Study of the distribution of some short exponential sums

Théo Untrau

THÈSE

PRÉSENTÉE POUR OBTENIR LE GRADE DE

DOCTEUR DE L'UNIVERSITÉ DE BORDEAUX

École Doctorale de Mathématiques et d'Informatique
Spécialité : Mathématiques pures

par **Théo UNTRAU**

Étude de la répartition de certaines sommes exponentielles courtes

Sous la direction de **Florent JOUVE** et **Guillaume RICOTTA**

Soutenue le 10 juillet 2023 à l'Institut de Mathématiques de Bordeaux.

Membres du jury :

Mme Cécile DARTYGE	Maîtresse de conférence, Université de Lorraine	Rapportrice
M. Emmanuel ROYER	Professeur, Université Clermont Auvergne	Rapporteur
M. Pascal AUTISSIER	Professeur, Université de Bordeaux	Président
M. Farrell BRUMLEY	Maître de conférence, Université Sorbonne Paris Nord	Examinateur
M. Florent JOUVE	Professeur, Université de Bordeaux	Directeur de thèse
M. Guillaume RICOTTA	Maître de conférence, Université de Bordeaux	Directeur de thèse

Étude de la répartition de certaines sommes exponentielles courtes

Résumé : Cette thèse porte sur des propriétés d'équirépartition de certaines sommes exponentielles qui apparaissent naturellement en théorie analytique des nombres. Dans un premier temps, nous étendons des résultats de Duke, Garcia, Hyde et Lutz concernant des sommes de caractères additifs sur $\mathbf{F}_p$, mais restreintes au groupe $\mu_d(\mathbf{F}_p)$ des racines d^{e} de l'unité, pour un entier d fixé. Nous démontrons d'abord un résultat d'équirépartition portant sur des familles de sommes exponentielles paramétrées par le corps fini tout entier. Nous montrons ensuite qu'il y a toujours équirépartition si nos familles sont paramétrées par des "petits" sous-groupes multiplicatifs de $\mathbf{F}_p^\times$. Cette généralisation s'appuie sur des majorations de sommes exponentielles qui ont été obtenues par Bourgain, Chang, Glibichuk et Konyagin par des méthodes de combinatoire additive.
Dans un second temps, nous présentons les résultats d'un travail en commun avec Kowalski, où nous étendons les résultats précédents au cas des sommes exponentielles indexées par l'ensemble des racines dans $\mathbf{F}_p$ d'un polynôme unitaire à coefficients entiers. Nous montrons que ces sommes s'équirépartissent par rapport à une mesure qui est liée au groupe des relations additives entre les racines complexes du polynôme. On établit l'équirépartition des sommes de caractères multiplicatifs indexées par les racines d'un polynôme, mais cette fois-ci par rapport à une mesure qui est liée au groupe des relations multiplicatives entre les racines complexes. Nous présentons également des généralisations à des sommes de fonctions traces plus générales, ayant pour principal corollaire un résultat d'équirépartition de sommes de sommes de Kloosterman translatées par les racines d'un polynôme.
Enfin, un chapitre de ce manuscrit est dédié à la majoration de la discrépance, qui est une mesure de la vitesse d'équirépartition.

Mots-clés : *équirépartition, sommes exponentielles, relations linéaires entre nombres algébriques, fonctions traces.*

Unité de recherche : Institut de Mathématiques de Bordeaux, UMR 5251, 351 cours de la Libération, F 33 405 Talence.

Study of the distribution of some short exponential sums

Abstract: This thesis is about equidistribution properties of some exponential sums which arise naturally in analytic number theory. First, we generalize results of Duke, Garcia, Hyde and Lutz concerning sums of additive characters of $\mathbf{F}_p$, but restricted to the group $\mu_d(\mathbf{F}_p)$ of d–th roots of unity, for a fixed integer d. We prove an equidistribution result for families of exponential sums parametrized by the whole finite field. Then, we show that this result still holds for families solely parametrized by "small" multiplicative subgroups of $\mathbf{F}_p^\times$. This generalization relies on strong bounds on exponential sums which were obtained by Bourgain, Chang, Glibichuk and Konyagin using methods from additive combinatorics.
Then, we present the results obtained as part of a joint work with Kowalski, in which we extend the previous results to the case of exponential sums over the roots in $\mathbf{F}_p$ of an arbitrary monic polynomial with integral coefficients. We show that these sums become equidistributed with respect to a measure that is related to the group of additive relations among the complex roots of the polynomial. Similarly, sums of multiplicative characters over the roots of a polynomial become equidistributed with respect to a measure that is related to the group of multiplicative relations among complex roots. We also present generalizations to sums of more general trace functions. The main corollary is an equidistribution result concerning sums of Kloosterman sums shifted by roots of a polynomial.
Finally, a chapter of this manuscript is dedicated to the estimation of the discrepancy, which measures how fast equidistribution happens.

Keywords: *equidistribution, exponential sums, linear relations between algebraic numbers, trace functions.*

Remerciements

Je tiens en premier lieu à remercier mes directeurs de thèse, Florent Jouve et Guillaume Ricotta, pour m'avoir proposé ce sujet de thèse qui s'est révélé plein de belles surprises, et qui m'a permis de tâtonner en dessinant les sommes avec un ordinateur, ce qui me donnait l'impression de pouvoir avancer sur des exemples concrets assez tôt dans ma thèse, m'évitant ainsi le découragement qu'aurait pu provoquer la nécessité d'apprendre un lourd bagage théorique avant de rentrer dans le vif du sujet. Merci pour tout le temps que vous avez dédié à nos rendez-vous, pour vos relectures, et pour votre aide et votre soutien constant, tout en me laissant l'autonomie nécessaire pour que je me sente fier de mon travail. La longueur[1] des phrases précédentes donne un aperçu de ma tendance à rédiger beaucoup, et donc du travail qu'a dû représenter la lecture de ce manuscrit. Pour cela je remercie sincèrement Cécile Dartyge et Emmanuel Royer pour leur relecture attentive et pour leurs rapports très positifs. Enfin, merci à Pascal Autissier et Farrell Brumley pour leur intérêt pour mon travail et pour avoir également accepté de faire partie de mon jury de thèse.

Je tiens ensuite à remercier toutes les personnes avec qui j'ai discuté de maths au cours de ma thèse, et plus particulièrement Rémi et Jean-François pour le temps qu'ils m'ont accordé quand mes questions se rapprochaient de la géométrie; mes grands frères de thèse Alexandre et Corentin (notamment pour m'avoir suggéré de regarder l'erratum d'un certain livre, ce qui m'a fait réaliser que j'utilisais l'un des lemmes contenant une typo); ainsi qu'Emanuele pour les discussions sur les nombres premiers délicats et pour son aide précieuse sur la question de l'indépendance linéaire des j-invariants (senza di te ci avrei pensato per 6 mesi e non so se ce l'avrei fatta). Mes remerciements mathématiques vont aussi à Adrien, Anne-Edgar, Bianca, Jean et Martin pour leur investissement dans le groupe de travail sur la théorie du corps de classe (j'ai beaucoup appris grâce à vous !); à mes cobureaux qui m'ont éclairés à de nombreuses reprises, et qui laissaient souvent ce qu'ils étaient en train de faire pour que l'on réfléchisse ensemble (ne vous inquiétez pas, je vous remercie plus loin pour tout un tas d'autres choses que les maths !); et à mon frère de thèse Mounir, qui a bien voulu m'écouter répéter des exposés. Je suis également reconnaissant envers Cécile Dartyge et Thomas Stoll pour l'opportunité de présenter mon travail à Nancy, et envers Gérald Tenenbaum qui m'a suggéré de m'intéresser aux questions de discrépances. On this subject, I would also like to thank Igor Shparlinski for sending me an unpublished note from which I borrowed some ideas. Merci beaucoup à Régis de la Bretèche pour son invitation aux rencontres de théorie analytique et élémentaire des nombres, où j'ai eu grand plaisir à aller que ce soit en tant qu'orateur ou en tant que spectateur. Je remercie également Bill Allombert pour ses réponses à mes questions sur le nombre de classe d'un ordre et pour avoir fait tourner les calculs de sommes de Kloosterman de rang 3 qui m'ont permis de faire les illustrations les concernant dans le dernier chapitre. Enfin, cette thèse doit beaucoup à Emmanuel Kowalski, à travers ses notes de cours qui ont fortement influencé ma formation en théorie analytique et probabiliste des nombres, et à travers les échanges que nous avons eus qui ont conduit à notre article en commun.

La cellule informatique a souvent été d'un grand secours pendant cette thèse : merci de m'avoir toujours accueilli avec le sourire même quand mes questions avaient déjà leur réponse sur votre site. Merci à Sandrine, Sylvain et Philippe d'avoir été si moteurs pour la course du ruban rose, j'ai maintenant un très beau T-shirt grâce à vous. Merci à Thomas pour son aide à plusieurs reprises également. Comptez sur moi pour faire la publicité des services de la PLM, je suis un utilisateur conquis. Je re-

[1] peut-être même lourdeur ?

mercie également Cyril de la BMI pour son dévouement et sa gentillesse.

Merci à Ida et Agnès d'avoir organisé avec une telle efficacité les déplacements durant cette thèse et pour leur aide inestimable dans l'organisation des journées Margaux, accompagnées de Muriel M. Enfin, merci à Karine et Muriel H. (à qui je souhaite une belle retraite !) pour leur investissement en faveur des doctorants et des stagiaires, notamment leurs efforts pour comprendre le système complexe d'obtention des cartes du Haut-Carré (merci également à Nicolas pour son aide dans ce combat) !

Ensuite, même si j'en connais un qui va dire que j'aime vraiment bien passer pour un grand blessé (que je ne suis pas, j'en conviens) : je remercie très sincèrement mon kiné Alexandre, qui m'a remis sur pieds plus d'une fois et a été une part importante de ma vie sociale pendant l'un des confinements !

Je suis aussi reconnaissant aux étudiants que j'ai connus en tant que chargé de TD à l'Université de Bordeaux, leur bonne humeur (certes, ni permanente ni uniformément distribuée, mais malgré tout présente assez souvent) et leur intérêt pour ce que je faisais quand je n'étais pas en TD avec eux étaient nécessaires à mon moral. Bravo à vous pour votre parcours dans ces années particulières de déconfinements / reconfinements, et bonne continuation ! Je remercie tout particulièrement Melvine et Alessa de m'avoir fait confiance pour leurs stages malgré ma faible expérience d'encadrant : je suis heureux de vous connaître, et je vous souhaite le meilleur pour la suite ! Je remercie également Chantal Menini et Éric Balandraud qui étaient responsables d'UE pour ma première année d'enseignement, et avec qui j'ai eu plaisir à échanger cette année là et les suivantes.

I am grateful to the UBICOMP group of the University of Oulu for welcoming me several times, especially to Steve Lavalle for believing in the usefulness of mathematicians, and to Timo Ojala for his help on my applications in Finland. I am also very happy to know Alessandro, Anna, Başak, Katherine, Kalle, and Eetu and I hope to see you soon!

Merci à mes amis de toujours, les licornes de Pierrevert (qui n'y habitent plus beaucoup) : même si je n'ai pas réussi à suivre toutes les évolutions de vos checks et de vos expressions, vous me faites sentir comme quelqu'un de la bande à chaque fois que l'on se revoit, malgré mes retours assez sporadiques dans le sud, alors merci pour ça (ainsi que pour les découvertes musicales) !
Merci à Aurore et Estelle pour leur amitié depuis le lycée, pour les sorties à Esparron et pout le contact que l'on arrive à garder malgré le temps et la distance.
Merci aux amis de prépa de la conversation *Ex-incarcéré.e.s de Thiers*, notamment Dany qui m'a presque fait aimer la physique et qui m'a appris à toujours dire "ça va être super" avant une colle, Raph pour la découverte de la série *Over the Garden Wall* et pour les passages piétons d'Aix-en-Provence, et Auriane parce que te voir deux jours me donnera toujours la patate pour deux mois.
Merci aux amis de Rennes et tout d'abord à ceux de la conversation *Belote de la galère* : David pour ses notes hors contexte que j'aime tant relire, Tibo pour m'avoir fait vivre mes années de collégien qui bavarde en cours avec un peu de retard, et Thomas pour son aide à plein de moments. Merci à toute la troupe de la comuze, pour l'année en question, mais aussi pour tous les souvenirs de vacances, les interminables parties de loup-garou, la motivation pour le piano que je n'aurais jamais eue sans vous. Des remerciements particuliers à Pierre pour les répétitions sous l'arbre devant la bibliothèque, et pour notre préparation commune du second concours, à Émilie pour sa visite à Bordeaux et pour son accueil à Lille, à Clémentine pour son passage à Bordeaux également, et à Mathias pour *The Office*, *Parks and Recreation*, *Brooklyn 99* et son humour qui les surpasse.

Merci aux amis de l'IMB : Samuel et Simon car je me suis un peu senti un *runner* en vous suivant sur Strava alors que je n'ai pas couru depuis 6 mois, Jean pour les discussions de badminton (désolé que nous n'ayons jamais pu faire ce tournoi de double), Adrien, Yiye, Pierre-Jean, Jean-Frédéric, Gauthier, Julien, Gautier, Léo pour toutes les conversations au Haut-Carré. Merci à Martin et Anne-Edgar pour vos débats sans fin qui m'ont fait rire et m'ont appris beaucoup. En particulier, merci Martin de m'avoir appris un peu de politique sans juger trop sévèrement mon ignorance voire ma passivité, et

merci Anne-Edgar pour le partage de tes connaissances impressionnantes en maths, je gagnais parfois plus de recul en un repas au Haut-Carré qu'en plusieurs semaines de travail. Enfin, merci Issa d'avoir accepté de coencadrer le stage d'Alessa avec moi, j'étais rassuré de pouvoir compter sur quelqu'un de plus solide que moi en probabilités, et d'aussi bienveillant.

L'IMB non sarebbe l'IMB senza tutti gli italiani: grazie a Giuseppe, Giorgia, Emma, Beatrice. È sempre un piacere parlare con voi. Voglio ringraziare Simone[2] per l'espressione "mi fai perdere le staffe", e mi dispiace che non ho ancora visto *Mediterraneo*.

Voglio ringraziare i miei cobureaux in un misto di francese e d'italiano, perché ci parliamo cosi comunque. Bianca, Bianca, Bianca... Non smettere mai di fare n'importe quoi, merci pour ton énergie communicative, grazie anche per questo confinement al Voltaire, pour nos synchronisations de courses, per le tue invitazione a mangiare, per la tua torta della nonna per il mio compleanno con la schiena bloccata, et pour tant d'autres choses. Grazie Marco pour tes jeux de mots soulignés d'un C oscillant fait avec 2 doigts, pour le mot *regazz*, pour la découverte du fonctionnement de la dynamo de mon vélo, et pour les souvenirs que je garderai de tes manières originales de t'asseoir sur une chaise de bureau. Merci Agathe pour tous tes bons gâteaux, pour tes bavardages quand tu corriges des copies, pour ton écoute aussi, et pour ta force et ton équilibre inspirants entre le sport, les maths, les amis, le sommeil : j'aimerais un jour être aussi capable que toi de jouer sur tant de tableaux. Enfin, même si tu n'étais pas officiellement un cobureau, je pense que c'est dans ce paragraphe que tu te trouveras le mieux : grazie Paul d'avoir été présent pour me faire des petites courses à certains moments, merci pour toutes les sorties cinéma pour se frotter au "côté abrasif de la réalité", bravo pour ta combativité au tennis (désolé de ne pas toujours bien jouer dans le terrain) et pour tes imitations légendaires qui me font toujours rire.

Merci à toute ma famille d'Alsace et de Franche-Comté pour leur porte toujours ouverte et pour leur compréhension quand je n'étais pas de toutes les sorties car je me disais que je devais réviser. Merci à mes parents pour leur aide tout au long de mes études pour que je n'aie quasiment qu'à m'inquiéter des choses scolaires. Merci papa d'avoir toléré ma participation parfois faible au ratissage des feuilles, et bon courage pour les feuilles à venir. Merci maman de t'être passionnée pour les mots "congru" et "modulo", tu verras que j'en ai mis beaucoup dans cette thèse. Merci à Alix de ne pas s'être trop pressée de soutenir, histoire que je reste un petit instant de plus son grand frère, et pas juste son frère.

Infine, grazie Nicoletta per tutte le cose che sono più belle con te: per esempio il salmone al forno, i pommes-noisettes, gli[3] spinaci, tornare a casa a piedi perché non ci sono più bus, guardare un Michael, piegare bene bene, i calcoli con le matrici, vaccinarsi, cantare, fare mini-footings, montare un letto, andare nei bar, couper les légumes en tout petits bouts... Merci pour tous les surnoms que l'on se donne, et pour ceux qu'il nous reste à inventer. Ti voglio bene.

[2] l'unico italiano che conosce più canzoni di Brassens di tutti francesi.

[3] Avevo scritto "i" spinaci, come un stupido[4]

[4] Aaa, uno stupido!

Résumé étendu en français

Dans ce résumé en français, on présente les contributions de la thèse informellement afin de limiter l'introduction de trop nombreuses notations. Des énoncés précis et des références à leur localisation dans le corps du manuscrit sont fournis dans la section "Outline of the thesis" page 43.

Cette thèse porte sur l'étude du comportement asymptotique de certaines familles de sommes exponentielles[5], c'est-à-dire des sommes de la forme

$$\sum_{j \in J} e^{i\theta_j},$$

où J est un ensemble fini et les θ_j sont des nombres réels. En tant que sommes de nombres complexes de module 1, celles-ci sont de module inférieur ou égal au cardinal de l'ensemble J. Cette borne, dite triviale, est atteinte lorsque tous les θ_j sont égaux modulo 2π. Cependant, dans de nombreuses situations, des compensations entre les arguments θ_j permettent d'obtenir de bien meilleures majorations. Les deux illustrations suivantes permettent de visualiser ces deux types de comportement.

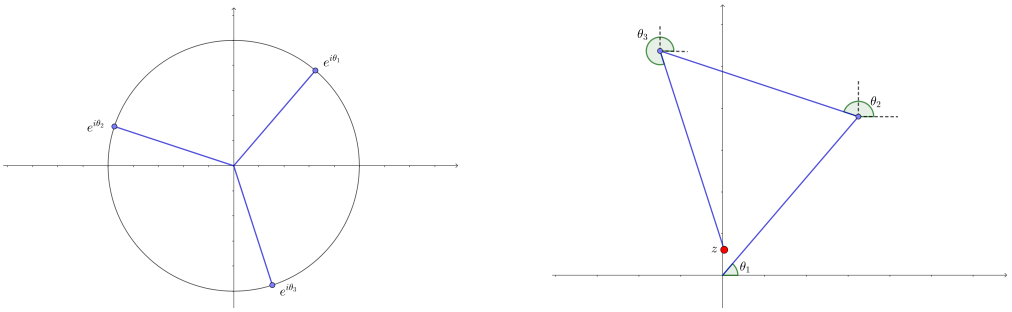


Figure 1: Le point $z = e^{i\theta_1} + e^{i\theta_2} + e^{i\theta_3}$ pour des angles $\theta_1, \theta_2, \theta_3$ "bien répartis" sur le cercle.

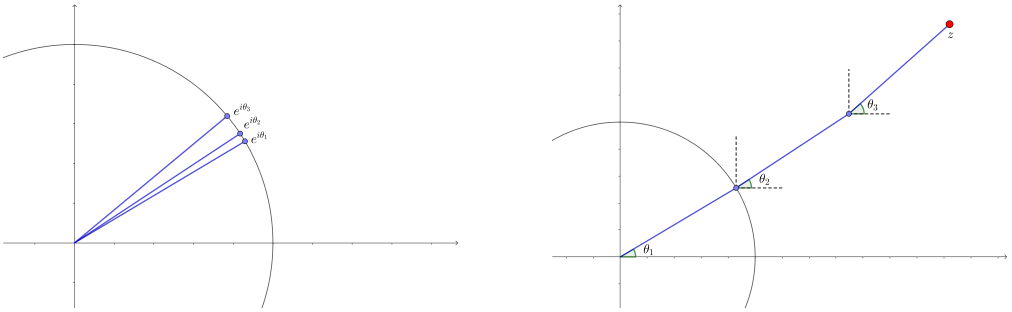


Figure 2: Le point $z = e^{i\theta_1} + e^{i\theta_2} + e^{i\theta_3}$ pour des angles $\theta_1, \theta_2, \theta_3$ presque égaux.

Lorsqu'elles apparaissent dans des problèmes de théorie des nombres, les sommes exponentielles font généralement intervenir des arguments θ_j de la forme $\frac{2\pi a_j}{n}$ pour un certain entier n, et des entiers a_j. Puisque le nombre complexe $e^{i\theta_j}$ ne dépend alors que de la classe de congruence de a_j modulo n, on

[5] Peut-être serait-il plus juste de les nommer sommes *d*'exponentielles, mais les deux terminologies semblent être utilisées.

parle alors de somme exponentielle "modulo n", ou "sur $\mathbf{Z}/n\mathbf{Z}$". L'étude des compensations entre les arguments qui conduisent à des majorations non-triviales du module de ces sommes est alors directement liée à la répartition des entiers a_j dans les classes de congruences modulo n.

Notation. Pour tout $t \in \mathbf{R}$, on note $e(t) := e^{2i\pi t}$ afin de ne pas encombrer les notations de $2i\pi$ (autrement dit, on rend l'exponentielle 1-périodique plutôt que $2i\pi$-périodique, ce qui est bien commode pour travailler avec des entiers).

Parmi les sommes que l'on rencontre fréquemment, on peut citer les sommes de Gauss :

$$\sum_{x \in \mathbf{Z}/n\mathbf{Z}} e\left(\frac{ax^2}{n}\right)$$

qui sont liées à la répartition des résidus quadratiques, et grâce auxquelles on peut démontrer la célèbre loi de réciprocité quadratique (voir section 1.1.1). Les sommes de Kloosterman

$$\mathrm{K}_n(a,b) := \sum_{x \in (\mathbf{Z}/n\mathbf{Z})^\times} e\left(\frac{ax + bx^{-1}}{n}\right), \tag{1}$$

où x^{-1} est l'inverse de x modulo n, ont également fait l'objet de nombreux travaux en théorie analytique des nombres. Elles apparaissent notamment dans une variante de la méthode du cercle introduite par Kloosterman pour étudier le nombre de façons dont un entier suffisamment grand peut-être représenté par la forme quadratique $ax^2 + by^2 + cz^2 + dt^2$ (voir section 1.1.3), ainsi que dans la théorie des formes modulaires (voir section 1.1.4).

On retrouve également des sommes exponentielles dans de nombreux problèmes d'équirépartition, grâce au célèbre critère de Weyl (voir section 1.2.2). En effet, ce dernier nous dit que pour prouver l'équirépartition d'une suite $(x_n)_{n \geqslant 1}$ dans l'intervalle $[0,1]$, il faut et il suffit de montrer que pour tout entier non-nul h,

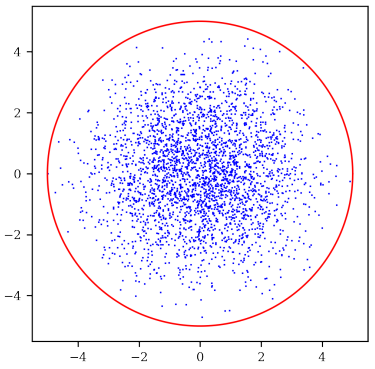
$$\frac{1}{N} \sum_{n=1}^{N} e(h \cdot x_n) \underset{N \to +\infty}{\longrightarrow} 0.$$

Ce critère fait clairement apparaître l'utilité de démontrer des majorations non-triviales du module de certaines sommes exponentielles.

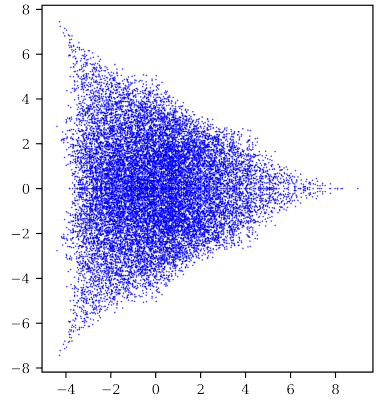
Cependant, après avoir démontré une majoration, c'est-à-dire après avoir prouvé que les sommes qui nous intéressent sont contraintes à vivre dans un certain disque du plan complexe, une question naturelle est : comment se répartissent-elles dans ce disque ? Si par exemple on considère des sommes de la forme $e^{i\theta_1} + \cdots + e^{i\theta_m}$ et que les θ_j "se comportent comme" des variables aléatoires indépendantes et uniformément réparties sur $[0, 2\pi]$, ces sommes vont progressivement remplir tout le disque de centre 0 et de rayon m, donnant lieu à des images comme le cas (a) de l'illustration ci-dessous. Cependant, ce comportement n'est pas toujours celui qui se produit, car les angles θ_j peuvent avoir des relations entre eux. Comme nous le verrons plus en détail dans cette thèse, si l'on considère les sommes de Kloosterman restreintes au sous-groupe d'ordre 9 pour un premier $p \equiv 1 \pmod 9$:

$$\mathrm{K}_p(a,b,9) := \sum_{\substack{x \in \mathbf{F}_p^\times \\ x^9 = 1}} e\left(\frac{ax + bx^{-1}}{p}\right)$$

alors celles-ci sont majorées en module par 9, mais le cas (b) de l'illustration ci-dessous suggère qu'elles sont loin de remplir le disque de centre 0 et de rayon 9 lorsque a et b parcourent $\mathbf{F}_p$. Elles semblent en effet se répartir suivant une mesure dont le support est strictement inclus dans ce disque.



(a) Plusieurs tirages d'une somme $X_1 + \cdots + X_5$ de variables aléatoires indépendantes et uniformément réparties sur $\mathbf{S}^1$.



(b) Les points $\mathrm{K}_p(a, b, 9)$ pour $p = 577$ et a et b variant dans $\mathbf{F}_p$.

Figure 3: Deux comportements différents de sommes exponentielles dont le module est borné respectivement par 5 et par 9.

Le principal but de cette thèse est de contribuer à la compréhension de la répartition de certaines sommes exponentielles particulières, notamment en déterminant quelles familles ont un comportement tel que celui qui est illustré dans le cas (a), et quelles familles ont un comportement tel qu'illustré dans le cas (b). Dans ce second cas, on se demande également quelles sont les relations de dépendance algébrique entre les termes de la somme qui la contraignent à tomber dans un certain sous-ensemble strict du disque, et quel est le lien entre la mesure pour laquelle ces sommes s'équirépartissent et ces relations algébriques.

Le chapitre 1 consiste en une introduction aux sommes exponentielles et à leurs applications en théorie des nombres, avant de présenter plus précisément les questions qui nous ont intéressés dans cette thèse. Le point de départ et la première motivation de ce sujet a été l'article [16], dans lequel les auteurs prouvent l'équirépartition des sommes de Kloosterman restreintes au sous-groupe d'ordre d :

$$\mathrm{K}_p(a, b, d) := \sum_{\substack{x \in \mathbf{F}_p^\times \\ x^d = 1}} e\left(\frac{ax + bx^{-1}}{p}\right),$$

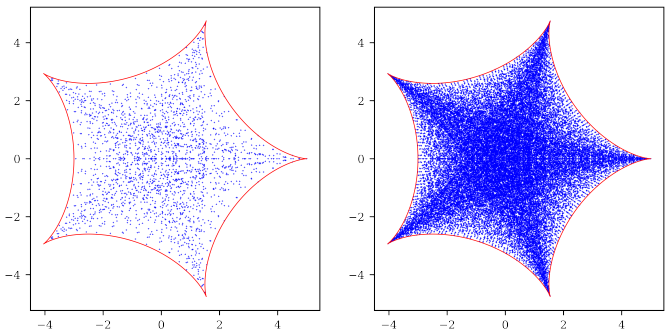
pour un entier d fixé et p tendant vers l'infini parmi les nombres premiers[6] congrus à 1 modulo d (cette condition assure qu'il y a bien d racines de l'unité distinctes dans $\mathbf{F}_p$). Par exemple, lorsque $d = 5$, ils montrent qu'il y a équirépartition dans la région du plan complexe délimitée par une hypocycloïde à 5 branches, comme l'illustre la Figure 4.
Cependant, ils démontrent ce résultat uniquement dans le cas où d est premier ou égal à 9, alors que dans le cas des sommes de la forme

$$\mathrm{S}_p(a, d) := \sum_{\substack{x \in \mathbf{F}_p \\ x^d = 1}} e\left(\frac{ax}{p}\right),$$

un résultat d'équirépartition analogue est démontré pour tout entier d, voir [32, 44].

Le chapitre 2 comble les cas restant entre [32, 44] et [16], en montrant l'équirépartition des sommes $\mathrm{K}_p(a, b, d)$ pour n'importe quel entier $d \geqslant 2$. De plus, nous étendons les résultats précédemment connus

[6] le cas des sommes modulo des puissances de tels nombres premiers est aussi traité de la même manière mais, dans ce résumé, nous n'évoquons que le cas des nombres premiers pour alléger les notations.



