma_1,\dots,\gamma_n) \oplus \mathrm{Vect}_{\mathbb{Q}}(\bigcup_{\chi \neq \chi_0} \Gamma(\chi) \setminus \{\gamma_1,\dots,\gamma_n\})$$

pour certains zéros $\gamma_1,\dots,\gamma_n$ tels que chaque γ_i n'appartienne qu'à un seul $\Gamma(\chi)$ et pour chaque $\chi \neq \chi_0$, au moins l'un des γ_i soit un zéro de $L(s,\chi)$ (cette dernière condition permettant de « séparer les participants » de la course). Notons que la condition ci-dessus est plus faible que de supposer que les zéros $\gamma_1,\dots,\gamma_n$ sont auto-suffisants : il peut y avoir des relations de dépendance linéaire entre eux. Cette hypothèse permet à Devin d'isoler un facteur de la fonction caractéristique $\hat{\mu}_{q;a_1,\dots,a_D}$ (qui ne se réduit pas à un facteur J_0 en l'absence d'indépendance linéaire parmi les γ_i) dont la décroissance à l'infini est établie à l'aide d'estimations d'intégrales oscillantes

1.3 Courses de polynômes irréductibles

Jusqu'ici on a parlé principalement du cadre usuel des courses entre diverses familles de nombres premiers (hormis une mention des angles des premiers de Gauss et les travaux de Meng à propos d'entiers ayant k facteurs premiers), mais la méthode de Rubinstein et Sarnak peut s'appliquer en fait à l'étude de bien d'autres phénomènes oscillatoires en théorie analytique des nombres. Dans cette section, on présente l'exemple fondateur, dû à Cha dans [Cha08], des courses entre polynômes irréductibles sur $\mathbb{F}_q[X]$. Dans toute cette section, q est une puissance de nombre premier fixée, et $\mathbb{F}_q$ désigne un corps à q éléments.

1.3.1 Arithmétique dans $\mathbb{F}_q[T]$

Il est bien connu que les anneaux $\mathbb{Z}$ et $\mathbb{F}_q[T]$ partagent de nombreuses propriétés arithmétiques communes. Ainsi, ce sont tous les deux des anneaux euclidiens, et aussi des anneaux de

Dedekind, leurs quotients non triviaux sont donc tous finis. La théorie si utile des caractères de Dirichlet dans $\mathbb{Z}$ se transpose donc sans mal à $\mathbb{F}_q[T]$. On renvoie le lecteur aux quatre premiers chapitres de [Ros02] pour les démonstrations de la plupart des résultats élémentaires utilisés ici.

Dans l'anneau $\mathbb{F}_q[T]$, le rôle des nombres premiers est naturellement joué par les polynômes irréductibles, puisque ce sont eux qui interviennent dans la factorisation des éléments de notre anneau. Tout comme dans $\mathbb{Z}$ où l'on choisit canoniquement les nombres premiers comme étant positifs, on choisit ici les polynômes irréductibles unitaires (cela revient à faire un choix de représentants modulo les inversibles de l'anneau pour avoir unicité dans la factorisation en produit d'éléments irréductibles). Dans cette section, la lettre P désignera uniquement un polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.

Si $M \in \mathbb{F}_q[T]$, on peut s'intéresser à la répartition des nombres premiers dans les progressions arithmétiques $A + M\mathbb{F}_q[T]$. Le fait que ces progressions soient en nombre fini et recouvrent $\mathbb{F}_q[T]$ est une manifestation des caractères euclidiens et de Dedekind de $\mathbb{F}_q[T]$, tout comme dans $\mathbb{Z}$. Cependant, dans $\mathbb{Z}$ on cherche à compter le nombre de nombres premiers inférieurs à x dans une progression arithmétique donnée, mais comment transposer le terme « inférieurs à x » dans le contexte des polynômes irréductibles ?

Là encore, c'est l'analogie avec $\mathbb{Z}$ qui nous guide : la taille d'un entier n (ou de l'idéal premier $n\mathbb{Z}$) est le cardinal $\#\mathbb{Z}/n\mathbb{Z}$. Par analogie, on pose $|f| := \#\mathbb{F}_q[T]/f\mathbb{F}_q[T] = q^{\deg f}$ pour tout $f \in \mathbb{F}_q[T] \setminus \{0\}$. Notons que la taille (ou norme) d'un tel polynôme est toujours une puissance de q, il sera donc naturel de remplacer la borne x par une borne de la forme q^n avec n entier.

Définition 1.27. *Soit $M \in \mathbb{F}_q[T]$. Pour tout $A \in \mathbb{F}_q[T]$ premier avec M, on pose pour tout $N \geq 1$,*

$$\pi(N; M, A) := \#\{P \mid P \equiv A \bmod M, \deg P = N\}.$$

Remarque 1.28. On préfère introduire une fonction de comptage de polynômes irréductibles de degré exactement N et pas ceux de degrés inférieurs à N car il est en général plus naturel d'étudier les premiers plutôt que les seconds. Par exemple, il est bien connu que les polynômes irréductibles de degré divisant N sur $\mathbb{F}_q$ sont exactement les facteurs irréductibles du polynôme $X^{q^n} - X$, avec multiplicité 1 (voir [IR90, Chapter 7, Theorem 2]), ce qui permet d'obtenir simplement une formule explicite pour $\pi_q(N) := \#\{P \mid \deg P = N\}$ par inversion de Möbius. Dans tous les cas, une estimation sur le nombre de polynômes irréductibles de degrés inférieurs à N s'obtient aisément en sommant sur les entiers inférieurs à N.

En notant $\Phi(M) := \#\left(\mathbb{F}_q[T]/M\mathbb{F}_q[T]\right)^\times$, on peut maintenant énoncer le théorème des polynômes premiers en progressions arithmétiques.

Théorème 1.29. *Soient $M, A \in \mathbb{F}_q[T]$ premiers entre eux. Alors*

$$\pi(N; M, A) \underset{N \to +\infty}{\sim} \frac{1}{\Phi(M)} \frac{q^N}{N}.$$

Remarques 1.30.

i) Si l'on note $X = q^N$, on en déduit que le nombre de polynômes irréductibles congrus à A modulo M de normes inférieures à X est équivalent quand X tend vers l'infini à $\frac{1}{\Phi(M)}\frac{X}{\log_q X}$, où $\log_q$ désigne la logarithme en base q. L'analogie avec le théorème des nombres premiers en progressions arithmétiques est totale.

ii) En sommant on obtient

$$\sum_{n=1}^{N} \pi(n; M, A) = \#\{P \mid P \equiv A \bmod M, \deg P \leq N\} \underset{N\to+\infty}{\sim} \frac{1}{\Phi(M)}\frac{q^N}{N}.$$

Dans ce contexte, il y a donc également équirépartition uniforme des P mod M dans les $\Phi(M)$ classes inversibles modulo M. On peut donc comme précédemment chercher à comparer plus finement les fonctions de comptage des polynômes irréductibles dans les progressions arithmétiques modulo M, c'est-à-dire s'intéresser à la fréquence à laquelle des inégalités du type

$$\sum_{n=1}^{N} \pi(n; M, A) > \sum_{n=1}^{N} \pi(n; M, B)$$

se produisent.

Comme dans le cas des nombres premiers, on démontre le théorème ci-dessus à l'aide de fonctions L de Dirichlet associées aux caractères du groupe $(\mathbb{F}_q[T]/M\mathbb{F}_q[T])^\times$, relevés en des fonctions complètement multiplicatives sur $\mathbb{F}_q[T]$, que l'on nomme naturellement caractères de Dirichlet modulo M. On notera X_M l'ensemble des caractères de Dirichlet modulo M.

Définition 1.31. *Soit $M \in \mathbb{F}_q[T]$ et χ un caractère de Dirichlet modulo M. La **fonction L de Dirichlet** associée à χ est*

$$s \mapsto L(s, \chi) := \sum_{f \in \mathbb{F}_q[T] \text{ unitaire}} \frac{\chi(f)}{|f|^s}.$$

Il est facile de voir que la série ci-dessus converge lorsque $\mathfrak{Re}(s) > 1$, et que l'on dispose alors d'une factorisation en produit eulérien indexé par les polynômes irréductibles unitaires. Le fait important concernant ces fonctions L de Dirichlet, qui fait que la situation est plus simple à traiter que dans le cas des nombres premiers, est que celles-ci s'expriment comme des fractions rationnelles (et même des polynômes quand χ n'est pas trivial) en la « variable » $u := q^{-s}$.

Théorème 1.32. *Soit $M \in \mathbb{F}_q[T]$. La fonction $L(s, \chi)$ est une fraction rationnelle en $u = q^{-s}$:*

$$\mathcal{L}(u, \chi_0) := L(s, \chi_0) = \frac{\prod_{j=1}^{M(\chi_0)}(1 - \gamma_j(\chi_0)u)}{(1-u)(1-qu)}$$

et pour tout caractère de Dirichlet $\chi \neq \chi_0$ modulo M, la fonction $L(s, \chi)$ est un polynôme en u :

$$\mathcal{L}(u, \chi) := L(s, \chi) = \prod_{j=1}^{M(\chi)} (1 - \gamma_j(\chi)u).$$

Les $\gamma_j(\chi)$ sont appelés les zéros inverses de $L(s, \chi)$.

Remarque 1.33. On a en fait $L(s,\chi_0) = \prod_{P|M}\left(1-\frac{1}{|P|^s}\right)\zeta_{\mathbb{F}_q(T)}(s)$ où $\zeta_{\mathbb{F}_q(T)} = \sum_{f \text{ unitaire}} \frac{1}{|f|^s} = \frac{1}{1-q^{1-s}} = \frac{1}{1-qu}$ est la fonction ζ du corps de fonctions $\mathbb{F}_q(T)$.

Il est connu que ces fonctions satisfont l'hypothèse de Riemann, comme l'a démontré André Weil (voir par exemple [Ros02, Appendix] pour une preuve moderne due à Bombieri), au sens où la partie réelle de leurs zéros est toujours 1/2 (ou 0). La présence de zéros « triviaux » de partie réelle 0 est simplement due à la non primitivité de certains caractères modulo M. Pour la variable $u = q^{-s}$, cela se traduit par le fait que les zéros inverses des $\mathcal{L}(u,\chi)$ ont pour module $\sqrt{q}$ ou 1. Les zéros triviaux ne jouant pas de rôle dans la suite, on notera donc dans la suite $\gamma_\chi = \sqrt{q}e^{i\theta_\chi}$ les zéros inverses de module $\sqrt{q}$ de $\mathcal{L}(u,\chi)$, et une indexation sur γ_χ portera sur l'ensemble des zéros inverses non triviaux de $\mathcal{L}(u,\chi)$, comptés avec multiplicités.

1.3.2 Généralisation des travaux de Rubinstein et Sarnak par Cha

Nous pouvons maintenant détailler la transposition de la méthode de Rubinstein et Sarnak par Cha dans [Cha08] dans le contexte des polynômes irréductibles dans $\mathbb{F}_q[T]$.

Définition 1.34. *Soient $M, A_1, \dots, A_D \in \mathbb{F}_q[T]$ avec $A_1, \dots, A_D$ premiers avec M. On définit*

$$\mathcal{P}_{M;A_1,\dots,A_D} := \left\{ X \in \mathbb{N} \mid \sum_{n=1}^{N} \pi(n;M,A_1) > \cdots > \sum_{n=1}^{N} \pi(n;M,A_D) \right\}.$$

La question est désormais d'étudier la densité *naturelle*

$$\delta(\mathcal{P}_{M;A_1,\dots,A_D}) := \lim_{X\to+\infty} \frac{1}{X} \#\mathcal{P}_{M;A_1,\dots,A_D} \cap [0,X],$$

en premier lieu son existence.

Remarques 1.35.

i) Les densités logarithmiques précédemment étudiées faisaient intervenir des intégrales. Ici, on travaille avec la densité naturelle d'un ensemble discret, on pressent donc que les intégrales apparaissant dans la méthode de Rubinstein et Sarnak doivent être remplacées par des sommes.

ii) On peut remarquer que l'on cherche directement une densité naturelle au lieu d'une densité logarithmique à cause du choix de la définition de nos fonctions de comptage. Si l'on avait travaillé avec $\#\{P \mid |P| \le X, P \equiv A \bmod M\} = \pi(\lfloor \log_q X \rfloor; M, A)$, il aurait fallu considérer une densité « q-logarithmique ».

iii) Le lecteur attentif peut naturellement se demander pourquoi ne pas considérer l'ensemble $P_{M;A_1,\dots,A_D} := \left\{ x \ge 2 \mid \sum_{n\le x} \pi(n;M,A_1) > \cdots > \sum_{n\le x} \pi(n;M,A_D) \right\}$ et la densité $\lim_{Y\to+\infty} \frac{1}{Y}\int_0^Y \mathbf{1}_{P_{M;A_1,\dots,A_D}}(t)\,\mathrm{d}t$ pour utiliser les mêmes techniques qu'avant. La raison est la suivante : on verra plus bas une formule explicite pour la quantité

$$\frac{X}{q^{X/2}}\left(\sum_{N=1}^{X} \Phi(M)\pi(N;M,A) - \pi_q(N)\right),$$

valable pour tout X **entier**, et on ne peut certainement pas extrapoler cette formule explicite à la quantité

$$\frac{x}{q^{x/2}}\left(\sum_{N\leq x}\Phi(M)\pi(N;M,A)-\pi_q(N)\right)$$

pour x réel. Notre seule porte d'entrée ne nous autorise donc qu'à manipuler des variables entières. On verra plus tard que cela crée de nouvelles difficultés liées à d'éventuelles relations de dépendance linéaire avec π.

Comme précédemment, on a besoin d'extraire la partie oscillante des $\sum_{n=1}^{N}\pi(n;M,A_i)$, au-delà du terme principal $\frac{1}{\Phi(M)}\frac{q^N}{N}$ commun à toutes les progressions modulo M.

Définition 1.36. *Pour tout $M, A\in\mathbb{F}_q[T]$ premiers entre eux et tout entier $X\geq 2$ on pose*

$$E(X,M,A):=\frac{X}{q^{X/2}}\left(\sum_{n=1}^{X}\Phi(M)\pi(n;M,A)-\pi_q(n)\right),$$

où

$$\pi_q(n):=\#\{P\mid \deg P=n\}.$$

Si $A_1,\dots,A_D\in\mathbb{F}_q[T]$ sont deux à deux distincts et premiers avec M, on pose pour $X\geq 2$ entier,

$$E_{M;A_1,\dots,A_D}(X)=(E(X;M,A_1),\dots,E(X;M,A_D)).$$

Ici encore, la première étape est d'établir l'existence d'une distribution limite.

Définition 1.37. *Soit $E:\mathbb{Z}\longrightarrow\mathbb{R}^D$. On dit que E admet une **distribution limite** lorsqu'il existe une mesure borélienne μ sur $\mathbb{R}^D$ telle que pour toute fonction continue bornée f sur $\mathbb{R}^D$ on a*

$$\lim_{X\to+\infty}\frac{1}{X}\sum_{n=1}^{X}E(f(n))=\int_{\mathbb{R}^D}f(t)\,\mathrm{d}t.$$

Cha démontre alors la formule explicite suivante.

Théorème 1.38 (Cha, [Cha08])**.** *Pour tout $M, A\in\mathbb{F}_q[T]$ premiers entre eux et tout entier $X\geq 2$ on a*

$$E(X,M,A)=-c(M,A)\mathcal{B}_q(X)-\sum_{\chi\neq\chi_0}\overline{\chi(A)}\sum_{\gamma_\chi}\frac{\gamma_\chi}{\gamma_\chi-1}e^{i\theta_\chi X}+o(1)$$

quand $X\to+\infty$, où $c(M,A):=-1+\#\{B\in\mathbb{F}_q[T]/M\mathbb{F}_q[T]\mid B^2\equiv A\ mod\ M\}$ et

$$\mathcal{B}_q(X):=\begin{cases}\frac{q}{q-1}\ \textit{si } q \textit{ est pair}\\ \frac{\sqrt{q}}{q-1}\ \textit{si } q \textit{ est impair.}\end{cases}$$

Remarques 1.39.

i) On retrouve un terme (presque) constant qui fait intervenir le nombre de racines carrées de A modulo M. C'est à nouveau ce facteur qui est à l'origine du biais de Tchebychev dans ce contexte.

ii) L'apparition du facteur $\mathcal{B}_q(X)$ et des coefficients $\frac{\gamma_\chi}{\gamma_\chi - 1}$ est dû au choix de Cha de considérer les courses entre les fonctions de comptage des polynômes irréductibles de degrés inférieurs à X et non pas de degrés égaux à X. Dans ce dernier cas, on peut établir la formule plus simple (qui permet de montrer la formule ci-dessus par sommation)

$$\frac{X}{q^{X/2}}(\Phi(M)\pi(X;M,A) - \pi_q(X)) = -c(M,A)\frac{1-(-1)^X}{2} - \sum_{\chi \neq \chi_0} \overline{\chi(A)} \sum_{\gamma_\chi} e^{i\theta_\chi X} + o(1)$$

quand $X \to +\infty$. Dans tous les cas, la présence d'un terme dépendant de la parité de X provient du caractère discret des sommes considérées.

Pour relier cette formule explicite à l'existence d'une distribution limite dont la définition même fait intervenir des sommes, on a besoin de la version suivante du théorème de Kronecker-Weyl, que l'on appellera la version discrète de ce théorème.

Théorème 1.40 (Kronecker-Weyl discret)**.** *Soit $\theta_1, \dots, \theta_r$ des nombres réels. Alors le sous-groupe $\Gamma = \{\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) \mid n \in \mathbb{Z}\}$ de $\mathbb{T}^r$ est équiréparti dans son adhérence $\overline{\Gamma}$. Autrement dit, pour toute fonction continue $f : \mathbb{T}^r \longrightarrow \mathbb{C}$, on a*

$$\lim_{X \to +\infty} \frac{1}{X} \sum_{n \leq X} f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) = \int_{\overline{\Gamma}} f(z)\, \mathrm{d}\mu(z)$$

où μ est la mesure de Haar normalisée de $\overline{\Gamma}$. De plus, si $\pi, \theta_1, \dots, \theta_r$ sont linéairement indépendant sur $\mathbb{Q}$ alors $\overline{\Gamma} = \mathbb{T}^r$.

Remarque 1.41. On voit deux grandes différences avec la version « continue » du théorème de Kronecker-Weyl. Tout d'abord, on ne prétend pas que $\overline{\Gamma}$ est un sous-tore de $\mathbb{T}^r$. En effet, ce dernier peut admettre plusieurs composantes connexes en fonction des relations de dépendance linéaire sur $\mathbb{Q}$ entre $\pi, \theta_1, \dots, \theta_r$ (voir Theorem 1.52 plus bas). De plus, on voit apparaître dans la dernière affirmation une condition d'indépendance linéaire avec π, qui s'explique par le fait que si a est un rationnel alors $e^{ia\pi n}$ prend des valeurs discrètes dans $\mathbb{T}$ pour $n \in \mathbb{Z}$. On y reviendra bien plus en détails dans la section 1.4.

À l'aide de ce théorème et de la formule explicite précédente, Cha établit l'existence d'une distribution limite $\mu_{M;A_1,\dots,A_D}$ pour la quantité $E_{M;A_1,\dots,A_D}$ lorsque $A_1, \dots, A_D \in \mathbb{F}_q[T]$ sont deux à deux distincts et premiers avec M. On notera que le terme $\mathcal{B}_q(X)$ de la formule explicite peut se réécrire $\frac{q+\sqrt{q}}{2(q-1)} + e^{i\pi X}\frac{q-\sqrt{q}}{2(q-1)}$, de sorte que, hormis le reste $o(1)$, la formule explicite ne fait intervenir que des termes de la forme ae^{ibX} avec $a, b \in \mathbb{R}$, ce qui permet d'appliquer la version discrète du théorème de Kronecker-Weyl.

L'étape suivante consiste, comme dans les travaux de Rubinstein et Sarnak, à établir l'existence de la densité naturelle $\delta(\mathcal{P}_{M;A_1,\dots,A_D})$ en passant des fonctions continues bornées sur $\mathbb{R}^D$ à l'indicatrice de $\{(x_1, \dots, x_D) \in \mathbb{R}^D \mid x_1 > \dots > x_D\}$. À nouveau c'est une certaine

régularité de la distribution limite $\mu_{M;A_1,\dots,A_D}$ qui permet cela, et Cha introduit alors une hypothèse d'indépendance linéaire similaire à GSH pour les fonctions L de Dirichlet modulo M, que l'on notera GSH_M.

Conjecture 1.42 (GSH_M)**.** *Le multi-ensemble*

$$\left\{\theta \in [0,\pi] \mid \exists \chi \in X_M, \mathcal{L}\left(\left(\sqrt{q}e^{i\theta}\right)^{-1}, \chi\right) = 0\right\} \cup \{\pi\}$$

(où l'on rappelle que X_M désigne l'ensemble des caractères de Dirichlet modulo M) est linéairement indépendant sur $\mathbb{Q}$.

Remarques 1.43.

i) La condition $0 \leq \theta \leq \pi$ est analogue à la condition $\gamma \geq 0$ dans l'hypothèse GSH : tout comme dans le cas des fonctions L de Dirichlet modulo un entier, les zéros viennent par paires. Si $\alpha = \sqrt{q}e^{i\theta}$ avec $0 \leq \theta \leq \pi$ est un zéro inverse de $\mathcal{L}(u,\chi)$ alors $q/\alpha = \sqrt{q}e^{-i\theta}$ est un zéro inverse de $\mathcal{L}(u,\overline{\chi})$ d'après l'équation fonctionnelle vérifiée par les fonctions L de Dirichlet modulo M, avec $-\pi \leq -\theta \leq 0$.

ii) Le caractère discret de la situation impose de faire l'hypothèse d'indépendance linéaire avec π. Disons tout de suite que, contrairement à ce qui est conjecturé pour l'hypothèse GSH, l'hypothèse GSH_M n'est pas toujours vérifiée. L'auteur de ces lignes ignore cependant si l'on connaît des polynômes M tels que le multi-ensemble $\{\theta \in]0,\pi[\mid \exists \chi \in X_M, \mathcal{L}(q^{-1/2}e^{-i\theta},\chi) = 0\}$ (noter les crochets ouverts) ne soit pas linéairement indépendant sur $\mathbb{Q}$.

Ainsi, bien que la situation semble plus facile dans ce cas en raison de la présence d'un nombre fini de zéros, son caractère discret la complique techniquement.

Une fois ce travail préliminaire fait, les démonstrations des résultats suivants sont similaires à celles de Rubinstein et Sarnak.

Théorème 1.44 (Cha, [Cha08])**.** *Soit $M \in \mathbb{F}_q[T]$ et $A_1,\dots,A_D \in \mathbb{F}_q[T]$ deux à deux distincts et premiers avec M. Alors $E_{M;A_1,\dots,A_D}$ admet une distribution limite $\mu_{M;A_1,\dots,A_D}$. Si GSH_M est vérifiée alors*

$$\hat{\mu}_{M;A_1,\dots,A_D} : \xi \mapsto \mathcal{B}_{M;A_1,\dots,A_D}(\xi) \times \prod_{\chi \neq \chi_0} \prod_{0<\gamma_\chi<\pi} J_0\left(2\left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right| \left|\sum_{j=1}^{D} \chi(A_j)\xi_j\right|\right)$$

où

$$\mathcal{B}_{M;A_1,\dots,A_D}(\xi) := \frac{1}{2}\left(\exp\left(-i\sum_{j=1}^{D}\frac{qc(M,A_j)}{q-1}\xi_j\right) + \exp\left(-i\sum_{j=1}^{D}\frac{\sqrt{q}c(M,A_j)}{q-1}\xi_j\right)\right)$$

et $\delta(\mathcal{P}_{M;A_1,\dots,A_D})$ existe. Si $(M_n)_{n\in\mathbb{N}}$ est une suite d'éléments de $\mathbb{F}_q[T]$ telle que GSH_{M_n} soit vraie pour tout $n \in \mathbb{N}$ et $\deg M_n \underset{n\to+\infty}{\longrightarrow} +\infty$, alors on a

$$\max_{A_1,\dots,A_D \in (\mathbb{F}_q[T]/M_n\mathbb{F}_q[T])^\times} \left|\delta(\mathcal{P}_{M_n;A_1,\dots,A_D}) - \frac{1}{D!}\right| \underset{n\to+\infty}{\longrightarrow} 0.$$

Cha obtient également des résultats similaires à ceux de Rubinstein et Sarnak pour la course entre les carrés et les non carrés modulo M dans le cas où M est irréductible. Celui-ci montre, en supposant GSH_M (ou plus précisément en faisant l'hypothèse d'indépendance linéaire usuelle pour les zéros inverses de la fonction L de Dirichlet associée au symbole de Legendre $\left(\frac{\cdot}{M}\right)$ modulo M), que le biais de Tchebychev est toujours présent au sens où $\delta(\mathcal{P}_{M;N,R}) > \frac{1}{2}$, avec

$$\mathcal{P}_{M;N,R} := \{X \in \mathbb{N} \mid \sum_{n=1}^{X} \pi(n;M,N) > \sum_{n=1}^{X} \pi(n;M,R)\},$$

où

$$\pi(n;M,R) := \#\{P \mid \deg P = n, P \equiv \square \bmod M\}$$

et

$$\pi(n;M,N) := \pi_q(n) - \pi(n;M,R).$$

Cependant, un fait nouveau apparaît dans ce contexte : si $\deg M = 2$ alors $L\left(s, \left(\frac{\cdot}{M}\right)\right)$ n'admet que des zéros triviaux. On a alors la formule explicite

$$\frac{X}{q^{X/2}} \left(\sum_{n=1}^{X} \pi(n;M,R) - \pi(n;M,N) \right) = -\mathcal{B}_q(X) + o(1),$$

de sorte que $\delta(\mathcal{P}_{M;N,R}) = 1$ puisque

$$\sum_{n=1}^{X} \pi(n;M,R) < \sum_{n=1}^{X} \pi(n;M,N)$$

à partir d'un certain rang X.

1.3.3 Violation de l'hypothèse GSH_M

Comme annoncé précédemment, il se peut cependant que l'hypothèse GSH_M ne soit pas vraie. Ainsi Cha donne dans [Cha08] les exemples suivants :

i) On prend $q = 3, M = T^3 + 2T + 1$. Alors

$$\mathcal{L}\left(u, \left(\frac{\cdot}{M}\right)\right) = 3u^2 - 3u + 1 = (1 - \gamma u)(1 - \overline{\gamma} u)$$

où

$$\gamma = \sqrt{3} e^{i\frac{\pi}{6}}.$$

Cha montre alors que $\delta(\mathcal{P}_{M;N,R}) = \frac{7}{12} > \frac{1}{2}$. Même si GSH_M n'est pas vérifiée, le biais est en faveur des non carrés modulo M.

ii) On prend $q = 5, M = T^4 + 4T^3 + 4T^2 + 4T + 1$. Alors

$$\mathcal{L}\left(u, \left(\frac{\cdot}{M}\right)\right) = -5u^3 + 5u^2 - u + 1 = (1 - u)(1 - \gamma u)(1 - \overline{\gamma} u)$$

où

$$\gamma = \sqrt{5}e^{i\frac{\pi}{2}}.$$

Cha montre alors que $\delta(\mathcal{P}_{M;N,R}) = \frac{1}{2}$. À cause du fait que GSH_M n'est pas vérifiée, il n'y a pas de biais entre les carrés et les non carrés modulo M.

iii) On prend $q = 5, M = T^5 + 3T^4 + 4T^3 + 2T + 2$. Alors

$$\mathcal{L}\left(u, \left(\frac{\cdot}{M}\right)\right) = 25u^4 - 25u^3 + 15u^2 - 5u + 1 = (1 - \gamma_1 u)(1 - \overline{\gamma_1}u)(1 - \gamma_2 u)(1 - \overline{\gamma_2}u)$$

où

$$\gamma_1 = \sqrt{5}e^{i\frac{2\pi}{5}}$$

et

$$\gamma_2 = \sqrt{5}e^{i\frac{4\pi}{5}}.$$

Cha montre alors que $\delta(\mathcal{P}_{M;N,R}) = \frac{2}{5} < \frac{1}{2}$. À cause du fait que GSH_M n'est pas vérifiée, le biais est en faveur des carrés modulo M.

Les exemples ci-dessus illustrent bien le fait que des violations de l'hypothèse GSH_M peuvent empêcher le biais de Tchebychev de se manifester. Dans ces exemples, l'hypothèse GSH_M était fausse car les zéros inverses étaient (au module près) des racines de l'unité, autrement dit parce que l'indépendance linéaire entre leurs arguments et π n'était pas respectée. Il se trouve que GSH_M peut même plus fortement être fausse en raison de zéros inverses égaux à $\sqrt{q}$, c'est-à-dire dont l'argument vaut 0. Ainsi, Li a montré dans [Li18] qu'en caractéristique impaire, il existe toujours une infinité de caractères de Dirichlet quadratiques χ vérifiant $L(1/2, \chi) = 0$. Ces caractères donnent un autre type de violation de l'hypothèse GSH_M.

Remarque 1.45. Les caractères obtenus par Li ont, quand on les ordonne selon le degré de leur conducteur, une densité nulle. Il semble raisonnable de conjecturer que l'ensemble

$$\{\chi \mid \exists M \in \mathbb{F}_q[T] \text{ unitaire et sans facteur carré}, \chi \in X_M, L(1/2, \chi) = 0\}$$

a une densité nulle : la présence d'un zéro en 1/2 serait un phénomène marginal (voir également ci-dessous une partie des résultats de Kowalski sur cette question).

Dans [DM20], Devin et Meng s'intéressent à la course entre les polynômes unitaires ayant k facteurs irréductibles qui sont des carrés modulo M face à ceux qui ne sont pas des carrés modulo M. Si GSH_M est vraie (il suffit même de supposer l'indépendance linéaire pour les zéros des fonctions L associées aux caractères quadratiques modulo M), alors le biais de Tchebychev est toujours en faveur des carrés modulo M, à moins que k soit impair et que l'on compte les facteurs irréductibles avec multiplicités auquel cas celui-ci est dans l'autre sens. De plus, Devin et Meng utilisent des polynômes M initialement introduits par Cha et Li ne vérifiant pas GSH_M afin d'obtenir des courses à biais complet, c'est-à-dire dont la densité associée vaut 1, sans biais, (la densité associée vaut 1/2) ou dans la mauvaise direction comme dans l'exemple iii) ci-dessus.

Bien que l'hypothèse GSH_M soit parfois fausse, on dispose cependant de résultats assurant que celle-ci est satisfaite génériquement en un certain sens pour des caractères quadratiques

(ceux qui jouent un rôle dans les courses entre les carrés et les non carrés). Ainsi Kowalski montre dans [Kow08] que, pour tout nombre nombre premier p impair et avec $q = p^n$, pour tout $f \in \mathbb{F}_q[T]$ sans facteur carré de degré pair et dont le discriminant n'est pas divisible par p, la proportion de t dans l'ouvert affine $U_f := \mathbb{F}_q \setminus f^{-1}(\{0\})$ tels que les zéros inverses de la fonction zêta de la courbe $C_t : y^2 = f(x)(x-t)$ satisfont une relation multiplicative non triviale est négligeable quand n tend vers l'infini. Il est facile de voir que cette fonction zêta admet une factorisation sous la forme $\frac{1}{1-q^{1-s}} P(s) L\left(s, \left(\frac{\cdot}{f(x)(x-t)}\right)\right)$, où P est un produit eulérien fini n'admettant que des zéros triviaux (voir les propriétés des fonctions L d'Artin dans le Chapitre 3). En conséquence, l'indépendance linéaire sur $\mathbb{Q}$ entre les arguments des zéros inverses de la fonction L de Dirichlet du caractère de Jacobi modulo M (et π) est vraie génériquement dans l'ensemble des polynômes unitaires $M \in \mathbb{F}_q[T]$ admettant un zéro simple.

1.4 Théorèmes de Kronecker-Weyl explicites et applications aux courses de nombres premiers

Cette section contient l'article original Explicit Kronecker-Weyl theorems and applications to prime number races [Bai20]. Le Theorem 1.82 et la section 1.4.2.2 traitent de courses entre idéaux premiers dans les corps de nombres et entre diviseurs premiers dans les corps de fonctions respectivement, notions qui seront reprises plus en détails dans les Chapitre 2 et 3.

Résumé détaillé : Dans cet article, on démontre des versions explicites des théorèmes de Kronecker-Weyl, dans leurs versions discrète et continue comme énoncées plus haut, sans aucune hypothèse d'indépendance linéaire. Notre méthode nous permet de décrire explicitement l'ensemble dans lequel le sous-groupe à un paramètre Γ_θ étudié est équiréparti, cette description faisant intervenir les relations de dépendance linéaire sur $\mathbb{Q}$ des réels $\theta_1, \dots, \theta_r$ définissant le groupe Γ_θ, ainsi que la dépendance linéaire de ces nombres avec π dans le cas discret. Cette description explicite nous permet de décrire et d'étudier des variables aléatoires dont les lois sont exactement les distributions limites associées à certains types de fonctions qui interviennent dans les formules explicites utilisées dans des problèmes de type courses de nombres premiers. On donne alors des conditions suffisantes garantissant l'existence de densités associées à de telles fonctions. Ces résultats peuvent être appliqués à l'étude de courses dans les corps de nombres (cas englobant la situation étudiée par Rubinstein et Sarnak pour les nombres premiers en progressions arithmétiques) et dans les corps de fonctions sur les corps finis (cas englobant la situation étudiée par Cha pour les polynômes irréductibles sur $\mathbb{F}_q$ en progressions arithmétiques). Dans ce dernier contexte, on obtient même des conditions suffisantes pour la stricte positivité de la densité en question, indépendamment de toute hypothèse d'indépendance linéaire. Les méthodes employées sont élémentaires, là où d'autres travaux font appel à des outils sophistiqués d'analyse harmonique, que ce soit pour démontrer le théorème de Kronecker-Weyl (bien qu'il en existe des preuves élémentaires, par exemple [MN17, Lemma B.3]), ou pour établir que les distributions limites étudiées n'attribuent pas de masses aux réunions d'hyperplans définissant les « cas d'égalité » dans les courses considérées.

Abstract : We prove explicit versions of the Kronecker-Weyl theorems, both the discrete

and the continuous ones, without any linear independence hypothesis. As an application, we propose an alternative approach to problems concerning asymptotic densities in prime number races, over number fields and over function fields in one variable over finite fields, in the language of random variables. Our approach allows us to prove new results on the existence and positivity of some of those densities, which, in the case of races over finite fields, do not require any linear independence hypothesis.

Introduction

The Kronecker-Weyl theorem is an important result of harmonic analysis, with links with ergodic theory, and which has been used to study many arithmetical problems of statistical nature. It is both a multidimensional generalization of Weyl's famous result on the equidistribution of the fractional parts of $n\alpha$ ($n \in \mathbb{N}$), when α is an irrational number, and a generalization of Kronecker's density result on the torus. More specifically, let $\theta_1, \dots, \theta_n$ be real numbers, then the one-parameter subgroup

$$\Gamma := \left\{ \left(e^{i\theta_1 x}, \dots, e^{i\theta_n x} \right) \mid x \in \mathbb{R} \right\}$$

is equidistributed in a subtorus inside the n-dimensional torus

$$\mathbb{T}^n := \{(z_1, \dots, z_n) \in \mathbb{C}^n \mid \forall i \in \{1, \dots, n\}, |z_i| = 1\}$$

with respect to its Haar measure $\mathrm{d}\mu$. In other words, the topological closure $\overline{\Gamma}$ of Γ in $\mathbb{T}^n$ is a closed connected subgroup of $\mathbb{T}^n$ with Haar measure $\mathrm{d}\mu$ and for every continuous function $f : \mathbb{T}^n \to \mathbb{C}$, one has

$$\frac{1}{X} \int_0^X f\left(e^{i\theta_1 x}, \dots, e^{i\theta_n x} \right) \mathrm{d}x \underset{X \to +\infty}{\longrightarrow} \int_{\overline{\Gamma}} f \, \mathrm{d}\mu.$$

Most relevant to the present work is the additional information that $\overline{\Gamma}$ is a m-dimensional torus, where m is the dimension of the $\mathbb{Q}$-vector space spanned by $\theta_1, \dots, \theta_n$. In particular, if $\theta_1, \dots, \theta_n$ are $\mathbb{Q}$-linearly independent, then $\overline{\Gamma} = \mathbb{T}^n$, so we obtain Kronecker's density result in a strong form (in the sense that equidistribution holds), and when $n = 1$, this is exactly Weyl's equidistribution result.

There exists a discrete version of the Kronecker-Weyl Theorem, in which we consider the discretely-parametrized subgroup

$$\Gamma := \left\{ \left(e^{i\theta_1 X}, \dots, e^{i\theta_n X} \right) \mid X \in \mathbb{Z} \right\}.$$

In this case, integrals are replaced by sums and we require the real numbers $\theta_1, \dots, \theta_n$ to be $\mathbb{Q}$-linearly independent with π. The reason for this is clear, since $e^{iq\pi X}$ assumes discrete values in $\mathbb{T}$ when X ranges over the integers, and q is a rational number. Usually, both the continuous and the discrete versions of the Kronecker-Weyl Theorem are proved using abstract harmonic analysis (see [QQ13, Theorem 2.2.5] or [Dev19, Theorem 4.2] for instance). In this paper, we give an elementary proof of a general version of Kronecker-Weyl's result, both in the discrete and the continuous case, in which we explicitly construct the set in which Γ equidistributes. We insist on the fact that no hypothesis of linear independance is required in

our result (see Corollary 1.51, Theorem 1.57 and Corollary 1.62). We note that an elementary and explicit proof of the continuous version of the Kronecker-Weyl theorem was given in the arXiv version [MN17] of [MN20], Appendix B.

The Kronecker-Weyl theorem is at the heart of the modern approach (initiated by Rubinstein and Sarnak in [RS94]) to the study of so-called "prime number races", which consists in investigating the properties of the set

$$\mathcal{P}_{q;a_1,\dots,a_D} := \{x \geq 2 \mid \pi(x;q,a_1) > \pi(x;q,a_2) > \cdots > \pi(x;q,a_D)\},$$

where $\pi(x;k,c)$ is the number of primes $p \leq x$ such that $p \equiv c \bmod k$. Here, the invertible classes $a_1,\dots,a_D$ are called the *contestants* of the prime number race. Assuming the Generalized Riemann Hypothesis, Rubinstein and Sarnak proved that functions of the form

$$E_{q;a_1,\dots,a_D} : y \mapsto \left(\pi(e^y;q,a_1) - \frac{\mathrm{Li}(e^y)}{\varphi(q)},\dots,\pi(e^y;q,a_D) - \frac{\mathrm{Li}(e^y)}{\varphi(q)}\right)$$

admit limiting distributions, according to the following definition.

Definition 1.46. *Let $E : \mathbb{R}^+ \longrightarrow \mathbb{R}^D$. We say E admits a limiting distribution μ when μ is a Borel probability measure on $\mathbb{R}^d$ such that for any bounded continuous function $f : \mathbb{R}^D \longrightarrow \mathbb{R}$, one has*

$$\frac{1}{X}\int_0^X f(E(y))\,\mathrm{d}y \underset{X\to+\infty}{\longrightarrow} \int_{\mathbb{R}^D} f\,\mathrm{d}\mu.$$

From there, and assuming the linear independence over $\mathbb{Q}$ of the non-negative imaginary parts of non-trivial zeros of Dirichlet L-functions mod q (an hypothesis called the Grand Simplicity Hypothesis or GSH in [RS94]), Rubinstein and Sarnak proved that sets of the form

$$\{x \geq 2 \mid \pi(e^x;q,a_1) > \pi(e^x;q,a_2) > \cdots > \pi(e^x;q,a_D)\}$$

admit natural densities strictly between 0 and 1.

The discrete version of the Kronecker-Weyl theorem has been used initially by Cha [Cha08], followed by other authors ([CI11], [CFJ16], [DM20]), to study other kinds of prime number races over function fields, still assuming some form of linear independence between the zeros of the corresponding L-functions.

Further works aimed at weakening those linear independence hypotheses. In [MN20], Martin and Ng introduced the notions of *exhaustivity*, *weak inclusiveness* and *inclusiveness* of prime number races, focusing on the unboundedness (resp. the existence of the logarithmic densities, resp. the positivity of the logarithmic densities) of sets of the form $\mathcal{P}_{q;a_1,\dots,a_D}$. They introduced the notion of *self-sufficient zero* ([MN20, Definition 1.3]), and assuming various hypotheses on the existence of such zeros, proved the weak inclusivenes or inclusiveness of the corresponding prime number races. These assumptions were weakened by Devin in [Dev19], who even studied the regularity of the corresponding limiting distributions in a more general setting.

Among the aforementioned properties we will mostly be interested in weak inclusiveness and inclusiveness. We recall the definition of these notions in the context of general prime number races.

Definition 1.47. *Let $a_1, \dots, a_D$ be contestants in a prime number race. We say the race between $a_1, \dots, a_D$ is weakly inclusive if for every permutation σ of $\{1, \dots, D\}$, the set $\{X \geq 2 \mid \Pi(X, a_{\sigma(1)}) > \cdots > \Pi(X, a_{\sigma(D)})\}$ admits a natural density, where the $\Pi(\cdot, a)$ are the corresponding rescaled prime counting functions. We say the prime number race is inclusive if moreover those densities are positive.*

The prime number races referred to in the above definition will be of two types in the present work. First, a prime number race over a number field denotes the race between unramified prime ideals in a Galois extension L/K of number fields with given Frobenius automorphisms in $\mathrm{Gal}(L/K)$, as was first suggested in [RS94, Section 5] and first studied in [Ng00, Chapter 5]. In that case, the contestants are distinct conjugacy classes $C_1, \dots, C_D$ of $\mathrm{Gal}(L/K)$, and the rescaled prime counting functions are

$$\Pi(X, C_i) := \frac{\pi(e^X; L/K, C_i)}{\#C_i} = \frac{1}{\#C_i} \#\{\mathfrak{p} \text{ prime ideal of } K \text{ unramified in } L \mid N\mathfrak{p} \leq e^X, \mathrm{Frob}_{\mathfrak{p}} = C_i\}.$$

That the variable has to be changed to e^X comes from the shape of the explicit formulas involved (see [Ng00, Chapter 5]).

Second, a prime number race over a function field denotes the race between unramified prime divisors in a Galois extension L/K of functions fields in one variable over a finite field with given Frobenius automorphisms in $\mathrm{Gal}(L/K)$. In that case, the contestants are distinct conjugacy classes $C_1, \dots, C_D$ of $\mathrm{Gal}(L/K)$, and the rescaled prime counting functions are

$$\Pi(X, C_i) := \frac{\pi(X; L/K, C_i)}{\#C_i} = \frac{1}{\#C_i} \#\{P \text{ prime divisor of } K \text{ unramified in } L \mid \deg P = X, \mathrm{Frob}_P = C_i\}.$$

One can also consider functions counting prime divisors of K with a given Frobenius automorphism of degree less than X, instead of equal to X, as was studied in [CI11]. Of course we recover the classical case of Rubinstein and Sarnak for primes in arithmetic progressions [RS94] in the number field case by considering an appropriate cyclotomic extension of $\mathbb{Q}$. Similarly we recover the races between irreducible polynomials in arithmetic progressions of [Cha08] by considering an appropriate Carlitz extension of $\mathbb{F}_q(T)$.

More general races have been studied in the literature, for instance the race between prime quadratic residues and prime non-quadratic residues modulo an integer q in [RS94], the race between $\pi(x)$ and $\mathrm{Li}(x)$ in [RS94] and [ANS14], the race between products of k irreducible polynomials over a finite field in [DM20], the race between the number of points on the reduction modulo good primes of elliptic curves in [CFJ16] and many more. In any case, it is clear to which category each of those races should belong, either over number fields or function fields. Our general results can be applied to those situations as well.

The first step in studying a prime number race over a function field is to write an explicit formula, *i.e.* express the corresponding prime counting functions as sums involving $e^{i\theta_1 X}, \dots, e^{i\theta_r X}$, where $\theta_1, \dots, \theta_r$ are the positive arguments (between 0 and π) of the inverse zeros of the corresponding rational L-functions. As an application of our version of the discrete Kronecker-Weyl theorem, we give sufficient conditions for the existence and for the positivity of the natural densities relevant to those kinds of races. Recently, Devin ([Dev20]) studied the question of the existence of those densities, and provided sufficient conditions on

the coefficients of the functions involved in the explicit formulas. Our approach is transverse to hers, as we give conditions on the functions themselves. Our approach is also considerably more elementary, as Devin relies on multiple tools of harmonic analysis to deduce that "ties have density zero" in such races. We avoid the use of such techniques thanks to our approach based on random variables and our key Lemma 1.56.

In the case of prime number races over number fields, the situation is technically more complicated, since explicit formulas for the (rescaled) prime counting functions involve infinite series in $e^{i\theta_1 t}, e^{i\theta_2 t}, \dots$ where $\theta_1, \theta_2, \dots$ are the positive imaginary parts of non-trivial zeros of the corresponding L-functions. Functions of this shape are often called almost-periodic functions. There are different classes of almost-periodic functions, depending on the way they can be approximated by trigonometric polynomials. The class which is most relevant to us is the (large) class of Besicovitch almost-periodic functions, called B^1 almost-periodic functions. The existence of the limiting distributions of such functions was shown in [ANS14, Theorem 2.9]. See also [Ble92, Theorem 4.1] for a similar proof in a slightly larger space than B^1. As an application of our version of the Kronecker-Weyl theorem, we give a more precise description of this limiting distribution, under various hypotheses on the almost-periods θ_n of the B^1 almost-periodic function which is being studied (Corollary 1.70). We also give a new proof of a recent result of Devin, giving sufficient conditions for the existence of the densities associated to B^1-almost periodic functions. Our approach is again more elementary and does not require the use of abstract harmonic analysis (see Corollary 1.79). We give an application to the existence of the densities involved in prime number races over number fields in Theorem 1.82.

The paper is organized as follows. In the first part, we prove explicit versions of the Kronecker-Weyl theorem, in three different cases (two discrete and one continuous) and derive consequences for the study of asymptotic densities of sets defined by strict inequalities between certain types of functions. The two discrete cases are the degenerate case in which each θ_i is a rational multiple of π (Proposition 1.50), and the non-degenerate case (Theorem 1.52). The continuous case is considered in Theorem 1.59. We apply those three theorems to obtain the existence of asymptotic densities for sets defined by strict inequalities between certain types of functions (Corollary 1.51, Theorem 1.57 and Theorem 1.62) without any linear independence hypothesis. In doing so, we prove Lemma 1.56 which allows us to bypass technical results from harmonic analysis to prove that the limiting distributions we consider do not admit atoms. We then generalize our methods in the presence of infinitely many real numbers $\theta_1, \theta_2, \dots$. In this context, we prove that B^1 almost-periodic functions admit limiting distributions (Theorem 1.65), and then under a weak linear independence assumption, we give a description of this limiting distribution (Theorem 1.70). We then tackle the problem of the existence of asymptotic densities for sets defined by strict inequalities between B^1 almost-periodic functions, assuming suitable hypotheses (Proposition 1.73 and Theorem 1.79). We then prove similar results for functions with an extra error term (Theorem 1.80), as those are the kind of functions appearing in explicit formulas for prime number races.

The second part of the paper is devoted to applications. First, we give criteria for the positivity of asymptotic densities of certain sets defined by strict inequalities (Propositions 1.84 and 1.86), with inclusiveness of prime number races over function fields in mind. We then apply the general results of the first section to the concrete problem of studying prime divisor races in geometric Galois extensions of function fields (in one variable) over finite

fields. In particular, we are able to study an example of prime divisor race in which the usual linear independence hypothesis fails to hold. In the last section of the paper, we discuss the first two moments of the random variables involved in those kinds of races.

It seems a reference to a proof of the discrete version of the Kronecker-Weyl theorem is hard to find in a published form so we provide a proof in an appendix. We borrowed the proof to P. Humphries' Masters thesis [Hum12]. For a proof of the general continuous version, see [Dev19, Theorem 4.2].

Notations. Some notations are introduced at various places and then used many times throughout the text and we gather them here for reference. The element ν_θ always denotes $\left(e^{i\theta_1}, \dots, e^{i\theta_r}\right)$. The quantities d and $h_{k,j}$ coming from linear dependence relations are introduced at the beginning of Section 1.4.1.1, Section 1.4.1.2 and Section 1.4.1.3, depending on the context. The subgroup $H_\theta \subset \mathbb{T}^r$ arising in the non-degenerate case is defined in Theorem 1.52. The random variables Z_θ are introduced, depending on the context, in Corollary 1.51 (degenerate case), Definition 2.57 (non-degenerate case) or Corollary 1.60 (continuous case).

1.4.1 Explicit Kronecker-Weyl theorems

We begin by recalling the definition of equidistribution that we are going to use throughout the text.

Definition 1.48. *Let $(z_n)_{n\in\mathbb{N}}$ be a sequence of elements of $\mathbb{T}^r$ and H a closed subgroup of $\mathbb{T}^r$, and let μ_H be the Haar measure of H. We say $(z_n)_{n\in\mathbb{N}}$ is equidistributed in H with respect to the measure μ_H if for every continuous $f : \mathbb{T}^r \to \mathbb{C}$, one has*

$$\frac{1}{X}\sum_{n\leq X} f(z_n) \underset{X\to+\infty}{\longrightarrow} \int_H f \,\mathrm{d}\mu_H.$$

This definition is equivalent to the weak convergence of the measures $\frac{1}{X}\sum_{n\leq X}\delta_{z_n}$ to the measure μ_H, where δ_{z_n} is the Dirac measure at z_n. In what follows, we identify such a sequence with the set $Z := \{z_n \mid n \in \mathbb{N}\}$. This is a slight abuse of notation since the set Z itself does not keep track of the numbering of the sequence. Note that if Z is equidistributed in H, then Z is in particular dense in H, so that $\overline{Z} = H$. The following is a weak version of the discrete Kronecker-Weyl theorem, which will be enough for our purpose of proving an explicit strong version.

Theorem 1.49. *Let $\theta_1, \dots, \theta_r$ be real numbers such that $\{\theta_1, \dots, \theta_r, \pi\}$ is linearly independent over $\mathbb{Q}$. Then the set*

$$\Gamma := \left\{\left(e^{i\theta_1 X}, \dots, e^{i\theta_r X}\right) \mid X \in \mathbb{Z}\right\}$$

is equidistributed in $\mathbb{T}^r$ (with respect to its Haar measure).

A proof is given in an appendix for reference. Notice the additional linear independence assumption with π. The goal of the following sections is to prove a precise version of this result (and of its continuous analog) with no assumption of linear independence (even with π) and with a description of the subset of $\mathbb{T}^r$ in which Γ is equidistributed. We also do so by elementary means, while many proofs of the full Kronecker-Weyl theorem use abstract harmonic analysis (Pontryagin duality and Poisson summation formula).

1.4.1.1 The degenerate discrete case

In this section, consider real numbers $\theta_1, \dots, \theta_r$ which are all rational multiples of π : $\theta_i = c_i\pi$ where each $c_i \in \mathbb{Q}$ for $1 \leq i \leq r$. Let $\nu_\theta = \left(e^{i\theta_1}, \dots, e^{i\theta_r}\right)$. Clearly ν_θ is of finite order d in $\mathbb{T}^r$. Write $\theta = (\theta_1, \dots, \theta_r)$. We then have the following result.

Proposition 1.50. *Let $\Gamma_\theta = \left\{\left(e^{i\theta_1 X}, \dots, e^{i\theta_r X}\right) \mid X \in \mathbb{Z}\right\}$. Then Γ_θ is equidistributed in the cyclic subgroup $\langle\nu_\theta\rangle$ generated by ν_θ with respect to its uniform measure. In fact for any function $f : \mathbb{T}^r \longrightarrow \mathbb{C}$, one has*

$$\frac{1}{X}\sum_{n\leq X} f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) \underset{X\to+\infty}{\longrightarrow} \frac{1}{d}\sum_{a=0}^{d-1} f(\nu_\theta^a).$$

Proof. Clearly we have $\Gamma_\theta = \{(1, \dots, 1), \nu_\theta, \nu_\theta^2, \dots, \nu_\theta^{d-1}\} = \langle\nu_\theta\rangle$. Let $f : \mathbb{T}^r \longrightarrow \mathbb{C}$ be any function. We then have

$$\begin{aligned}
\frac{1}{X}\sum_{n\leq X} f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) &= \frac{1}{X}\sum_{q=0}^{\left\lfloor\frac{X}{d}\right\rfloor}\sum_{a=0}^{d-1} f(\nu_\theta^{qd+a}) + o(1) \\
&= \frac{1}{X}\sum_{q=0}^{\left\lfloor\frac{X}{d}\right\rfloor}\sum_{a=0}^{d-1} f(\nu_\theta^{a}) + o(1) \\
&= \frac{\left\lfloor\frac{X}{d}\right\rfloor}{X}\sum_{a=0}^{d-1} f(\nu_\theta^{a}) + o(1) \underset{X\to+\infty}{\longrightarrow} \frac{1}{d}\sum_{a=0}^{d-1} f(\nu_\theta^{a}).
\end{aligned}$$

□

Corollary 1.51. *Let $f_1, \dots, f_D : \mathbb{T}^r \longrightarrow \mathbb{R}$ and let $F_j : t \mapsto f_j\left(e^{i\theta_1 t}, \dots, e^{i\theta_r t}\right)$ for $1 \leq j \leq D$. Then*

$$\frac{1}{X}\#\left\{n \leq X \mid F_1(n) > \cdots > F_D(n)\right\} \underset{X\to+\infty}{\longrightarrow} \mathbb{P}(f_1(Z_\theta) > \cdots > f_D(Z_\theta))$$

where Z_θ is a (discrete) uniform random variable on $\langle\nu_\theta\rangle$.

Proof. Apply Theorem 1.50 to the function $\mathbf{1}_{x_1>\cdots>x_D} \circ (f_1, \dots, f_D)$. □

1.4.1.2 The non-degenerate discrete case

We now consider real numbers $\theta_1, \dots, \theta_r$, at least one of which is not a rational multiple of π, say θ_1. Write again $\theta = (\theta_1, \dots, \theta_r)$.

Up to reindexing, extract a basis $\{2\pi, \theta_1, \dots, \theta_m\}$ of the $\mathbb{Q}$-vector space $\mathrm{Span}_{\mathbb{Q}}(\pi, \theta_1, \dots, \theta_r)$. Now, we write the decomposition of $\theta_{m+1}, \dots, \theta_r$ in this basis :

$$\theta_j = 2\pi c_j + \sum_{k=1}^{m} b_{k,j}\theta_k \text{ for } m+1 \leq j \leq r$$

with $c_j, b_{k,j} \in \mathbb{Q}$.