(a) $p = 151$ (b) $p = 631$

Figure 4: Les ensembles $\{\mathrm{K}_p(a, b, d);\ a, b \in \mathbf{F}_p\}$ pour $d = 5$ et deux valeurs de $p \equiv 1 \pmod 5$.

au cas des sommes de la forme

$$\sum_{\substack{x \in \mathbf{F}_p \\ x^d = 1}} e\left(\frac{a_1 x^{m_1} + \cdots + a_n x^{m_n}}{p}\right) \tag{2}$$

pour des entiers m_i quelconques (pouvant être négatifs, comme c'est le cas pour les sommes de Kloosterman) et des paramètres a_i variant dans $\mathbf{F}_p$. Lorsque les m_i sont tous premiers avec d, la mesure par rapport à laquelle ces sommes s'équirépartissent est la même que celle qui était déjà connue pour les sommes $\mathrm{S}_p(a, d)$ et $\mathrm{K}_p(a, b, d)$. En fait, nous montrons que plus généralement les sommes modulo des puissances de nombres premiers

$$\sum_{\substack{x \in \mathbf{Z}/p^\alpha\mathbf{Z} \\ x^d = 1}} e\left(\frac{a_1 x^{m_1} + \cdots + a_n x^{m_n}}{p^\alpha}\right)$$

satisfont ce résultat d'équirépartition lorsque p^α tend vers l'infini (p étant toujours supposé congru à 1 modulo d), sans faire aucune hypothèse sur le fait que la divergence vers l'infini soit due à la croissance de α ou à celle de p, ou à leurs croissances combinées.
Un aspect frappant de la preuve est le fait que les sommes qui apparaissent lorsque l'on applique le critère de Weyl ne tendent pas seulement vers 0, mais sont stationnaires. Cela est dû au fait que l'on autorise les paramètres a_i à varier dans tout $\mathbf{Z}/p^\alpha\mathbf{Z}$, ce qui donne des sommes complètes, qui valent soit 0 soit 1 par orthogonalité des caractères additifs de $\mathbf{Z}/p^\alpha\mathbf{Z}$. Ainsi, il est naturel de se demander si l'équirépartition est préservée lorsque l'on restreint les paramètres a_i à varier dans des sous-ensembles de $\mathbf{Z}/p^\alpha\mathbf{Z}$ (avec l'espoir qu'il y ait toujours convergence vers 0 dans le critère de Weyl, mais plus lentement).

C'est la question abordée au chapitre 3, dans lequel nous montrons que l'on peut restreindre les paramètres a_i à parcourir seulement de "petits" sous-groupes multiplicatifs de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$. Pour simplifier la présentation, supposons que $\alpha = 1$. Dans un premier temps, des estimations classiques sur le module des sommes de Gauss nous permettent de montrer qu'il y a toujours équirépartition des ensembles de sommes

$$\{\mathrm{S}_p(a, d),\ a \in H_p\}$$

par rapport à la même mesure que précédemment, à condition que H_p soit un sous-groupe multiplicatif de $\mathbf{F}_p^\times$ tel que $|H_p| \gg \sqrt{p}$. Dans un second temps, nous utilisons des majorations de sommes exponentielles obtenues par Bourgain, Chang, Glibichuk et Konyagin par des méthodes de combinatoire additive pour améliorer le résultat en remplaçant la condition $|H_p| \gg \sqrt{p}$ par $|H_p| \gg p^\delta$ pour n'importe quel $\delta > 0$. Cette généralisation ne se limite pas au cas des sommes de la forme $\mathrm{S}_p(a, d)$, mais est vraie plus généralement pour les sommes du type (2), à condition de laisser les paramètres a_i parcourir des sous-groupes multiplicatifs de $\mathbf{F}_p^\times$ suffisamment grands.

Le contenu des chapitres 2 et 3 a donné lieu à la prépublication [103].

Dans le chapitre 4, nous nous intéressons à la question plus générale de l'équirépartition de sommes exponentielles de la forme

$$\sum_{\substack{x\in\mathbf{F}_p\\ g(x)\equiv 0\,(\mathrm{mod}\,p)}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{p}\right) \tag{3}$$

lorsque g est un polynôme unitaire à coefficients entiers, et que p tend vers l'infini dans une certaine sous-suite de la suite des nombres premiers. En effet, dans le cas où $g(X)=X^d-1$, nous avions déjà besoin dans les chapitres précédents de la condition $p\equiv 1\,(\mathrm{mod}\,d)$ pour assurer que toutes les sommes considérées avaient bien le même nombre de termes. De même, dans ce cadre plus général, nous nous restreignons essentiellement aux valeurs de p pour lesquelles g est scindé à racines simples dans $\mathbf{F}_p$.
Les méthodes employées dans les chapitres précédents s'appuyaient sur le fait que pour le polynôme X^d-1, il est possible de choisir une racine primitive puis d'ordonner les racines en les écrivant comme les puissances successives de celle-ci. Cependant, pour un polynôme g quelconque, nous ne pouvons plus tirer avantage d'une telle paramétrisation des racines.
Dans le travail en commun [77] avec Emmanuel Kowalski, nous parvenons à franchir cette difficulté et à conclure à un résultat d'équirépartition pour ces sommes, qui fait apparaître une mesure limite qui est liée au groupe des relations additives entre les racines de g, c'est-à-dire le groupe

$$\mathrm{R}_g := \left\{\alpha\colon \mathrm{Z}_g\to\mathrm{Z}_g,\ \sum_{x\in\mathrm{Z}_g}\alpha(x)x\right\}$$

où Z_g est l'ensemble des racines complexes de g. Dans certaines situations (notamment lorsque le groupe de Galois de g est égal à tout le groupe symétrique), ce groupe des relations additives peut-être déterminé explicitement, et cela donne comme corollaire un résultat d'équirépartition relativement concret pour les sommes du type (3). Dans ce chapitre, nous traitons également le cas des sommes modulo des puissances de nombres premiers, et la question de la restriction des paramètres a_i à de petits sous-groupes multiplicatifs. Ce chapitre correspond aux sections 1 à 5 de la prépublication [77], écrite en collaboration avec Emmanuel Kowalski.

Dans le chapitre 5, nous étudions une notion de discrépance associée aux résultats d'équirépartition des chapitres précédents, afin de donner une majoration de la "vitesse d'équirépartition". Pour cela, nous avons été amenés à démontrer une généralisation de l'inégalité d'Erdös-Turán-Koksma à des sous-groupes fermés de $(\mathbf{S}^1)^k$. La classification de ces sous-groupes est bien connue, et nous dit qu'ils sont tous isomorphes à $(\mathbf{R}/\mathbf{Z})^d\oplus F$ pour un certain $d\leqslant k$ et un groupe abélien fini F. Ainsi, notre généralisation consiste à définir la discrépance via le choix d'un isomorphisme avec un groupe de la forme $(\mathbf{R}/\mathbf{Z})^d\oplus F$, puis à adapter la preuve classique de l'inégalité d'Erdös-Turán-Koksma pour tenir compte du facteur abélien fini qui est d'habitude absent.
Ensuite, en exploitant le fait que les sommes de Weyl sont nulles à partir d'un certain rang que l'on peut explicitement minorer, nous en déduisons une majoration de la discrépance en p^{-c_g}, où c_g est une constante strictement positive ne dépendant que du polynôme g dans la définition des sommes (3).

Enfin, le chapitre 6 traite de sommes de fonctions traces indexées par les racines d'un polynôme g satisfaisant les mêmes hypothèses que précédemment. Les fonctions traces sont des fonctions

$$t_p\colon \mathbf{F}_p\to\mathbf{C}$$

"ayant une origine algébrique", dont l'exemple le plus simple est celui des caractères additifs et multiplicatifs de $\mathbf{F}_p$. Ainsi, les sommes de la forme

$$\sum_{\substack{x\in\mathbf{F}_p\\ g(x)\equiv 0\,(\mathrm{mod}\,p)}} e\left(\frac{ax}{p}\right)$$

peuvent être vues comme un cas particulier de sommes de la forme

$$\sum_{\substack{x\in\mathbf{F}_p\\ g(x)\equiv 0\,(\mathrm{mod}\,p)}} t_p(ax)$$

et l'on peut se demander si des résultats d'équirépartition analogues à ceux des chapitres précédents peuvent être démontrés pour des fonctions traces plus générales. En fait, c'est le cas pour des fonctions traces associés à des faisceaux ℓ-adiques généreux au sens de Fouvry, Kowalski et Michel ("bountiful" en anglais). Un cas particulier de tel faisceau est le faisceau de Kloosterman, dont la fonction trace associée prend pour valeurs les sommes de Kloosterman définies en (1) (à une renormalisation près). En s'appuyant sur des faits déjà connus sur l'équirépartition de ces sommes prises individuellement, et sur l'indépendance des translatés qui provient du caractère généreux du faisceau, nous obtenons le résultat suivant :

Soit $g \in \mathbf{Z}[X]$ un polynôme unitaire séparable n'admettant pas 0 comme racine. Notons K_g le corps de décomposition de g sur $\mathbf{Q}$, et rappelons la définition des sommes de Kloosterman normalisées :

$$\mathrm{Kl}_2(a,p) := \frac{1}{\sqrt{p}} \sum_{x\in\mathbf{F}_p^\times} e\left(\frac{ax+x^{-1}}{p}\right).$$

Alors les sommes

$$\sum_{\substack{x\in\mathbf{F}_p\\ g(x)\equiv 0\,(\mathrm{mod}\,p)}} \mathrm{Kl}_2(ax,p),$$

paramétrées par $a \in \mathbf{F}_p$, s'équirépartissent dans $\mathbf{R}$ par rapport à une mesure qui est la loi d'une somme de $\deg(g)$ variables aléatoire indépendantes, chacune suivant la loi de Sato–Tate sur $[-2,2]$, lorsque p tend vers l'infini parmi les nombres premiers totalement décomposés dans K_g.

Ce chapitre correspond aux sections 6 et 7 de la prépublication [77].

Enfin nous concluons cette thèse en évoquant quelques perspectives de recherche qui constituent une suite naturelle aux questions étudiées jusqu'à présent : le caractère optimal de la condition en p^δ pour l'équirépartition de sous-groupes de $\mathbf{F}_p^\times$, la détermination du module des relations additives ou multiplicatives entre racines pour d'autres familles de polynômes que celles considérées dans cette thèse, et enfin les problèmes "horizontaux" correspondant à nos résultats d'équirépartition dits "verticaux".

Contents

Notations

- The number of elements of a finite set X is denoted by $|X|$ or $\#X$.
- If $a, b \in \mathbf{Z}$, we denote by (a, b) their gcd (greatest (positive) common divisor).
- If $a \in \mathbf{Z}$ and p is a prime number, we denote by $v_p(a)$ the p-adic valuation of a.
- $m \mid n$ means that the integer m divides the integer n.
- $p^\alpha \mid\mid n$ means that $p^\alpha \mid n$ and $p^{\alpha+1} \nmid n$ (in other words, $\alpha = v_p(n)$).
- If d is a positive integer, ϕ_d denotes the d^{th} cyclotomic polynomial over $\mathbf{Q}$ and $\varphi(d)$ its degree.
- If $x \in \mathbf{R}$, we denote by $\{x\} := x - \lfloor x \rfloor$ its fractional part. If $\mathbf{x} = (x_1, \dots, x_m) \in \mathbf{R}^m$, we denote by $\{\mathbf{x}\} := (\{x_1\}, \dots, \{x_m\})$ the fractional part of $\mathbf{x}$ taken componentwise.
- Let $(X, \mathscr{A})$ and $(Y, \mathscr{B})$ be two measurable spaces, and let λ be a measure on the former. If $f \colon X \to Y$ is $(\mathscr{A}, \mathscr{B})$-measurable, then we denote by $f_*\lambda$ the pushforward measure of λ via f. It is defined as the measure on $(Y, \mathscr{B})$ such that $(f_*\lambda)(B) = \lambda(f^{-1}(B))$ for all $B \in \mathscr{B}$.
- $\mathbf{S}^1$ denotes the multiplicative group of complex numbers of modulus 1, while $\mathbb{T}$ denotes the additive group $\mathbf{R}/\mathbf{Z}$. We also use the standard notation

$$e(t) := \exp(2i\pi t) \quad \text{for all } t \in \mathbf{R}.$$

- If f and g are two functions defined on a set X, with values in $\mathbf{R}_+$, we write $f(x) \ll g(x)$ to say that there exists a positive constant C such that for all $x \in X$, $f(x) \leqslant Cg(x)$. If we want to stress that C depends on other constants of the problem, say ε and δ, we write $f(x) \ll_{\varepsilon,\delta} g(x)$.
- $A \approx B$ is used in a very informal sense, it is sometimes used in heuristic reasonings to signify that A and B have approximately the same size.
- If A is a commutative ring, and n is a positive integer, we denote by $A_n[X]$ the set of polynomials with coefficients in A of degree less than or equal to n.
- $\mu_d(K)$ denotes the set of d-th roots of unity on a field K, while $\mu_d^\star(K)$ denotes the subset of *primitive* d-th roots of unity.
- If G is a group, we denote by $G^\sharp$ the space of conjugacy classes of G.

Chapter 1

Introduction

In the first part of this introduction, we present some historical background to show that exponential sums appear in many different contexts in number theory. For instance, we will see that they play a role in the study of solutions to polynomial equations over finite fields, but also over $\mathbf{Z}$, via the application of the circle method. One can also be interested in exponential sums for their presence in the theory of modular and automorphic forms. Then, we give a brief reminder on equidistribution (in particular equidistribution modulo 1) and we explain that some arithmetic quantities tend to behave "randomly", in the sense that they become equidistributed in certain spaces. Finally, we combine both aspects by stating a few equidistribution results where the arithmetic quantities of interest are themselves exponential sums.
In a second part, we give an overview of the topics discussed in the thesis, and we state the contributions that one can find in the following chapters.

Contents

Part A: Historical background

1.1. Exponential sums in number theory

In this section, we present several applications of exponential sums in number theory, in order to give many different motivations for their study. Just for simplicity of exposition in this introduction, what we will call exponential sums *modulo* m will be sums of m-th roots of unity of the form

$$\sum_{x\in A} e\left(\frac{f(x)}{m}\right)$$

where A is a finite set and f is a function defined on A, with values in $\mathbf{Z}/m\mathbf{Z}$. In a few cases, one can prove a closed formula for such sums, but generically it is completely out of reach, and we are interested in finding good upper and lower bounds for their absolute value, or getting a better understanding of their distribution when considered in families. For these sums, we always have the so-called trivial bound:

$$\left|\sum_{x\in A} e\left(\frac{x}{m}\right)\right| \leqslant |A|$$

which follows from the triangle inequality and the fact that we are summing complex numbers of modulus 1. Very often, improvements on this trivial bound have consequences in problems of arithmetic nature, as we will see in the examples below.

1.1.1. Quadratic reciprocity law

If p and q are distinct prime numbers, we tend to think of the arithmetic modulo p and the arithmetic modulo q as being independent. Indeed, the Chinese Remainder Theorem states for instance that belonging to a certain residue class modulo p does not impose any restriction on the residue class modulo q. The quadratic reciprocity law is the surprising fact that the events "p is a quadratic residue modulo q" and "q is a quadratic residue modulo p" are actually not at all independent!
There are hundreds of proofs of the quadratic reciprocity law, and many of them rely on properties of exponential sums. Following [69], we will present what is perhaps the most classical proof, which relies on the explicit evaluation of the quadratic Gauss sums.
But before that, let us recall the definition of the Legendre symbol and state the main theorem.

Definition 1.1. *If p is an odd prime number, we define the Legendre symbol $\left(\frac{\cdot}{p}\right)$ as follows:*

$$\begin{array}{rccc} \left(\frac{\cdot}{p}\right) & : & \mathbf{F}_p & \to & \{-1,0,1\} \\ & & a & \mapsto & \left(\frac{a}{p}\right), \end{array}$$

where

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if there exists } x \in \mathbf{F}_p^\times \text{ such that } a = x^2 \\ 0 & \text{if } a = 0 \\ -1 & \text{otherwise.} \end{cases}$$

In the first case, we say that a is a *quadratic residue* modulo p, while in the last case we say that it is a *quadratic nonresidue*.

Actually, one can prove that the Legendre symbol coincides with the map $a \mapsto a^{\frac{p-1}{2}}$, hence is a group homomorphism on $\mathbf{F}_p^\times$.

Theorem 1.2 (Quadratic reciprocity law, Gauss 1796)**.** *If p and q are two distinct odd prime numbers, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}.$$

In other words,

- if either p or q is congruent to 1 modulo 4, then p is a quadratic residue modulo q if and only if q is a quadratic residue modulo p.
- if p and q are congruent to 3 modulo 4, then p is a quadratic residue modulo q if and only if q is a quadratic nonresidue modulo p.

One of the classical proofs of Theorem 1.2 involves the quadratic Gauss sums, defined for any integer $m \geqslant 2$ as follows:

$$G_m := \sum_{x \in \mathbf{Z}/m\mathbf{Z}} e\left(\frac{x^2}{m}\right).$$

These sums belong to the small class of examples where a closed formula can be obtained. Namely, one has the following theorem.

Theorem 1.3 (Gauss). *For all odd integers $m \geqslant 3$, we have*

$$G_m = \begin{cases} \sqrt{m} & \text{if } m \equiv 1 \,(\mathrm{mod}\, 4) \\ i\sqrt{m} & \text{if } m \equiv 3 \,(\mathrm{mod}\, 4) \end{cases}$$

We will come back to this type of sums in Chapter 3, and in particular we give references in Appendix 3.A for the fact that if m is prime, then $|G_m| = \sqrt{m}$ (this is fairly elementary). However, proving that the exact value is $\sqrt{m}$ or $i\sqrt{m}$ depending on the reduction of m modulo 4 is much more difficult, see for instance [53, Chapter 6].

Once we admit the above theorem on quadratic Gauss sums, the proof of Theorem 1.2 is quite short.

Proof of Theorem 1.2. It suffices to prove that

$$G_{pq} = G_p G_q \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \tag{1.1}$$

because then it follows from Theorem 1.3 that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \text{ or if } q \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Now, in order to prove (1.1), we first observe that the map

$$\begin{array}{ccc} \mathbf{F}_p \times \mathbf{F}_q & \to & \mathbf{Z}/pq\mathbf{Z} \\ (x_1, x_2) & \mapsto & qx_1 + px_2 \end{array}$$

is a bijection. Indeed, it is well defined because if x_1 changes by a multiple of p, the outcome changes by a multiple of pq, and similarly if x_2 changes by a multiple of q. Moreover it is surjective because p and q are coprime. The conclusion follows from the equality of the cardinalities on both sides.
Thus, we have

$$\begin{aligned} G_{pq} &= \sum_{x \in \mathbf{Z}/pq\mathbf{Z}} e\left(\frac{x^2}{pq}\right) = \sum_{x_1 \in \mathbf{F}_p} \sum_{x_2 \in \mathbf{F}_q} e\left(\frac{(qx_1 + px_2)^2}{pq}\right) \\ &= \left(\sum_{x_1 \in \mathbf{F}_p} e\left(\frac{qx_1^2}{p}\right)\right)\left(\sum_{x_2 \in \mathbf{F}_q} e\left(\frac{px_2^2}{q}\right)\right) \end{aligned}$$

using the fact that $2pqx_1x_2 \equiv 0 \bmod pq$. Now, we can rewrite the first sum as

$$\sum_{x_1 \in \mathbf{F}_p} e\left(\frac{qx_1^2}{p}\right) = \sum_{y \in \mathbf{F}_p} \left(1 + \left(\frac{y}{p}\right)\right) e\left(\frac{qy}{p}\right)$$

because any non-zero square has exactly two square roots and 0 has only one. Besides,

$$\sum_{y\in\mathbf{F}_p} e\left(\frac{qy}{p}\right) = 0$$

by orthogonality of the additive characters of $\mathbf{F}_p$ (or more elementarily by summation of a geometric series), because q is non-zero modulo p. Therefore,

$$\begin{aligned}\sum_{x_1\in\mathbf{F}_p} e\left(\frac{qx_1^2}{p}\right) &= \sum_{y\in\mathbf{F}_p}\left(\frac{y}{p}\right) e\left(\frac{qy}{p}\right) = \sum_{z\in\mathbf{F}_p}\left(\frac{q^{-1}z}{p}\right) e\left(\frac{z}{p}\right)\\ &= \left(\frac{q^{-1}}{p}\right)\sum_{z\in\mathbf{F}_p}\left(\frac{z}{p}\right) e\left(\frac{z}{p}\right) = \left(\frac{q}{p}\right)\sum_{z\in\mathbf{F}_p}\left(\frac{z}{p}\right) e\left(\frac{z}{p}\right)\\ &= \left(\frac{q}{p}\right) G_p\end{aligned}$$

Switching the roles of p and q, the same proof shows that

$$\sum_{x_2\in\mathbf{F}_q} e\left(\frac{px_2^2}{q}\right) = \left(\frac{p}{q}\right) G_q$$

and this finishes the proof of (1.1). □

1.1.2. Point counting on varieties defined over finite fields

Another number theoretic context in which exponential sums arise is when one is interested in the number of solutions of polynomial equations over finite fields. Indeed, if p is a prime number and we denote by $\widehat{\mathbf{F}_p}$ the dual of $(\mathbf{F}_p, +)$ (i.e. the group of additive characters of $\mathbf{F}_p$), then by orthogonality of characters we have

$$\frac{1}{p}\sum_{\psi\in\widehat{\mathbf{F}_p}} \psi(x) = \begin{cases} 1 \text{ if } x = 0\\ 0 \text{ otherwise.}\end{cases}$$

In other words, this average over the additive characters gives a functions which detects the residue class 0 modulo p. Thus, if we are given a polynomial $Q \in \mathbf{F}_p[X_1, \dots, X_m]$, the number of solutions $(x_1, \dots, x_m) \in \mathbf{F}_p^m$ to the equation

$$Q(x_1, \dots, x_m) = 0$$

is given by

$$N_Q(p) = \frac{1}{p}\sum_{x_1,\dots,x_m\in\mathbf{F}_p}\sum_{\psi\in\widehat{\mathbf{F}_p}} \psi(Q(x_1, \dots, x_m)). \tag{1.2}$$

Finally, since we have an explicit description of the additive characters of $\mathbf{F}_p$, namely

$$\widehat{\mathbf{F}_p} = \{\psi_h,\ h \in \mathbf{F}_p\}$$

where

$$\begin{array}{rccc}\psi_h & : & \mathbf{F}_p & \to & \mathbf{C}^*\\ & & x & \mapsto & e\left(\frac{hx}{p}\right)\end{array}$$

the formula (1.2) indeed gives the number of solutions to a polynomial equation in terms of exponential sums.

Example 1.4. Let $p \geqslant 3$ be a prime number. For $a \in \mathbf{F}_p$, we denote by

$$S(a, p) := \{(x, y, z) \in \mathbf{F}_p^3 \mid x^2 + y^2 + z^2 = a\},$$

which is an algebraic variety of $\mathbf{F}_p^3$, given by the equation of a sphere. Then, thanks to the above discussion, the cardinality of $S(a,p)$ may be written as

$$|S(a,p)| = \frac{1}{p} \sum_{x,y,z \in \mathbf{F}_p} \sum_{h \in \mathbf{F}_p} e\left(\frac{h}{p}(x^2+y^2+z^2-a)\right)$$

Changing the order of summation, we obtain

$$|S(a,p)| = \frac{1}{p} \sum_{h \in \mathbf{F}_p} \tau(h)^3 e\left(\frac{-ah}{p}\right)$$

where

$$\tau(h) := \sum_{x \in \mathbf{F}_p} e\left(\frac{hx^2}{p}\right).$$

Now, one can show elementarily that for all $h \in \mathbf{F}_p^\times$, $|\tau(h)| = \sqrt{p}$ (we give references and generalizations of this fact in Appendix 3.A), and since $\tau(0) = p$, we deduce that

$$|S(a,p)| \underset{p \to \infty}{=} p^2 + O(p^{\frac{3}{2}})$$

where the implied constant is independent of a.

1.1.3. The circle method

This method first appeared in a paper of Hardy and Ramanujan in 1918 concerning the number of partitions of an integer: [48]. In this section, we aim to present the main ideas of the method, and to show that understanding the order of magnitude of certain exponential sums over finite fields or finite rings plays a crucial role in the resolution of several additive problems in number theory. We follow substantial parts of [108] and [54].

Additive problems in number theory. Let us introduce what we will call an additive problem in number theory. Usually, we are given s subsets of the set of natural numbers, which we will denote by $\mathcal{A}_1, \dots, \mathcal{A}_s$, and we want to understand whether or not a positive integer N can be written as a sum $a_1 + \cdots + a_s$, where each a_j belongs to $\mathcal{A}_j$. In other words, we want to determine whether or not the set $\{(a_1, \dots, a_s) \in \mathcal{A}_1 \times \cdots \times A_s;\ a_1 + \cdots + a_s = N\}$ is empty. More generally, one may ask about the cardinality of this set, and one seeks for exact formulas, or rather asymptotic estimates as N goes to infinity when exact formulas are out of reach.

In many famous problems, all the $\mathcal{A}_j$ are the same set $\mathcal{A}$, and in that case we will denote by $r_{\mathcal{A}}(s,N)$ the number of representations of N as a sum of s elements of $\mathcal{A}$, that is the cardinality of the set

$$\{(a_1, \dots, a_s) \in \mathcal{A}^s;\ a_1 + \cdots + a_s = N\}.$$

For example, in what is known as Waring's problem, we fix an integer k and let $\mathcal{A}$ be the set of k-th powers of natural numbers, so the question we are asking is: can we write N as $a_1^k + \cdots + a_s^k$ for some natural numbers $a_1, \dots, a_s$? What is the least s for which any positive integer is the sum of s k-th powers? For instance, when $k = 2$, Lagrange's four square theorem asserts that for any positive integer N there are always four integers a_i such that $N = a_1^2 + \cdots + a_4^2$. Moreover it is well-known that not all positive integers may be written as a sum of one, two or three squares, so this answers Waring's problem for $k = 2$: the least number of squares one needs to allow in order to write all natural numbers as a sum of squares is 4.

Another famous additive problem is called Goldbach's conjecture, and consists in taking $s = 2$ and for $\mathcal{A}$ the set of prime numbers. The conjecture asserts that any even number larger than 3 can be written as the sum of two prime numbers. In our notations, this amounts to saying that $r_{\mathcal{A}}(2, 2m) > 0$ for all

$m \in \mathbf{Z}_{\geqslant 2}$.

Finally, since we are going to use it to illustrate some ideas of the circle method in a simplified setting, let us discuss one easier problem. We take $\mathcal{A}$ to be the set of all non-negative integers, and $s \geqslant 1$. Then for all $N \geqslant 1$, $r_{\mathcal{A}}(s, N)$ counts the number of ways N may be written as a sum of s non-negative integers. In other words, $r_{\mathcal{A}}(s, N)$ is the cardinality of the set

$$\{(a_1, \dots, a_s) \in \mathbf{N};\ a_1 + \cdots + a_s = N\}.$$

This problem can actually be solved without appealing to the circle method, just by using a combinatorial argument. Start by writing N as $1+1+\cdots+1$, and then replace 1's by dots. Then decompositions of N as sums s of natural numbers correspond to the different choices of positions of $(s-1)$ bars between these dots. For instance the decomposition $7 = 4+2+1$ corresponds to $\bullet\bullet\bullet\bullet\,|\,\bullet\bullet|\bullet$, while $7 = 3+0+4$ corresponds to $\bullet\bullet\bullet||\,\bullet\bullet\bullet\bullet$. So counting decompositions of N as sums of s natural numbers amounts to counting the number of words in the alphabet $\{\bullet, |\}$ made of N dots and $s-1$ bars. Therefore,

$$r_{\mathcal{A}}(s, N) = \binom{N+s-1}{s-1}.$$

In the following section, we propose another approach to this problem, which gives a first idea of what the circle method is, and why it bears that name.

A first glance at the circle method. In the remainder of this introduction to the circle method, we will always assume that the set $\mathcal{A}$ is infinite. Let $\mathcal{A}$ be such a subset of $\mathbf{N}$. We define the power series

$$f_{\mathcal{A}}(z) := \sum_{n=0}^{+\infty} a(n) z^n, \tag{1.3}$$

where $a(n) = 1$ if $n \in \mathcal{A}$ and $a(n) = 0$ otherwise. For all $\rho \in [0, 1[$, the series

$$\sum_{n=0}^{+\infty} a(n)\rho^n$$

is absolutely convergent, while the series

$$\sum_{n=0}^{+\infty} a(n)$$

diverges because of the assumption on the cardinality of $\mathcal{A}$. Therefore, the power series (1.3) has radius of convergence 1. For all $|z| < 1$, we have

$$\begin{aligned} f_{\mathcal{A}}^s(z) &= \left(\sum_{n_1=0}^{+\infty} a(n_1) z^{n_1}\right) \cdots \left(\sum_{n_s=0}^{+\infty} a(n_s) z^{n_s}\right) \\ &= \sum_{n_1=0}^{+\infty} \cdots \sum_{n_s=0}^{+\infty} a(n_1) \cdots a(n_s) z^{n_1+\cdots+n_s} \\ &= \sum_{N=0}^{+\infty} c(N) z^N \end{aligned}$$

where

$$c(N) = \sum_{\substack{(n_1,\dots,n_s)\in\mathbf{N}^s \\ n_1+\cdots+n_s=N}} a(n_1)\cdots a(n_s) = \sum_{\substack{(n_1,\dots,n_s)\in\mathcal{A}^s \\ n_1+\cdots+n_s=N}} 1 = r_{\mathcal{A}}(s, N)$$

Therefore, the coefficients $c(N)$ of the Taylor series of the holomorphic function $f_{\mathcal{A}}^s(z)$ are exactly the numbers $r_{\mathcal{A}}(s, N)$ that we are trying to evaluate!