Finally, we let d be the least common multiple of the denominators of each c_j and each $b_{k,j}$, so that $l_j := dc_j \in \mathbb{Z}, h_{k,j} := db_{k,j} \in \mathbb{Z}$.

Theorem 1.52. *Let* $\Gamma_\theta = \left\{\left(e^{i\theta_1 X}, \dots, e^{i\theta_r X}\right) \mid X \in \mathbb{Z}\right\}$. *Then* Γ_θ *is equidistributed in* $\overline{\Gamma_\theta} = \bigcup_{a=0}^{d-1} \nu_\theta^a H_\theta = \langle \nu_\theta \rangle H_\theta$, *where* $\nu_\theta = \left(e^{i\theta_1}, \dots, e^{i\theta_r}\right)$ *and*

$$H_\theta = \left\{ \left(z_1^d, \dots, z_m^d, \prod_{k=1}^m z_k^{h_{k,m+1}}, \dots, \prod_{k=1}^m z_k^{h_{k,r}} \right) \mid (z_1, \dots, z_m) \in \mathbb{T}^m \right\} \subset \mathbb{T}^r$$

with Haar measure μ_{H_θ}. *The measure with respect to which* Γ_θ *is equidistributed is* $\frac{1}{d}\sum_{a=0}^{d-1} \mu_a$, *where* μ_a *is the pushforward of* μ_{H_θ} *to* $\nu_\theta^a H_\theta$.

Proof. We first show that

$$\Gamma_\theta = \bigcup_{a=0}^{d-1} \nu_\theta^a \tilde{H}$$

where

$$\tilde{H} := \left\{ \left(e^{id\theta_1 q}, \dots, e^{id\theta_m q}, \dots, \prod_{k=1}^m e^{ih_{k,j}\theta_k q}, \dots \right) \mid q \in \mathbb{Z} \right\}.$$

To do this, we split Γ_θ according to its congruence classes modulo d :

$$\Gamma_\theta = \bigcup_{a=0}^{d-1} \Gamma_a,$$

where

$$\Gamma_a := \left\{ \left(e^{i\theta_1 X}, \dots, e^{i\theta_r X}\right) \mid X \equiv a \bmod d \right\}.$$

Expressing each θ_j with $m+1 \le j \le r$ in the basis $\{2\pi, \theta_1, \dots, \theta_m\}$, we find for $0 \le a \le d-1$,

$$\begin{aligned}
\Gamma_a &= \left\{ \left(e^{ia\theta_1} e^{id\theta_1 q}, \dots, e^{ia\theta_m} e^{id\theta_m q}, \dots, e^{2i\pi l_j q} e^{2i\pi a c_j} \prod_{k=1}^m e^{iab_{k,j}\theta_k} \prod_{k=1}^m e^{ih_{k,j}\theta_k q}, \dots \right) \mid q \in \mathbb{Z} \right\} \\
&= \left\{ \left(\nu_1^a e^{id\theta_1 q}, \dots, \nu_m^a e^{id\theta_m q}, \dots, \nu_j^a \prod_{k=1}^m e^{ih_{k,j}\theta_k q}, \dots \right) \mid q \in \mathbb{Z} \right\}
\end{aligned}$$

where we wrote

$$\nu_j = e^{i\theta_j} \text{ for } 1 \le j \le m$$

and

$$\nu_j = e^{2i\pi c_j} \prod_{k=1}^m e^{ib_{k,j}\theta_k} = e^{i\theta_j} \text{ for } m+1 \le j \le r.$$

We have thus shown that

$$\Gamma_\theta = \bigcup_{a=0}^{d-1} \nu_\theta^a \tilde{H}$$

as announced.

Let us show that this union is disjoint : let $a, b \in \{0, \dots, d-1\}$. If $\nu_1^a e^{id\theta_1 q} = \nu_1^b e^{id\theta_1 q'}$ then we have $\theta_1(a + qd - b - q'd) = 2k\pi$ for some $k \in \mathbb{Z}$. Since θ_1 is not a rational multiple of π, we find $a + qd = b + q'd$, hence $a = b$ by uniqueness of the remainder in euclidean division.

Now the discrete Kronecker-Weyl theorem 1.49 implies that $\left\{\left(e^{i\theta_1 X},\dots,e^{i\theta_m X}\right) \mid X\in\mathbb{Z}\right\}$ is equidistributed in $\mathbb{T}^m$. Lifting by the continuous surjective homomorphism

$$\begin{array}{rccc} & \mathbb{T}^m & \longrightarrow & H_\theta \\ \varphi: & (z_1,\dots,z_m) & \mapsto & \left(z_1^d,\dots,z_m^d,\prod_{k=1}^m z_k^{h_{k,m+1}},\dots,\prod_{k=1}^m z_k^{h_{k,r}}\right)\end{array}$$

we find that for every continuous $f:\mathbb{T}^r\to\mathbb{C}$, one has

$$\begin{aligned}\frac{1}{X}\sum_{q\le X} f\left(e^{id\theta_1 q},\dots,e^{id\theta_m q},\dots,\prod_{k=1}^m e^{ih_{k,j}\theta_k q},\dots\right) &= \frac{1}{X}\sum_{q\le X} f\circ\varphi\left(e^{i\theta_1 q},\dots,e^{i\theta_m q}\right)\\ &\underset{X\to+\infty}{\longrightarrow} \int_{\mathbb{T}^m} f\circ\varphi\,\mathrm{d}\mu\\ &= \int_{H_\theta} f\,\mathrm{d}(\varphi_*\lambda).\end{aligned}$$

where $\varphi_*\lambda$ is the pushforward measure of the Lebesgue measure on $\mathbb{T}^m$ by φ. This measure is readily verified to be the Haar measure μ_{H_θ} on H_θ, since it has mass one and it is invariant by translations.

We have thus shown that for every continuous $f:\mathbb{T}^r\to\mathbb{C}$, one has

$$\frac{1}{X}\sum_{q=1}^{X} f\left(e^{id\theta_1 q},\dots,e^{id\theta_m q},\dots,\prod_{k=1}^m e^{ih_{k,j}\theta_k q},\dots\right)\underset{X\to+\infty}{\longrightarrow}\int_{H_\theta} f\,\mathrm{d}\mu_{H_\theta},$$

i.e. that $\tilde{H}$ is equidistributed in H_θ with respect to its Haar measure. If we take any such f and sum it over Γ_θ instead, we now find, using the previous disjoint decomposition of Γ_θ, that

$$\begin{aligned}\frac{1}{X}\sum_{n\le X} f\left(e^{i\theta_1 n},\dots,e^{i\theta_r n}\right) &= \frac{1}{X}\sum_{a=0}^{d-1}\sum_{q=0}^{\left\lfloor\frac{X}{d}\right\rfloor} f\left(\nu_1^a e^{id\theta_1 q},\dots,\nu_m^a e^{id\theta_m q},\dots,\nu_j^a\prod_{k=1}^m e^{ih_{k,j}\theta_k q},\dots\right)+o(1)\\ &= \frac{1}{d}\sum_{a=0}^{d-1}\frac{1}{\left\lfloor\frac{X}{d}\right\rfloor}\sum_{q=1}^{\left\lfloor\frac{X}{d}\right\rfloor} f_a\left(e^{id\theta_1 q},\dots,e^{id\theta_m q},\dots,\prod_{k=1}^m e^{ih_{k,j}\theta_k q},\dots\right)+o(1)\end{aligned}$$

where $f_a: z\mapsto f(\nu_\theta^a z)$ for $0\le a\le d-1$. We finally obtain

$$\frac{1}{X}\sum_{n\le X} f\left(e^{i\theta_1 n},\dots,e^{i\theta_r n}\right)\underset{X\to+\infty}{\longrightarrow}\frac{1}{d}\sum_{a=0}^{d-1}\int_{H_\theta} f_a\,\mathrm{d}\mu_{H_\theta}=\int_{\overline{\Gamma_\theta}} f\,\mathrm{d}\nu_\theta.$$

□

Remarks 1.53.

i) The element ν_θ of the above theorem is not of finite order in $\mathbb{T}^r$, since $\nu_1=e^{i\theta_1}$ has infinite order in $\mathbb{T}$, but it has finite order dividing d in $\mathbb{T}^r/H_\theta$. Therefore the product of the two subgroups $\langle\nu_\theta\rangle$ and H_θ is indeed $\bigcup_{a=0}^{d-1}\nu_\theta^a H_\theta$.

ii) The subgroup H_θ is a subtorus of $\mathbb{T}^r$ of dimension m, and the conclusion of the above theorem is that Γ_θ is equidistributed in the union of d translates of this subtorus. Note that this union is not necessarily disjoint, as it would imply $\overline{\Gamma_\theta}$ has exactly d connected components, but the number d can be modified by choosing a different basis of $\mathrm{Span}_{\mathbb{Q}}(\pi, \theta_1, \dots, \theta_r)$ without changing Γ_θ.

iii) If $\{\pi, \theta_1, \dots, \theta_r\}$ is $\mathbb{Q}$-linearly independent, then we have $m = r, d = 1$ and $\overline{\Gamma_\theta} = \mathbb{T}^r$ as in Theorem 1.49.

Definition 1.54. *The random vector associated with $\theta_1, \dots, \theta_r$ is the $\mathbb{T}^r$-valued random vector*

$$Z_\theta := \left(Z_1^d, \dots, Z_m^d, \dots, \prod_{k=1}^m Z_k^{h_{k,j}}, \dots \right)$$

where m, d and $h_{k,j}$ are defined at the beginning of Section 1.4.1.2, and where $Z_1, \dots, Z_m$ are independent uniform random variables on $\mathbb{T}$. We also note $\nu_\theta = \left(e^{i\theta_1}, \dots, e^{i\theta_r}\right)$.

Corollary 1.55. *For any continuous $f : \mathbb{T}^r \to \mathbb{C}$, we have*

$$\frac{1}{X} \sum_{n \leq X} f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) \underset{X \to +\infty}{\longrightarrow} \frac{1}{d} \sum_{a=0}^{d-1} \mathbb{E}\left(f\left(\nu_\theta^a Z_\theta\right)\right).$$

Proof. This is just a reformulation of Theorem 1.52, where we observe that the distribution of the random vector $\nu_\theta^a Z_\theta$ is simply the measure μ_a. □

In the context of prime number races over function fields, one approaches prime counting functions by functions of the form $t \mapsto c + \sum_{j=1}^r a_j e^{i\theta_j t} + \overline{a_j} e^{-i\theta_j t}$, with real c and complex a_j. Note that those are in particular polynomials in $e^{i\theta_1 t}, e^{-i\theta_1 t}, \dots, e^{i\theta_r t}, e^{-i\theta_1 t}$, *i.e.* Laurent polynomials in $e^{i\theta_1 t}, \dots, e^{i\theta_1 r}$, for which we prove the following key elementary lemma.

Lemma 1.56. *Let $f \in \mathbb{C}(X_1, \dots, X_r)$ with no pole in $\mathbb{T}^r$. Then for $0 \leq a \leq d-1$, one has $\mathbb{P}(f(\nu_\theta^a Z_\theta) = 0) = 0$ if and only if there exists $n \equiv a \bmod d$ such that $f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) \neq 0$.*

Proof. Recall that $\Gamma_a = \left\{ \left(e^{i\theta_1 X}, \dots, e^{i\theta_r X}\right) \mid X \equiv a \bmod d \right\}$ is equidistributed in $\nu_\theta^a H_\theta$ and that the distribution of Z_θ is precisely the Haar measure on H_θ. Therefore, if $f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) = 0$ for all $n \equiv a \bmod d$, then by continuity of f and density of Γ_a in $\nu_\theta^a H_\theta$, we have $\mathbb{P}(f(\nu_\theta^a Z_\theta) = 0) = 1$.

We prove the converse statement by induction on m. If $m = 1$, then the equation

$$f\left(\nu_{\theta,1}^a z^d, \nu_{\theta,2}^a z^{h_{1,2}}, \dots, \nu_{\theta,r}^a z^{h_{1,r}}\right) = 0$$

reduces, by clearing denominators, to a polynomial equation $P(z) = 0$ with one unknown. This equation is non-trivial because, writing $n = qd + a$ with $q \in \mathbb{Z}$, we have

$$\begin{aligned} f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) &= f\left(e^{ia\theta_1} e^{iq\theta_1 d}, e^{i(qd+a)(2\pi c_2 + b_{1,2}\theta_1)}, \dots, e^{i(qd+a)(2\pi c_r + b_{1,r}\theta_1)}\right) \\ &= f\left(\nu_{\theta,1}^a e^{iq\theta_1 d}, \nu_{\theta_2}^a e^{iq\theta_1 h_{1,2}}, \dots, \nu_{\theta_r}^a e^{iq\theta_1 h_{1,r}}\right) \neq 0 \end{aligned}$$

by hypothesis, so that $P\left(e^{iq\theta_1}\right) \neq 0$. Therefore, this equation has a finite number of solutions in $\mathbb{C}$, and in particular in $\mathbb{T}$. Since Z_1 is uniform on the circle, we certainly have

$$\mathbb{P}(f(\nu_\theta^a Z_\theta) = 0) = \mathbb{P}\left(f\left(\nu_{\theta,1}^a Z_1^d, \nu_{\theta,2}^a Z_1^{h_{1,2}}, \dots, \nu_{\theta,r}^a Z_1^{h_{1,r}}\right) = 0\right) = 0.$$

Now assume the result is true for $m-1 \in \mathbb{N}$. As before, by clearing denominators, the equation

$$f\left(\nu_{\theta,1}^a z_1^d, \dots, z_m^d, \dots, \nu_{\theta,j}^a \prod_{k=1}^m z_k^{h_{k,j}}, \dots\right) = 0$$

is equivalent to a non-zero polynomial equation $P(z_1, \dots, z_m) = 0$ with m unknowns. Moreover, the set F of all $z_m \in \mathbb{T}$ such that $P(X_1, \dots, X_{m-1}, z_m) = 0$ is finite, since it is the zero set of the $P(X_1, \dots, X_{m-1}, Y) \in \mathbb{C}[X_1, \dots, X_{m-1}][Y]$, which is non-zero because as above we have $P\left(e^{iq\theta_1}, \dots, e^{iq\theta_m}\right) \neq 0$ by hypothesis on $n = qd + a$. By the Fubini-Tonelli theorem, we find

$$\begin{aligned}
\mathbb{P}\left(f\left(\nu_\theta^a Z_\theta\right) = 0\right) &= \mathbb{P}\left(f\left(\nu_{\theta,1}^a Z_1^d, \dots, \nu_{\theta,m}^a Z_m^d, \dots, \nu_{\theta,j}^a \prod_{k=1}^m Z_k^{h_{k,j}}, \dots\right) = 0\right) \\
&= \mathbb{P}(P(Z_1, \dots, Z_m) = 0) \\
&= \int_{\mathbb{T}^m} \mathbf{1}_{P^{-1}(\{0\})}(z)\, \mathrm{d}z \\
&= \int_{\mathbb{T}\setminus F} \left(\int_{\mathbb{T}^{m-1}} \mathbf{1}_{P(\cdot, z_m)^{-1}(\{0\})}(z_1, \dots, z_{m-1})\, \mathrm{d}z_1 \dots \mathrm{d}z_{m-1}\right) \mathrm{d}z_m
\end{aligned}$$

The inner integral is zero by the induction hypothesis, so we conclude that $\mathbb{P}\left(f\left(\nu_\theta^a Z_\theta\right) = 0\right) = 0$. □

We can now prove the following theorem which allows us to pass from continuous functions to indicator functions of subsets of $\mathbb{R}^D$ defined by strict inequalities between functions as in Lemma 1.56.

Theorem 1.57. *For $1 \leq j \leq D$, let $f_j \in \mathbb{C}(X_1, \dots, X_r)$ be real-valued and without pole on $\mathbb{T}^r$ and let $F_j : t \mapsto f_j\left(e^{i\theta_1 t}, \dots, e^{i\theta_r t}\right)$. Then we have*

$$\frac{1}{X}\#\left\{n \leq X \mid F_1(n) > \dots > F_D(n)\right\} \underset{X\to+\infty}{\longrightarrow} \frac{1}{d}\sum_{a=0}^{d-1} \mathbb{P}(f_1(\nu_\theta^a Z_\theta) > \dots > f_D(\nu_\theta^a Z_\theta)).$$

Proof. We first remark that, by Lemma 1.56 and its proof, if for some $0 \leq a \leq d-1$, there exists $1 \leq j \leq D-1$ such that $f_j\left(e^{in\theta_1}, \dots, e^{in\theta_r}\right) = f_{j+1}\left(e^{in\theta_1}, \dots, e^{in\theta_r}\right)$ for every $n \equiv a \bmod d$, then $\mathbb{P}(f_j(\nu_\theta^a Z_\theta) = f_{j+1}(\nu_\theta^a Z_\theta)) = 1$, so that $\mathbb{P}(f_1(\nu_\theta^a Z_\theta) > \dots > f_D(\nu_\theta^a Z_\theta)) = 0$, while we have $\lim_{X\to+\infty} \frac{1}{X}\#\left\{n \leq X \mid n \equiv a \bmod q, F_1(n) > \dots > F_D(n)\right\} = 0$. Therefore, writing

$$\frac{1}{X}\#\left\{n \leq X \mid F_1(n) > \dots > F_D(n)\right\} = \frac{1}{d}\sum_{a=0}^{d-1} \frac{1}{X}\#\left\{n \leq X \mid n \equiv a \bmod d, F_1(n) > \dots > F_D(n)\right\} + o(1),$$

and using the decomposition $\Gamma = \bigcup_{a=0}^{d-1} \nu_\theta^a \tilde{H}$ as in the proof of Theorem 1.52, we may assume that for every $0 \leq a \leq d-1, 1 \leq j \leq D-1$, there exists $n \equiv a \bmod d$ such

that $f_j\left(e^{in\theta_1},\dots,e^{in\theta_r}\right) \neq f_{j+1}\left(e^{in\theta_1},\dots,e^{in\theta_r}\right)$. By Lemma 1.56 we then have $\mathbb{P}(f_j(\nu_\theta^a Z_\theta) = f_{j+1}(\nu_\theta^a Z_\theta)) = 0$ for every such a and j.

Now, we need to approximate the indicator function $\mathbf{1}_{x_1>\cdots>x_D}$ by continuous functions from above and below. We proceed in the following way : for every integer $k \geq 1$ and $x, y \in \mathbb{R}$, let

$$g_k(x,y) := \begin{cases} 0 \text{ if } x \leq y - \frac{1}{k} \\ k(x-y)+1 \text{ if } y - \frac{1}{k} < x \leq y \\ 1 \text{ if } x > y \end{cases}.$$

Then for each integer $k \geq 1$, g_k is continuous on $\mathbb{R}^2$ and for all $x, y \in \mathbb{R}$,

$$\mathbf{1}_{x_1>x_2}(x,y) \leq g_k(x,y) \leq \mathbf{1}_{x_1>x_2-\frac{1}{k}}(x,y).$$

For $k \geq 1$ let $G_k : (x_1,\dots,x_D) \mapsto \prod_{j=1}^{D-1} g_k(x_j, x_{j+1})$. Then for every $k \geq 1$ and $n \in \mathbb{Z}$, we have

$$\begin{aligned}
\mathbf{1}_{x_1>\cdots>x_D}(F_1(n),\dots,F_D(n)) &= \prod_{j=1}^{D-1} \mathbf{1}_{x_j>x_{j+1}}(F_j(n),F_{j+1}(n)) \\
&\leq \prod_{j=1}^{D-1} g_k(F_j(n),F_{j+1}(n)) \\
&= G_k(F_1(n),\dots,F_D(n)) \\
&\leq \prod_{j=1}^{D-1} \mathbf{1}_{x_j>x_{j+1}-\frac{1}{k}}(F_j(n),F_{j+1}(n)) \\
&= \mathbf{1}_{x_1>x_2-\frac{1}{k}>\cdots>x_D-\frac{D-1}{k}}(F_1(n),\dots,F_D(n))
\end{aligned}$$

Now, by Corollary 1.55, for every $k \geq 1$,

$$\begin{aligned}
\limsup_{X\to+\infty} \frac{1}{X}\sum_{n=1}^{X} \mathbf{1}_{x_1>\cdots>x_D}(F_1(n),\dots,F_D(n)) &\leq \limsup_{X\to+\infty} \frac{1}{X}\sum_{n=1}^{X} G_k(F_1(n),\dots,F_D(n)) \\
&= \frac{1}{d}\sum_{a=0}^{d-1} \mathbb{E}(G_k(f_1(\nu_\theta^a Z_\theta),\dots,f_D(\nu_\theta^a Z_\theta))) \\
&\leq \frac{1}{d}\sum_{a=0}^{d-1} \mathbb{E}\left(\mathbf{1}_{x_1>x_2-\frac{1}{k}>\cdots>x_D-\frac{D-1}{k}}(f_1(\nu_\theta^a Z_\theta),\dots,f_D(\nu_\theta^a Z_\theta)\right) \\
&= \frac{1}{d}\sum_{a=0}^{d-1} \mathbb{P}\left(f_1(\nu_\theta^a Z_\theta) > \cdots > f_D(\nu_\theta^a Z_\theta) - \frac{D-1}{k}\right).
\end{aligned}$$

By downward continuity of $\mathbb{P}$, we get, by letting $k \to +\infty$,

$$\limsup_{X\to+\infty} \frac{1}{X}\sum_{n=1}^{X} \mathbf{1}_{x_1>\cdots>x_D}(F_1(n),\dots,F_D(n)) \leq \frac{1}{d}\sum_{a=0}^{d-1} \mathbb{P}\left(f_1(\nu_\theta^a Z_\theta) \geq \cdots \geq f_D(\nu_\theta^a Z_\theta)\right).$$

Similarly, by considering the functions defined by

$$(x,y) \mapsto \begin{cases} 0 \text{ if } x < y \\ k(x-y) \text{ if } y \leq x < y + \frac{1}{k} \\ 1 \text{ if } x > y + \frac{1}{k} \end{cases},$$

we find

$$\liminf_{X\to+\infty}\frac{1}{X}\sum_{n=1}^{X}\mathbf{1}_{x_1>\cdots>x_D}\left(F_1(n),\dots,F_D(n)\right)\geq\frac{1}{d}\sum_{a=0}^{d-1}\mathbb{P}\left(f_1(\nu_\theta^a Z_\theta)>\cdots>f_D(\nu_\theta^a Z_\theta)\right).$$

It remains to observe that the event

$$\{f_1(\nu_\theta^a Z_\theta)\geq\cdots\geq f_D(\nu_\theta^a Z_\theta)\}\setminus\{f_1(\nu_\theta^a Z_\theta)>\cdots>f_D(\nu_\theta^a Z_\theta)\}$$

is included in

$$\bigcup_{j=1}^{D-1}\{f_j(\nu_\theta^a Z_\theta)=f_{j+1}(\nu_\theta^a Z_\theta)\}$$

which has probability zero, so that

$$\mathbb{P}\left(f_1(\nu_\theta^a Z_\theta)\geq\cdots\geq f_D(\nu_\theta^a Z_\theta)\right)=\mathbb{P}\left(f_1(\nu_\theta^a Z_\theta)>\cdots>f_D(\nu_\theta^a Z_\theta)\right).$$

□

Proposition 1.51 and Theorem 1.57 yield the following general result.

Theorem 1.58. *Let $\theta_1,\dots,\theta_r$ be real numbers. For any $f_1,\dots,f_D\in\mathbb{C}(X_1,\dots,X_r)$ real-valued and without pole on $\mathbb{T}^r$,*

$$\lim_{X\to+\infty}\frac{1}{X}\#\left\{n\leq X\mid F_1(n)>\cdots>F_D(n)\right\}$$

exists.

We note that this does not prove that every prime number race over a function field is weakly inclusive (as defined in Definition 1.47) because the normalized prime counting functions in this context have an extra $o(1)$ term (see Section 1.4.2.2). We will deal with such functions in Section 1.4.1.5.

1.4.1.3 The continuous case

We now tackle the continuous case of the Kronecker-Weyl theorem.

Let $\theta_1,\dots,\theta_r$ be real numbers. Extract a basis $\{\theta_1,\dots,\theta_m\}$ of $\mathrm{Span}_{\mathbb{Q}}(\theta_1,\dots,\theta_r)$, and write

$$\theta_j=\sum_{k=1}^{m}b_{k,j}\theta_k\text{ for }m+1\leq j\leq r$$

with $b_{k,j}\in\mathbb{Q}$. Let d be the least common multiple of the denominators of each $b_{k,j}$ so that $h_{k,j}:=db_{k,j}\in\mathbb{Z}$.

The proof of the following theorem is similar to the proof of Theorem 1.52. We simply mention the necessary changes : discrete sums up to X are replaced by integrals between 0 and X, the splitting according to congruence classes modulo d is replaced by the change of variable $y\longrightarrow dy$ and we appeal to the continuous version of the Kronecker-Weyl theorem (see [Dev19, Theorem 4.2] or the remark at the end of the appendix). We note that most results in this section are made easier than in the previous section because linear dependence with π doesn't have any effect on the continuous densities being studied.

Theorem 1.59. *The one-parameter subgroup*

$$\Gamma_\theta = \left\{ \left(e^{i\theta_1 y}, \dots, e^{i\theta_r y} \right) \mid y \in \mathbb{R} \right\}$$

is equidistributed in

$$H_\theta = \left\{ \left(z_1^d, \dots, z_m^d, \dots, \prod_{k=1}^m z_k^{h_{k,j}}, \dots \right) \mid (z_1, \dots, z_m) \in \mathbb{T}^m \right\},$$

that is for every continuous $f : \mathbb{T}^r \longrightarrow \mathbb{C}$ one has

$$\frac{1}{X} \int_0^X f\left(e^{i\theta_1 y}, \dots, e^{i\theta_r y} \right) \mathrm{d}y \underset{X \to +\infty}{\longrightarrow} \int_{H_\theta} f \, \mathrm{d}\mu_{H_\theta}$$

where μ_{H_θ} is the normalized Haar measure on H_θ.

Interpreting the Haar measure μ_{H_θ} as the distribution of a random vector Z_θ defined as in Definition 2.57 we obtain the following.

Corollary 1.60. *For any continuous $f : \mathbb{T}^r \to \mathbb{C}$, we have*

$$\frac{1}{X} \int_0^X f\left(e^{i\theta_1 y}, \dots, e^{i\theta_r y} \right) \mathrm{d}y \underset{X \to +\infty}{\longrightarrow} \mathbb{E}\left(f\left(Z_\theta \right) \right)$$

where Z_θ is defined as in Definition 2.57.

Note that the analog of Lemma 1.56 holds with the only hypothesis that $f\left(e^{i\theta_1 y}, \dots, e^{i\theta_r y} \right) \neq 0$ for at least one $y \in \mathbb{R}$.

Lemma 1.61. *Let $f \in \mathbb{C}(X_1, \dots, X_r)$ with no pole in $\mathbb{T}^r$. Then one has $\mathbb{P}(f(Z_\theta) = 0) = 0$ if and only if there exists $y \in \mathbb{R}$ such that $f\left(e^{i\theta_1 y}, \dots, e^{i\theta_r y} \right) \neq 0$.*

The proof of the continuous analog of Theorem 1.57 then goes similarly.

Theorem 1.62. *Let $f_1, \dots, f_D \in \mathbb{C}(X_1, \dots, X_r)$ be real-valued and without poles on $\mathbb{T}^r$ and let $F_j : t \mapsto f_j\left(e^{i\theta_1 t}, \dots, e^{i\theta_r t} \right)$. Then we have*

$$\frac{1}{X} \int_0^X \mathbf{1}_{x_1 > \dots > x_D}\left(F_1(y), \dots, F_D(y) \right) \mathrm{d}y \underset{X \to +\infty}{\longrightarrow} \mathbb{P}\left(f_1(Z_\theta) > \dots > f_D(Z_\theta) \right).$$

1.4.1.4 An infinite-dimensional version

The goal of this section is to prove a result analogous to Theorem 1.62 but with converging series in an infinite number of $e^{i\theta_n t}$, as a natural generalization of the above Laurent polynomials. This is the kind of functions we have to deal with in the context of prime number races over number fields, because the associated L-functions have an infinite number of non-trivial zeros. Those functions are often called *almost-periodic functions*.

Definition 1.63. *The B^1 semi-norm of a locally integrable function f is*

$$||f||_{B^1} := \limsup_{X\to+\infty} \frac{1}{X}\int_0^X |f(y)|\,\mathrm{d}y.$$

A function $F : \mathbb{R}^+ \longrightarrow \mathbb{R}$ is said to be B^1 almost-periodic if there exists a sequence $(P_N)_{N\geq 1}$ of trigonometric polynomials of the form

$$P_N : t \mapsto \sum_{n=1}^{D_N} r_{n,N} e^{i\lambda_{n,N}t}$$

for some integer $D_N \geq 1$, $r_{n,N} \in \mathbb{C}$ and $\lambda_{n,N} \in \mathbb{R}$, such that

$$||F - P_N||_{B^1} \underset{N\to+\infty}{\longrightarrow} 0.$$

It turns out that prime counting functions over number fields are B^2-almost periodic, after applying the change of variable $x \to e^x$ (see [Ng00, Lemma 5.1.3] or [Dev19, Proposition 4.4] for a general statement), where B^2 semi-norm is defined by $||f||_{B^2} = \left(||f^2||_{B^1}\right)^{1/2}$. The Cauchy-Schwarz inequality easily implies that such functions are in particular B^1-almost periodic.

We simply quote the following important fact about B^1 almost-periodic functions ([Bes55, p.104]).

Proposition 1.64. *Let $F : \mathbb{R}^+ \longrightarrow \mathbb{R}$ be B^1 almost-periodic. There exists a countable set $\Lambda(F) = \{\lambda_n \mid n \geq 1\} \subset \mathbb{R}$ called the support of F, such that for every $n \geq 1$,*

$$a_n := \lim_{X\to+\infty} \frac{1}{X}\int_0^X f(y)e^{-i\lambda_n y}\,\mathrm{d}y \neq 0.$$

Moreover we have $||F - P_N||_{B^1} \underset{N\to+\infty}{\longrightarrow} 0$, where $P_N(F) : t \mapsto \sum_{n=1}^N a_n e^{-i\lambda_n t} + \overline{a_n} e^{-i\lambda_n t}$.

The upshot of the above Proposition is that there exists a canonical way to approximate a given B^1 almost-periodic function by trigonometric polynomials with respect to the B^1 semi-norm.

We begin by proving that B^1-almost periodic functions admit limiting distributions. The argument is essentially the one given in the proof of [ANS14, Theorem 2.9]. We note that the left-hand side of formula (2.10) in *loc. cit.* should be replaced by $\limsup_{Y\to+\infty} \frac{1}{Y}\int_0^Y |\phi(y) - P_N(y)|\,\mathrm{d}y$, and that Y should be assumed large enough in the last inequality in the proof of [ANS14, Theorem 2.9].

Theorem 1.65. *Let $F : \mathbb{R}^+ \longrightarrow \mathbb{R}$ be a B^1 almost-periodic function. There exists a random variable S such that for any continuous bounded function g on $\mathbb{R}$ we have*

$$\frac{1}{X}\int_0^X g(F(y))\,\mathrm{d}y \underset{X\to+\infty}{\longrightarrow} \mathbb{E}(g(S)).$$

In other words, F admits $\mathbb{P}_S$, the distribution of S, as a limiting distribution.

Proof. The goal is to apply Corollary 1.60 to each $P_N(F)$ before passing to the limit in N. Let g be a bounded Lipschitz function on $\mathbb{R}$, with Lipschitz constant c_g. Then for any $N \geq 1$,

$$\frac{1}{X}\int_0^X g(F(y))\,\mathrm{d}y = \frac{1}{X}\int_0^X g(P_N(y))\,\mathrm{d}y + \frac{1}{X}\int_0^X \left(g(F(y)) - g(P_N(y))\right)\,\mathrm{d}y.$$

By the triangular inequality one has

$$\left|\frac{1}{X}\int_0^X \left(g(F(y)) - g(P_N(y))\right)\,\mathrm{d}y\right| \leq \frac{c_g}{X}\int_0^X |F(y) - P_N(y)|\,\mathrm{d}y$$

so that $\limsup_{X\to+\infty}\left|\frac{1}{X}\int_0^X \left(g(F(y)) - g(P_N(y))\right)\,\mathrm{d}y\right| \underset{N\to+\infty}{\longrightarrow} 0$. On the other hand, Corollary 1.60 yields

$$\frac{1}{X}\int_0^X g(P_N(y))\,\mathrm{d}y \underset{X\to+\infty}{\longrightarrow} \mathbb{E}(g(S_N))$$

for some random variable S_N built from the linear relations over $\mathbb{Q}$ between the real numbers $\lambda_{1,N},\dots,\lambda_{D_N,N}$.

This proves that

$$\limsup_{X\to+\infty}\frac{1}{X}\int_0^X g(F(y))\,\mathrm{d}y = \mathbb{E}(g(S_N)) + o(1)$$

as N tends to infinity, and similarly we have

$$\liminf_{X\to+\infty}\frac{1}{X}\int_0^X g(F(y))\,\mathrm{d}y = \mathbb{E}(g(S_N)) + o(1)$$

as N tends to infinity. Therefore

$$\limsup_{X\to+\infty}\frac{1}{X}\int_0^X g(F(y)) - \liminf_{X\to+\infty}\frac{1}{X}\int_0^X g(F(y)) = 0$$

since it is independent of N and $o(1)$ with respect to N. We have thus shown that $\frac{1}{X}\int_0^X g(F(y))\,\mathrm{d}y$ admits a limit as X tends to infinity, and $\mathbb{E}(g(S_N))$ converges to this (same) limit as N tends to infinity.

We now prove that the sequence $(S_N)_{N\geq 1}$ converges in distribution to some random variable Z. To do so, we apply Prohorov's theorem [Bil99, Theorem 5.1] (or Helly's selection theorem as it is called in [ANS14, Lemma 2.8]), which in particular states that a tight sequence of probability measures on $\mathbb{R}$ admits a weakly converging subsequence. Recall that a family $(\mu_n)_{n\geq 1}$ of probability measures on $\mathbb{R}$ is tight when there is no "escape of mass to infinity" along the family, *i.e.* for every $\varepsilon > 0$, one can find a compact $K \subset \mathbb{R}$ such that $\mu_n(K) \geq 1-\varepsilon$ for every $n \geq 1$. Assuming that $(\mathbb{P}_{S_N})_{N\geq 1}$ is tight, and denoting by μ the weak limit of one of its subsequence, $(\mathbb{E}(g(S_N)))_{N\geq 1}$ can only converge to $\int_{\mathbb{R}} g\,\mathrm{d}\mu$ when g is a bounded continuous function on $\mathbb{R}$. Since this holds for every bounded Lipschitz function on $\mathbb{R}$ by the above computations, the Portmanteau theorem [Bil99, Theorem 2.1] implies that $(\mathbb{P}_{S_N})_{n\geq 1}$ converges weakly to μ. Finally, the limit probability measure μ is the distribution of $S := F^{-1}(U)$, where F is the distribution function of μ, F^{-1} its generalized inverse and U

is uniform on $[0,1]$ (see [Dev86, Theorem 2.1]), so that $(S_N)_{N\geq 1}$ converges in distribution to S.

It only remains to prove that $(\mathbb{P}_{S_N})_{N\geq 1}$ is tight. Let $\varepsilon > 0$ and $A > 0$. As a straightforward application of Theorem 1.62, we obtain

$$\mathbb{P}(|S_N| > A) = \lim_{X\to+\infty} \frac{1}{X}\int_0^X \mathbf{1}_{x>A}(|P_N(y)|)\,\mathrm{d}y.$$

By Markov's inequality, we have for every $N \geq 1$ and $X > 0$,

$$\frac{1}{X}\int_0^X \mathbf{1}_{x>A}(|P_N(y)|)\,\mathrm{d}y \leq \frac{1}{AX}\int_0^X |P_N(y)|\,\mathrm{d}y.$$

For every $N \geq 1$ and $y \in \mathbb{R}^+$, one has $|P_N(y)| \leq |F(y)| + |F(y) - P_N(y)|$. Now $L := \limsup_{X\to+\infty} \frac{1}{X}\int_0^X |F(y)|\,\mathrm{d}y < +\infty$ since $\limsup_{X\to+\infty} \frac{1}{X}\int_0^X |F(y) - P_n(y)|\,\mathrm{d}y < +\infty$ for at least one n, and $\limsup_{X\to+\infty} \frac{1}{X}\int_0^X |P_n(y)|\,\mathrm{d}y < +\infty$ by Corollary 1.60. Finally we obtain

$$\mathbb{P}(|S_N| > A) \leq \frac{1}{A}\limsup_{X\to+\infty} \frac{1}{X}\int_0^X |F(y) - P_N(y)|\,\mathrm{d}y + \frac{L}{A} \ll \frac{1}{A}$$

and this can be made smaller than ε by choosing A large enough, independently of N. □

Remark 1.66. The proof goes similarly for vector-valued B^1 almost-periodic functions, as in [ANS14, Theorem 2.9].

The key argument in the above proof was Prohorov's theorem, or Helly's selection theorem, but this is an indirect argument. Our goal is now to give a more explicit description of the random variable S in terms of the function F. We can do so thanks to our explicit version of the Kronecker-Weyl theorem. Also, moment estimates such as Chebyshev's inequality can prove very useful to obtain bounds on $\lim_{X\to+\infty} \frac{1}{X}\int_0^X \mathbf{1}_{x>0}(F(y))\,\mathrm{d}y$ (when it exists, see Corollary 1.79 below), so we would like to have at least the first two moments of S at our disposal. This is possible at the cost of assuming additional hypotheses on the coefficients a_n of the function F, and on the linear relations between the almost-periods of F, *i.e.* the elements of the support $\Lambda(F)$ of F. We give below two distinct hypotheses that allow us to compute the second moment.

Let $\theta = (\theta_n)_{n\geq 1}$ be a sequence of pairwise distinct positive real numbers and for any $N \geq 1$ let $\Theta_N = \{\theta_n \mid n \leq N\}$ and $\Theta = \bigcup_{N\geq 1} \Theta_N$. We are going to do an analysis close to what we did in the previous sections, but we alter our notations to take into account the infinite number of θ_n's. Define inductively $\mathcal{B}_1 := \{\theta_1\}$ and for $N \geq 2$,

$$\mathcal{B}_N := \begin{cases} \mathcal{B}_{N-1} \text{ if } \theta_N \in \mathrm{Span}_{\mathbb{Q}}(\Theta_{N-1}) \\ \mathcal{B}_{N-1} \cup \{\theta_N\} \text{ otherwise.} \end{cases}$$

We let $\mathcal{B} := \bigcup_{N\geq 1} \mathcal{B}_N$, so that $\mathcal{B}$ is a basis of $\mathrm{Span}_{\mathbb{Q}}\,\Theta$. For any $j \geq 1$, write the decomposition of θ_j in $\mathcal{B}$ as

$$\theta_j = \sum_{\theta\in\mathcal{B}} c_{\theta,j}\theta$$

and let d_j be the least common multiple of the denominators of the $c_{\theta,k}$ (written in irreducible form), for $\theta \in \mathcal{B}_j$ and $k \leq j$. Since the sequence of sets $(\mathcal{B}_j)_{j\geq 1}$ is increasing, we see that d_j really only depends on j.

Definition 1.67. *Let $(Z_\theta)_{\theta\in\mathcal{B}}$ be a sequence of independent random variables, uniform on $\mathbb{T}$. For any $N \geq 1$ and $n \leq N$, let*

$$Z_{n,N} = \prod_{\theta\in\mathcal{B}} Z_\theta^{d_N c_{\theta,n}}.$$

Notice that, by definition, $d_N c_{n,\theta} \in \mathbb{Z}$ for $n \leq N$, and that for every $n \geq 1$, $c_{\theta,n} = 0$ for all but finitely many $\theta \in \mathcal{B}$, so the above product is a finite product.

Lemma 1.68. *Let $c \in \mathbb{C}$, $(a_n)_{n\geq 1} \in \ell^2(\mathbb{C})$ and for every $N \geq 1$,*

$$S_{\Theta_N} := c + \sum_{n\leq N} a_n Z_{n,N} + \overline{a_n}\overline{Z_{n,N}}.$$

Assume that no θ_n is an integer multiple of another, that is for every $i, j \geq 1$ with $i \neq j$, we have $\theta_i \notin \theta_j\mathbb{Z}$. Then $(S_{\Theta_N})_{N\geq 1}$ converges in L^2.

Proof. Since L^2 is complete, it is enough to prove that $(S_{\Theta_N})_{N\geq 1}$ is Cauchy in L^2. Let $m > n \geq 1$, then

$$\mathbb{E}(|S_{\Theta_m} - S_{\Theta_n}|^2) = \mathbb{E}\left(\left|\sum_{k=1}^{m}(a_k Z_{k,m} + \overline{a_k}\overline{Z_{k,m}}) - \sum_{k=1}^{n}(a_k Z_{k,n} + \overline{a_k}\overline{Z_{k,n}})\right|^2\right).$$

Expanding the square, we end up with terms of twelve different kinds : $a_k a_j \mathbb{E}(Z_{k,p}Z_{j,p})$, $a_k\overline{a_j}\mathbb{E}(Z_{k,p}\overline{Z_{j,p}})$ for $p \in \{m, n\}$ and $1 \leq j, k \leq p$, $-a_k a_j \mathbb{E}(Z_{k,m}Z_{j,n}), -a_k\overline{a_j}\mathbb{E}(Z_{k,m}\overline{Z_{j,n}})$ for $1 \leq k \leq m, 1 \leq j \leq n$ and their conjugates. Each $Z_{k,p}$ is uniform on $\mathbb{T}$ and the product of two uniform random variables on $\mathbb{T}$ is either 1 or uniform on $\mathbb{T}$, in which case it has mean zero. Thus, it is enough to detect in which of the above cases we end up with 1.

- For $p \in \{m, n\}$ and $1 \leq j, k \leq p$ we have

  $$Z_{k,p}Z_{j,p} = \prod_{\theta\in\mathcal{B}} Z_\theta^{d_p(c_{\theta,k}+c_{\theta,j})}.$$

  Since the $Z_\theta, \theta \in \mathcal{B}$ are independent, this product is (almost-surely) 1 if and only if $d_p(c_{\theta,k} + c_{\theta,j}) = 0$ for every $\theta \in \mathcal{B}$. By definition, this means that $\theta_j = -\theta_k$ which can't be because each θ_n is positive. So those terms contribute 0.
- Similarly, we have

  $$Z_{k,p}\overline{Z_{j,p}} = \prod_{\theta\in\mathcal{B}} Z_\theta^{d_p(c_{\theta,k}-c_{\theta,j})}.$$

  This is equal to 1 when $j = k$, but when $j \neq k$ there is at least one non-zero exponent since the θ_n's are pairwise distinct.
- Now for $1 \leq k \leq m, 1 \leq j \leq n$,

  $$Z_{k,m}Z_{j,n} = \prod_{\theta\in\mathcal{B}} Z_\theta^{d_m c_{\theta,k}+d_n c_{\theta,j}}.$$

  As before, this is 1 if and only if $\theta_k = -\frac{d_n}{d_m}\theta_j$, which can't be since the θ_n's are positive.

- Finally for $1 \leq k \leq m, 1 \leq j \leq n$,

$$Z_{k,m}\overline{Z_{j,n}} = \prod_{\theta \in \mathcal{B}} Z_\theta^{d_m c_{\theta,k} - d_n c_{\theta,j}},$$

and this is 1 if and only if $\theta_j = \frac{d_m}{d_n}\theta_k$. But by definition, d_n divides d_m for $m > n$, so by hypothesis on the θ_n's the previous equality can only happen if and only if $k = j$.

Gathering everything, we have

$$\mathbb{E}(|S_{\Theta_m} - S_{\Theta_n}|^2) = 2\sum_{k=1}^{m} |a_k|^2 + 2\sum_{k=1}^{n} |a_k|^2 - 4\sum_{k=1}^{n} |a_k|^2 = 2\sum_{k=n+1}^{m} |a_k|^2.$$

Since $(a_n)_{n\geq 1} \in \ell^2(\mathbb{C})$, this proves that $(S_{\Theta_N})_{N\geq 1}$ is Cauchy for the L^2 norm. □

If the sequence $(d_j)_{j\geq 1}$ is bounded, it is stationary since it is non-decreasing. In that case, we let d be its limit and $N_0 \geq 1$ be such that $d_N = d$ for every $N \geq N_0$. Then $Z_{n,N} = Z_{n,N_0}$ for any $N \geq \max(N_0, n)$, so for any $n \geq 1$ we let $Z_n := Z_{n,N_0}$. With these notations, we can now state the following result.

Lemma 1.69. *Let $c \in \mathbb{C}$, $(a_n)_{n\geq 1} \in \ell^2(\mathbb{C})$ and for every $N \geq 1$,*

$$S_{\Theta_N} := c + \sum_{n \leq N} a_n Z_{n,N} + \overline{a_n}\overline{Z_{n,N}}.$$

Assume that $(d_j)_{j\geq 1}$ is bounded. Then $(S_{\Theta_N})_{N\geq 1}$ converges in L^2.

Proof. The proof is made easier in this case by the fact that $S_{\Theta_m} - S_{\Theta_n} = \sum_{k=n+1}^{m}(a_k Z_k + \overline{a_k}\overline{Z_k})$, and those are easily seen to be pairwise orthogonal. We conclude exactly as in the previous proof. □

Corollary 1.70. *Let $F \sim c + \sum_{n\geq 1} a_n e^{i\theta_n t} + \overline{a_n} e^{-i\theta_n t}$ be B^1 almost-periodic (see Theorem 1.65), where $c \in \mathbb{C}$ and $(a_n)_{n\geq 1} \in \ell^2(\mathbb{C})$. Assume either that no θ_i is an integer multiple of another or that $(d_j)_{j\geq 1}$ is bounded. Then we can choose $S_\Theta := \lim_{N\to+\infty} c + \sum_{n\leq N} a_n Z_{n,N} + \overline{a_n}\overline{Z_{n,N}}$ (the limit being taken in L^2 norm) in the conclusion of Theorem 1.65, i.e. for every bounded continuous function g on $\mathbb{R}$, one has*

$$\frac{1}{X}\int_0^X g(F(y))\,\mathrm{d}y \underset{X\to+\infty}{\longrightarrow} \mathbb{E}(g(S_\Theta)).$$

Moreover, we have $\mathbb{E}(S_\Theta) = c$ and $\mathrm{Var}(S_\Theta) = 2\sum_{n\geq 1} |a_n|^2$.

Remark 1.71. The above notation $\sim$ does not necessarily mean that the series for F converges pointwise to F. It only means that its partial sums converge to F for the B^1 semi-norm.

Proof. The first part is an immediate consequence of Theorem 1.65 and the previous two lemmas. The last two formulas are straightforward. □

Remarks 1.72.

i) It is tempting to say that $(S_{\Theta_N})_{N\geq 1}$ converges to S_Θ in L^1 under no other hypothesis than F being B^1 almost-periodic, since $\limsup_{X\to+\infty}\frac{1}{X}\int_0^X |F(y)-P_N(y)|\,\mathrm{d}y$ goes to zero as N tends to infinity. However we don't know if the previous quantity equals $\mathbb{E}(|S_\Theta - S_{\Theta_N}|)$.

ii) If the θ_n's are linearly independent over $\mathbb{Q}$, so that $\mathcal{B}=\Theta$, then the Z_n's are pairwise independent, and one can prove the almost-sure convergence of $(S_{\Theta_N})_{N\geq 1}$ by Kolmogorov's two series theorem for example (see [Dur19, Theorem 2.5.6]). The almost-sure convergence does not immediatly follow from the assumption that the series for $F(t)$ converges for every $t\in\mathbb{R}$: the set $\Gamma := \left\{\left(e^{i\theta t}\right)_{\theta\in\mathcal{B}} \mid t\in\mathbb{R}\right\}$ is easily seen to be dense in $\mathbb{T}^{\mathcal{B}}$ as a consequence of the continuous version of the Kronecker-Weyl theorem, but it has measure zero. By the Riesz-Fischer theorem, we at least know that $(S_{\Theta_N})_{N\geq 1}$ admits an almost-surely converging subsequence.

The next step in our analysis is to pass from bounded Lipschitz functions to indicator functions of sets defined by strict inequalities. Mimicking the proof of Theorem 1.57, we obtain the following.

Proposition 1.73. *Let $F_1,\dots,F_D:\mathbb{R}^+\longrightarrow\mathbb{R}$ be B^1 almost-periodic functions with $\Lambda(F_j)\subset\Theta$ for $1\leq j\leq D$. Let $S_1,\dots,S_D$ be the random variables associated to $F_1,\dots,F_D$ in Theorem 1.65. Then*

$$\begin{aligned}\mathbb{P}(S_1>\cdots>S_D) &\leq \liminf_{X\to+\infty}\frac{1}{X}\int_0^X \mathbf{1}_{x_1>\cdots>x_D}(F_1(y),\dots,F_D(y))\,\mathrm{d}y\\ &\leq \limsup_{X\to+\infty}\frac{1}{X}\int_0^X \mathbf{1}_{x_1>\cdots>x_D}(F_1(y),\dots,F_D(y))\,\mathrm{d}y \leq \mathbb{P}(S_1\geq\cdots\geq S_D).\end{aligned}$$

Remark 1.74. We cannot expect an equality without any hypothesis on Θ. For instance, consider the case $D=2$, $F_2=0$ and F_1 a non-zero continuous function with compact support on $\mathbb{R}$. For a less trivial example, we can use an everywhere converging Fourier series with a locally constant sum.

We now look for conditions on Θ to imply equality in the previous Proposition. Such a condition was found by Devin in [Dev20] : if $\mathrm{Span}_{\mathbb{Q}}\,\Theta$ decomposes as a direct sum $\mathrm{Span}_{\mathbb{Q}}\,T\oplus\mathrm{Span}_{\mathbb{Q}}(\Theta\setminus T)$, where T is a finite subset of Θ, then the random variable associated to a non-constant B^1 almost-periodic function S as in Theorem 1.65 does not admit atoms. Note that this hypothesis on $\mathrm{Span}_{\mathbb{Q}}\,\Theta$ is a weakening of the hypothesis of the existence of "self-sufficient zeros" in [MN20]. The proof of Devin consists in showing that the characteristic function of S is decaying sufficiently fast at infinity, by using known bounds on oscillatory integrals, and then using a lemma of Wiener, relating this decay to the continuity of the distribution of S (see the proof of Theorem 1.2 and Corollary 1.4 in [Dev20]). Our method allows us to show the same thing but with a considerably simpler proof thanks to Lemma 1.61.

Theorem 1.75 (Devin)**.** *Assume* $\mathrm{Span}_{\mathbb{Q}}(\Theta)=\mathrm{Span}_{\mathbb{Q}}(\theta_1,\dots,\theta_m)\oplus\mathrm{Span}_{\mathbb{Q}}(\{\theta_n\mid n>m\})$. *Let $F:\mathbb{R}^+\longrightarrow\mathbb{R}$ be such that $||F-P_N||_{B^1}\underset{N\to+\infty}{\longrightarrow}0$ where*

$$P_N : t\mapsto c+\sum_{n\leq N} a_n e^{i\theta_n t}+\overline{a_n}e^{-i\theta_n t}.$$

Let μ_F, μ_{F-P_m} and μ_{P_m} be the limiting distributions of $F, F-P_m$ and P_m respectively. Then $\mu_F = \mu_{F-P_m} * \mu_{P_m}$. In particular, if P_m is not constant, then $\mu_F(\{x\}) = 0$ for any $x \in \mathbb{R}$.

Proof. The function F and $R = F - P_m$ are B^1-almost periodic functions, and therefore admit limiting distributions μ_F and μ_R by Theorem 1.65. On the other hand, P_m also admits a limiting distribution because of Theorem 1.59, say μ_{P_m}.

For $N > m$, let $P'_N : t \mapsto \sum_{m<n\leq N} a_n e^{i\theta_n t} + \overline{a_n} e^{-i\theta_n t}$. Just as P_m, those admit limiting distributions $\mu_{P'_N}$ and by the proof of Theorem 1.65, $\left(\mu_{P'_N}\right)_{N>m}$ converges weakly to μ_R. Also, for every $N > m$, $\mu_{P'_N+P_m} = \mu_{P'_N} * \mu_{P_m}$ because, by construction and the hypothesis on $\mathrm{Span}_{\mathbb{Q}} \Theta$, every $Z_{n,N}, 1 \leq n \leq m$ is independent of every $Z_{n',N}, m < n' \leq N$. As above, $\left(\mu_{P'_N+P_m}\right)_{N>m}$ converges weakly to μ_F.

For any Borel probability measure on $\mathbb{R}$, let $\hat{\mu}$ be its characteristic function. Then for every $N > m$, $\widehat{\mu_{P'_N} * \mu_{P_m}} = \hat{\mu}_{P'_N} \hat{\mu}_{P_m}$ and this converges pointwise to $\hat{\mu}_R \hat{\mu}_{P_m} = \widehat{\mu_R * \mu_{P_m}}$. By Lévy's continuity theorem ([Dur19, Theorem 3.3.17]), this means that $(\mu_{P'_N} * \mu_{P_m})_{N>m}$ converges weakly to $\mu_R * \mu_{P_m}$. Therefore we have proved that $\mu_F = \mu_R * \mu_{P_m}$.

Now if P_m is not constant, then by Lemma 1.61, we have $\mu_{P_m}(\{y\}) = 0$ for every $y \in \mathbb{R}$, and thus for any $x \in \mathbb{R}$,

$$\mu_F(\{x\}) = (\mu_R * \mu_{P_m})(\{x\}) = \int_{\mathbb{R}} \mu_{P_m}(\{x-y\}) \, \mathrm{d}\mu_R(y) = 0.$$

□

Combining the previous Theorem with Proposition 1.73 we obtain the following.

Corollary 1.76. *Assume $\mathrm{Span}_{\mathbb{Q}} \Theta = \mathrm{Span}_{\mathbb{Q}} T \oplus \mathrm{Span}_{\mathbb{Q}}(\Theta \setminus T)$ for some non-empty finite subset T of Θ. Let $F_1, \dots, F_D : \mathbb{R}^+ \longrightarrow \mathbb{R}$ be B^1 almost-periodic functions such that for $1 \leq j \leq D, F_j \sim c_j + \sum_{\theta\in\Theta} a_{\theta,j} e^{i\theta t} + \overline{a_{\theta,j}} e^{-i\theta t}$. Let $S_1, \dots, S_D$ be the random variables associated to $F_1, \dots, F_D$ in Theorem 1.65. If for every $1 \leq j \leq D-1$, the function $t \mapsto \sum_{\theta\in T}(a_{\theta,j} - a_{\theta,j+1}) e^{i\theta y} + (\overline{a_{\theta,j}} - \overline{a_{\theta,j+1}}) e^{-i\theta y}$ is not constant, then*

$$\lim_{X\to+\infty} \frac{1}{X} \int_0^X \mathbf{1}_{x_1>\cdots>x_D}(F_1(y), \dots, F_D(y)) \, \mathrm{d}y = \mathbb{P}(S_1 > \cdots > S_D).$$

The condition that a certain linear combination of $e^{i\theta t}$ is not constant can be easily translated by the non-vanishing of its coefficients.