The next step, which is the reason why this method is called the circle method, consists in applying Cauchy's theorem to write these coefficients in terms of an integral over a circle. Precisely, since

$$f_{\mathcal{A}}^s(z) = \sum_{N=0}^{+\infty} r_{\mathcal{A}}(s,N) z^N$$

with radius of convergence 1, we have that for any $\rho \in]0,1[$,

$$r_{\mathcal{A}}(s,N) = \frac{1}{2\pi i} \int_{\mathscr{C}(0,\rho)} \frac{f_{\mathcal{A}}^s(z)}{z^{N+1}} \mathrm{d}z. \tag{1.4}$$

Therefore, the question of evaluating or finding the asymptotic behaviour of $r_{\mathcal{A}}(s,n)$ has been translated into a question about the integral over a circle on the right-hand side of (1.4). Let us see what this gives in the simple example where $\mathcal{A} = \mathbf{N}$. In that case we have

$$f_{\mathcal{A}}(z) = \sum_{n=0}^{+\infty} z^n = \frac{1}{1-z},$$

so (1.4) becomes

$$r_{\mathcal{A}}(s,N) = \frac{1}{2\pi i} \int_{\mathscr{C}(0,\rho)} \frac{1}{(1-z)^s z^{N+1}} \mathrm{d}z. \tag{1.5}$$

Now, thanks to the generalized binomial theorem, the following holds for all z in the interior of the unit disk:

$$\frac{1}{(1-z)^s} = \sum_{k=0}^{+\infty} \binom{s+k-1}{k} z^k, \tag{1.6}$$

and the series converges uniformly on any closed disk centered at 0 and of radius $\rho < 1$. Therefore, in (1.5), we can replace $(1-z)^{-s}$ by its series expansion given by equation (1.6), and permute the sum and the integral. This leads to the equality

$$r_{\mathcal{A}}(s,n) = \sum_{k=0}^{+\infty} \binom{s+k-1}{k} \frac{1}{2\pi i} \int_{\mathscr{C}(0,\rho)} z^{k-N-1} \mathrm{d}z.$$

Finally, we conclude using the fact that

$$\frac{1}{2\pi i} \int_{\mathscr{C}(0,\rho)} z^{k-N-1} \mathrm{d}z = \mathbb{1}_{k=N}$$

hence

$$r_{\mathcal{A}}(s,N) = \binom{s+N-1}{N} = \binom{s+N-1}{s-1},$$

which is indeed the result we found using a purely combinatorial argument. However, we have been extremely lucky, it is not always the case that one can explicitly evaluate the integral (1.4)! One may also object that we made this look like an analytic method by hiding the combinatorial nature in the generalized binomial theorem, which we did not prove. However, we hope that this convinces the reader that Cauchy's formula might be useful to study $r_{\mathcal{A}}(s,N)$ with more analytic tools at our disposition. In the next paragraph, we present Vinogradov's refinement of the method, and go a little bit further into the details.

Vinogradov's refinement and the apparition of exponential sums. In many additive questions, it is clear that only "sufficiently small" integers will have a contribution in the counting problem. For instance, if we want to study the number of representations of N as a sum of squares $x_1^2 + \cdots + x_s^2$, we only need to focus our attention on integers x_i such that $|x_i| \leqslant \sqrt{N}$. Therefore, the generating series (1.3)

$$\sum_{n=0}^{+\infty} a(n) z^n$$

(where $a(n) = 1$ if n is a square, and equals 0 otherwise) may be replaced by a *finite* sum for the study of the number of representations of N (namely: up to $n = \sqrt{N}$ in the current example). This has the advantage of letting us choose the circle of integration to be always of radius 1, because the issue of the convergence of the generating series does not arise. Therefore, we can make the change of variables $z = e(\alpha)$ and the only Cauchy's integral formula we will need is actually

$$\int_0^1 e(m\alpha)\mathrm{d}\alpha = \begin{cases} 1 & \text{if } m = 0 \\ 0 & \text{otherwise,} \end{cases}$$

which is just another writing for

$$\int_{\mathscr{C}(0,1)} z^m \mathrm{d}z = \begin{cases} 1 & \text{if } m = -1 \\ 0 & \text{otherwise.} \end{cases}$$

Let us now give a brief overview of how the circle method can be applied to tackle a Diophantine problem. The following lines are inspired to a large extent by the presentation of [54].

Let $f \in \mathbf{Z}[X_1, \dots, X_s]$ be a polynomial of degree k. We want to count integral solutions to the equation

$$f(x_1, \dots, x_s) = 0$$

inside a certain bounded box $\mathcal{B} := [-B, B]^s$ of $\mathbf{R}^s$ (for instance, in Waring's problem associated with k-th powers, one wants to study the number of representations of an integer N in the form $x_1^k + \cdots + x_s^k$, hence one is naturally led to consider the polynomial $f(X_1, \dots, X_s) := X_1^k + \cdots + X_s^k - N$ and taking $B \approx N^{1/k}$ will ensure that the solutions inside $\mathcal{B}$ are actually *all* solutions).

Remark 1.5. Since there are $\approx B^s$ possible points $(x_1, \dots, x_s)$ in $\mathcal{B} \cap \mathbf{Z}^s$ and f maps them into a set of $\approx B^k$ points (because f has degree k and we hope that generically it will vary enough to reach most integer points), we expect that if any point in the image gets a fair share of preimages, the point 0 will have $\approx B^{s-k}$ preimages. So we expect that unless there are some obstructions to this pseudo-random behaviour, the equation $f(x_1, \dots, x_s) = 0$ will have $\approx B^{s-k}$ solutions in $\mathcal{B} \cap \mathbf{Z}^s$. So we see here that there is hope to prove that solutions exist when s is substantially larger than k, i.e. when the number of variables is sufficiently larger than the degree of the polynomial.

The first step of the circle method consists in writing, for all $x = (x_1, \dots, x_s) \in \mathbf{Z}^s$,

$$\mathbb{1}_{f(x)=0} = \int_0^1 e(f(x)\alpha)\mathrm{d}\alpha$$

which implies that the counting function

$$\nu_f(\mathcal{B}) := |\{x \in \mathcal{B} \cap \mathbf{Z}^s,\ f(x) = 0\}|$$

is given by the following integral:

$$\nu_f(\mathcal{B}) = \int_0^1 \underbrace{\left(\sum_{x \in \mathcal{B} \cap \mathbf{Z}^s} e(f(x)\alpha) \right)}_{=: S_f(\alpha)} \mathrm{d}\alpha. \tag{1.7}$$

The next step consists in splitting the integral into minor arcs and major arcs. The idea is that the contributions to the counting function will be handled very differently depending on whether α is "close to" a rational with "small" denominator or not. A motivation for doing this is that when α is close to a rational a/q, the contribution of $S_f(\alpha)$ to the integral (1.7) is related to the behaviour of $f(x)$ in residue classes modulo q, a problem which seems more manageable than the original Diophantine equation, especially if q is not too large. On the other hand, if α is not close to a rational number with small denominator, we hope that the behaviour of $e(\alpha f(x))$, as x varies, will be random enough to ensure cancellations in $S_f(\alpha)$, so that it will give a negligible contribution. This is motivated, for

instance, by the uniform distribution modulo 1 of the sequence $(\alpha n)_{n\geqslant 1}$ when α is irrational.

The precise meaning of "close to" and "small" depends on the problem, so we choose to remain vague on this point.

Definition 1.6 (major arcs, minor arcs)**.** *Let P and Q be two positive integers satisfying $2Q \leqslant P$. For any rational number $\frac{a}{q} \in [0,1[$ with $(a,q)=1$ and $q \leqslant Q$, denote by*

$$\mathfrak{M}(q,a) := \left\{\alpha \in [0,1[,\ \left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{qP}\right\}$$

It is called the major arc centered at $\frac{a}{q}$. Then we denote by

$$\mathfrak{M} := \bigcup_{\substack{(a,q)=1\\ q\leqslant Q}} \mathfrak{M}(q,a)$$

the set of all major arcs, and by $\mathfrak{m} := [0,1[\setminus\mathfrak{M}$ the set of minor arcs.

The assumption that $2Q \leqslant P$ ensures that two major arcs centered at different rationals do not overlap.

Remark 1.7. The parameters P and Q need to be chosen carefully depending on the specific problem one is interested in, and typically depend on B, hence on N in Waring's problem $x_1^k + \cdots + x_s^k = N$. Therefore, whenever we write "error term" in the remainder of this section, one needs to have in mind that the error terms depend on B, P and Q, and only become error terms after a suitable choice of dependences between these parameters. Quoting [1]: *Applying the Circle Method is all about finding the right balance between choosing the minor arcs small enough so their contribution is insignificant and choosing the major arcs small enough such that the integral is easily computable.*

Now, let us study the sum $S_f(\alpha)$ when $\alpha \in \mathfrak{M}$. Write $\alpha = \frac{a}{q} + \theta$ where $q \leqslant Q$, $(a,q)=1$ and $|\theta| \leqslant \frac{1}{qP}$. Then we have

$$S_f(\alpha) = \sum_{x\in\mathcal{B}\cap\mathbf{Z}^s} e(f(x)\alpha) = \sum_{u \,(\mathrm{mod}\, q)} \sum_{\substack{x\in\mathcal{B}\cap\mathbf{Z}^s\\ x\equiv u \,(\mathrm{mod}\, q)}} e\left(f(x)\left(\frac{a}{q}+\theta\right)\right)$$

where the sum ranges over $u = (u_1,\dots,u_s)$ in $(\mathbf{Z}/q\mathbf{Z})^s$ and the notation $x \equiv u \,(\mathrm{mod}\, q)$ means that $x_i \equiv u_i \,(\mathrm{mod}\, q)$ for all $i \in \{1,\dots,s\}$. Thus,

$$S_f(\alpha) = \sum_{u \,(\mathrm{mod}\, q)} e\left(\frac{a}{q} f(u)\right) \sum_{\substack{x\in\mathcal{B}\cap\mathbf{Z}^s\\ x\equiv u \,(\mathrm{mod}\, q)}} e\left(\theta f(x)\right).$$

Next, by a truncated version of Poisson summation formula (see [54, eq. above (20.31) and Lemma 8.8]), we can replace the inner sum by $\frac{1}{q^s}\mathcal{B}_f(\theta)$, where

$$\mathcal{B}_f(\theta) := \int_{\mathcal{B}} e\left(\theta f(x)\right) \mathrm{d}x$$

with a good error term under certain conditions (we need θ to be small, so we need P to be relatively large, since $|\theta| \leqslant \frac{1}{qP}$). This implies that

$$S_f(\alpha) = \mathcal{C}_f(a/q)\mathcal{B}_f(\theta) + (\text{error term}),$$

with

$$\mathcal{C}_f(a/q) := \frac{1}{q^s} \sum_{u \,(\mathrm{mod}\, q)} e\left(\frac{a}{q} f(u)\right).$$

Therefore, the contribution of the major arcs to the counting function $\nu_f(\mathcal{B})$ is:

$$\begin{aligned}\int_{\mathfrak{M}} S_f(\alpha)\mathrm{d}\alpha &= \sum_{q\leqslant Q}\sum_{a\in(\mathbf{Z}/q\mathbf{Z})^\times}\int_{|\theta|\leqslant\frac{1}{qP}} S_f\left(\frac{a}{q}+\theta\right)\mathrm{d}\theta\\ &= \sum_{q\leqslant Q}\sum_{a\in(\mathbf{Z}/q\mathbf{Z})^\times} \mathcal{C}_f(a/q)\int_{|\theta|\leqslant\frac{1}{qP}}\mathcal{B}_f(\theta)\mathrm{d}\theta + (\text{error term})\\ &= \sum_{q\leqslant Q} c_f(q)\int_{|\theta|\leqslant\frac{1}{qP}}\mathcal{B}_f(\theta)\mathrm{d}\theta + (\text{error term})\end{aligned}$$

where

$$c_f(q) = \frac{1}{q^s}\sum_{a\in(\mathbf{Z}/q\mathbf{Z})^\times}\sum_{u\,(\mathrm{mod}\,q)} e\left(\frac{a}{q}f(u)\right).$$

Next, it can be shown that in several applications of the circle method (such as Waring's problem), $|\mathcal{B}_f(\theta)| \ll_{\mathcal{B}} \theta^{-1-\gamma}$ for some $\gamma > 0$ so that the integral over $|\theta| \leqslant \frac{1}{qP}$ can be approximated by the integral over the whole real line, with a good error term:

$$\int_{|\theta|\leqslant\frac{1}{qP}}\mathcal{B}_f(\theta)\mathrm{d}\theta = \underbrace{\int_{\mathbf{R}}\mathcal{B}_f(\theta)\mathrm{d}\theta}_{=:V_f(\mathcal{B})} + (\text{error term})$$

Thus, we conclude that the contribution of the integral over the major arcs takes the following form:

$$\int_{\mathfrak{M}} S_f(\alpha)\mathrm{d}\alpha = V_f(\mathcal{B})\sum_{q\leqslant Q} c_f(q) + (\text{error term}). \tag{1.8}$$

The *singular integral* $V_f(\mathcal{B})$ admits an interpretation in terms of density of the real zeros of f in $\mathcal{B}$, but we will not focus on that, as we wish to shed more light on the places where exponential sums appear.

Up to this point, we progressively turned the counting problem into an analytic problem involving integrals and exponential sums, but we did not use any bound on exponential sums. The following assumption is a first example of non-trivial exponential sum estimate which plays a crucial role in the asymptotic evaluation of the sum of the $c_f(q)$.

Assumption 1.8. *There exists $\eta > 0$ such that for all $q \geqslant 1$, for all $a \in (\mathbf{Z}/q\mathbf{Z})^\times$, $\mathcal{C}_f(a/q) \ll q^{-2-\eta}$.*

Recall that

$$\mathcal{C}_f(a/q) := \frac{1}{q^s}\sum_{u\,(\mathrm{mod}\,q)} e\left(\frac{a}{q}f(u)\right),$$

so this assumption really is about finding non-trivial cancellations in an exponential sum. If Assumption 1.8 is satisfied, then it is easy to deduce that

$$\left|\sum_{q>Q} c_f(q)\right| \ll Q^{-\eta}.$$

This implies that in (1.8), we can replace the finite sum up to Q by the sum of the series, up to an acceptable error term:

$$\int_{\mathfrak{M}} S_f(\alpha)\mathrm{d}\alpha = V_f(\mathcal{B})\mathfrak{S}_f + (\text{error term}).$$

where $\mathfrak{S}_f = \sum_{q=1}^{+\infty} c_f(q)$ is called the *singular series*. It turns out that this series contains the information on the p-adic solutions to the equation $f(x) = 0$, as we will explain now. Indeed, we have

$$c_f(q) = \frac{1}{q^s} \sum_{u \,(\mathrm{mod}\, q)} \left[\sum_{a \in (\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{a}{q} f(u)\right) \right]$$

and the inner sum is a well known type of exponential sum called a *Ramanujan sum*. It can be evaluated explicitly using Möbius inversion formula, and this gives:

$$\sum_{a \in (\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{a}{q} f(u)\right) = \sum_{\substack{d|q \\ d|f(u)}} \mu\left(\frac{q}{d}\right) d.$$

Therefore,

$$c_f(q) = \frac{1}{q^s} \sum_{d|q} \mu\left(\frac{q}{d}\right) d \sum_{\substack{u \,(\mathrm{mod}\, q) \\ d|f(u)}} 1.$$

Moreover,

$$|\{u \bmod q,\ f(u) \equiv 0 \bmod d\}| = \frac{q^s}{d^s} |\{x \bmod d,\ f(x) \equiv 0 \bmod d\}|,$$

so

$$c_f(q) = \sum_{d|q} \mu\left(\frac{q}{d}\right) \underbrace{\frac{|\{x \bmod d,\ f(x) \equiv 0 \bmod d\}|}{d^{s-1}}}_{=:\omega_f(d)} = (\mu \star \omega_f)(q),$$

where the star denotes the Dirichlet convolution of arithmetic functions. Now, since ω_f is multiplicative and the convolution of multiplicative functions is multiplicative, we deduce that

$$c_f(q) = \prod_{p^\alpha || q} \left(\omega_f(p^\alpha) - \omega_f(p^{\alpha-1})\right).$$

Thus,

$$\mathfrak{S}_f = \sum_{q=1}^{+\infty} c_f(q) = \sum_{q=1}^{+\infty} \prod_{p^\alpha || q} \left(\omega_f(p^\alpha) - \omega_f(p^{\alpha-1})\right) = \prod_p \delta_f(p),$$

where $\delta_f(p) = 1 + \sum_{\alpha=1}^{+\infty} \left(\omega_f(p^\alpha) - \omega_f(p^{\alpha-1})\right)$. Under Assumption 1.8, all the infinite series and products converge, and we have

$$\delta_f(p) = \lim_{\alpha \to +\infty} \omega_f(p^\alpha).$$

As

$$\omega_f(p^\alpha) = \frac{|\{x \in (\mathbf{Z}/p^\alpha\mathbf{Z})^s,\ f(x) \equiv 0 \bmod p^\alpha\}|}{(p^\alpha)^{s-1}},$$

the factor $\delta_f(p)$ can be interpreted as the density of p-adic solutions to the equation $f(x) = 0$. Indeed, a heuristic reasoning as in Remark 1.5 shows that if all the residue classes modulo p^α get a fair share of preimages under the map induced by f between $(\mathbf{Z}/p^\alpha\mathbf{Z})^s$ and $\mathbf{Z}/p^\alpha\mathbf{Z}$, then $(p^\alpha)^{s-1}$ is actually the expected number of solutions, so $\omega_f(p^\alpha)$ should be close to 1 in situations where the heuristic can be made rigorous.

As a conclusion, the contribution of the major arcs is given by

$$\int_{\mathfrak{M}} S_f(\alpha) \mathrm{d}\alpha = V_f(\mathcal{B}) \mathfrak{S}_f + (\text{error term}),$$

where $V_f(\mathcal{B})$ can be interpreted as the density of the real solutions to the equation $f(x) = 0$, while the singular series $\mathfrak{S}_f$ admits a factorization as an infinite product over the primes, each factor measuring the density of solutions modulo prime powers.

The final task is to prove that the contribution of the minor arcs is negligible in front of the main term $V_f(\mathcal{B})\mathfrak{S}_f$ that was obtained for the major arcs. There also, estimates on exponential sums play a role, see e.g. [54, Chapter 20].

Kloosterman's variant. In his article [66], Kloosterman introduced a variant of the circle method to study the question of the number of representations of an integer in the form $ax^2+by^2+cy^2+dt^2$, under some conditions on the coefficients $a,b,c,d \in \mathbf{N}$. Along the way, he was led to introduce the following exponential sums (defined for any prime number p), which are now named after him:

$$\mathrm{K}_p(a,b) := \sum_{x\in\mathbf{F}_p^\times} e\left(\frac{ax+bx^{-1}}{p}\right) \quad \text{for } a,b\in\mathbf{F}_p$$

These sums are real numbers, and they are trivially bounded by $p-1$. However, Kloosterman needed to prove a non-trivial bound in order to understand what was the main term, and what was negligible in his variant of the circle method. By considering the 4-th moment of the family of Kloosterman sums, that is:

$$\sum_{a,b\in\mathbf{F}_p^\times} |\mathrm{K}_p(a,b)|^4$$

he reduced to an elementary counting problem, namely the problem of counting solutions $(x_1,x_2),(y_1,y_2)$ in $(\mathbf{F}_p^\times)^2$ to the equations

$$\begin{cases} x_1+x_2 = y_1+y_2 \\ x_1^{-1}+x_2^{-1} = y_1^{-1}+y_2^{-1}. \end{cases}$$

He obtained the following non-trivial bound: for all $a,b\in\mathbf{F}_p^\times$, $|\mathrm{K}_p(a,b)| \leqslant 2p^{3/4}$, and this allowed him to conclude on the question of representation of integers by diagoonal quadratic forms in four variables.

1.1.4. Fourier coefficients of modular forms

Kloosterman sums also arise naturally in the study of modular forms and more generally of automorphic forms, and in this section we aim at providing an idea of what those specific functions are, why they are studied by number theorists, and at which place do Kloosterman sum play a role. This section is mostly based on [54, Chap. 14 & 15] and [15], where a far more detailed introduction to the subject can be found.

Let $\mathbf{H} := \{z\in\mathbf{C} \mid \mathrm{Im}(z)>0\}$ denote the Poincaré upper-half plane. The group $\mathrm{SL}_2(\mathbf{R})$ acts on $\mathbf{H}$ by Möbius transformations: if $\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbf{R})$ and $z\in\mathbf{H}$, then

$$\gamma.z = \frac{az+b}{cz+d}.$$

We will be interested in the restriction of this action to discrete subgroups of $\mathrm{SL}_2(\mathbf{R})$, such as $\mathrm{SL}_2(\mathbf{Z})$. For arithmetic applications, one also often encounters the *congruence* subgroups

$$\Gamma_0(q) := \left\{ \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \mid c\equiv 0 \,(\mathrm{mod}\, q)\right\}.$$

Note that $\Gamma_0(1)=\mathrm{SL}_2(\mathbf{Z})$. We can now define modular forms: they are holomorphic functions on $\mathbf{H}$ which transform nicely under the action of the modular group $\mathrm{SL}_2(\mathbf{Z})$ or one of its congruence subgroup.

Definition 1.9. *For two positive integers $k,q\geqslant 1$, a modular form of weight k and level q is a holomorphic function $f\colon \mathbf{H}\to\mathbf{C}$ such that for all $\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \Gamma_0(q)$, for all $z\in\mathbf{H}$,*

$$f(\gamma.z) = (cz+d)^k f(z)$$

and such that it is holomorphic at cusps.

For modular forms of level 1 (i.e. modular forms of the full modular group $\mathrm{SL}_2(\mathbf{Z})$), the holomorphy at the cusp ∞ can be explained in a rather elementary way: since $z \mapsto z+1 \in \mathrm{SL}_2(\mathbf{Z})$, any level 1 modular form is 1-periodic, hence admits a Fourier expansion of the form

$$\sum_{n=-\infty}^{+\infty} a_f(n) e(nz)$$

we say that

- f is meromorphic at ∞ if there exits $N \in \mathbf{Z}$ such that for all $n \leqslant N$, $a_f(n) = 0$;
- f is holomorphic at ∞ if for all $n < 0$, $a_f(n) = 0$;
- f is a cusp form if it is holomorphic at ∞ and moreover $a_f(0) = 0$.

The second condition above is precisely the condition of holomorphy at the cusp ∞ of Definition 1.9.

Several important questions in the theory of modular forms are related to the order of magnitude of the Fourier coefficients $a_f(n)$. For instance, a motivation can come from the fact that in order to understand the domain of definition of the associated L-function

$$L(f,s) := \sum_{n=1}^{+\infty} \frac{a_f(n)}{n^s}$$

one needs to have estimates for the growth of the sequence $(a_f(n))_{n\geqslant 1}$. It turns out that for the definition of the L-functions, the following estimate due to Hardy suffices:

Proposition 1.10 ([15, Proposition 1.3.5]). *If f is a cusp form of weight k and level 1, then*

$$a_f(n) \ll n^{k/2}.$$

However a conjecture of Ramanujan of 1916, later called the Ramanujan-Petersson conjecture in a more general context, asserts that under the same assumptions

$$a_f(n) \ll_\varepsilon n^{\frac{k-1}{2}+\varepsilon}.$$

This was proved by Deligne many years later, as a consequence of his work on the Weil conjectures, and has found fruitful applications since then. For instance, this bound plays a central role in the construction of Ramanujan graphs by Lubotzky, Phillips and Sarnak [80] (actually, they do not need the full generality of the Ramanujan-Petersson conjecture as proved by Deligne, and rather rely on earlier works of Eichler and Igusa). Such graphs give examples of *expander graphs*, which are graphs satisfying certain extremality properties (for instance it is related to the existence of a large spectral gap: a gap between the trivial eigenvalue and the other eigenvalues of the adjacency matrix of the graph). This type of estimates on Fourier coefficients of modular forms also appears in the proof that a certain graph is an expander in the article [33], which concerns a very concrete number theoretic question. Namely, they study the distribution of the tuples

$$\left\{ \frac{1}{\sqrt{d}}(x,y,z) \;\middle|\; (x,y,z) \in \mathbf{Z}^3 \text{ such that } x^2+y^2+z^2 = d \right\}$$

on the sphere $\mathbf{S}^2$ as d goes to infinity among the integers which can be represented as a sum of three squares, and $d \equiv \pm 1 \pmod 5$. Using a modern reformulation of an ergodic method of Linnik, they prove the equidistribution of these tuples, and the proof relies on the fact that a certain graph has a spectral gap. The condition $d \equiv \pm 1 \pmod 5$ is due to a technical limitation of this specific approach, and it can actually be removed. This was achieved by Duke in [30], by considerations on the Fourier

coefficients *half-integral weight* Maass forms, a generalization of the notion of modular forms which need not be holomorphic.
In the previous application, estimates of Kloosterman sums play a crucial role in the proof. This comes from the fact that they appear in many instances of *trace formulas*, such as Petersson's trace formula (for holomorphic cusp forms) or Kuznetsov's trace formula (for more general automorphic forms). We state here a simple form of Petersson's trace formula, which can be seen quasi orthogonality relation for Fourier coefficients of cusp forms.

Proposition 1.11 ([54, Proposition 14.5]). *Let $\mathcal{F}$ be an orthonormal*[1] *basis of the space of cusp forms of $\mathrm{SL}_2(\mathbf{Z})$ of weight k. Then for any $m, n \geqslant 1$,*

$$\frac{\Gamma(k-1)}{(4\pi\sqrt{mn})^{k-1}} \sum_{f\in\mathcal{F}} a_f(n)\overline{a_f(m)} = \delta_{m,n} + 2\pi i^{-k} \sum_{c>0} \frac{\mathrm{K}_c(m,n)}{c} J_{k-1}\left(\frac{4\pi\sqrt{mn}}{c}\right)$$

where $\delta_{m,n}$ is the Kronecker symbol, $\mathrm{K}_c(m,n)$ is the Kloosterman sum

$$\sum_{x\in(\mathbf{Z}/c\mathbf{Z})^\times} e\left(\frac{mx+nx^{-1}}{c}\right) \tag{1.9}$$

and J_{k-1} is a Bessel function.

The idea of the proof is to consider the expansion

$$P_m = \sum_{f\in\mathcal{F}} \langle f, P_m\rangle f,$$

where P_m is a specific cusp form called a Poincaré series, and to identify the n-th Fourier coefficients of both sides. We refer to [54, Chapter 14] for complete proofs. The reason why Kloosterman sums appear is because they appear in the Fourier coefficients of Poincaré series, and it is actually as such that they first made an apparition in the literature (see the article [72] by E. Kowalski).

Generalizations of Proposition 1.11 in the form of what is called Kuznetsov's trace formula are widely used in questions related to counting geodesics of length less than $\log(X)$ on arithmetic surfaces, typically on the modular surface $\mathrm{PSL}_2(\mathbf{Z})\backslash\mathbf{H}$. In this context as well, estimates on Kloosterman sums are important to control the size of the error term in an asymptotic formula (as the length of the geodesics tends to infinity) called the *prime geodesic theorem*. An illustration of that claim is the paper [4], which improves the error term obtained in earlier works by improving the estimates on sums of Kloosterman sums.

Finally, let us mention another very concrete number theoretic question which has been answered relying partially on estimates on Kloosterman sums: the equidistribution of roots of quadratic congruences modulo primes by Duke, Friedlander and Iwaniec [31]. More precisely, what it this statement about ? Fix a degree 2 irreducible polynomial $P(X) = aX^2+bX+c \in \mathbf{Z}[X]$. Then for any prime p which does not divide a, the reduction of $P(X)$ modulo p is a quadratic polynomial with coefficients in $\mathbf{F}_p$, so it has at most two roots in $\mathbf{F}_p$. We denote by $\rho(p)$ the number of roots of $P(X)$ in $\mathbf{F}_p$, and by

$$\rho(x) = \sum_{p\leqslant x} \rho(p).$$

For a root $\nu \in \mathbf{F}_p$ of $P(X)$, we denote by $\left\{\frac{\nu}{p}\right\}$ the fractional part of any rational number of the form $\frac{\tilde{\nu}}{p}$ where $\tilde{\nu}$ is an integer whose reduction modulo p equals ν. The equidistribution of the roots of $P(X)$ is the following statement:

[1] with respect to the Petersson inner product, see e.g. [54, eq. (14.11)]

Theorem 1.12 (Duke-Friedlander-Iwaniec). *for any interval* $[a,b] \subseteq [0,1]$,

$$\frac{1}{\rho(x)} \# \left\{ (p,\nu) \;\mid\; p \leqslant x,\ P(\nu) \equiv 0 \,(\mathrm{mod}\, p) \text{ and } a \leqslant \left\{ \frac{\nu}{p} \right\} \leqslant b \right\} \underset{x \to +\infty}{\longrightarrow} b - a.$$

Kowalski's book [70] gives a mostly self-contained exposition of the proof of this theorem, and its introduction already explains many important ideas. First, one needs to apply Weyl's criterion (we will discuss it in the next section on equidistribution) and this reduces the question to showing that certain exponential sums converge to zero. Next, a non-trivial step consists in relating these exponential sums to certain modular forms. Then one needs to prove that these modular forms have harmonic properties which guarantee the convergence towards zero of the Weyl sums. These harmonic properties essentially require us to study again the growth of some Fourier coefficients, and this part also makes use of Kuznetsov's trace formula, and of estimates on Kloosterman sums.

Remark 1.13. The analogous statement for roots of polynomial congruences modulo natural numbers (and not only primes) is actually easier, and was proved by Hooley in [51] for *irreducible* polynomials of arbitrary degree. On the other hand, the case of *reducible* polynomials is still not completely understood. In [82], Martin and Sitar studied the case of reducible quadratic polynomials, and quite recently Dartyge and Martin [24] obtained results for reducible polynomials of degree 3 as well as for polynomials which are a product of an arbitrary number of linear factors.

We hope that all those examples will convince the reader of the relevance of the study of exponential sums, as they keep on appearing in many places in number theory. In the next section, we give a brief overview of some facts in the theory of equidistribution, in a more general context than that of the interval $[0,1]$.