Lemma 1.77. *Let T be a finite subset of Θ and for each $\theta \in T$, let $a_\theta \in \mathbb{C}$. If the function $t \mapsto \sum_{\theta\in T} a_\theta e^{i\theta t} + \overline{a_\theta} e^{-i\theta t}$ is constant then $a_\theta = 0$ for every $\theta \in T$.*

Proof. Let $P : t \mapsto \sum_{\theta\in T} a_\theta e^{i\theta t} + \overline{a_\theta} e^{-i\theta t}$ and assume it is constant. Then all of its derivatives are zero. In particular, we have for $1 \leq k \leq 2\#T$,

$$P^{(k)}(0) = \sum_{\theta\in T} (a_\theta + (-1)^k \overline{a_\theta}) \theta^k = 0,$$

which means that $(a_\theta + \overline{a_\theta})_{\theta\in T}$ and $(a_\theta - \overline{a_\theta})_{\theta\in T}$ are both solutions of Vandermonde linear systems with non-zero determinant since the elements of Θ, and therefore of T, are non-zero

and pairwise distinct. This implies $a_\theta = \overline{a_\theta}$ and $a_\theta = -\overline{a_\theta}$ for every $\theta \in T$, and thus $a_\theta = 0$ for every $\theta \in T$. □

Remark 1.78. This lemma can also be seen as an application of Artin's lemma on the linear independence of characters (see [Lan02, VI, Theorem 4.1]).

Corollary 1.79. *Assume* $\mathrm{Span}_{\mathbb{Q}} \Theta = \mathrm{Span}_{\mathbb{Q}} T \oplus \mathrm{Span}_{\mathbb{Q}}(\Theta \setminus T)$ *for some non-empty finite subset* T *of* Θ. *Let* $F_1, \dots, F_D : \mathbb{R}^+ \longrightarrow \mathbb{R}$ *be* B^1 *almost-periodic functions such that for* $1 \leq j \leq D, F_j \sim c_j + \sum_{\theta \in \Theta} a_{\theta,j} e^{i\theta t} + \overline{a_{\theta,j}} e^{-i\theta t}$. *Let* $S_1, \dots, S_D$ *be the random variables associated to* $F_1, \dots, F_D$ *in Theorem 1.65. If for every* $1 \leq j \leq D-1$, *there exists* $\theta \in T$ *such that* $a_{\theta,j} \neq a_{\theta,j+1}$ *then*

$$\lim_{X \to +\infty} \frac{1}{X} \int_0^X \mathbf{1}_{x_1 > \dots > x_D}(F_1(y), \dots, F_D(y)) \, \mathrm{d}y = \mathbb{P}(S_1 > \dots > S_D).$$

Proof. Simply combine the previous two results. □

1.4.1.5 Quantities with an error term

We now investigate to what extent Corollary 1.51, Theorem 1.57, Theorem 1.62 and Corollary 1.79 still hold for functions with an extra error term. To simplify notations, when $G_1, \dots, G_D$ are functions and $\mathcal{R}$ is a D-ary relation ($\mathcal{R}$ will be $\{(x_1, \dots, x_D) \in \mathbb{R}^D \mid x_1 > \dots > x_D\}$ or $\{(x_1, \dots, x_D) \in \mathbb{R}^D \mid x_1 \geq \dots \geq x_D\}$ below), we set

$$\underline{\delta}(\mathcal{R}(G_1, \dots, G_D)) := \liminf_{X \to +\infty} \frac{1}{X} \#\{n \in \{1, \dots, X\} \mid \mathcal{R}(G_1(n), \dots, G_D(n))\}$$

and

$$\overline{\delta}(\mathcal{R}(G_1, \dots, G_D)) := \limsup_{X \to +\infty} \frac{1}{X} \#\{n \in \{1, \dots, X\} \mid \mathcal{R}(G_1(n), \dots, G_D(n))\}$$

When $\underline{\delta}(\mathcal{R}(G_1, \dots, G_D)) = \overline{\delta}(\mathcal{R}(G_1, \dots, G_D))$ we denote by $\delta(\mathcal{R}(G_1, \dots, G_D))$ their common value.

Theorem 1.80. *Let* $\theta_1, \dots, \theta_r$ *be real numbers and* $f_1, \dots, f_D \in \mathbb{C}(X_1, \dots, X_r)$ *be real-valued and without pole on* $\mathbb{T}^r$. *Let* $G : t \mapsto (F_1(t), \dots, F_D(t)) + r(t)$ *where* $F_j(t) = f_j\left(e^{i\theta_1 t}, \dots, e^{i\theta_r t}\right)$ *for* $1 \leq j \leq D$, *and* $r(t) = (r_1(t), \dots, r_D(t)) = o(1)$ *as* $t \to +\infty$.

i) Degenerate case : Assume that $\theta_i \in \pi\mathbb{Q}$ *for* $1 \leq i \leq r$. *Then*

$$\begin{aligned} \mathbb{P}(f_1(Z_\theta) > \dots > f_D(Z_\theta)) &\leq \underline{\delta}(G_1 > \dots > G_D) \\ &\leq \overline{\delta}(G_1 > \dots > G_D) \leq \mathbb{P}(f_1(Z_\theta) \geq \dots \geq f_D(Z_\theta)). \end{aligned}$$

In particular, if for every $1 \leq j \leq D-1$ *and every* $n \in \mathbb{Z}$ *one has* $F_j(n) \neq F_{j+1}(n)$, *then* $\delta(G_1 > \dots > G_D)$ *exists and we have*

$$\delta(G_1 > \dots > G_D) = \mathbb{P}(f_1(Z_\theta) > \dots > f_D(Z_\theta)).$$

ii) Non-degenerate case : Assume $\theta_i \notin \pi\mathbb{Q}$ for at least one $i \in \{1, \dots, r\}$. Then

$$\frac{1}{d}\sum_{a=0}^{d-1} \mathbb{P}(f_1(\nu_\theta^a Z_\theta) > \cdots > f_D(\nu_\theta^a Z_\theta)) \le \underline{\delta}(G_1 > \cdots > G_D)$$
$$\le \overline{\delta}(G_1 > \cdots > G_D) \le \frac{1}{d}\sum_{a=0}^{d-1} \mathbb{P}(f_1(\nu_\theta^a Z_\theta) \ge \cdots \ge f_D(\nu_\theta^a Z_\theta)).$$

Moreover, if for every $1 \le j \le D-1$ and $0 \le a \le d-1$, there exists $n \equiv a \bmod d$ such that $F_j(n) \ne F_{j+1}(n)$, then $\delta(G_1 > \cdots > G_D)$ exists and

$$\delta(G_1 > \cdots > G_D) = \frac{1}{d}\sum_{a=0}^{d-1} \mathbb{P}(f_1(\nu_\theta^a Z_\theta) > \cdots > f_D(\nu_\theta^a Z_\theta)).$$

Proof. Let $\varepsilon > 0$. There exists $n_0 \ge 1$ such that for every $n \ge n_0$, we have $|r_j(n)| < \varepsilon$. Now for every $n \ge n_0$, one has

$$F_1(n) > F_2(n) + 2\varepsilon > \cdots > F_D(n) + 2(D-1)\varepsilon \Rightarrow G_1(n) > G_2(n) > \cdots > G_D(n)$$
$$\Rightarrow F_1(n) > F_2(n) - 2\varepsilon > \cdots > F_D(n) - 2(D-1)\varepsilon$$

In the degenerate case, this implies by Proposition 1.51 that

$$\mathbb{P}(f_1(Z_\theta) > \cdots > f_D(Z_\theta) + 2(D-1)\varepsilon) \le \underline{\delta}(G_1 > \cdots > G_D)$$
$$\le \overline{\delta}(G_1 > \cdots > G_D) \le \mathbb{P}(f_1(Z_\theta) > \cdots > f_D(Z_\theta) - 2(D-1)\varepsilon),$$

while in the non-degenerate case, this implies by Theorem 1.57

$$\frac{1}{d}\sum_{a=0}^{d-1} \mathbb{P}(f_1(\nu_\theta^a Z_\theta) > \cdots > f_D(\nu_\theta^a Z_\theta) + 2(D-1)\varepsilon) \le \underline{\delta}(G_1 > \cdots > G_D)$$
$$\le \overline{\delta}(G_1 > \cdots > G_D)$$
$$\le \frac{1}{d}\sum_{a=0}^{d-1} \mathbb{P}(f_1(\nu_\theta^a Z_\theta) > \cdots > f_D(\nu_\theta^a Z_\theta) - 2(D-1)\varepsilon).$$

In both cases, we obtain the announced inequalities on $\underline{\delta}(G_1 > \cdots > G_D)$ and $\overline{\delta}(G_1 > \cdots > G_D)$ by letting ε tend to 0 as in the proof of Theorem 1.57.

Finally, the last hypotheses imply that $\mathbb{P}(f_1(Z_\theta) > \cdots > f_D(Z_\theta)) = \mathbb{P}(f_1(Z_\theta) \ge \cdots \ge f_D(Z_\theta))$ in the degenerate case since Z_θ is uniform on $\langle \nu_\theta \rangle$, while they imply $\mathbb{P}(f_1(\nu_\theta^a Z_\theta) > \cdots > f_D(\nu_\theta^a Z_\theta)) = \mathbb{P}(f_1(\nu_\theta^a Z_\theta) \ge \cdots \ge f_D(\nu_\theta^a Z_\theta))$ for every $0 \le a \le D-1$ in the non-degenerate case because of Lemma 1.56. □

The proof of the next theorem is completely similar, based on Theorem 1.62 and Corollary 1.79. This time, $\delta(\mathcal{R}(G_1, \dots, G_D))$ means, when it exists,

$$\lim_{X \to +\infty} \frac{1}{X} \int_0^X \mathbf{1}_{\mathcal{R}}(G_1(y), \dots, G_D(y))\, \mathrm{d}y,$$

and $\underline{\delta}(\mathcal{R}(G_1, \dots, G_D))$ and $\overline{\delta}(\mathcal{R}(G_1, \dots, G_D))$ the corresponding lim inf and lim sup.

Theorem 1.81. *i) Let $\theta_1, \dots, \theta_m$ be real numbers, $f_1, \dots, f_D \in \mathbb{C}(X_1, \dots, X_r,)$ be pairwise distinct and real-valued on $\mathbb{T}^r$. Let $G : t \mapsto (F_1(t), \dots, F_D(t)) + o(1)$ as $t \to +\infty$, where $F_j(t) = f_j\left(e^{i\theta_1 t}, \dots, e^{i\theta_r t}\right)$ for $1 \leq j \leq D$. Then*

$$\begin{aligned}\mathbb{P}(f_1(Z_\theta) > \cdots > f_D(Z_\theta)) &\leq \underline{\delta}(G_1 > \cdots > G_D) \\ &\leq \overline{\delta}(G_1 > \cdots > G_D) \leq \mathbb{P}(f_1(Z_\theta) \geq \cdots \geq f_D(Z_\theta)).\end{aligned}$$

Moreover, if for every $1 \leq j \leq D-1$, there exists $y \in \mathbb{R}$ such that $F_j(y) \neq F_{j+1}(y)$, then $\delta(G_1 > \cdots > G_D)$ exists and we have

$$\delta(G_1 > \cdots > G_D) = \mathbb{P}(f_1(Z_\theta) > \cdots > f_D(Z_\theta)).$$

ii) Let $\theta = (\theta_n)_{n\geq 1}$ be a sequence of pairwise distinct positive real numbers and $\Theta = \{\theta_n \mid n \geq 1\}$. Let $F_1, \dots, F_D : \mathbb{R}^+ \longrightarrow \mathbb{R}$ be B^1 almost-periodic functions such that for $1 \leq j \leq D, F_j \sim c_j + \sum_{\theta\in\Theta} a_{\theta,j} e^{i\theta t} + \overline{a_{\theta,j}} e^{-i\theta t}$ and $G : t \mapsto (F_1(t), \dots, F_D(t)) + o(1)$ as $t \to +\infty$. Then, with $S_1, \dots, S_D$ the random variables associated to $F_1, \dots, F_D$ in Theorem 1.65, we have

$$\begin{aligned}\mathbb{P}(S_1 > \cdots > S_D) &\leq \underline{\delta}(G_1 > \cdots > G_D) \\ &\leq \overline{\delta}(G_1 > \cdots > G_D) \leq \mathbb{P}(S_1 \geq \cdots \geq S_D).\end{aligned}$$

Moreover, if $\operatorname{Span}_{\mathbb{Q}} \Theta = \operatorname{Span}_{\mathbb{Q}} T \oplus \operatorname{Span}_{\mathbb{Q}}(\Theta \setminus T)$ for some non-empty finite subset T of Θ, and if for every $1 \leq j \leq D-1$, there exists $\theta \in T$ such that $a_{\theta,j} \neq a_{\theta,j+1}$, then $\delta(G_1 > \cdots > G_D)$ exists and

$$\delta(G_1 > \cdots > G_D) = \mathbb{P}(S_1 > \cdots > S_D).$$

Let us provide a consequence of the above result for prime number races over number fields with any number of participants. Using the explicit formula [Ng00, (5.12)] and Theorem 1.81 *ii)*, we obtain the following.

Theorem 1.82. *Let L/K be a Galois extension of number fields, with Galois group G. Assume ζ_L satisfies the Riemann Hypothesis. Let Θ be the set of positive imaginary parts of the non-trivial zeros of Artin L-functions attached to irreducible complex characters of G, and assume that $\operatorname{Span}_{\mathbb{Q}} \Theta = \operatorname{Span}_{\mathbb{Q}} T \oplus \operatorname{Span}_{\mathbb{Q}}(\Theta \setminus T)$ for some non-empty finite subset T of Θ. Let $C_1, \dots, C_D$ be distinct conjugacy classes of G. If for every $1 \leq j \leq D-1$, there exists $\theta \in T$ such that*

$$\sum_{\chi \neq \chi_0} \operatorname{ord}_{s=\frac{1}{2}+i\theta} L(s,\chi)\,(\chi(C_j) - \chi(C_{j+1})) \neq 0$$

then the logarithmic density

$$\delta(L/K; C_1, \dots, C_D) := \lim_{X\to+\infty} \frac{1}{X} \int_2^X \mathbf{1}_{\pi_{C_1}(e^t) > \cdots > \pi_{C_D}(e^t)}\, \mathrm{d}t$$

exists.

Remarks 1.83.

i) Using the unconditional explicit formula from [FJ20a, Corollary 3.10], we could provide a similar statement for the existence of the above logarithmic density, under a suitable hypothesis of non-vanishing coefficient as above and without assuming the Riemann Hypothesis for ζ_L.

ii) Because of the special properties of Artin L-functions with respect to induction of characters, one could state a linear independence hypothesis about the set of zeros of Artin L-functions attached to irreducible complex characters of G^+ instead, where G^+ is the Galois group of the Galois closure of L over $\mathbb{Q}$. That this is a more natural set of zeros to consider was noted by the author, and used for the first time in [FJ20a].

1.4.2 Applications

1.4.2.1 Non-critical densities

We give sufficient conditions for the densities we study to be positive.

Proposition 1.84. *Let $\theta_1, \dots, \theta_r$ be real numbers. Let $f_1, \dots, f_D, F_1, \dots, F_D$ and $G_1, \dots, G_D$ be as in Theorem 1.80.*

i) Degenerate case : Assume that $\theta_i \in \pi\mathbb{Q}$ for $1 \leq i \leq r$. If there exists $n \in \mathbb{Z}$ such that $F_1(n) > \cdots > F_D(n)$, then $0 < \underline{\delta}(G_1 > \cdots > G_D)$ and if there exists $n \in \mathbb{Z}$ such that $F_1(n) \geq \cdots \geq F_D(n)$ does not hold, then $\overline{\delta}(G_1 > \cdots > G_D) < 1$.

ii) Non-degenerate case : Assume $\theta_i \notin \pi\mathbb{Q}$ for at least one $i \in \{1, \dots, r\}$. If there exist $a \in \{0, \dots, d-1\}$ and $z \in H_\theta$ such that $f_1(\nu_\theta^a z) > \cdots > f_D(\nu_\theta^a z)$ then $0 < \underline{\delta}(G_1 > \cdots > G_D)$. Also, if there exist $a \in \{0, \dots, d-1\}$ and $z \in H_\theta$ such that $f_1(\nu_\theta^a z) \geq \cdots \geq f_D(\nu_\theta^a z)$ does not hold, then $\overline{\delta}(G_1 > \cdots > G_D) > 1$. In particular, if there exists $n \in \mathbb{Z}$ such that $F_1(n) > \cdots > F_D(n)$, then $0 < \underline{\delta}(G_1 > \cdots > G_D)$, and if there exists $n \in \mathbb{Z}$ such that $F_1(n) \geq \cdots \geq F_D(n)$ does not hold, then $\overline{\delta}(G_1 > \cdots > G_D) < 1$.

Proof.

i) It is immediate by Corollary 1.51 and Theorem 1.80 i).

ii) Assume that there exist $a \in \{0, \dots, d-1\}$ and $z \in H_\theta$ such that $f_1(\nu_\theta^a z) > \cdots > f_D(\nu_\theta^a z)$. By continuity of $f_1, \dots, f_D$, there exists an open subset U of H_θ such that $z \in U$ and for all $z' \in U$, $f_1(\nu_\theta^a z') > \cdots > f_D(\nu_\theta^a z')$. Therefore, we have

$$\begin{aligned}\mathbb{P}(f_1(\nu_\theta^a Z_\theta) > \cdots > f_D(\nu_\theta^a Z_\theta)) &\geq \mathbb{P}(Z_\theta \in U) \\ &= \mathbb{P}((Z_1, \dots, Z_m) \in \varphi^{-1}(U)) \\ &= \lambda(\varphi^{-1}(U)) > 0,\end{aligned}$$

where φ is the continuous map

$$\begin{array}{rccc} & \mathbb{T}^m & \longrightarrow & H_\theta \\ \varphi : & (z_1, \dots, z_m) & \mapsto & \left(z_1^d, \dots, z_m^d, \prod_{k=1}^m z_k^{h_{k,m+1}}, \dots, \prod_{k=1}^m z_k^{h_{k,r}}\right) \end{array}$$

and λ is the Lebesgue measure on $\mathbb{T}^m$. By Theorem 1.80 *ii)*, we obtain $\underline{\delta}(F_1 > \cdots > F_D) \geq \frac{\mathbb{P}(f_1(\nu_\theta^a Z_\theta) > \cdots > f_D(\nu_\theta^a Z_\theta))}{d} > 0$. The proof of the second statement is similar since the negation of $f_1(\nu_\theta^a z) \geq \cdots \geq f_D(\nu_\theta^a z)$ is also an open condition on z.
The last stament is immediate since, if $n \equiv a \bmod d$, then $\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) = \nu_\theta^a z$ for some $z \in H_\theta$ by construction.

□

Remarks 1.85.

i) In the degenerate case, we actually have the lower bound $\frac{1}{d} \leq \underline{\delta}(G_1 > \cdots > G_D)$ whenever $\underline{\delta}(G_1 > \cdots > G_D) > 0$, and the upper bound $\overline{\delta}(G_1 > \cdots > G_D) \leq 1 - \frac{1}{d}$ whenever $\overline{\delta}(G_1 > \cdots > G_D) < 1$.

ii) The converses of the above statements are false in general. For example it may happen that $f_1(z) = \cdots = f_D(z)$ for every $z \in \mathbb{T}^r$, but $\underline{\delta}(G_1 > \cdots > G_D) > 0$ because $r_1(n) > \cdots > r_D(n)$ for a positive proportion of $n \in \mathbb{N}$.

The continuous version of the above Proposition is proved in the same way as *ii)* above.

Proposition 1.86. *Let $\theta_1, \ldots, \theta_r$ be real numbers. Let $f_1, \ldots, f_D, F_1, \ldots, F_D$ and G be as in Theorem 1.81 i). If there exists $z \in H_\theta$ such that $f_1(z) > \cdots > f_D(z)$ then $0 < \underline{\delta}(G_1 > \cdots > G_D)$. Also, if there exists $z \in H_\theta$ such that $f_1(z) \geq \cdots \geq f_D(z)$ does not hold, then $\overline{\delta}(G_1 > \cdots > G_D) > 1$. In particular, if there exists $y \in \mathbb{R}$ such that $F_1(y) > \cdots > F_D(y)$, then $0 < \underline{\delta}(G_1 > \cdots > G_D)$, and if there exists $n \in \mathbb{Z}$ such that $F_1(n) \geq \cdots \geq F_D(n)$ does not hold, then $\overline{\delta}(G_1 > \cdots > G_D) < 1$.*

Remark 1.87. In the infinite-dimensional case, the only known lower bounds on the density are shown in particular cases by using delicate combinatorial arguments (*cf.* [RS94, 2.2] and [Dev19, Theorem 2.5.1 (1)]).

1.4.2.2 Prime divisor races over global function fields

We now give an application of the previous results to the study of prime divisor races over global function field extensions.

Let L/K be a geometric Galois extension of function fields, with constant field $\mathbb{F}_q$, the finite field with q elements, *i.e.* K is a finitely generated extension of $\mathbb{F}_q$, has transcendence degree 1 over $\mathbb{F}_q$, $\mathbb{F}_q$ is algrebraically closed in K and L/K is Galois. We let g_K and g_L denote the genus of K and L respectively. Let $C_1, \ldots, C_D$ be $D \geq 1$ distinct conjugacy classes of $G := \mathrm{Gal}(L/K)$. Define

$$\pi_{C_i}(n) := \#\{P \text{ prime divisor of } K \text{ unramified in } L \mid \deg(P) = n, \mathrm{Frob}_P = C_i\},$$

where Frob_P denotes the Frobenius conjugacy class of P in G. The Chebotarev density theorem ([Ros02, Theorem 9.13B]) states that

$$\pi_{C_i}(n) = \frac{|C_i|}{|G|}\frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

This shows that

$$\frac{\pi_{C_i}(n)}{|C_i|} \underset{n\to+\infty}{\sim} \frac{\pi_{C_j}(n)}{|C_j|}$$

for any two $i \neq j$, but we want to compare those two quantities beyond this first order asymptotic. The question is, how often can it happen that

$$\frac{\pi_{C_1}(n)}{|C_1|} > \cdots > \frac{\pi_{C_D}(n)}{|C_D|}\,?$$

More precisely, we are interested in the following density, provided it exists,

$$\delta(L/K; C_1, \dots, C_D) := \lim_{X \to +\infty} \frac{\#\left\{n \leq X \;\middle|\; \frac{\pi_{C_1}(n)}{|C_1|} > \dots > \frac{\pi_{C_D}(n)}{|C_1|}\right\}}{X}.$$

When studying the densities $\delta(L/K; C_{\sigma(1)}, \dots, C_{\sigma(D)})$ for every permutation σ of $\{1, \dots, D\}$, we say we study the prime divisor race between $C_1, \dots, C_D$. As usual, we will denote by $\underline{\delta}(L/K; C_1, \dots, C_D)$ the corresponding lim inf and lim sup.

To study the above densities, we use the Artin L-functions associated to irreducible characters of G. If χ is such a character, one has the following convenient expression :

$$\log L(s, \chi) = \sum_P \sum_{n \geq 1} \frac{\chi(P^n) q^{-n \deg(P) s}}{n}$$

for $\mathfrak{Re}(s) > 1$, where $\chi(P^n)$ is a short way of writing

$$\frac{1}{e(P)} \sum_{j=1}^{e(P)} \chi(g_j(\mathrm{Frob}_P)^n).$$

Here, $e(P)$ is the ramification index of P in L, and $g_1, \dots, g_{e(P)}$ are the elements of the inertia subgroup $I(\mathfrak{P})$, for any prime $\mathfrak{P}$ of L dividing P (recall that those quantities only depend on P up to conjugacy, so the above summands are well-defined since χ is a central function on G).

It is convenient to move from the variable s to the variable $u := q^{-s}$, and to write $\mathcal{L}(u, \chi) := L(s, \chi)$. Then one has the following important theorem ([Ros02, Theorems 9.16A and 9.16B]) :

Theorem 1.88 (Weil)**.** *The function $L(s, \chi_0)$, where χ_0 is the trivial character of G, is the zeta function ζ_K of K, which is a rational function in u with integer coefficients :*

$$\zeta_K(s) = \mathcal{L}(u, \chi_0) = \frac{\prod_{j=1}^{2g_K}(1 - \gamma(\chi_0, j)u)}{(1-u)(1-qu)}.$$

If $\chi \neq \chi_0$ is a non-trivial irreducible character of G, then $\mathcal{L}(u, \chi)$ is a polynomial in u with integer coefficients :

$$\mathcal{L}(u, \chi) = \prod_{j=1}^{M_\chi}(1 - \gamma(\chi, j)u)$$

for some integer $M_\chi \geq 0$. The $\gamma(\chi, j)$ are called the inverse zeros of $\mathcal{L}(u, \chi)$ and have absolute value $\sqrt{q}$ (Riemann Hypothesis for curves over $\mathbb{F}_q$). Moreover, if γ is an inverse zero of $\mathcal{L}(u, \chi)$ then $\frac{q}{\gamma} = \overline{\gamma}$ is an inverse zero of $\mathcal{L}(u, \overline{\chi})$.

The last statement of the theorem is a simple consequence of the functional equation satisfied by Artin L-functions, which we do not formulate here (for non-trivial characters, one has to combine the functional equation of Hecke L-series and Brauer's induction theorem as in the case of Artin L-functions over number fields [BCdS$^+$03, p.81-83]).

We now make some preliminary work to study the prime divisor races in L/K. We let C be a conjugacy class of G.

On the one hand, by the definition of Artin L-functions, one has

$$u\frac{\mathrm{d}}{\mathrm{d}u}\log\mathcal{L}(u,\chi)=\sum_{P}\sum_{n\geq 1}\deg P\chi(P^n)u^{n\deg P}=\sum_{n\geq 1}\left(\sum_{\substack{P\\ \deg P\mid n}}\deg P\chi(P^{\frac{n}{\deg P}})\right)u^n.$$

On the other hand, from the above factorisations, we obtain

$$u\frac{\mathrm{d}}{\mathrm{d}u}\log\mathcal{L}(u,\chi_0)=\sum_{n\geq 1}\left(q^n+1-\sum_{j=1}^{2g_K}\gamma(\chi,j)^n\right)u^n$$

and for $\chi\neq\chi_0$

$$u\frac{\mathrm{d}}{\mathrm{d}u}\log\mathcal{L}(u,\chi)=\sum_{n\geq 1}\left(-\sum_{j=1}^{M_\chi}\gamma(\chi,j)^n\right)u^n.$$

Writing

$$u\frac{\mathrm{d}}{\mathrm{d}u}\log\mathcal{L}(u,\chi)=\sum_{n\geq 1}c_n(\chi)u^n,$$

and using the second orthogonality relations on characters, we find from the first formula for $c_n(\chi)$ above that

$$\begin{aligned}\sum_{\chi}\overline{\chi(C)}c_n(\chi)&=\sum_{\substack{P\\ \deg P\mid n}}\deg P\sum_{\chi}\chi(P^{\frac{n}{\deg P}})\overline{\chi(C)}\\&=\frac{\#G}{\#C}\sum_{d\mid n}d\#\{P\mid\deg P=d,\mathrm{Frob}_P^{\frac{n}{d}}\subset C\}\\&=\frac{\#G}{\#C}n\pi_C(n)+R_C(n)+O\left(q^{n/3}\right),\end{aligned}$$

where

$$R_C(n)=\begin{cases}\frac{n}{2}\frac{\#G}{\#C}\#\{P\mid\deg P=\frac{n}{2},\mathrm{Frob}_P^2\subset C\}\text{ if }n\text{ is even}\\0\text{ otherwise.}\end{cases}$$

Using now the second formula for $c_n(\chi)$ above, we obtain

$$\sum_{\chi}\overline{\chi(C)}c_n(\chi)=q^n+1-\sum_{j=1}^{2g_K}\gamma(\chi_0,j)^n-\sum_{\chi\neq\chi_0}\overline{\chi(C)}\sum_{j=1}^{M_\chi}\gamma(\chi,j)^n.$$

Combining those formulas we obtain

$$\frac{\#G}{\#C}\pi_C(n)=\frac{q^n}{n}-\frac{R_C(n)}{n}-\frac{1}{n}\sum_{j=1}^{2g_K}\gamma(\chi_0,j)^n-\frac{1}{n}\sum_{\chi\neq\chi_0}\overline{\chi(C)}\sum_{j=1}^{M_\chi}\gamma(\chi,j)^n+O\left(\frac{q^{n/3}}{n}\right).$$

We now introduce $C^{1/2}:=\{g\in G\mid g^2\in C\}$, and remark it is stable by conjugation in G, so it is the disjoint union of conjugacy classes $D_1,\dots,D_t$ of G, and $\#\{P\mid\deg P=$

$\frac{n}{2}, \mathrm{Frob}_P^2 \subset C\} = \sum_{i=1}^t \pi_{D_i}\left(\frac{n}{2}\right) = \sum_{i=1}^t \frac{\#D_i}{\#G}\frac{2}{n}q^{n/2} + O(q^{n/4}) = \frac{\#(C^{1/2})}{\#G}\frac{2}{n}q^{n/2} + O(q^{n/4})$ by the above formula.

This shows that

$$R_C(n) = \begin{cases} \frac{\#(C^{1/2})}{\#C}q^{n/2} + O(q^{n/4}) \text{ if } n \text{ is even} \\ 0 \text{ otherwise,} \end{cases} = \frac{\#(C^{1/2})}{2\#C}q^{n/2} + \frac{\#(C^{1/2})}{2\#C}q^{n/2}e^{i\pi n} + O(q^{n/4}).$$

Finally, we have

$$\frac{\#G}{\#C}\pi_C(n) = \frac{q^n}{n} - \frac{\#(C^{1/2})}{\#C}\frac{q^{n/2}}{2n} - \frac{\#(C^{1/2})}{\#C}\frac{q^{n/2}}{2n}e^{i\pi n} - \frac{1}{n}\sum_{j=1}^{2g_K}\gamma(\chi_0, j)^n - \frac{1}{n}\sum_{\chi\neq\chi_0}\overline{\chi(C)}\sum_{j=1}^{M_\chi}\gamma(\chi, j)^n + O\left(\frac{q^{n/3}}{n}\right).$$

Similarly, with $\pi_K(n) := \#\{P \mid \deg P = n\}$, one has

$$\pi_K(n) = \frac{q^n}{n} - \frac{q^{n/2}}{2n} - e^{i\pi n}\frac{q^{n/2}}{2n} - \frac{1}{n}\sum_{j=1}^{2g_K}\gamma(\chi_0, j)^n + O\left(q^{n/3}\right).$$

Combining those formulas, we obtain

$$\frac{n}{q^{n/2}}\left(\frac{\#G}{\#C}\pi_C(n) - \pi_K(n)\right) = \frac{1 - \frac{\#(C^{1/2})}{\#C}}{2} + \frac{1 - \frac{\#(C^{1/2})}{\#C}}{2}e^{i\pi n} - \sum_{\chi\neq\chi_0}\overline{\chi(C)}\sum_{j=1}^{M_\chi}\left(\frac{\gamma(\chi, j)}{\sqrt{q}}\right)^n + o(1)$$

as $n \to +\infty$.

Grouping pairs of conjugate inverse zeros we have shown :

Proposition 1.89. *Let $\gamma_1, \dots, \gamma_r$ be the inverse zeros with positive imaginary part of the $\mathcal{L}(u, \chi)$, for $\chi \neq \chi_0$, counted without multiplicity. For $1 \leq j \leq r$, write $\gamma_j = \sqrt{q}e^{i\theta_j}$. Then for any conjugacy class C of G we have*

$$\frac{n}{q^{n/2}}\left(\frac{\#G}{\#C}\pi_C(n) - \pi_K(n)\right) = r_C + z_C + a_\pi(C)e^{i\pi n} - \sum_{j=1}^{r}\left(a_j(C)e^{i\theta_j n} + \overline{a_j(C)}e^{-i\theta_j n}\right) + o(1)$$

as $n \to +\infty$, where

$$r_C := \frac{1 - \frac{\#(C^{1/2})}{\#C}}{2},$$

$$z_C := -\sum_{\chi\neq\chi_0}\overline{\chi(C)}\,\mathrm{ord}_{u=q^{-1/2}}\,\mathcal{L}(u, \chi),$$

$$a_\pi(C) = r_C - \sum_{\chi\neq\chi_0}\overline{\chi(C)}\,\mathrm{ord}_{u=-q^{-1/2}}\,\mathcal{L}(u, \chi),$$

and for $1 \leq j \leq r$,

$$a_j(C) := \sum_{\chi\neq\chi_0}\overline{\chi(C)}\,\mathrm{ord}_{u=\gamma_j^{-1}}\,\mathcal{L}(u, \chi).$$

We have thus shown that a suitable rescaling of $\pi_C(n)$ is of the form we studied in the previous sections. The rescaling of $\frac{\pi_C(n)}{\#C}$ does not depend on C, so that will allow us to study prime divisor races between conjugacy classes of G.

Theorem 1.90. *Let $C_1, \dots, C_D$ be conjugacy classes of G. For $1 \leq j \leq D$, let $f_j = r_{C_j} + z_{C_j} + a_\pi(C_j)\frac{X_{r+1}+X_{r+1}^{-1}}{2} - \sum_{k=1}^{r}\left(a_k(C_j)X_j + \overline{a_k(C_j)}X_j^{-1}\right) \in \mathbb{C}(X_1, \dots, X_{r+1})$ and $F_j : t \mapsto f_j\left(e^{i\theta_1 t}, \dots, e^{i\theta_r t}, e^{i\pi t}\right)$.*

i) Degenerate case : Assume $\theta_i \in \pi\mathbb{Q}$ for $1 \leq i \leq r$, i.e. that each $\mathcal{L}(u,\chi)$, $\chi \neq \chi_0$, is a product of rescaled cyclotomic polynomials. If there exists $n \in \mathbb{Z}$ such that $F_1(n) > \cdots > F_D(n)$, then $0 < \underline{\delta}(L/K; C_1, \dots, C_D)$ and if there exists $n \in \mathbb{Z}$ such that $F_1(n) \geq \cdots \geq F_D(n)$ does not hold, then $\overline{\delta}(L/K; C_1, \dots, C_D) < 1$. Moreover, if for $1 \leq j \leq D-1$, and for $0 \leq n \leq d-1$, one has $F_j(n) \neq F_{j+1}(n)$, then $\delta(L/K; C_1, \dots, C_D)$ exists.

ii) Non-degenerate case : Assume $\theta_i \notin \pi\mathbb{Q}$ for at least one $i \in \{1, \dots, r\}$. If there exist $a \in \{0, \dots, d-1\}$ and $z \in H_\theta$ such that $f_1(\nu_\theta^a z) > \cdots > f_D(\nu_\theta^a z)$ then $0 < \underline{\delta}(L/K; C_1, \dots, C_D)$. Also, if there exist $a \in \{0, \dots, d-1\}$ and $z \in H_\theta$ such that $f_1(\nu_\theta^a z) \geq \cdots \geq f_D(\nu_\theta^a z)$ does not hold, then $\overline{\delta}(L/K; C_1, \dots, C_D) < 1$. In particular, if there exists $n \in \mathbb{Z}$ such that $F_1(n) > \cdots > F_D(n)$, then $0 < \underline{\delta}(L/K; C_1, \dots, C_D)$, and if there exists $n \in \mathbb{Z}$ such that $F_1(n) \geq \cdots \geq F_D(n)$ does not hold, then $\overline{\delta}(L/K; C_1, \dots, C_D) < 1$. Moreover, if for $0 \leq a \leq d-1$ and $1 \leq j \leq D-1$, there exists $n \equiv a \bmod d$ such that $F_j(n) \neq F_{j+1}(n)$, then $\delta(L/K; C_1, \dots, C_D)$ exists.

Proof. This is an immediate application of Proposition 1.89, Theorem 1.80 and Proposition 1.84. □

We now treat an example for which there is linear dependence between the θ_i's. This example was featured in [CI11], but since it did not satisfy the required linear independence condition under which the authors worked, they couldn't say anything about it. Take $K = \mathbb{F}_7(t)$ and $L = K(\alpha)$ where α has minimal polynomial $f = X^6 - (t^2+t)X^3 - 1$ over K. Then as detailed in [CI11, 4.2], $G = \mathrm{Gal}(L/K) \simeq \mathfrak{S}_3$. We note $C_1 = \{\mathrm{id}\}$, $C_2 = \{(1\,2), (1\,3), (2\,3)\}$ and $C_3 = \{(1\,2\,3), (1\,3\,2)\}$, and it is well-known that we have the following character table for G :

$\mathfrak{S}_3$	C_1	C_2	C_3
χ_0	1	1	1
χ_1	1	-1	1
χ_2	2	0	-1

One has

$$\mathcal{L}(u, \chi_1) = 1 + 4u + 7u^2 = (1 - \gamma_1 u)(1 - \overline{\gamma_1} u),$$

$$\mathcal{L}(u, \chi_2) = 1 + u + 7u^2 = (1 - \gamma_2 u)(1 - \overline{\gamma_2} u),$$

with (those two values are inverted in [CI11])

$$\gamma_1 = -2 + i\sqrt{3}$$

and

$$\gamma_2 = \frac{-1 + 3i\sqrt{3}}{2}.$$

Then we have $\theta_1 = \arctan\left(-\frac{\sqrt{3}}{2}\right)$, $\theta_2 = \arctan(-3\sqrt{3})$ and $\theta_1 + \theta_2 = \frac{4\pi}{3}$. Adding $\theta_3 = \pi$ because of the coefficient $a_\pi(C)$, we are in the non-degenerate case (because $\theta_2 = -\arccos\left(\frac{1}{\sqrt{28}}\right)$ as one easily verifies, and such a number is known not to be a rational multiple of π [Var06]). With notations from Section 1.4.1.2, we have $m = 1, d = 6, c_2 = \frac{2}{3}, b_{1,2} = -1, c_3 = \frac{1}{2}, b_{1,3} = 0$.

A quick computation using PARI/GP shows that for $i \neq j \in \{1,2,3\}$ and every $a \in \{0,1,2,3,4,5\}$, there exists $n \equiv a \bmod 6$ such that $F_i(n) \neq F_j(n)$, so for every permutation $\sigma \in \mathfrak{S}_3$, the density $\delta(L/K; C_{\sigma(1)}, C_{\sigma(2)}, C_{\sigma(3)})$ exists, *i.e.* the race between C_1, C_2 and C_3 is weakly inclusive (Definition 1.47). Also, for every permutation $\sigma \in \mathfrak{S}_3$, the inequality $F_{\sigma(1)}(n) > F_{\sigma(2)}(n) > F_{\sigma(3)}(n)$ happens for some $n \leq 7$ so we may conclude that $0 < \delta(L/K; C_{\sigma(1)}, C_{\sigma(2)}, C_{\sigma(3)}) < 1$ and in particular the race between C_1, C_2 and C_3 is inclusive (Definition 1.47).

Remark 1.91. If one wants to study races between functions counting prime divisors of degree less than n, instead of equal to n as above, one can use the following explicit formula ([CI11, Theorem 2.1]) :

$$\frac{n}{q^{n/2}}\left(\frac{\#G}{\#C}\sum_{k=1}^{n}\pi_C(k) - \pi_K(n)\right) = r_C\frac{q+\sqrt{q}}{q-1} + r_C\frac{q-\sqrt{q}}{q-1}e^{in\pi} - 2\sum_{j=1}^{2g_K}\frac{\gamma(\chi_0,j)}{\gamma(\chi_0,j)-1}e^{in\theta(\chi_0,j)} - \sum_{\chi\neq\chi_0}\overline{\chi(C)}\sum_{j=1}^{M_\chi}\frac{\gamma(\chi,j)}{\gamma(\chi,j)-1}e^{in\theta(\chi,j)} + o(1)$$

as $n \to +\infty$, and use our method similarly since this has the shape we studied above.

1.4.2.3 Moments

To bound the probabilities involved in our results in the case $D = 2$, moment estimates, such as Chebyshev's inequality, can prove very useful. In particular, races where, for each a, $\mathbb{P}(f_1(\nu_\theta^a Z_\theta) > f_2(\nu_\theta^a Z_\theta)) \underset{q\to+\infty}{\longrightarrow} 1$ or 0 ("extremely biased races") or each $\mathbb{P}(f(\nu_\theta^a Z_\theta) > f_2(\nu_\theta^a Z_\theta)) \underset{q\to+\infty}{\longrightarrow} \frac{1}{2}$ ("moderately biased races") can be obtained from sufficiently good estimates on the corresponding means and variances as in [FJ20a]. Here the limits are taken with respect to a parameter q attached to the prime number races considered. To go beyond the first two moments, and for example have an explicitly computable characteristic function at our disposal as in [Cha08, Theorem 3.4] or [CI11, Theorem 2.4]), we would need to assume extra linear independence.

In the next Proposition, we give formulas for the first two moments of the random variables $f_j(\nu_\theta^a Z_\theta)$ for some particular types of functions f_j.

Proposition 1.92. *Let $f = c + \sum_{k=1}^{r} a_k X_k + \overline{a_k} X_k^{-1} \in \mathbb{C}(X_1, \ldots, X_r)$. Let $\theta_1, \ldots, \theta_r$ be real numbers such that $\theta_i \notin \pi\mathbb{Q}$ for $i \leq n$, and $\theta_i \in \pi\mathbb{Q}$ for $n < i \leq r$. Then for $0 \leq a \leq d-1$, one has*

$$\mathbb{E}(f(\nu_\theta^a Z_\theta)) = c + \sum_{n<k\leq r}(a_k e^{ia\theta_k} + \overline{a_k}e^{-ia\theta_k})$$

and

$$\mathrm{Var}(f(\nu_\theta^a Z_\theta)) = 2\sum_{1\le k\le n}|a_k|^2 + 4\mathfrak{Re}\left(\sum_{\substack{1\le i<j\le n\\ \theta_i+\theta_j\in\pi\mathbb{Q}}} a_i a_j e^{ia(\theta_i+\theta_j)}\right) + 4\mathfrak{Re}\left(\sum_{\substack{1\le i<j\le n\\ \theta_i-\theta_j\in\pi\mathbb{Q}}} a_i\overline{a_j}e^{ia(\theta_i-\theta_j)}\right).$$

In particular if $\theta_i \notin \pi\mathbb{Q}$ for $1\le i\le r$, then $\mathbb{E}(f(\nu_\theta^a Z_\theta)) = c$ does not depend on a, and if no relation of the form $\theta_i \pm \theta_j \in \pi\mathbb{Q}$ holds for $1\le i<j\le n$, then $\mathrm{Var}(f(\nu_\theta^a Z_\theta)$ does not depend on a.

Proof. We note that the n first components of Z_θ are products of non-zero integral powers of independent uniform random variables on $\mathbb{T}$, so they are uniform on $\mathbb{T}$, while the last $r-n$ components of Z_θ are (almost-surely) equal to 1. The result for the mean is then straightforward. For the variance, we expand the squared modulus squared and remark that $Z_{\theta,i}Z_{\theta,j} = 1$ if and only if $\theta_i+\theta_j \in \pi\mathbb{Q}$, and $Z_{\theta,i}\overline{Z_{\theta,j}} = 1$ if and only if $\theta-\theta_j\in\pi\mathbb{Q}$. □

As a corollary of the above Proposition, we deduce another sufficient condition for ties between those functions to have density zero.

Corollary 1.93. *For $1\le j\le D$, let $f_j = c_j + \sum_{k=1}^r a_k^{(j)}X_k + \overline{a_k^{(j)}}X_k^{-1} \in \mathbb{C}(X_1,\dots,X_r)$. Let $\theta_1,\dots,\theta_r$ be real numbers such that $\theta_i\notin\pi\mathbb{Q}$ for $i\le n$, and $\theta_i\in\pi\mathbb{Q}$ for $n<i\le r$. Finally, let $G_j : t\mapsto f_j\left(e^{i\theta_1 t},\dots,e^{i\theta_r t}\right)+o(1)$ as $t\to+\infty$.*

i) If $n>1$ (i.e. we are in the non-degenerate case), and if for every $a\in\{0,\dots,d-1\}$, the map $j\mapsto \sum_{1\le k\le n}|a_k^{(j)}|^2 + 2\mathfrak{Re}\left(\sum_{\substack{1\le i<k\le n\\ \theta_i+\theta_k\in\pi\mathbb{Q}}} a_i^{(j)}a_k^{(j)}e^{ia(\theta_i+\theta_k)}\right) + 2\mathfrak{Re}\left(\sum_{\substack{1\le i<k\le n\\ \theta_i-\theta_k\in\pi\mathbb{Q}}} a_i^{(j)}\overline{a_k^{(j)}}e^{ia(\theta_i-\theta_k)}\right)$ is injective then for every permutation σ of $\{1,\dots,D\}$, $\delta(G_{\sigma(1)}>\cdots>G_{\sigma(D)})$ exists.

ii) If for every $a\in\{0,\dots,d-1\}$, the map $j\mapsto c_j+\sum_{k=n}^r\left(a_k^{(j)}e^{ia\theta_k}+\overline{a_k^{(j)}}e^{-ia\theta_k}\right)$ is injective then for every permutation σ of $\{1,\dots,D\}$, $\delta(G_{\sigma(1)}>\cdots>G_{\sigma(D)})$ exists.

Proof.

i) The hypothesis implies that $\mathrm{Var}(f_i(\nu_\theta^a Z_\theta) - f_j(\nu_\theta^a Z_\theta)) \neq 0$ for any $a\in\{0,\dots,d-1\}$ and any distinct $i,j\in\{1,\dots,D\}$ by Proposition 1.92, so that the random variable $f_i(\nu_\theta^a Z_\theta) - f_j(\nu_\theta^a Z_\theta)$ is almost-surely non-constant. By Lemma 1.56, this implies $\mathbb{P}(f_i(\nu_\theta^a Z_\theta) = f_j(\nu_\theta^a Z_\theta)) = 0$, and the result follows from Theorem 1.80 *ii)*.

ii) The proof is similar, except that this time $\mathbb{E}(f_i(\nu_\theta^a Z_\theta) - f_j(\nu_\theta^a Z_\theta)) \neq 0$, which implies again that $\mathbb{P}(f_i(\nu_\theta^a Z_\theta) = f_j(\nu_\theta^a Z_\theta)) = 0$.

□

Appendix : a proof of the discrete Kronecker-Weyl theorem

Proof of Theorem 1.49. Recall $\theta_1,\dots,\theta_r$ are real numbers such that $\{\pi,\theta_1,\dots,\theta_r\}$ is linearly independent over $\mathbb{Q}$,

$$\Gamma = \left\{\left(e^{i\theta_1 X},\dots,e^{i\theta_r X}\right) \mid X\in\mathbb{Z}\right\}$$

and we want to show that for every continuous $f : \mathbb{T}^r \to \mathbb{C}$,

$$\frac{1}{X}\sum_{n=1}^{X} f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) \underset{X\to+\infty}{\longrightarrow} \int_{\mathbb{T}^r} f \,\mathrm{d}\lambda,$$

where λ is the Lebesgue measure on $\mathbb{T}^r$.

By the Stone-Weierstrass theorem, it is enough to prove the result when f is a trigonometric polynomial, that is a linear combination of monomials in $z_1, \dots, z_r$. Indeed, if the result is true for such functions, then for any $\varepsilon > 0$, we can find trigonometric polynomial g such that $||f - g||_\infty < \varepsilon$, and for every X big enough we have

$$\left|\frac{1}{X}\sum_{n=1}^{X} g\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) - \int_{\mathbb{T}^r} g \,\mathrm{d}\lambda\right| < \varepsilon.$$

For such X, we find

$$\begin{aligned}\left|\frac{1}{X}\sum_{n=1}^{X} f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) - \int_{\mathbb{T}^r} f \,\mathrm{d}\lambda\right| &\leq \left|\frac{1}{X}\sum_{n=1}^{X} (f-g)\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) - \int_{\mathbb{T}^r} (f-g) \,\mathrm{d}\lambda\right| \\ &\quad + \left|\frac{1}{X}\sum_{n=1}^{X} g\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) - \int_{\mathbb{T}^r} g \,\mathrm{d}\lambda\right| < 3\varepsilon\end{aligned}$$

which proves that

$$\frac{1}{X}\sum_{n=1}^{X} f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) \underset{X\to+\infty}{\longrightarrow} \int_{\mathbb{T}^r} f \,\mathrm{d}\lambda.$$

By linearity, we now only have to prove the theorem for monomials

$$\begin{array}{rccc} & \mathbb{T}^r & \longrightarrow & \mathbb{C} \\ f : & (z_1, \dots, z_r) & \mapsto & z_1^{n_1} \dots z_r^{n_r}, \end{array}$$

where $n_1, \dots, n_r \in \mathbb{Z}$.

The result is obviously true if $(n_1, \dots, n_r) = (0, \dots, 0)$, *i.e.* if $f = 1$ since both sides are equal to 1. Now assume at least one n_i is non-zero. On the one hand we have

$$\int_{\mathbb{T}^r} f \,\mathrm{d}\lambda = \prod_{k=1}^{r} \int_{\mathbb{T}} z^{n_k} \,\mathrm{d}\lambda = 0.$$

On the other hand, since $\{\pi, \theta_1, \dots, \theta_r\}$ is linearly independant over $\mathbb{Q}$, we have that $n_1\theta_1 + \dots + n_r\theta_r \notin 2\pi\mathbb{Z}$, so that $e^{i(n_1\theta_1+\dots+n_r\theta_r)} \neq 1$. Now, summing the geometric progression, we find

$$\begin{aligned}\frac{1}{X}\sum_{n=1}^{X} f\left(e^{i\theta_1 n}, \dots, e^{i\theta_r n}\right) &= \frac{1}{X}\sum_{n=1}^{X} e^{in(n_1\theta_1+\dots+n_r\theta_r)} \\ &= \frac{1}{X}\frac{e^{i(X+1)(n_1\theta_1+\dots+n_r\theta_r)} - e^{i(n_1\theta_1+\dots+n_r\theta_r)}}{e^{i(n_1\theta_1+\dots+n_r\theta_r)} - 1} \\ &\underset{X\to+\infty}{\longrightarrow} 0\end{aligned}$$

since $\frac{e^{i(X+1)(n_1\theta_1+\cdots+n_r\theta_r)}-e^{i(n_1\theta_1+\cdots+n_r\theta_r)}}{e^{i(n_1\theta_1+\cdots+n_r\theta_r)}-1}$ is bounded. □

Remark 1.94. The continuous version of the Kronecker-Weyl theorem states that, assuming $\theta_1, \ldots, \theta_r$ are linearly independent over $\mathbb{Q}$, for every continuous function $f : \mathbb{T}^r \to \mathbb{C}$, one has

$$\frac{1}{X}\int_0^X f\left(e^{i\theta_1 y}, \ldots, e^{i\theta_r y}\right) \mathrm{d}y \underset{X\to+\infty}{\longrightarrow} \int_{\mathbb{T}^r} f \,\mathrm{d}\mu.$$

Its proof is similar as the one given above. The first step reduces to the case of trigonometric polynomials by using the Stone-Weierstrass theorem, and the last calculation is done with integrals instead of discrete sums.

Chapitre 2

Biais de Tchebychev dans les corps de nombres

Dans ce chapitre, on s'intéresse à des questions de type courses de nombres premiers dans le contexte général de la répartition des automorphismes de Frobenius dans les groupes de Galois d'extensions de corps de nombres. Si L/K est une telle extension, galoisienne de groupe de Galois G, on peut associer à (presque) tous les idéaux premiers $\mathfrak{p}$ de K une classe de conjugaison $\mathrm{Frob}_\mathfrak{p}$ de G, appelée automorphisme de Frobenius de $\mathfrak{p}$. Cette classe de conjugaison encode l'arithmétique de chaque extension résiduelle $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ où $\mathcal{O}_L$ et $\mathcal{O}_K$ désignent les anneaux d'entiers de L et de K respectivement, et $\mathfrak{P}$ est n'importe quel idéal premier de L au-dessus de K. Autrement dit cet automorphisme de Frobenius en $\mathfrak{p}$ encode l'information locale en $\mathfrak{p}$ dans l'extension L/K. Par exemple, on a $\mathrm{Frob}_\mathfrak{p} = \{1_G\}$ si et seulement si $\mathfrak{p}$ est totalement décomposé dans L.

Le célèbre théorème de Chebotarev, vaste généralisation du théorème des nombres premiers en progressions arithmétiques, énonce que les automorphismes de Frobenius des idéaux premiers de K s'équirépartissent dans l'ensemble $G^\sharp$ des classes de conjugaison de G pour la mesure de comptage. Ce théorème se démontre en reliant la répartition des idéaux premiers de K à la répartition des zéros de fonctions L dites d'Artin, généralisations « non abéliennes » des fonctions L de Dirichlet (voire, par la théorie du corps de classes, des fonctions L de Hecke). Une fois cette observation faite, il est naturel de se demander si des phénomènes du type du biais de Tchebychev se produisent dans ce contexte. Plus précisément, fixons deux classes de conjugaison C_1 et C_2 de G et soit

$$\pi(x, C_i, L/K) := \#\{\mathfrak{p} \text{ idéal premier de } \mathcal{O}_K \text{ non ramifié dans } L \mid N(\mathfrak{p}) \leq x, \mathrm{Frob}_\mathfrak{p} = C_i\}$$

pour $i \in \{1, 2\}$, où $N(\mathfrak{p})$ désigne la norme de l'idéal $\mathfrak{p}$, c'est-à-dire $\#(\mathcal{O}_k/\mathfrak{p})$. Le théorème de Chebotarev dit alors que

$$\pi(x, C_i, L/K) \underset{x\to+\infty}{\sim} \frac{\#C}{\#G}\,\mathrm{Li}(x)$$

et, comme initialement suggéré dans l'article [RS94] de Rubinstein et Sarnak, on peut chercher à quelle fréquence une inégalité de la forme

$$\frac{\pi(x, C_1, L/K)}{\#C_1} \lessgtr \frac{\pi(x, C_2, L/K)}{\#C_2}$$

se produit.