1.2. Equidistribution

1.2.1. Generalities

In this section we present the necessary definitions to speak about equidistribution in compact topological spaces, a setting which will be sufficiently general to state all the equidistribution results of this thesis. We have taken inspiration from the presentation of [73].

Given a compact topological space X, we denote by $\mathscr{B}(X)$ the σ-algebra of Borel sets, and we call *Borel probability measure* any measure μ on $(X, \mathscr{B}(X))$ such that $\mu(X) = 1$. In this setting, assume that we are also given a sequence $(Y_n)_{n \geqslant 1}$ of finite sets together with maps

$$\theta_n \colon Y_n \to X.$$

Definition 1.14. *We say that* $(Y_n, \theta_n)_{n \geqslant 1}$ *becomes equidistributed in* X *with respect to* μ *if for all continuous functions* $f \colon X \to \mathbf{C}$, *we have*

$$\frac{1}{|Y_n|} \sum_{y \in Y_n} f(\theta_n(y)) \underset{n \to +\infty}{\longrightarrow} \int_X f(x) \mathrm{d}\mu(x)$$

Equivalently, $(Y_n, \theta_n)_{n \geqslant 1}$ becomes equidistributed with respect to μ if and only if for any Borel set $A \subseteq X$ whose boundary ∂A satisfies $\mu(\partial A) = 0$, we have

$$\frac{|\{y \in Y_n \;\mid\; \theta_n(y) \in A\}|}{|Y_n|} \underset{n \to +\infty}{\longrightarrow} \mu(A).$$

Of course, these definitions can easily be ajusted to the case of sequences (Y_p, θ_p) indexed by prime numbers, or even $(Y_{\mathfrak{a}}, \theta_{\mathfrak{a}})$ indexed by ideals of the ring of integers of a number field K (in that case, the limit is taken as $\|\mathfrak{a}\|$ goes to infinity, where $\|\mathfrak{a}\|$ is the index of $\mathfrak{a}$ in $\mathcal{O}_K$). We will see an instance of that in Chapter 4.

Remark 1.15. Note that saying that the sequence $(Y_n, \theta_n)_{n\geqslant 1}$ becomes equidistributed in X with respect to μ is equivalent to saying that the sequence of "empirical" measures

$$\mu_n := \frac{1}{|Y_n|} \sum_{y\in Y_n} \delta_{\theta_n(y)}$$

converges weakly to μ. Yet another way of rephrasing this: if we view each finite set Y_n as a probability space with the normalized counting measure, then the maps θ_n are viewed as X-valued random variables, and we are saying that these random variables converge in law to a random variable whose law is μ.

Finally let us state an easy consequence of the definitions concerning pushforward measures which will be used in many places of the next chapters.

Lemma 1.16. *Let X and Y be two compact topological spaces, endowed with their respective Borel σ-algebras, and let $f\colon X \to Y$ be a continuous map. Let μ be a Borel probability measure on X.*
If $(A_n, \theta_n)_{n\geqslant 1}$ becomes equidistributed in X with respect to μ, then $(A_n, f\circ\theta_n)_{n\geqslant 1}$ becomes equidistributed in Y with respect to the pushforward measure $f_*\mu$.

Proof. Let $g\colon Y \to \mathbf{C}$ be a continuous map. We want to prove that

$$\frac{1}{|A_n|} \sum_{a\in A_n} g(f(\theta_n(a))) \underset{n\to+\infty}{\longrightarrow} \int_Y g(y)\mathrm{d}(f_*\mu)(y).$$

Since g is continuous, so is $g\circ f$, hence we can use the assumption that (A_n, θ_n) becomes equidistributed in X to deduce that the left hand side converges to

$$\int_X (g\circ f)\mathrm{d}\mu.$$

But this last integral equals $\int_Y g(y)\mathrm{d}(f_*\mu)(y)$ (by a standard argument: one first shows that it is true when g is the characteristic function of a Borel set by definition of $f_*\mu$, and then extends the results to any measurable functions by approximation by step functions). □

1.2.2. Equidistribution modulo 1 and Weyl's criterion

We now turn our attention to a particular case: the equidistribution in $[0,1[$ with respect to the Lebesgue measure, which is also called *equidistribution modulo* 1. It is historically the case considered by Weyl, in his famous article [107], where he introduced the criterion which bears his name, and has been generalized to more general settings since then.

A sequence $(x_n)_{n\geqslant 1}$ of real numbers is said to be *uniformly distributed modulo* 1 if its fractional parts $\{x_n\}$ become equidistributed in $[0,1[$ with respect to the Lebesgue probability measure: in other words, if for all subintervals $[a,b[\subseteq[0,1[$,

$$\frac{\#\{1\leqslant n\leqslant N,\ \{x_n\}\in[a,b[\}}{N} \underset{N\to+\infty}{\longrightarrow} b-a. \tag{1.10}$$

With the notations of the previous section, this corresponds to the case where $Y_N = \{1,\dots,N\}$ and

$$\begin{array}{rccc} \theta_N & : & Y_N & \to & [0,1[\\ & & n & \mapsto & \{x_n\} \end{array}$$

while (X,μ) is the interval $[0,1[$ endowed with its Lebesgue measure.

The following theorem is a well known criterion due to Weyl, which states that one can actually check uniform distribution modulo 1 only on a nice subset of the continuous functions on $[0,1]$: the set of trigonometric polynomials (which form a dense subset, with respect to the uniform norm, of the set of continuous and 1-periodic functions).

Theorem 1.17 (Weyl's criterion). *A sequence $(x_n)_{n\geqslant 1}$ is uniformly distributed modulo 1 if and only if for all $h \in \mathbf{Z} \setminus \{0\}$,*

$$\frac{1}{N}\sum_{n=1}^{N} e(h \cdot x_n) \underset{N\to\infty}{\longrightarrow} 0. \tag{1.11}$$

For a proof, see for instance [29, Theorem 1.19]. This criterion reduces the study of uniform distribution modulo 1 to the problem of estimating exponential sums.

A first easy application of this criterion is the uniform distribution modulo 1 of the sequence $(n\alpha)_{n\geqslant 1}$ for any given $\alpha \in \mathbf{R} \setminus \mathbf{Q}$. Here we want to stress that *without* Weyl's criterion, this "easy" application is not so easy!

An even more difficult application is the uniform distribution modulo 1 of the sequence $(p\alpha)_{p \text{ prime}}$ for α also irrational. This was proved by Vinogradov, and via Weyl's criterion, it is implied by the following estimate: if $\beta \in \mathbf{R} \setminus \mathbf{Q}$ then

$$\sum_{p\leqslant x} e(\beta p) \underset{x\to+\infty}{=} o\left(\frac{x}{\log(x)}\right).$$

We refer to [70, Prop. 5.5.1] for a proof.

Weyl's criterion admits generalizations to far more general settings, where equidistribution with respect to the Haar measure on a compact group can be proved using sums of characters of the group. We will come back to this in Appendix 4.A and use these more general versions at several places of this manuscript. However, the case of equidistribution modulo 1 still plays an important role in this thesis, as many of the groups we will be interested in are of the form $(\mathbf{R}/\mathbf{Z})^d$ for some integer d.

1.2.3. A quantitative result: Erdös-Turán inequality

Now, a natural question which comes to mind is to ask what kind of information on the distribution of the fractional parts $\{x_n\}$ can be deduced from estimates on the exponential sums which appear in Weyl's criterion? For instance, if we have a good understanding of the rate of convergence towards zero in (1.11), can we deduce an explicit rank N after which the ratio

$$\frac{\#\{1 \leqslant n \leqslant N,\ \{x_n\} \in [a,b[\}}{N}$$

is close to $b-a$, up to a well-understood error?
In other words, we would like to find a *quantitative* form of the uniform distribution modulo 1. We want to replace the qualitative convergence of (1.10) by an explicit upper bound for the gap

$$\left|\frac{\#\{1 \leqslant n \leqslant N,\ \{x_n\} \in [a,b[\}}{N} - (b-a)\right|$$

in terms of exponential sums, so that information on the distribution can be derived from quantitative estimates of the decay towards zero of the exponential sums involved in Weyl's criterion.

Erdös-Turán inequality enables one to achieve this goal, and can be stated as follows:

Theorem 1.18 (Erdös-Turán). *For any interval $I := [a,b[\subset \mathbf{R}$ such that $b-a \leqslant 1$ we denote by $\overline{I}$ its image in $[0,1[$ obtained by taking the fractional parts of the elements of I. Erdös-Turán inequality is the following result:*
there exist two absolute constants c_1 and c_2 such that for any sequence $(x_n)_{n\geqslant 1}$ of real numbers, for any interval $I := [a,b[\subset \mathbf{R}$ such that $b-a \leqslant 1$, for any $H > 0$:

$$\left|\frac{\#\left\{1 \leqslant n \leqslant N;\ \{x_n\} \in \overline{I}\right\}}{N} - (b-a)\right| \leqslant \frac{c_1}{H} + c_2 \sum_{0<|h|<H} \left(\frac{1}{|h|} - \frac{1}{H}\right) \left|\frac{1}{N}\sum_{n=1}^{N} e(h \cdot x_n)\right|.$$

Remark 1.19. The article [92] contains interesting results on the optimal constants c_1 and c_2 one can hope for, and gives explicit constants close to the expected optimal ones.

Remark 1.20. We recall that if μ is a Borel measure on $[0,1[$, we can define its Fourier coefficients as follows:

$$\forall h \in \mathbf{Z}, \quad \widehat{\mu}(h) := \int_0^1 e(-ht)\mathrm{d}\mu(t).$$

In the case of Theorem 1.18, if one considers the "empirical measure"

$$\mu_N := \frac{1}{N}\sum_{n=1}^{N} \delta_{\{x_n\}}$$

then its Fourier coefficients are $\widehat{\mu_N}(h) = \frac{1}{N}\sum_{n=1}^{N} e(h \cdot x_n)$ whereas the Fourier coefficients of the Lebesgue measure λ are all equal to zero, except $\widehat{\lambda}(0)$ which equals 1. Therefore, one can rewrite Erdös-Turán inequality as

$$\sup_{\substack{I=[a,b[\subset\mathbf{R}\\ b-a\leqslant 1}} |\mu_N\left(\overline{I}\right) - \lambda\left(\overline{I}\right)| \leqslant \frac{c_1}{H} + c_2 \sum_{0\leqslant|h|<H} \left(\frac{1}{|h|} - \frac{1}{H}\right)\left|\widehat{\mu_N}(h) - \widehat{\lambda}(h)\right|.$$

The supremum on the left hand side of this inequality is usually called the *discrepancy* of the sequence $(x_n)_{n\geqslant 1}$. Thus, Erdös-Turán inequality is a statement which controls the discrepancy between two measures by the difference between their Fourier coefficients. More general statements of this type are proved for instance in [88], where the analogy with Berry-Esseen inequality in probability theory is also pointed.

1.2.4. Sample of equidistribution results in number theory

Many "arithmetically defined" objects happen to show a random-like behaviour, in the sense that they become equidistributed in certain spaces. In this short section, we wish to give two classical examples (other than the exponential sums we will be focusing in the next section).

Primes in arithmetic progressions. The prime number theorem of Hadamard and de la Vallée Poussin states that the prime counting function $\pi(x) := |\{2 \leqslant p \leqslant x \mid p \text{ is prime}\}|$ is equivalent, as x goes to infinity, to

$$\mathrm{Li}(x) := \int_2^x \frac{1}{\log(t)}\mathrm{d}t$$

(which is itself equivalent to $x/\log(x)$). An analogous theorem gives the asymptotic for the number of prime numbers less than or equal to x, *in a certain arithmetic progression*. In other words, we fix an integer $q \geqslant 2$ and an invertible residue class $a \,(\mathrm{mod}\, q)$, and we are interested in

$$\pi(x; q, a) := |\{p \leqslant x \mid p \text{ is prime and } p \equiv a \,(\mathrm{mod}\, q)\}$$

The prime number theorem in arithmetic progressions states that

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

In other words, if one looks at the proportion of primes less than or equal to x which belong to an invertible residue class modulo q, then this proportion converges to $1/\varphi(q)$. For instance, for $q = 4$ we have $\varphi(q) = 2$, and the theorem tells us that the proportion of primes congruent to 1 modulo 4 and the proportion of primes congruent to 3 modulo 4 both converge to $1/2$.

Let us rephrase this theorem in the language of equidistribution. We let Y_x denote the set of prime numbers less than or equal to x and

$$\begin{array}{rccc} \theta_x & : & Y_x & \to & \mathbf{Z}/q\mathbf{Z} \\ & & p & \mapsto & p \,(\mathrm{mod}\, q) \end{array}$$

We endow $\mathbf{Z}/q\mathbf{Z}$ with the probability measure

$$\mu := \frac{1}{\varphi(q)} \sum_{a \in (\mathbf{Z}/q\mathbf{Z})^\times} \delta_a.$$

Then the prime number theorem in arithmetic progressions states that $(Y_x, \theta_x)_{x \geqslant 2}$ become equidistributed in $\mathbf{Z}/q\mathbf{Z}$ with respect to μ in the sense of Definition 1.14.

Sato-Tate law for elliptic curves. This paragraph owes a lot to the survey paper [100] by A. Sutherland. For background on elliptic curves, we refer to the famous book of Silverman [98] (see also the book of Cox [23]: even though its title does not mention elliptic curves, it is a great introduction to the subject!).
An elliptic curve over $\mathbf{Q}$ is a curve given by an equation of the form

$$E\colon y^2 = x^3 + ax + b$$

with $a, b \in \mathbf{Z}$. By introducing a third variable z, and turning the equation defining E into a homogeneous equation, we can view E as a projective curve in $\mathbf{P}^2(\mathbf{Q})$. Elliptic curves have been at the heart of development of the Langlands program, which consists in many conjectures and theorems concerning connections between elliptic curves, modular forms, and Galois representations. For instance, the modularity conjecture discussed in the book of Diamond and Shurman [27] is a key step in the proof of Fermat's last theorem by Andrew Wiles.

The Sato-Tate law for elliptic curves we wish to present in this paragraph concerns the distribution of the error term in the number of points on the reduction modulo p of E. However, we need to exclude some primes where the reduction modulo p is "bad". More precisely, there is a notion of *discriminant* of an elliptic curve, which is defined by the formula $\Delta = -16(4a^3 + 27b^2)$, and for any prime number p, we say that E *has good reduction at* p if p does not divide Δ. For such primes, we can reduce the equation defining E modulo p, and obtain an elliptic curve over the finite field $\mathbf{F}_p$, which we denote by E_p. The number of $\mathbf{F}_p$-points of E_p satisfies the bound

$$|\#E_p(\mathbf{F}_p) - (p+1)| \leqslant 2\sqrt{p}$$

(this is called the Hasse bound), so that if we denote by

$$t_p := p + 1 - \#E_p(\mathbf{F}_p)$$

the numbers $t_p/\sqrt{p}$ all belong to the interval $[-2, 2]$, and one may want to understand more precisely their distribution in this interval.
At this point, we need to one last definition in order to state the Sato-Tate theorem: the notion of curve with or without complex multiplication. Since defining the group law on an elliptic curve is far from the purpose of this introduction, we will just state as a fact that one can endow E with a group law, so that it makes sense to write $P + Q$ for two points P and Q of the elliptic curve. This turns E into an abelian group and in particular, for any positive integer n, we can define an endomorphism φ_n of the curve E which is given by the multiplication by n:

$$\varphi_n(P) = \underbrace{P + \cdots + P}_{n \text{ times}}.$$

If n is negative, we define $\varphi_n(P)$ as $-P - \cdots - P$ ($-n$ times). This shows that the ring of endomorphisms of E contains a subring isomorphic to $\mathbf{Z}$. However, it can happen that the curve admits other endomorphisms than those of the form φ_n. In that case, one can show that the $\mathrm{End}(E)$ is isomorphic to the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. We say that E is a curve *with complex multiplication*, or a CM elliptic curve. Otherwise, it is said to be non-CM, or *an elliptic curve without complex multiplication*. We can now sate the Sato-Tate conjecture, which is now a theorem, published in the years 2010-2011 by Barnet-Lamb, Clozel, Gee, Geraghty, Harris, Shepherd-Barron and Taylor (the precise articles are referenced in the survey [100]).

Theorem 1.21 (Sato-Tate law for non-CM elliptic curves). *Let E be an elliptic curve over $\mathbf{Q}$ without complex multiplication. For all prime numbers p, denote by*

$$t_p := p + 1 - \#E_p(\mathbf{F}_p).$$

Then for any closed interval $[a, b] \subseteq [-2, 2]$, we have

$$\frac{\#\left\{p \leqslant x \;\middle|\; \frac{t_p}{\sqrt{p}} \in [a,b]\right\}}{\pi(x)} \underset{x\to+\infty}{\longrightarrow} \int_a^b \frac{1}{2\pi}\sqrt{4-t^2}\mathrm{d}t.$$

In other words, if Y_x is again the set of prime numbers less than or equal to x and

$$\begin{array}{rccc} \theta_x & : & Y_x & \to & [-2,2] \\ & & p & \mapsto & \frac{t_p}{\sqrt{p}} \end{array}$$

then $(Y_x, \theta_x)_{x\geqslant 2}$ become equidistributed in $[-2, 2]$ with respect to the Sato-Tate measure:

$$\mathrm{d}\mu_{\mathrm{ST}}(t) = \frac{1}{2\pi}\sqrt{4-t^2}\mathrm{d}t. \tag{1.12}$$

This is another instance of an arithmetic quantity (an error term for the number of points on an elliptic curve over varying finite fields) which shows a random behaviour, and the "randomness" is well-understood since we know that the limit measure is the Sato-Tate measure.

1.3. Equidistribution of exponential sums

In the two previous sections, we first gave several applications of exponential sums to show that they are indeed arithmetic objects which appear in many parts of number theory, and then we gave examples of equidistribution results concerning arithmetic quantities. In this section, we want to combine both aspects, by showing that some exponential sums which arise naturally in number theory satisfy themselves equidistribution results.

1.3.1. Gauss sums with varying multiplicative character

If ψ is an additive character of $\mathbf{F}_p$ and χ a multiplicative character of $\mathbf{F}_p^\times$, the associated Gauss sum is defined as

$$\tau(\chi, \psi) := \sum_{x\in\mathbf{F}_p^\times} \chi(x)\psi(x).$$

These sums enjoy an equidistribution property, but only after a suitable normalization. Indeed, an elementary computation of $|\tau(\chi, \psi)|^2$ shows that as soon as ψ and χ are both non-trivial, we have

$$|\tau(\chi, \psi)| = \sqrt{p}$$

(a proof of this fact can be found in [58, §1.3]). Thus, if for all prime numbers p we fix a non-trivial additive character ψ_p of $\mathbf{F}_p$, then the set

$$\left\{\frac{1}{\sqrt{p}}\tau(\chi, \psi_p),\ \chi \text{ non-trivial character of } \mathbf{F}_p^\times\right\} \tag{1.13}$$

is a subset of the unit circle $\mathbf{S}^1$, and one may ask how its elements distribute on $\mathbf{S}^1$. Even though it only involves elementary objects, this question turns out to be very difficult. The answer is given by the following theorem, which is due to Deligne:

Theorem 1.22. *As p tends to infinity, the $p-2$ points of the set (1.13) become equidistributed on $\mathbf{S}^1$ with respect to the Haar measure on $\mathbf{S}^1$.*

The proof of this theorem starts with the application of Weyl's criterion, but then the exponential sums one needs to bound in order to show that there is convergence towards zero are hyper-Kloosterman sums, which are not so easy to bound. The conclusion follows from the work of Deligne, who proved the optimal upper bounds for the absolute value of these sums, relying on the construction of an ℓ-adic sheaf that admits hyper-Kloosterman sums as trace function. We refer to [58, §1.3] for more details on the proof of this equidistribution theorem.

1.3.2. Katz' theorem on Kloosterman sums

Let $q = p^\alpha$, where p is an odd prime and $\alpha \in \mathbf{Z}_{\geqslant 1}$. The classical Kloosterman sums modulo q are the real numbers $\mathrm{K}_q(a,b)$ already defined at equation (1.9). They first appeared in a paper of Poincaré, but they are named after Kloosterman because he was the first to prove a non-trivial upper bound for their absolute value, a result which was crucial in his work [66] on representation of large integers by diagonal quadratic forms in 4 variables, as we discussed on page 32.
Many years after Kloosterman's paper, as a consequence of Weil's work on the Riemann hypothesis for curves over finite fields, the best possible upper bound for the absolute value of these sums was obtained and takes the following form:

$$|\mathrm{K}_p(a,b)| \leqslant 2\sqrt{p} \quad \text{for all } a,b \in \mathbf{F}_p^\times.$$

This only covers the case of Kloosterman sums modulo prime numbers, and not prime powers, but more generally one can show that these sums satisfy the bound[2]:

$$|\mathrm{K}_q(a,b)| \leqslant 2\sqrt{q} \quad \text{for all } a,b \in (\mathbf{Z}/q\mathbf{Z})^\times \tag{1.14}$$

Note that it is a far more elementary problem in the case of prime powers than in the case of primes (see [64, Corollary 1] for an elementary proof of a slightly more general statement concerning *twisted* Kloosterman sums). The bound (1.14) raises the question of the distribution of the sets of sums

$$\left\{ \frac{1}{\sqrt{q}}\mathrm{K}_q(a,b);\ a,b \in (\mathbf{Z}/q\mathbf{Z})^\times \right\}$$

in the interval $[-2,2]$ as q goes to $+\infty$. When $q = p$ is a prime number, this question is very deep, and the answer was given by Katz in 1988, using techniques from ℓ-adic étale cohomology introduced and developed by Grothendieck and Deligne. We will come back to this algebraic point of view on exponential sums in Chapter 6, but for now let us just state the beautiful result obtained by Katz:

Theorem 1.23 ([59, Example 13.6]). *For any odd prime number p, denote by*

$$\mathrm{Kl}_2(a,p) := -\frac{1}{\sqrt{p}} \sum_{x \in \mathbf{F}_p^\times} e\left(\frac{ax + x^{-1}}{q}\right)$$

the normalized Kloosterman sums modulo p. As $p \to +\infty$ through primes, the sets of sums

$$\left\{ \mathrm{Kl}_2(a,p);\ a \in \mathbf{F}_p^\times \right\}$$

become equidistributed with respect to the Sato-Tate measure on $[-2,2]$ (defined at equation (1.12)).

Concretely: for any interval $[c,d]$ contained in $[-2,2]$ we have

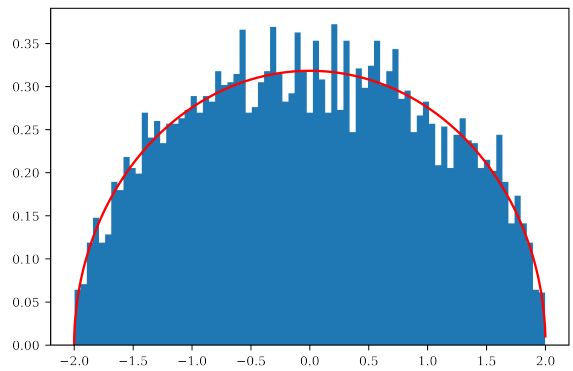
$$\frac{\#\left\{a \in \mathbf{F}_p^\times;\ \mathrm{Kl}_2(a,p) \in [c,d]\right\}}{p-1} \xrightarrow[p\to\infty]{} \int_c^d \frac{1}{2\pi}\sqrt{4-x^2}\mathrm{d}x,$$

On the other hand, in the case where $q = p^\alpha$ is a non-trivial prime power (i.e. $\alpha \geqslant 2$), one can prove via elementary methods an equidistribution result for the sets $\left\{\frac{1}{\sqrt{q}}\mathrm{K}_q(a,1);\ a \in (\mathbf{Z}/q\mathbf{Z})^\times\right\}$ as q goes to infinity, see [64, Remark 1.1]. In this case, the measure with respect to which the sums become equidistributed is the measure μ defined as follows:

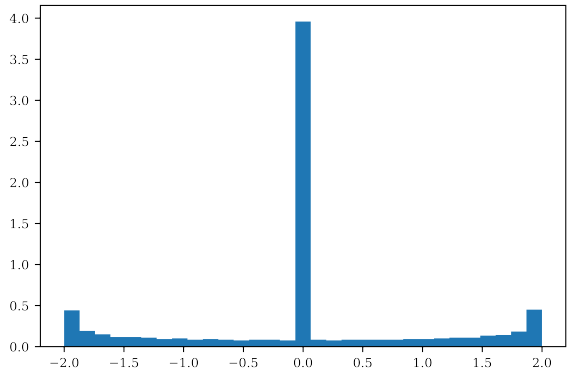
$$\mathrm{d}\mu(x) = \frac{1}{2}\delta_0(x) + \frac{1}{2\pi}\frac{1}{\sqrt{4-x^2}}\mathrm{d}x. \tag{1.15}$$

The following figure illustrates these two different behaviours.

[2] Here one really needs to assume that p is an odd prime. When $q = 2^\alpha$ with $\alpha \geqslant 5$, the upper bound (1.14) needs to be replaced by $|\mathrm{K}_q(a,b)| \leqslant (2\sqrt{2})\sqrt{q}$ (see the corrigendum [41] to the article [40]).



(a) Distribution of the values $\frac{1}{\sqrt{6007}}\mathrm{K}_{6007}(a,1)$ in $[-2,2]$ as a ranges in $\mathbf{F}_{6007}^{\times}$. The red curve is the graph of $x \mapsto \frac{1}{2\pi}\sqrt{4-x^2}$.



(b) Distribution of the values $\frac{1}{31}\mathrm{K}_{31^2}(a,1)$ in $[-2,2]$ as a ranges in $(\mathbf{Z}/31^2\mathbf{Z})^{\times}$.

Figure 1.1: Distribution of normalized Kloosterman sums modulo a prime and modulo a prime power.

Remark 1.24. (1) Since Katz' equidistribution theorem, finer results on the asymptotic behaviour of Kloosterman sums have been obtained, through the study of the asymptotic distribution of *Kloosterman paths*. A first achievement was made by Kowalski and Sawin, who studied in [76] the distribution of the polygonal paths connecting the successive partial sums of Kloosterman sums, and proved their convergence in the sense of finite distributions towards an explicit random Fourier series. Their article only focuses on Kloosterman sums modulo prime numbers, but shortly after, Ricotta and Royer [91] answered the analogous question for Kloosterman sums modulo prime powers p^n in the regime where $n \geqslant 2$ is a fixed integer and p goes to infinity. Finally, the regime where p is a fixed prime and the power n goes to infinity was settled by Milićević and Zhang in [83].

(2) A related question concerning *twisted* Kloosterman sums was investigated by Kelmer in [64]. Namely, he studied the distribution of sums of the form

$$\frac{1}{\sqrt{q}} \sum_{x \in (\mathbf{Z}/q\mathbf{Z})^{\times}} e\left(\frac{a(x-x^{-1})}{q}\right) \chi(x)$$

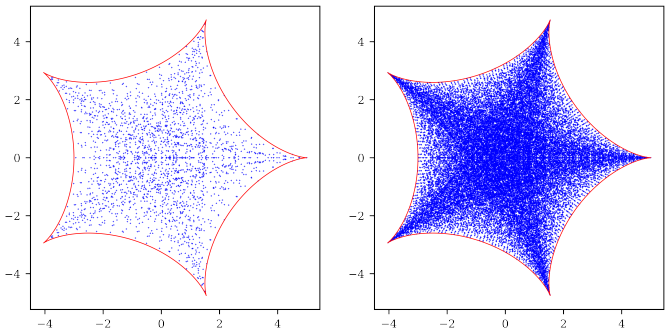
where χ varies among Dirichlet characters modulo q and a is a fixed non-zero integer. Here $q = p^k$ for a fixed integer $k \geqslant 2$ and a prime p going to infinity. He obtained that these sums become equidistributed in $[-2,2]$ with respect to the same measure μ as in (1.15).

Part B: Outline of the thesis

Initial motivation. The starting point of this thesis was the study of the article [16], which investigates certain visual properties of Kloosterman sums restricted to the subgroup of d-th roots of unity:

$$\mathrm{K}_p(a,b,d) := \sum_{\substack{x\in\mathbf{F}_p^\times \\ x^d=1}} e\left(\frac{ax+bx^{-1}}{p}\right),$$

for a fixed d and p tending to infinity, under the condition that $p \equiv 1 \pmod d$ (this condition ensures that the group of d-th roots of unity is indeed made of d elements in $\mathbf{F}_p$). Indeed, for a given large value of p and the parameters a and b varying in $\mathbf{F}_p$, one obtains the following pictures:



(a) $p = 151$ (b) $p = 631$

Figure 1.2: The sets $\{\mathrm{K}_p(a,b,d);\ a,b \in \mathbf{F}_p\}$ for $d = 5$ and two different values of $p \equiv 1 \pmod 5$.

In the arXiv version of the article [16], the authors show that there is indeed a density result for such sums. They prove that when d is prime, the sums $\mathrm{K}_p(a,b,d)$ become dense in the region of the complex plane delimited by a d-cusp hypocycloid. They also prove a density result for $d = 9$. The first question I tried to answer in my thesis was: *is it possible to prove that these sums actually become equidistributed with respect to some measure?*

It turns out that this question was quickly answered, because in the published version of *loc. cit.*, a remark states that the proof of the density actually shows that there is equidistribution with respect to an ad hoc pushforward measure. However, the fact that it was only proved for values of d which were prime or equal to 9 was surprising, as the exact same results were obtained for *any* value of d for the simpler sums:

$$\mathrm{S}_p(a,d) := \sum_{\substack{x\in\mathbf{F}_p \\ x^d=1}} e\left(\frac{ax}{p}\right)$$

in [32, 44]. I was rather striked by the fact that the sums $\mathrm{S}_p(a,d)$ and $\mathrm{K}_p(a,b,d)$ became equidistributed with respect to the same measure. Thus, I tried to understand what was the reason behind this, and which other sums satisfy the same equidistribution results. The key observation that explains the similarity of their asymptotic behaviour is that the exponents $+1$ and -1 which appear in "$ax+bx^{-1}$" in the definition of the Kloosterman sums are coprime with d, for any integer d.

In **Chapter 2** , we extend certain known equidistribution results from [32, 44] and [16], regarding sums of the type $\mathrm{S}_p(a,d)$ and $\mathrm{K}_p(a,b,d)$, to more general families of exponential sums, namely sums of the form

$$\sum_{\substack{x\in\mathbf{F}_p \\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{p}\right)$$

for arbitrary integers m_i and parameters a_i varying in $\mathbf{F}_p$. Here is a sample statement in the special case where the m_i are coprime with d:

Theorem 1.25 ([103, Proposition B (b)], Proposition 2.12 p.59 in this manuscript)**.** *Let $d \geqslant 1$ and let $m_1, \dots, m_n$ be integers all coprime with d. Then the sets of sums*

$$\left\{ \sum_{\substack{x \in \mathbf{F}_p \\ x^d = 1}} e\left(\frac{a_1 x^{m_1} + \cdots + a_n x^{m_n}}{p} \right) ; \ (a_1, \dots, a_n) \in (\mathbf{F}_p)^n \right\}$$

become equidistributed in the image of an explicit Laurent polynomial $g_d \colon (\mathbf{S}^1)^{\varphi(d)} \to \mathbf{C}$ (with respect to the pushforward measure via g_d of the probability Haar measure on $(\mathbf{S}^1)^{\varphi(d)}$) as p goes to infinity among the prime numbers congruent to 1 modulo d.

Let us stress that the Laurent polynomial g_d is the same as the one which appears in the description of the pushforward measure in the previous articles on the subject.

Example 1.26. If $d = \ell$ is a prime number, the Laurent polynomial g_ℓ is given by:

$$z_1 + \cdots + z_{\ell-1} + \frac{1}{z_1 \dots z_{\ell-1}}$$

and it maps $(\mathbf{S}^1)^{\ell-1}$ to the region of the complex plane delimited by a hypocycloid with ℓ cusps. For $\ell = 5$, Figure 2.5 p.58 illustrates Theorem 1.25 in the special case of Kloosterman sums restricted to the subgroup of order 5.

The strategy of the proof of Theorem 1.25 is the following:

- First, we pick a primitive d-th root of unity w_p in $\mathbf{F}_p$, write
$$\left\{ x \in \mathbf{F}_p \ \mid \ x^d = 1 \right\} = \left\{ w_p^k, \ 0 \leqslant k \leqslant d-1 \right\},$$
and rewrite the sums in terms of the w_p^k.
- Then, we take into account that there are linear relations with integral coefficients between the powers of w_p. Indeed, the fact that the d-th cyclotomic polynomial ϕ_d vanishes at w_p gives such a linear relation.
- This allows us to rewrite our exponential sums of interest as a Laurent polynomial in $\varphi(d)$ variables in $\mathbf{S}^1$ (where φ denotes the Euler totient function), which only depend on the w_p^k for $k < \varphi(d)$.
- Finally, it remains to prove the uniform distribution modulo 1 of a tuple in $(\mathbf{R}/\mathbf{Z})^{\varphi(d)}$ which only depends on those small powers of w_p. For instance, in the simplest case of the sums $\mathrm{S}_p(a, d)$, we need to prove the uniform distribution of
$$\left\{ \mathbf{x}_a(p) := \left(\frac{a w_p^0}{p}, \frac{a w_p^1}{p}, \dots, \frac{a w_p^{\varphi(d)-1}}{p} \right) ; \ a \in \mathbf{F}_p \right\} \subset (\mathbf{R}/\mathbf{Z})^{\varphi(d)}. \tag{1.16}$$
We do this using Weyl's criterion, and a striking feature of this problem is that the Weyl sums are actually stationary (equal to zero for a big enough range of summation)!

Remark 1.27. In the same chapter, we also extend Theorem 1.25 to sums over elements of $\mathbf{Z}/q\mathbf{Z}$, where q is a power of a prime congruent to 1 modulo d. This generalization involves Hensel's lemma to show that the vanishing of ϕ_d at a primitive d-th root of unity still holds (this is proved in Lemma 2.14). Finally, the statement also admits a generalization to the case where the integers m_i are not assumed to be coprime with d, as shown in [103, Proposition B (a)].
The most general form of Theorem 1.25, which gathers these different extensions, can be found at Proposition 2.20 p.68 of this manuscript.

After a talk I gave at a seminar in Nancy, G. Tenenbaum suggested that I look into discrepancy questions related to the equidistribution properties I am interested in. This is the subject of Appendix 2.B. As we already observed, the proof of Theorem 1.25 mostly relies on the uniform distribution modulo 1 of the sets of tuples (1.16), and there is a classical notion of discrepancy for such subsets of $(\mathbf{R}/\mathbf{Z})^{\varphi(d)}$, which measures how quickly a sequence becomes uniformly distributed modulo 1.

Definition 1.28. *For all $p \equiv 1 \pmod d$, we define the discrepancy of the finite subset of $(\mathbf{R}/\mathbf{Z})^{\varphi(d)}$ of eq. (1.16) as follows:*

$$D_p := \sup_{I \in \mathscr{I}} \left| \frac{1}{p} \sum_{a=0}^{p-1} \mathbb{1}_I(\mathbf{x}_a(p)) - \lambda_{\varphi(d)}(I) \right|$$

where $\mathscr{I}$ denotes the set of products of intervals $I = [a_1, b_1] \times \cdots \times [a_{\varphi(d)}, b_{\varphi(d)}]$ of $(\mathbf{R}/\mathbf{Z})^{\varphi(d)}$ and $\lambda_{\varphi(d)}$ denotes the probability Haar measure on $(\mathbf{R}/\mathbf{Z})^{\varphi(d)}$.

Using the Erdös-Turàn-Koksma inequality combined with arguments adapted from an unpublished note sent to me by I. Shparlinski, I obtained the following estimate:

Proposition 1.29 (Proposition 2.38 p.86 in this manuscript)**.** *For all $d \geqslant 1$, we have that for all $p \equiv 1 \pmod d$,*

$$D_p \ll_d p^{-\frac{1}{\varphi(d)}}.$$

The fact that the discrepancy decreases quite quickly is due to the very striking fact that the Weyl sums for the equidistribution of the sets (1.16) are *eventually equal to* 0, due to an orthogonality of characters which holds for p large enough.

As a second step, I have been interested in generalizations of Theorem 1.25 to sparser sets, by restricting the parameters a_i to range over "small" subgroups of $\mathbf{F}_p^\times$. This is the content of **Chapter 3**.
For multiplicative subgroups of $\mathbf{F}_p^\times$ whose cardinality grows faster than $\sqrt{p}$, a standard completion technique[3] combined with classical estimates on Gauss sums shows that Theorem 1.25 also holds if the parameters a_i vary in such subgroups (see Theorem 3.9 p.97 of this manuscript).

However, one may ask if the barrier $\sqrt{p}$ can be crossed: *is there still equidistribution if the parameters vary in multiplicative subgroups of cardinality smaller than $\sqrt{p}$?*
The answer is yes, and actually a sufficient condition is that the cardinality of the multiplicative subgroups is of size p^δ for some (arbitrarily small) $\delta > 0$. This refinement relies on strong bounds coming from additive combinatorics, and especially from the work of Bourgain, Chang, Glibichuk and Konyagin, see e.g. [13] and [11]. For Kloosterman sums for instance, Theorem 1.25 states that the sets

$$\{\mathrm{K}_p(a, b, d);\ (a, b) \in \mathbf{F}_p \times \mathbf{F}_p\}$$

become equidistributed in the image of g_d with respect to the suitable pushforward measure. The generalization provided by the results of Chapter 3 allows one to restrict the parameters a and b to range over very small subgroups of $\mathbf{F}_p^\times$ in the following sense:

Theorem 1.30 (special case of [103, Theorem A] and Theorem 3.13 p.105 of this manuscript)**.** *For all $p \equiv 1 \pmod d$, we fix subgroups $H_p^{(1)}$ and $H_p^{(2)}$ of $\mathbf{F}_p^\times$. Then, if there exists $\delta > 0$ such that for all p,*

$$|H_p^{(1)}||H_p^{(2)}| \geqslant p^\delta,$$

the sets

$$\{\mathrm{K}_p(a, b, d);\ (a, b) \in H_p^{(1)} \times H_p^{(2)}\}$$

become equidistributed in the image of g_d with respect to the same measure as in Theorem 1.25.

The key ingredient is the following theorem of Bourgain, building on previous works with Chang, Glibichuk and Konyagin:

[3] for instance, this approach is often used to prove the Pólya-Vinogradov inequality.

Theorem 1.31 ([11]). *For any $\delta > 0$, there exists a constant $\varepsilon(\delta) > 0$ such that for any integer $q \geqslant 2$ and for any subgroup H of $(\mathbf{Z}/q\mathbf{Z})^\times$ such that $|H| \geqslant q^\delta$,*

$$\max_{a\in(\mathbf{Z}/q\mathbf{Z})^\times} \left|\sum_{x\in H} e\left(\frac{ax}{q}\right)\right| \ll \frac{|H|}{q^{\varepsilon(\delta)}}.$$

This type of estimate is strongly related to sum-product theorems in additive combinatorics. More precisely, it is related to the question of the existence of *approximate subrings*, i.e. subsets $A \subseteq (\mathbf{Z}/q\mathbf{Z})^\times$ such that $|A + A|$ and $|A \cdot A|$ are not much larger than $|A|$.

In an appendix to Chapter 3, we also study the question of the optimality of the growth condition $|H| \geqslant q^\delta$ in the above theorem. We give a more detailed exposition of an argument found in lecture notes by Konyagin, which explains that if H is a subgroup of $\mathbf{F}_p^\times$ such that $|H| \ll \log(p)$ then it cannot satisfy

$$\max_{a\in\mathbf{F}_p^\times} \left|\sum_{x\in H} e\left(\frac{ax}{p}\right)\right| = o(|H|).$$

This does not give a complete answer because there is still a gap between the regimes $\log(p)$ and p^δ, but it explains that it is not sufficient to only ask that $|H|$ grows with p, one really needs some assumption on the rate of growth.

Let us summarize what we did so far: starting from known equidistribution results for the exponential sums

$$\sum_{\substack{x\in\mathbf{F}_p\\ x^d=1}} e\left(\frac{ax}{p}\right) \quad \text{and} \quad \sum_{\substack{x\in\mathbf{F}_p\\ x^d=1}} e\left(\frac{ax+bx^{-1}}{p}\right),$$

we first extended them by allowing more general Laurent polynomials inside the exponentials, namely Laurent polynomials $a_1x^{m_1} + \cdots + a_nx^{m_n}$ for arbitrary integers m_i. This generalizes the cases of ax and $ax + bx^{-1}$. Then, we also studied the question of restricting the parameters a_i to range over small multiplicative subgroups, getting equidistribution results for sparser sets of sums. Another aspect which has not been mentioned yet is changing the condition $x^d = 1$ by another restriction. One could think of two natural generalizations:

- We could allow d to vary with p. However, it seems like our techniques do not allow us to handle this case easily. Indeed, the dimension of the torus in which the tuple (1.16) lives would vary with p, which makes less clear how to apply Weyl's criterion in a fixed compact group.
- We could view the condition $x^d = 1$ as a special case of the condition $g(x) = 0$ for some polynomial $g \in \mathbf{Z}[X]$, and try to generalize our results to this setting. Here also, it seems like our techniques are not well-suited to handle such a generalization. Indeed, as we see from the strategy of the proof of Theorem 1.25, we rely a lot on the choice of a primitive root of unity, and on the fact that all the roots of the polynomial $X^d - 1$ can be expressed as powers of this primitive root.

However, after I sent the preprint [103] to E. Kowalski, he answered with an idea of a better setting to handle this second generalization, and this led to the joint work [77], which we present in chapters 4 and 6.

In **Chapter 4**, we explain how the previous results can be extended to the case of exponential sums of the form

$$\sum_{\substack{x\in\mathbf{F}_q\\ g(x)\equiv 0 \,(\mathrm{mod}\, q)}} e\left(\frac{ax}{q}\right), \tag{1.17}$$

or more generally

$$\sum_{\substack{x\in\mathbf{F}_q\\ g(x)\equiv 0 \,(\mathrm{mod}\, q)}} e\left(\frac{a_1x^{m_1} + \cdots + a_nx^{m_n}}{q}\right),$$

for any fixed monic polynomial $g \in \mathbf{Z}[X]$, and prime numbers q tending to infinity under certain conditions (of the same nature as the assumption $p \equiv 1 \pmod d$ in the case of $g = X^d - 1$). We also handle the natural continuation of the problem to sums modulo prime powers.

Let us denote by $\mathrm{Z}_g(\mathbf{F}_q)$ the set $\{x \in \mathbf{F}_q \mid g(x) \equiv 0 \pmod p\}$. To study the distribution of the sums (1.17), a first idea that may come to mind is to introduce the map

$$a \in \mathbf{F}_q \mapsto \left(e\left(\frac{ax}{q}\right)\right)_{x \in \mathrm{Z}_g(\mathbf{F}_q)}$$

which we view as a random variable defined on the probability space $\mathbf{F}_q$ (endowed with the normalized counting measure), with values in $\mathrm{C}(\mathrm{Z}_g(\mathbf{F}_q), \mathbf{S}^1)$ (the set of functions from $\mathrm{Z}_g(\mathbf{F}_q)$ to $\mathbf{S}^1$). Indeed, if for instance we are able to show that this random variable behaves like a tuple of independent and uniformly distributed random variables in $\mathbf{S}^1$, then the sum of its values, which is the sum of interest for us, will behave like a sum $X_1 + \cdots + X_{\deg g}$ of such random variables. This is a natural analogue of the study of the tuple (1.16) for the sums over the roots of $X^d - 1$, except that we overcame the issue of ordering the roots by introducing the "unordered" version of $\mathbf{S}^1 \times \cdots \times \mathbf{S}^1$ given by $\mathrm{C}(\mathrm{Z}_g(\mathbf{F}_q), \mathbf{S}^1)$.

However, we cannot easily apply Weyl's criterion in a fixed compact group, as the space $\mathrm{C}(\mathrm{Z}_g(\mathbf{F}_q), \mathbf{S}^1)$ depends on q. This is where a small change of point of view will help us: we will work with prime ideals of the splitting field of g rather than prime numbers.
Let us introduce some notations. We let Z_g be the set of complex roots of g and more generally we denote by $\mathrm{Z}_g(K)$ the set of roots of g in a given field K. Since our results only depend on Z_g, we assume without loss of generality that g is separable. We also denote by $K_g := \mathbf{Q}(\mathrm{Z}_g)$ the splitting field of g and by $\mathbf{O}_g$ its ring of integers. Now for any prime ideal $\mathfrak{p} \subset \mathbf{O}_g$ (lying above q, say) we have the canonical projection $\varpi_\mathfrak{p} \colon \mathbf{O}_g \to \mathbf{O}_g/\mathfrak{p}$, which allows us to map the set of roots of g in $\mathbf{C}$ to the set of roots of g in certain finite fields. Assuming that $\mathfrak{p}$ does not divide the discriminant of g and is of residual degree 1 (which essentially means that q splits completely in K_g) we show that this gives a bijection between Z_g and $\mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})$, so that the study of our sums (1.17) can be reduced to the study of the random variables

$$\begin{array}{rccc} U_\mathfrak{p} & : & \mathbf{O}_g/\mathfrak{p} & \to & \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1) \\ & & a & \mapsto & U_\mathfrak{p}(a) \end{array}$$

where

$$\begin{array}{rccc} U_\mathfrak{p}(a) & : & \mathrm{Z}_g & \to & \mathbf{S}^1 \\ & & x & \mapsto & e\left(\frac{a\varpi_\mathfrak{p}(x)}{q}\right) \end{array}$$

and we identified $\mathbf{O}_g/\mathfrak{p}$ with $\mathbf{F}_q$ since $\mathfrak{p}$ lies over q and has residual degree 1 (we will not make this abuse of notation in Chapter 4, and check carefully that we can indeed deduce results for sums of $\mathrm{Z}_g(\mathbf{F}_q)$ from results for sums over the roots of g in $\mathbf{O}_g/\mathfrak{p}$). These random variables do not necessarily converge in law towards a uniformly distributed random variables on $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$, but we prove the following:

Theorem 1.32 ([77, Prop. 2.2] or Theorem 4.30 p.128 of this manuscript)**.** *If we denote by* R_g *the submodule of* $\mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$ *of additive relations between the roots of* g*:*

$$\mathrm{R}_g := \left\{ \alpha \colon \mathrm{Z}_g \to \mathbf{Z},\ \sum_{x \in \mathrm{Z}_g} \alpha(x) x = 0 \right\};$$

and by H_g *the subgroup of* $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ *which is "dual" to* R_g *in the following sense:*

$$\mathrm{H}_g := \left\{ f \in \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1),\ \forall \alpha \in \mathrm{R}_g,\ \prod_{x \in \mathrm{Z}_g} f(x)^{\alpha(x)} = 1 \right\};$$

then the random variables $U_\mathfrak{p}$ *converge in law, as the norm of the ideal* $\mathfrak{p}$ *goes to infinity, to a random variable* U *which is uniformly distributed on* H_g*.*

As a corollary, we obtain the equidistribution of the sums (1.17) with respect to the suitable pushforward measure:

Corollary 1.33 (A more general form allowing prime powers is stated at Corollary 4.40 (2), p.132 of this manuscript)**.** *For q prime totally split in K_g, the sums*

$$\sum_{\substack{x\in\mathbf{F}_q\\ g(x)\equiv 0\,(\mathrm{mod}\,q)}} e\Big(\frac{ax}{q}\Big),$$

parametrized by $a\in\mathbf{F}_q$, become equidistributed in $\mathbf{C}$ as $q\to+\infty$ with limiting measure μ_g given by the law of $\sigma(U)$, where U is uniformly distributed on H_g and $\sigma\colon \mathrm{C}(\mathrm{Z}_g,\mathbf{C})\to\mathbf{C}$ is the linear form defined by

$$f\mapsto\sum_{x\in\mathrm{Z}_g} f(x).$$

The restriction to primes that split completely in K_g was actually already present in the case of sums over the roots of X^d-1 considered in Chapter 2, since a well known result states that a prime q is totally split in the cyclotomic field $\mathbf{Q}(\zeta_d)$ if and only if $q\equiv 1\,(\mathrm{mod}\,d)$.

Since the above theorem tells us that the measure with respect to which exponentials sums over roots of g become equidistributed is connected to the group of additive relations between its complex roots, we present some examples of explicit determination of that group. For instance, when $\mathrm{Gal}\,(K_g/\mathbf{Q})$ is the full symmetric group, the $\mathbf{Z}$-module of additive relations can only be $\{0\}$ or of rank 1, generated by the constant function equal to 1 (in which case we can read it on the coefficient of $X^{\deg(g)-1}$ of the polynomial, since this corresponds to the sum of the roots being zero). We reproduce a known proof of this fact based on the representation theoretic approach introduced by Girstmair in Proposition 4.50 p.139.
We also present a proof of the fact that the module of additive relations of the Hilbert class polynomial is $\{0\}$ for any negative discriminant not equal to -3. This can be interpreted as the non-existence of non-trivial $\mathbf{Q}$-linear relations between the j-invariants of elliptic curves with CM by the same given imaginary quadratic order. The main result is proved in Proposition 4.56 p.144 of this manuscript, which handles all discriminants less than or equal to -9. Then, the remaining discriminants are easily handled since they correspond to order with class number one. The key ideas of this proof should be attributed to Emanuele Tron, with whom I discussed this question, I only checked the details and looked for explicit bounds for the class number in the literature.

In **Chapter 5**, which is not included in [77], we go back to the study of the discrepancy related to our equidistribution results, in the more general setting of Chapter 4.
In Theorem 1.32, we have seen that our random variables $U_{\mathfrak{p}}$ converge in law to a random variable which is uniformly distributed on the closed subgroup H_g of $\mathrm{C}(\mathrm{Z}_g,\mathbf{S}^1)\simeq(\mathbf{S}^1)^{\deg g}$. Therefore, we are looking for a suitable notion of discrepancy for sequences with values in such closed subgroups. In order to do this, we use a classification theorem for closed subgroups of a torus, which tell us that there exists an isomorphism of topologival groups

$$\varphi\colon \mathrm{H}_g\to(\mathbf{R}/\mathbf{Z})^d\oplus F$$

where F is a finite abelian group. Now, on the right-hand side, there is a natural notion of discrepancy, defined by taking the supremum over rectangles of $(\mathbf{R}/\mathbf{Z})^d$ and over singletons of F:

Definition 1.34. *If $z=(z_n)_{n\geqslant 1}$ is a sequence of elements of $(\mathbf{R}/\mathbf{Z})^d\oplus F$, we define its discrepancy as*

$$D_N(z):=\sup_{\substack{I\in\mathscr{I}_d\\ y\in F}}\left|\frac{\#\left\{1\leqslant n\leqslant N,\ z_n\in I\times\{y\}\right\}}{N}-\frac{\lambda_d(I)}{|F|}\right|$$

where $\mathscr{I}_d$ denotes the set of rectangles $I=[a_1,b_1]\times\cdots\times[a_d,b_d]$ of $(\mathbf{R}/\mathbf{Z})^d$.

Via the isomorphism φ, we can thus define a natural notion of φ-discrepancy of a sequence $(x_n)_{n\geqslant 1}$ with values in H_g (just by defininining it as the natural discrepancy of the sequence $(\varphi(x_n))_{n\geqslant 1}$). Then by extending the Erdös-Turán-Koksma inequality to the case of a group of the form $(\mathbf{R}/\mathbf{Z})^d \oplus F$, we can deduce an upper bound for the φ-discrepancy associated with the equidistribution of the random variables $U_{\mathfrak{p}}$. We obtain that its decay is upper bounded by

$$\|\mathfrak{p}\|^{-\frac{1}{[K_g:\mathbf{Q}]}}$$

where $\|\mathfrak{p}\|$ denotes the norm of the ideal $\mathfrak{p}$. The precise statement is given by Theorem 5.30 p.172 of this manuscript. Note that this upper bound matches the one obtained in Appendix 2.B in the case of $g = X^d - 1$ (because in that case $[K_g : \mathbf{Q}] = \varphi(d)$).

Finally, in **Chapter 6**, we go back to the exposition of the results of the joint work [77] with E. Kowalski. We show that the equidistribution result stated in Corollary 1.33, concerning sums of additive characters over the roots of g in $\mathbf{F}_q$, can be extended to more general *trace functions* over $\mathbf{F}_q$.

To give some motivation for these generalizations, we first show that sums of multiplicative characters also enjoy similar equidistribution properties as sums of additive characters. In that case, the relevant object which governs the limit measure is the module of multiplicative relations among the roots of g, i.e. relations of the form

$$\prod_{x\in \mathrm{Z}_g} x^{\beta(x)} = 1,$$

where the powers $\beta(x)$ are integers.

Next, once we have these two examples of equidistribution results for sums of *functions of algebraic nature* over $\mathrm{Z}_g(\mathbf{F}_q)$, we try to extend them to trace functions, which are a wide class of functions $\mathbf{F}_q \to \mathbf{C}$ having an algebraic origin. They were originally studied by Grothendieck and later by Deligne from the point of view of ℓ-adic cohomology. However, they admit a more concrete interpretation as traces of some representations, so that the only prerequisite to understand how to apply the work of Deligne in concrete situations (at least the ones we faced) is some familiarity with the language of representations. We also rely a lot on difficult results previously established by Katz and Fouvry, Kowalski and Michel (especially the determination of the monodromy groups of sheaves which are useful in applications), but these can be used directly without the need to fully understand the proofs, and this is what we will do.

Let us give a more precise description of the type of results that we obtain. For a fixed monic polynomial $g \in \mathbf{Z}[X]$, we assume that for all prime ideals $\mathfrak{p} \subset \mathbf{O}_g$ unramified of and of residual degree 1, we are given a middle-extension sheaf $\mathcal{F}_{\mathfrak{p}}$ on the affine line over the finite field $\mathbf{O}_g/\mathfrak{p}$, with associated trace function $t_{\mathfrak{p}}$. Then we are interested in the asymptotic distribution of the following families of sums of trace functions:

$$\left\{ \sum_{x\in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} t_{\mathfrak{p}}(a+x);\ a \in \mathbf{O}_g/\mathfrak{p} \right\}$$

or

$$\left\{ \sum_{x\in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} t_{\mathfrak{p}}(ax);\ a \in \mathbf{O}_g/\mathfrak{p} \right\}$$

and under some conditions on the sheaf $\mathcal{F}_{\mathfrak{p}}$, we obtain equidistribution results as the norm of the ideal $\mathfrak{p}$ goes to infinity. More precisely, we ask that the sheaves are *bountiful* in the sense of Fouvry, Kowalski and Michel [38]. The most general result of this chapter can be found in Theorem 6.27.
Since Kloosterman sums are trace functions associated with bountiful sheaves, we obtain the following concrete corollary (adding a little extra step to identify the finite field $\mathbf{O}_g/\mathfrak{p}$ with $\mathbf{F}_q$).

Theorem 1.35 ([77, Th. 1.1 (2)], or Corollary 6.31 p.191 of this manuscript)**.** *Let $g \in \mathbf{Z}[X]$ be a monic polynomial of degree $d \geqslant 1$. Assume that $0 \notin \mathrm{Z}_g$. Recall the definition of the normalized Kloosterman sum modulo a prime number q:*

$$\mathrm{Kl}_2(a,q) := \frac{1}{\sqrt{q}} \sum_{x \in \mathbf{F}_q^\times} e\left(\frac{ax + x^{-1}}{q}\right).$$

Then, as $q \to +\infty$ among prime numbers unramified and totally split in K_g, the sums

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_2(ax,q)$$

parameterized by $a \in \mathbf{F}_q$ become equidistributed in $\mathbf{C}$ with respect to the measure which is the law of the sum of d independent Sato–Tate random variables.

By taking $g = X - 1$, we see that we recover Katz' equidistribution theorem (Theorem 1.23 in this introduction). However, I would say the main input in our proof is still the determination of the monodromy group of the Kloosterman sheaf by Katz, so even though our statement is more general, the most difficult part is due to Katz. We also rely on the study in sums of products [38] by Fouvry, Kowalski and Michel, where they determined precise conditions under which shifts of Kloosterman sheaves are "independent".

We conclude the manuscript with some research perspectives related to the questions addressed in this thesis. For instance, the study of the optimality of the growth condition in Bourgain's estimate, the explicit determination of the additive or multiplicative relations between the roots of polynomials, and finally the analogous horizontal equidistribution results one could want to prove.

Chapter 2

Equidistribution of exponential sums indexed by a subgroup of fixed cardinality

In this chapter, we present the path which led to Proposition B in the article [103]. This proposition is an equidistribution result for families of exponential sums of the form

$$\sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times\\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right)$$

parametrized by $a_1,\dots,a_n\in\mathbf{Z}/q\mathbf{Z}$, which extends previous results of Duke, Garcia, Hyde and Lutz on sums of the form

$$\sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times\\ x^d=1}} e\left(\frac{ax}{q}\right)$$

and of Burkhardt, Chan, Currier, Garcia, Luca and Suh on

$$\sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times\\ x^d=1}} e\left(\frac{ax+bx^{-1}}{q}\right).$$

The Jupyter Notebook that was written to obtain most of the pictures of this chapter is available in html format at the URL: `http://perso.eleves.ens-rennes.fr/people/theo.untrau/sumssubgroups`

The pictures were made with the open-source software `sagemath`: [102].

Contents

2.1. Presentation of the problem

The equidistribution results stated in the introduction can be seen as a special case of the following question: for any prime power $q := p^\alpha$, we are given a set $\mathcal{F}_q$ of Laurent polynomials with coefficients in $\mathbf{Z}/q\mathbf{Z}$, and we want to study how the sets of sums

$$\left\{ \sum_{x \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{f(x)}{q}\right);\ f \in \mathcal{F}_q \right\} \tag{2.1}$$

become distributed as p goes to infinity, or as α goes to infinity, or both at the same time. Theorem 1.23 for instance, corresponds (up to the normalization factor) to the case where $\alpha = 1$ and $\mathcal{F}_p = \left\{aX + X^{-1}, a \in \mathbf{F}_p^\times\right\}$. More generally, one may ask about the distribution of the sets of "restricted" sums

$$\left\{ \sum_{x \in A_q} e\left(\frac{f(x)}{q}\right);\ f \in \mathcal{F}_q \right\} \tag{2.2}$$

where the summation is restricted to some subsets A_q of $\mathbf{Z}/q\mathbf{Z}$. For example, one can fix an integer d and take $A_q := \left\{x \in \mathbf{Z}/q\mathbf{Z};\ x^d = 1\right\}$: the set of d-th roots of unity modulo q. In that case, it is natural to impose a condition on p to ensure that the subgroup of d-th roots of unity is non-trivial. Namely, we will only consider values of p which are odd and congruent to 1 modulo d, so that $\left\{x \in \mathbf{Z}/p^\alpha\mathbf{Z};\ x^d = 1\right\}$ is the unique subgroup of order d of the cyclic group $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$.

Definition 2.1. *An integer q will be called d-admissible if it is of the form p^α for some odd prime number p congruent to 1 modulo d, and some integer $\alpha \geqslant 1$. We denote by $\mathcal{A}_d$ the set of d-admissible integers.*

Moreover, we will need the following notation to describe the sets of Laurent polynomials to be considered in this chapter.

Definition 2.2.