Cette question peut alors s'étudier en suivant une stratégie proche de celle et de Rubinstein et Sarnak. C'est Ng qui, dans sa thèse [Ng00], a donné les détails de cette méthode

dans ce contexte. On retrouve beaucoup de caractéristiques communes avec le contexte des courses de nombres premiers : on commence par établir une formule explicite pour les fonctions de comptage $\pi(x, C_i, L/K)$, on montre l'existence d'une distribution (logarithmique) limite intimement liée aux zéros de certaines fonctions L, et une hypothèse d'indépendance linéaire convenable portant sur ces zéros permet d'étudier plus en détails cette distribution limite. Un phénomène de biais de Tchebychev, favorisant les non carrés par rapport aux carrés, est toujours présent dans ce contexte. Il y a cependant des différences notables avec le cas classique étudié par Rubinstein et Sarnak, dues à la nature plus complexe des fonctions L d'Artin. L'une d'elles est l'existence de telles fonctions s'annulant en le point central $1/2$, phénomène qui peut avoir une influence sur le biais de Tchebychev, comme observé numériquement dans [Ng00, Chapter 5]. Cette observation constitue le point de départ de l'article [Bai19], reproduit dans la Section 2.3 de cette thèse. Une autre différence, sur laquelle on reviendra, est la difficulté d'énoncer une hypothèse d'indépendance linéaire satisfaisante dans ce contexte, à cause des différentes factorisations naturelles des fonctions L d'Artin. Ainsi l'hypothèse LI employée dans [Ng00, Chapter 5] ne peut en l'état être vraie que dans le cas où le corps de base K est $\mathbb{Q}$.

Dans les travaux présentés dans ce chapitre, on supposera plusieurs conjectures (conjecture d'Artin, hypothèse de Riemann et indépendance linéaire) qui sont pour l'instant nécessaires à l'obtention de résultats aussi satisfaisants que ceux de Rubinstein et Sarnak dans le contexte des courses d'idéaux premiers. On pourra trouver des énoncés inconditionnels plus faibles, ou supposant des hypothèses moins fortes, dans l'esprit de la section 1.2.3 dans l'article [FJ20a] de Fiorilli et Jouve.

2.1 Fonctions L d'Artin et théorème de Chebotarev

Dans cette section, on introduit les outils au cœur de l'étude de la répartition des automorphismes de Frobenius dans les groupes de Galois des corps de nombres, les fonctions L d'Artin, dont l'étude fine mène au théorème de Chebotarev, analogue du théorème des nombres premiers en progressions arithmétiques dans ce contexte. On fixe une extension galoisienne L/K de corps de nombres, dont le groupe de Galois est G.

2.1.1 Automorphismes de Frobenius

Il est bien connu que les idéaux des anneaux d'entiers $\mathcal{O}_K$ et $\mathcal{O}_L$ admettent une factorisation unique à l'ordre près comme produits d'idéaux premiers de ces mêmes anneaux ([Lan94, I, Theorem 2]). Si $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$ (on dira souvent abusivement idéal premier de K), alors $\mathfrak{p}\mathcal{O}_L$ s'écrit comme un produit

$$\prod_{i=1}^{g(\mathfrak{p})} \mathfrak{P}_i^{e(\mathfrak{P}_i/\mathfrak{p})}$$

où chaque $\mathfrak{P}_i$ est un idéal premier de $\mathcal{O}_L$ et $e(\mathfrak{P}_1/\mathfrak{p}), \dots, e(\mathfrak{P}_g/\mathfrak{p}) \geq 1$. L'extension L/K étant galoisienne, on montre facilement ([Lan94, I, Proposition 11]) que le groupe de Galois G agit transitivement sur les $\mathfrak{P}_i$, ce qui implique que $e(\mathfrak{P}_1/\mathfrak{p}) = \cdots = e(\mathfrak{P}_g/\mathfrak{p}) =: e(\mathfrak{p})$. Si $e(\mathfrak{p}) \geq 2$, on dit que $\mathfrak{p}$ est ramifié dans L, et on dit que $\mathfrak{p}$ est non ramifié dans L sinon. Il

n'existe qu'un nombre fini d'idéaux premiers de K ramifiés dans L, ce sont exactement ceux qui divisent le discriminant de l'extension L/K ([Lan94, I, Proposition 8]).

Les idéaux premiers (non nuls) de $\mathcal{O}_K$ sont en fait maximaux (ce qui revient à dire que la norme $N(\mathfrak{p}) = \#(\mathcal{O}_K/\mathfrak{p})$ d'un tel idéal $\mathfrak{p}$ est finie), et il en est de même dans $\mathcal{O}_L$ ([Lan94, I, Proposition 10]). Ainsi, si $\mathfrak{p}$ est un idéal premier de K et $\mathfrak{P}$ est un idéal premier de L au-dessus de $\mathfrak{p}$, alors on dispose d'une extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ de corps finis, où $\mathbb{F}_\mathfrak{P} := \mathcal{O}_L/\mathfrak{P}$ et $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. Une telle extension est toujours cyclique, son groupe de Galois étant engendré par l'automorphisme de Frobenius $x \mapsto x^{N(\mathfrak{p})}$. Comme L/K est galoisienne, il existe une manière de remonter cet automorphisme en un automorphisme de L/K. On introduit pour cela les sous-groupes suivant de $G = \mathrm{Gal}(L/K)$.

Définition 2.1. *Soit $\mathfrak{P}$ un idéal premier de L. On appelle **sous-groupe de décomposition** de $\mathfrak{P}$ le sous-groupe*

$$D_\mathfrak{P} := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

*et on appelle **sous-groupe d'inertie** de $\mathfrak{P}$ le sous-groupe*

$$\mathcal{I}_\mathfrak{P} := \{\sigma \in G \mid \forall x \in \mathcal{O}_L, \sigma(x) \equiv x \bmod \mathfrak{P}\}.$$

Par définition, tout élément σ de $D_\mathfrak{P}$ induit un élément $\overline{\sigma}$ de $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ défini par

$$\overline{x} \mapsto \overline{\sigma(x)}$$

où les barres désignent la réduction modulo $\mathfrak{P}$ dans $\mathcal{O}_L$ et l'application $\sigma \mapsto \overline{\sigma}$ est évidemment un morphisme de groupes de $D_\mathfrak{P}$ dans $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$, dont le noyau est $\mathcal{I}_\mathfrak{P}$. Ce morphisme est en fait surjectif ([Lan94, I, Proposition 14]).

Définition 2.2. *Soit $\mathfrak{p}$ un idéal premier de K et $\mathfrak{P}$ un idéal premier de L au-dessus de $\mathfrak{p}$. On appelle **automorphisme de Frobenius** de $\mathfrak{P}/\mathfrak{p}$ l'image réciproque $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ du Frobenius $x \mapsto x^{N(\mathfrak{p})} \in \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ dans $D_\mathfrak{P}/\mathcal{I}_\mathfrak{P}$. En particulier, si $\mathcal{I}_\mathfrak{P} = \{1_G\}$ alors $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}} \in G$.*

On voit immédiatement que $D_\mathfrak{P}$ constitue le stabilisateur de $\mathfrak{P}$ pour l'action de G sur les idéaux premiers de L au-dessus de $\mathfrak{p}$. Il vient donc que, si $\mathfrak{P}$ et $\mathfrak{P}'$ sont tous les deux au-dessus de $\mathfrak{p}$, alors $D_\mathfrak{P}$ et $D_{\mathfrak{P}'}$ sont conjugués (par un élément de G envoyant $\mathfrak{P}$ sur $\mathfrak{P}'$), et il en est de même pour $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ et $\mathrm{Frob}_{\mathfrak{P}'/\mathfrak{p}}$. De plus, la relation orbite-stabilisateur nous donne l'égalité

$$g(\mathfrak{p}) = \frac{\#G}{\#D_\mathfrak{P}},$$

où $g(\mathfrak{p})$ est le nombre d'idéaux premiers de L au-dessus de $\mathfrak{p}$. La relation bien connue $e(\mathfrak{p})f(\mathfrak{p})g(\mathfrak{p}) = \#G$, où $f(\mathfrak{p}) = [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}]$, implique donc que $\#D_\mathfrak{P} = ef$, et que $\#\mathcal{I}_\mathfrak{P} = e$, de sorte que $\mathfrak{p}$ est non ramifié dans L si et seulement si $\mathcal{I}_\mathfrak{P}$ est trivial.

Définition 2.3. *Soit $\mathfrak{p}$ un idéal premier de K non ramifié dans L. On appelle (classe d')**automorphisme de Frobenius** de $\mathfrak{p}$ la classe de conjugaison $\mathrm{Frob}_\mathfrak{p}$ de G formée des $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ pour $\mathfrak{P}$ parcourant l'ensemble des idéaux premiers de L au-dessus de $\mathfrak{p}$.*

Remarque 2.4. Lorsque l'on s'intéresse à des propriétés invariantes par conjugaison, on parlera abusivement du Frobenius de $\mathfrak{p}$ comme un élément de G. Si G est abélien, ses classes de conjugaison sont réduites à des singletons et $\mathrm{Frob}_\mathfrak{p}$ correspond donc à un élément de G.

Ainsi, si $\mathfrak{p}$ est non ramifié dans L, $\mathrm{Frob}_\mathfrak{p}$ est caractérisé comme étant la classe de conjugaison des $\sigma \in G$ tels qu'il existe $\mathfrak{P}$ premier dans L au-dessus de $\mathfrak{p}$ et pour tout $x \in \mathcal{O}_L, \sigma(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{P}$. De plus, on voit que $\mathrm{Frob}_\mathfrak{p}$ est d'ordre $f(\mathfrak{p}) = [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}]$, de sorte que $\mathfrak{p}$ est totalement décomposé dans L (c'est-à-dire admet $[L : K]$ facteurs premiers dans L) si et seulement si $\mathrm{Frob}_\mathfrak{p} = \{1_G\}$, et $\mathfrak{p}$ est inerte (c'est-à-dire est premier dans $\mathcal{O}_L$) si et seulement si $\mathrm{Frob}_\mathfrak{p} = D_\mathfrak{p}$.

Exemples 2.5.

i) Si $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z}$ est sans facteur carré, alors $\mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma\}$ où $\sigma : \sqrt{d} \mapsto -\sqrt{d}$ est d'ordre 2. Le discriminant de L/K est d si $d \equiv 1 \bmod 4$ et $4d$ sinon, de sorte que les premiers ramifiés sont les facteurs premiers de d, et 2 si $d \equiv 2, 3 \bmod 4$. Si p est un nombre premier non ramifié dans L, alors le critère de Dedekind ([Lan94, I, Proposition 23]) nous dit que p admet autant de facteurs premiers dans L que le polynôme $X^2 - d$ admet de facteurs irréductibles dans $\mathbb{F}_p$. Il vient donc que

$$\mathrm{Frob}_p = \begin{cases} \mathrm{id} \text{ si } \left(\frac{d}{p}\right) = 1 \\ \sigma \text{ si } \left(\frac{d}{p}\right) = -1. \end{cases}$$

ii) Si $K = \mathbb{Q}$ et $L = \mathbb{Q}(\zeta_q)$, où ζ_q est une racine primitive q-ième de l'unité alors $\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ via $a \mapsto \sigma_a : \zeta_q \mapsto \zeta_q^a$, et les seuls premiers ramifiés dans L sont les facteurs premiers de q ([Lan94, IV, Theorem 2]). Si p ne divise pas q alors, puisque $\mathcal{O}_L = \mathbb{Z}[\zeta_q]$ ([Lan94, IV, Theorem 4]), on a, pour tout idéal premier $\mathfrak{P}$ de L divisant p et tout $x = \sum_{i=0}^{\varphi(q)} a_i \zeta_q^i \in \mathbb{Z}[\zeta_q]$,

$$\begin{aligned} \mathrm{Frob}_\mathfrak{P}(x) &\equiv \left(\sum_{i=0}^{\varphi(q)} a_i \zeta_q^i\right)^p \bmod \mathfrak{P} \\ &\equiv \sum_{i=0}^{\varphi(q)} a_i^p \zeta_q^{ip} \bmod \mathfrak{P} \\ &\equiv \sum_{i=0}^{\varphi(q)} a_i \zeta_q^{ip} \bmod \mathfrak{P} \\ &\equiv \sigma_a(x) \bmod \mathfrak{P} \end{aligned}$$

où $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ est tel que $p \equiv a \bmod q$. On en déduit donc que $\mathrm{Frob}_p = \sigma_a$, autrement dit l'automorphisme de Frobenius de p est entièrement déterminé par la classe de p modulo q.

iii) Soit K un corps de nombres, et $L := H_K$ le corps de classes de Hilbert de K. L'extension L/K est caractérisée comme étant l'extension abélienne non ramifiée maximale de K. De plus, l'application d'Artin (prolongement de l'application $\mathfrak{p} \mapsto \mathrm{Frob}_\mathfrak{p}$ à toutes les classes d'idéaux fractionnaires de K) réalise un isomorphisme entre le groupe $\mathcal{C}\ell(K)$

des classes d'idéaux fractionnaires de K et $\mathrm{Gal}(H_K/K)$ ([Lan94, XI, §5]). En particulier, $\mathfrak{p}$ est principal si et seulement si $\mathrm{Frob}_\mathfrak{p} = 1_G$.

2.1.2 Théorie des représentations

Toutes les démonstrations connues du théorème de la progression arithmétique de Dirichlet et du théorème des nombres premiers en progressions arithmétiques utilisent de manière cruciale les caractères de Dirichlet et leurs relations d'orthogonalité qui permettent de détecter analytiquement une congruence $p \equiv a \bmod q$. On peut dire qu'il s'agit de faire de l'analyse harmonique discrète sur des groupes abéliens finis.

Dans la situation qui nous intéresse désormais, les groupes considérés, qui sont des groupes de Galois d'extensions de corps de nombres, sont en général non abéliens. Il convient donc, pour notamment détecter analytiquement la condition $\mathrm{Frob}_\mathfrak{p} = C$, où C est une classe de conjugaison d'un tel groupe de Galois, de développer une théorie analogue à celle des caractères de Dirichlet, adaptée à ce contexte non abélien. C'est la théorie des représentations linéaires complexes qui joue ce rôle, cette théorie pouvant être vue comme de l'analyse harmonique sur les groupes finis. On renvoie le lecteur aux excellents livres d'Isaacs [Isa94] et de Serre [Ser98] pour les démonstrations des résultats de cette section.

Définition 2.6. *Soit G un groupe fini. On appelle **représentation linéaire complexe** de G (ou pour faire court, représentation de G) tout morphisme de groupes $\rho : G \longrightarrow \mathbf{GL}(V)$, où V est un $\mathbb{C}$-espace vectoriel de dimension finie. Si ρ est une représentation de G, son **caractère** χ est l'application*

$$\begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ g & \mapsto & \mathrm{tr}(\rho(g)). \end{array}$$

*La représentation (ρ, V) de G est dite **réductible** s'il existe deux sous-espaces vectoriels V_1, V_2 de V tels que $V_1, V_2 \neq \{0\}, V = V_1 \oplus V_2$ et $\rho(G)(V_i) \subset V_i$ pour $i = 1, 2$. On dit que (ρ, V) est **irréductible** dans le cas contraire, et on appelle **caractère irréductible** de G le caractère d'une telle représentation de G. L'ensemble des caractères irréductibles de G est noté* $\mathrm{Irr}(G)$. *Le **degré** du caractère χ est $\chi(1_G) = \dim V$.*

*Deux représentations (ρ_1, V_1) et (ρ_2, V_2) sont **isomorphes** lorsqu'il existe un isomorphisme $f : V_1 \longrightarrow V_2$ tel que pour tout $g \in G$, $f \circ \rho_1(g) = \rho_2(g) \circ f$.*

Remarque 2.7. On pourrait employer le langage des modules, une représentation de G n'étant rien d'autre que la donnée d'un $\mathbb{C}[G]$-module, où $\mathbb{C}[G]$ est l'algèbre du groupe G, c'est-à-dire l'ensemble des combinaisons linéaires formelles à coefficients dans $\mathbb{C}$ d'éléments de G, muni des opérations usuelles. Étant donné que nous n'avons pas besoin d'aller très loin dans la théorie des représentations, on préfère utiliser le point de vue d'action linéaire de G sur un $\mathbb{C}$-espace vectoriel.

Dans la suite, on identifiera sans plus de précisions des représentations isomorphes. L'intérêt de la notion de représentation irréductible est le théorème suivant, propre à la caractéristique zéro.

Théorème 2.8 (Maschke)**.** *Toute représentation d'un groupe fini est semi-simple, c'est-à-dire qu'elle se décompose sous la forme d'une somme directe de représentations irréductibles.*

Ainsi, il est très souvent suffisant de se ramener à des représentations irréductibles pour étudier des représentations générales.

Proposition 2.9. *Soit G un groupe fini. Les caractères irréductibles de G forment une base orthonormée de l'ensemble des fonctions centrales sur G, c'est-à-dire $\{f : G \longrightarrow \mathbb{C} \mid \forall g, h \in G, f(ghg^{-1}) = f(h)\}$, pour le produit scalaire*

$$(f, g) \mapsto \langle f, g\rangle := \frac{1}{|G|}\sum_{h\in G} f(h)\overline{g(h)}.$$

On dispose des formules d'orthogonalité suivantes : pour tout $\chi, \chi' \in \mathrm{Irr}(G)$,

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\chi'(g)} = \begin{cases} 1 \text{ si } \chi = \chi' \\ 0 \text{ sinon.}\end{cases}$$

et pour tout $g, g' \in G$,

$$\sum_{\chi\in\mathrm{Irr}(G)}\chi(g)\overline{\chi(g')} = \begin{cases} \frac{|G|}{|C|} \text{ si } g \text{ et } g' \text{ engendrent la même classe de conjugaison } C \\ 0 \text{ sinon.}\end{cases}$$

Les formules d'orthogonalité ci-dessus sont fondamentales pour notre étude : elles permettront de détecter analytiquement l'appartenance à une classe de conjugaison donnée, et donc de détecter les idéaux premiers dont l'automorphisme de Frobenius correspond à une telle classe. Combinée au Théorème de Maschke, la Proposition précédente implique le résultat suivant.

Corollaire 2.10. *Deux représentations d'un groupe fini ayant le même caractère sont isomorphes.*

Par la suite on pourra donc parler sans distinction de caractères ou de représentations d'un tel groupe.

Partant d'une représentation (ρ, V) de G, et étant donné un sous-groupe H de G, on dispose naturellement d'une représentation $\mathrm{Res}^G_H \rho$ par restriction de ρ à H. Dans le sens inverse, on peut construire naturellement une représentation de G à partir d'une représentation de H.

Définition 2.11. *Soit G un groupe fini et H un sous-groupe de G. Si (ρ, W) est une représentation de H, on définit la* ***représentation induite*** $\mathrm{Ind}^G_H \rho$ *par ρ sur G de la manière suivante : on fixe un système $(\sigma_i)_i$ de représentants de G/H et on pose $V = \oplus_i W_i$ avec $W_i = W$. Alors pour $v \in W_i$ et $g = \sigma_j h$ avec $h \in H$, on définit l'action de g sur v par*

$$\mathrm{Ind}^G_H(g)v := f_{i,j}(\rho(h)v)$$

où $f_{i,j} : W_i \longrightarrow W_k$ correspond à l'identité sur W, et k est tel que $\sigma_i\sigma_j H = \sigma_k H$.

De manière plus visuelle, la représentation induite est construire « par blocs ». On écrit tout élément de G sous la forme $\sigma_i h$ avec $h \in H$, on fait agir h localement sur l'espace W, puis on envoie les blocs W indexés par G/H les uns sur les autres, cette dernière étape étant déterminée par l'action par multiplication à gauche de G sur G/H.

Remarques 2.12.

i) La représentation ainsi construite ne dépend pas, à isomorphisme près, du système de représentants de G/H choisi.
ii) De manière plus abstraite, si W est un $\mathbb{C}[H]$-module, on peut définir la représentation induite induite associée par $\mathbb{C}[G] \otimes W$.

Exemple 2.13. Soit $\mathbf{1}$ le caractère unité du sous-groupe $\{1_G\}$ de G. Alors $\mathrm{Ind}_H^G \mathbf{1} = \mathrm{reg}_G$, la représentation régulière de G définie par l'action de multiplication à gauche dans l'algèbre $\mathbb{C}[G]$. En effet, l'espace W est ici une droite vectorielle, et le quotient $G/\{1_G\}$ s'identifie à G.

Proposition 2.14. *Soit ρ une représentation de H de caractère χ. Le caractère de $\mathrm{Ind}_H^G \rho$ est*

$$\mathrm{Ind}_H^G \chi : g \mapsto \frac{1}{|H|} \sum_{s \in G} \dot{\chi}(s^{-1}gs),$$

où $\dot{\chi}$ est le prolongement par zéro de χ à G tout entier.

Terminons cette partie par un théorème de Brauer qui nous sera très utile pour obtenir des informations sur les fonctions L d'Artin en général.

Théorème 2.15 (Brauer)**.** *Tout caractère de G est combinaison linéaire à coefficients entiers de caractères induits de caractères de degré* 1*.*

Remarques 2.16.
i) Ce théorème améliore d'une certaine manière un résultat antérieur d'Artin, énonçant le fait que tout caractère de G est combinaison linéaire à coefficients rationnels de caractères induits de sous-groupes cycliques. Nous verrons dans la prochaine partie en quoi le théorème de Brauer est meilleur en vue des applications aux fonctions L d'Artin.
ii) Le théorème de Brauer est en fait légèrement plus précis. Les caractères de degré 1 en question sont des caractères de groupes dits élémentaires, c'est-à-dire produits directs d'un p-groupe et d'un groupe cyclique d'ordre premier à p, avec p un nombre premier.

2.1.3 Fonctions L d'Artin

On introduit maintenant les généralisations des fonctions L de Dirichlet, appelées fonctions L d'Artin, dont les propriétés analytiques régissent la répartition des automorphismes de Frobenius.

Fixons une extension galoisienne de corps de nombres L/K, de groupe de Galois G.

Définition 2.17. *Soit ρ une représentation de G, de caractère χ. Pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ et $s \in \mathbb{C}$, on définit le* ***facteur local d'Artin*** *en $\mathfrak{p}$ de la manière suivante :*

$$L_{\mathfrak{p}}(s, \chi, L/K) = \det\left(\left(\mathrm{id}_V - \rho(\mathrm{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s}\right)_{|V^{\mathcal{I}_{\mathfrak{p}}}}\right)^{-1}$$

où $\mathcal{I}_\mathfrak{p}$ désigne le groupe d'inertie de l'un des premiers de L au-dessus de $\mathfrak{p}$ et $V^{\mathcal{I}_\mathfrak{p}}$ est le sous-espace de V constitué des éléments invariants par $I_\mathfrak{p}$. En particulier, si $\mathfrak{p}$ est non ramifié dans L (c'est-à-dire si $\mathcal{I}_\mathfrak{p}$ est réduit à $\{1_G\}$) alors

$$L_\mathfrak{p}(s, \chi, L/K) = \det(\mathrm{id}_V - \rho(\mathrm{Frob}_\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}.$$

Remarques 2.18.

i) Cette définition ne dépend pas du choix de l'élément de Frobenius associé à $\mathfrak{p}$ dans G (ou dans $G/\mathcal{I}_\mathfrak{p}$ dans le cas ramifié) car le déterminant, et donc le polynôme caractéristique, est invariant par conjugaison.

ii) Comme χ détermine ρ à conjugaison près, il n'y a pas d'ambigüité en notant ceci comme une fonction de χ.

iii) Certains auteurs, dont Artin lui-même, définissent les fonctions L d'Artin à travers une série de Dirichlet exprimant $\log L(s, \chi)$. Ces définitions sont bien sûr équivalentes.

À partir de ces facteurs locaux, on construit une fonction L « globale », comme pour la plupart des fonctions L utilisées en théorie des nombres.

Définition 2.19. *Soit χ un caractère de G. La **fonction L d'Artin** associée à ce caractère est définie par*

$$L(s, \chi, L/K) = \prod_\mathfrak{p} L_\mathfrak{p}(s, \chi, L/K)$$

avec $s \in \mathbb{C}$.

Proposition 2.20. *Soit χ un caractère de G. Alors $s \mapsto L(s, \chi, L/K)$ est définie et holomorphe sur le demi-plan $\{s \in \mathbb{C} \mid \mathfrak{Re}(s) > 1\}$.*

Démonstration. Notons ρ une représentation associée à χ. Si $\mathfrak{p}$ est un idéal premier de K, soit $\lambda_1, \ldots, \lambda_n$ les valeurs propres de $\rho(\mathrm{Frob}_\mathfrak{p})_{|V^{I_\mathfrak{p}}}$. Alors pour tout $s \in \mathbb{C}$ on a

$$\left|\det\left(\left(\mathrm{id}_V - \rho(\mathrm{Frob}_\mathfrak{p})N(\mathfrak{p})^{-s}\right)_{|V^{I_\mathfrak{p}}}\right)\right| = \prod_{i=1}^{n} |1 - \lambda_i N(\mathfrak{p})^{-s}| \geq \prod_{i=1}^{n} (1 - N(\mathfrak{p})^{-\mathfrak{Re}(s)}),$$

car les λ_i sont d'ordre fini donc sont des racines de l'unité dans $\mathbb{C}$ et $|N(\mathfrak{p})^{-s}| = N(\mathfrak{p})^{-\mathfrak{Re}(s)}$. La convergence uniforme sur tout compact de $\{s \in \mathbb{C} \mid \mathfrak{Re}(s) > 1\}$ de la série de fonctions

$$\sum_\mathfrak{p} \frac{1}{N(\mathfrak{p})^s}$$

donne le résultat. □

Exemples 2.21.

i) On a pour tout corps de nombres K et tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$,

$$L(s, \chi_0, K/K) = \prod_\mathfrak{p} (1 - N(\mathfrak{p})^{-s})^{-1} = \zeta_K(s),$$

où χ_0 désigne le caractère trivial de $\mathrm{Gal}(K/K)$.

ii) On considère $L = \mathbb{Q}(\zeta_q)$ où ζ_q est une racine primitive q-ième de l'unité et $K = \mathbb{Q}$. Alors les caractères irréductibles du groupe de Galois $\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ sont les caractères de Dirichlet modulo q et l'on a vu précédemment que l'élément de Frobenius correspondant au nombre premier $p \equiv a \bmod q$ est $\sigma_a : \zeta_q \mapsto \zeta_q^a$. Les premiers ramifiés étant exactement ceux divisant q, on obtient pour $\mathfrak{Re}(s) > 1$,

$$L(s, \chi, L/K) = \prod_{p \nmid m} (1 - \chi(p)p^{-s})^{-1} \times P = L(s, \chi) \times P(s),$$

où $L(s, \chi)$ désigne la série L de Dirichlet traditionnelle, et $P(s)$ désigne un produit eulérien fini.

Plus généralement, si L/K est abélienne, la théorie du corps de classes, et plus précisément la loi de réciprocité d'Artin, permet d'identifier le groupe $\mathrm{Gal}(L/K)$ avec un groupe de classes généralisées $I_K(\mathfrak{f})/H$, où $\mathfrak{f}$ est le conducteur de l'extension L/K, et donc d'identifier leurs groupes de caractères (au sens des groupes abéliens, donc caractères de degré 1). Une fois cette identification faite, on voit que les facteurs locaux de nos fonctions L d'Artin ne sont rien d'autre que les facteurs locaux des fonctions L de Hecke associées à ces mêmes caractères, et ces fonctions L coïncident donc (voir [Lan02, XII, Theorem 2]). Or Hecke (et plus tard Tate par d'autres méthodes) a montré que ces fonctions L admettent un prolongement méromorphe à $\mathbb{C}$ avec 1 pour unique pôle si le caractère en question est trivial, et qu'elles vérifient une équation fonctionnelle similaire à celle vérifiée par les fonctions L de Dirichlet (voir [Lan02, XIII, §3]). Nous verrons plus loin comment ces résultats sont utilisés pour montrer des propriétés similaires pour les fonctions L d'Artin générales.

La proposition suivante (voir [Lan02, p.233]) résume les propriétés fondamentales des fonctions L d'Artin vis-à-vis des opérations sur les caractères. Elle se démontre en considérant chaque facteur local séparément.

Proposition 2.22. *Les fonctions L d'Artin vérifient les propriétés suivantes :*

i) Additivité : Si χ_1 et χ_2 sont des caractères de G alors pour tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$, $L(s, \chi_1 + \chi_2, L/K) = L(s, \chi_1, L/K)L(s, \chi_2, L/K)$.

ii) Inflation : Si H est un sous-groupe distingué de G, et χ est un caractère de G/H, alors pour tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$, $L(s, \chi, L^H/K) = L(s, \pi_H \circ \chi, L/K)$, où $\pi_H : G \twoheadrightarrow G/H$ est la projection dans le quotient.

iii) Induction : Si $K \subset M \subset L$ avec $\mathrm{Gal}(L/M) = H$ et χ est un caractère de H, on a pour tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$, $L(s, \chi, L/M) = L(s, \mathrm{Ind}_H^G \chi, L/K)$.

La première propriété ci-dessus, combinée au théorème de Maschke, montre que toute fonction L d'Artin se décompose comme produit de fonctions L d'Artin associée à des caractères irréductibles, et l'étude des premières se ramènent donc souvent à l'étude des secondes.

Les deux autres propriétés, et notamment la dernière, sont également fondamentales. En effet, posons L^+ la clôture galoisienne de L sur $\mathbb{Q}$, $G^+ := \mathrm{Gal}(L^+/\mathbb{Q})$ et $\tilde{G} := \mathrm{Gal}(L^+/K)$. Si χ est un caractère de G, on sait d'après *ii)* ci-dessus que

$$L(s, \chi, L/K) = L(s, \tilde{\chi}, L^+/K)$$

où $\tilde{\chi}$ est le caractère $\chi \circ \pi_G$, avec $\pi_G : \tilde{G} \twoheadrightarrow G$ la projection dans le quotient (si $L/\mathbb{Q}$ est déjà galoisienne, cette étape est vide). Ensuite, la propriété *iii)* nous donne que

$$L(s, \chi, L/K) = L(s, \mathrm{Ind}_{\tilde{G}}^{G^+} \tilde{\chi}, L^+/\mathbb{Q}).$$

Pour finir, cette dernière fonction L s'exprime, d'après la propriété *i)* comme produit de fonctions L d'Artin associées à des caractères irréductibles de G^+. Ainsi, toute fonction L d'Artin s'exprime comme produit de fonctions L associées à des caractères irréductibles d'extensions de $\mathbb{Q}$. Cette observation importante motivera le choix des hypothèses d'indépendance linéaire portant sur les zéros de telles fonctions L dans la suite.

Exemple 2.23. Pour $\mathfrak{Re}(s) > 1$, écrivons

$$\begin{aligned}
\zeta_L(s) &= L(s, \chi_0, L/L) \\
&= L(s, \mathrm{Ind}_{\{\mathrm{id}_L\}}^{G} \chi_0, L/K) \\
&= L(s, \mathrm{reg}_G, L/K) \\
&= \prod_{\chi \in \mathrm{Irr}(G)} L(s, \chi, L/K)^{\chi(1)} \\
&= \zeta_K(s) \prod_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi \neq \mathbf{1}}} L(s, \chi, L/K)^{\chi(1)}.
\end{aligned}$$

On voit ainsi apparaître un lien entre les fonctions zêta de Dedekind de nos deux corps de nombres. C'est en observant de telles factorisations de fonctions zêta d'extensions abéliennes de $\mathbb{Q}$ qu'Artin en est venu à définir ses fonctions L.

Une autre conséquence importante de la propriété d'induction est la suivante :

Proposition 2.24. *Toute fonction L d'Artin admet un prolongement méromorphe à $\mathbb{C}$.*

Démonstration. Par le théorème de Brauer, on peut écrire tout caractère χ de G sous la forme

$$\chi = \sum_{i \in S} m_i \, \mathrm{Ind}_{H_i}^{G} \chi_i,$$

où $(H_i)_{i \in S}$ est une famille de sous-groupes élémentaires de G et les χ_i sont des caractères de degré 1. Ainsi, on a pour tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$,

$$L(s, \chi, L/K) = \prod_{i \in S} L(s, \chi_i, L/L^{H_i})^{m_i}.$$

Or les extensions L/L^{H_i} sont abéliennes. Les fonctions L apparaissant dans ce produit s'identifient donc à des fonctions L de Hecke, et admettent donc un prolongement méromorphe à $\mathbb{C}$. Les puissances étant des entiers relatifs, on obtient que notre fonction L est bien méromorphe sur $\mathbb{C}$. □

Remarque 2.25. Le théorème d'Artin cité dans la Remarque 2.16 *i)* ne nous aurait pas permis d'obtenir un résultat aussi fort. En effet, la présence de coefficients rationnels n'implique

a priori la méromorphie que d'une puissance convenable de nos fonctions L.

Notons qu'il s'agit d'un prolongement méromorphe et pas, *a priori*, holomorphe. En réalité, l'holomorphie des fonctions L d'Artin hors de l'éventuel pôle 1 est un problème largement ouvert, appelé la conjecture d'Artin.

Conjecture 2.26 (Artin)**.** *Soit χ un caractère de G. Alors le seul pôle éventuel de la fonction $s \mapsto L(s,\chi)$ est 1, avec multiplicité exactement $\langle \chi, \chi_0 \rangle$.*

Grâce à la décomposition des caractères de G dans la base orthonormée des caractères irréductibles, on voit qu'il est équivalent de dire que la fonction L d'Artin de n'importe quel caractère irréductible non trivial est holomorphe sur $\mathbb{C}$. La conjecture d'Artin est connue au moins pour les caractères de degré 1 grâce aux travaux de Hecke dont on a parlé précédemment. Par induction, la conjecture est vraie pour tout caractère qui est combinaison linéaire à coefficients entiers naturels de caractères « monomiaux », c'est-à-dire induit par des caractères de degré 1. La conjecture d'Artin est ainsi connue pour certaines familles de groupes de Galois, dont ceux du type suivant ([BDJ+82, Chapter 2, Corollary 3.5]).

Proposition 2.27. *Supposons que G soit super-résoluble, c'est-à-dire tel qu'il existe des sous-groupes $G_1, \dots, G_r$ tels que $\{1_G\} = G_1 \lhd \dots \lhd G_r = G$ et G_{i+1}/G_i est cyclique pour tout $i \in \{1, \dots, r-1\}$. Alors la conjecture d'Artin est vraie pour toute fonction L d'Artin associée à un caractère de G.*

La conjecture d'Artin serait notamment conséquence de la (conjecturale) loi de réciprocité de Langlands (voir par exemple [BCdS+03, Chapter 9]), qui prévoit que toute fonction L d'Artin est la fonction L d'une représentation cuspidale automorphe.

L'analogie entre les fonctions L d'Artin et les fonctions zêta de Dedekind va plus loin que le prolongement méromorphe : celles-ci vérifient une certaine équation fonctionnelle reliant leurs valeurs en s aux valeurs en $1-s$ de la fonction L associée à la représentation duale (ou au caractère conjugué, ce qui est équivalent). Pour en parler, il faut compléter ces fonctions par des facteurs correspondant aux places infinies et un facteur exponentiel.

Définition 2.28. *On définit les fonctions $\Gamma_{\mathbb{R}}$ et $\Gamma_{\mathbb{C}}$ par*

$$\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)$$

et

$$\Gamma_{\mathbb{C}}(s) := 2(2\pi)^{-s}\Gamma(s).$$

*Si (χ, V) est un caractère de G, on définit le **facteur local** d'Artin associé à la valeur absolue archimédienne v de K par*

$$L_v(s,\chi,L/K) = \begin{cases} \Gamma_{\mathbb{R}}(s)^{\dim V^{D_v}}\Gamma_{\mathbb{R}}(s+1)^{\operatorname{codim} V^{D_v}} & \text{si } v \text{ est réelle} \\ \Gamma_{\mathbb{C}}(s)^{\chi(1)} & \text{si } v \text{ est complexe} \end{cases},$$

où D_v est le sous-groupe de décomposition de v, trivial si v s'étend en une place réelle dans L, et $D_v = \{\mathrm{id}, c\}$ sinon, où c est la conjugaison complexe. Enfin, on pose $A(\chi) = d_K^{\chi(1)} N_{K/\mathbb{Q}}(\mathfrak{f}_\chi)$,

où d_K est le discriminant de K et $\mathfrak{f}_\chi$ est le ***conducteur d'Artin*** *de χ (voir ci-dessous). La* ***fonction L d'Artin complétée*** *est la fonction*

$$\Lambda(s,\chi,L/K) := A(\chi)^{s/2}L(s,\chi,L/K)\prod_{v|\infty}L_v(s,\chi,L/K).$$

Le conducteur d'Artin d'un caractère de G est défini à l'aide des sous-groupes de ramification supérieure de G. On en trouvera une définition et quelques propriétés importantes utilisées dans la suite dans la section 2.3.2.1.

Toutes ces définitions servent à donner une expression très simple de l'équation fonctionnelle satisfaite par nos fonctions L d'Artin. Les fonctions Λ jouent le rôle de la fonction Ξ pour la fonction ζ. L'équation fonctionnelle se démontre en se ramenant à des fonctions L de Hecke comme précédemment par le théorème de Brauer et prend la forme suivante ([MM97, p.28]).

Théorème 2.29. *La fonction L d'Artin complétée associée au caractère χ de G vérifie*

$$\Lambda(s,\chi,L/K) = W(\chi)\Lambda(1-s,\overline{\chi},L/K)$$

pour tout $s\in\mathbb{C}$ où elle est définie, avec $W(\chi)$ un nombre complexe de module 1 appelé le « root number » de χ.

Le root number est un invariant en général mal connu. Dans tous les cas, si on a $W(\chi) = -1$ alors il est facile de voir (en utilisant le fait que les fonctions Gamma et exponentielle ne s'annulent jamais) que $L(1/2,\chi,L/K) = 0$. Il se trouve qu'un telle annulation en $1/2$ peut avoir une influence sur le biais de Tchebychev dans le contexte de la répartition des automorphismes de Frobenius dans les groupes de Galois de corps de nombres. L'objectif de l'article [Bai19], reproduit dans la section 2.3, est de mettre ce phénomène en évidence.

2.1.4 Théorème de Chebotarev

L'étude des propriétés analytiques des fonctions L d'Artin mène à la démonstration du théorème suivant.

Théorème 2.30 (Chebotarev)**.** *Soit C une classe de conjugaison de G. Alors*

$$\pi(x,C,L/K) \underset{x\to+\infty}{\sim} \frac{\#C}{\#G}\operatorname{Li}(x).$$

Remarques 2.31.

i) En réalité, Chebotarev avait seulement montré le résultat plus faible

$$\frac{\sum_{\mathfrak{p},\mathrm{Frob}_\mathfrak{p}=C}\frac{1}{N(\mathfrak{p})^s}}{\sum_\mathfrak{p}\frac{1}{N(\mathfrak{p})^s}} \underset{s\to1}{\longrightarrow} \frac{\#C}{\#G},$$

avec une densité de Dirichlet plutôt qu'une densité naturelle, tout comme Dirichlet avait obtenu son théorème de la progression arithmétique soixante ans avant la démonstration du théorème des nombres premiers en progressions arithmétiques. Le

passage à la densité naturelle a été obtenu par Hecke ([SL96]). Dans tous les cas, le résultat de Chebotarev implique en particulier que chaque classe de conjugaison de G est de la forme $\mathrm{Frob}_{\mathfrak{p}}$ avec $\mathfrak{p}$ premier de K, ce qui, dans le cas d'une extension abélienne, correspond à la surjectivité de l'application d'Artin. Ceci permit à Artin de terminer la démonstration de sa loi de réciprocité dans le cas général ([Mar77, I, §4]).

ii) Le théorème de Chebotarev avait été conjecturé par Frobenius, qui était parvenu à un résultat plus faible : pour tout sous-groupe cyclique H de G, il existe une infinité de premiers $\mathfrak{p}$ de K tels que $\mathrm{Frob}_{\mathfrak{p}}$ engendre H (voir [Mar77, I, §1]).

L'idée de la démonstration du théorème de Chebotarev est très proche de celle de la démonstration du théorème des nombres premiers dans les progressions arithmétiques de de la Vallée-Poussin. On se ramène à montrer l'estimation

$$\psi(x, C, L/K) := \sum_{N(\mathfrak{p})^m \leq x, \mathrm{Frob}_{\mathfrak{p}}^m = C} \log N(\mathfrak{p}) \underset{x \to +\infty}{\sim} \frac{\#C}{\#G} x$$

par sommation par parties. En utilisant les relations d'orthogonalité, on décompose $\psi(x, C, L/K)$ comme une combinaison linéaire de fonctions sommatoires que l'on réécrit chacune par la formule de Perron comme une intégrale sur une droite verticale de $-\frac{L'}{L}(s, \chi, L/K)\frac{x^s}{s}$, pour χ variant dans $\mathrm{Irr}(G)$. On déplace le contour d'intégration « vers la gauche » pour récupérer les contributions des zéros et des pôles de ces fonctions. Une région sans zéros pour ζ_L implique une région sans zéros pour les $L(s, \chi, L/K)$ à cause de la factorisation de l'Exemple 2.23, et on termine la démonstration en rassemblant convenablement les termes d'erreur. Il est remarquable qu'il est inutile de supposer la conjecture d'Artin dans cet argument : on se ramène en fait à une sous-extension cyclique L/E de L/K, où $\mathrm{Gal}(L/E)$ est engendré par un élément quelconque de C. L'holomorphie des $L(s, \chi, L/E)$ (sauf pour $L(s, \chi_0, L/E) = \zeta_E(s)$ en 1), pour χ variant dans $\mathrm{Irr}(\mathrm{Gal}(L/E))$ permet de mener le raisonnement jusqu'au bout.

Cette stratégie mène à l'estimation inconditionnelle suivante, obtenue dans [LO77].

Théorème 2.32 (Lagarias, Odlyzko)**.** *Il existe des constantes absolues explicitement calculables $c_1, c_2 > 0$ telles que pour toute classe de conjugaison C de G et tout $x \geq \exp(10[L : \mathbb{Q}](\log d_L)^2)$ on a*

$$\left|\pi(x, C, L/K) - \frac{\#C}{\#G}\,\mathrm{Li}(x)\right| \leq \frac{\#C}{\#G}\,\mathrm{Li}(x^{\beta_0}) + c_1 x \exp(-c_2[L : \mathbb{Q}]^{-1/2}(\log x)^{1/2}),$$

où d_L désigne le discriminant absolu de L et $1 - \frac{1}{4\log d_L} \leq \beta_0 \leq 1$ est un zéro de Siegel exceptionnel de ζ_L (si un tel zéro n'existe pas, le terme $\frac{\#C}{\#G}\,\mathrm{Li}(x^{\beta_0})$ n'intervient pas).

En supposant l'hypothèse de Riemann pour ζ_L on obtient l'estimation plus précise suivante ([Ser81, Théorème 4]).

Théorème 2.33 (Lagarias, Odlyzko, Serre)**.** *Supposons l'hypothèse de Riemann pour ζ_L. Alors pour toute classe de conjugaison C de G et tout $x > 2$ on a*

$$\left|\pi(x, C, L/K) - \frac{\#C}{\#G}\,\mathrm{Li}(x)\right| = O\left(\frac{\#C}{\#G} x^{1/2} \log(d_L x^{[L:\mathbb{Q}]})\right).$$

2.2 Courses d'idéaux premiers dans les corps de nombres

On fixe toujours un extension galoisienne L/K de corps de nombres, de groupe de Galois G. On développe dans cette section l'adaptation, dûe à Ng ([Ng00]), des idées de Rubinstein et Sarnak pour les courses entre idéaux premiers dans l'extension L/K.

On souhaite désormais étudier des courses d'idéaux premiers de K dont les Frobenius sont des classes de conjugaison de G. À cause du théorème de Chebotarev, on voit que, pour que les courses soient équilibrées, il faut renormaliser les fonctions de comptage. On va donc comparer les quantités $\frac{\pi(x,C_1,L/K)}{\#C_1}$ et $\frac{\pi(x,C_2,L/K)}{\#C_2}$, et comme précédemment on s'intéresse à la fréquence à laquelle une inégalité de la forme

$$\frac{\pi(x,C_1,L/K)}{\#C_1} \leqslant \frac{\pi(x,C_2,L/K)}{\#C_2}$$

se produit.

Si $C_1,\dots,C_D$ sont des classes de conjugaison de G, on définit, si la limite existe,

$$\delta(L/K;C_1,\dots,C_D) := \lim_{X\to+\infty} \frac{1}{X}\int_0^X \mathbf{1}_{\frac{\pi(e^t,C_1,L/K)}{\#C_1}>\dots>\frac{\pi(e^t,C_D,L/K)}{\#C_D}}\,\mathrm{d}t$$

la densité logarithmique associée. Notre but est d'établir l'existence de cette quantité et de l'étudier, sous des hypothèses convenables.

2.2.1 Formule explicite

Notre porte d'entrée est une nouvelle fois une formule explicite pour ces fonctions de comptage, faisant intervenir les zéros des fonctions L d'Artin.

Théorème 2.34. *Soit C une classe de conjugaison de G. Supposons l'hypothèse de Riemann pour ζ_L et la conjecture d'Artin pour les fonctions L d'Artin associées aux caractères irréductibles de G. Alors on a*

$$\frac{\log x}{\sqrt{x}}\left(\frac{\#G}{\#C}\pi(x,C,L/K)-\pi_K(x)\right) = 1-\frac{\#(C^{1/2})}{\#C} - \sum_{\chi\in\mathrm{Irr}(G)}\overline{\chi(C)}\sum_{\gamma_\chi}\frac{x^{i\gamma_\chi}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{\log x}\right),$$

où

$$C^{1/2} := \{g\in G \mid g^2\in C\},$$

$$\pi_K(x) := \#\{\mathfrak{p} \text{ premier de } K \mid N(\mathfrak{p})\leq x\}$$

et la sommation sur γ_χ se fait sur le (multi-)ensemble des zéros non triviaux de $L(s,\chi,L/K)$.

Remarques 2.35.

i) La raison de l'utilisation de l'hypothèse de Riemann pour ζ_L (et donc pour les fonctions L d'Artin associées aux caractères irréductibles de G) est claire : elle induit la renormalisation par $\frac{\sqrt{x}}{\log x}$. L'emploi de la conjecture d'Artin est peut-être plus mystérieuse ici. En suivant [LO77, §7], la formule ci-dessus est obtenue à partir d'une formule explicite pour $\psi(x,C,L/K)$ par sommation par parties. Pour étudier cette dernière

quantité, on utilise la formule de Perron, faisant intervenir les intégrales sur des segments verticaux (disons entre les parties imaginaires $-T$ et T) des $-\frac{L'}{L}(s,\chi,L/K)$ pour χ parcourant $\mathrm{Irr}(G)$. On déplace ces segments « vers la gauche », captant ainsi par le théorème des résidus les contributions des zéros et pôles de $L(s,\chi,L/K)$ qui sont les pôles de $\frac{L'}{L}(s,\chi,L/K)$. Comme expliqué dans [Bel16, Remarque 12], il faudrait alors disposer de majorations du nombre de zéros et de pôles de $L(s,\chi,L/K)$ sur un segment $-T \leq \mathfrak{Im}(s) \leq T$ pour terminer la démonstration, mais les techniques usuelles basées sur le principe de l'argument ne permettent que d'obtenir une estimation de la différence entre ces deux quantités. Il se pourrait donc que le nombre de zéros soit tel que le terme d'erreur dans l'estimation « à hauteur T » soit plus grand que le terme principal.

ii) Dans [FJ20a], on peut trouver une formule explicite ne nécessitant pas l'hypothèse de Riemann ([FJ20a, Corollary 3.10, (38)]), faisant intervenir la borne supérieure β_L des parties réelles des zéros de ζ_L, et également une formule explicite ne nécessitant pas la conjecture d'Artin ([FJ20a, Corollary 3.10, (37)]). Cette dernière formule est établie à l'aide du même « transfert » à une sous-extension abélienne qui permet de montrer le théorème de Chebotarev sans la conjecture d'Artin.

En utilisant la formule explicite ci-dessus, et suivant la méthode de Rubinstein et Sarnak via l'utilisation du théorème de Kronecker-Weyl, Ng montre alors ([Ng00, Theorem 5.1.2]) le résultat suivant.

Théorème 2.36 (Ng)**.** *Supposons l'hypothèse de Riemann pour ζ_L et la conjecture d'Artin pour les fonctions L d'Artin associées aux caractères irréductibles de G. Alors pour toutes classes de conjugaison $C_1,\dots,C_D$ de G, deux à deux distinctes, la quantité*

$$x \mapsto E_{G;C_1,\dots,C_D}(x) := \frac{\log x}{\sqrt{x}}\left(\frac{\#G}{\#C_1}\pi(x,C_1,L/K)-\pi_K(x),\dots,\frac{\#G}{\#C_D}\pi(x,C_D,L/K)-\pi_K(x)\right)$$

admet une distribution logarithmique limite $\mu_{G;C_1,\dots,C_D}$.

En prenant un peu d'avance sur les hypothèses d'indépendance linéaire employées par la suite (ou en invoquant le Corollary 1.70 par exemple), on voit que la valeur moyenne de

$$\frac{\pi(x,C_1,L/K)}{\#C_1}-\frac{\pi(x,C_2,L/K)}{\#C_2}$$

est

$$\frac{\#(C_2^{1/2})}{\#C_2}-\frac{\#(C^{1/2})}{\#C_2}+2\sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}}(\overline{\chi(C_2)}-\overline{\chi(C_1)})\,\mathrm{ord}_{s=1/2}\,L(s,\chi,L/K).$$

Ainsi, le fait « d'être un carré » joue à nouveau en la défaveur d'un participant à une course d'idéaux premiers, autrement dit le biais de Tchebychev est toujours présent, mais la présence de zéros en $1/2$ peut cependant théoriquement avoir une influence sur ce biais.

Dans sa thèse, Ng a observé numériquement ce phénomène. En considérant une extension explicite de $\mathbb{Q}$ construire par Serre dont le groupe de Galois est le groupe des quaternions $\mathbb{H}_8$ à 8 éléments, et dont la fonction L d'Artin associée à l'unique caractère non abélien de ce

groupe admet un zéro en 1/2 ([Ng00, 5.3.3 (i)]), Ng vérifie numériquement qu'une certaine inégalité de la forme

$$\pi(x, C_1, L/K) > \pi(x, C_2, L/K)$$

(les classes de conjugaison C_1 et C_2 étant réduites à un seul élément) a lieu pour une proportion $\approx 0,8454\ldots$ du temps, malgré le fait que $\#(C_1^{1/2}) > \#(C_2^{1/2})$. Cette inversion du sens du biais attendu dans une course d'idéaux premiers constitue la motivation de l'article [Bai19], reproduit dans la section 2.3. Là aussi, les groupes de Galois de type quaternion jouent un rôle important.

2.2.2 Discussion de l'hypothèse d'indépendance linéaire

Pour poursuivre l'étude de la distribution logarithmique limite, on en vient à introduire des hypothèses d'indépendance linéaire sur les zéros des fonctions L d'Artin.

L'hypothèse employée par Ng dans [Ng00] est la suivante : le (multi)-ensemble

$$\{\gamma > 0 \mid \exists \chi \in \mathrm{Irr}(G), L(1/2 + i\gamma, \chi, L/K) = 0\}$$

est linéairement indépendant sur $\mathbb{Q}$.

En travaillant avec cette hypothèse, Ng obtient une formule pour la fonction caractéristique $\hat{\mu}_{G;C_1,\ldots,C_D}$ de $\mu_{G;C_1,\ldots,C_D}$. Les résultats de Devin dans [Dev19] impliquent alors des résultats similaires à ceux de Rubinstein et Sarnak concernant l'existence et la stricte positivité de $\delta(L/K, C_1, \ldots, C_D)$. Cependant, l'hypothèse d'indépendance linéaire de Ng ne peut être vraie en général. En effet, soit χ un caractère irréductible de G. En utilisant les propriétés fonctorielles des fonctions L d'Artin par rapport à leurs caractères, on a montré au-dessus de l'Exemple 2.23 que l'on a

$$L(s, \chi, L/K) = L(s, \mathrm{Ind}_{\tilde{G}}^{G^+} \tilde{\chi}, L^+/\mathbb{Q}),$$

où L^+ est la clôture galoisienne de $L/\mathbb{Q}$, $\tilde{G} = \mathrm{Gal}(L^+/K)$, $G^+ = \mathrm{Gal}(L^+/\mathbb{Q})$ et $\tilde{\chi} = \chi \circ \pi_G$, avec $\pi_G : \tilde{G} \twoheadrightarrow G$ la projection dans le quotient. Notons $\psi := \mathrm{Ind}_{\tilde{G}}^{G^+} \tilde{\chi}$. Alors on peut de plus factoriser

$$L(s, \psi, L^+/\mathbb{Q}) = \prod_{\lambda \in \mathrm{Irr}(G^+)} L(s, \lambda, L^+/\mathbb{Q})^{\langle \psi, \lambda \rangle}.$$

Ainsi, partant de deux caractères irréductibles χ, χ' distincts (et donc orthogonaux) de G, les caractères ψ et ψ' associés comme ci-dessus peuvent ne plus être orthogonaux, et les fonctions $L(s, \chi, L/K)$ et $L(s, \chi', L/K)$ peuvent admettre des « facteurs communs », et en particulier des zéros communs. Dans le cas où $K \neq \mathbb{Q}$, on ne peut donc pas espérer que les zéros des fonctions L d'Artin associées aux caractères irréductibles de G soient indépendants.

Une hypothèse d'indépendance linéaire plus raisonnable devrait donc porter sur les zéros des fonctions L d'Artin dont le corps de base est $\mathbb{Q}$. Cette hypothèse est introduite pour la première fois dans [FJ20a].

Conjecture 2.37 (LI$^{\mathrm{r}}$)**.** *Le multi-ensemble*

$$\{\gamma > 0 \mid \exists \lambda \in \mathrm{Irr}(G^+), L(1/2 + i\gamma, \lambda, L^+/\mathbb{Q}) = 0\}$$

est linéairement indépendant sur $\mathbb{Q}$*.*

Remarque 2.38. La raison de l'échec de l'hypothèse de Ng en général est, comme on l'a vu, l'existence de factorisations non triviales des fonctions L d'Artin quand le corps de base n'est pas $\mathbb{Q}$ (on parlera d'extensions relatives). Rien n'interdit *a priori* que de telles factorisations existent également pour les fonctions L d'Artin d'extensions galoisiennes de $\mathbb{Q}$, mais il semble raisonnable de penser que de telles fonctions sont primitives au sens de Rudnick et Sarnak [RS96], et enfin de penser que les zéros de telles fonctions sont bien indépendants.

Pour exploiter cette hypothèse d'indépendance linéaire, il faut bien sûr avoir à disposition une formule explicite pour les fonctions de comptage d'idéaux premiers faisant intervenir les zéros des $L(s, \lambda, L^+/\mathbb{Q})$, avec $\lambda \in \mathrm{Irr}(G^+)$. Une telle formule est obtenue dans [FJ20a, Corollary 3.10] à l'aide d'un transfert des fonctions de comptage entre les différentes extensions de corps de nombres en jeu.

Théorème 2.39 (Fiorilli, Jouve)**.** *Supposons que $L/\mathbb{Q}$ et $K/\mathbb{Q}$ soient galoisiennes (de sorte que $L^+ = L$ et $G^+ = \mathrm{Gal}(L/\mathbb{Q})$), l'hypothèse de Riemann pour ζ_L et la conjecture d'Artin pour les fonctions L d'Artin associées aux caractères irréductibles de G^+. Alors pour toute classe de conjugaison C de G, on a*

$$\frac{\log x}{\sqrt{x}}\left(\frac{\#G}{\#C}\pi(x, C, L/K) - \pi_K(x)\right) = 1 - \frac{\#(C^{1/2})}{\#C} - 2\sum_{\chi\in\mathrm{Irr}(G)} \overline{\chi(C)}\,\mathrm{ord}_{s=1/2}\, L(s, \chi, L/K) - \sum_{\lambda\in\mathrm{Irr}(G^+)} \overline{\lambda(C^+)} \sum_{\gamma_\lambda\neq 0} \frac{x^{i\gamma_\lambda}}{\frac{1}{2} + i\gamma_\lambda} + O\left(\frac{1}{\log x}\right),$$

où $C^+ := \bigcup_{g\in G^+} gCg^{-1}$ désigne la classe de conjugaison engendrée par C dans G^+.

À ce stade, nous sommes donc en mesure d'énoncer des résultats généraux concernant les courses d'idéaux premiers dans l'extension L/K, avec des hypothèses convenables.

Théorème 2.40 (Ng, Devin)**.** *Supposons l'hypothèse de Riemann pour ζ_L et la conjecture d'Artin pour les fonctions L d'Artin associées aux caractères irréductibles de G. Alors pour toutes classes de conjugaison $C_1, \dots, C_D$ de G, deux à deux distinctes, $E_{G;C_1,\dots,C_D}$ admet une distribution logarithmique limite $\mu_{G;C_1,\dots,C_D}$. Si de plus $L/\mathbb{Q}$ et $K/\mathbb{Q}$ sont galoisiennes, la conjecture d'Artin pour les fonctions L d'Artin associées aux caractères irréductibles de* $\mathrm{Gal}(L/\mathbb{Q})$ *et* LI^- *sont vraies, alors $\delta(L/K; C_1, \dots, C_D)$ existe et vérifie $0 < \delta(L/K; C_1, \dots, C_D) < 1$.*

2.2.3 Évolution du biais de Tchebychev en familles

On souhaite maintenant étudier l'évolution de la quantité $\delta(L/K; C_1, \dots, C_D)$ dans des familles d'extensions de corps de nombres. On se limite à des courses à deux participants où l'on peut déjà observer beaucoup de comportements différents. Dans [FJ20a], Fiorilli et Jouve mettent en évidence deux types de comportements radicalement opposés pour l'évolution du biais. Pour ce faire, ils introduisent des variables aléatoires représentant la distribution limite $\mu_{G;C_1,C_2}$.

Définition 2.41. *Soient C_1, C_2 deux classes de conjugaison de G. On introduit une suite de variables aléatoires $(Z_{\gamma_\lambda})_{\gamma_\lambda, \lambda \in \mathrm{Irr}(G^+)\setminus\{\lambda_0\}}$, indépendantes et uniformes sur le cercle unité, et on note $X_{\gamma_\lambda} = \mathfrak{Re}(Z_{\gamma_\lambda})$. Alors on pose*

$$X(L/K; C_1, C_2) := c(C_2) - c(C_1) + \sum_{\lambda \in \mathrm{Irr}(G^+)\setminus\{\lambda_0\}} |\lambda(C_1^+) - \lambda(C_2^+)| \sum_{\gamma_\lambda > 0} \frac{2X_{\gamma_\lambda}}{\sqrt{\frac{1}{4} + \gamma_\lambda^2}}$$

où

$$c(C_i) := \frac{\#(C_i^{1/2})}{\#C_i} + 2 \sum_{\chi \in \mathrm{Irr}(G)\setminus\{\chi_0\}} \overline{\chi(C_i)}\, \mathrm{ord}_{s=1/2}\, L(s, \chi, L/K)$$

pour $i = 1, 2$.

En appliquant la formule explicite du Théorème 2.39 et les résultats de la section 1.4.1.4, on obtient le résultat suivant, conforme à ce qui est attendu. On supposera désormais que $L/\mathbb{Q}$ et $K/\mathbb{Q}$ sont galoisiennes, et on rappelle que G^+ désigne $\mathrm{Gal}(L/\mathbb{Q})$.

Proposition 2.42. *Supposons l'hypothèse de Riemann pour ζ_L, LI^- et la conjecture d'Artin pour les fonctions L d'Artin associées aux caractères irréductibles de G^+. Soient C_1, C_2 deux classes de conjugaison de G. La loi de $X(L/K; C_1, C_2)$ est la distribution limite $\mu_{G;C_1,C_2}$ du Théorème 2.36. De plus,*

$$\mathbb{E}(X(L/K; C_1, C_2)) = c(C_2) - c(C_1)$$

et

$$\mathrm{Var}(X(L/K; C_1, C_2)) = 2 \sum_{\lambda \in \mathrm{Irr}(G^+)} |\lambda(C_2^+) - \lambda(C_1^+)|^2 \sum_{\gamma_\lambda > 0} \frac{1}{\frac{1}{2} + \gamma_\lambda^2}.$$

Remarque 2.43. En fait la formule explicite de Fiorilli et Jouve, combinée aux résultats généraux de Devin ([Dev19]) permettent de calculer l'espérance et la variance de $\mu_{G;C_1,C_2}$ sans plus d'hypothèse que la conjecture d'Artin. À nouveau, on peut se dispenser de l'hypothèse de Riemann en remplaçant les occurrences de $1/2$ par β_L, la borne supérieure des parties réelles des zéros de ζ_L. La difficulté de la représentation de $\mu_{G;C_1,C_2}$ par une variable aléatoire aussi explicite sans hypothèse d'indépendance linéaire est partiellement expliquée par l'étude de la section 1.4.1.4.

Deux comportements limites opposés pour $X(L/K; C_1, C_2)$ au sein d'une famille d'extensions sont mis en évidence par Fiorilli et Jouve. La quantité qui régit ces comportements est

$$B(L/K; C_1, C_2) := \frac{\mathbb{E}(X(L/K; C_1, C_2))}{\sqrt{\mathrm{Var}(X(L/K; C_1, C_2))}}.$$

Dans l'esprit du papier original de Rubinstein et Sarnak, un phénomène de type « théorème central limite », menant à un biais modéré, peut se produire dans certaines familles d'extensions ([FJ20a, Theorem 5.10]).

Théorème 2.44. *Supposons l'hypothèse de Riemann pour ζ_L, LI^- et la conjecture d'Artin pour les fonctions L d'Artin associées aux caractères irréductibles de G^+. Alors pour toutes classes de conjugaison distinctes C_1 et C_2 de G, on a*

$$\delta(L/K; C_1, C_2) = \frac{1}{2} + \frac{B(L/K; C_1, C_2)}{\sqrt{2\pi}} + O(B(L/K; C_1, C_2)^3 + \mathrm{Var}(X(L/K; C_1, C_2))^{-1/3}).$$

Notons que cette estimation n'a d'intérêt que si $B(L/K;C_1,C_2)$ tend vers 0 le long de la famille d'extensions considérée. De plus, le terme principal dans le développement de $\delta(L/K;C_1,C_2)-\frac{1}{2}$ est réellement $\frac{B(L/K;C_1,C_2)}{\sqrt{2\pi}}$ lorsque $\mathrm{Var}(X(L/K;C_1,C_2))^{1/6}=o(|\mathbb{E}(X(L/K;C_1,C_2))|)$ et $\mathbb{E}(X(L/K;C_1,C_2))=o(\mathrm{Var}(X(L/K;C_1,C_2))^{1/2})$.

Ensuite, inspirés par les résultats de biais extrêmes de Fiorilli dans [Fio14], Fiorilli et Jouve dégagent également des conditions suffisantes pour obtenir de tels biais dans le contexte des courses d'idéaux premiers dans les corps de nombres.

Théorème 2.45. *Supposons l'hypothèse de Riemann pour ζ_L, LI et la conjecture d'Artin pour les fonctions L d'Artin associées aux caractères irréductibles de G^+. Il existe une constante absolue $c>0$ telle que pour toutes classes de conjugaison distinctes C_1 et C_2 de G vérifiant $\mathbb{E}(X(L/K;C_1,C_2))\geq 0$, on a*

$$1-\delta(L/K;C_1,C_2)<\exp(-cB(L/K;C_1,C_2)^2).$$

Remarques 2.46.

i) Cette fois-ci, l'estimation n'a d'intérêt que si $B(L/K;C_1,C_2)$ tend vers $+\infty$ le long de la famille d'extensions considérées.

ii) En supposant seulement que les multiplicités des zéros de ζ_L sont bornées au lieu de LI, on peut obtenir une inégalité plus faible portant sur $1-\underline{\delta}(L/K;C_1,C_2)$, où la barre désigne la limite inférieure dans la définition de $\delta(L/K;C_1,C_2)$, en invoquant l'inégalité de Bienaymé-Tchebychev.

On peut également obtenir une minoration de la quantité $1-\delta(L/K;C_1,C_2)$ sous certaines conditions supplémentaires. La difficulté provient du fait que, dans l'optique d'utiliser un résultat de grandes déviations de Montgomery-Odlyzko ([MO88, Theorem 2]), on a besoin de contrôler l'espérance de $X(L/K;C_1,C_2)$, qui s'exprime comme une somme portant sur les caractères de G, par un reste de la série exprimant la variance de $X(L/K;C_1,C_2)$, série faisant intervenir les caractères de G^+. Un certain contrôle des « collusions » entre les caractères induits de G à G^+ est nécessaire pour mener le raisonnement à bien. C'est fait dans le Theorem 2.99, issu de l'article [Bai19] reproduit dans la section 2.3.

À l'aide de leurs résultats, Fiorilli et Jouve étudient certaines familles particulières d'extensions de corps de nombres : des extensions à groupes de Galois D_ℓ avec ℓ premier, des extensions de la forme $H_d/\mathbb{Q}$ où H_d désigne le corps de Hilbert de $\mathbb{Q}(\sqrt{d})$, des extensions radicielles (engendrées par X^p-a avec p premier ne divisant pas a) et des extensions à groupes de Galois $\mathfrak{S}_n$.

2.2.4 Root numbers et zéros en $1/2$

Dans la suite, notre but est d'étudier l'influence de l'existence de zéros en $1/2$ sur le biais de Tchebychev. Il semble a priori possible que le biais puisse changer de sens le long de deux familles d'extensions ayant les mêmes groupes de Galois, à cause de la différence de signe dans les espérances des $\mathbb{E}(X(L/K;C_1,C_2))$ induite par la présence, ou non, de tels zéros.

Il est cependant nécessaire d'introduire des hypothèses supplémentaires sur les conditions d'existence de tels zéros pour être capable d'obtenir des énoncés. En l'état actuel des choses, on ne sait essentiellement rien dire sur les zéros en $1/2$ (tout au plus sait-on majorer leurs multiplicités éventuelles comme zéros de ζ_L, voir [IK04, Proposition 5.34]) des fonctions L d'Artin en général. Comme précédemment, ces hypothèses devront porter sur des caractères de groupes de Galois d'extensions dont le corps de base est $\mathbb{Q}$. Le root number du caractère χ (constante dans l'équation fonctionnelle de $\Lambda(s, \chi, L/K)$, voir le Théorème 2.29) vérifie $W(\overline{\chi}) = \overline{W(\chi)}$ (cela peut se montrer en utilisant le fait que cette propriété est vérifiée pour les caractères de Hecke, puis se servir du théorème de Brauer et la multiplicativité du root number [Mar02, Corollary p.18]). Ainsi, si χ est un caractère réel, et du fait que $|W(\chi)| = 1$, on a $W(\chi) = \pm 1$. Comme expliqué précédemment, si $W(\chi) = -1$ alors $L(1/2, \chi, L/K) = 0$. Réciproquement, il est conjecturé que, dans certaines conditions, un tel zéro en $1/2$ provient nécessairement d'un root number égal à -1. On conjecture également que, si χ est irréductible, seuls certains types de caractères, appelés symplectiques, peuvent vérifier $W(\chi) = -1$ (pour les caractères dits orthogonaux, on sait d'après [FQ73] que $W(\chi) = 1$). C'est l'objet des conjectures LI et LI^+ introduites dans [FJ20a] initialement, et réutilisées dans [Bai19]. On trouvera une discussion plus détaillée de ces conjectures dans la section 2.3.1.2 tirée de l'article [Bai19].

Des groupes finis possédant beaucoup de caractères symplectiques sont les groupes de quaternions généralisés

$$\mathbb{H}_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, yxy^{-1} = x^{-1} \rangle$$

pour $n \geq 3$, d'ordre 2^n. Ces groupes sont donc des candidats naturels pour des groupes de Galois d'extensions de corps de nombres dont les fonctions L d'Artin peuvent admettre des zéros en $1/2$. Ces groupes de Galois sont au cœur de l'article *Chebyshev's bias in dihedral and generalized quaternion groups* [Bai19], reproduit dans la section suivante. Il se trouve que le groupe $\mathbb{H}_{2^n}$ a la même table de caractères que le groupe diédral $D_{2^{n-1}}$, qui lui ne possède pas de caractères symplectiques, et l'étude des différences entre les courses d'idéaux premiers dans des familles d'extensions ayant ces groupes pour groupes de Galois est également menée dans [Bai19].

La théorie des modules galoisiens développée par Fröhlich dans [Frö83] permet de donner une autre interprétation aux root numbers des caractères symplectiques des groupes de Galois $\mathbb{H}_{2^n}$. Joint à la théorie du corps de classes, Fröhlich énonce des résultats d'existence d'extensions de $\mathbb{Q}$ dont le groupe de Galois est un groupe de quaternions généralisé et dont la fonction ζ de Dedekind admet un zéro en $1/2$, ou non. Ce genre de résultats est exploité dans [Bai19] pour construire des familles d'extensions permettant de mettre en évidence l'influence de l'existence de tels zéros sur le biais de Tchebychev.

2.3 Biais de Tchebychev dans les groupes de Galois diédraux et de quaternions généralisés

Cette section contient l'article original Chebyshev's bias in dihedral and generalized quaternion Galois groups [Bai19] qui a été accepté pour publication dans Algebra & Number

Theory.

Résumé détaillé : On étudie les disparités dans la répartition des automorphismes de Frobenius dans des extensions de corps de nombres dont les groupes de Galois sont les groupes diédraux D_{2^n} et les groupes de quaternions généralisés $\mathbb{H}_{2^n}$. Sous des hypothèses naturelles, des familles d'extensions possédant de tels groupes de Galois sont étudiées. Tout d'abord dans un aspect « horizontal », où le groupe de Galois est fixé, puis dans un aspect « vertical », où le degré tend vers l'infini. Grâce à la théorie des modules galoisiens de Fröhlich, on est capable de construire des extensions de $\mathbb{Q}$ à groupes de Galois quaternionniens en prescrivant l'existence ou la non existence de zéros en $1/2$ pour leurs fonctions ζ de Dedekind. Ceci nous permet de mettre en évidence l'influence radicale qu'a l'existence ou non de tels zéros sur le biais de Tchebychev pour les courses d'idéaux premiers dans ces extensions. Un nouveau résultat de grandes déviations est également obtenu, complétant un énoncé récent de Fiorilli et Jouve dans [FJ20a]. Enfin, bien que les groupes $\mathbb{H}_{2^n}$ et $D_{2^{n-1}}$ ont les mêmes tables de caractères, notre étude montre que les courses d'idéaux premiers dans les extensions ayant de tels groupes de Galois ont des comportements différents.

Abstract : We study the inequities in the distribution of Frobenius elements in Galois extensions of the rational numbers with Galois groups that are either dihedral D_{2^n} or (generalized) quaternion $\mathbb{H}_{2^n}$ of two-power order. In the spirit of recent work of Fiorilli and Jouve [FJ20a], we study, under natural hypotheses, some families of such extensions, in a horizontal aspect, where the degree is fixed, and in a vertical aspect, where the degree goes to infinity. Our main contribution uncovers in families of extensions a phenomenon, for which Ng gave numerical evidence in [Ng00] : real zeros of Artin L-functions sometimes have a radical influence on the distribution of Frobenius elements.

Introduction

The prime number theorem in arithmetic progressions states that if $q \geq 1$ is an integer and a is prime to q, then

$$\pi(x,q,a) := |\{p \leq x \mid p = a \bmod q\}| \underset{x\to+\infty}{\sim} \frac{1}{\varphi(q)} \operatorname{Li}(x),$$

where Li is the logarithmic integral. Even though for a and b coprime to q, $\pi(x,q,a)$ and $\pi(x,q,b)$ have the same asymptotic value, it may happen that one count could be larger than the other most of the time. This is Chebyshev's bias : there seems to be more primes congruent to 3 mod 4 than 1 mod 4 in generic intervals $[2,x]$.

These so-called "prime number races" have been studied extensively by Rubinstein and Sarnak in [RS94]. They managed to explain conditionally Chebyshev's bias : under natural hypotheses which we will consider later, the inequality $\pi(x,4,3) > \pi(x,4,1)$ holds "99% of the time" (this will be explained rigorously in a later paragraph). For a general modulus q, they have shown a bias towards non-quadratic residues mod q against quadratic residues mod q.

In [Ng00], Ng, following a suggestion made in [RS94], extended Rubinstein and Sarnak's framework to conjugacy classes of the Galois group G of a Galois extension L/K of number

fields, in the context of the Chebotarev density theorem. Recall that if C is such a conjugacy class, then

$$\pi(x, C, L/K) := \left| \left\{ \mathfrak{p} \lhd \mathcal{O}_K \text{ unramified} \mid N(\mathfrak{p}) \leq x, \left(\frac{\mathfrak{p}}{L/K} \right) = C \right\} \right| \underset{x \to +\infty}{\sim} \frac{|C|}{|G|} \operatorname{Li}(x),$$

where $N(\mathfrak{p})$ is the norm of the prime ideal $\mathfrak{p}$ and $\left(\frac{\mathfrak{p}}{L/K}\right)$ is the Artin symbol, or Frobenius conjugacy class, at $\mathfrak{p}$. Taking $L = \mathbb{Q}(\zeta_q)$, where ζ_q is a primitive q-th root of unity in $\mathbb{C}$, and $K = \mathbb{Q}$, we get the prime number theorem in arithmetic progressions and one recovers the setting of [RS94]. We say we study *Chebotarev biases* when comparing the behaviours of prime ideal counting functions $\pi(x, C_1, L/K)$ and $\pi(x, C_2, L/K)$ for distinct conjugacy classes C_1, C_2 of $\mathrm{Gal}(L/K)$.

In recent work, Fiorilli and Jouve ([FJ20a]) have shown some Chebotarev races to be extremely biased (*i.e.* as for the original case where one compares $\pi(x, 4, 3)$ and $\pi(x, 4, 1)$, the underlying density is close to 1) by using large deviations principles. In the opposite direction, they managed to show central limit theorem behaviours which correspond to moderately biased Chebotarev races (*i.e.* the underlying density is close to $\frac{1}{2}$). In both cases, the asymptotic results appear as we let the conductors go to infinity. In [FJ20a], the theoretical results are applied to some families of number field extensions with Galois groups dihedral of order $2p$ (p an odd prime), quasidihedral, symmetric or Frobenius of order $p(p-1)$.

In this paper, we exploit work of Fröhlich on root numbers of quaternion extensions and we perform class field theoretic constructions to study, in the context of [FJ20a], Chebyshev's bias in some families of number field extensions with Galois groups of 2-power order : dihedral or (generalized) quaternion. Our main contributions highlight the role of central zeros of Artin L-functions in the study of this bias. They come as the result of the two following points of view. We first work in a "horizontal aspect", in which the Galois group is fixed (up to isomorphism). In this context, thanks to a result of Fröhlich (Theorem 2.79), we construct two different kinds of families of number fields which have quaternion Galois groups over $\mathbb{Q}$, but in which the existence or not of a central zero for the corresponding Dedekind zeta function leads to opposite biases (Theorem 2.82). Second, in the "vertical aspect", we build arbitrarily high degree towers of number field extensions with Galois groups dihedral or quaternion of 2-power order, and exhibit different kinds of behaviours in both families (Theorems 2.100 and 2.102). We obtain extreme bias, moderate bias and unbiased races (the underlying density is plainly equal to $\frac{1}{2}$). We emphasize that some of these behaviours are directly linked to the existence or not of a central zero for the corresponding Dedekind zeta functions in the quaternion case. This provides the first theoretical construction that confirms numerical evidence obtained by Ng. Finally, we are able to prove partial monotonicity phenomena in the evolution of the bias inside the tower itself (Theorem 2.104).

Outline of the paper

In Section 2.3.1 we introduce the preliminary results and conjectures needed to study Chebyshev's bias in number field extensions, and state abridged versions of our main results. In Section 2.3.2.1 we recall the definition of the Artin conductor of a complex character of the Galois group of a number field extension, and relate it to the study of Chebyshev's bias in the extension considered. Then in Section 2.3.2.2, we study the character-theoretic properties of

dihedral and generalized quaternion groups of 2-power order. In Section 2.3.3 we focus on the "horizontal aspect" of our study, in which the Galois group is fixed to be a quaternion group of order 8. In Sections 2.3.4.1 and 2.3.4.2 we give bounds on moments of the random variables governing Chebyshev's bias in Galois extensions with Galois groups dihedral and generalized quaternion groups of 2-power order. In Section 2.3.4.3 we construct such extensions with controlled ramification, and in Section 2.3.4.4 we give estimates on Chebyshev's bias in those extensions.

2.3.1 Chebotarev biases in Galois groups of number fields

2.3.1.1 Notations and recollection on Artin characters

We recall the following standard notations.

In this section and sections 1.2 and 1.4, we let L/K be a Galois number field extension with Galois group G. Let C_1 and C_2 be distinct conjugacy classes of G. We would like to give a notion of measure to the set

$$\mathcal{P}_{L/K,C_1,C_2} := \{x \geq 2 \mid \frac{\pi(x, C_1, L/K)}{|C_1|} > \frac{\pi(x, C_2, L/K)}{|C_2|}\},$$

where C_1 and C_2 are conjugacy classes of G. A first guess would be to use the natural density, defined as the limit as x tends to $+\infty$ of

$$\frac{\left|\mathcal{P}_{L/K,C_1,C_2} \cap [0, x]\right|}{x},$$

where $|.|$ denotes the Lebesgue measure. Unfortunately, it has been shown that this limit does not exist, even in the case of prime number races [Kac93]. Therefore, we use the notion of logarithmic density, better-suited to the study of Chebyshev's bias as was first observed in [Win41].

Definition 2.47. *Let A be a Borel set in $\mathbb{R}$. Its logarithmic density is, when it exists,*

$$\delta(A) := \lim_{X \to +\infty} \frac{1}{X} \int_2^X \mathbf{1}_A(\mathrm{e}^t)\, dt.$$

If C_1 and C_2 are conjugacy classes of G, we write $\delta(L/K, C_1, C_2)$ for $\delta(\mathcal{P}_{L/K,C_1,C_2})$. We say the race between C_1 and C_2 is unbiased if $\delta(L/K, C_1, C_2) = \frac{1}{2}$, that it is biased towards C_1 if $\delta(L/K, C_1, C_2) > \frac{1}{2}$ and biased towards C_2 if $\delta(L/K, C_1, C_2) < \frac{1}{2}$.

Ng has shown in [Ng00] that this logarithmic density always exists under some natural hypotheses (see section 1.3). Our goal will be to give estimates for such densities. Following [FJ20a], we introduce some quantities related to the conjugacy classes under consideration, but also to the irreducible characters of G.

Definition 2.48. *Let C be a conjugacy class of G. Then we define*

$$C^{1/2} := \{g \in G \mid g^2 \in C\}$$

and

$$z(C) := 2 \sum_{\chi \neq \chi_0} \chi(C) \operatorname{ord}_{s=1/2} L(s, \chi, L/K),$$

where the sum is taken over all the non-trivial irreducible characters χ of G, and $s \mapsto L(s, \chi, L/K)$ is the Artin L-function associated to χ.

A certain class of characters of G plays a particular role in our study, the class of symplectic characters. To introduce them, we need the notion of Frobenius-Schur index of a character.

Definition 2.49. *Let χ be a character of G. We define its Frobenius-Schur index by*

$$\varepsilon_2(\chi) := \frac{1}{|G|} \sum_{g \in G} \chi(g^2).$$

We also define $\mathrm{Irr}(G)$ to be the set of irreducible characters of G, and $\mathrm{Irr}^{\mathrm{real}}(G)$ to be the set of real-valued irreducible characters of G.

The Frobenius-Schur index of an irreducible (complex) character of G determines if such a character can be afforded by a real-valued representation or not, thanks to the following well-known result from character theory.

Theorem 2.50 ([Isa94] p.58)**.** *Let χ be an irreducible complex character of G. Then only one of the following three statements holds :*

i) $\varepsilon_2(\chi) = 0$, in this case χ is not real-valued. We say that χ is unitary.

ii) $\varepsilon_2(\chi) = 1$, in this case χ is real-valued and can be afforded by a real-valued representation of G. We say that χ is orthogonal.

iii) $\varepsilon_2(\chi) = -1$, in this case χ is real-valued and cannot be afforded by a real-valued representation of G. We say that χ is symplectic.

It is expected that symplectic characters are exactly the irreducible characters which can yield real zeros for their associated Artin L-function (see conjecture LI below).

Finally, we recall that if χ is an irreducible character of G, then its Artin L-function satisfies a functional equation ([MM97, p.28]) of the form

$$\Lambda(s, \chi, L/K) = W(\chi, L/K)\Lambda(1 - s, \overline{\chi}, L/K),$$

where $W(\chi, L/K)$ is a complex number of modulus 1, called the root number of χ, and $s \mapsto \Lambda(s, \chi, L/K)$ is the completed Artin L-function associated to χ, which is the product of $s \mapsto L(s, \chi, L/K)$ with Gamma factors coming from archimedian places. Unless there is an ambiguity in the extension considered, we will usually write $W(\chi)$ for $W(\chi, L/K)$. The root number satisfies $\overline{W(\chi)} = W(\overline{\chi})$. In particular if χ is real-valued then $W(\chi) = \pm 1$. We have the following important way to detect central zeros of Artin L-functions.

Proposition 2.51. *If $\chi \in \mathrm{Irr}^{\mathrm{real}}(G)$ with $W(\chi) = -1$, then $L\left(\frac{1}{2}, \chi, L/K\right) = 0$.*

Proof. Since χ is real-valued, evaluating the functional equation at $\frac{1}{2}$ we find

$$\Lambda\left(\frac{1}{2},\chi\right) = -\Lambda\left(\frac{1}{2},\chi\right),$$

i.e. $\Lambda\left(\frac{1}{2},\chi\right) = 0$. Since the Gamma function never vanishes on $\mathbb{C}$, this implies that $L\left(\frac{1}{2},\chi,L/K\right) = 0$. □

It is expected that the converse also holds for real-valued characters when the base field is $\mathbb{Q}$, see conjecture LI^+ below.

2.3.1.2 Conjectures

As in [FJ20a], we consider natural conjectures on the distribution of zeros and poles of Artin L-functions, some of which are generalizations of conjectures used in the work of Rubinstein and Sarnak. Recall that L/K is a Galois extension of number fields.

Conjecture 2.52 (Artin's conjecture)**.** *If χ is a non-trivial irreducible character of G, then $s \mapsto L(s,\chi,L/K)$ is entire.*

Conjecture 2.53 (GRH)**.** *If χ is an irreducible character of G, then the non-trivial zeros of $s \mapsto L(s,\chi,L/K)$ have real part $\frac{1}{2}$.*

Conjecture 2.54 (LI^-)**.** *Let $L_0/\mathbb{Q}$ be the Galois closure of $L/\mathbb{Q}$. Then the multiset of imaginary parts of zeros*

$$\Gamma_{L_0/\mathbb{Q}} := \bigcup_{\chi\in\mathrm{Irr}(\mathrm{Gal}(L_0/\mathbb{Q}))} \left\{\gamma > 0 \mid L\left(\frac{1}{2}+i\gamma,\chi,L_0/\mathbb{Q}\right) = 0\right\}$$

is linearly independent over $\mathbb{Q}$.

Conjecture 2.55 (LI)**.** LI^- *is true and if $\chi \neq \chi_0$ is a unitary or orthogonal character of* $\mathrm{Gal}(L_0/\mathbb{Q})$ *(see Theorem 2.50) then $L(\frac{1}{2},\chi,L_0/\mathbb{Q}) \neq 0$. If χ is a symplectic character of* $\mathrm{Gal}(L_0/\mathbb{Q})$ *then* $\mathrm{ord}_{s=1/2}\, L(s,\chi,L_0/\mathbb{Q})$ *is bounded by some absolute constant M_0.*

Conjecture 2.56 (LI^+)**.** LI *is true and if χ is a symplectic irreducible character of* $\mathrm{Gal}(L_0/\mathbb{Q})$ *then* $\mathrm{ord}_{s=1/2}\, L(s,\chi,L_0/\mathbb{Q}) = \frac{1-W(\chi)}{2}$.

Let us make a few comments about these conjectures.

- First, Artin's conjecture needs to be assumed in order to be able to prove explicit formulas for number field analogs of Chebyshev's ψ function, involving sums over zeros of Artin L-functions, and discarding the existence of possible poles. In the cases we will consider, namely when G is a dihedral group or generalized quaternion group, Artin's conjecture is known to be true, because such groups are supersolvable, which means they have a normal series

  $$\{1\} = G_1 \lhd G_2 \lhd \ldots \lhd G_k = G$$

  where each quotient G_{i+1}/G_i is cyclic for $1 \leq i \leq k-1$. This implies that their irreducible characters are induced by those of abelian subgroups. By inductive properties

of Artin L-functions, we are reduced to knowing Artin's conjecture in the case of characters of abelian Galois groups, but this is exactly one of the consequences of class field theory, together with work of Hecke on the L-functions bearing his name.

- The Generalized Riemann Hypothesis (GRH) needs to be assumed so that, for conjugacy classes C_1 and C_2 of G,

$$\frac{|G|}{|C_2|}\pi(x, C_1, L/K) - \frac{|G|}{|C_2|}\pi(x, C_2, L/K)$$

is oscillating with amplitude of size roughly $\sqrt{x}$. This is central in the analysis of Chebyshev's bias. One can still show the existence of a limiting logarithmic distribution for a convenient renormalization of $\frac{|G|}{|C_2|}\pi(x, C_1, L/K) - \frac{|G|}{|C_2|}\pi(x, C_2, L/K)$ without assuming GRH (see [Dev19]), though it depends on the supremum of real parts of non-trivial zeros of the Artin L-functions considered.

- The hypothesis LI$^-$ actually contains two statements. The most obvious one is the linear independence of the positive imaginary parts of zeros of Artin L-functions. This hypothesis appears because, in order to understand Chebyshev's bias using explicit formulas for prime counting functions, one needs good information on the joint distribution of the values of $\mathrm{e}^{i\gamma y_1}, e^{i\gamma_2 y}, \dots$ in $\mathbb{S}^1$, where $\gamma_1, \gamma_2, \dots$ denotes the aforementioned positive imaginary parts of zeros, and y varies in $\mathbb{R}$. Again, weaker hypotheses have been used to show the existence of a limiting logarithmic distribution ([Dev19]) and results on the bias. Another aspect of LI we highlight is that it is stated for L-functions over $\mathbb{Q}$ instead of L-functions over K. Indeed, those L-functions over K factorize as products of L-functions relative to $L_0/\mathbb{Q}$, so linear independence is typically false. The last aspect adressed by LI is about the multiplicity of the zeros of Artin L-functions over $\mathbb{Q}$. One should expect those Artin L-functions to be "primitive" in the sense of [RS96], and those should not satisfy any kind of non-trivial algebraic relations, except for their respective functional equations. Instead of the simplicity of the zeros, we could have opted for an hypothesis about the boundedness of the multiplicities of such zeros (called BM in [FJ20a]), which would have been enough for a few intermediate results of this paper.
- The assumptions on the order of vanishing at $\frac{1}{2}$ in LI and LI$^+$ appear because the quantity $z(C)$ defined above is involved in the mean of the random variables attached to the limiting distribution governing the bias. Examples of symplectic characters with root numbers -1 were first given by Armitage ([Arm72]) and Serre (unpublished). In particular, they yield Artin L-functions vasnishing at $1/2$ because of Proposition 2.51. As was pointed out by the author of the present paper to the authors of [FJ20a] while both papers were under preliminary form, using one of the aforementionned examples, the conjecture "Artin L-functions attached to orthogonal or unitary characters do not vanish at $1/2$" could not hold over general number fields K. Indeed, consider Serre's example, as described in [Ng00, section 5.3.3] : let $L = \mathbb{Q}(\theta)$, where $\theta = \sqrt{\frac{5+\sqrt{5}}{2}\frac{41+\sqrt{5\cdot 41}}{2}}$. It is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to the quaternion group $\mathbb{H}_8$ (see section 2). The root number of its non-abelian (symplectic) character ψ is -1, so $L(1/2, \psi, L/\mathbb{Q}) = 0$. Now consider the subfield $K = \mathbb{Q}(\sqrt{5}) \subset L$. We have $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ which does not admit any irreducible symplectic character.

But we have the classical factorization

$$\begin{aligned}\zeta_L(s) &= P_1(s)L(s,\psi,L/\mathbb{Q})^2\\ &= P_2(s),\end{aligned}$$

where P_1 is the product of the Artin L-functions attached to the four abelian irreducible characters of $\mathrm{Gal}(L/\mathbb{Q})$, and P_2 is the product of the Artin L-functions attached to the four irreducible characters of $\mathrm{Gal}(L/K)$. Since $L(1/2,\psi,L/\mathbb{Q})=0$, at least one of those Artin L-functions, attached to a non-symplectic irreducible character, must vanish at $1/2$. This shows that we cannot expect easy non-vanishing statements at the central point in the relative case L/K when $K\neq\mathbb{Q}$, and that such a statement should involve the way irreducible characters of G are "induced" to Artin characters over $\mathbb{Q}$.

2.3.1.3 Main results

Our first result is in a horizontal aspect : we exhibit moderately biased races in families of extensions of $\mathbb{Q}$ with fixed Galois group isomorphic to $\mathbb{H}_8$, the usual quaternion group of order 8.

Theorem A. *Assume* GRH *and* LI$^+$. *For any function f such that $f(n)\underset{n\to+\infty}{\longrightarrow}+\infty$, there exist two families $(K_d)_d$ and $(L_d)_d$ of number fields, indexed by square-free integers satisfying $d>1$ and $d=1$ mod 4, such that for any d in the index set :*

i) $\mathbb{Q}(\sqrt{d})\subset K_d\cap L_d$.

ii) $\mathrm{Gal}(K_d/\mathbb{Q})\simeq\mathrm{Gal}(L_d/\mathbb{Q})\simeq\mathbb{H}_8$.

iii) $0<\frac{1}{2}-\delta(K_d/\mathbb{Q},C_1,C_{-1})\ll\frac{1}{f(d)}$, *where C_1 and C_{-1} denote the conjugacy classes of 1 and -1 in $\mathbb{H}_8$.*

iv) $0<\delta(L_d/\mathbb{Q},C_1,C_{-1})-\frac{1}{2}\ll\frac{1}{f(d)}$.

The most important feature of this result is that we are able to exhibit two families in which the biases are opposite to each other, one is $<\frac{1}{2}$ while the other is $>\frac{1}{2}$, the difference coming from the existence of a central zero for the corresponding Dedekind zeta function in the first case, and the absence of such a zero in the second case. Moreover, the prime number races considered can be specified to be as moderately biased as possible, in the sense that the logarithmic densities can be made arbitrarily close to $\frac{1}{2}$ when d grows, while ensuring that $\mathbb{Q}(\sqrt{d})\subset K_d\cap L_d$. In fact the choice of f allows one to have arbitrarily large variances for the random variables $X(K_d/\mathbb{Q},C_1,C_{-1})$ and $X(L_d/\mathbb{Q},C_1,C_{-1})$ governing the biases (see Theorem 2.57).

The second part of our work is in a vertical aspect : we build families of extensions of $\mathbb{Q}$ with Galois groups dihedral and quaternion of 2-power order, in which we are able to show extreme biases, moderate biases and absence of bias.

Theorem B. *Assume* GRH *and* LI$^+$. *There exist absolute constants $c_1,c_2,c_3>0$ and a family $(\mathcal{D}_n)_n$ of number fields such that for any $n\geq 3$, the following hold :*

i) $\mathrm{Gal}(\mathcal{D}_n/\mathbb{Q})\simeq D_{2^{n-1}}=\langle r,s\mid r^{2^{n-1}}=s^2=1,srs^{-1}=r^{-1}\rangle$.

ii) $c_1 \exp(-c_2 2^n) < \delta(\mathcal{D}_n/\mathbb{Q}, C_1, C_{-1}) < \exp\left(-c_3 \frac{2^n}{n}\right)$ *where* C_a *denotes the conjugacy class of* a*, and* -1 *denotes* $r^{2^{n-2}} \in D_{2^{n-1}}$.

iii) $0 < \frac{1}{2} - \delta(\mathcal{D}_n/\mathbb{Q}, C_{-1}, C_s) \ll \frac{1}{2^{n/3}}$.

iv) $\delta(\mathcal{D}_n/\mathbb{Q}, C_{r^k}, C_s) = \delta(\mathcal{D}_n/\mathbb{Q}, C_{r^k}, C_{rs}) = \frac{1}{2}$ *when* $1 \leq k \leq 2^{n-2} - 1$ *is odd.*

We chose a sample of possible couples of conjugacy classes in the above statement. For an exhaustive treatment of conjugacy classes, see Theorem 2.100. In [FJ20a], Fiorilli and Jouve, relying on a construction of Klüners, only deal with dihedral groups of order $2p$ with p varying in the set of odd primes. The following result deals with generalized quaternion Galois groups.

Theorem C. *Assume* GRH *and* LI^+. *There exist absolute constants* $c_1, c_2, c_3 > 0$ *and two families* $(\mathcal{Q}_n^+)_n$ *and* $(\mathcal{Q}_n^-)_n$ *of number fields such that for any* $n \geq 3$*, the following hold :*

i) $\mathrm{Gal}(\mathcal{Q}_n^\pm/\mathbb{Q}) \simeq \mathbb{H}_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$*, and the root number of each symplectic character of* $\mathrm{Gal}(\mathcal{Q}_n^\pm/\mathbb{Q})$ *is the same (we denote it by* $W_{\mathcal{Q}_n^\pm}$*). Moreover,* $W_{\mathcal{Q}_n^+} = 1$ *and* $W_{\mathcal{Q}_n^-} = -1$.

ii) $c_1 \exp(-c_2 2^n) < \left|\frac{1 - W_{\mathcal{Q}_n^\pm}}{2} - \delta(\mathcal{Q}_n^\pm/\mathbb{Q}, C_1, C_{-1})\right| < \exp\left(-c_3 \frac{2^n}{n}\right)$*, where* C_a *denotes the conjugacy class of* a*, and* -1 *denotes* $x^{2^{n-2}}$.

iii) $\delta(\mathcal{Q}_n^+/\mathbb{Q}, C_1, C_{x^k}) = \frac{1}{2}$ *when* $1 \leq k \leq 2^{n-2} - 1$ *is even and* $c_1 \exp(-c_2 32^n) < \delta(\mathcal{Q}_n^-/\mathbb{Q}, C_1, C_{x^k}) < \exp\left(-c_3 \frac{2^n}{n}\right)$ *for* $1 \leq k \leq 2^{n-2} - 1$.

iv) $0 < \frac{1}{2} - \delta(\mathcal{Q}_n^+/\mathbb{Q}, C_1, C_y) \ll \frac{1}{2^{n/3}}$ *and* $c_1 \exp(-c_2 2^n) < \delta(\mathcal{Q}_n^-/\mathbb{Q}, C_1, C_y) < \exp\left(-c_3 \frac{2^n}{n}\right)$.

Again, we chose to focus on a sample of meaningful cases of bias estimates in ii), iii) and iv), but more have been computed and are stated in Theorem 2.102. The new and remarkable feature of this theorem is that it highlights the role played by the existence or not of a central zero for the corresponding Dedekind zeta function. The presence (or the inexistence) of such a zero leads to : extreme biases of opposite signs in ii), extreme biases or no biases in iii), extreme bias or moderate bias in iv).

Finally, our last contribution is to show that we can observe a monotonicity phenomenon in the evolution of Chebyshev's bias in subextensions of dihedral extensions of $\mathbb{Q}$.

Theorem D. *Assume* GRH *and* LI. *Consider the number fields* $(\mathcal{D}_n)_n$ *as in Theorem B. For every* $n \geq 3$*, there are dihedral subfields* $\mathbb{Q} = \mathcal{D}_n^{(n)} \subset \mathcal{D}_n^{(n-1)} \subset \cdots \subset \mathcal{D}_n^{(3)} \subset \mathcal{D}_n$ *such that* $\mathrm{Gal}(\mathcal{D}_n/\mathcal{D}_n^{(i)}) \simeq D_{2^n}$ *for* $3 \leq i \leq n$*, and such that for any* $\varepsilon > 0$ *and any sufficiently large* n*, for* $3 \leq i < j \leq n$ *such that* $i \leq n\frac{1+\varepsilon}{2}$ *and* $j \geq n\left(\frac{1+3\varepsilon}{2}\right)$*, we have*

$$\delta(\mathcal{D}_n/\mathcal{D}_n^{(j)}, C_1^{(j)}, C_{-1}^{(j)}) < \delta(\mathcal{D}_n/\mathcal{D}_n^{(i)}, C_1^{(i)}, C_{-1}^{(i)}),$$

where $C_1^{(k)}$ *and* $C_{-1}^{(k)}$ *denote the conjugacy classes of* 1 *and* -1 *in* $\mathrm{Gal}(\mathcal{D}_n/\mathcal{D}_n^{(k)})$.

This statement means that, in the subextensions of $\mathcal{D}_n/\mathcal{D}_n^{(i)}$, Chebyshev's bias is more extreme at the bottom of the tower than at the top. A more general result including the quaternion fields $\mathcal{Q}_n^\pm$ of Theorem C is stated as Theorem 2.104. The proof relies on a new large deviation bound for the values of Chebyshev's bias in families of number field extensions (see Theorem 2.99).

2.3.1.4 The probabilistic approach to Chebotarev biases

Let us recall the setting of [FJ20a] together with useful results. As before, L/K is a Galois extension of number fields with group G. We will assume $L/\mathbb{Q}$ is Galois, with Galois group G^+, so that G is a subgroup of G^+. This will be the case in our applications. If C is a conjugacy class of G, then we denote by C^+ the conjugacy class generated by C in G^+, *i.e.* $C^+ := \bigcup_{a\in G^+} aCa^{-1}$. In what follows, if F/E is a Galois extension of number fields and $\chi \in \mathrm{Irr}(\mathrm{Gal}(F/E))$, a summation over $\gamma_\chi > 0$ means a summation over the corresponding zero multiset

$$\Gamma_{F/E,\chi} := \{\gamma > 0 \mid L(1/2 + i\gamma, \chi, F/E) = 0\}.$$

We also write $\Gamma_{F/E} := \bigcup_{\chi\in\mathrm{Irr}(\mathrm{Gal}(F/E))} \Gamma_{F/E,\chi}$ and $\Gamma^{\mathrm{real}}_{F/E} := \bigcup_{\chi\in\mathrm{Irr}^{\mathrm{real}}(\mathrm{Gal}(F/E))} \Gamma_{F/E,\chi}$.

We summarize in the next statement the main result giving a probabilistic interpretation of the logarithmic densities we are studying.

Theorem 2.57 ([FJ20a], Proposition 3.18 and Lemma 3.20)**.** *Assume Artin's conjecture,* GRH *and* LI$^-$*. For any $\gamma \in \Gamma_{L/\mathbb{Q}}$, we introduce the random variable $X_\gamma = \mathfrak{Re}(Z_\gamma)$, where $(Z_\gamma)_\gamma$ is a family of independent random variables uniform on the unit circle. Then for any conjugacy classes C_1 and C_2 of G, we have*

$$\delta(L/K, C_1, C_2) = \mathbb{P}(X(L/K, C_1, C_2) > 0)$$

where

$$X(L/K, C_1, C_2) := \frac{|C_2^{1/2}|}{|C_2|} - \frac{|C_1^{1/2}|}{|C_1|} + z(C_2) - z(C_1) + 2\sum_{\lambda\in\mathrm{Irr}(G^+)} |\lambda(C_2^+) - \lambda(C_1^+)| \sum_{\gamma_\lambda>0} \frac{X_{\gamma_\lambda}}{\sqrt{\frac{1}{4} + \gamma_\lambda^2}},$$

unless $C_1^+ = C_2^+$.

Moreover, under the previous condition, we have

$$\mathbb{E}(X(L/K, C_1, C_2)) = \frac{|C_2^{1/2}|}{|C_2|} - \frac{|C_1^{1/2}|}{|C_1|} + z(C_2) - z(C_1)$$

and

$$\mathrm{Var}(X(L/K, C_1, C_2)) = 2\sum_{\lambda\in\mathrm{Irr}(G^+)} |\lambda(C_1^+) - \lambda(C_2^+)|^2 \sum_{\gamma_\lambda>0} \frac{1}{\frac{1}{4} + \gamma_\lambda^2}.$$

Theorem 2.57 is not the exact transcription of [FJ20a, Proposition 3.18], but it is the same, specialized to the case of the class function $\frac{|G|}{|C_1|}\mathbf{1}_{C_1} - \frac{|G|}{|C_2|}\mathbf{1}_{C_2}$, under the hypothesis LI$^-$: each zero in the sum giving $\mathrm{Var}(X(L/K, C_1, C_2))$ is a zero of exactly one function $s \mapsto L(s, \chi, L/\mathbb{Q})$, with multiplicity one. In other words, the union

$$\Gamma_{L/\mathbb{Q}} = \bigcup_{\chi\in\mathrm{Irr}(G^+)} \Gamma_{L/\mathbb{Q},\chi}$$

is a disjoint union, and each of its elements appears only once in the sums indexed by $\lambda \in \mathrm{Irr}(G^+)$. Note that the expression of $\mathrm{Var}(X(L/K, C_1, C_2))$ involves zeros of L-functions

attached to characters of G^+, not of G. This is because our linear independence and simplicity hypothesis LI^- was stated over $\mathbb{Q}$. If $C_1^+ = C_2^+$ then the approach to Chebyshev's bias initiated by Rubinstein and Sarnak [RS94] and generalized by Ng [Ng00], breaks down. It may then be the case that $\pi(x, C_1, L/K) = \pi(x, C_2, L/K)$ for any $x \geq 2$, but other situations may occur as illustrated in [FJ20b].

The random variables at play are symmetric about their mean m. This is because their characteristic functions are products of Bessel J_0 functions, which are even, multiplied by $t \mapsto \mathrm{e}^{imt}$ ([Ng00, Theorem 5.2.1]). Therefore, it is easily seen that the corresponding logarithmic density δ will be $< \frac{1}{2}$, $> \frac{1}{2}$ or $= \frac{1}{2}$ according to whether $m < 0$, $m > 0$ or $m = 0$, respectively. They also do not have any atoms, as was shown in [Dev19, Theorem 2.2].

We introduce one more quantity in order to state the main results of [FJ20a] on Chebyshev's bias in families of number fields.

Definition 2.58. *Let C_1 and C_2 be conjugacy classes of G such that $C_1^+ \neq C_2^+$. Assuming Artin's conjecture, GRH and LI^-, the bias factor of the race between C_1 and C_2 is*

$$B(L/K, C_1, C_2) := \frac{\mathbb{E}(X(L/K, C_1, C_2))}{\sqrt{\mathrm{Var}(X(L/K, C_1, C_2))}}.$$

Note that the above variance is non-zero since $C_1^+ \neq C_2^+$.

The next theorem is a result giving extremely biased races.

Theorem 2.59 ([FJ20a], Proposition 5.3)**.** *Assume $\mathsf{GRH}, \mathsf{LI}$ and Artin's Conjecture. Then there exists an absolute constant $c_3 > 0$ such that for any conjugacy classes C_1, C_2 of G satisfying $C_1^+ \neq C_2^+$ and $B(L/K, C_1, C_2) > 0$, we have*

$$1 - \delta(L/K, C_1, C_2) < \exp(-c_3 B(L/K, C_1, C_2)^2).$$

Remark 2.60. This theorem is based on a large deviation result due to Montgomery and Odlyzko (see Theorem 2.98 below). The idea is that if the quantity B is positive and large, then the mean of the associated random variable X is large compared to its variance, and the distribution of the random variable X is very concentrated around its (positive) mean, and therefore it takes positive values with high probability.

We are actually able to provide lower bounds in the context of Theorem 2.59, but not as uniform as the previous upper bounds (see Theorem 2.99). This new bound will allow us to exhibit a monotonicity phenomenon in the values of Chebyshev's bias in certain towers of number field extensions (see Theorem 2.104).

The second result can be seen as a converse to the above theorem. We can roughly state it as saying that if the quantity B is small, then the race will be moderately biased, *i.e.* the logarithmic density δ will be close to $\frac{1}{2}$.

Theorem 2.61 ([FJ20a], Theorem 5.10)**.** *Assume* $\mathsf{GRH}, \mathsf{LI}^-$ *and Artin's Conjecture. Then for any conjugacy classes* C_1, C_2 *of* G *such that* $C_1^+ \neq C_2^+$*, if* $|B(L/K, C_1, C_2)|$ *is small enough then we have*

$$\delta(L/K, C_1, C_2) = \frac{1}{2} + \frac{B(L/K, C_1, C_2)}{\sqrt{2\pi}} + O\left(B(L/K, C_1, C_2)^3 + \mathrm{Var}(X(L/K, C_1, C_2))^{-1/3}\right).$$

Remarks 2.62.

i) This result is a consequence of a central limit behaviour for the random variable $X(L/K, C_1, C_2)$ (explaining the $\sqrt{2\pi}$ factor), provided its variance is large enough, which can be established thanks to bounds on Bessel J_0 functions which appear in the characteristic functions of $X(L/K, C_1, C_2)$.

ii) If $\mathbb{E}(X(L/K, C_1, C_2))$ is bounded and $B(L/K, C_1, C_2)$ approaches zero then the main term besides $\frac{1}{2}$ is $\mathrm{Var}(X(L/K, C_1, C_2))^{-1/3}$. On the other hand, if $\mathrm{Var}(X(L/K; C_1, C_2))^{1/6} = o(|\mathbb{E}(X(L/K; C_1, C_2))|)$ and $\mathbb{E}(X(L/K; C_1, C_2)) = o(\mathrm{Var}(X(L/K; C_1, C_2))^{1/2})$ then we have $\delta(L/K, C_1, C_2) - \frac{1}{2} \sim \frac{B(L/K, C_1, C_2)}{\sqrt{2\pi}}$ as $B(L/K, C_1, C_2)$ goes to zero.

2.3.2 Recollection on ramification and on dihedral and quaternion groups of 2-power order

2.3.2.1 Artin conductors

Let L/K be a Galois extension of number fields with Galois group G and C_1, C_2 be distinct conjugacy classes of G. In [FJ20a], bounds for the variance of $X(L/K, C_1, C_2)$ are given in terms of the local ramification data of the extension L/K. More precisely, a link between this variance and the Artin conductors of the irreducible characters of G is established.

Recall that if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ is a prime ideal in $\mathcal{O}_L$ above $\mathfrak{p}$, the inertia subgroup $\mathcal{I}(\mathfrak{P}/\mathfrak{p}) := \{g \in G \mid \forall x \in \mathcal{O}_L, g(x) = x \bmod \mathfrak{P}\} \subset G$ admits a filtration $(G_i(\mathfrak{P}/\mathfrak{p}))_{i\geq 0}$ defined as follows : for integers $i \geq 0$, define

$$G_i(\mathfrak{P}/\mathfrak{p}) := \{g \in G \mid \forall x \in \mathcal{O}_L, g(x) = x \bmod \mathfrak{P}^{i+1}\} \subset G.$$

Obviously, $G_0(\mathfrak{P}/\mathfrak{p}) = \mathcal{I}(\mathfrak{P}/\mathfrak{p})$ and the subgroups $G_i(\mathfrak{P}, \mathfrak{p})$ of G only depend on $\mathfrak{P}$ up to conjugacy, so in the sequel we drop the dependency on $\mathfrak{P}$ and denote them by $G_i(\mathfrak{p})$. It is also known that the elements of this filtration are eventually trivial. We note that if L/K is tamely ramified, then $G_i(\mathfrak{p})$ is trivial for $i \geq 1$ ([Ser80, Chapitre IV §2 Corollaire 3]). If $\rho : G \to \mathbf{GL}(V)$ is a complex representation, we obtain complex representations of all the ramification subgroups $G_i(\mathfrak{p})$ by restriction. If χ is the character ρ, we define

$$n(\chi, \mathfrak{p}) := \sum_{i\geq 0} \frac{|G_i(\mathfrak{p})|}{|G_0(\mathfrak{p})|} \mathrm{codim}(V^{G_i(\mathfrak{p})}),$$

which only depends on $\mathfrak{p}$ and not on $\mathfrak{P}$ since the $G_i(\mathfrak{P}/\mathfrak{p})$ are conjugates in G and so the dimension of their invariant subspaces are all the same. This sum is finite since the $G_i(\mathfrak{p})$ are eventually trivial, but it is also known that this sum is an integer ([Ser80, Chapitre VI §2 Corollaire 2]), so we can finally define the Artin conductor of the character χ by

$$\mathfrak{f}(L/K, \chi) := \prod_{\mathfrak{p}} \mathfrak{p}^{n(\chi, \mathfrak{p})}.$$

This ideal of $\mathcal{O}_K$ is well-defined since it is easy to see that for $\mathfrak{p}$ unramified in L we have $n(\chi, \mathfrak{p}) = 0$, so that there are only finitely many prime ideals actually contributing to the product. We recall the important conductor-discriminant formula ([Ser80, Chapitre VI §3 Corollaire 2]).

Theorem 2.63. *We have*

$$D_{L/K} = \prod_{\chi \in \mathrm{Irr}(G)} \mathfrak{f}(L/K, \chi)^{\chi(1)},$$

where $D_{L/K}$ is the relative discriminant of L/K.

The following quantity appears in the functional equation of the Artin L-functions associated to a character χ.

Definition 2.64 ([MM97] p.28)**.** *For any irreducible character χ of G, define*

$$A(\chi) := |d_K|^{\chi(1)} N_{K/\mathbb{Q}}(\mathfrak{f}(L/K, \chi)),$$

where d_K is the absolute discriminant of K.

Lemma 2.65 ([FJ20a], Lemma 4.3)**.** *Assume Artin's conjecture. Then for any irreducible character χ of G, we have*

$$B_0(\chi) := \sum_{\gamma_\chi \neq 0} \frac{1}{\frac{1}{4} + \gamma_\chi^2} \asymp \log A(\chi).$$

Recall that the sums $B_0(\chi)$, for non-trivial irreducible characters χ of G, appear in the variances in Theorem 2.57. That explains why we will be interested in bounding the quantities $\log A(\chi)$.