- *Given $\mathbf{m} = (m_1, \dots, m_n) \in \mathbf{Z}^n$ and $q \geqslant 1$, we denote by $\mathcal{F}_{\mathbf{m},q}$ the following set of Laurent polynomials with coefficients in $\mathbf{Z}/q\mathbf{Z}$:*

$$\mathcal{F}_{\mathbf{m},q} := \{a_1 X^{m_1} + a_2 X^{m_2} + \cdots + a_n X^{m_n};\ (a_1, \dots, a_n) \in (\mathbf{Z}/q\mathbf{Z})^n\}$$

- *Given an integer $d \geqslant 1$ we say that a vector $\mathbf{m} = (m_1, \dots, m_n) \in \mathbf{Z}^n$ is coprime with d if all the m_i are coprime with d.*

We now have all the notations needed to introduce the question of interest in this chapter: we will discuss equidistribution results for the families of exponential sums

$$\left\{ \sum_{\substack{x \in (\mathbf{Z}/q\mathbf{Z})^\times \\ x^d = 1}} e\left(\frac{a_1 x^{m_1} + \cdots + a_n x^{m_n}}{q}\right);\ (a_1, \dots, a_n) \in (\mathbf{Z}/q\mathbf{Z})^n \right\} \tag{2.3}$$

as q goes to infinity among the d-admissible integers. In other words, these are sets of exponential sums of the form (2.2) with $\mathcal{F}_q$ equal to $\mathcal{F}_{\mathbf{m},q}$ for some $\mathbf{m} \in \mathbf{Z}^n$ and the subset A_q being the subset of d-th roots of unity.

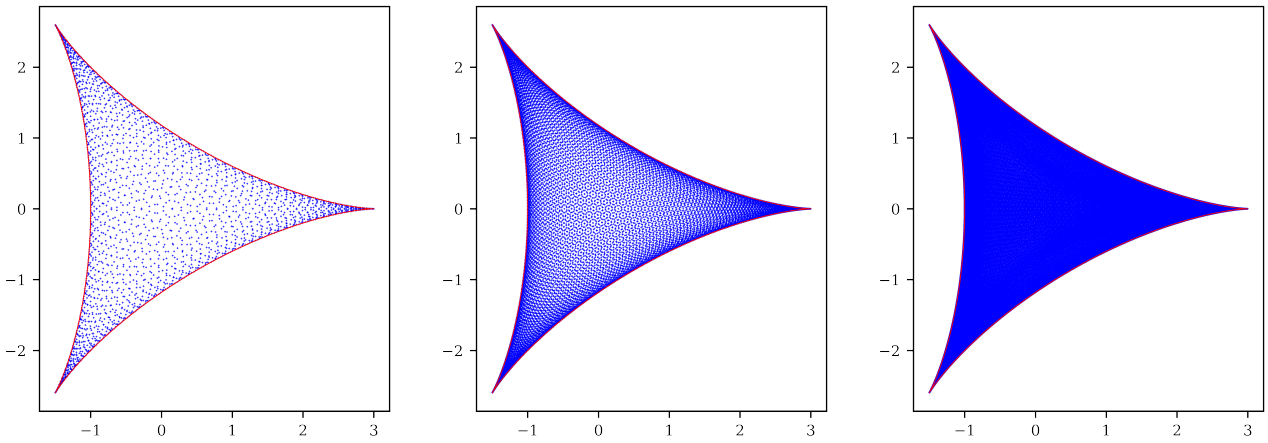
2.2. Relation to previous works

The study of this type of questions is motivated by the equidistribution results already known for complete sums, such as the one presented in section 1.3.2, as well as the appealing pictures shown in

the articles [16, 32] and [44]. In the last two, the authors fix an integer d and introduce the "restricted" geometric sums:

$$\mathrm{S}_q(a,d) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax}{q}\right) \tag{2.4}$$

Then, the equidistribution of the sets $\mathcal{S}_q(-,d) := \{\mathrm{S}_q(a,d);\ a\in\mathbf{Z}/q\mathbf{Z}\}$ as q tends to infinity is investigated. Let us remark that this is indeed a special case of the more general sums (2.3) we would like to study. These sets of sums have striking visual features, as shown in the following pictures. The pictures below correspond to the choice of three increasing d-admissible values of q, and for each fixed q, the blue points are all the complex numbers $\mathrm{S}_q(a,d)$ as a varies in $\mathbf{Z}/q\mathbf{Z}$.



(a) $q = 7759$ (b) $q = 51361$ (c) $q = 326041 = 571^2$

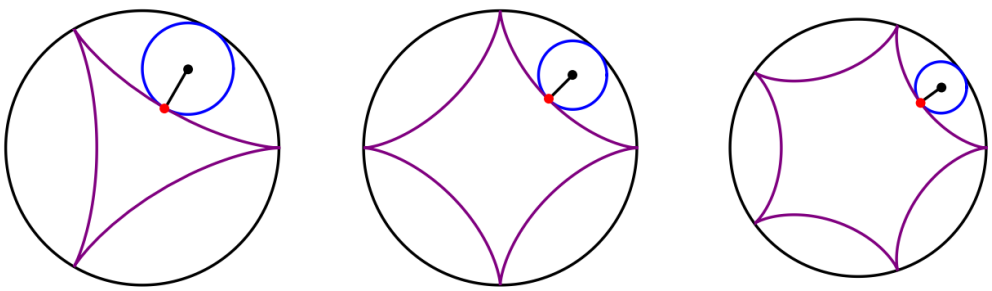
Figure 2.1: The sets $\mathcal{S}_q(-,d)$ for $d = 3$ and three 3-admissible values of q.

It seems that the sets $\mathcal{S}_q(-,3)$ become dense in a shape whose boundary is given by what is called a 3-*cusp hypocycloid*.

Definition 2.3. *The d-cusp hypocycloid is the curve given by the image of:*

$$\begin{array}{ccc} \mathbf{R} & \mapsto & \mathbf{C} \\ \theta & \mapsto & (d-1)\exp(i\theta) + \exp((1-d)i\theta) \end{array}$$

It is a curve described by a point of a circle of radius 1 *rolling inside a circle of radius d.*



(a) $d = 3$
a deltoid

(b) $d = 4$
an astroid

(c) $d = 5$

Figure 2.2: Some hypocycloids (image extracted from the article [16])

Definition 2.4. *For all* $d \geqslant 2$*, we denote by* $\mathbb{H}_d$ *the compact region of the complex plane of boundary the d-cusp hypocycloid.*

Note that the 2-cusp hypocycloid is just the interval $[-2,2]$, so it does not really enclose an area of the complex plane. Thus $\mathbb{H}_2$ is simply the interval $[-2,2]$ as well.

In [32, Theorem 6.3 and proof of Theorem 1.1] and [44, Theorem 1 and Proposition 1], the density statement suggested by Figure 2.1 is proved for any prime d, and their proof actually shows a more precise fact: there is equidistribution with respect to a suitable pushforward measure. Precisely, their proof shows the following equidistribution result.

Theorem 2.5 (Duke, Garcia, Hyde, Lutz, 2015)**.** *Let d be a prime number. Then the sets of sums $\{\mathrm{S}_q(a,d);\ a\in\mathbf{Z}/q\mathbf{Z}\}$ become equidistributed in $\mathbb{H}_d$ with respect to the pushforward measure of the probability Haar measure on $(\mathbf{S}^1)^{d-1}$ via the map*

$$g_d\colon (z_1,\dots,z_{d-1})\mapsto z_1+\cdots+z_{d-1}+\frac{1}{z_1\cdots z_{d-1}}$$

as q goes to infinity among the d-admissible integers.

This theorem extends to composite values of d, although the region of equidistribution cannot always be determined as explicitly. In order to state the more general result proved in [32, 44], we need one last definition.

Definition 2.6. *Let $d\geqslant 1$. For all $k\in\{0,\dots,d-1\}$, we denote by $(c_{j,k})_{0\leqslant j<\varphi(d)}$ the coefficients of the remainder in the euclidean division of X^k by ϕ_d, the d^{th} cyclotomic polynomial over $\mathbf{Q}$; precisely, these coefficients are defined by the property*

$$X^k\equiv\sum_{j=0}^{\varphi(d)-1}c_{j,k}X^j \bmod \phi_d.$$

Then, we define the Laurent polynomial

$$\begin{array}{rccc} g_d & : & (\mathbf{S}^1)^{\varphi(d)} & \to & \mathbf{C} \\ & & (z_1,\dots,z_{\varphi(d)}) & \mapsto & \displaystyle\sum_{k=0}^{d-1}\prod_{j=0}^{\varphi(d)-1}z_{j+1}^{c_{j,k}} \end{array}$$

With these notations, the main theorem of [32, 44] on the asymptotic behaviour of sums of type (2.4) can be stated as follows. In *loc. cit.* the theorem is stated as a density result, but the proof actually shows that equidistribution holds with respect to the appropriate pushforward measure.

Theorem 2.7 ([32, Theorem 6.3] and [44, Theorem 1])**.** *Let $d\geqslant 1$. The sets $\{\mathrm{S}_q(a,d);\ a\in\mathbf{Z}/q\mathbf{Z}\}$ become equidistributed in the image of g_d with respect to the pushforward measure of the probability Haar measure λ on $(\mathbf{S}^1)^{\varphi(d)}$ via g_d, as q goes to infinity among the d-admissible integers. In other words, for any continuous map $F\colon g_d\left((\mathbf{S}^1)^{\varphi(d)}\right)\to\mathbf{C}$,*

$$\frac{1}{q}\sum_{a\in\mathbf{Z}/q\mathbf{Z}}F\left(\mathrm{S}_q(a,d)\right)\underset{\substack{q\to\infty\\ q\in\mathcal{A}_d}}{\longrightarrow}\int_{(\mathbf{S}^1)^{\varphi(d)}}(F\circ g_d)\mathrm{d}\lambda.$$

Now, the fact that a more explicit description of the region of equidistribution can be obtained when d is prime, as shown in Theorem 2.5, simply comes from the knowledge of the coefficients of the cyclotomic polynomials associated with prime numbers. Indeed, this allows us to determine explicitly the polynomial g_d of Definition 2.6.

Proposition 2.8 ([44, Proposition 1])**.** *Let d be a prime number. The polynomial g_d from Definition 2.6 is given by:*

$$\begin{array}{rccc} g_d & : & (\mathbf{S}^1)^{\varphi(d)}=(\mathbf{S}^1)^{d-1} & \to & \mathbf{C} \\ & & (z_1,\dots,z_{d-1}) & \mapsto & z_1+\ldots+z_{d-1}+\dfrac{1}{z_1z_2\ldots z_{d-1}} \end{array}$$

Proof. Since d is prime, the d^{th} cyclotomic polynomial ϕ_d is given by:

$$\phi_d = X^{d-1} + X^{d-2} + \cdots + X + 1.$$

Given this explicit formula, one can easily compute the coefficients $c_{j,k}$ that appear in the reduction modulo ϕ_d of X^k. Indeed, we have:

$$\begin{aligned}
&1 \equiv 1 \bmod \phi_d \\
&X \equiv X \bmod \phi_d \\
&\vdots \\
&X^{d-1} \equiv X^{d-1} \bmod \phi_d \\
&X^d \equiv -1 - X - \ldots X^{d-1} \bmod \phi_d
\end{aligned}$$

so that for all $k \in \{0, \ldots, d-2\}$, $c_{j,k} = \delta_{j,k}$ and for $k = d-1$, all the $c_{j,d-1}$ are equal to -1. Replacing the $c_{j,k}$ by their values in Definition 2.6 leads to the formula for g_d stated in the proposition. □

Besides, the image of $(\mathbf{S}^1)^{d-1}$ via this explicit Laurent polynomial is well-understood thanks to the following geometric lemma.

Lemma 2.9. *Let $d \geqslant 2$. The image of the map:*

$$\begin{array}{rccc} f & : & (\mathbf{S}^1)^{d-1} & \to & \mathbf{C} \\ & & (z_1, \ldots, z_{d-1}) & \mapsto & z_1 + \cdots + z_{d-1} + \frac{1}{z_1 \ldots z_{d-1}} \end{array}$$

is the region $\mathbb{H}_d$ from Definition 2.4, that is: the closed region of boundary the d-cusp hypocycloid.

Proof. See [22, Theorem 3.2.3] or [57, section 3]. Note that this is equivalent to asking the question: "which complex numbers arise as the trace of a matrix in $\mathrm{SU}_d(\mathbf{C})$?" □

Combining Theorem 2.7 with Proposition 2.8 and Lemma 2.9 gives the concrete geometric description of the region of equidistribution stated in Theorem 2.5.
This concrete description, which refines a little bit Theorem 2.7 in the case where d is prime, relies mostly on the fact that in that case, we have an explicit formula for the d^{th} cyclotomic polynomial. As there is also an explicit formula for the d^{th} cyclotomic polynomial when $d = r^b$ is a prime power, namely

$$\phi_{r^b}(X) = \sum_{j=0}^{r-1} X^{jr^{b-1}} \left(= \phi_r\left(X^{r^{b-1}}\right)\right),$$

it is not surprising that our understanding of the image of g_d can also be improved in that case. In fact, the explicit formula above leads to the following proposition.

Proposition 2.10 ([44, Corollary 1])**.** *Let $d := r^b$ be a power of a prime number r. The polynomial g_d from Definition 2.6 is given by*

$$\begin{array}{rccc} g_d & : & (\mathbf{S}^1)^{\varphi(d)} = (\mathbf{S}^1)^{(r-1)r^{b-1}} & \to & \mathbf{C} \\ & & (z_1, \ldots, z_{(r-1)r^{b-1}}) & \mapsto & \displaystyle\sum_{j=1}^{(r-1)r^{b-1}} z_j + \sum_{m=1}^{r^{b-1}} \prod_{\ell=0}^{r-2} z_{m+\ell r^{b-1}}^{-1} \end{array}$$

and the image of $(\mathbf{S}^1)^{\varphi(d)}$ via g_d is the Minkowski sum

$$\sum_{j=1}^{r^{b-1}} \mathbb{H}_r := \left\{\xi_1 + \cdots + \xi_{r^{b-1}};\ \xi_1, \ldots, \xi_{r^{b-1}} \in \mathbb{H}_r\right\}.$$

Proof. We have the following expression for the d^{th} cyclotomic polynomial ϕ_d:

$$\phi_{r^b}(X) = \sum_{j=0}^{r-1} X^{jr^{b-1}}$$

This allows us to perform the reductions modulo ϕ_d of the monomials X^k for all $k \in \{0, \dots, d-1\}$:

For all $k \in \{0, \dots, (r-1)r^{b-1}-1\}$, we have that X^k is itself the unique polynomial of degree less than $\varphi(d)$ which is congruent to X^k modulo ϕ_d. Thus, $(c_{j,k})_{0 \leqslant j < \varphi(d)} = (\delta_{j,k})_{0 \leqslant j < \varphi(d)}$.
Now, if $k \in \{(r-1)r^{b-1}, \dots, r^b - 1\}$, we write $k = (r-1)r^{b-1} + m$ with $m \in \{0, \dots, r^{b-1}-1\}$. Then, if we multiply by X^m the congruence:

$$X^{(r-1)r^{b-1}} \equiv -\sum_{j=0}^{r-2} X^{jr^{b-1}} \bmod \phi_d$$

we obtain:

$$X^k = X^{(r-1)r^{b-1}+m} \equiv -\sum_{j=0}^{r-2} X^{jr^{b-1}+m} \bmod \phi_d$$

This tells us that for all $j \in \{0, \dots, \varphi(d)-1\}$, $c_{j,k} = -1$ if $j \equiv m \bmod r^{b-1}$ and $c_{j,k} = 0$ otherwise. So if we replace the exponents $c_{j,k}$ by their values in the definition of g_d (Definition 2.6), it gives:

$$\begin{aligned}
\sum_{k=0}^{d-1} \prod_{j=0}^{\varphi(d)-1} z_{j+1}^{c_{j,k}} &= \sum_{k=0}^{(r-1)r^{b-1}-1} \left(\prod_{j=0}^{(r-1)r^{b-1}-1} z_{j+1}^{c_{j,k}} \right) + \sum_{k=(r-1)r^{b-1}}^{r^b-1} \left(\prod_{j=0}^{\varphi(d)-1} z_{j+1}^{c_{j,k}} \right) \\
&= \sum_{k=0}^{(r-1)r^{b-1}-1} \left(\prod_{j=0}^{(r-1)r^{b-1}-1} z_{j+1}^{\delta_{j,k}} \right) + \sum_{m=0}^{r^{b-1}-1} \left(\prod_{j=0}^{(r-1)r^{b-1}-1} z_{j+1}^{c_{j,(r-1)r^{b-1}+m}} \right)
\end{aligned}$$

Recalling that $c_{j,(r-1)r^{b-1}+m} = -1$ if $j \equiv m \bmod r^{b-1}$ and equals zero otherwise, we obtain:

$$\begin{aligned}
\sum_{k=0}^{d-1} \prod_{j=0}^{\varphi(d)-1} z_{j+1}^{c_{j,k}} &= \sum_{k=0}^{(r-1)r^{b-1}-1} z_{k+1} + \sum_{m=0}^{r^{b-1}-1} \left(\prod_{\substack{0 \leqslant j < (r-1)r^{b-1} \\ j \equiv m \bmod r^{b-1}}} z_{j+1}^{-1} \right) \\
&= \sum_{k=0}^{(r-1)r^{b-1}-1} z_{k+1} + \sum_{m=1}^{r^{b-1}} \left(\prod_{\substack{1 \leqslant j \leqslant (r-1)r^{b-1} \\ j \equiv m \bmod r^{b-1}}} z_j^{-1} \right) \qquad (2.5) \\
&= \sum_{j=1}^{(r-1)r^{b-1}} z_j + \sum_{m=1}^{r^{b-1}} \prod_{\ell=0}^{r-2} z_{m+\ell r^{b-1}}^{-1}
\end{aligned}$$

This finishes the proof of the formula for g_{r^b}. Now, as we have seen at line (2.5) above, we have: for all $z_1, \dots, z_{\varphi(r^b)} \in \mathbf{S}^1$,

$$g_{r^b}(z_1, \dots, z_{\varphi(r^b)}) = \sum_{j=1}^{(r-1)r^{b-1}} z_j + \sum_{m=1}^{r^{b-1}} \left(\prod_{\substack{1 \leqslant j \leqslant (r-1)r^{b-1} \\ j \equiv m \bmod r^{b-1}}} z_j^{-1} \right)$$

Hence:

$$\begin{aligned} g_{r^b}(z_1,\dots,z_{\varphi(r^b)}) &= \sum_{m=1}^{r^{b-1}} \left(\sum_{\substack{1\leqslant j\leqslant \varphi(r^b)\\ j\equiv m \bmod r^{b-1}}} z_j \right) + \sum_{m=1}^{r^{b-1}} \left(\prod_{\substack{1\leqslant j\leqslant \varphi(r^b)\\ j\equiv m \bmod r^{b-1}}} z_j^{-1} \right) \\ &= \sum_{m=1}^{r^{b-1}} \left(\sum_{\substack{1\leqslant j\leqslant \varphi(r^b)\\ j\equiv m \bmod r^{b-1}}} z_j + \prod_{\substack{1\leqslant j\leqslant \varphi(r^b)\\ j\equiv m \bmod r^{b-1}}} z_j^{-1} \right) \\ &= \sum_{m=1}^{r^{b-1}} g_r(\mathbf{z}_m) \end{aligned}$$

where $\mathbf{z}_m$ denotes the element $(z_{m+\ell r^{b-1}})_{0\leqslant \ell\leqslant r-2}$ of $(\mathbf{S}^1)^{r-1}$. In other words, $\mathbf{z}_m$ is the vector obtained from $(z_1,\dots,z_{\varphi(r^b)})$ by only keeping the z_j with $j\equiv m \bmod r^{b-1}$.

By Proposition 2.8, the image of $(\mathbf{S}^1)^{r-1}$ via g_r is the region $\mathbb{H}_r$ of boundary the d-cusps hypocycloid. Therefore, the image of $(\mathbf{S}^1)^{\varphi(r^b)}$ via g_{r^b} is:

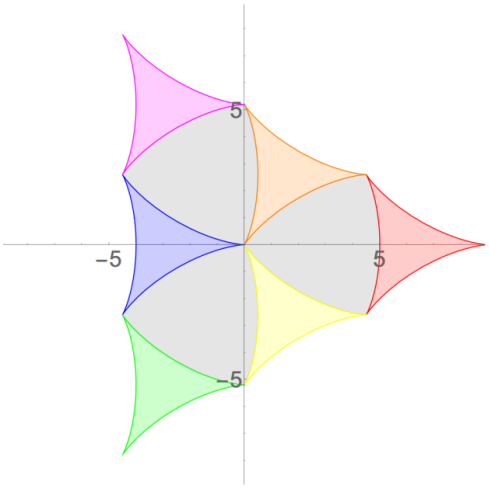
$$\sum_{j=1}^{r^{b-1}} \mathbb{H}_r = \{\xi_1+\cdots+\xi_{r^{b-1}};\ \xi_1,\dots,\xi_{r^{b-1}}\in\mathbb{H}_r\}$$

the Minkowski sum of r^{b-1} copies of $\mathbb{H}_r$. This finishes the proof. □

Example 2.11. For instance, as it is done in [16, Theorem 10], for $r=3$ and $b=2$ we have:

$$g_9(z_1,\dots,z_6) = \underbrace{z_1+z_4+\frac{1}{z_1z_4}}_{\in\mathbb{H}_3} + \underbrace{z_2+z_5+\frac{1}{z_2z_5}}_{\in\mathbb{H}_3} + \underbrace{z_3+z_6+\frac{1}{z_3z_6}}_{\in\mathbb{H}_3}$$

The following picture shows what the Minkowski sum of three copies of $\mathbb{H}_3$ looks like.



(A) A geometric interpretation of $H_3+H_3+H_3$

Figure 2.3: Image of $(\mathbf{S}^1)^6$ via g_9 (image extracted from the article [44, Figure 11])

.

Since Theorem 2.7 asserts that the sets of sums $\mathcal{S}_q(-,9)$ become equidistributed in the image of g_9 with respect to some measure, and Proposition 2.10 tells us that the image of g_9 is the Minkowski

sum of three copies of $\mathbb{H}_3$, we expect to observe a shape as in Figure 2.3 when plotting the elements of $\mathcal{S}_q(-,9)$ for some large q. This is indeed what happens, as the picture below shows.

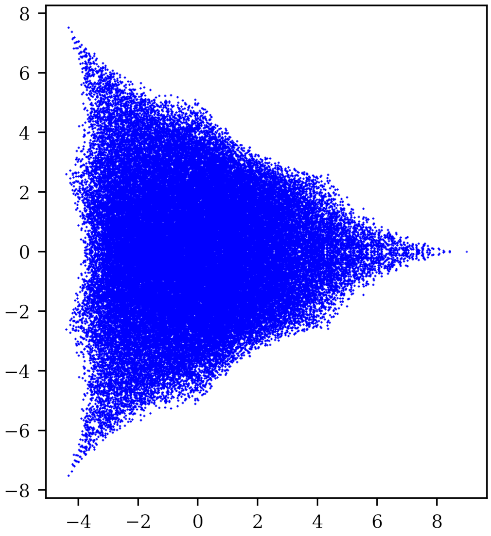


Figure 2.4: The sets $\mathcal{S}_q(-,9)$ for $q = 811^2$

Besides the case of sums of the form (2.4), Kloosterman sums restricted to the subgroup of order d have also been studied. These are the sums

$$\mathrm{K}_q(a,b,d) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax+bx^{-1}}{q}\right), \tag{2.6}$$

which are indeed a particular case of that of sums

$$\sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right)$$

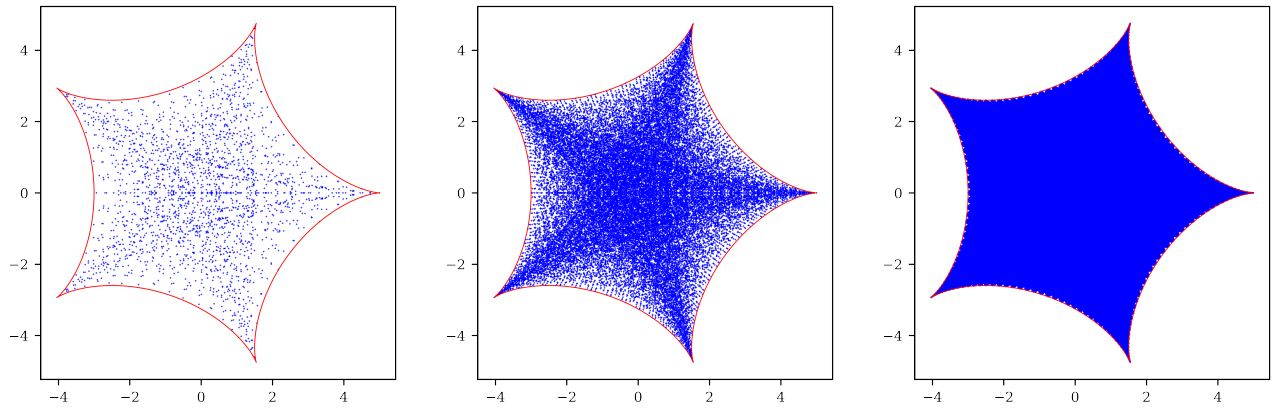
introduced in (2.3).

It was proved in [16, Theorem 7 and Theorem 10] that when d is a prime number or $d = 9$, the same equidistribution result as Theorem 2.7 holds for the sets of restricted Kloosterman sums

$$\mathcal{K}_q(-,-,d) := \left\{\mathrm{K}_q(a,b,d);\ a,b\in(\mathbf{Z}/q\mathbf{Z})^2\right\}.$$

For instance, when $d = 5$, the statement [16, Theorem 7] asserts that the sets $\mathcal{K}_q(-,-,d)$ become equidistributed in the region $\mathbb{H}_5$ of boundary the 5-cusp hypocycloid, with respect to the same measure as in Theorem 2.5 (the statement concerns the density, but the remark after their proof explains that there is equidistribution). Again, this asymptotic behaviour is only true when q goes to infinity *among the 5-admissible integers*, since this condition ensures that the set indexing the sum is not trivial.

The following picture illustrates this asymptotic behaviour. For three different 5-admissible values of q, we represented the q^2 complex numbers $\mathrm{K}_q(a,b,5)$ for $a,b\in\mathbf{Z}/q\mathbf{Z}$.



(a) $q = 151$ (b) $q = 631$ (c) $q = 3721 = 61^2$

Figure 2.5: The sets $\left\{\mathrm{K}_q(a,b,d);\ a,b \in (\mathbf{Z}/q\mathbf{Z})^2\right\}$ for $d = 5$ and three 5-admissible values of q.

2.3. Extension to more general families of Laurent polynomials

2.3.1. The case of exponents coprime with d

It is quite striking that the sets of sums of type (2.4) and (2.6) of [16, 32] and [44] satisfy the same equidistribution result, and so it is natural to ask what is the reason behind this similarity. Actually, a careful look at their proof shows that the common point between the two is that the exponents of x appearing inside the exponentials in

$$\mathrm{S}_q(a,d) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax}{q}\right) \quad \text{and} \quad \mathrm{K}_q(a,b,d) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax+bx^{-1}}{q}\right)$$

are respectively 1 and $(1,-1)$, and these are all *coprime with* d, for any d. As we will see in the proof, this is really the reason why these different families of exponential sums satisfy the same equidistribution result. This observation allows us to state a generalization of the known theorems, by extending Theorem 2.7 to sets of sums of the form

$$\left\{ \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right);\ (a_1,\dots,a_n)\in(\mathbf{Z}/q\mathbf{Z})^n \right\} \tag{2.7}$$

provided the vector $\mathbf{m} = (m_1,\dots,m_n) \in \mathbf{Z}^n$ is coprime with d in the sense of Definition 2.2. Theorem 2.7 corresponds to the case $\mathbf{m} = (1)$ while Kloosterman sums restricted to the subgroup of order d corresponds to the case $\mathbf{m} = (1,-1)$. Moreover, we noticed that one can fix some of the parameters and let the others vary, and still obtain the equidistribution result. For instance, in the case of restricted Kloosterman sums, the same method allows one to prove the equidistribution of the sets

$$\mathcal{K}_q(1,-,d) := \{\mathrm{K}_q(1,b,d);\ b\in\mathbf{Z}/q\mathbf{Z}\}.$$

(with respect to the same measure as the sets $\mathcal{K}_q(-,-,d)$).

We state below our first extension of Theorem 2.7, and give its proof, which relies on the exact same arguments as in [32, 44]. The main idea is that the exponential sums we are considering, which are sums of d particular roots of unity, can in fact be expressed as a Laurent polynomial in a smaller number of roots to unity. Then it remains to show that this set of roots of unity becomes equidistributed in some multi-dimensional torus. This step can be translated into a statement on equidistribution modulo 1, to which standard tools such as Weyl's criterion can be applied.

Proposition 2.12. *Let $d \geqslant 1$ and let $\mathbf{m} = (m_1, \dots, m_n) \in \mathbf{Z}^n$ be a vector coprime with d. Let $s \in \{1, \dots, n\}$ and let $\{i_1, \dots, i_s\} \subseteq \{1, \dots, n\}$. We fix $n-s$ integers a_i for $i \in \{1, \dots, n\} \setminus \{i_1, \dots, i_s\}$. Then the sets of sums*

$$\left\{ \sum_{\substack{x \in (\mathbf{Z}/q\mathbf{Z})^\times \\ x^d = 1}} e\left(\frac{a_1 x^{m_1} + \cdots + a_n x^{m_n}}{q} \right);\ (a_{i_1}, \dots, a_{i_s}) \in (\mathbf{Z}/q\mathbf{Z})^s \right\}$$

become equidistributed in the image of g_d (with respect to the pushforward measure via g_d of the probability Haar measure on $(\mathbf{S}^1)^{\varphi(d)}$) as q goes to infinity among the d-admissible integers.