2.3.2.2 Character theory of dihedral and quaternion groups of 2-power order

We obtain our main contributions in the setting of Galois extensions of number fields with Galois groups dihedral or quaternion of 2-power order. The goal of this section is to recollect some character-theoretic facts about these groups which will be used throughout sections 3 and 4. Let us first recall the classical presentations of those groups.

Definition 2.66. *Let $n \geq 3$ be an integer. The dihedral group of order 2^n is*

$$D_{2^{n-1}} := \langle r, s \mid r^{2^{n-1}} = s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

The generalized quaternion group of order 2^n is

$$\mathbb{H}_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle.$$

The group $\mathbb{H}_8$ is the usual quaternion group of order 8, with elements usually denoted i, j, k satisfying

$$i^2 = j^2 = k^2 = ijk = -1, (-1)^2 = 1.$$

This notation will be used in section 3. In $D_{2^{n-1}}$, we will denote by -1 the element $r^{2^{n-2}}$, and in $\mathbb{H}_{2^n}$ we will also denote by -1 the element $x^{2^{n-2}} = y^2$. Both of those elements are of

order 2 and generate the center of the respective group they belong to.

These groups are special instances of metacyclic groups (*i.e.* groups admitting a cyclic normal subgroup with cyclic quotient). As a consequence, computations are easily carried in such groups and the conjugacy classes are easily identified ([Ska13]).

Lemma 2.67. *Let $n \geq 3$ be an integer. Then $D_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1, srs^{-1} = r^{-1} \rangle$ has the following $2^{n-2}+3$ conjugacy classes :*

i) The trivial conjugacy class $\{1\}$, denoted by C_1.

ii) The conjugacy class $\{-1\}$, denoted by C_{-1}.

iii) Pairs of powers $\{r^k, r^{-k}\}$ for $1 \leq k \leq 2^{n-2}-1$, denoted by C_{r^k}.

iv) The conjugacy class $\{r^k s \mid 0 \leq k \leq 2^{n-2}-1 \text{ even}\}$ of s, denoted by C_s.

v) The conjugacy class $\{r^k s \mid 0 \leq k \leq 2^{n-1}-1 \text{ odd}\}$ of rs, denoted by C_{rs}.

Lemma 2.68. *Let $n \geq 3$ be an integer. Then $\mathbb{H}_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$ has the following $2^{n-2}+3$ conjugacy classes :*

i) The trivial conjugacy class $\{1\}$, denoted by C_1.

ii) The conjugacy class $\{-1\}$, denoted by C_{-1}.

iii) Pairs of powers $\{x^k, x^{-k}\}$ for $1 \leq k \leq 2^{n-2}-1$, denoted by C_{x^k}.

iv) The conjugacy class $\{x^k y \mid 0 \leq k \leq 2^{n-1}-1 \text{ even}\}$ of y, denoted by C_y.

v) The conjugacy class $\{x^k y \mid 0 \leq k \leq 2^{n-1}-1 \text{ odd}\}$ of xy, denoted by C_{xy}.

In particular, both $D_{2^{n-1}}$ and $\mathbb{H}_{2^n}$ have $2^{n-2}+3$ isomorphism classes of irreducible complex representations. We refer the reader to [Isa94] for classical facts about the representation theory of finite groups. It is a well-known fact that even though those two groups are not isomorphic, they have the same character table.

Lemma 2.69. *Let $n \geq 3$ be an integer and let $D_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1, srs^{-1} = r^{-1} \rangle$. Let also $\zeta_n = \exp\left(\frac{2i\pi}{2^{n-1}}\right) \in \mathbb{C}$. Then the following homomorphisms are representatives of the $2^{n-2}+3$ isomorphism classes of irreducible complex representations of $D_{2^{n-1}}$:*

i) Four abelian representations, coming from the abelianization of $D_{2^{n-1}}$, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, given as follows :

$$\chi_0 : r, s \mapsto 1 \quad \chi_1 : r \mapsto 1, s \mapsto -1 \quad \chi_2 : r \mapsto -1, s \mapsto 1 \quad \chi_3 : r \mapsto -1, s \mapsto -1.$$

ii) For $1 \leq j \leq 2^{n-2}-1$, a degree 2 representation given by :

$$r \mapsto \begin{pmatrix} \zeta_n^j & 0 \\ 0 & \zeta_n^{-j} \end{pmatrix}, \quad s \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

with character denoted by ψ_j.

The character table of $D_{2^{n-1}}$ is

	C_1	C_{-1}	$C_{r^k}, 1 \leq k \leq 2^{n-2}-1$	C_s	C_{rs}
χ_0	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	1	$(-1)^k$	1	-1
χ_3	1	1	$(-1)^k$	-1	1
$\psi_j, 1 \leq j \leq 2^{n-2}-1$	2	$(-1)^j 2$	$\zeta_n^{jk} + \zeta_n^{-jk} = 2\cos\left(\frac{jk\pi}{2^{n-2}}\right)$	0	0

Lemma 2.70. *Let $n \geq 3$ be an integer and let $\mathbb{H}_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$. Let also $\zeta_n = \exp\left(\frac{2i\pi}{2^{n-1}}\right) \in \mathbb{C}$. Then the following homomorphisms are representatives of the $2^{n-2}+3$ isomorphism classes of irreducible complex representations of $\mathbb{H}_{2^n}$:*

i) Four abelian representations, coming from the abelianization of $\mathbb{H}_{2^n}$, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, given as follows :

$$\chi_0 : x, y \mapsto 1 \quad \chi_1 : x \mapsto 1, y \mapsto -1 \quad \chi_2 : x \mapsto -1, y \mapsto 1 \quad \chi_3 : x \mapsto -1, y \mapsto -1.$$

ii) For $1 \leq j \leq 2^{n-2}-1$, a degree 2 representation given by :

$$x \mapsto \begin{pmatrix} \zeta_n^j & 0 \\ 0 & \zeta_n^{-j} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

with character denoted by ψ_j.

The character table of $\mathbb{H}_{2^n}$ is

	C_1	C_{-1}	$C_{x^k}, 1 \leq k \leq 2^{n-2}-1$	C_y	C_{xy}
χ_0	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	1	$(-1)^k$	1	-1
χ_3	1	1	$(-1)^k$	-1	1
$\psi_j, 1 \leq j \leq 2^{n-2}-1$	2	$(-1)^j 2$	$\zeta_n^{jk} + \zeta_n^{-jk} = 2\cos\left(\frac{jk\pi}{2^{n-2}}\right)$	0	0

We remark that all the irreducible characters of $D_{2^{n-1}}$ and $\mathbb{H}_{2^n}$ are real-valued (which does not necessarily mean they are afforded by real-valued representations, see Lemma 2.72) and they have bounded degrees (at most 2) with respect to n.

Lemma 2.71. *With the same notations as in Lemma 2.69, the irreducible character ψ_j of $D_{2^{n-1}}$, for $1 \leq j \leq 2^{n-2}-1$, is faithful if and only if j is odd. The same holds for the irreducible characters of $\mathbb{H}_{2^n}$ as in Lemma 2.70.*

Proof. Recall that a character χ of a group G is faithful if the corresponding representation is faithful (that is, injective). This happens if and only if $\chi(g) \neq \chi(1)$ for any $g \in G \setminus \{1\}$.

Obviously, if j is even then $\psi_j(-1) = 2 = \psi_j(1)$ so ψ_j is not faithful. Conversely, if j is odd, then $\chi(r^k)$ is never equal to 2, for $1 \leq k \leq 2^{n-2}-1$. Indeed, since j is odd, the 2-adic valuation of jk is the same as that of k, which is $< n-2$, therefore $\frac{jk}{2^{n-1}}$ is not an integer, and $\frac{jk\pi}{2^{n-2}} = \frac{2jk\pi}{2^{n-1}}$ is not an integer multiple of 2π. □

Lemma 2.72. *Every irreducible character of $D_{2^{n-1}}$ is orthogonal, and with the same notations as in Lemma 2.70, the irreducible character ψ_j of $\mathbb{H}_{2^n}$, for $1 \leq j \leq 2^{n-2}-1$, is symplectic if and only if j is odd.*

Proof. Clearly, χ_0, χ_1, χ_2 and χ_3 are afforded by real representations so, they are orthogonal (even in the case of $\mathbb{H}_{2^n}$). Consider now a non-abelian character ψ_j, $1 \leq j \leq 2^{n-2}-1$, of $D_{2^{n-1}}$. Then by definition

$$\varepsilon_2(\psi_j) = \frac{1}{2^n} \sum_{g \in D_{2^{n-1}}} \psi_j(g^2).$$

Since each $r^k s$, with $0 \leq k \leq 2^{n-1}-1$, satisfies $(r^k s)^2 = 1$ and $1^2 = 1$, the sum on the right-hand side contains at least $2^{n-1}+1$ terms equal to $\psi_j(1) = 2$. Since this is more than half the number of elements in $D_{2^{n-1}}$ and each $\psi_j(g)$ is smaller than 2 in absolute value, the reverse triangular inequality implies that $\varepsilon_2(\chi) > 0$. By Theorem 2.50 it must be 1, and ψ_j is orthogonal.

Now let ψ_j, $1 \leq j \leq 2^{n-2}-1$, be a non-abelian irreducible character of $\mathbb{H}_{2^n}$. The squares in $\mathbb{H}_{2^n}$ are precisely the even powers of x. Indeed, since $y^{-1} = -y$, we have, for any $k \in \{0, \ldots, 2^{n-1}-1\}$,

$$(x^k y)^2 = -x^k y x^k y^{-1} = -1.$$

From this, and denoting $r(h)$ the number of square roots of $h \in \mathbb{H}_{2^n}$, we see that $r(-1) = 2^{n-1}+2$ while $r(x^{2k}) = 2$ for $0 \leq k \leq 2^{n-3}-1$. Now if j is odd, then

$$\begin{aligned}\varepsilon_2(\psi_j) &= \frac{1}{2^n}\left(4 - 2(2^{n-1}+2) + 4\sum_{k=1}^{2^{n-3}-1} \cos\left(\frac{2jk\pi}{2^{n-2}}\right)\right) \\ &= -1 + \frac{1}{2^{n-2}} \sum_{k=1}^{2^{n-3}-1} \cos\left(\frac{2jk\pi}{2^{n-2}}\right).\end{aligned}$$

It is easily seen from the triangular inequality that this quantity has to be negative. As before, this shows that $\varepsilon_2(\psi_j) = -1$.

Conversely, if j is even, the reverse triangular inequality implies that

$$\varepsilon_2(\psi_j) = \frac{1}{2^n}\left(4 + 2(2^{n-1}+2) + 4\sum_{k=1}^{2^{n-3}-1} \cos\left(\frac{2jk\pi}{2^{n-2}}\right)\right) > 0,$$

which implies that $\varepsilon_2(\psi_j) = 1$. □

Let us remark that for $n \geq 4$, the group $\mathbb{H}_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1}\rangle$ contains $\mathbb{H}_{2^{n-1}}$ as a subgroup generated by $\{x^2, y\}$, and inductively, contains $\mathbb{H}_{2^i} = \langle x^{2^{n-i}}, y\rangle$ for every $3 \leq i \leq n$. Similarly, for $n \geq 3$, $D_{2^{n-2}}$ appears as a subgroup of $D_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1, srs^{-1} = r^{-1}\rangle$ generated by $\langle r^2, s\rangle$. In particular when L/K is a Galois extension of number field extension with group $\mathbb{H}_{2^n}$ or $D_{2^{n-1}}$, it contains subextensions with Galois groups $\mathbb{H}_{2^i}$ or $D_{2^{i-1}}$ for every $3 \leq i \leq n$. To study Chebyshev's bias in such subextensions, we will need to know how irreducible characters are induced from such $\mathbb{H}_{2^i}$ to $\mathbb{H}_{2^n}$, and from $D_{2^{i-1}}$ to $D_{2^{n-1}}$.

Lemma 2.73. *With the same notations as in Lemma 2.70, denote by $\psi_k^{(i)}$, for $3 \leq i \leq n$, $1 \leq k \leq 2^{i-2}-1$, the character of the subgroup $\mathbb{H}_{2^i}$ of $\mathbb{H}_{2^n}$ associated to the representation*

$$x^{2^{n-i}} \mapsto \begin{pmatrix} \zeta_i^k & 0 \\ 0 & \zeta_i^{-k} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

and denote by $\chi_0^{(i)}, \chi_1^{(i)}, \chi_2^{(i)}$ and $\chi_3^{(i)}$ the four abelian characters of $\mathbb{H}_{2^i}$ corresponding to the notations of Lemma 2.70. For $k \in \{1, \dots, 2^{i-2}-1\}$, one has

$$\mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \psi_k^{(i)} = \sum_{\substack{1 \leq l \leq 2^{n-2}-1 \\ l = \pm k \bmod 2^{i-1}}} \psi_l.$$

Also,

$$\mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \chi_0^{(i)} = \mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \chi_1^{(i)} = \chi_0 + \chi_1 + \chi_2 + \chi_3 + \sum_{\substack{1 \leq j \leq 2^{n-2}-1 \\ j = 0 \bmod 2^{i-1}}} \psi_j$$

and

$$\mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \chi_2^{(i)} = \mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \chi_3^{(i)} = \sum_{\substack{1 \leq j \leq 2^{n-2}-1 \\ j = 0 \bmod 2^{i-2}, j \neq 0 \bmod 2^{i-1}}} \psi_j.$$

Those equalities also hold when $\mathbb{H}_{2^n}$ and $\mathbb{H}_{2^i}$ are replaced by $D_{2^{n-1}}$ and $D_{2^{i-1}}$ respectively.

Proof. Let $1 \leq j \leq 2^{n-2}-1$. We use the Frobenius reciprocity formula and the character table in Lemma 2.70 to compute

$$\begin{aligned}
\langle \mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \psi_k^{(i)}, \psi_j \rangle_{\mathbb{H}_{2^n}} = \langle \psi_k^{(i)}, \psi_{j|\mathbb{H}_{2^i}} \rangle_{\mathbb{H}_{2^i}} &= \frac{1}{2^i} \sum_{g \in \mathbb{H}_{2^i}} \psi_k^{(i)}(g) \overline{\psi_j(g)} \\
&= \frac{1}{2^i} \left(2 \cdot 2 + (-1)^{k+j} \cdot 4 + 2 \sum_{1 \leq l \leq 2^{i-2}-1} \psi_k^{(i)}(x^{2^{n-i}l}) \overline{\psi_j(x^{2^{n-i}l})} \right) \\
&= \frac{1}{2^i} \left(4(1 + (-1)^{k+j}) + 2 \sum_{1 \leq l \leq 2^{i-2}-1} \left(\zeta_i^{kl} + \zeta_i^{-kl} \right) \left(\zeta_n^{jl2^{n-i}} + \zeta_n^{-jl2^{n-i}} \right) \right).
\end{aligned}$$

Since $\zeta_n^{2^m} = \zeta_{n-m}$ for any $0 \leq m \leq n-1$, we find

$$\begin{aligned}
\langle \mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \psi_k^{(i)}, \psi_j \rangle_{\mathbb{H}_{2^n}} &= \frac{1}{2^i} \left(4(1 + (-1)^{k+j}) + 2 \sum_{1 \leq l \leq 2^{i-2}-1} \left(\zeta_i^{kl} + \zeta_i^{-kl} \right) \left(\zeta_i^{jl} + \zeta_i^{-jl} \right) \right) \\
&= \frac{1}{2^i} \left(4(1 + (-1)^{k+j}) + 2 \sum_{1 \leq l \leq 2^{i-2}-1} \left(\zeta_i^{(k+j)l} + \zeta_i^{-(k+j)l} + \zeta_i^{(k-j)l} + \zeta_i^{(j-k)l} \right) \right) \\
&= \frac{1}{2^i} \left(4(1 + (-1)^{k+j}) + 2 \sum_{\substack{1 \leq l \leq 2^{i-1}-1 \\ l \neq 2^{i-2}}} \left(\zeta_i^{(k+j)l} + \zeta_i^{(k-j)l} \right) \right).
\end{aligned}$$

Now, if $k+j=0 \bmod 2^{i-1}$ then $k-j \neq 0 \bmod 2^{i-1}$, otherwise we would get $2k=0 \bmod 2^{i-1}$, *i.e.* $k=0 \bmod 2^{i-2}$, which cannot be because $1 \leq k \leq 2^{i-2}-1$. Therefore, the geometric progressions missing two terms sum to

$$\sum_{\substack{1\leq l\leq 2^{i-1}-1 \\ l\neq 2^{i-2}}} \left(\zeta_i^{(k+j)l}+\zeta_i^{(k-j)l}\right) = 2^{i-1}-2+\left(\frac{1-\zeta_i^{(k-j)2^{i-1}}}{1-\zeta_i^{(k-j)}}-\zeta_i^{(k-j)2^{i-2}}-1\right)$$
$$= 2^{i-1}-4.$$

Similarly, if $k-j=0 \bmod 2^{i-1}$, then $k+j \neq 0 \bmod 2^{i-1}$, and we find

$$\sum_{\substack{1\leq l\leq 2^{i-1}-1 \\ l\neq 2^{i-2}}} \left(\zeta_i^{(k+j)l}+\zeta_i^{(k-j)l}\right) = 2^{i-1}-4.$$

Finally, if $k+j \neq 0 \bmod 2^{i-1}$ and $k-j \neq 0 \bmod 2^{i-1}$, we find

$$\sum_{\substack{1\leq l\leq 2^{i-1}-1 \\ l\neq 2^{i-2}}} \left(\zeta_i^{(k+j)l}+\zeta_i^{(k-j)l}\right) = -(-1)^{k+j}\cdot 2-2.$$

To sum up, we have found

$$\langle \mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \psi_k^{(i)}, \psi_j\rangle_{\mathbb{H}_{2^n}} = \begin{cases} 1 \text{ if } k+j=0 \bmod 2^{i-1} \text{ or } k-j=0 \bmod 2^{i-1} \\ 0 \text{ otherwise} \end{cases}.$$

We have found 2^{n-i} irreducible components of $\mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \psi_k^{(i)}$ of degree 2. Since $\mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \psi_k^{(i)}(1) = [\mathbb{H}_{2^n}:\mathbb{H}_{2^i}]\psi_k^{(i)}(1) = 2^{n-i+1}$, these are the only ones.

The other induced characters are computed in a similar manner, using the Frobenius reciprocity formula. The fact that $\mathbb{H}_{2^n}$ and $D_{2^{n-1}}$ have the same character table with conjugacy classes indexed similarly with respect to their generators imply that the same computations work in the $D_{2^{n-1}}$ case. □

Corollary 2.74. *Let $3 \leq i \leq n-1$. If $\chi \in \mathrm{Irr}(\mathbb{H}_{2^i})$ then for any $\chi' \in \mathrm{Irr}(\mathbb{H}_{2^i}) \setminus \{\chi\}$, inducing from $\mathbb{H}_{2^i}$ to $\mathbb{H}_{2^n}$ we have $(\chi,\chi')=1$ unless $\deg(\chi)=1$, where $(\chi,\chi')=1$ means that $\langle \mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \chi, \mathrm{Ind}_{\mathbb{H}_{2^i}}^{\mathbb{H}_{2^n}} \chi'\rangle = 0$ (see the paragraph above Theorem 2.99). This also holds when $\mathbb{H}_{2^n}$ and $\mathbb{H}_{2^i}$ are replaced by $D_{2^{n-1}}$ and $D_{2^{i-1}}$ respectively.*

The above conditions will allow us to obtain a lower bound for $1-\delta$ for relative number field extensions (i.e. with base field different from $\mathbb{Q}$) with Galois groups $\mathbb{H}_{2^i}$ and $\mathcal{D}_{2^{i-1}}$ using Theorem 2.99.

The following lemma will be used to compute moments in Section 4.

Lemma 2.75. *For $i \geq 3$ and $1 \leq k \leq 2^{i-2}-1$,*

$$\sum_{\substack{j=1 \\ j \text{ odd}}}^{2^{i-2}-1} \left(\zeta_i^{jk}+\zeta_i^{-jk}\right) = 0.$$

Proof. This is clear for $i = 3$, so assume $i \geq 4$. This sum can be rewritten

$$\sum_{j=1}^{2^{i-2}-1} \left(\zeta_i^{jk} + \zeta_i^{-jk}\right) - \sum_{h=1}^{2^{i-3}-1} \left(\zeta_i^{2hk} + \zeta_i^{-2hk}\right).$$

As in the previous proof, we see that the first sum is simply

$$\sum_{j=0}^{2^{i-1}-1} \zeta_i^{jk} - \zeta_i^0 - \zeta_i^{k2^{i-2}} = -1 - (-1)^k$$

since $0 < k < 2^{i-1}$ and so $\zeta_i^k \neq 1$. The second sum

$$\sum_{h=1}^{2^{i-3}-1} \left(\zeta_i^{2hk} + \zeta_i^{-2hk}\right)$$

is being dealt with similarly, because $\zeta_i^2 = \zeta_{i-1}$ and $0 < k < 2^{i-2}$, so it also equals $-1-(-1)^k$. Thus the two sums cancel each other. □

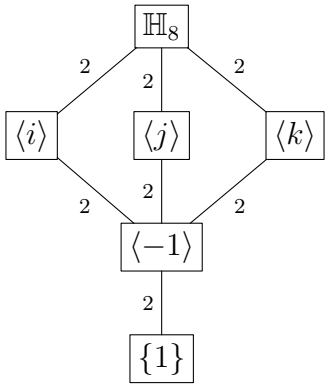
2.3.3 Extensions of $\mathbb{Q}$ of group $\mathbb{H}_8$: horizontal Chebotarev biases

In this section, we will depart temporarily from the notations we used in section 2, and we will use the more familiar i, j, k notations for elements of $\mathbb{H}_8$. Our goal is to prove Theorem A. We will be constructing two distinct families of number fields with Galois group over $\mathbb{Q}$ isomorphic to $\mathbb{H}_8$ and with opposite biases along each family, due to the existence or not of a central zero for the corresponding Dedekind zeta functions.

Recall that $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group of order 8. Its elements all commute with -1 and satisfy the following relations

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ki = j \text{ and } ik = -j.$$

Here is the lattice of subgroups of $\mathbb{H}_8$ (see [Deb16])



The character table of $\mathbb{H}_8$ is

	C_1	C_{-1}	C_i	C_j	C_k
χ_0	1	1	1	1	1
χ_i	1	1	1	-1	-1
χ_j	1	1	-1	1	-1
χ_k	1	1	-1	-1	1
ψ	2	-2	0	0	0

where C_x denotes the conjugacy class of $x \in \mathbb{H}_8$.

Let $K/\mathbb{Q}$ be a Galois extension, with Galois group G isomorphic to $\mathbb{H}_8$. Assuming LI, we can compute the values of the different means and variances, according to the formulas given in Theorem 2.57 (since

$$\mathbb{E}(X(K/\mathbb{Q}, C_1, C_2)) = -\mathbb{E}(X(K/\mathbb{Q}, C_2, C_1)) \text{ and } \operatorname{Var}(X(K/\mathbb{Q}, C_1, C_2)) = \operatorname{Var}(X(K/\mathbb{Q}, C_2, C_1)),$$

there are only $\binom{5}{2} = 10$ races to consider).

Proposition 2.76. *Assume* LI *for the extension* $K/\mathbb{Q}$. *Let* $\mathfrak{o} = \operatorname{ord}_{s=\frac{1}{2}} L(s, \psi, K/\mathbb{Q})$, *where* ψ *is the non-abelian character of* $\mathbb{H}_8$ *in the above character table. Then one has*

a	b	$\mathbb{E}(X(K/\mathbb{Q}, C_a, C_b))$	$\operatorname{Var}(X(K/\mathbb{Q}, C_a, C_b))$
1	-1	$4(1-2\mathfrak{o})$	$16B_0(\psi)$
1	i,j,k	$-2(1+2\mathfrak{o})$	$4\sum_{\chi\neq\chi_b} B_0(\chi)$
-1	i,j,k	$2(2\mathfrak{o}-3)$	$4\sum_{\chi\neq\chi_b} B_0(\chi)$
i,j,k	i,j,k	0	$4B_0(\chi_a)+4B_0(\chi_b)$

where B_0 *is defined in Lemma 2.65.*

Remarks 2.77. Let us make a few comments on these values :

i) The presence or not of a zero at $\frac{1}{2}$ for $s \mapsto L(s, \psi, K/\mathbb{Q})$ changes the sign of $\mathbb{E}(X(K/\mathbb{Q}, C_1, C_{-1}))$.
ii) The race between C_1 and C_b, for $b \in \{i, j, k\}$, is always biased towards C_b. This was expected since 1 is a square in G, and b is not.
iii) The presence or not of a zero with multiplicity at least 2 at $\frac{1}{2}$ for $s \mapsto L(s, \psi, K/\mathbb{Q})$ changes the sign of $\mathbb{E}(X(K/\mathbb{Q}, C_{-1}, C_b))$, for $b \in \{i, j, k\}$.
iv) There is no bias in the race between C_a and C_b, for $a \in \{i, j, k\}$ and $b \in \{i, j, k\} \setminus \{a\}$.

Since we will be using the hypothesis LI^+, under which the order of vanishing $\mathfrak{o}$ can only be 0 or 1, and we want to exhibit a change of leading conjugacy class in Chebotarev races, we will now focus on the conjugacy classes C_1 and C_{-1}. When $K/\mathbb{Q}$ is tamely ramified, we can deduce more precise bounds for the variances.

Proposition 2.78. *Assume* LI^- *and that* $K/\mathbb{Q}$ *is tamely ramified. Then*

$$\operatorname{Var}(X(K/\mathbb{Q}, C_1, C_{-1})) \asymp \log|d_K|.$$

Proof. Since $K/\mathbb{Q}$ tame, the filtration of the inertia subgroup (see section 2.1) at any prime number ramified in K only has length 1, *i.e.* for any prime p and $i \geq 1$, $|G_i(p)| = 1$. In particular, for any non-trivial character χ of G and any prime number p, one has

$$n(\chi, p) = \operatorname{codim} V^{\mathcal{I}(p)},$$

where V is the space of the representation affording χ.

Using the definition, we find for any prime p ramified in K (so that $\mathcal{I}(p) = G_0(p) \neq \{1\}$),

$$n(\chi_i, p) = \begin{cases} 1 \text{ if } \mathcal{I}(p) = \langle j \rangle \text{ or } \mathcal{I}(p) = \langle k \rangle \\ 0 \text{ otherwise,} \end{cases}$$

$$n(\chi_j, p) = \begin{cases} 1 \text{ if } \mathcal{I}(p) = \langle i \rangle \text{ or } \mathcal{I}(p) = \langle k \rangle \\ 0 \text{ otherwise,} \end{cases}$$

$$n(\chi_k, p) = \begin{cases} 1 \text{ if } \mathcal{I}(p) = \langle i \rangle \text{ or } \mathcal{I}(p) = \langle j \rangle \\ 0 \text{ otherwise} \end{cases}$$

and

$$n(\psi, p) = 2.$$

This yields

$$\mathfrak{f}(K/\mathbb{Q}, \chi_i) = \prod_{\substack{p | d_K \\ \mathcal{I}(p) = \langle j \rangle}} p \times \prod_{\substack{p | d_K \\ \mathcal{I}(p) = \langle k \rangle}} p,$$

$$\mathfrak{f}(K/\mathbb{Q}, \chi_j) = \prod_{\substack{p | d_K \\ \mathcal{I}(p) = \langle i \rangle}} p \times \prod_{\substack{p | d_K \\ \mathcal{I}(p) = \langle k \rangle}} p,$$

$$\mathfrak{f}(K/\mathbb{Q}, \chi_k) = \prod_{\substack{p | d_K \\ \mathcal{I}(p) = \langle i \rangle}} p \times \prod_{\substack{p | d_K \\ \mathcal{I}(p) = \langle j \rangle}} p$$

and

$$\mathfrak{f}(K/\mathbb{Q}, \psi) = \prod_{p | d_K} p^2.$$

Since the base field is $\mathbb{Q}$, we have $A(\chi) = \mathfrak{f}(K/\mathbb{Q}, \chi)$ for any character χ of G, and the conductor-discriminant formula (Theorem 2.63) thus gives

$$|d_K| = \prod_{\substack{p | d_K \\ e_p = 8}} p^4 \prod_{\substack{p | d_K \\ e_p = 4}} p^6 \prod_{\substack{p | d_K \\ e_p = 2}} p^4,$$

where e_p is the ramification index of the ramified prime p. In particular, we have

$$A(\psi)^2 \leq d_K \leq A(\psi)^3,$$

so that

$$\log A(\psi) \asymp \log d_K.$$

Finally, Theorem 2.57 and Lemma 2.65 yield

$$\mathrm{Var}(X(K/\mathbb{Q}, C_1, C_{-1})) \asymp B_0(\psi) \asymp \log A(\psi) \asymp \log |d_K|.$$

□

The fact that a bound such as Proposition 2.78 holds follows from the fact that the character ψ is faithful, because this implies that each ramified prime appears with positive

exponent in $A(\chi) = \{(K/\mathbb{Q}, \psi)$. This observation will be used again in our study of biases in towers of extensions (see Proposition 2.87).

We will use the following theorem of Fröhlich to construct the quaternion extensions of $\mathbb{Q}$ we will be interested in :

Theorem 2.79 ([Frö72])**.** *Let d be a square-free integer, $d > 1$ and $d = 1$ mod 4. Let $\mathfrak{R}$ be a finite set of primes unramified in $\mathbb{Q}(\sqrt{d})$ and not containing 2. Then there exist infinitely many tamely ramified extensions $K/\mathbb{Q}$ and $L/\mathbb{Q}$ such that :*

i) $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{H}_8$.
ii) $\mathbb{Q}(\sqrt{d}) \subset K \cap L$.
iii) Every prime in $\mathfrak{R}$ is ramified in K and L.
iv) $W(\psi, K/\mathbb{Q}) = -1$ *and* $W(\psi, L/\mathbb{Q}) = 1$.

Remark 2.80. Theorem 2.79 is in fact a weak version of Fröhlich's theorem in [Frö72]. Actually, one can specify any finite number of unramified primes in K and L as well (the ramification must be compatible with the fact that $\mathbb{Q}(\sqrt{d}) \subset K \cap L$), and one can also ask for K and L to be totally real or totally imaginary.

Corollary 2.81. *For any square-free integer $d > 1$ with $d = 1$ mod 4 and any prime p, there exist infinitely many tamely ramified extensions $K/\mathbb{Q}$ and $L/\mathbb{Q}$ such that :*

i) $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{H}_8$.
ii) $\mathbb{Q}(\sqrt{d}) \subset K \cap L$.
iii) p is ramified in K and L.
iv) $L\left(\frac{1}{2}, \psi, K/\mathbb{Q}\right) = 0$ *and if* LI^+ *holds then* $L\left(\frac{1}{2}, \psi, L/\mathbb{Q}\right) \neq 0$.

Proof. The existence of the number fields K follows from Theorem 2.79 without the assumption of LI^+ : we consider tamely ramified extensions $K/\mathbb{Q}$ with Galois group $\mathbb{H}_8$, ramified at p, containing $\mathbb{Q}(\sqrt{d})$ and such that $W(\psi) = -1$. Proposition 2.51 shows that $L(1/2, \psi, K/\mathbb{Q}) = 0$.

The existence of the number fields L follows similarly because, assuming LI^+, $W(\psi) = 1$ implies that $s \mapsto L(s, \psi, L/\mathbb{Q})$ does not vanish at $\frac{1}{2}$. □

We are now ready to prove Theorem A, which we recall for convenience.

Theorem 2.82. *Assume* GRH *and* LI^+*. For any function f such that $f(n) \underset{n\to+\infty}{\longrightarrow} +\infty$, there exist two infinite families $(K_d)_d$ and $(L_d)_d$ of Galois extensions of $\mathbb{Q}$, indexed by square-free integers satisfying $d > 1$ and $d = 1$ mod 4, such that for any d in the index set :*

i) $\mathbb{Q}(\sqrt{d}) \subset K_d \cap L_d$.
ii) $\mathrm{Gal}(K_d/\mathbb{Q}) \simeq \mathrm{Gal}(L_d/\mathbb{Q}) \simeq \mathbb{H}_8$.
iii) $0 < \frac{1}{2} - \delta(K_d/\mathbb{Q}, C_1, C_{-1}) \ll \frac{1}{f(d)}$.
iv) $0 < \delta(L_d/\mathbb{Q}, C_1, C_{-1}) - \frac{1}{2} \ll \frac{1}{f(d)}$.

Proof. For any square-free $d > 1$ with $d = 1$ mod 4, we choose a field K_d given in the first part of Corollary 2.81, ramified at the smallest prime larger than $e^{f(d)^3}$. By construction of K_d we have

$$B(X(K_d/\mathbb{Q}, C_1, C_{-1})) = \frac{\mathbb{E}(X(K_d/\mathbb{Q}, C_1, C_{-1}))}{\sqrt{\mathrm{Var}(X(K_d/\mathbb{Q}, C_1, C_{-1}))}} = \frac{1 - 2\mathfrak{o}}{B_0(\psi)^{1/2}} = -\frac{1}{B_0(\psi)^{1/2}}.$$

In particular, $\mathbb{E}(X(K_d/\mathbb{Q}, C_1, C_{-1}))$ is negative, because of the existence of a real zero of $s \mapsto L(s, \psi, K_d/\mathbb{Q})$, and this implies that $\delta(K_d/\mathbb{Q}, C_1, C_{-1}) < \frac{1}{2}$. Lemma 2.65 yields

$$B_0(\psi) \asymp \log A(\psi),$$

and as we saw in the proof of Proposition 2.78 we have

$$\log A(\psi) \asymp \log |d_{K_d}|,$$

since ψ is faithful and $K_d/\mathbb{Q}$ is tamely ramified. Moreover, since $K_d/\mathbb{Q}$ is ramified at the smallest prime larger than $e^{f(d)^3}$, we have

$$\log |d_{K_d}| \gg \log \left(e^{f(d)^3}\right) = f(d)^3.$$

Therefore,

$$|B(X(K_d/\mathbb{Q}, C_1, C_{-1}))| \ll \frac{1}{f(d)^{3/2}}.$$

Similarly, we have

$$\mathrm{Var}(X(K_d/\mathbb{Q}, C_1, C_{-1}))^{-1} \ll \frac{1}{f(d)^3}.$$

Since Artin's conjecture holds for extensions with Galois group $\mathbb{H}_8$ (recall that this group is supersolvable, and that Artin's conjecture is known in that case), Theorem 2.61 implies that

$$0 < \frac{1}{2} - \delta(K_d/\mathbb{Q}, C_1, C_{-1}) \ll \frac{1}{f(d)}.$$

The construction of L_d follows along the same lines, by choosing fields as in the second part of Corollary 2.81. In that case, the mean is positive because there is no real zero of $s \mapsto L(s, \psi, L_d/\mathbb{Q})$, so $\delta(K_d/\mathbb{Q}, C_1, C_{-1}) > \frac{1}{2}$, and the estimates are the same. □

Remark 2.83. If we had a statement analoguous to Theorem 2.79 in which we could specify if $s \mapsto L(s, \psi, K/\mathbb{Q})$ vanishes, or not, at $\frac{1}{2}$ with multiplicty at least two, then we would be able to obtain a result similar to Theorem A for the race between C_{-1} and C_b, for $b \in \{i, j, k\}$, *i.e.* moderately biased races with biases of opposite signs, bounded in absolute value by $\frac{1}{f(d)}$, for any function f going to infinity. Such a result would of course contradict LI^+.

2.3.4 Chebyshev's bias in towers

We now consider the vertical aspect of our problem. Our goal is to prove Theorems B, C and D. Instead of working with a family of extensions of $\mathbb{Q}$ with fixed Galois group, we want to study different Galois extensions of $\mathbb{Q}$ with Galois groups dihedral of order a power of two or generalized quaternion of increasing sizes. We also want to compare Chebyshev's bias in subextensions. For this to make sense, we need to make a few observations first.

For $n \geq 4$, $\mathbb{H}_{2^{n-1}}$ appears as a (normal) subgroup of $\mathbb{H}_{2^n}$. Indeed, if $\mathbb{H}_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$, then it is easy to see that $\langle x^2, x^k y \rangle$ is a normal subgroup of $\mathbb{H}_{2^n}$ isomorphic to $\mathbb{H}_{2^{n-1}}$, for any $0 \leq k \leq 2^{n-2} - 1$. Therefore, if $K/\mathbb{Q}$ is a number field extension with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{H}_{2^n}$ then there exist number fields $K \supset K_3 \supset K_4 \supset \cdots \supset K_{n-1} \supset K_n = \mathbb{Q}$

with $\mathrm{Gal}(K/K_i) \simeq \mathbb{H}_{2^i}$ for all $3 \leq i \leq n$, namely the subfields fixed by $\langle x^{2^{n-i}}, y\rangle$. In the following, we will always assume that the quaternion subgroups have been chosen so that $\mathrm{Gal}(K/K_i)$ is generated by $x^{2^{n-i}}$ and y, for $3 \leq i \leq n-1$. Similarly, if $n \geq 3$ then $D_{2^{n-1}}$ is a normal subgroup of $D_{2^n} = \langle r, s \mid r^{2^{n-1}} = s^2, srs^{-1} = r^{-1}\rangle$, generated for example by r^2 and s. Those observations will allow us to compare Chebyshev's bias in subextensions (see Theorem 2.104).

2.3.4.1 Moments in generalized quaternion Galois groups

In this section, we compute bounds on the moments of the random variables attached to the different Chebotarev races in number field extensions with Galois group generalized quaternion. They will be used in the proof of Theorem C.

We will use the following fact about root numbers of symplectic characters of generalized quaternion groups.

Theorem 2.84 ([Frö74], Theorem 3)**.** *Let N/L be a tamely ramified extension of number fields, with Galois group generalized quaternion. Then the root numbers of the symplectic irreducible characters of* $\mathrm{Gal}(N/L)$ *are all equal.*

Now, let $n \geq 3$, and assume that $K/\mathbb{Q}$ is a Galois extension with Galois group

$$G := \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1}\rangle \simeq \mathbb{H}_{2^n},$$

and let $\mathbb{Q} = K_n \subset \cdots \subset K_3 \subset K$ be intermediate number fields as before, that is

$$G_i := \langle x^{2^{n-i}}, y\rangle \simeq \mathbb{H}_{2^i}$$

and

$$K_i := K^{G_i},$$

for $3 \leq i \leq n$. We will denote $x^{2^{n-i}}$ by x_i so that $G_i = \langle x_i, y\rangle$. Conjugacy classes in G_i will be denoted, according to our notations in Lemma 2.68, by $C_1^{(i)}, C_{-1}^{(i)}, C_{x_i^k}^{(i)}, C_y^{(i)}$ and $C_{x_iy}^{(i)}$. Note that each G_i is supersolvable, so Artin's conjecture is known to hold for Artin L-functions attached to irreducible characters of G_i.

Recall that if C is a conjugacy class of G_i, then C^+ is the conjugacy class $\bigcup_{g\in G} gCg^{-1}$ of $G_i^+ = G$. The following lemma is immediate.

Lemma 2.85. *Let $i \in \{3, \ldots, n-1\}$. Using the notations of section 2, we have*

i) $C_1^{(i)+} = C_1$.

ii) $C_{-1}^{(i)+} = C_{-1}$.

iii) For any $1 \leq k \leq 2^{i-2} - 1$, $C_{x_i^k}^{(i)+} = C_{x_i^k}$.

iv) $C_y^{(i)+} = C_y$.

v) $C_{x_iy}^{(i)+} = C_y$.

In particular, if C_1 and C_2 are distinct conjugacy classes of G_i, then $C_1^+ \neq C_2^+$, unless, $\{C_1, C_2\} = \{C_y^{(i)}, C_{x_iy}^{(i)}\}$.

When $K/\mathbb{Q}$ is tamely ramified, we denote by W_{K/K_i} the root number of any of the symplectic characters of $\mathrm{Gal}(K/K_i)$. We first relate the root numbers of symplectic characters of G to those of each G_i, and the orders of vanishing at $1/2$ of the corresponding Artin L-functions.

Proposition 2.86. *Assume* LI^+ *and assume* $K/\mathbb{Q}$ *is tamely ramified. Then for any* $3 \leq i \leq n$*, we have* $W_{K/K_i} = W_K$*, where* $W_K = W_{K/\mathbb{Q}}$ *is the root number of any symplectic character of* G*. Moreover, if* $W_K = -1$ *then only the symplectic characters of* G_i *have their Artin L-function vanish at* $1/2$*, and the order of vanishing is* 2^{n-i}*.*

Proof. Clearly, K/K_i is tamely ramified so our definition of W_{K/K_i} makes sense using Theorem 2.84. For any $3 \leq j \leq n$, consider the classical decomposition

$$\begin{aligned}\zeta_K(s) &= L(s, \chi_0, K/K)\\ &= L(s, \mathrm{Ind}_{\{1\}}^{G_j} \chi_0, K/K_j)\\ &= L(s, \mathrm{reg}_{G_j}, K/K_j)\\ &= L(s, \sum_{\chi \in \mathrm{Irr}(G_j)} \chi(1)\chi, K/K_j)\\ &= \prod_{\chi \in \mathrm{Irr}(G_j)} L(s, \chi, K/K_j)^{\chi(1)},\end{aligned}$$

where reg_{G_j} is the character of the regular representation of G_j.

If $W_K = 1$, consider the previous factorization with $j = n$. By LI^+, none of the factors vanish at $1/2$, and so ζ_K does not vanish at $1/2$. Using now the decomposition with $j = i$, we see that $L(1/2, \chi, K/K_i) \neq 0$ for each irreducible character χ of G_i. In particular, $W_{K/K_i} \neq -1$, i.e. $W_{K/K_i} = 1$.

Conversely, if $W_K = -1$, then ζ_K vanishes at $1/2$ to order 2^{n-2}. Indeed, under LI^+, the only factors that vanish at $1/2$ are the $L(s, \chi, K/\mathbb{Q})^{\chi(1)}$ for $\chi = \chi_0$ or χ symplectic. There are 2^{n-3} symplectic characters, all vanishing at $1/2$ to order one (again, because of LI^+, and the fact all such characters have root number -1) and satisfying $\chi(1) = 2$. Moreover, $L(s, \chi_0, K/\mathbb{Q}) = \zeta(s)$ is the classical Riemann ζ function, which is known not to vanish at $1/2$. Using Lemma 2.73, we see that for $1 \leq k \leq 2^{i-2} - 1$ odd we have

$$\begin{aligned}L(s, \psi_k^{(i)}, K/K_i) &= L(s, \mathrm{Ind}_{G_i}^{G} \psi_k^{(i)}, K/\mathbb{Q})\\ &= L(s, \sum_{\substack{0 \leq l \leq 2^{n-2}-1\\ l = \pm k \bmod 2^{i-1}}} \psi_l, K/\mathbb{Q})\\ &= \prod_{\substack{0 \leq l \leq 2^{n-2}-1\\ l = \pm k \bmod 2^{i-1}}} L(s, \psi_l, K/\mathbb{Q}).\end{aligned}$$

Since each $L(s, \psi_l, K/\mathbb{Q})$, with $1 \leq l \leq 2^{n-2} - 1$ odd, vanishes at $1/2$ to order one, we see that each $L(s, \psi_k^{(i)}, K/K_i)$ vanishes at $1/2$ as well, to order 2^{n-i}, for $1 \leq k \leq 2^{i-2} - 1$ odd. In particular, $W_{K/K_i} = -1$. Moreover, the 2^{i-3} symplectic characters of G_i contribute to the vanishing of ζ_K at $1/2$ to order $2 \times 2^{i-3} \times 2^{n-i} = 2^{n-2}$, so no other irreducible character of G_i have its Artin L-function vanishing at $1/2$. □

In Propositions 2.87, 2.88 and 2.89, we give bounds on the variances and compute the means of the random variables attached to the Chebotarev races in the extensions K/K_i.

Proposition 2.87. *Assume* GRH *and* LI$^-$. *Then for any* $3 \leq i \leq n$ *and any distinct conjugacy classes* C_1, C_2 *of* G_i *such that* $\{C_1, C_2\} \neq \{C_y^{(i)}, C_{x_iy}^{(i)}\}$,

$$\mathrm{Var}(X(K/K_i, C_1, C_2)) \ll \log |d_K|.$$

Moreover if $K/\mathbb{Q}$ *is tamely ramified and* $\{C_1, C_2\} \not\subset \{C_{x_i^{2^{i-3}}}^{(i)}, C_y^{(i)}, C_{x_iy}^{(i)}\}$ *then for any* $3 \leq i \leq n$,

$$\mathrm{Var}(X(K/K_i, C_1, C_2)) \gg \frac{\log |d_K|}{16^n},$$

and if $\{C_1, C_2\} \cap \{C_{x_i^k}^{(i)} \mid 1 \leq k \leq 2^{i-2} - 1\} = \emptyset$ *this can be improved to*

$$\mathrm{Var}(X(K/K_i, C_1, C_2)) \gg \log |d_K|.$$

Proof. By Lemma 2.85, the condition $\{C_1, C_2\} \neq \{C_y^{(i)}, C_{x_iy}^{(i)}\}$ ensures that $C_1^+ \neq C_2^+$. Recall that

$$\mathrm{Var}(X(K/K_i, C_1, C_2)) = \sum_{\chi \in \mathrm{Irr}(G^+)} |\chi(C_1^+) - \chi(C_2^+)|^2 B_0(\chi)$$

by Theorem 2.57, with

$$B_0(\chi) \asymp \log A(\chi)$$

by Lemma 2.65. In particular, we see using Lemma 2.85 that our estimates on $\mathrm{Var}(X(K/K_i, C_1, C_2))$ do not depend on K_i, so it is enough to prove them in the case $i = n$, that is $K_i = \mathbb{Q}$.

Since the values taken by the irreducible characters of G are bounded in absolute value uniformly in n, we get

$$\mathrm{Var}(X(K/\mathbb{Q}, C_1, C_2)) \ll \sum_{\chi \in \mathrm{Irr}(G)} \log A(\chi) \leq \sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \log A(\chi).$$

Recall that for any irreducible character χ of G,

$$A(\chi) = \mathfrak{f}(K/\mathbb{Q}, \chi)$$

is the Artin conductor of χ, so the conductor-discriminant formula (Theorem 2.63) yields

$$\begin{aligned} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \log A(\chi) &= \sum_{\chi} \chi(1) \log \mathfrak{f}(K/\mathbb{Q}, \chi) \\ &= \log |d_K|. \end{aligned}$$

This proves the stated upper bound.

To prove the first lower bound, assume $K/\mathbb{Q}$ is tamely ramified. If χ is an irreducible symplectic character of G then χ is faithful by Lemma 2.71. This implies that there are no invariant vectors for the representation of character χ. Moreover, since $K/\mathbb{Q}$ is tamely ramified, the ramification groups of index ≥ 2 are trivial for any prime p ramified in K,

and for any such prime we find $n(\chi, p) = 2$ (see section 2.1 for the definition of $n(\chi, p)$). In particular,

$$A(\chi) = \mathfrak{f}(K/\mathbb{Q}, \chi) = \prod_{p | d_K} p^2.$$

Now, since $K/\mathbb{Q}$ is tamely ramified, each prime $\mathfrak{p}$ of K above a ramified prime number p appears in the factorization of $\partial_{K/\mathbb{Q}}$, the different of $K/\mathbb{Q}$, with exponent $e_\mathfrak{p} - 1$ where $e_\mathfrak{p}$ denotes the corresponding ramification index ([Neu99, Theorem 2.6]). Since the discriminant of $K/\mathbb{Q}$ is the $K/\mathbb{Q}$-norm of the different, this yields

$$|d_K| = \prod_{\mathfrak{p} | \partial_{K/\mathbb{Q}}} N_{K/\mathbb{Q}}(\mathfrak{p})^{e_\mathfrak{p} - 1} = \prod_{p | d_K} p^{(e_p - 1) f_p g_p},$$

where f_p (respectively g_p) denotes the residual degree of (respectively the number of primes above) the prime p. In particular, this exponent is less than $e_p f_p g_p = [K : \mathbb{Q}] = 2^n$. Therefore we have

$$\begin{aligned} \prod_{p | d_K} p^{2^n} &\geq \prod_{p | d_K} p^{(e_p - 1) f_p g_p} \\ &= |d_K|. \end{aligned}$$

Recall there are exactly 2^{n-3} symplectic characters of G, so we find

$$\begin{aligned} \prod_{\chi \text{ symplectic}} A(\chi) &= \prod_{p | d_K} p^{2^{n-2}} \\ &\geq |d_K|^{1/4}, \end{aligned}$$

and we find

$$\sum_{\chi \text{ symplectic}} \log A(\chi) \gg \log |d_K|.$$

We now need to lower bound the quantity $|\chi(C_1) - \chi(C_2)|$ as χ ranges over the set of symplectic characters of G. A straightforward inspection of all cases shows that $\chi(C_1) = \chi(C_2)$ can only happen if $\{C_1, C_2\} \subset \{C_{x^{2^{n-3}}}, C_y, C_{xy}\}$. In all the other cases, we see that the minimum value of $|\chi(C_1) - \chi(C_2)|$, when χ varies in the set of symplectic irreducible characters of G, is $\gg \frac{1}{4^n}$. Indeed, if $\{C_1, C_2\} = \{C_{x^k}, C_{x^l}\}$ with $1 \leq k < l \leq 2^{n-2} - 1$, then by the mean value theorem, we have for any $1 \leq j \leq 2^{n-2} - 1$,

$$|\psi_j(C_1) - \psi_j(C_2)| = 2 \left| \cos\left(\frac{jk\pi}{2^{n-2}}\right) - \cos\left(\frac{jl\pi}{2^{n-2}}\right) \right| = \frac{j|k-l|\pi}{2^{n-3}} |\sin(\xi_n)|$$

for some $\frac{jk\pi}{2^{n-2}} < \xi_n < \frac{jl\pi}{2^{n-2}}$. By π-periodicity of $|\sin|$ and the fact that $x \mapsto \left|\sin\left(\frac{\pi}{2} - x\right)\right|$ is even, it is easy to see that $|\sin(\xi_n)| = |\sin(\xi_n')|$ for some $\frac{\pi}{2^{n-2}} < |\xi_n'| < \frac{\pi}{2}$ (*i.e.* we move to the first quadrant). By the classical inequality $|\sin(x)| \geq \frac{2}{\pi}|x|$ for $|x| \leq \frac{\pi}{2}$ and the fact that $|k - l| \geq 1$ and $j \geq 1$ we finally get $|\psi_j(C_1) - \psi_j(C_2)| \gg \frac{1}{4^n}$. The cases involving C_1, C_{-1}, C_y and C_{xy} are similar. This yields

$$\mathrm{Var}(X(K/\mathbb{Q}, C_1, C_2)) \gg \frac{1}{16^n} \sum_{\chi \text{ symplectic}} \log A(\chi) \gg \frac{\log |d_K|}{16^n}.$$

As for the last lower bound, if $\{C_1, C_2\} \cap \{C_{x^k} \mid 1 \leq k \leq 2^{n-2}-1\} = \emptyset$ then we actually have $|\chi(C_1) - \chi(C_2)| \geq 2$ for χ irreducible symplectic, so

$$\mathrm{Var}(X(K/\mathbb{Q}, C_1, C_2)) \gg \sum_{\chi \text{ symplectic}} \log A(\chi) \gg \log |d_K|.$$

□

Proposition 2.88. *Assume* GRH *and* LI^+. *If $K/\mathbb{Q}$ is tamely ramified then for any $3 \leq i \leq n$,*

$$\mathbb{E}(X(K/K_i, C_1^{(i)}, C_{-1}^{(i)})) = -2^{n-1}(1 - W_K) + 2^{i-1},$$

where $W_k = W_{k/\mathbb{Q}}$ is the root number of any symplectic character of G.

Proof. From Theorem 2.57 we have

$$\mathbb{E}(X(K/K_i, C_1^{(i)}, C_{-1}^{(i)})) = \frac{|(C_{-1}^{(i)})^{1/2}|}{|C_{-1}^{(i)}|} - \frac{|(C_1^{(i)})^{1/2}|}{|C_1^{(i)}|} + 2 \sum_{\chi \neq \chi_0} (\chi(C_{-1}^{(i)}) - \chi(C_1^{(i)})) \operatorname{ord}_{s=1/2} L(s, \chi, K/K_i).$$

Since we are assuming LI^+, Proposition 2.86 shows that only symplectic characters, i.e. the $\psi_j^{(i)}$ with $1 \leq j \leq 2^{i-2}-1$ odd, contribute to the sum. By the same proposition, their root numbers are all equal to W_K and the order of vanishing of their Artin L-functions is 0 or 2^{n-i}, so

$$2 \sum_{\chi \neq \chi_0} (\chi(C_{-1}^{(i)}) - \chi(C_1^{(i)})) \operatorname{ord}_{s=1/2} L(s, \chi, K/K_i) = \begin{cases} 0 \text{ if } W_K = 1 \\ 2 \sum_{\chi \text{ symplectic}} (-4) \cdot 2^{n-i} = -2^n \text{ if } W_K = -1. \end{cases}$$

In the proof of Lemma 2.72, we have observed that -1 has $2^{i-1}+2$ square roots in $\mathrm{Gal}(K/K_i)$, while 1 has 2. This yields

$$\mathbb{E}(X(K/K_i, C_1^{(i)}, C_{-1}^{(i)})) = \begin{cases} 2^{i-1} \text{ if } W_K = 1 \\ 2^{i-1} - 2^n \text{ if } W_K = -1. \end{cases}$$

□

For the sake of completeness, we give below an exhaustive list of $\mathbb{E}(X(K/K_i, C_1, C_2))$ for each $3 \leq i \leq n$ and for all possible choices of distinct conjugacy classes C_1, C_2 of G_i.

Proposition 2.89. *Assume* GRH *and* LI^+. *If $K/\mathbb{Q}$ is tamely ramified then for any $3 \leq i \leq n$,*

C_1	C_2	$\mathbb{E}(X(K/K_i, C_1, C_2))$	*Conditions on the classes*
$C_1^{(i)}$	$C_{-1}^{(i)}$	$-2^{n-1}(1-W_K) + 2^{i-1}$	*none*
$C_1^{(i)}$	$C_{x_i^k}^{(i)}$	$-2^{n-2}(1-W_K) + (-1)^k - 1$	$1 \leq k \leq 2^{i-2}-1$
$C_1^{(i)}$	$C_y^{(i)}/C_{x_iy}^{(i)}$	$-2^{n-2}(1-W_K) - 2$	*none*
$C_{-1}^{(i)}$	$C_{x_i^k}^{(i)}$	$2^{n-2}(1-W_K) - 1 + (-1)^k - 2^{i-1}$	$1 \leq k \leq 2^{i-2}-1$
$C_{-1}^{(i)}$	$C_y^{(i)}/C_{x_iy}^{(i)}$	$2^{n-2}(1-W_K) - 2 - 2^{i-1}$	*none*
$C_{x_i^k}^{(i)}$	$C_{x_i^l}^{(i)}$	$(-1)^l - (-1)^k$	$1 \leq k, l \leq 2^{i-2}-1, k \neq l$
$C_{x_i^k}^{(i)}$	$C_y^{(i)}/C_{x_iy}^{(i)}$	$(-1)^{k+1} - 1$	$1 \leq k \leq 2^{i-2}-1$
$C_y^{(i)}$	$C_{x_iy}^{(i)}$	0	*none*

Proof. The first row was computed in Proposition 2.88. Each of the sums

$$\sum_{\chi \neq \chi_0} \chi(C_{x_i^k}^{(i)}) \operatorname{ord}_{s=1/2} L(s, \chi, K/K_i)$$

for $1 \leq k \leq 2^{i-2} - 1$ is zero, because Proposition 2.86 shows they only involve symplectic characters, for which $\operatorname{ord}_{s=1/2} L(s, \chi, K/K_i)$ does not depend on χ, and those sums reduce to

$$\operatorname{ord}_{s=1/2} L(s, \psi_1^{(i)}, K/K_i) \sum_{\substack{j=1 \\ j \text{ odd}}}^{2^{i-2}-1} \left(\zeta_i^{jk} + \zeta_i^{-jk}\right),$$

which is zero by Lemma 2.75. Therefore using Theorem 2.57, we see that the remaining computations only involves counting square roots in $G_i \simeq \mathbb{H}_{2^i}$, and, when one of the conjugacy classes is $C_1^{(i)}$ or $C_{-1}^{(i)}$, the fact there are 2^{i-3} irreducible symplectic characters of G_i with L-functions vanishing at $1/2$ to order $2^{n-i-1}(1 - W_K)$. The last row is clear because the elements of $C_y^{(i)}$ and $C_{x_i y}^{(i)}$ have no square root in G_i and symplectic characters vanish on those conjugacy classes. □

The table of 2.89 that any Chebotarev race involving the classes $C_1^{(i)}$ or $C_{-1}^{(i)}$ is influenced by the root number of symplectic characters of G.

2.3.4.2 Moments in dihedral Galois groups of order a power of two

We now turn to the case of number field extensions with dihedral Galois group of 2-power order. The same methods as in the previous section are applied to get bounds on the moments of the random variables attached to the different Chebotarev races in such extensions. Those bounds will be used to prove Theorem B.

Let $n \geq 2$ and let $L/\mathbb{Q}$ be a Galois extension with Galois group $D_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1, srs^{-1} = r^{-1} \rangle$. Let $\mathbb{Q} = L_n \subset L_{n-1} \subset \cdots \subset L_3 \subset L$ be the subextensions such that $G_i := \langle r^{2^{n-i}}, s \rangle$ and $L_i = L^{G_i}$. We will denote $r^{2^{n-i}}$ by r_i. Conjugacy classes in G_i will be denoted, following our notations in Lemma 2.67, by $C_1^{(i)}, C_{-1}^{(i)}, C_{r_i^k}^{(i)}, C_s^{(i)}$ and $C_{r_i s}^{(i)}$. The estimates from the previous section are proved similarly in the dihedral case, so we state them without proof. Since each irreducible character of $D_{2^{n-1}}$ is orthogonal by Lemma 2.72, and since we will be working under the hypothesis LI, no considerations on root numbers are involved.

Proposition 2.90. *Assume* GRH *and* LI$^-$*. Then for any $2 \leq i \leq n$ and any distinct conjugacy classes C_1, C_2 of G_i such that $\{C_1, C_2\} \neq \{C_s^{(i)}, C_{r_i s}^{(i)}\}$,*

$$\operatorname{Var}(X(L/L_i, C_1, C_2)) \ll \log |d_L|.$$

Moreover if $L/\mathbb{Q}$ is tamely ramified and $\{C_1, C_2\} \not\subset \{C_{r_i^{2^{i-3}}}^{(i)}, C_s^{(i)}, C_{r_i s}^{(i)}\}$ then for any $2 \leq i \leq n$,

$$\operatorname{Var}(X(L/L_i, C_1, C_2)) \gg \frac{\log |d_L|}{16^n},$$

and if $\{C_1, C_2\} \cap \{C_{r_i^k}^{(i)} \mid 1 \leq k \leq 2^{i-2}-1\} = \emptyset$ *this can be improved to*

$$\mathrm{Var}(X(L/L_i, C_1, C_2)) \gg \log |d_L|.$$

Proposition 2.91. *Assume* GRH *and* LI. *For any* $3 \leq i \leq n$,

C_1	C_2	$\mathbb{E}(X(L/L_i, C_1, C_2))$	*Conditions on the classes*
$C_1^{(i)}$	$C_{-1}^{(i)}$	-2^{i-1}	*none*
$C_1^{(i)}$	$C_{r_i^k}^{(i)}$	$-2^{i-1}+(-1)^k-1$	$1 \leq k \leq 2^{i-2}-1$
$C_1^{(i)}$	$C_s^{(i)}/C_{r_i s}^{(i)}$	$-2^{i-1}-2$	*none*
$C_{-1}^{(i)}$	$C_{r_i^k}^{(i)}$	$(-1)^k-1$	$1 \leq k \leq 2^{i-2}-1$
$C_{-1}^{(i)}$	$C_s^{(i)}/C_{r_i s}^{(i)}$	-2	*none*
$C_{r_i^k}^{(i)}$	$C_{r_i^l}^{(i)}$	$(-1)^l-(-1)^k$	$1 \leq k, l \leq 2^{i-2}-1, k \neq l$
$C_{r_i^k}^{(i)}$	$C_s^{(i)}/C_{r_i s}^{(i)}$	$(-1)^{k+1}-1$	$1 \leq k \leq 2^{i-2}-1$
$C_s^{(i)}$	$C_{r_i s}^{(i)}$	0	*none*

2.3.4.3 Construction of the towers

We now construct towers of dihedral and generalized quaternion extensions of $\mathbb{Q}$ which are tamely ramified, and with controlled discriminants, properties which will enable us to apply effectively the results from sections 4.1 and 4.2.

Proposition 2.92. *Assume* GRH *for the Dedekind zeta functions of the number fields* $\mathbb{Q}(\sqrt[5\cdot 2^{n-1}]{\varepsilon}, \mu_{5\cdot 2^{n-1}})$, *where* μ_k *denotes a primitive* k*-th root of unity and* $\varepsilon = \frac{3+\sqrt{5}}{2}$. *There exists a sequence* $(\mathcal{D}_n)_{n\geq 3}$ *of number fields such that for any* $n \geq 3$ *:*

i) The extension $\mathcal{D}_n/\mathbb{Q}$ *is tamely ramified and Galois with Galois group isomorphic to the dihedral group* $D_{2^{n-1}}$ *of order* 2^n.

ii) $\mathbb{Q}(\sqrt{5}) \subset \mathcal{D}_n$.

iii) $2^n \ll \log |d_{\mathcal{D}_n/\mathbb{Q}}| \ll n2^n$.

Proof. Fix $K = \mathbb{Q}(\sqrt{5})$, let $n \geq 3$ and let $\varepsilon = \frac{3+\sqrt{5}}{2}$ be the fundamental totally positive unit of K. Using class field theory, it is shown in the proof of [Pla04, Theorem 3.2] that there exists a number field $\mathcal{D}_n$ which has Galois group over $\mathbb{Q}$ isomorphic to $D_{2^{n-1}}$, containing K and such that only 5 and another odd prime p ramify in $\mathcal{D}_n$. The prime number p is chosen so that p splits in the extension $M_n := \mathbb{Q}(\sqrt[5\cdot 2^{n-1}]{\varepsilon}, \mu_{5\cdot 2^{n-1}})$.

Using the bound for the least prime ideal in the Chebotarev density theorem stated in [LMO79, (1.2)], we can find such a p satisfying

$$p \ll (\log |d_{M_n}|)^2.$$

Now, M_n is obtained in at most $2n$ steps of adjoining square roots of algebraic units, starting from the field $\mathbb{Q}(\sqrt[5]{\varepsilon}, \mu_5)$. If M/L is one of those steps, we have $M = L(\sqrt{\eta})$, where η is a unit of L, and the relative discriminant $D_{M/L}$ has to divide the discriminant of $X^2-\eta$, which is $4\eta\mathcal{O}_L = 4\mathcal{O}_L$. Since

$$|d_M| = N_{L/\mathbb{Q}}(D_{M/L})|d_L|^{[M:L]} \leq 4^{[L:\mathbb{Q}]}|d_L|^2,$$

we find

$$|d_M|^{\frac{1}{[M:\mathbb{Q}]}} \leq 2|d_L|^{\frac{1}{[L:\mathbb{Q}]}}.$$

Using this iteratively on the (at most) $2n$ steps, we find that

$$|d_{M_n}|^{\frac{1}{[M_n:\mathbb{Q}]}} \ll 2^{2n}.$$

Using the same reasoning, we see that

$$[M_n : \mathbb{Q}] \ll 4^n,$$

so finally we can choose the prime p so that

$$p \ll (n[M_n : \mathbb{Q}])^2 \ll n^2 16^n.$$

As in the proof of Proposition 2.87,

$$|d_{\mathcal{D}_n}| = 5^{(e_5-1)f_5g_5} \times p^{(e_p-1)f_pg_p} \leq (5p)^{2^n},$$

where e_q (respectively f_q, g_q) denotes the ramification index of the prime number q (respectively the residual degree of q, the number of primes above q). This shows that

$$\log|d_{\mathcal{D}_n}| \ll 2^n \log p \ll n2^n.$$

The lower bound on the discriminant simply comes from Minkowski's bound ([Lan94] p.120)

$$|d_{\mathcal{D}_n}| \geq \frac{2^{n2^n}}{(2^n)!}\left(\frac{\pi}{4}\right)^{2^{n-1}}.$$

Since $[\mathcal{D}_n : \mathbb{Q}] = 2^n$ and $d_{\mathcal{D}_n}$ is odd, $\mathcal{D}_n/\mathbb{Q}$ is tamely ramified. □

Remark 2.93. The quadratic field $\mathbb{Q}(\sqrt{5})$ plays no particular role in our construction. For our purpose, we could replace the integer 5 by any positive square-free integer d which is 1 mod 4.

Proposition 2.94. *Assume* GRH. *There exists two sequences* $(\mathcal{Q}_n^+)_{n\geq 3}$ *and* $(\mathcal{Q}_n^-)_{n\geq 3}$ *of number fields such that for any* $n \geq 3$ *:*

i) The extension $\mathcal{Q}_n^\pm/\mathbb{Q}$ *is tamely ramified and Galois with Galois group isomorphic to the generalized quaternion group* $\mathbb{H}_{2^n}$*.*
ii) $\mathbb{Q}(\sqrt{5}) \subset \mathcal{Q}_n^\pm$*.*
iii) $2^n \ll \log|d_{\mathcal{Q}_n^\pm/\mathbb{Q}}| \ll n2^n$*.*
iv) $W_{\mathcal{Q}_n^+} = 1$ *and* $W_{\mathcal{Q}_n^-} = -1$*.*

Proof. We use the same notations as in the proof of Proposition 2.92 : we let $K = \mathbb{Q}(\sqrt{5})$ and $\varepsilon = \frac{3+\sqrt{5}}{2}$ be the fundamental totally positive unit of K. We use again a theorem of Fröhlich [Frö83, Chapter V, Proposition 3.1]. It states that for $e \in \{-1, 1\}$, the set of prime numbers p such that there exists a number field $N[p]$ such that the only ramified primes in $N[p]$ are 5 and p, satisfying $\mathrm{Gal}(N[p]/\mathbb{Q}) \simeq \mathbb{H}_{2^n}$, $\mathbb{Q}(\sqrt{5}) \subset N[p]$ and $W_{N[p]} = e$ have positive density. It is shown by translating the last two conditions into an arithmetic condition on p, and then

using Chebotarev's density theorem. The arithmetic condition amounts to prescribing the Frobenius conjugacy class of p in $\mathrm{Gal}(M_n'/\mathbb{Q})$, where $M_n' = K(\mu_{2^{n-1}}, \sqrt[2^{n-2}]{\varepsilon})$, with $\mu_{2^{n-1}}$ a primitive 2^{n-1}-th root of unity. As in the proof of Proposition 2.92, we apply, under GRH, the bound on the least prime ideal in Chebotarev's density theorem of [LMO79] to choose

$$p \ll (\log |d_{M_n'}|)^2 \ll n^2 16^n.$$

Call $\mathcal{Q}_n^{\pm}$ the number field constructed this way (the superscript $\pm$ indicating which root number was prescribed). Since only 5 and p ramify in $\mathcal{Q}_n^{\pm}$, we get as in the proof of Proposition 2.92

$$\log |d_{\mathcal{Q}_n^{\pm}/\mathbb{Q}}| \ll n2^n.$$

The lower bound on the discriminant follows once again from Minkowski's bound, and tame ramification follows from the fact that $d_{\mathcal{Q}_n^{\pm}}$ is odd. □

Remark 2.95. If we do not want to specify the root numbers in our quaternion extensions of $\mathbb{Q}$, we could use the methods of [DM73] to construct extensions of $\mathbb{Q}$ satisfying i), ii) and iii) using the extensions $\mathcal{D}_n/\mathbb{Q}$ of Proposition 2.92. Indeed, it is shown in [DM73] that, if $Q/\mathbb{Q}$ is a tamely ramified extension with Galois group $\mathbb{H}_8$ and $\mathbb{Q}(\sqrt{5}) \subset Q$ (again, the number 5 has no particular significance), then the composite field $Q\mathcal{D}_n$ contains a subfield Q_n with Galois group $\mathbb{H}_{2^n}$ over $\mathbb{Q}$, and the upper bound on $\log |d_{\mathcal{D}_n}|$ then implies a similar bound on $\log |d_{Q_n}|$. Tame ramification follows from the tame ramification of $Q/\mathbb{Q}$ and $\mathcal{D}_n/\mathbb{Q}$, and the lower bound on the discriminant from Minkowski's bound.

2.3.4.4 A large deviation result for Chebyshev's bias

In this section we prove a lower bound in the context of Theorem 2.59. We will make use of the following bounds on sums of zeros of Artin L-functions. The first one is the so-called Riemann-Von Mangoldt formula, stated in [IK04], in the particular case of Artin L-functions, for which the conductor of $s \mapsto L(s, \chi, L/K)$ is simply $A(\chi)$ and its analytic conductor is bounded by $A(\chi)(|s|+4)^{[K:\mathbb{Q}]\chi(1)}$ (see [IK04, §5.13]).

Lemma 2.96. *Let χ be an irreducible character of G, and for any $T > 0$, define $N(T, \chi)$ to be the number of zeros $\rho = \beta + i\gamma$ of $s \mapsto L(s, \chi, L/K)$ with $0 \leq \beta \leq 1$ and $0 < \gamma \leq T$. Then we have*

$$N(T, \chi) = \frac{T}{2\pi} \log \left(A(\chi) \left(\frac{T}{2\pi e} \right)^{[K:\mathbb{Q}]\chi(1)} \right) + O\left(\log \left(A(\chi)(T+4)^{[K:\mathbb{Q}]\chi(1)} \right) \right).$$

Proof. This is essentially [IK04, Theorem 5.8], except that we are counting zeros $\beta + i\gamma$ with $0 < \gamma \leq T$ and not $|\gamma| \leq T$. Our main term is half the one in [IK04, Theorem 5.8], in which the count is made by adding the contributions of zeros $\beta + i\gamma$ with $\gamma \geq 0$ for $s \mapsto L(s, \chi, L/K)$ and for $s \mapsto L(s, \overline{\chi}, L/K)$. It is also stated in the proof that the number of real zeros is taken into account in the error term. □

Lemma 2.97 ([FJ20a], Lemma 5.4)**.** *Assume Artin's conjecture. Then for any irreducible character χ of G and for $T \geq 1$, we have*

$$\sum_{0<\gamma_\chi\leq T} \frac{1}{\sqrt{\frac{1}{4}+\gamma_\chi^2}} = \frac{\log T}{2\pi}\log\left(A(\chi)\left(\frac{T^{1/2}}{2\pi e}\right)^{[K:\mathbb{Q}]\chi(1)}\right) + O\left(\log\left(A(\chi)(T+4)^{[K:\mathbb{Q}]\chi(1)}\right)\right).$$

In order to state our improvement of Theorem 2.59, we first recall the large deviation result of Montgomery and Odlyzko which was used to derive Theorem 2.59, and will be used to prove Theorem 2.99.

Theorem 2.98 ([MO88], Theorem 2)**.** *Let $(W_n)_{n\geq 1}$ be a family of independent real random variables such that*

i) For all $n \geq 1$, $\mathbb{E}(W_n) = 0$.

ii) For all $n \geq 1$, $|W_n| \leq 1$ a.s.

iii) There exists $c > 0$ such that for all $n \geq 1$, $\mathbb{E}(W_n^2) > c$.

Let $(r_n)_n$ be a real sequence decreasing to zero such that $\sum_{n\geq 1} r_n^2 < +\infty$ and let $W = \sum_{n\geq 1} r_n W_n$. Let $V \geq 0$ and $\alpha > 0$. If $\sum_{r_n\geq\alpha} r_n \leq \frac{V}{2}$ then

$$\mathbb{P}(W \geq V) \leq \exp\left(-\frac{1}{16}V^2\left(\sum_{r_n<\alpha} r_n^2\right)^{-1}\right),$$

If $\sum_{r_n\geq\alpha} r_n \geq 2V$ then

$$\mathbb{P}(W \geq V) \geq a_1\exp\left(-a_2V^2\left(\sum_{r_n<\alpha} r_n^2\right)^{-1}\right),$$

where a_1 and a_2 are positive constants depending only on c.

The following theorem provides a lower bound for $1-\delta$, which was not obtained in [FJ20a], in the context of Theorem 2.59. The proof proceeds by taking into account distinct characters of G whose corresponding induced characters to G^+ are not orthogonal, which in general leads to complications in estimating Chebyshev's bias. This is because, in Theorem 2.57, the means are expressed using values of characters of G, while the variances involve values of characters of G^+.

Before stating the result, we set a few notations for readability. If $\chi \in \mathrm{Irr}(G)$ and $\lambda \in \mathrm{Irr}(G^+)$ we will write $\lambda \mid \chi$ if $\langle\lambda, \mathrm{Ind}_G^{G^+}\chi\rangle \neq 0$, that is if λ is a component of the character $\mathrm{Ind}_G^{G^+}\chi$ of G^+, and $\lambda \nmid \chi$ otherwise. For $\chi, \chi' \in \mathrm{Irr}(G)$, we write $(\chi, \chi') = 1$ when $\langle\mathrm{Ind}_G^{G^+}\chi, \mathrm{Ind}_G^{G^+}\chi'\rangle = 0$, *i.e.* when $\lambda \mid \chi$ implies $\lambda \nmid \chi'$.

Theorem 2.99. *Assume* GRH, LI *and Artin's Conjecture. Let*

$$S = \{\chi \in \mathrm{Irr}(G) \mid \forall\chi' \in \mathrm{Irr}(G)\setminus\{\chi\}, (\chi,\chi') = 1\}$$

and $R = \mathrm{Irr}(G)\backslash(S\cup\{\chi_0\})$. *Let* $b_1 := \max_{\chi\in R}\chi(1)$, $b_2 := |R|$ *and* $M = \max_{\chi\in R}\mathrm{ord}_{s=1/2}\,L(s,\chi,L/K)+1$. *There exist absolute constants* $c_1, c_2 > 0$ *such that for any conjugacy classes* C_1, C_2 *of* G *satisfying* $C_1^+ \neq C_2^+$ *and* $B(L/K, C_1, C_2) > 0$, *we have*

$$c_1 \exp\left(-c_2 Q(C_1,C_2) B(L/K,C_1,C_2)^2\right) \leq 1 - \delta(L/K,C_1,C_2)$$

where $Q(C_1,C_2) = \max\left(e^{C\sqrt{\frac{Mb_1b_2}{\lambda^*(1)b_3(C_1,C_2)}}}, C\frac{b_3(C_1,C_2)}{b_4(C_1,C_2)}, C\right)$ *for some absolute constant* $C > 0$ *and where* $\lambda^* \in \mathrm{Irr}(G^+)$ *is such that* $|\lambda^*(C_2^+) - \lambda^*(C_1^+)| = \max_{\lambda\in\mathrm{Irr}(G^+)}|\lambda(C_2^+) - \lambda(C_1^+)| =: b_3(C_1,C_2) > 0$ *and* $b_4(C_1,C_2) = \min_{\lambda\in\mathrm{Irr}(G^+),\lambda(C_2^+)\neq\lambda(C_1^+)}|\lambda(C_2^+) - \lambda(C_1^+)| > 0$.

Proof. We introduce the random variable $W = X(L/K,C_1,C_2) - \mathbb{E}(X(L/K,C_1,C_2))$. It obviously satisfies the hypotheses of Theorem 2.98 with $(r_n)_n$ the ordered sequence of non-zero $\frac{2|\lambda(C_2^+)-\lambda(C_1^+)|}{\sqrt{\frac{1}{4}+\gamma_\lambda^2}}$, λ varying in $\mathrm{Irr}(G^+)$ and γ_λ in $\Gamma_{L/\mathbb{Q},\lambda}$, and $(W_n)_n$ the accordingly ordered sequence of X_γ. Indeed, the series

$$\sum_{\gamma_\lambda>0}\frac{1}{\frac{1}{4}+\gamma_\lambda^2}$$

converges for any $\lambda \in \mathrm{Irr}(G^+)$.

We set $V = \mathbb{E}(X(L/K,C_1,C_2))$ and look for $\alpha > 0$ such that $\sum_{r_n\geq\alpha} r_n \geq 2V$. By Theorem 2.57, we have

$$\begin{aligned}\mathbb{E}(X(L/K,C_1,C_2)) &= \frac{|C_2^{1/2}|}{|C_2|} - \frac{|C_1^{1/2}|}{|C_1|} + z(C_2) - z(C_1)\\ &= \sum_{\chi\in\mathrm{Irr}(G)}(\chi(C_2)-\chi(C_1))(\varepsilon_2(\chi) + 2\,\mathrm{ord}_{s=1/2}\,L(s,\chi,L/K)).\end{aligned}$$

If $\chi \in S$, then for some $\lambda \in \mathrm{Irr}(G^+)$ we have, by a quick computation using the Frobenius reciprocity formula,

$$\begin{aligned}|\lambda(C_2^+) - \lambda(C_1^+)| = |\lambda_{|G}(C_2) - \lambda_{|G}(C_1)| &= \left|\sum_{\chi'\in\mathrm{Irr}(G)}(\chi'(C_2)-\chi'(C_1))\langle\lambda_{|G},\chi'\rangle\right|\\ &= |\chi(C_2)-\chi(C_1)|\langle\lambda,\mathrm{Ind}_G^{G^+}\chi\rangle.\end{aligned}$$

From the factorisation

$$L(s,\chi,L/K) = \prod_{\lambda\in\mathrm{Irr}(G^+)} L(s,\lambda,L/\mathbb{Q})^{\langle\lambda,\mathrm{Ind}_G^{G^+}\chi\rangle},$$

we see that

$$\mathrm{ord}_{s=1/2}\,L(s,\chi,L/K) = \sum_{\lambda\in\mathrm{Irr}(G^+)}\langle\lambda,\mathrm{Ind}_G^{G^+}\chi\rangle\,\mathrm{ord}_{s=1/2}\,L(s,\lambda,L/\mathbb{Q}) \leq M_0\sum_{\lambda\in\mathrm{Irr}(G^+)}\langle\lambda,\mathrm{Ind}_G^{G^+}\chi\rangle$$

(recall that M_0 comes from the hypothesis LI). Therefore,

$$\begin{aligned}\sum_{\chi\in S}(\chi(C_2)-\chi(C_1))(\varepsilon_2(\chi)+2\operatorname{ord}_{s=1/2}L(s,\chi,L/K)) &\leq \sum_{\chi\in S}|\chi(C_2)-\chi(C_1)|(1+2M_0\sum_{\lambda|\chi}\langle\lambda,\operatorname{Ind}_G^{G^+}\chi\rangle)\\ &= (1+2M_0)\sum_{\lambda\in S^+}|\lambda(C_2^+)-\lambda(C_1^+)|\end{aligned}$$

where $S^+=\{\lambda\in\operatorname{Irr}(G^+)\mid\exists\chi\in S,\lambda\mid\chi\}$. We now see that it is enough to have

$$\sum_{0<\gamma_\lambda\leq T_0(\lambda)}\frac{1}{\sqrt{\frac{1}{4}+\gamma_\lambda^2}}\geq(2+4M_0)$$

for any $\lambda\in S^+$ and some $T_0(\lambda)>0$, to bound from above the contribution of characters of S in $2V$. It remains to bound from above the sum

$$2\sum_{\chi\in R}(\chi(C_2)-\chi(C_1))(\varepsilon(\chi)+2\operatorname{ord}_{s=1/2}L(s,\chi,L/K))\leq 4M\sum_{\chi\in R}|\chi(C_2)-\chi(C_1)|.$$

By definition of b_1 and b_2, this last sum is $\leq 8Mb_1b_2$, so we choose $T_0(\lambda^*)>0$ such that

$$\sum_{0<\gamma_{\lambda^*}\leq T_0(\lambda^*)}\frac{1}{\sqrt{\frac{1}{4}+\gamma_{\lambda^*}^2}}\geq\frac{8Mb_1b_2}{b_3(C_1,C_2)}.$$

To do so, we use Lemma 2.97 (for the extension $L/\mathbb{Q}$) to get

$$\sum_{0<\gamma_\lambda\leq T}\frac{1}{\sqrt{\frac{1}{4}+\gamma_\lambda^2}}=\frac{\log T}{2\pi}\log\left(A(\lambda)\left(\frac{T^{1/2}}{2\pi e}\right)^{\lambda(1)}\right)+O\left(\log\left(A(\lambda)(T+4)^{\lambda(1)}\right)\right)$$

for any $\lambda\in\operatorname{Irr}(G^+)$. A simple computation shows that it is enough to choose $T_0(\lambda^*)=\max\left((2\pi e)^4,e^{\sqrt{\frac{64\pi Mb_1b_2}{\lambda^*(1)b_3(C_1,C_2)}}},e^{16\pi C'}\right)$ to ensure

$$\sum_{0<\gamma_{\lambda^*}<T_0(\lambda^*)}\frac{1}{\sqrt{\frac{1}{4}+\gamma_{\lambda^*}^2}}\geq\frac{8Mb_1b_2}{b_3(C_1,C_2)},$$

where $C'>0$ is such that

$$\left|\sum_{0<\gamma_{\lambda^*}\leq T}\frac{1}{\sqrt{\frac{1}{4}+\gamma_{\lambda^*}^2}}-\frac{\log T}{2\pi}\log\left(A(\lambda^*)\left(\frac{T^{1/2}}{2\pi e}\right)^{\lambda^*(1)}\right)\right|\leq C'\log\left(A(\lambda^*)(T+4)^{\lambda^*(1)}\right),$$

while we have

$$\sum_{0<\gamma_\lambda\leq A}\frac{1}{\sqrt{\frac{1}{4}+\gamma_\lambda^2}}\geq(2+4M_0)$$

for any $\lambda\in\operatorname{Irr}(G^+)$ and some absolute constant $A>0$, so we set $T_0(\lambda)=A$ for every $\lambda\neq\lambda^*$.

We now turn to the choice of $\alpha \geq 0$ such that

$$\sum_{r_n \geq \alpha} r_n \geq 2V.$$

It is enough to have

$$\sum_{r_n \geq \alpha} r_n \geq \sum_{\lambda \in \mathrm{Irr}(G^+)} \sum_{0 < \gamma_\lambda \leq T_0(\lambda)} \frac{2|\lambda(C_2^+) - \lambda(C_1^+)|}{\sqrt{\frac{1}{4} + \gamma_\lambda^2}},$$

so we require that

$$0 < \gamma_\lambda \leq T_0(\lambda) \Rightarrow \gamma_\lambda \leq \sqrt{\frac{4|\lambda(C_2^+) - \lambda(C_1^+)|^2}{\alpha^2} - \frac{1}{4}} =: R_{\alpha,\lambda}.$$

We choose α to be the minimal (positive) value of $\frac{2|\lambda(C_2^+) - \lambda(C_1^+)|}{\sqrt{\frac{1}{4} + T_0(\lambda)^2}}$, attained for some $\lambda_m \in \mathrm{Irr}(G^+)$ (recall that we discarded the characters $\lambda \in \mathrm{Irr}(G^+)$ such that $\lambda(C_2^+) = \lambda(C_1^+)$ in our definition of the r_n's). For this choice of α we therefore have $\sum_{r_n \geq \alpha} r_n \geq 2V$.

Theorem 2.98 now yields

$$\mathbb{P}(W \geq V) \geq a_1 \exp\left(-a_2 V^2 \left(\sum_{r_n < \alpha} r_n^2\right)^{-1}\right).$$

We have

$$\begin{aligned}
\sum_{r_n < \alpha} r_n^2 &= \sum_{\lambda \in \mathrm{Irr}(G^+)} \sum_{\gamma_\lambda > R_{\alpha,\lambda}} \frac{4|\lambda(C_2^+) - \lambda(C_1^+)|^2}{\frac{1}{4} + \gamma_\lambda^2} \\
&\geq \sum_{\lambda \in \mathrm{Irr}(G^+)} \sum_{2R_{\alpha,\lambda} \geq \gamma_\lambda > R_{\alpha,\lambda}} \frac{4|\lambda(C_2^+) - \lambda(C_1^+)|^2}{\frac{1}{4} + \gamma_\lambda^2} \\
&\geq \sum_{\lambda \in \mathrm{Irr}(G^+)} \frac{4|\lambda(C_2^+) - \lambda(C_1^+)|^2}{\frac{1}{4} + 4R_{\alpha,\lambda}^2} (N(2R_{\alpha,\lambda}, \lambda) - N(R_{\alpha,\lambda}, \lambda))
\end{aligned}$$

As in the proof of [FJ20a, Lemma 4.3] we see, using Lemma 2.96, that

$$N(2R_{\alpha,\lambda}, \lambda) - N(R_{\alpha,\lambda}, \lambda) \gg R_{\alpha,\lambda} \log A(\lambda).$$

Thus,

$$\sum_{r_n < \alpha} r_n^2 \gg \frac{1}{\max_{\lambda \in \mathrm{Irr}(G^+)} R_{\alpha,\lambda}} \sum_{\lambda \in \mathrm{Irr}(G^+)} |\lambda(C_2^+) - \lambda(C_1^+)|^2 \log A(\lambda).$$

Combining Theorem 2.57 and Lemma 2.65, we finally get

$$\sum_{r_n < \alpha} r_n^2 \gg \frac{1}{\max_{\lambda \in \mathrm{Irr}(G^+)} R_{\alpha,\lambda}} \mathrm{Var}(X(L/K, C_1, C_2)).$$

We can now conclude that

$$\mathbb{P}(W \geq V) \geq a_1 \exp\left(-a_3(\max_{\lambda \in \mathrm{Irr}(G^+)} R_{\alpha,\lambda}) B(L/K, C_1, C_2)^2\right)$$

for some absolute constant $a_3 > 0$. But, recalling the choice we made for α,

$$\max_{\lambda \in \mathrm{Irr}(G^+)} R_{\alpha,\lambda} = \sqrt{\left(\frac{1}{4} + T_0(\lambda_m)^2\right) \frac{|\lambda^*(C_2^+) - \lambda^*(C_1^+)|^2}{|\lambda_m(C_2^+) - \lambda_m(C_1^+)|^2}}.$$

To determine the size of this quantity, we consider two cases : either $\lambda_m = \lambda^*$, in which case we find $\max_{\lambda \in \mathrm{Irr}(G^+)} R_{\alpha,\lambda} \asymp T_0(\lambda^*) \asymp e^{C\sqrt{\frac{Mb_1b_2}{\lambda^*(1)b_3(C_1,C_2)}}}$, or $\lambda_m \neq \lambda^*$, in which case $\max_{\lambda \in \mathrm{Irr}(G^+)} R_{\alpha,\lambda} \asymp \frac{b_3(C_1,C_2)}{b_4(C_1,C_2)}$ since $T_0(\lambda_m)$ was chosen as an absolute constant.

It simply remains to note that, by symmetry of W about 0, we have

$$\mathbb{P}(W \geq V) = \mathbb{P}(W \leq -V) = 1 - \mathbb{P}(X(L/K, C_1, C_2) > 0) = 1 - \delta(L/K, C_1, C_2).$$

□

Note that when $K = \mathbb{Q}$ in the previous theorem, we have $R = \emptyset$ so that $Q(C_1, C_2)$ can be taken to be $C\left(\frac{b_3(C_1,C_2)}{b_4(C_1,C_2)} + 1\right)$, where $C > 0$ is an absolute constant. In our applications (Theorems 2.100 and 2.102), the quantities b_1, b_2, M and $\frac{b_3(C_1,C_2)}{b_4(C_1,C_2)}$ will be bounded.

2.3.4.5 Estimates on the bias in the towers

Using the number fields constructed in Proposition 2.92 and Proposition 2.94, we can now state the following result, a more exhaustive version of Theorem B.

Theorem 2.100. *Assume* GRH *and* LI *for the number fields $\mathcal{D}_n$ of Proposition 2.92. There exist absolute constants $c_1, c_2, c_3 > 0$ such that for any $n \geq 3$, the following hold :*

C_a	C_b	*Estimate on* $\delta(\mathcal{D}_n/\mathbb{Q}, C_1, C_2)$	*Condition on the classes*
C_1	C_{-1}, C_s, C_{rs}	$c_1 \exp(-c_2 2^n) < \delta(\mathcal{D}_n/\mathbb{Q}, C_1, C_b) < \exp\left(-c_3 \frac{2^n}{n}\right)$	*none*
C_1	C_{r^k}	$c_1 \exp(-c_3 32^n) < \delta(\mathcal{D}_n/\mathbb{Q}, C_1, C_{r^k}) < \exp\left(-c_4 \frac{2^n}{n}\right)$	*none*
C_{-1}	C_{r^k}	$\frac{1}{2}$	k *even*
C_{-1}	C_s, C_{rs}	$0 < \frac{1}{2} - \delta(\mathcal{D}_n/\mathbb{Q}, C_{-1}, C_b) \ll \frac{1}{2^n}$	*none*
C_{r^k}	C_{r^l}	$\frac{1}{2}$	$k = l \ mod\ 2$
C_{r^k}	C_s, C_{rs}	$\frac{1}{2}$	k *odd*
C_s	C_{rs}	$\frac{1}{2}$	*none*

Proof. For the first part of the theorem, the bounds obtained in Proposition 2.90 (for the variance), Proposition 2.91 (for the mean) and Proposition 2.92 (for the discriminant) show that

$$\frac{2^n}{n} \ll B(\mathcal{D}_n/\mathbb{Q}, C_1, C_b)^2 = \frac{\mathbb{E}(X(\mathcal{D}_n/\mathbb{Q}, C_1, C_b))^2}{\mathrm{Var}(X(\mathcal{D}_n/\mathbb{Q}, C_1, C_b))} \ll 2^n.$$

We combine this estimate with Theorems 2.59 and 2.99 (and the fact $\mathbb{E}(X(\mathcal{D}_n/\mathbb{Q}, C_1, C_b)) < 0$) to get

$$c_1 \exp(-c_2 2^n) < \delta(\mathcal{D}_n/\mathbb{Q}, C_1, C_{-1}) < \exp\left(-c_3 \frac{2^n}{n}\right),$$

for some absolute constants $c_1, c_2, c_3 > 0$ (which may differ from the constants of Theorems 2.59 and 2.99, but by an absolute factor).

The proof is similar for $\delta(\mathcal{D}_n/\mathbb{Q}, C_1, C_{r^k})$, the only difference being the lower bound

$$\mathrm{Var}(X(\mathcal{D}_n/\mathbb{Q}, C_1, C_{r^k})) \gg \frac{\log|d_{\mathcal{D}_n}|}{16^n} \gg \frac{1}{8^n}$$

from Proposition 2.90 and 2.92. To deal with $\delta(\mathcal{D}_n/\mathbb{Q}, C_{-1}, C_b)$, $b = s$ or $b = rs$, we simply apply Theorem 2.61, together with Proposition 2.90.

Finally, each case in which $\delta(C_1, C_2, L/\mathbb{Q}) = \frac{1}{2}$ comes from the fact that $\mathbb{E}(X(C_1, C_2, L/\mathbb{Q})) = 0$. □

Remark 2.101. We could not produce estimates for $\delta(\mathcal{D}_n/\mathbb{Q}, C_{r^k}, C_b)$ for $b = -1$ (when k is odd), $b = r^l$ (when k and l do not have the same parity) and $b = s$ or $b = rs$ (when k is even) because we do not have good enough bounds on $\mathrm{Var}(X(\mathcal{D}_n/\mathbb{Q}, C_{r^k}, C_b))$ to conclude that $B(\mathcal{D}_n/\mathbb{Q}, C_{r^k}, C_b)$ is large or not.

We now turn our attention to the extensions $\mathcal{Q}_n^{\pm}/\mathbb{Q}$ built in Proposition 2.94. The proof of the next theorem is the same as for Theorem 2.100, except that the value of $W_{\mathcal{Q}_n^{\pm}}$ determines in some cases the class towards which there is a bias. This is a more exhaustive version of Theorem C.

Theorem 2.102. *Assume* GRH *and* LI^+ *for the number fields* $\mathcal{Q}_n^{\pm}$ *of Proposition 2.94. There exist absolute constants* $c_1, c_2, c_3 > 0$ *such that for any* $n \geq 3$*, denoting* $\mathcal{Q}_n^{\pm}$ *by* $\mathcal{Q}_n$*, the following hold :*

C_a	C_b	*Estimate on* $\delta(\mathcal{Q}_n/\mathbb{Q}, C_a, C_b)$	*Conditions*
C_{-1}	C_1	$c_1 \exp(-c_2 2^n) < \left\lvert \frac{1-W_{\mathcal{Q}_n}}{2} - \delta(\mathcal{Q}_n/\mathbb{Q}, C_{-1}, C_b) \right\rvert < \exp\left(-c_3 \frac{2^n}{n}\right)$	*none*
C_{-1}	C_y, C_{xy}	$c_1 \exp(-c_2 2^n) < \delta(\mathcal{Q}_n/\mathbb{Q}, C_{-1}, C_b) < \exp\left(-c_3 \frac{2^n}{n}\right)$	$W_{\mathcal{Q}_n} = 1$
C_{-1}	C_y, C_{xy}	$0 < \frac{1}{2} - \delta(\mathcal{Q}_n/\mathbb{Q}, C_{-1}, C_b) \ll \frac{1}{2^{n/3}}$	$W_{\mathcal{Q}_n} = -1$
C_{-1}	C_{x^k}	$c_1 \exp(-c_2 32^n) < \delta(\mathcal{Q}_n/\mathbb{Q}, C_{-1}, C_{x^k}) < \exp\left(-c_3 \frac{2^n}{n}\right)$	$W_{\mathcal{Q}_n} = 1$
C_{-1}	C_{x^k}	$\frac{1}{2}$	$W_{\mathcal{Q}_n} = -1$ *and* k *even*
C_1	C_{x^k}	$\frac{1}{2}$	$W_{\mathcal{Q}_n} = 1$ *and* k *even*
C_1	C_{x^k}	$c_1 \exp(-c_2 32^n) < \delta(\mathcal{Q}_n/\mathbb{Q}, C_1, C_{x^k}) < \exp\left(-c_3 \frac{2^n}{n}\right)$	$W_{\mathcal{Q}_n} = -1$
C_1	C_y, C_{xy}	$0 < \frac{1}{2} - \delta(\mathcal{Q}_n/\mathbb{Q}, C_1, C_b) \ll \frac{1}{2^{n/3}}$	$W_{\mathcal{Q}_n} = 1$
C_1	C_y, C_{xy}	$c_1 \exp(-c_2 2^n) < \delta(\mathcal{Q}_n/\mathbb{Q}, C_1, C_b) < \exp\left(-c_3 \frac{2^n}{n}\right)$	$W_{\mathcal{Q}_n} = -1$
C_{x^k}	C_{x^l}	$\frac{1}{2}$	$k = l \bmod 2$
C_{x^k}	C_y, C_{xy}	$\frac{1}{2}$	k *odd*
C_y	C_{xy}	$\frac{1}{2}$	*none*

Remark 2.103. As in Theorem 2.100, we could not produce bounds for $\delta(\mathcal{Q}_n/\mathbb{Q}, C_{x^k}, C_b)$ for $b = 1$ (when k is odd and $W_{\mathcal{Q}_n} = 1$), $b = -1$ (when k is odd and $W_{\mathcal{Q}_n} = -1$), $b = x^l$ (when k and l do not have the same parity) and $b = y$ or $b = xy$ (when k is even).

We now prove a more general version of Theorem D : we are able to observe monotonicity in the evolution of the bias in the subextensions of $\mathcal{D}_n/\mathbb{Q}$ and $\mathcal{Q}_n^+/\mathbb{Q}$.

Theorem 2.104. *Assume* GRH *and* LI^+ *(*LI *is sufficient for the dihedral case). For any $n \geq 3$ and $3 \leq i \leq n$, let $\mathcal{D}_n^{(i)} = \mathcal{D}_n^{\langle r_i, s\rangle}$ as in section 4.2, and $(\mathcal{Q}_n^+)^{(i)} = (\mathcal{Q}_n^+)^{\langle x_i, y\rangle}$ as in section 4.1. Then for any $\varepsilon > 0$ and any sufficiently large n, for $3 \leq i < j \leq n$ such that $i \leq n\frac{1+\varepsilon}{2}$ and $j \geq n\left(\frac{1+3\varepsilon}{2}\right)$, we have*

$$\delta(\mathcal{D}_n/\mathcal{D}_n^{(j)}, C_1^{(j)}, C_{-1}^{(j)}) < \delta(\mathcal{D}_n/\mathcal{D}_n^{(i)}, C_1^{(i)}, C_{-1}^{(i)}),$$

$$1 - \delta(\mathcal{Q}_n^+/(\mathcal{Q}_n^+)^{(j)}, C_1^{(j)}, C_{-1}^{(j)}) < 1 - \delta(\mathcal{Q}_n^+/(\mathcal{Q}_n^+)^{(i)}, C_1^{(i)}, C_{-1}^{(i)})$$

and

$$\delta(\mathcal{Q}_n^-/(\mathcal{Q}_n^-)^{(j)}, C_1^{(j)}, C_{-1}^{(j)}) < \delta(\mathcal{Q}_n^-/(\mathcal{Q}_n^-)^{(i)}, C_1^{(i)}, C_{-1}^{(i)}).$$

Proof. We combine the bounds of Propositions 2.90, 2.91 and 2.92, with Theorems 2.59 and 2.99. With notations from Theorem 2.99, it is easy to see from Corollary 2.74 that $R = \{\chi_2, \chi_3\}$ so that $b_1 = b_2 = 2, M = 1$, and $\frac{b_3(C_1,C_{-1})}{b_4(C_1,C_{-1})} = 1$. We thus find

$$c_1 \exp(-c_2 2^{2i-n}) < \delta(\mathcal{D}_n/\mathcal{D}_n^{(i)}, C_1^{(i)}, C_{-1}^{(i)}) < \exp\left(-c_3\frac{2^{2i-n}}{n}\right)$$

for any $3 \leq i \leq n$ and for some absolute $c_1, c_2, c_3 > 0$.

In order to have $\delta(\mathcal{D}_n/\mathcal{D}_n^{(j)}, C_1^{(j)}, C_{-1}^{(j)}) < \delta(\mathcal{D}_n/\mathcal{D}_n^{(i)}, C_1^{(i)}, C_{-1}^{(i)})$, it is therefore enough to have

$$\exp\left(-c_3\frac{2^{2j-n}}{n}\right) < c_1 \exp(-c_2 2^{2i-n}).$$

This is equivalent to

$$c_2 2^{2i} < c_3\frac{2^{2j}}{n} + 2^n \log(c_1).$$

Now if $j \geq n\left(\frac{1+3\varepsilon}{2}\right)$ and n is large enough then $c_3\frac{2^{2j}}{n} \geq c_3\frac{2^{n(1+3\varepsilon)}}{n} > 2^{n(1+2\varepsilon)}$ while if $i \leq n\left(\frac{1}{2}+\varepsilon\right)$ and n is large enough we have $c_2 2^{2i} + 2^n \log(1/c_1) \leq 2^{n(1+2\varepsilon)}$ and the desired inequality holds.

The proof is similar in the case of $\mathcal{Q}_n^{\pm}$ by using the bounds of Proposition 2.87, Proposition 2.89 and Proposition 2.94 with Theorems 2.59 and 2.99. □

Remark 2.105. A similar proof can be applied to the other extremely biased Chebotarev races from Theorems 2.100 and 2.102, which yields similar monotonicity results.

Chapitre 3

Biais de Tchebychev dans les corps de fonctions

Dans ce chapitre, plus court que les autres, on cherche à transposer les idées du chapitre précédent au contexte de la répartition des automorphismes de Frobenius dans les groupes de Galois d'extensions géométriques de corps de fonctions en une variable sur un corps fini. Pour ce faire, on commence par rappeler les notions nécessaires de l'arithmétique de ces extensions de corps. Le point de vue adopté pour étudier ces extensions de corps est purement algébrique, mais il est à noter que l'on pourrait employer un langage plus géométrique, en faisant le lien avec la théorie des courbes sur les corps finis. On détaille ensuite l'adaptation, dûe à Cha et Im dans [CI11], de la méthode de Rubinstein et Sarnak à ce contexte, et on mentionne quelques affaiblissements d'hypothèses obtenus dans [Bai20]. Enfin, on montre un nouveau résultat de type théorème central limite pour certaines familles d'extensions hyperelliptiques et superelliptiques.

3.1 Arithmétique des corps de fonctions

Les résultats de cette section sont empruntés aux livres [Ros02] et [VS06].

3.1.1 Définitions

Commençons par définir les corps et les extensions de corps qui vont nous intéresser.

Définition 3.1. *Soit k un corps. On appelle* ***corps de fonctions algébriques en une variable*** *sur k (on dira simplement* ***corps de fonctions*** *sur k) toute extension K/k finiment engendrée, de degré de transcendance 1 et telle que k soit algébriquement clos dans K, autrement dit telle que tout élément de $K \setminus k$ soit transcendant sur k. Le corps k est alors appelé le* ***corps des constantes*** *de K.*

L'hypothèse k algébriquement clos dans K est en quelque sorte bénigne. En effet, on peut montrer que la clôture algébrique de k dans K est de degré fini sur k ([VS06, p.16]). En particulier, comme dans la suite le corps k sera fini, sa clôture algébrique dans K sera également finie, et on ne perd pas de généralité à supposer directement k algébriquement clos dans K.

Exemples 3.2.

i) Soit k un corps. Le corps des fractions rationnelles $k(x)$ est un corps de fonctions sur k.
ii) Si $\mathcal{C}$ est une courbe projective irréductible et lisse sur un corps fini k alors le corps des fonctions rationnelles $k(\mathcal{C})$ de $\mathcal{C}$ est un corps de fonctions sur k (quitte à changer k en un corps fini plus grand).
iii) La plupart des corps de fonctions dont on parlera dans la suite seront présentés comme corps de rupture de polynômes irréductibles sur $k(x)$. Il se peut que de telles extensions aient pour corps des constantes une extension (forcément finie d'après la remarque ci-dessus) de k, mais ça n'aura pas d'importance au vu du problème de répartition d'automorphismes de Frobenius considéré.

Les corps de fonctions sur les corps finis possèdent de nombreuses similarités avec les corps de nombres, comme on le verra notamment lorsque l'on parlera des automorphismes de Frobenius et du théorème de Chebotarev. Ces deux familles de corps forment ce que l'on appelle les corps globaux, dont les complétés sont les corps locaux. Cependant, une différence notable entre ces deux types de corps est la suivante : là où le corps de nombres le plus simple, $\mathbb{Q}$, est un corps premier, le corps de fonctions $\mathbb{F}_q(T)$ contient une infinité de sous-corps qui sont des corps de fonctions sur $\mathbb{F}_q$, par exemple les $\mathbb{F}_q(T^n)$, $n \geq 1$. On ne peut pas se référer à un sous-corps « canonique » tel que $\mathbb{Q}$. Cependant, tout corps de fonctions K sur $\mathbb{F}_q$ contient un (et donc une infinité) de sous-corps isomorphe à $\mathbb{F}_q(T)$, il suffit de considérer le sous-corps engendré par n'importe quel élément de $K \setminus \mathbb{F}_q$.

Introduisons maintenant deux types d'extensions de corps de fonctions.

Définition 3.3. *Soient k un corps, K/k un corps de fonctions sur k et L/K une extension algébrique. On dit que L/K est une* ***extension des constantes*** *lorsque $L = \overline{k}^L K$, où $\overline{k}^L$ désigne la clôture algébrique de k dans L. On dit que L/K est une* ***extension géométrique*** *lorsque k est algébriquement clos dans L, autrement dit lorsque $\overline{k}^L = k$.*

Il est clair qu'une extension des constantes et une extension géométrique d'un corps de fonctions sur k sont également des corps de fonctions sur $\overline{k}^L$ et k respectivement. Notons que si L/K est une extension algébrique, alors on dispose de deux extensions intermédiaires $L/\overline{k}^L K$ et $\overline{k}^L K/K$, la première étant une extension géométrique et la seconde une extension des constantes. Les questions de répartition des premiers dans les extensions des constantes étant essentiellement triviales lorsque le corps des constantes est fini (voir par exemple [Ros02, Proposition 8.13]), on se contentera d'étudier des extensions géométriques de corps de fonctions.

Définition 3.4. *Soit K/k un corps de fonctions sur le corps k. On appelle* ***diviseur premier*** *(ou simplement* ***premier****) de K tout anneau de valuation discrète contenant k et dont le corps des fractions est K. On identifie un tel anneau à son idéal premier non nul. La valuation associée au premier $\mathcal{P}$ est notée $v_\mathcal{P}$. Si $\mathcal{P}$ est un premier de K, le* ***corps résiduel*** *en $\mathcal{P}$ est $k_\mathcal{P}$ le quotient de l'anneau de valuation discrète associé par $\mathcal{P}$. Le* ***degré*** *de $\mathcal{P}$, noté $\deg(\mathcal{P})$ est le degré $[k_\mathcal{P} : k] < +\infty$ ([VS06, Theorem 2.4.12]). Si k est fini, la* ***norme*** *de $\mathcal{P}$ est $\#k_\mathcal{P} = \#k^{\deg(\mathcal{P})}$. Un* ***diviseur*** *de K est un produit formel de diviseurs premiers de K (autrement dit le groupe des diviseurs de K est défini comme le groupe abélien libre*

engendré par l'ensemble de ses diviseurs premiers). On étend le degré additivement et on étend la norme multiplicativement à tous les diviseurs. Un ***diviseur effectif*** *est un diviseur dont les exposants sont tous positifs. Le diviseur* $\mathfrak{A}$ *divise le diviseur* $\mathfrak{B}$*, noté* $\mathfrak{A} \mid \mathfrak{B}$ *lorsque* $v_{\mathcal{P}}(\mathfrak{B}) \geq v_{\mathcal{P}}(\mathfrak{A})$ *pour tout premier* $\mathcal{P}$*, ou de manière équivalente lorsqu'il existe un diviseur effectif* $\mathfrak{C}$ *tel que* $\mathfrak{B} = \mathfrak{A}\mathfrak{C}$*.*

Remarque 3.5. La donnée d'un anneau de valuation discrète contenant k et dont le corps des fractions est K est équivalente à la donnée d'une classe d'équivalence de valeurs absolues sur K qui sont triviales sur k, elle-même équivalente à la donnée d'une classe d'équivalence de places sur K qui sont triviales sur k ([VS06, Definition 2.2.12]).

3.1.2 Genre d'un corps de fonctions

Un invariant important d'un corps de fonctions K est son **genre** g_K. Pour nos besoins dans cette thèse il n'est pas nécessaire de rentrer dans les détails de sa définition. Nous mentionnerons simplement que celui-ci peut être interprété comme la dimension (sur le corps des constantes k de K) de l'espace des formes différentielles holomorphes (c'est-à-dire sans pôle) sur K, et que son importance provient du théorème de Riemann-Roch ([VS06, Theorem 3.5.4]) qui permet de montrer l'existence d'éléments de K vérifiant certaines contraintes.

Exemples 3.6.

i) On peut montrer ([VS06, Proposition 9.6.2]) que les corps de fonctions sur k de genre 0 sont les corps de fonctions rationnelles de la forme $k(x)$ avec x transcendant sur k et les corps de fonctions de coniques sur k, qui sont des extensions quadratiques de $k(x)$.

ii) De même, les corps de fonctions sur k de genre 1 (et contenant un premier de degré 1, ce qui est automatique si k est fini d'après un théorème de Schmidt [VS06, Theorem 6.3.8]) sont les corps de fonctions des courbes elliptiques sur k ([VS06, Theorem 4.2.6]).

Dans la suite, on se servira des résultats suivants, qui donnent le genre de certains types particuliers de corps de fonctions.

Proposition 3.7. *Soit* k *un corps parfait.*

- ***Corps hyperelliptiques*** *: Supposons que la caractéristique de* k *est impaire. Soit* $f \in k[x]$ *de degré* $d \geq 5$*, sans facteur carré et considérons le corps de fonctions* $K := k(x, y)$*, avec* $y^2 = f(x)$*. Alors le genre de* K *est*

$$g_K = \left\lfloor \frac{d+1}{2} \right\rfloor - 1.$$

- ***Corps superelliptiques*** *: Soit* $n \geq 3$*. Soit* $f \in k[x]$ *sans facteur carré de degré* $d > n$ *et considérons le corps de fonctions* $K := k(x, y)$*, avec* $y^n = f(x)$*. Alors le genre de* K *est*

$$g_K = \frac{1}{2}(n(d-1) - d - (n, d)) + 1.$$

Démonstration. Le cas des corps hyperelliptiques est traité dans [VS06, Example 9.4.4] et celui des corps superelliptiques dans [MS19, p.128]. □

Remarque 3.8. Remarquons que k n'est pas nécessairement algébriquement clos dans $K := k(x, y)$ avec $y^n = f(x)$. Dans tous les cas, on peut montrer que le genre est invariant par extension des constantes au-dessus d'un corps parfait ([Ros02, Proposition 8.9]). Dans la suite, on supposera que k contient les racines n-ièmes de l'unité dans le cas des courbes superelliptiques afin que l'extension $K/k(x)$ soit galoisienne et géométrique. Dans le cas $k = \mathbb{F}_q$, cela reviendra à supposer $q \equiv 1 \bmod n$.