Remark 2.13. Let us stress that the Laurent polynomial g_d does not depend on $\mathbf{m}$. This implies that the region of equidistribution almost does not depend on the shape of the numerators in the exponentials: it will be the same for any $\mathbf{m}$ coprime with d. This explains why [16, Theorem 7] and [32, Theorem 6.3] give rise to the same kind of pictures, and this leads to many other examples.

Proof. 1. *Reduction to a statement on equidistribution modulo* 1*:*

For all d-admissible integers q, let

$$Y_{\mathbf{m},q} := \prod_{j=1}^{s} \mathbf{Z}/q\mathbf{Z}$$

and denote by $\theta_{\mathbf{m},q} \colon Y_{\mathbf{m},q} \to \mathbf{C}$ the map defined by

$$(a_{i_1}, \dots, a_{i_s}) \mapsto \sum_{\substack{x \in (\mathbf{Z}/q\mathbf{Z})^\times \\ x^d = 1}} e\left(\frac{a_1 x^{m_1} + \cdots + a_n x^{m_n}}{q} \right). \tag{2.8}$$

Moreover, let w_q be an element of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$ (recall q is d-admissible). Then w_q is a generator of the unique subgroup of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$. In other words,

$$\left\{ x \in (\mathbf{Z}/q\mathbf{Z})^\times;\ x^d = 1 \right\} = \left\{ w_q^k;\ k \in \{0, \dots, d-1\} \right\}$$

meaning that we can describe the subgroup of order d in terms of the successive powers of w_q. Then, for all $(a_{i_1}, \dots, a_{i_s}) \in Y_{\mathbf{m},q}$,

$$\begin{aligned} \theta_{\mathbf{m},q}(a_{i_1}, \dots, a_{i_s}) &= \sum_{\substack{x \in (\mathbf{Z}/q\mathbf{Z})^\times \\ x^d = 1}} e\left(\frac{a_1 x^{m_1} + \cdots + a_n x^{m_n}}{q} \right) \\ &= \sum_{k=0}^{d-1} e\left(\frac{a_1 (w_q^k)^{m_1} + \cdots + a_n (w_q^k)^{m_n}}{q} \right) \\ &= \sum_{k=0}^{d-1} e\left(\frac{a_1 (w_q^{m_1})^k + \cdots + a_n (w_q^{m_n})^k}{q} \right). \end{aligned}$$

Now, for all $i \in \{1, \dots, n\}$, since m_i is coprime with d (which is the order of w_q), $w_q^{m_i}$ has the same order as w_q. Thus, as an element of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$, it satisfies $\overline{\phi}_d(w_q^{m_i}) = 0$ in $\mathbf{Z}/q\mathbf{Z}$. This comes from the following lemma, whose proof is included after the proof of Proposition 2.12.

Lemma 2.14. *Let $d \geqslant 2$ be an integer, and let ϕ_d be the d^{th} cyclotomic polynomial. Let $q = p^\alpha$ be a d-admissible integer. Let $x \in (\mathbf{Z}/q\mathbf{Z})^\times$ be an element of order d. Then we have:*

$$\overline{\phi}_d(x) = 0 \text{ in } \mathbf{Z}/q\mathbf{Z}$$

where $\overline{\phi}_d$ denotes the polynomial obtained from ϕ_d by reducing its coefficients modulo q.

Thus, for all $k \in \{0, \dots, d-1\}$, if one reduces modulo q the congruence

$$X^k \equiv \sum_{j=0}^{\varphi(d)-1} c_{j,k} X^j \bmod \phi_d$$

and evaluate it at $w_q^{m_i}$, the term $\overline{\phi}_d(w_q^{m_i})$ is equal to zero, hence:

$$(w_q^{m_i})^k = \sum_{j=0}^{\varphi(d)-1} c_{j,k} (w_q^{m_i})^j \text{ in } \mathbf{Z}/q\mathbf{Z}$$

Replacing this in the expression of $\theta_{\mathbf{m},q}(a_1, \dots, a_n)$ obtained above, we get:

$$\begin{aligned}
\theta_{\mathbf{m},q}(a_{i_1}, \dots, a_{i_s}) &= \sum_{k=0}^{d-1} e\left(\frac{a_1 (w_q^{m_1})^k + \cdots + a_n (w_q^{m_n})^k}{q}\right) \\
&= \sum_{k=0}^{d-1} e\left(\frac{a_1 \sum_{j=0}^{\varphi(d)-1} c_{j,k} (w_q^{m_1})^j + \cdots + a_n \sum_{j=0}^{\varphi(d)-1} c_{j,k} (w_q^{m_n})^j}{q}\right) \\
&= \sum_{k=0}^{d-1} \prod_{j=0}^{\varphi(d)-1} e\left(\frac{a_1 (w_q^{m_1})^j + \cdots + a_n (w_q^{m_n})^j}{q}\right)^{c_{j,k}}
\end{aligned}$$

Therefore, if we define for all $j \in \{0, \dots, \varphi(d) - 1\}$,

$$z_j = z_j(a_{i_1}, \dots, a_{i_s}, q, j) := e\left(\frac{a_1 (w_q^{m_1})^j + \cdots + a_n (w_q^{m_n})^j}{q}\right)$$

we have:

$$\theta_{\mathbf{m},q}(a_{i_1}, \dots, a_{i_s}) = g_d(z_0, \dots, z_{\varphi(d)-1})$$

with the Laurent polynomial g_d defined at Definition 2.6 and the z_j's being elements of $\mathbf{S}^1$. This already shows that $\theta_{\mathbf{m},q}(a_{i_1}, \dots, a_{i_s})$ belongs to the image of g_d. In order to show that these sums become equidistributed with respect to the pushforward measure of the probability Haar measure on $(\mathbf{S}^1)^{\varphi(d)}$, it suffices, by Lemma 1.16, to show that the sets

$$\left\{ \left(e\left(\frac{a_1 (w_q^{m_1})^0 + \cdots + a_n (w_q^{m_n})^0}{q}\right), \dots, e\left(\frac{a_1 (w_q^{m_1})^{\varphi(d)-1} + \cdots + a_n (w_q^{m_n})^{\varphi(d)-1}}{q}\right)\right); \right.$$
$$\left. a_{i_1}, \dots, a_{i_s} \in \mathbf{Z}/q\mathbf{Z} \right\}$$

become equidistributed in $(\mathbf{S}^1)^{\varphi(d)}$ with respect to this measure, as q goes to infinity among the d-admissible integers.

To do so, it is equivalent to show that the "angles" which appear in the exponentials become equidistributed modulo 1. In other words, we will get the conclusion if we are able to show that the following subsets of $(\mathbf{R}/\mathbf{Z})^{\varphi(d)}$:

$$\left\{ \overbrace{\left(\frac{a_1 (w_q^{m_1})^0 + \cdots + a_n (w_q^{m_n})^0}{q}, \dots, \frac{a_1 (w_q^{m_1})^{\varphi(d)-1} + \cdots + a_n (w_q^{m_n})^{\varphi(d)-1}}{q} \right)}^{=: \mathbf{x}(a_{i_1}, \dots, a_{i_s}, q)}; \right.$$
$$\left. a_{i_1}, \dots, a_{i_s} \in \mathbf{Z}/q\mathbf{Z} \right\}$$

become equidistributed modulo 1 as q goes to infinity among the d-admissible integers.

2. *Proof of the equidistribution modulo* 1*:*

By Weyl's criterion, these sets become equidistributed if and only if for any $\mathbf{y} := (y_0, \dots, y_{\varphi(d)-1}) \in \mathbf{Z}^{\varphi(d)} \setminus \{0\}$ we have

$$\frac{1}{q^s} \times \left(\sum_{(a_{i_1},\dots,a_{i_s}) \in (\mathbf{Z}/q\mathbf{Z})^s} e\left(\mathbf{x}(a_{i_1}, \dots, a_{i_s}, q) \cdot \mathbf{y}\right) \right) \underset{\substack{q \to \infty \\ q \in \mathcal{A}_d}}{\longrightarrow} 0. \tag{2.9}$$

But the left-hand side can be rewritten as:

$$\prod_{i \in \{i_1,\dots,i_s\}} \left[\frac{1}{q} \sum_{a_i \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{a_i f(w_q^{m_i})}{q} \right) \right] \times \prod_{i \notin \{i_1,\dots,i_s\}} e\left(\frac{a_i f(w_q^{m_i})}{q} \right) \tag{2.10}$$

where f is the polynomial $y_0 + y_1 X + \cdots + y_{\varphi(d)-1} X^{\varphi(d)-1}$.

Now, since $(m_i, d) = 1$, we have that for all $i \in \{1, \dots, n\}$ the element $w_q^{m_i}$ is still of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$. Also, $f \in \mathbf{Z}[X] \setminus \{0\}$ and $\deg f < \varphi(d)$. Then we use the following lemma due to Gerald Myerson (see [86, proof of Theorem 12]), as formulated in [32]. A proof is given below.

Lemma 2.15 (Myerson's lemma, [32, Lemma 6.2])**.** *Let $d \geqslant 1$ be an integer, and let $f \in \mathbf{Z}[X] \setminus \{0\}$ be a polynomial of degree strictly less than $\varphi(d)$. Then there exists an integer m_f such that for all d-admissible integer q such that $q > m_f$, for any element w_q of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$,*

$$\sum_{a \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{f(w_q)}{q} a \right) = 0.$$

This lemma tells us that the sums

$$\sum_{a_i \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{a_i f(w_q^{m_i})}{q} \right)$$

in (2.10) are eventually equal to zero when q exceeds a certain rank, so the convergence (2.9) holds, and this gives the conclusion.

□

Proof of Lemma 2.14. We consider the polynomial $P(X) := X^d - 1$, seen as an element in $\mathbf{Z}_p[X]$, where $\mathbf{Z}_p$ is the ring of p-adic integers. Let $\tilde{x}$ be a lift in $\mathbf{Z}$ of the class x modulo q. Then we have

$$P(\tilde{x}) \equiv 0 \bmod q$$

since x has order d. Therefore $|P(\tilde{x})|_p \leqslant \frac{1}{p^\alpha}$, where we denoted by $|\cdot|_p$ the standard p-adic absolute value on the field of p-adic numbers $\mathbf{Q}_p$. On the other hand, we have $P'(\tilde{x}) = d\tilde{x}^{d-1}$, which has p-adic valuation zero since $(d, p) = 1$ (because d divides $p - 1$) and $(\tilde{x}, p) = 1$ since x is invertible modulo p^α. Thus, $|P'(\tilde{x})|_p = 1$ and so:

$$|P(\tilde{x})|_p \leqslant \frac{1}{p^\alpha} = \frac{1}{p^\alpha} |P'(\tilde{x})|_p^2$$

Therefore, by Hensel's lemma (see [17, chapter II, appendix C]) there exists a unique $\tilde{z} \in \mathbf{Z}_p$ such that

$$\begin{cases} P(\tilde{z}) = 0 \\ |\tilde{z} - \tilde{x}|_p \leqslant \frac{1}{p^\alpha} \end{cases} \tag{2.11}$$

We deduce that:

$$0 = \tilde{z}^d - 1 = \prod_{m|d} \phi_m(\tilde{z}) \quad \text{in } \mathbf{Z}_p \tag{2.12}$$

Now since $\mathbf{Z}_p$ is an integral domain, at least one of the factors $\phi_m(\tilde{z})$ must be zero.
Assume for a contradiction that this happens for an m which is not equal to d. Then this would imply that $\tilde{z}^m = 1$ in $\mathbf{Z}_p$, hence:

$$|\tilde{x}^m - 1|_p = |\tilde{x}^m - \tilde{z}^m|_p \leqslant |\tilde{x} - \tilde{z}|_p \leqslant \frac{1}{p^\alpha}$$

by the second condition in (2.11). Thus, $\tilde{x}^m \equiv 1 \bmod p^\alpha$ for an $m < d$, contradicting the fact that x has order exactly d in $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$. Therefore, in the product (2.12), it is the term $\phi_d(\tilde{z})$ which equals zero. Now, since $|\tilde{x} - \tilde{z}|_p \leqslant \frac{1}{p^\alpha}$ we have:

$$|\phi_d(\tilde{x})|_p = |\phi_d(\tilde{x}) - \phi_d(\tilde{z})|_p \leqslant \frac{1}{p^\alpha}$$

and this is equivalent to $\phi_d(\tilde{x}) \equiv 0 \bmod p^\alpha$, that is: $\overline{\phi}_d(x) = 0$ in $\mathbf{Z}/p^\alpha\mathbf{Z}$.

□

Proof of Lemma 2.15. This proof can be found in [32, lemma 6.2], but we include it here because we will need some precise knowledge brought by the proof in order to prove our generalizations. Besides, we want to stress the role played by Lemma 2.14.
It is well known that ϕ_d is a monic polynomial with coefficients in $\mathbf{Z}$, that it is irreducible in $\mathbf{Q}[X]$, and that it has degree $\varphi(d)$. On the other hand, the polynomial f has degree less than or equal to $\varphi(d) - 1$ and is non-zero. Thus, f and ϕ_d are coprime in $\mathbf{Q}[X]$. This yields a Bézout relation between them in $\mathbf{Q}[X]$ (which is a principal ideal domain, that is why we viewed the polynomials in $\mathbf{Q}[X]$ instead of staying in $\mathbf{Z}[X]$). Now if we chase the denominators in such a Bézout relation, we get that there exist $n \in \mathbf{Z} \setminus \{0\}$ and $a, b \in \mathbf{Z}[X]$ such that:

$$a(X)\phi_d(X) + b(X)f(X) = n \tag{2.13}$$

Up to replacing (a, b) by $(-a, -b)$ we can assume that $n \geqslant 1$. Let $q > n$ be a d-admissible integer. Since the map:

$$a \mapsto e\left(\frac{f(w_q)}{q}a\right)$$

is an additive character of $\mathbf{Z}/q\mathbf{Z}$, the orthogonality of characters tells us that:

$$\sum_{a \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{f(w_q)}{q}a\right) = \begin{cases} 0 & \text{if } f(w_q) \not\equiv 0 \bmod q \\ q & \text{if } f(w_q) \equiv 0 \bmod q \end{cases} \tag{2.14}$$

Let us prove that the choice of $q > n$ implies that $f(w_q) \not\equiv 0 \bmod q$ (so that the sum is zero).
First, we evaluate relation (2.13) at any integer $\tilde{w}_q$ which lifts w_q. We obtain an equality in $\mathbf{Z}$, which we can reduce modulo q. This yields:

$$a(\tilde{w}_q)\phi_d(\tilde{w}_q) + b(\tilde{w}_q)f(\tilde{w}_q) \equiv n \bmod q$$

Now, thanks to Lemma 2.14 we have that $\phi_d(\tilde{w}_q) \equiv 0 \bmod q$, hence: $b(\tilde{w}_q)f(\tilde{w}_q) \equiv n \bmod q$. So if we assume for a contradiction that q divides $f(\tilde{w}_q)$ then this implies that q divides n, which is impossible since $q > n$. Thus, q does not divide $f(\tilde{w}_q)$ and $\sum_{a \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{f(w_q)}{q}a\right) = 0$ thanks to (2.14). Therefore, we proved that one can take the integer m_f of the statement to be the integer n from (2.13), and that for all $q > m_f$ we indeed have:

$$\sum_{a \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{f(w_q)}{q}a\right) = 0.$$

□

Remark 2.16. The name "Myerson's Lemma" comes from the fact that the above proof is used in the proof of [86, Theorem 12].

Some applications. First of all, Proposition 2.12 allows one to recover the equidistribution results from [32, 44] and [16]. Indeed, the sets

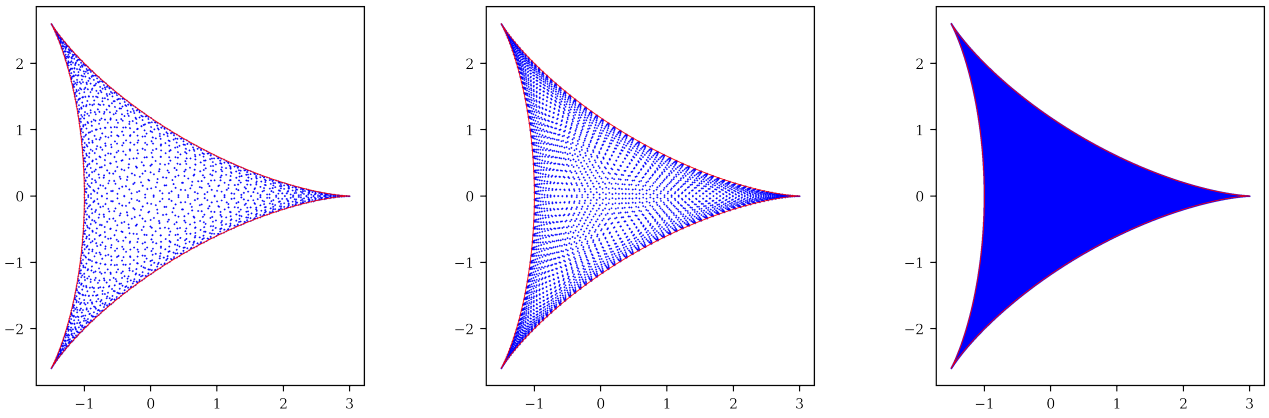
$$\mathcal{S}_q(-,d) := \left\{ \mathrm{S}_q(a,d) = \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax}{q}\right);\ a\in\mathbf{Z}/q\mathbf{Z} \right\}$$

and

$$\mathcal{K}_q(-,-,d) := \left\{ \mathrm{K}_q(a,b,d) = \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax+bx^{-1}}{q}\right),\quad a,b\in\mathbf{Z}/q\mathbf{Z} \right\}$$

clearly fulfill the assumptions of Proposition 2.12 for any d, hence become equidistributed in the image of g_d with respect to the suitable pushforward measure, as q goes to infinity among the d-admissible integers. Combining this fact with the geometric interpretations of the image of g_d provided by Lemma 2.9 and Proposition 2.10 leads to the equidistribution theorems inside explicit regions, as illustrated in Figure 2.1, Figure 2.4 and Figure 2.5. Moreover, our proposition already refines [16, Theorems 7 and 10], because it extends their results on Kloosterman sums restricted to subgroups to *any fixed* d (whereas only the cases where d is prime and $d = 9$ were studied in *loc. cit.*) and it states the more precise fact that one can fix one of the two parameters a and b, and still obtain equidistribution. For instance, in the following picture we illustrate the asymptotic distribution of the sets of sum

$$\mathcal{K}_q(1,-,d) := \left\{ \mathrm{K}_q(1,b,d) = \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{x+bx^{-1}}{q}\right),\quad b\in\mathbf{Z}/q\mathbf{Z} \right\}$$



(a) $q = 6673$ (b) $q = 13591$ (c) $q = 877^2$

Figure 2.6: The sets $\mathcal{K}_q(1,-,d)$ for $d = 3$ and three 3-admissible values of q.

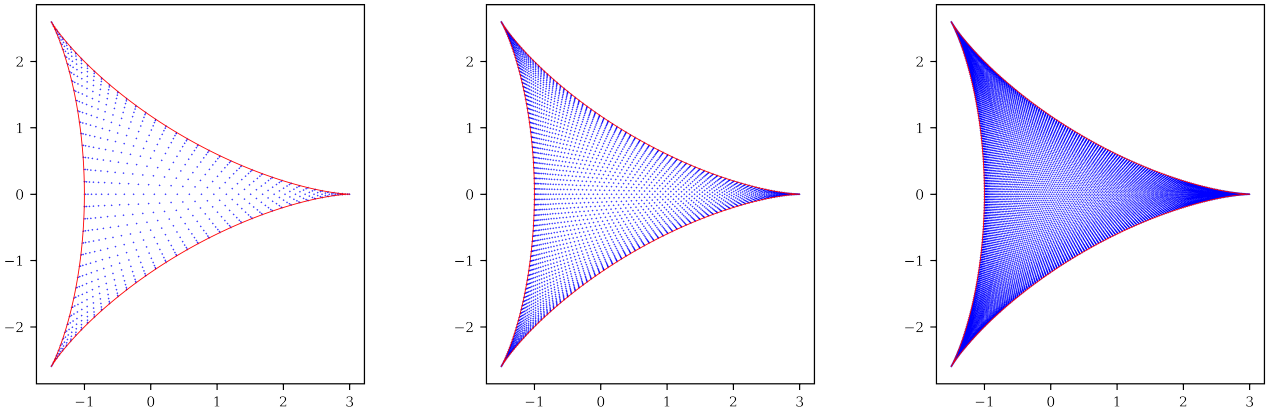
Moreover, Proposition 2.12 substantially enlarges the family of exponential sums satisfying the same asymptotic behaviour as the ones above. Indeed, sums with ax or $ax + bx^{-1}$ inside the exponentials may now be replaced by sums with $a_1x^{m_1} + \ldots a_nx^{m_n}$ inside the exponentials, provided the m_i are coprime with d. For instance, one can consider the sums

$$\mathrm{Q}_q(a,b,c,d) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax^4+bx^2+cx}{q}\right) \text{ for } a,b,c\in\mathbf{Z}/q\mathbf{Z},$$

for all d-admissible integer q. In particular, if we look again at the case $d = 3$ and we draw the sets

$$\mathcal{Q}_q(-,-,-,3) = \{\mathrm{Q}_q(a,b,c,3);\ a,b,c\in\mathbf{Z}/q\mathbf{Z}\}$$

for different 3-admissible values of q, we observe the same equidistribution as for the other types of sums, inside a 3-cusp hypocycloid.



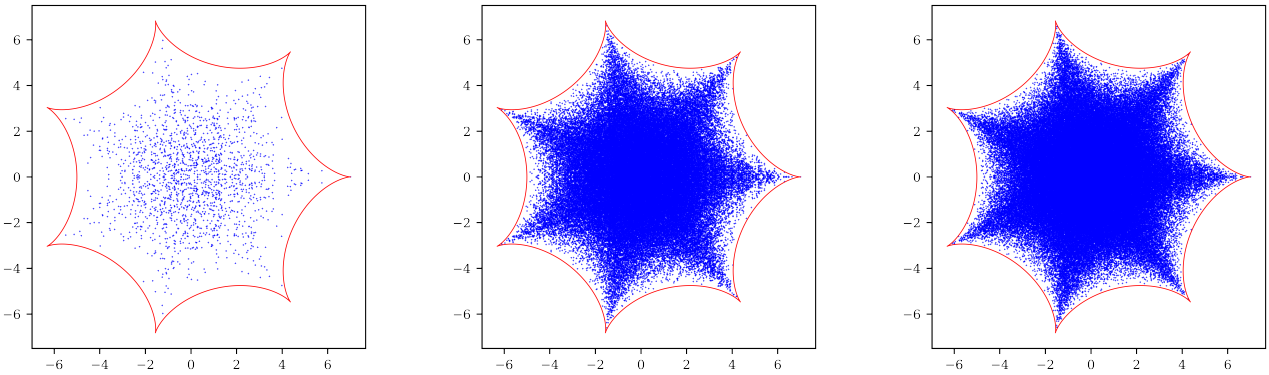
(a) $q = 67$ (b) $q = 157$ (c) $q = 307$

Figure 2.7: The sets $\mathcal{Q}_q(-,-,-,d)$ for $d = 3$ and three 3-admissible values of q.

One could also want to consider sets of Birch sums restricted to a subgroup, that is:

$$\mathrm{B}_q(a,b,d) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax^3+bx}{q}\right) \text{ où } a,b \in \mathbf{Z}/q\mathbf{Z}$$

For instance if we take $d = 7$ and look at the sets $\mathcal{B}_q(-,-,7) := \{\mathrm{B}_q(a,b,7);\ a,b \in \mathbf{Z}/q\mathbf{Z}\}$, then Proposition 2.12 (combined with Proposition 2.8 and Lemma 2.9) states that they should become equidistributed in $\mathbb{H}_7$ (the region of boundary the 7-cusp hypocycloid) as q goes to infinity among the 7-admissible integers. This is indeed what the following pictures suggest:



(a) $q = 113$ (b) $q = 827$ (c) $q = 1009$

Figure 2.8: The sets $\mathcal{B}_q(-,-,d)$ for $d = 7$ and three 7-admissible values of q.

Remark 2.17. Note that in Proposition 2.12, the measure with respect to which the sums become equidistributed is the pushforward measure via g_d of the Haar measure on $(\mathbf{S}^1)^{\varphi(d)}$. This explains why one does not observe a "uniform" distribution in the sense of the Lebesgue measure.

On the other hand, one could want to consider Birch sums restricted to the subgroup of order 6 say, that is sums of the type:

$$\mathrm{B}_q(a,b,3) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^6=1}} e\left(\frac{ax^3+bx}{q}\right) \text{ où } a,b \in \mathbf{Z}/q\mathbf{Z}$$

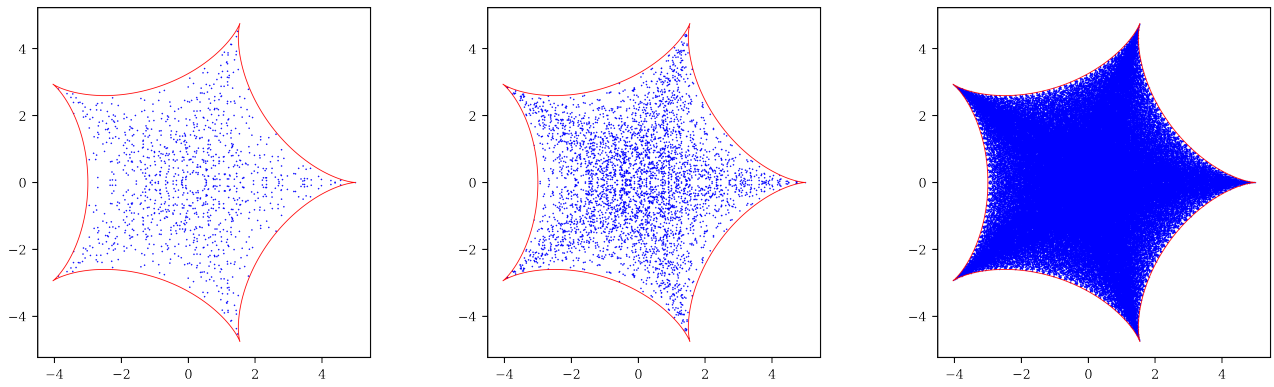
However, this type of sum does not fall inside the range of application of Proposition 2.12 , because the exponent 3 in the polynomial expression $ax^3 + bx$ is not coprime with the order of the subgroup. In the next section, we address this remaining issue.

2.3.2. The case of exponents not coprime with d

Some experiments. Before stating the general equidistribution result which can be obtained, we present some experiments on the particular case of Gauss sums, which explain the main ideas that led to Proposition 2.20. Namely, let us focus on Gauss sums restricted to the unique subgroup of order d:

$$\mathrm{G}_q(a,d) := \sum_{\substack{x\in\mathbf{Z}/q\mathbf{Z}\\ x^d=1}} e\left(\frac{ax^2}{q}\right)$$

for d-admissible values of q. We denote by $\mathcal{G}_q(-,d)$ the set $\{\mathrm{G}_q(a,d),\ a\in\mathbf{Z}/q\mathbf{Z}\}$. When d is odd, it is coprime with 2, which is the exponent of x which appears inside the exponential. Therefore, when d is odd, the sets $\mathcal{G}_q(-,d)$ satisfy the assumptions of Proposition 2.12, hence satisfy the same equidistribution properties as the sets $\mathcal{S}_q(-,d)$ or $\mathcal{K}_q(-,-,d)$ discussed in the previous section. For instance when $d=5$, these sets become equidistributed in a 5-cusp hypocycloid:



(a) $q = 5861$ (b) $q = 20441$ (c) $q = 811^2$

Figure 2.9: The sets $\mathcal{G}_q(-,5)$ and three 5-admissible values of q.

and when $d=9$, they become equidistributed in the Minkowski sum of three 3-cusp hypocycloids:

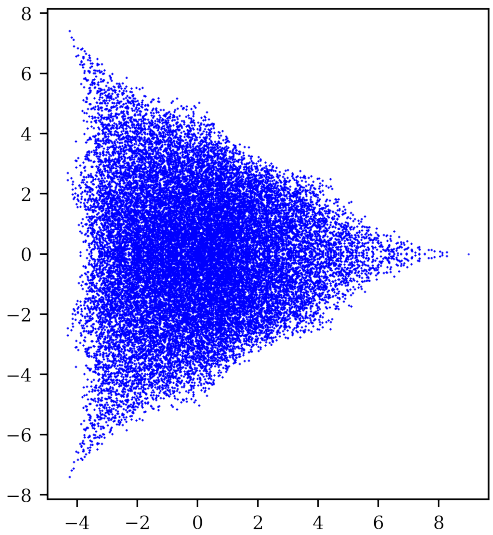


Figure 2.10: The points of the set $\mathcal{G}_q(-,9)$ for $q = 250993$

However, they do not only satisfy the same equidistribution properties, they are actually equal to the sums of type $\mathrm{S}_q(a,d)$! Indeed, if we let w_q denote a generator of the unique subgroup of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$, then w_q is an element of order d. Therefore, w_q^2 is also an element of order d as soon as d is odd, thanks to the following classical lemma.