3.1.3 Théorie de la ramification dans les extensions galoisiennes de corps de fonctions

On considère désormais une extension géométrique galoisienne L/K de corps de fonctions sur le corps fini k, de groupe de Galois G. La théorie de la ramification pour une telle extension est complètement analogue à celle des extensions de corps de nombres.

Définition 3.9. *Soit $\mathfrak{P}$ un premier de L. On dit que $\mathfrak{P}$ est au-dessus du premier $\mathcal{P}$ de K lorsque $v_{\mathfrak{P}|K}$ est équivalente à $v_{\mathcal{P}}$. Dans ce cas, l'**indice de ramification** $e(\mathfrak{P}/\mathcal{P})$ de $\mathfrak{P}$ sur $\mathcal{P}$ est l'indice $[v_{\mathcal{P}}(K^*) : v_{\mathfrak{P}}(K^*)]$. On dit que $\mathfrak{P}$ est **ramifié** au-dessus de $\mathcal{P}$ si $e(\mathfrak{P}/\mathcal{P}) \geq 2$, et que $\mathcal{P}$ se ramifie dans L s'il existe un premier $\mathfrak{P}$ de L ramifié au-dessus de $\mathcal{P}$.*

On montre qu'il n'existe qu'un nombre fini de premiers dans L au-dessus d'un premier de K donné ([VS06, 5.1.13])) et qu'il n'y a qu'un nombre fini de premiers de K ramifiés dans L ([VS06, Theorem 5.2.33]). Comme l'extension L/K est supposée galoisienne, les indices de ramification au-dessus de tout premier de K sont tous les mêmes. Lorsque $\mathfrak{P}$ est au-dessus de $\mathcal{P}$, on dispose d'une extension de corps finis $k_{\mathfrak{P}}/k_{\mathcal{P}}$, de degré $\deg(\mathfrak{P}) - \deg(\mathcal{P})$.

Définition 3.10. *Soit $\mathfrak{P}$ un premier de L au-dessus du premier $\mathcal{P}$ de K. Le groupe de décomposition de $\mathfrak{P}$ est*

$$D_{\mathfrak{P}} := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

où $\mathfrak{P}$ est vu comme idéal premier associé à l'anneau de valuation discrète sous-jacent. Le groupe d'inertie $\mathcal{I}_{\mathfrak{P}}$ est le noyau du morphisme

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathcal{P}}) \\ \sigma & \mapsto & (\overline{x} \mapsto \overline{\sigma(x)}) \end{array}.$$

Comme dans le cas des corps de nombres, on montre que le morphisme ci-dessus est surjectif et que le groupe d'inertie est d'ordre l'indice de ramification de $\mathfrak{P}$ au-dessus de $\mathcal{P}$ ([Ros02, Theorem 9.6]). Le groupe G agissant transitivement sur les premiers au-dessus de $\mathcal{P}$, les groupes de décomposition associés sont conjugués dans G. Ceci nous permet de définir l'automorphisme de Frobenius en $\mathcal{P}$ dans G.

Définition 3.11. *Soit $\mathcal{P}$ un premier de K non ramifié dans L. On appelle (classe d')**automorphisme de Frobenius** de $\mathcal{P}$ la classe de conjugaison $\mathrm{Frob}_{\mathcal{P}}$ de G formée des images réciproques du Frobenius $x \mapsto x^{N(\mathcal{P})} \in \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathcal{P}})$, pour $\mathfrak{P}$ variant dans l'ensemble des premiers de L au-dessus de $\mathcal{P}$.*

Ainsi, on peut associer à tous les premiers $\mathcal{P}$ de K, sauf au plus un nombre fini, une classe de conjugaison particulière dans G qui encode l'arithmétique des extensions résiduelles $k_{\mathfrak{P}}/k_{\mathcal{P}}$ pour $\mathfrak{P}$ variant dans l'ensemble des premiers de L au-dessus de $\mathcal{P}$. À nouveau, il faudra également considérer les premiers ramifiés dans la définition à venir des fonctions L d'Artin : les Frobenius associés sont alors des éléments des $D_{\mathfrak{P}}/\mathcal{I}_{\mathfrak{P}}$, qui s'identifie naturellement au groupe de Galois d'une extension intermédiaire de L/K.

3.1.4 Fonctions L d'Artin et théorème de Chebotarev

Dans cette section, L/K est toujours une extension géométrique et galoisienne de corps de fonctions sur $k = \mathbb{F}_q$, de groupe de Galois G.

Afin d'étudier la répartition des premiers de K dont la classe de Frobenius est prescrite, on introduit les fonctions L d'Artin selon le même modèle que pour les extensions de corps de nombres.

Définition 3.12. *Soit $\rho : G \longrightarrow \mathbf{GL}(V)$ une représentation de G, de caractère χ. On définit la **fonction L d'Artin** associée à χ par*

$$L(s, \chi, L/K) := \prod_{\mathcal{P} \text{ premier de } K} \det\left(\left(\mathrm{id}_V - \rho(\mathrm{Frob}_{\mathcal{P}})N(\mathcal{P})^{-s}\right)_{|V^{\mathcal{I}_{\mathcal{P}}}}\right)^{-1},$$

pour tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$. La fonction ζ_K est définie comme

$$\sum_{\mathfrak{A} \text{ diviseur effectif de} K} \frac{1}{N(\mathfrak{A})^s} = \prod_{\mathcal{P} \text{ premier de } K} \left(1 - N(\mathcal{P})^{-s}\right)^{-1} = L(s, \chi_0, M/K)$$

pour n'importe quelle extension galoisienne M de K.

Remarque 3.13. Le facteur associé au premier $\mathcal{P}$ de K ne dépend que de $\mathcal{P}$ puisque le polynôme caractéristique est invariant par conjugaison et les sous-groupes d'inertie et les Frobenius associés aux premiers de L au-dessus de $\mathcal{P}$ sont conjugués.

Ces fonctions satisfont les mêmes propriétés fonctorielles que les fonctions L d'Artin des corps de nombres (voir la Proposition 2.22). En particulier, on obtient de nouveau la factorisation suivante :

$$\zeta_L(s) = \prod_{\chi \in \mathrm{Irr}(G)} L(s, \chi, L/K)^{\chi(1)} = \zeta_K(s) \prod_{\chi \in \mathrm{Irr}(G)\setminus\{\chi_0\}} L(s, \chi, L/K)^{\chi(1)}.$$

Une différence majeure avec les corps de nombres apparaît ici : les fonctions L d'Artin d'extensions de corps de fonctions sont en fait des fractions rationnelles en la variable q^{-s} (rappelons que le corps des constantes est $k = \mathbb{F}_q$), et satisfont l'analogue de l'hypothèse de Riemann dans ce contexte. Dans toute la suite on pose la variable $u := q^{-s}$.

Théorème 3.14 (Weil)**.** *Avec $u = q^{-s}$, on a une factorisation de la forme*

$$\zeta_K(s) = \mathcal{Z}_K(u) := \frac{\prod_{j=1}^{2g_K}(1 - \gamma(\chi_0, j)u)}{(1-u)(1-qu)}$$

pour certains $\gamma(\chi_0, j) \in \mathbb{C}$. *Si* $\chi \in \mathrm{Irr}(G)\backslash\{\chi_0\}$, *alors* $L(s, \chi, L/K) = \mathcal{L}(u, \chi)$ *est un polynôme en* u *à coefficients entiers :*

$$\mathcal{L}(u, \chi) = \prod_{j=1}^{M_\chi} (1 - \gamma(\chi, j)u)$$

pour un certain entier pair (possiblement nul) M_χ *et pour certains* $\gamma(\chi, j) \in \mathbb{C}$. *Les* $\gamma(\chi, j)$ *sont appelés les* ***zéros inverses*** *de* $\mathcal{L}(u, \chi)$ *et sont de module* $\sqrt{q}$ *(Hypothèse de Riemann pour les courbes sur* $\mathbb{F}_q$*). De plus si* γ *est un zéro inverse de* $\mathcal{L}(u, \chi)$ *alors* $\frac{q}{\gamma} = \overline{\gamma}$ *est un zéro inverse* $\mathcal{L}(u, \overline{\chi})$.

Remarques 3.15.

i) Le fait que les zéros inverses des fonctions L d'Artin soient de module $\sqrt{q}$ correspond à l'hypothèse de Riemann car on a alors

$$L(s, \chi, L/K) = 0 \Rightarrow |q^{-s}| = q^{-1/2} \Rightarrow \mathfrak{Re}(s) = 1/2.$$

Ce résultat a été établi par Weil à l'aide de méthodes géométriques (voir par exemple [Ros02, Appendix] ou [VS06, §7.2] pour une démonstration de ce fait).

ii) Le dernier point provient de l'équation fonctionnelle, que l'on n'explicitera pas ici, reliant les valeurs de $L(s, \chi, L/K)$ et $L(1 - s, \overline{\chi}, L/K)$, c'est-à-dire $\mathcal{L}(u, \chi)$ et $\mathcal{L}\left(\frac{1}{qu}, \chi\right)$.

L'existence d'une expression des fonctions L d'Artin qui est une fraction rationnelle en u permet de démontrer l'analogue du théorème de Chebotarev beaucoup plus simplement que dans le cas des corps de nombres : le calcul des dérivées logarithmiques des fonctions L d'Artin se fait par de simples développements en séries entières. De plus, le résultat de Weil sur l'hypothèse de Riemann permet d'obtenir essentiellement le terme d'erreur optimal dans ce théorème ([Ros02, Theorem 9.13B]).

Théorème 3.16 (« de Chebotarev »)**.** *Soit* C *une classe de conjugaison de* G. *Alors*

$$\pi_C(X) := \#\{\mathcal{P} \text{ premier de } K \mid \deg(\mathcal{P}) = X, \mathrm{Frob}_\mathcal{P} = C\} = \frac{\#C}{\#G}\frac{q^X}{X} + O\left(\frac{q^{X/2}}{X}\right).$$

Remarques 3.17.

i) En sommant, on obtient le même développement asymptotique pour la fonction de comptage des premiers de degré inférieur à X au lieu d'égal à X.

ii) On retrouve le théorème des polynômes irréductibles en progressions arithmétiques 1.29 en considérant $K = \mathbb{F}_q(x)$ et L un module de Carlitz convenable ([Ros02, Theorem 12.10]).

Dans la suite, on aura besoin d'informations sur le degré M_χ du polynôme $\mathcal{L}(u, \chi)$. Celui-ci a également été déterminé par Weil (voir [Ros02, p.131]).

Proposition 3.18. *Soit* $\chi \in \mathrm{Irr}(G) \setminus \{\chi_0\}$. *Alors*

$$M_\chi = \chi(1)(2g_K - 2) + \deg \mathfrak{f}(\chi),$$

où $\mathfrak{f}(\chi)$ *est un diviseur effectif de* K *appelé conducteur du caractère d'Artin de* χ.

Le conducteur d'Artin d'un caractère de G est un diviseur de K dont la définition est complètement analogue à celle des conducteurs d'Artin des caractères de groupes de Galois d'extensions de corps de nombres (voir la section 2.3.2.1). En vue de minorer des variances comme dans la démonstration de la Proposition 2.87, nous aurons besoin de l'observation suivante.

Lemme 3.19. *Supposons que L/K soit modérément ramifiée, c'est-à-dire que les indices de ramification des premiers de K dans L soient premiers avec la caractéristique de k. Si $\chi \in \mathrm{Irr}(G)$ est de degré 1 alors $\deg \mathfrak{f}(\chi) \leq \sum_{P \text{ ramifié dans } L} \deg P$ avec égalité si χ est fidèle (c'est-à-dire que la représentation associée est fidèle).*

Démonstration. Si L/K est modérément ramifiée alors la filtration des sous-groupes de ramification de chaque premier P de K ramifié dans L s'arrête au sous-groupe d'inertie $\mathcal{I}_P$ ([Ser80, Chapitre IV §2 Corollaire 3]). Soit donc $\chi \in \mathrm{Irr}(G)$ de degré 1. Par définition, on a donc $\deg \mathfrak{f}_\chi = \sum_P \mathrm{codim}\, V^{\mathcal{I}_P} \deg P$ où $V \simeq \mathbb{C}$ est l'espace de la représentation associée à χ et on a en particulier $\mathrm{codim}\, V^{\mathcal{I}_P} \leq 1$ pour tout premier P de K. De plus, si χ est fidèle, $\chi_{|\mathcal{I}_P}$ ne peut agir trivialement sur V, d'où $\mathrm{codim}\, V^{\mathcal{I}_P} = 1$ pour tout premier P de K ramifié dans L. □

En utilisant la factorisation

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi \in \mathrm{Irr}(G)\setminus\{\chi_0\}} L(s, \chi, L/K)^{\chi(1)},$$

et en comparant les degrés en u de chaque côté, on obtient la formule suivante, reliant les genres des deux corps de fonctions L et K aux degrés des conducteurs d'Artin des caractères irréductibles de G.

Corollaire 3.20 (Formule de Riemann-Hurwitz)**.** *On a*

$$2g_L - 2 = [L : K](2g_K - 2) + \sum_{\chi \in \mathrm{Irr}(G)\setminus\{\chi_0\}} \chi(1) \deg \mathfrak{f}(\chi).$$

Remarque 3.21. La formule de Riemann-Hurwitz fait usuellement intervenir le degré de la différente de L/K, qui est un diviseur effectif de L, au lieu des degrés des conducteurs d'Artin des caractères irréductibles de G. Notre formulation lui est équivalente en invoquant la formule conducteur-discriminant ([Ser80, VI, §3, Corollaire 2]).

3.2 Courses de diviseurs premiers dans des extensions géométriques de corps de fonctions

Le théorème de Chebotarev dans le contexte des corps de fonctions amène une nouvelle fois à étudier les disparités dans la répartition des automorphismes de Frobenius. La transposition de la méthode de Rubinstein et Sarnak à ce contexte a été faite par Cha et Im dans [CI11]. Citons au passage que Cha et Im étudient complètement le cas où L/K est une extension des constantes, qui peut être traité sans aucun recours à l'analyse avec des arguments purement algébriques. On considère désormais une extension galoisienne géométrique L/K de corps de fonctions sur $k := \mathbb{F}_q$, de groupe de Galois G.

3.2.1 Les résultats de Cha et Im

Définition 3.22. *Si C est une classe de conjugaison de G, on pose*

$$E_C : X \mapsto \frac{X}{q^{X/2}} \left(\frac{\#G}{\#C} \pi_C(X) - \pi_K(X) \right),$$

où $\pi_K(X) := \#\{\mathcal{P} \text{ premier de } K \mid \deg(\mathcal{P}) = X\}$. Si $C_1, \ldots, C_D$ sont des classes de conjugaison de G deux à deux distinctes, on pose

$$E_{G;C_1,\ldots,C_D} = (E_{C_1}, \ldots, E_{C_D}).$$

On montre alors la formule explicite suivante.

Proposition 3.23. *Soit $\gamma_1, \ldots, \gamma_r$ les zéros inverses de $\mathcal{L}(u, \chi)$ de parties imaginaires strictement positives, pour $\chi \neq \chi_0$, comptés sans multiplicités. Pour $1 \leq j \leq r$, notons $\gamma_j = \sqrt{q} e^{i\theta_j}$. Alors pour toute classe de conjugaison C de G on a*

$$E_C(X) = r_C + z_C + a_\pi(C) e^{i\pi X} - \sum_{j=1}^{r} \left(a_j(C) e^{i\theta_j X} + \overline{a_j(C)} e^{-i\theta_j X} \right) + o(1)$$

quand $X \to +\infty$, où

$$r_C := \frac{1 - \frac{\#(C^{1/2})}{\#C}}{2},$$

$$z_C := - \sum_{\chi \neq \chi_0} \overline{\chi(C)} \operatorname{ord}_{u=q^{-1/2}} \mathcal{L}(u, \chi),$$

$$a_\pi(C) = r_C - \sum_{\chi \neq \chi_0} \overline{\chi(C)} \operatorname{ord}_{u=-q^{-1/2}} \mathcal{L}(u, \chi),$$

et pour $1 \leq j \leq r$,

$$a_j(C) := \sum_{\chi \neq \chi_0} \overline{\chi(C)} \operatorname{ord}_{u=\gamma_j^{-1}} \mathcal{L}(u, \chi).$$

Remarque 3.24. Il est possible que $r = 0$ dans l'énoncé ci-dessus. Cela se produit si et seulement si le numérateur de ζ_L est de la forme $(1 - \sqrt{q}u)^{2g_L}$, ce qui est par exemple le cas pour les corps de fonctions des courbes supersingulières construites dans [vdGvdV95].

La démonstration de cette formule est faite au-dessus de la Proposition 1.89. Notons que Cha et Im établissent une formule explicite analogue pour la fonction de comptage des diviseurs premiers de degré inférieur à X. Dans les deux cas, la formule est obtenue en calculant la dérivée logarithmique des fonctions L d'Artin de deux manières, l'une à partir du produit eulérien, l'autre à partir de l'expression polynomiale.

Partant de cette expression, la méthode déjà employée par Cha dans [Cha08] pour les polynômes irréductibles sur $\mathbb{F}_q$, utilisant le théorème de Kronecker-Weyl discret, et détaillée dans la section 1.3.2, montre l'existence d'une distribution limite pour $E_{G;C_1,\ldots,C_D}$.

Théorème 3.25 (Cha-Im, [CI11]). *Soient $C_1, \dots, C_D$ des classes de conjugaison de G deux à deux distinctes. La quantité $E_{G;C_1,\dots,C_D}$ admet une distribution limite (voir Définition 1.37) $\mu_{G;C_1,\dots,C_D}$.*

Remarque 3.26. Cha et Im travaillent en fait avec les fonctions de comptage de premiers de degrés inférieurs à X et non pas égal à X, mais ça ne change pas la nature des résultats présentés.

Pour étudier plus en détails cette distribution limite, et plus particulièrement sa fonction caractéristique, Cha et Im introduisent une hypothèse d'indépendance linéaire portant sur les θ_i et π, analogue à l'hypothèse GSH_M (voir Conjecture 1.42).

Conjecture 3.27 (LI). *On dit que l'extension L/K satisfait l'hypothèse LI lorsque le (multi)-ensemble*

$$\left\{\theta \in [0,\pi] \mid \exists \chi \in \mathrm{Irr}(G) \setminus \{\chi_0\}, \mathcal{L}\left(\left(\sqrt{q}e^{i\theta}\right)^{-1}, \chi\right) = 0\right\} \cup \{\pi\}$$

est linéairement indépendant sur $\mathbb{Q}$.

Sous cette hypothèse, Cha et Im étudient les différentes symétries de la mesure $\mu_{G;C_1,\dots,C_D}$, et justifient par là même l'existence d'un biais de Tchebychev, dû encore une fois aux différences entre les nombres de racines carrés d'éléments des classes de conjugaison considérées [CI11, §3].

3.2.2 En l'absence d'indépendance linéaire

Dans l'article [Bai20], on s'intéresse à la méthode de Rubinstein et Sarnak dans un cadre général, en cherchant à obtenir des énoncés faisant appel le moins possible à des hypothèses d'indépendance linéaire. Notre méthode nous permet notamment de montrer le résultat suivant dans le cas des courses de premiers dans les corps de fonctions sur un corps fini (voir Theorem 1.90 pour un énoncé un peu plus général). Si $C_1, \dots, C_D$ sont des classes de conjugaison de G, on note

$$\delta(L/K; C_1, \dots, C_D) := \lim_{X \to +\infty} \frac{1}{X} \# \left\{ n \leq X \mid \frac{\pi_{C_1}(n)}{\#C_1} > \dots > \frac{\pi_{C_D}(n)}{\#C_D} \right\}$$

quand cette limite existe, et $\underline{\delta}(L/K; C_1, \dots, C_D)$ les limites supérieures et inférieures correspondantes.

Théorème 3.28. *Soient $C_1, \dots, C_D$ des classes de conjugaison de G. Pour $1 \leq j \leq D$, soit $f_j = r_{C_j} + z_{C_j} + a_\pi(C_j)\frac{X_{r+1}+X_{r+1}^{-1}}{2} - \sum_{k=1}^{r}\left(a_k(C_j)X_j + \overline{a_k(C_j)}X_j^{-1}\right) \in \mathbb{C}(X_1, \dots, X_{r+1})$ (voir la formule explicite Proposition 3.23) et $F_j : t \mapsto f_j\left(e^{i\theta_1 t}, \dots, e^{i\theta_r t}, e^{i\pi t}\right)$.*

i) Cas dégénéré : Supposons que $\theta_i \in \pi\mathbb{Q}$ pour $1 \leq i \leq r$, c'est-à-dire que chaque $\mathcal{L}(u, \chi)$, $\chi \neq \chi_0$, est un produit de polynômes cyclotomiques (renormalisés par $\sqrt{q}$). S'il existe $n \in \mathbb{Z}$ tel que $F_1(n) > \dots > F_D(n)$, alors $0 < \underline{\delta}(L/K; C_1, \dots, C_D)$ et s'il existe $n \in \mathbb{Z}$ tel que $F_1(n) \geq \dots \geq F_D(n)$ soit fausse, alors $\overline{\delta}(L/K; C_1, \dots, C_D) < 1$. De plus, si pour $1 \leq j \leq D-1$, et pour $0 \leq n \leq d-1$, on a $F_j(n) \neq F_{j+1}(n)$, alors $\delta(L/K; C_1, \dots, C_D)$ existe.

ii) Cas non dégénéré : Supposons que $\theta_i \notin \pi\mathbb{Q}$ pour au moins un $i \in \{1, \dots, r\}$. S'il existe $n \in \mathbb{Z}$ tel que $F_1(n) > \cdots > F_D(n)$, alors $0 < \underline{\delta}(L/K; C_1, \dots, C_D)$, et s'il existe $n \in \mathbb{Z}$ tel que $F_1(n) \geq \cdots \geq F_D(n)$ soit fausse, alors $\overline{\delta}(L/K; C_1, \dots, C_D) < 1$. De plus, si pour $0 \leq a \leq d-1$ et $1 \leq j \leq D-1$, il existe $n \equiv a \bmod d$ tel que $F_j(n) \neq F_{j+1}(n)$, alors $\delta(L/K; C_1, \dots, C_D)$ existe.

Dans l'énoncé ci-dessus, d désigne le PGCD des dénominateurs des coefficients intervenant dans d'éventuelles relations de dépendance linéaire sur $\mathbb{Q}$ entre $2\pi, \theta_1, \dots, \theta_r$.

Ce résultat nous permet d'étudier des courses d'idéaux premiers que la méthode de Cha et Im ne pouvait étudier car LI n'est pas vérifié dans l'extension considérée. Reprenant un exemple de [Bai20], prenons $K = \mathbb{F}_7(x)$ et $L = K(\alpha)$ où α a pour polynôme minimal $f = T^6 - (x^2 + x)T^3 - 1$ sur K. Alors on a (voir [CI11, 4.2]), $G = \mathrm{Gal}(L/K) \simeq \mathfrak{S}_3$.

On a

$$\mathcal{L}(u, \chi_1) = 1 + 4u + 7u^2 = (1 - \gamma_1 u)(1 - \overline{\gamma_1} u),$$
$$\mathcal{L}(u, \chi_2) = 1 + u + 7u^2 = (1 - \gamma_2 u)(1 - \overline{\gamma_2} u),$$

avec (les deux valeurs sont inversées par erreur dans [CI11])

$$\gamma_1 = -2 + i\sqrt{3}$$

et

$$\gamma_2 = \frac{-1 + 3i\sqrt{3}}{2}.$$

Alors $\theta_1 = \arctan\left(-\frac{\sqrt{3}}{2}\right)$, $\theta_2 = \arctan(-3\sqrt{3})$ et $\theta_1 + \theta_2 = \frac{4\pi}{3}$. Ainsi, l'hypothèse LI n'est pas vérifiée dans L/K. En notant $C_1 = \{\mathrm{id}\}$, $C_2 = \{(1\,2), (1\,3), (2\,3)\}$ et $C_3 = \{(1\,2\,3), (1\,3\,2)\}$ les classes de conjugaison de G, une vérification numérique et le théorème ci-dessus permettent tout de même d'établir que pour toute permutation $\sigma \in \mathfrak{S}_3$, la densité $\delta(L/K; C_{\sigma(1)}, C_{\sigma(2)}, C_{\sigma(3)})$ existe et est strictement entre 0 et 1 (voir la discussion au-dessus de la Remark 1.91).

3.3 Un théorème central limite

Notre but ici est d'établir, dans des conditions convenables, un théorème central limite donnant le comportement asymptotique de $\delta(L/K, C_1, C_2) - \frac{1}{2}$ le long de certaines familles d'extensions galoisiennes géométriques L/K de corps de fonctions sur $k := \mathbb{F}_q$ et où C_1 et C_2 sont des classes de conjugaison de $\mathrm{Gal}(L/K)$.

D'après les résultats généraux de l'article [Bai20], notamment le Theorem 1.80 *ii)* du Chapitre 1.4.1, la densité $\delta(L/K; C_1, C_2)$ peut être représentée de la manière suivante. On supposera LI pour éviter les problèmes liés aux zéros inverses égaux à $\pm\sqrt{q}$.

Proposition 3.29. *Soit L/K une extension galoisienne géométrique de corps de fonctions sur $\mathbb{F}_q$, de groupe de Galois G. Supposons que* LI *soit vérifiée dans l'extension de corps de fonctions L/K. Pour toutes classes de conjugaison distinctes C_1 et C_2 de G, il existe deux variables aléatoires réelles $Y^+(L/K; C_1, C_2)$ et $Y^-(L/K; C_1, C_2)$ telles que*

$$\delta(L/K; C_1, C_2) = \frac{1}{2}\left(\mathbb{P}(Y^+(L/K; C_1, C_2) > 0) + \mathbb{P}(Y^-(L/K; C_1, C_2) > 0)\right).$$

Plus précisément, en notant Γ_χ *l'ensemble des arguments de zéros inverses de* $\mathcal{L}(u,\chi)$ *dans* $]0,\pi[$ *et en prenant* $(Z_\theta)_{\theta\in\Gamma_\chi,\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}}$ *des variables aléatoires indépendantes uniformes sur le cercle unité, on a*

$$Y^+(L/K;C_1,C_2) := r_{C_1} - r_{C_2} + 2\mathfrak{Re}\left(\sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}}(\chi(C_2)-\chi(C_1))\sum_{\theta\in\Gamma_\chi}Z_\theta\right)$$

et

$$Y^-(L/K;C_1,C_2) := 2\mathfrak{Re}\left(\sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}}(\chi(C_2)-\chi(C_1))\sum_{\theta\in\Gamma_\chi}Z_\theta\right).$$

De plus, on a

$$E(Y^+(L/K;C_1,C_2)) = r_{C_1} - r_{C_2},$$
$$E(Y^-(L/K;C_1,C_2)) = 0$$

et

$$\mathrm{Var}(Y^+L/K;C_1,C_2)) = \mathrm{Var}(Y^-(L/K;C_1,C_2)) = \sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}}|\chi(C_1)-\chi(C_2)|^2M_\chi,$$

où M_χ *est le degré du polynôme* $\mathcal{L}(u,\chi)$*.*

Il est facile de voir que $\mathbb{P}(Y^-(L/K;C_1,C_2)>0)=\frac{1}{2}$ car les variables aléatoires $Y^\pm(L/K;C_1,C_2)$ sont symétriques par rapport à leurs espérances. Il reste donc à estimer $\mathbb{P}(Y^+(L/K;C_1,C_2)>0)-\frac{1}{2}$. Pour ce faire, on va employer l'inégalité classique de Berry-Esseen ([Ess45, Chapter 2, Theorem 2a]), donnant une estimation de l'erreur dans le théorème central limite usuel.

Proposition 3.30. *Soit* Y *une variable aléatoire réelle, dont la fonction caractéristique est notée* φ_Y *et la fonction de répartition* F_Y*. Alors pour tout* $T>0$*, on a*

$$\sup_{x\in\mathbb{R}}\left|F_Y(x)-\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}e^{-\frac{t^2}{2}}\,\mathrm{d}t\right| \ll \int_{-T}^{T}\left|\frac{\varphi_Y(t)-e^{-\frac{t^2}{2}}}{t}\right|\mathrm{d}t+\frac{1}{T}.$$

Proposition 3.31. *Soit* L/K *une extension galoisienne géométrique de corps de fonctions sur* $\mathbb{F}_q$*, de groupe de Galois* G*. Supposons que* LI *est vérifiée dans* L/K *et que* G *est cyclique d'ordre* n *premier avec la caractéristique de* k*. Alors pour toutes classes de conjugaison distinctes* C_1 *et* C_2 *de* G*, on a*

$$\mathrm{Var}(Y^\pm(L/K;C_1,C_2)) \ll g_L.$$

Si de plus $g_K\in\{0,1\}$*, alors*

$$\mathrm{Var}(Y^\pm(L/K;C_1,C_2)) \gg \frac{\varphi(n)}{n^3}g_L,$$

où $\varphi(n)$ *est l'indicatrice d'Euler de* n*.*

Démonstration. D'après la Proposition 3.29, on a

$$\mathrm{Var}(Y^{\pm}(L/K;C_1,C_2)) = \sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}} |\chi(C_1)-\chi(C_2)|^2 M_\chi.$$

Or G est cyclique d'ordre n, ses caractères irréductibles s'identifient donc simplement aux caractères de Dirichlet modulo n, tous de degré 1, et $\varphi(n)$ d'entre eux sont fidèles. De plus, n est premier avec la caractéristique de k, et donc l'extension L/K est modérément ramifiée (puisque les indices de ramification divisent n). Ainsi, d'après la Proposition 3.18 et le Lemme 3.19 on a

$$\sum_{\chi\in\mathrm{Irr}(G)\text{ fidèle}} \deg\mathfrak{f}(\chi) = \varphi(n)R \leq \sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}} \deg\mathfrak{f}(\chi) \leq (n-1)R,$$

où $R := \sum_{P \text{ ramifié dans } L} \deg P$. Si χ est un caractère fidèle de G, alors $\chi(C_1)-\chi(C_2)$ est de la forme $e^{\frac{2i\pi ak}{n}} - e^{\frac{2i\pi al}{n}}$ avec $k \not\equiv l \bmod n$ (puisque C_1 et C_2 sont supposées distinctes) et $a \in \mathbb{Z}/n\mathbb{Z}$ inversible. Un simple développement limité à l'ordre 1 montre donc que $|\chi(C_1)-\chi(C_2)| \gg \frac{1}{n}$, tandis qu'on a évidemment $|\chi(C_1)-\chi(C_2)| \leq 2$. On a donc d'un côté

$$\begin{aligned}
\mathrm{Var}(Y^{\pm}(L/K;C_1,C_2)) &\leq 2 \sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}} M_\chi \\
&= 2 \sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}} ((2g_K-2) + \deg\mathfrak{f}(\chi)) \\
&= 2\left([L:K](2g_K-2) + \sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}} \chi(1)\deg\mathfrak{f}(\chi) - (2g_K-2)\right) = 4(g_L-g_K)
\end{aligned}$$

d'après la formule de Riemann-Hurwitz (Corollaire 3.20). De l'autre côté, on a

$$\begin{aligned}
\mathrm{Var}(Y^{\pm}(L/K;C_1,C_2)) &= \sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}} |\chi(C_1)-\chi(C_2)|^2 M_\chi \\
&\gg \frac{1}{n^2} \sum_{\chi\in\mathrm{Irr}(G)\text{ fidèle}} M_\chi \\
&\gg \frac{1}{n^2} \sum_{\chi\in\mathrm{Irr}(G)\text{ fidèle}} \deg\mathfrak{f}(\chi) \\
&\gg \frac{\varphi(n)}{n^3} \sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}} \deg\mathfrak{f}(\chi) \\
&= \frac{\varphi(n)}{n^3}(2g_L - 2 - [L:K](2g_K-2)),
\end{aligned}$$

toujours d'après la formule de Riemann-Hurwitz (Corollaire 3.20). Si $g_K \in \{0,1\}$ on obtient bien $\mathrm{Var}(Y^{\pm}(L/K;C_1,C_2)) \gg \frac{\varphi(n)}{n^3} g_L$. □

On peut désormais énoncer et démontrer notre théorème central limite pour des familles d'extensions superelliptiques.

Théorème 3.32. *Fixons $K := \mathbb{F}_q(x)$. Soit $n \geq 3$ tel que $q \equiv 1 \bmod n$. Pour tout $d > n$, on suppose que l'on dispose d'un polynôme $f_d \in \mathbb{F}_q[x]$ sans facteur carré de degré d tel que l'extension L_d/K satisfasse* LI*, où $L_d = K(y)$ avec $y^n = f_d$. Alors*

$$\max_{C_1,C_2 \in \mathrm{Gal}(L_d/K)^\sharp} \left|\delta(L_d/K; C_1, C_2) - \frac{1}{2}\right| \asymp_n \frac{1}{\sqrt{d}}.$$

Démonstration. Rappelons qu'il nous suffit d'estimer $\mathbb{P}(Y^+(L_d/K; C_1, C_2) > 0) - \frac{1}{2}$ puisqu'on a $\delta(L_d/K; C_1, C_2) = \frac{1}{4} + \frac{1}{2}\mathbb{P}(Y^+(L_d/K; C_1, C_2) > 0)$ d'après la Proposition 3.29 et la discussion qui la suit. Un calcul immédiat utilisant l'indépendance des Z_θ montre que la fonction caractéristique φ_{Y^+} de $Y^+(L_d/K; C, C_2)$ vaut

$$t \mapsto e^{i(r_{C_1} - r_{C_2})t} \prod_{\chi \in \mathrm{Irr}(G)\setminus\{\chi_0\}} J_0\left(2|\chi(C_2) - \chi(C_1)|t\right)^{M_\chi/2}$$

où J_0 est la fonction de Bessel de première espèce.

Posons

$$B(L_d/K; C_1, C_2) := \frac{\mathbb{E}(Y^+(L_d/K; C_1, C_2)}{\sqrt{\mathrm{Var}(Y^+(L_d/K; C_1, C_2))}}$$

et

$$W := \frac{Y^+(L_d/K; C_1, C_2) - \mathbb{E}(Y^+(L_d/K; C_1, C_2)}{\sqrt{\mathrm{Var}(Y^+(L_d/K; C_1, C_2))}}.$$

Il est clair que $\mathbb{E}(Y^+(L_d/K; C_1, C_2) = r_{C_1} - r_{C_2}$ est borné, tandis qu'on a $\mathrm{Var}(Y^+(L_d/K; C_1, C_2) \asymp_n d$ d'après la Proposition 3.31 et la Proposition 3.7. On réécrit maintenant

$$\begin{aligned}\mathbb{P}(Y^+(L_d/K; C_1, C_2) > 0) &= \mathbb{P}(W > -B(L_d/K; C_1, C_2)) \\ &= 1 - F_W(-B(L_d/K; C_1, C_2))\end{aligned}$$

où F_W désigne la fonction de répartition de W. D'après l'inégalité de Berry-Esseen, on a donc, en notant φ_W la fonction caractéristique de W,

$$F_W(-B(L_d/K; C_1, C_2)) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-B(L_d/K; C_1, C_2)} e^{-\frac{t^2}{2}}\,\mathrm{d}t + O\left(\int_{-T}^{T} \left|\frac{\varphi_W(t) - e^{-\frac{t^2}{2}}}{t}\right| \mathrm{d}t + \frac{1}{T}\right)$$

pour tout $T > 0$. Or, on a pour tout $t \in \mathbb{R}$,

$$\begin{aligned}\varphi_W(t) &= \varphi_{Y^+}\left(\frac{t}{\sqrt{\mathrm{Var}(Y^+(L_d/K; C_1, C_2)}}\right) e^{-iB(L_d/K; C_1, C_2)t} \\ &= \prod_{\chi \in \mathrm{Irr}(G)\setminus\{\chi_0\}} J_0\left(\frac{2|\chi(C_1) - \chi(C_2)|t}{\sqrt{\mathrm{Var}(L_d/K; C_1, C_2)}}\right)^{M_\chi/2}.\end{aligned}$$

Puisque $J_0(t) = 1 - \frac{t^2}{4} + O(t^4)$ au voisinage de 0, on a également $\log J_0(t) = -\frac{t^2}{4} + O(t^4)$. Ainsi, pour $|t| \leq \sqrt{\mathrm{Var}(Y^+(L_d/K; C_1, C_2))}$, et en se rappelant que $\sum_{\chi \in \mathrm{Irr}(G)\setminus\{\chi_0\}} |\chi(C_1) -$

$\chi(C_2)|^2 M_\chi = \mathrm{Var}(Y^+(L_d/K; C_1, C_2))$, on a

$$\begin{aligned}\varphi_W(t) &= \exp\left(-\sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}} \frac{M_\chi}{2}\frac{|\chi(C_1)-\chi(C_2)|^2t^2}{\mathrm{Var}(Y^+(L_d/K;C_1,C_2))} + O\left(\sum_{\chi\in\mathrm{Irr}(G)\setminus\{\chi_0\}}\frac{M_\chi|\chi(C_1)-\chi(C_2)|^4t^4}{\mathrm{Var}(Y^+(L_d/K;C_1,C_2))^2}\right)\right)\\ &= \exp\left(-\frac{t^2}{2}+O\left(\frac{t^4}{\mathrm{Var}(Y^+(L_d/K;C_1,C_2))}\right)\right)\\ &= e^{-\frac{t^2}{2}}\left(1+O\left(\frac{t^4}{\mathrm{Var}(Y^+(L_d/K;C_1,C_2))}\right)\right),\end{aligned}$$

où la deuxième égalité provient du fait que $|\chi(C_1)-\chi(C_2)|^4 \leq 4|\chi(C_1)-\chi(C_2)|^2$ puisque χ est de degré 1.

Posons maintenant $T = \mathrm{Var}(Y^+(L_d/K; C_1, C_2))$. On a alors

$$\int_{-\sqrt{T}}^{\sqrt{T}}\left|\frac{\varphi_W(t)-e^{-\frac{t^2}{2}}}{t}\right|\mathrm{d}t \ll \frac{1}{T}\int_0^{\sqrt{T}} t^3 e^{-\frac{t^2}{2}}\,\mathrm{d}t \ll \frac{1}{T}.$$

En raisonnant comme dans [FM13, Proposition 2.14], on obtient que si $\sqrt{T} \leq |t|$ alors $|\varphi_W(t)| \leq \varphi_W(\sqrt{T})$. On en déduit

$$\int_{\sqrt{T}\leq|t|\leq T}\left|\frac{\varphi_W(t)-e^{-\frac{t^2}{2}}}{t}\right|\mathrm{d}t \ll \varphi_W(\sqrt{T})\log T + \int_{\sqrt{T}\leq|t|\leq T}\frac{e^{-\frac{t^2}{2}}}{|t|}\,\mathrm{d}t \ll e^{-\frac{T}{3}}.$$

Finalement, on a montré que

$$\int_{-T}^{T}\left|\frac{\varphi_W(t)-e^{-\frac{t^2}{2}}}{t}\right|\mathrm{d}t \ll \frac{1}{T}.$$

Un développement de Taylor donne

$$\begin{aligned}\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{-B(L_d/K;C_1,C_2)} e^{-\frac{t^2}{2}}\,\mathrm{d}t &= \frac{1}{2}-\frac{1}{\sqrt{2\pi}}\int_{-B(L_d/K;C_1,C_2)}^{0} e^{-\frac{t^2}{2}}\,\mathrm{d}t\\ &= \frac{1}{2}-\frac{B(L_d/K;C_1,C_2)}{\sqrt{2\pi}}+O(B(L_d/K;C_1,C_2)^2).\end{aligned}$$

Finalement on a montré que

$$\mathbb{P}(Y^+(L_d/K;C_1,C_2)>0) = \frac{1}{2}+\frac{B(L_d/K;C_1,C_2)}{\sqrt{2\pi}}+O(B(L_d/K;C_1,C_2)^2)+O\left(\frac{1}{\mathrm{Var}(Y^+(L_d/K;C_1,C_2))}\right),$$

avec $B(L_d/K;C_1,C_2) = O\left(\frac{1}{\sqrt{\mathrm{Var}(Y^+(L_d/K;C_1,C_2))}}\right)$. D'après la Proposition 3.29, on a

$$\mathrm{Var}(Y^+(L_d/K;C_1,C_2)) \asymp_n g_{L_d}$$

et d'après la Proposition 3.7, on a

$$g_{L_d} \asymp_n d,$$

ce qui termine la démonstration. □

Remarque 3.33. Les résultats de Kowalski dans [Kow08] montrent que LI est vérifiée génériquement dans certaines extensions hyperelliptiques de $\mathbb{F}_q(x)$. Le long de telles extensions, la démonstration ci-dessus s'adapte immédiatement pour obtenir un théorème central limite inconditionnel. Le prix à payer est de devoir faire tendre q (puissance d'un nombre premier impair fixé) vers l'infini avec d pour garantir l'existence de telles courbes.

3.4 Perspectives

Pour terminer, voici quelques directions dans lesquelles on pourrait (et sur lesquelles l'auteur de ces lignes souhaite réfléchir) s'orienter pour établir de nouveaux résultats concernant l'évolution du biais de Tchebychev dans des familles d'extensions de corps de fonctions.

Il serait intéressant d'établir un énoncé analogue au Théorème 3.32 où le degré n est autorisé à varier avec d. Une analyse plus fine de la contribution de chaque conducteur d'Artin dans la formule de Riemann-Hurwitz (et pas simplement des caractères fidèles) ainsi que des quantités de la forme $|\chi(C_1)-\chi(C_2)|$ pourrait permettre d'atteindre un tel objectif en fournissant une minoration plus optimale de la variance $\mathrm{Var}(Y^{\pm}(L/K;C_1,C_2))$. On pourrait également étudier d'autres familles d'extensions où la ramification est suffisamment explicite pour obtenir des résultats asymptotiques similaires (par exemple des extensions d'Artin-Schreier).

Il serait également intéressant d'établir un résultat de grandes déviations analogue au Théorème 2.59 de Fiorilli et Jouve dans le cas où la quantité $B(L/K;C_1,C_2)$ tend vers l'infini. Un tel résultat devrait être appliqué à des familles où l'espérance $\mathbb{E}(Y^{\pm}(L/K;C_1,C_2))$ tend vers l'infini. Une telle chose peut se produire si l'on parvient à prescrire de nombreux zéros inverses en $\sqrt{q}$. Il semble donc envisageable de mener un travail comparable à ce qui est fait dans [Bai19] pour mettre en évidence l'influence de tels zéros sur le biais de Tchebychev.

Enfin, la théorie de Honda-Tate permet de prescrire un certain nombres de zéros inverses de fonctions zêta (et donc de fonctions L d'Artin). Des configurations convenables de zéros pourraient permettre de mettre en évidence d'autres types de comportements asymptotiques.

Bibliographie

[ANS14] A. Akbary, N. Ng, and M. Shahabi. Limiting distributions of the classical error terms of prime number theory. *Q. J. Math.*, 65(3) :743–780, 2014.

[Arm72] J. V. Armitage. Zeta functions with a zero at $s = \frac{1}{2}$. *Invent. Math.*, 15 :199–205, 1972.

[Bai19] A. Bailleul. Chebyshev's bias in dihedral and generalized quaternion Galois groups. arXiv:2001.06671, 2019.

[Bai20] A. Bailleul. Explicit Kronecker-Weyl and applications to prime number races. arXiv:2007.05763, 2020.

[BCdS+03] D. Bump, J. W. Cogdell, E. de Shalit, D. Gaitsgory, E. Kowalski, and S. S. Kudla. *An introduction to the Langlands program*. Birkhäuser Boston, Inc., Boston, MA, 2003. Lectures presented at the Hebrew University of Jerusalem, Jerusalem, March 12–16, 2001, Edited by Joseph Bernstein and Stephen Gelbart.

[BDJ+82] H. G. Bray, W. E. Deskins, D. Johnson, J. F. Humphreys, B. M. Puttaswamaiah, P. Venzke, and G. L. Walls. *Between nilpotent and solvable*. Polygonal Publ. House, Washington, N. J., 1982. Edited and with a preface by Michael Weinstein.

[Bel16] J. Bellaïche. Théorème de Chebotarev et complexité de Littlewood. *Ann. Sci. Éc. Norm. Supér. (4)*, 49(3) :579–632, 2016.

[Bes55] A. S. Besicovitch. *Almost periodic functions*. Dover Publications, Inc., New York, 1955.

[Bil99] P. Billingsley. *Convergence of probability measures*. Wiley Series in Probability and Statistics : Probability and Statistics. John Wiley & Sons, Inc., New York, second edition, 1999. A Wiley-Interscience Publication.

[Ble92] P. Bleher. On the distribution of the number of lattice points inside a family of convex ovals. *Duke Math. J.*, 67(3) :461–481, 09 1992.

[CFJ16] B. Cha, D. Fiorilli, and F. Jouve. Prime number races for elliptic curves over function fields. *Ann. Sci. Éc. Norm. Supér. (4)*, 49(5) :1239–1277, 2016.

[Cha08] B. Cha. Chebyshev's bias in function fields. *Compos. Math.*, 144(6) :1351–1374, 2008.

[CI11] B. Cha and B.-H. Im. Chebyshev's bias in Galois extensions of global function fields. *J. Number Theory*, 131(10) :1875–1886, 2011.

[Dav00] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[Deb16] A. Debreil. *Groupes finis et treillis de leurs sous-groupes*. Mathématiques en devenir. Calvage et Mounet, 2016.

[Dev86] L. Devroye. *Nonuniform random variate generation*. Springer-Verlag, New York, 1986.

[Dev19] L. Devin. Chebyshev's bias for analytic L-functions. In *Mathematical Proceedings of the Cambridge Philosophical Society*, pages 1–38. Cambridge University Press, 2019.

[Dev20] L. Devin. Limiting properties of the distribution of primes in an arbitrarily large number of residue classes. *Canadian Mathematical Bulletin*, pages 1–13, 2020.

[DM73] P. Damey and J. Martinet. Plongement d'une extension quadratique dans une extension quaternionienne. *J. Reine Angew. Math.*, 262/263 :323–338, 1973. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday.

[DM20] L. Devin and X. Meng. Chebyshev's bias for products of irreducible polynomials. arXiv:1809.09662, 2020.

[Dur19] R. Durrett. *Probability—theory and examples*, volume 49 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, Cambridge, 2019. Fifth edition.

[Ess45] C.-G. Esseen. Fourier analysis of distribution functions. A mathematical study of the Laplace-Gaussian law. *Acta Math.*, 77 :1–125, 1945.

[FHL19] K. Ford, A. J. Harper, and Y. Lamzouri. Extreme biases in prime number races with many contestants. *Math. Ann.*, 374(1-2) :517–551, 2019.

[Fio14] D. Fiorilli. Highly biased prime number races. *Algebra Number Theory*, 8(7) :1733–1767, 2014.

[FJ20a] D. Fiorilli and F. Jouve. Distribution of Frobenius elements in families of Galois extensions. arXiv:2001.05428, 2020.

[FJ20b] D. Fiorilli and F. Jouve. Unconditional Chebyshev biases in number fields. arXiv:2012.12245, 2020.

[FK02] K. Ford and S. Konyagin. The prime number race and zeros of L-functions off the critical line. *Duke Math. J.*, 113(2) :313–330, 2002.

[FK03] K. Ford and S. Konyagin. The prime number race and zeros of L-functions off the critical line. II. In *Proceedings of the Session in Analytic Number Theory and Diophantine Equations*, volume 360 of *Bonner Math. Schriften*, page 40. Univ. Bonn, Bonn, 2003.

[FLK13] K. Ford, Y. Lamzouri, and S. Konyagin. The prime number race and zeros of Dirichlet L-functions off the critical line : Part III. *Q. J. Math.*, 64(4) :1091–1098, 2013.

[FM00] A. Feuerverger and G. Martin. Biases in the Shanks-Rényi prime number race. *Experiment. Math.*, 9(4) :535–570, 2000.

[FM13] D. Fiorilli and G. Martin. Inequities in the Shanks-Rényi prime number race : an asymptotic formula for the densities. *J. Reine Angew. Math.*, 676 :121–212, 2013.

[FQ73] A. Fröhlich and J. Queyrut. On the functional equation of the Artin L-function for characters of real representations. *Invent. Math.*, 20 :125–138, 1973.

[Frö72] A. Fröhlich. Artin root numbers and normal integral bases for quaternion fields. *Invent. Math.*, 17 :143–166, 1972.

[Frö74] A. Fröhlich. The Galois module structure of algebraic integer rings in fields with generalised quaternion group. pages 81–86. Bull. Soc. Math. France Mém. 27, 1974.

[Frö83] A. Fröhlich. *Galois module structure of algebraic integers*, volume 1 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1983.

[FS10] K. Ford and J. Sneed. Chebyshev's bias for products of two primes. *Experiment. Math.*, 19(4) :385–398, 2010.

[HL18] A. J. Harper and Y. Lamzouri. Orderings of weakly correlated random variables, and prime number races with many contestants. *Probab. Theory Related Fields*, 170(3-4) :961–1010, 2018.

[Hum12] P. Humphries. The Mertens and Pólya conjectures in function fields. Australian National University, 2012.

[IK04] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[IR90] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Isa94] I. M. Isaacs. *Character theory of finite groups*. Dover Publications, Inc., New York, 1994. Corrected reprint of the 1976 original [Academic Press, New York ; MR0460423 (57 #417)].

[JLY02] C. U. Jensen, A. Ledet, and N. Yui. *Generic polynomials*, volume 45 of *Mathematical Sciences Research Institute Publications*. Cambridge University Press, Cambridge, 2002. Constructive aspects of the inverse Galois problem.

[Kac93] J. Kaczorowski. A contribution to the Shanks-Rényi race problem. *Quart. J. Math. Oxford Ser. (2)*, 44(176) :451–458, 1993.

[Kac95] J. Kaczorowski. On the distribution of primes (mod 4). *Analysis*, 15(2) :159–171, 1995.

[Kow08] E. Kowalski. The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros. *Int. Math. Res. Not. IMRN*, pages Art. ID rnn 091, 57, 2008.

[KT62] S. Knapowski and P. Turán. Comparative prime-number theory. i. *Acta Math. Acad. Sci. Hungar.*, 13 :299–314, 1962.

[Lam12] Y. Lamzouri. The Shanks-Rényi prime number race with many contestants. *Math. Res. Lett.*, 19(3) :649–666, 2012.

[Lam13] Y. Lamzouri. Prime number races with three or more competitors. *Math. Ann.*, 356(3) :1117–1162, 2013.

[Lan94] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Lan02] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Li18] W. Li. Vanishing of hyperelliptic L-functions at the central point. *J. Number Theory*, 191 :85–103, 2018.

[Lit14] J. E. Littlewood. Sur la distribution des nombres premiers. *C. R. Acad. des Sciences Paris*, 158 :1869–1872, 1914.

[LMO79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3) :271–296, 1979.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464, 1977.

[Mar77] J. Martinet. Character theory and Artin L-functions. In *Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 1–87, 1977.

[Mar02] G. Martin. Asymmetries in the Shanks-Rényi prime number race. In *Number theory for the millennium, II (Urbana, IL, 2000)*, pages 403–415. A. K. Peters, Natick, MA, 2002.

[Men18] X. Meng. Chebyshev's bias for products of k primes. *Algebra Number Theory*, 12(2) :305–341, 2018.

[MM97] M. Ram Murty and V. Kumar Murty. *Non-vanishing of L-functions and applications*. Modern Birkhäuser Classics. Birkhäuser/Springer Basel AG, Basel, 1997. [2011 reprint of the 1997 original] [MR1482805].

[MN17] G. Martin and N. Ng. Inclusive prime number races. arXiv:1710.00088v1, 2017.

[MN20] G. Martin and N. Ng. Inclusive prime number races. *Trans. Amer. Math. Soc.*, 373(5) :3561–3607, 2020.

[MO88] Hugh L. Montgomery and Andrew M. Odlyzko. Large deviations of sums of independent random variables. *Acta Arith.*, 49(4) :427–434, 1988.

[MS19] A. Malmendier and T. Shaska. From hyperelliptic to superelliptic curves. *Albanian J. Math.*, 13(1) :107–200, 2019.

[MV07] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Ng00] N. Ng. *Limiting distributions and zeros of Artin L-functions*. PhD thesis, University of British Columbia, 2000.

[Odl90] A. M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions : a survey of recent results. *Sém. Théor. Nombres Bordeaux (2)*, 2(1) :119–141, 1990.

[Pla04] B. Plans. On the minimal number of ramified primes in some solvable extensions of $\mathbb{Q}$. *Pacific J. Math.*, 215(2) :381–391, 2004.

[QQ13] H. Queffélec and M. Queffélec. *Diophantine approximation and Dirichlet series*, volume 2 of *Harish-Chandra Research Institute Lecture Notes*. Hindustan Book Agency, New Delhi, 2013.

[Rie59] B. Riemann. Ueber die anzahl der primzahlen unter einer gegebenen grosse. 1859.

[Ros02] M. Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[RS94] M. Rubinstein and P. Sarnak. Chebyshev's bias. *Experiment. Math.*, 3(3) :173–197, 1994.

[RS96] Z. Rudnick and P. Sarnak. Zeros of principal L-functions and random matrix theory. *Duke Math. J.*, 81(2) :269–322, 1996. A celebration of John F. Nash, Jr.

[Ser80] J.-P. Serre. *Corps locaux*. Hermann, 1980.

[Ser81] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54) :323–401, 1981.

[Ser98] J.-P. Serre. *Représentations linéaires des groupes finis, cinquieme édition corrigée et augmentée de nouveaux exercices, Coll.* Méthodes, Hermann, 1998.

[Ska13] D. Skabelund. *Character Tables of Metacyclic Groups*. PhD thesis, Brigham Young University, 2013.

[SL96] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2) :26–37, 1996.

[Sny02] N. Snyder. *Artin's L-functions : A Historical Approach*. PhD thesis, Harvard University, 2002.

[Tch53] P. Tchebychev. 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*, 1853.

[Tôy55] H. Tôyama. A note on the different of the composed field. In *Kodai Mathematical Seminar Reports*, volume 7, pages 43–44. Department of Mathematics, Tokyo Institute of Technology, 1955.

[Var06] J. L. Varona. Rational values of the arccosine function. *Cent. Eur. J. Math.*, 4(2) :319–322, 2006.

[vdGvdV95] G. van der Geer and M. van der Vlugt. On the existence of supersingular curves of given genus. *J. Reine Angew. Math.*, 458 :53–61, 1995.

[VS06] G. D. Villa Salvador. *Topics in the theory of algebraic function fields*. Mathematics : Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.

[Wat95] G. N. Watson. *A treatise on the theory of Bessel functions*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1995. Reprint of the second (1944) edition.

[Win41] A. Wintner. On the distribution function of the remainder term of the prime number theorem. *Amer. J. Math.*, 63 :233–248, 1941.