Lemma 2.18. *Let G be an abelian group, and let $x \in G$ be an element of order d. Then for all $n \geqslant 1$, the order of x^n is $\frac{d}{(n,d)}$. In particular, if $(n,d) = 1$, then x^n has the same order as x.*

Therefore, the subgroup generated by w_q^2 is also the unique subgroup of order d, so we have

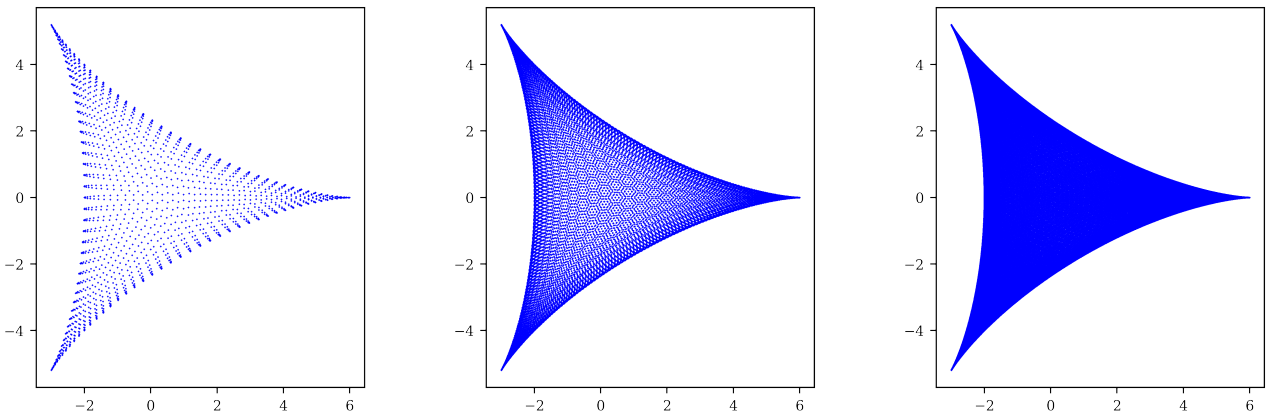
$$\sum_{\substack{x \in \mathbf{Z}/q\mathbf{Z} \\ x^d = 1}} e\left(\frac{ax^2}{q}\right) = \sum_{k=0}^{d-1} e\left(\frac{a\left(w_q^k\right)^2}{q}\right) = \sum_{k=0}^{d-1} e\left(\frac{a\left(w_q^2\right)^k}{q}\right) = \sum_{\substack{x \in \mathbf{Z}/q\mathbf{Z} \\ x^d = 1}} e\left(\frac{ax}{q}\right),$$

that is:

$$\mathrm{G}_q(a,d) = \mathrm{S}_q(a,d).$$

This elementary observation that raising an element of order d to some power n may or may not change its order, depending on the gcd of n and d, is the key observation which led to Proposition 2.20.

Before stating this proposition, let us show on this example what happens when d is even. First, the sums $\mathrm{S}_q(a,d)$ and $\mathrm{K}_q(a,b,d)$ from the previous section are real-valued when d is even, because $x \mapsto -x$ is a permutation of the subgroup of order d. However, this is not the case for the Gauss sums $\mathrm{G}_q(a,d)$. Indeed, if we consider for example the sums restricted to the subgroup of order 6, we obtain the following pictures:



(a) $q = 5479$ (b) $q = 50497$ (c) $q = 250441$

Figure 2.11: The sets $\mathcal{G}_q(-,6)$ and three 6-admissible values of q.

This shows a striking difference with the sums previously studied, because theses sums are not always real-valued. The fact that these sums do not behave as the previous ones is due to the fact that 6 (the order of the subgroup) is not coprime with 2 (the exponent of x which appears in the exponentials). However, the picture suggests that one can relate these sums with the previous sums, because there seems to be equidistribution in a dilated 3-cusp hypocycloid. Indeed, this one seems to be the image of the standard 3-cusp hypocycloid of Figure 2.1 under the homothety with ratio 2.

This is actually the case. Indeed, when d is even, if we keep on denoting by w_q a generator of the unique subgroup of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$, we have that w_q^2 has order $d/2$ thanks to Lemma 2.18. Therefore, if we denote by $\Lambda_d(q)$ the unique subgroup of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$, the group homomorphism

$$\begin{array}{ccc} \Lambda_d(q) & \to & \Lambda_{d/2}(q) \\ x & \mapsto & x^2 \end{array}$$

is surjective, with kernel $\{-1,1\}$. Therefore, any $y \in \Lambda_{d/2}(q)$ has exactly two square roots in $\Lambda_d(q)$, and this implies the following equality:

$$\mathrm{G}_q(a,d) = \sum_{x\in\Lambda_d(q)} e\left(\frac{ax^2}{q}\right) = 2\sum_{y\in\Lambda_{d/2}(q)} e\left(\frac{ay}{q}\right) = 2\mathrm{S}_q(a,d).$$

As the sums $\mathrm{S}_q(a,d)$ on the right-hand side become equidistributed in $\mathbb{H}_3$ as a varies in $\mathbf{Z}/q\mathbf{Z}$ and q goes to infinity, this equality explains why the sets of sums $\mathcal{G}_q(-,d)$ become equidistributed in $2\mathbb{H}_3 = \{2z,\ z\in\mathbb{H}_3\}$ with respect to the pushforward measure of the Haar measure on $(\mathbf{S}^1)^2$ via the Laurent polynomial $2g_3$.

The above examples helped us noticing the fact that the key point towards understanding the distribution of more general sums is the change of order of an element, when raised to a power which is not coprime with its order.

The general result. The first step of the proof of Proposition 2.12 relied a lot on the fact that $\phi_d(w_q^k) = 0$ in $\mathbf{Z}/q\mathbf{Z}$ as soon as w_q^k is a primitive d-th root of unity, which was ensured by taking for w_q an element of order d and k coprime with d. Now, if we allow k to share some prime factors with d, the order of w_q^k may be a strict divisor of d, say d', in which case the relevant cyclotomic polynomial to transpose the argument of the proof of Proposition 2.12 will be $\phi_{d'}$, not ϕ_d. This is the reason why the suitable Laurent polynomials in this setting will be the ones introduced in the following definition.

Definition 2.19. *Let $d \geqslant 1$ and let $\mathbf{m} = (m_1,\dots,m_n) \in \mathbf{Z}^n$. For all $i \in \{1,\dots,n\}$, we denote by*

$$d_i := \frac{d}{(d,m_i)}$$

and by $\left(c_{j,k}^{(i)}\right)_{0\leqslant j<\varphi(d_i)}$ the coefficients that appear in the reduction modulo ϕ_{d_i} of X^k for each k in $\{0,\dots,d-1\}$. In other words, these are the unique integers such that:

$$\forall k \in \{0,\dots,d-1\}, \qquad X^k \equiv \sum_{j=0}^{\varphi(d_i)-1} c_{j,k}^{(i)} X^j \bmod \phi_{d_i}.$$

Then we define the Laurent polynomial $f_{d,\mathbf{m}}$ as follows:

$$\begin{array}{rccc} f_{d,\mathbf{m}} & : & (\mathbf{S}^1)^{\varphi(d_1)+\cdots+\varphi(d_n)} & \to & \mathbf{C} \\ & & ((z_{1,j})_{0\leqslant j<\varphi(d_1)},\dots,(z_{n,j})_{0\leqslant j<\varphi(d_n)}) & \mapsto & \displaystyle\sum_{k=0}^{d-1}\prod_{i=1}^{n}\prod_{j=0}^{\varphi(d_i)-1} z_{i,j}^{c_{j,k}^{(i)}} \end{array} \tag{2.15}$$

We can now give the statement of our second generalization:

Proposition 2.20. *Let $d \geqslant 1$, and let $\mathbf{m} = (m_1,\dots,m_n) \in \mathbf{Z}^n$. The sets of sums*

$$\left\{ \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right);\ (a_1,\dots,a_n)\in(\mathbf{Z}/q\mathbf{Z})^n \right\}$$

become equidistributed in the image of the Laurent polynomial $f_{d,\mathbf{m}}$ (from Definition 2.19) with respect to the pushforward measure via $f_{d,\mathbf{m}}$ of the probability Haar measure on $(\mathbf{S}^1)^{\varphi(d_1)+\cdots+\varphi(d_n)}$, as q tends to infinity among the d-admissible integers.

Remark 2.21. We will see in Section 2.3.3 how the proof of this proposition can be slightly modified to recover Proposition 2.12 when $\mathbf{m}$ is coprime with d.

Proof of Proposition 2.20. 1. *Reduction to a statement on equidistribution modulo* 1*:*

As in the proof of Proposition 2.12, for all d-admissible integer q, we denote by

$$Y_{\mathbf{m},q} := (\mathbf{Z}/q\mathbf{Z})^n$$

and by $\theta_{\mathbf{m},q}\colon Y_{\mathbf{m},q} \to \mathbf{C}$ the map defined by

$$(a_1,\dots,a_n) \mapsto \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right).$$

We also let w_q be a generator of the unique subgroup of order d of $(\mathbf{Z}/q\mathbf{Z})^\times$. Then for all $(a_1,\dots,a_n)\in Y_{\mathbf{m},q}$,

$$\begin{aligned}\theta_{\mathbf{m},q}(a_1,\dots,a_n) &\overset{\text{def}}{=} \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right)\\ &= \sum_{k=0}^{d-1} e\left(\frac{a_1(w_q^k)^{m_1}+\cdots+a_n(w_q^k)^{m_n}}{q}\right)\\ &= \sum_{k=0}^{d-1} e\left(\frac{a_1(w_q^{m_1})^{k}+\cdots+a_n(w_q^{m_n})^{k}}{q}\right)\end{aligned}$$

Now, for all $i\in\{1,\dots,n\}$, $w_q^{m_i}$ has order d_i, hence $\phi_{d_i}(w_q^{m_i})=0$ in $\mathbf{Z}/q\mathbf{Z}$ thanks to Lemma 2.14.

Thus, for all $k\in\{0,\dots,d-1\}$, if one reduces modulo q the congruence:

$$X^k = \sum_{j=0}^{\varphi(d_i)-1} c_{j,k}^{(i)} X^j \bmod \phi_{d_i}$$

and evaluate it at $w_q^{m_i}$, the term $\overline{\phi}_{d_i}(w_q^{m_i})$ is equal to zero, hence:

$$(w_q^{m_i})^k = \sum_{j=0}^{\varphi(d_i)-1} c_{j,k}^{(i)} (w_q^{m_i})^j \text{ in } \mathbf{Z}/q\mathbf{Z}.$$

Therefore:

$$\forall i\in\{1,\dots n\},\ \forall k\in\{0,\dots,d-1\},\qquad (w_q^{m_i})^k = \sum_{j=0}^{\varphi(d_i)-1} c_{j,k}^{(i)} (w_q^{m_i})^j \quad \text{in } \mathbf{Z}/q\mathbf{Z}.$$

Replacing this in the expression of $\theta_{\mathbf{m},q}(a_1,\dots,a_n)$ obtained above, we get:

$$\begin{aligned}\theta_{\mathbf{m},q}(a_1,\dots,a_n) &= \sum_{k=0}^{d-1}\prod_{i=1}^{n} e\left(\frac{a_i(w_q^{m_i})^k}{q}\right)\\ &= \sum_{k=0}^{d-1}\prod_{i=1}^{n}\prod_{j=0}^{\varphi(d_i)-1} e\left(\frac{a_i(w_q^{m_i})^j}{q}\right)^{c_{j,k}^{(i)}}\end{aligned}$$

Therefore, if we define for all $i\in\{1,\dots,n\}$ and for all $j\in\{0,\dots,\varphi(d_i)-1\}$,

$$z_{i,j} = z_{i,j}(a_1,\dots,a_n,q) := e\left(\frac{a_i(w_q^{m_i})^j}{q}\right) \tag{2.16}$$

we have:

$$\theta_{\mathbf{m},q}\left(a_1,\dots,a_n\right) = f_{d,\mathbf{m}}\left((z_{1,j})_{0\leqslant j<\varphi(d_1)},\dots,(z_{n,j})_{0\leqslant j<\varphi(d_n)}\right) \tag{2.17}$$

with the Laurent polynomial $f_{d,\mathbf{m}}$ defined at Definition 2.19 and the $z_{i,j}$'s being elements of $\mathbf{S}^1$. This already shows that the sums $\theta_{\mathbf{m},q}\left(a_1,\dots,a_n\right)$ belongs to the image of $f_{d,\mathbf{m}}$. In order to show that these sums become equidistributed with respect to the pushforward measure of the probability Haar measure on $(\mathbf{S}^1)^{\varphi(d_1)+\cdots+\varphi(d_n)}$, it suffices to show that the following subsets of $(\mathbf{R}/\mathbf{Z})^{\varphi(d_1)+\cdots+\varphi(d_n)}$:

$$\left\{\overbrace{\left(\left(\frac{a_1(w_q^{m_1})^j}{q}\right)_{0\leqslant j<\varphi(d_1)},\dots,\left(\frac{a_n(w_q^{m_n})^j}{q}\right)_{0\leqslant j<\varphi(d_n)}\right)}^{=:\mathbf{x}(a_1,\dots,a_n,q)};\quad (a_1,\dots,a_n)\in(\mathbf{Z}/q\mathbf{Z})^n\right\},$$

become equidistributed modulo 1 as q goes to infinity among the d-admissible integers.

2. *Proof of the equidistribution modulo* 1*:*

We are interested in the equidistribution modulo 1 of the following sets of $(\varphi(d_1)+\cdots+\varphi(d_n))$-tuples:

$$\left\{\mathbf{x}(a_1,\dots,a_n,q);\ (a_1,\dots,a_n)\in(\mathbf{Z}/q\mathbf{Z})^n\right\}, \tag{2.18}$$

with the notation $\mathbf{x}(a_1,\dots,a_n,q)$ from above. By Weyl's criterion (see [78, Theorem 6.2]), these sets become equidistributed modulo 1 if and only if for any $\mathbf{y}=\left(y_0,\dots,y_{\varphi(d_1)+\cdots+\varphi(d_n)-1}\right)\in\mathbf{Z}^{\varphi(d_1)+\cdots+\varphi(d_n)}\setminus\{0\}$, we have the following convergence towards zero:

$$\frac{1}{q^n}\times\sum_{(a_1,\dots,a_n)\in(\mathbf{Z}/q\mathbf{Z})^n} e\left(\mathbf{x}(a_1,\dots,a_n,q)\cdot\mathbf{y}\right)\underset{\substack{q\to\infty\\ q\in\mathcal{A}_d}}{\longrightarrow}0. \tag{2.19}$$

Let us denote by $\mathbf{y}_1$ the vector extracted from $\mathbf{y}$ by taking the first $\varphi(d_1)$ entries, $\mathbf{y}_2$ the vector formed by the next $\varphi(d_2)$ entries and so on:

$$\mathbf{y}_1=(y_0,\dots,y_{\varphi(d_1)-1}),\quad \mathbf{y}_2=(y_{\varphi(d_1)},\dots,y_{\varphi(d_1)+\varphi(d_2)-1})\quad \mathbf{y}_3=\cdots$$

so that $\mathbf{y}=(\mathbf{y}_1,\dots,\mathbf{y}_n)$. We also introduce the following notations to decompose the vector $\mathbf{x}(a_1,\dots,a_n,q)$ in a parallel way:

$$\mathbf{x}_1(a_1,q):=\left(\frac{a_1(w_q^{m_1})^j}{q}\right)_{0\leqslant j<\varphi(d_1)},\dots,\ \mathbf{x}_n(a_n,q):=\left(\frac{a_n(w_q^{m_n})^j}{q}\right)_{0\leqslant j<\varphi(d_n)}$$

Then we have

$$\frac{1}{q^n}\times\sum_{(a_1,\dots,a_n)\in(\mathbf{Z}/q\mathbf{Z})^n} e\left(\mathbf{x}(a_1,\dots,a_n,q)\cdot\mathbf{y}\right)=\prod_{i=1}^{n}\left[\frac{1}{q}\sum_{a_i\in\mathbf{Z}/q\mathbf{Z}} e(\mathbf{x}_i(a_i,q)\cdot\mathbf{y}_i)\right]. \tag{2.20}$$

Now, since $\mathbf{y}\neq 0$, there exists at least one index $i\in\{1,\dots,n\}$ such that $\mathbf{y}_i\neq 0$. For such an i, the factor

$$\frac{1}{q}\sum_{a_i\in\mathbf{Z}/q\mathbf{Z}} e(\mathbf{x}_i(a_i,q)\cdot\mathbf{y}_i) \tag{2.21}$$

tends to 0 as q goes to infinity among the d-admissible integers thanks to Lemma 2.15. Indeed, we have

$$\frac{1}{q}\sum_{a_i\in\mathbf{Z}/q\mathbf{Z}} e(\mathbf{x}_i(a_i,q)\cdot\mathbf{y}_i) = \frac{1}{q}\sum_{a\in\mathbf{Z}/q\mathbf{Z}} e\left(\frac{af_i(w_q^{m_i})}{q}\right),$$

where f_i is the polynomial associated with $\mathbf{y}_i = \left(y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})},\dots,y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})+\varphi(d_i)-1}\right)$ as follows: $f_i = y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})} + y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})+1}X + \cdots + y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})+\varphi(d_i)-1}X^{\varphi(d_i)-1}$. This is a non-zero polynomial with integer coefficients and with degree strictly less than $\varphi(d_i)$, and $w_q^{m_i}$ is an element of order d_i in $(\mathbf{Z}/q\mathbf{Z})^\times$. Thus, we can apply Lemma 2.15 which states that there exists a rank m_{f_i} such that for all $q > m_{f_i}$ such that q is d-admissible,

$$\sum_{a\in\mathbf{Z}/q\mathbf{Z}} e\left(\frac{af_i(w_q^{m_i})}{q}\right) = 0$$

and this proves the convergence of (2.21) towards zero. As all the other factors of (2.20) have absolute value bounded above by 1, the whole product converges to zero, and this concludes the proof.

□

Remark 2.22. The proof shows why it is important to let all the a_i's vary in $\mathbf{Z}/q\mathbf{Z}$, unlike in Proposition 2.12 where we could fix an arbitrary number of them, as long as one varied. Indeed, let us fix an index $j \in \{1,\dots,n\}$. Then if we take $\mathbf{y} = (\mathbf{y}_1,\dots,\mathbf{y}_n) \in \mathbf{Z}^{\varphi(d_1)+\cdots+\varphi(d_n)} \setminus \{0\}$ defined by $\mathbf{y}_i = (0,\dots,0) \in \mathbf{Z}^{\varphi(d_i)}$ for all $i \neq j$ and $\mathbf{y}_j = (1,\dots,1) \in \mathbf{Z}^{\varphi(d_j)}$, then the absolute value of the product (2.20) is equal to the absolute value of the factor corresponding to the index j, since all the other factors are equal to 1. Therefore, to prove the convergence towards zero in Weyl's criterion for this specific vector $\mathbf{y}$, we have no other choice than proving that the factor corresponding to the index j tends to 0. In order to achieve that, we really need to be able to apply Lemma 2.15 to this factor, hence we really need to require that a_j varies in $\mathbf{Z}/q\mathbf{Z}$. As j was arbitrary, this shows that *in general* one cannot fix an arbitrary a_j and let the others vary, as this could prevent the equidistribution from happening. Actually one can be more precise about the conditions under which some parameters may be fixed, while the others vary in $\mathbf{Z}/q\mathbf{Z}$, and this is the content of Remark 2.24 of the following section.

Example 2.23. Let us consider the following sums, for d-admissible values of q:

$$\mathrm{G}_q(a,b,d) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax^2+bx}{q}\right) \text{ with } a,b\in\mathbf{Z}/q\mathbf{Z}.$$

These sums are associated with the vector $\mathbf{m} = (2,1)$ in the notations of Proposition 2.20. If we take $d = 12$, then $\mathbf{m}$ is not coprime with d, so we really need to use the previous proposition rather than Proposition 2.12. What Proposition 2.20 tells us is that the Laurent polynomial involved in the equidistribution result depends on the coefficients of the remainders of the euclidean divisions of the monomials X^k by the cyclotomic polynomials ϕ_{12} and ϕ_6. Indeed, if $w_q \in (\mathbf{Z}/q\mathbf{Z})^\times$ is an element of order 12, then w_q^2 has order 6, so the relation $\phi_6(w_q^2) = 0$ will also come into play. Therefore, we write

$$X^k \equiv \sum_{j=0}^{\varphi(6)-1} c_{j,k}^{(1)} X^j \bmod \phi_6$$

and

$$X^k \equiv \sum_{j=0}^{\varphi(12)-1} c_{j,k}^{(2)} X^j \bmod \phi_{12}.$$

Then, by respectively evaluating these congruences at w_q^2 and w_q and using Lemma 2.14, we obtain

$$w_q^{2k} = \sum_{j=0}^{\varphi(6)-1} c_{j,k}^{(1)} w_q^{2j}$$

and

$$w_q^k = \sum_{j=0}^{\varphi(12)-1} c_{j,k}^{(2)} w_q^j.$$

Thanks to these equalities, one can replace high powers of w_q by lower powers when writing

$$\mathrm{G}_q(a,b,12) = \sum_{k=0}^{11} e\left(\frac{a(w_q^k)^2 + bw_q^k}{q}\right)$$

Using the explicit formulas for ϕ_6 and ϕ_{12} we can calculate the $c_{j,k}^{(1)}$ and the $c_{j,k}^{(2)}$, and this gives the following equality:

$$\begin{aligned}\mathrm{G}_q(a,b,12) = \quad & e\left(\frac{a+b}{q}\right) + e\left(\frac{aw_q^2+bw_q}{q}\right) + e\left(\frac{a(w_q^2-1)+bw_q^2}{q}\right) + e\left(\frac{-a+bw_q^3}{q}\right) \\ & + e\left(\frac{-aw_q^2+b(w_q^2-1)}{q}\right) + e\left(\frac{a(1-w_q^2)+b(w_q^3-w_q)}{q}\right) + e\left(\frac{a-b}{q}\right) \\ & + e\left(\frac{aw_q^2-bw_q}{q}\right) + e\left(\frac{a(w_q^2-1)-bw_q^2}{q}\right) + e\left(\frac{-a-bw_q^3}{q}\right) \\ & + e\left(\frac{-aw_q^2+b(1-w_q^2)}{q}\right) + e\left(\frac{a(1-w_q^2)+b(w_q-w_q^3)}{q}\right).\end{aligned}$$

Thus, $\mathrm{G}_q(a,b,12)$ is a Laurent polynomial in the following 6 variables in $\mathbf{S}^1$:

$$z_{1,0} := e\left(\frac{a}{q}\right),\ z_{1,1} := e\left(\frac{aw_q^2}{q}\right),\ z_{2,0} := e\left(\frac{b}{q}\right),\ z_{2,1} := e\left(\frac{bw_q}{q}\right),\ z_{2,2} := e\left(\frac{bw_q^2}{q}\right),\ z_{2,3} := e\left(\frac{bw_q^3}{q}\right)$$

Indeed, we have shown that:

$$\begin{aligned}\mathrm{G}_q(a,b,12) = \quad & z_{1,0}z_{2,0} + z_{1,1}z_{2,1} + \frac{z_{1,1}z_{2,2}}{z_{1,0}} + \frac{z_{2,3}}{z_{1,0}} + \frac{z_{2,2}}{z_{1,1}z_{2,0}} + \frac{z_{1,0}z_{2,3}}{z_{1,1}z_{2,1}} + \frac{z_{1,0}}{z_{2,0}} + \frac{z_{1,1}}{z_{2,1}} \\ & + \frac{z_{1,1}}{z_{1,0}z_{2,2}} + \frac{1}{z_{1,0}z_{2,3}} + \frac{z_{2,0}}{z_{1,1}z_{2,2}} + \frac{z_{1,0}z_{2,1}}{z_{1,1}z_{2,3}}.\end{aligned}$$

Proposition 2.20 states that the sets of sums

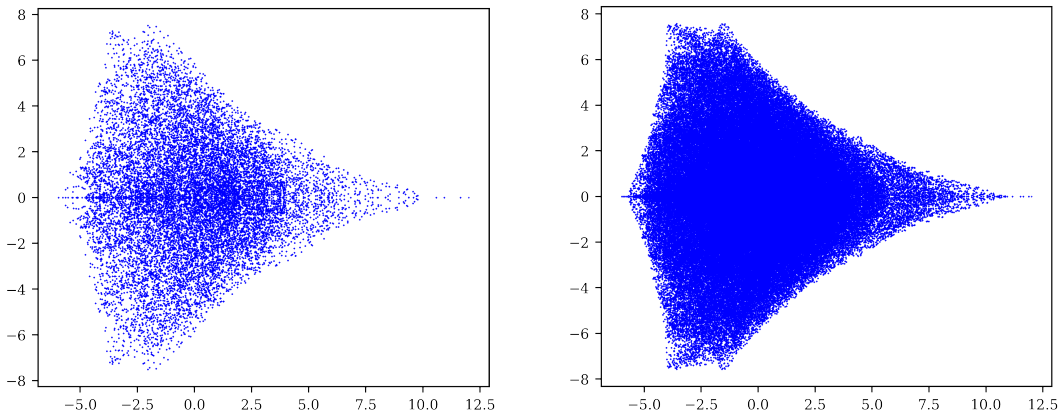
$$\mathcal{G}_q(-,-,12) = \left\{\mathrm{G}_q(a,b,12);\ (a,b) \in (\mathbf{Z}/q\mathbf{Z})^2\right\}$$

become equidistributed in the image of $(\mathbf{S}^1)^6$ via the Laurent polynomial above, with respect to the pushforward measure of the Haar measure on $(\mathbf{S}^1)^6$. The result comes from the fact that the sets

$$\left\{\left(e\left(\frac{a}{q}\right), e\left(\frac{aw_q^2}{q}\right), e\left(\frac{b}{q}\right), e\left(\frac{bw_q}{q}\right), e\left(\frac{bw_q^2}{q}\right), e\left(\frac{bw_q^3}{q}\right)\right);\ (a,b) \in (\mathbf{Z}/q\mathbf{Z})^2\right\}$$

become equidistributed in $(\mathbf{S}^1)^6$ as q goes to infinity among the 12-admissible integers.

The following picture illustrates the equidistribution of the sets $\mathcal{G}_q(-,-,12)$. However, it does not seem easy to describe the region of equidistribution in other terms than as the image of $(\mathbf{S}^1)^6$ under a complicated-looking Laurent polynomial. A description in terms of geometrically meaningful shapes such as hypocycloids or Minkowski sums of known geometric objects would certainly be very satisfactory, but we did not succeed in obtaining them in this particular case. Appendix 2.A is an exposition of some cases where we were able to describe the region of equidistribution for the sums $\mathrm{G}_q(a,b,d)$.



(a) $q = 433$ (b) $q = 1297$

Figure 2.12: The sets $\mathcal{G}_q(-,-,12)$ for two 12-admissible values of q.

2.3.3. Comparison between the two cases

Proposition 2.20 does not exclude the case where $\mathbf{m}$ is coprime with d. Therefore, it is natural to ask whether it gives the same equidistribution result as Proposition 2.12 in this case. In fact, when the m_i are all coprime with d, all d_i are equal to d, and so we use a single cyclotomic polynomial to do all the euclidean divisions of X^k needed in the proof of Proposition 2.20: the polynomial ϕ_d. Indeed, for any $i \in \{1,\dots,n\}$, $w_q^{m_i}$ is of order d, so we can use the relation $\phi_d(w_q^{m_i})$ to deduce the number of powers of $w_q^{m_i}$ that we must take into account to ensure equidistribution. Thus, for all $i \in \{1,\dots,n\}$, the sequence of $c_{j,k}^{(i)}$ is the same as the sequence of $c_{j,k}^{(1)}$, and we will simply denote it by $(c_{j,k})$. Then, in the rewriting of $\theta_{\mathbf{m},q}(a_1,\dots,a_n)$ in the form

$$\sum_{k=0}^{d-1}\prod_{i=1}^{n}\prod_{j=0}^{\varphi(d_i)-1} e\left(\frac{a_i(w_q^{m_i})^j}{q}\right)^{c_{j,k}^{(i)}} = \sum_{k=0}^{d-1}\prod_{i=1}^{n}\prod_{j=0}^{\varphi(d)-1} e\left(\frac{a_i(w_q^{m_i})^j}{q}\right)^{c_{j,k}}$$

we can interchange the product on i and the product on j to obtain:

$$\theta_{\mathbf{m},q}(a_1,\dots,a_n) = \sum_{k=0}^{d-1}\prod_{j=0}^{\varphi(d)-1} e\left(\frac{a_1(w_q^{m_1})^j + \cdots + a_n(w_q^{m_n})^j}{q}\right)^{c_{j,k}}.$$

In this form, this is exactly what appears in the proof of Proposition 2.12, and we can finish the proof the same way. The gain of this rewriting is strong: we pass from a Laurent polynomial in $n\varphi(d)$ variables to a Laurent polynomial in $\varphi(d)$ variables. The fact that the Laurent polynomial is simpler sometimes makes it easier to interpret geometrically the region inside which the sums become equidistributed.

Moreover, in the proof of the Proposition 2.20, we had to split the vector $\mathbf{y}$ of Weyl's criterion into "sections" $(\mathbf{y}_0,\dots,\mathbf{y}_n)$ because we had to handle differently the terms associated with different m_i, due to the fact that the $w_q^{m_i}$ do not necessarily have the same order. As a consequence of the fact that an index i such that $\mathbf{y}_i \neq 0$ can be any $i \in \{1,\dots,n\}$ as $\mathbf{y}$ varies in $\mathbf{Z}^{n\varphi(d)}$, we had to assume that all the parameters a_i varied in all $\mathbf{Z}/q\mathbf{Z}$. In the case where all m_i are coprime with d, there is no longer any need to make this splitting, and so we can fix some a_i and only let the others vary in $\mathbf{Z}/q\mathbf{Z}$.

Remark 2.24. In the previous paragraph, we did nothing more than group together the terms $w_q^{m_i}$ that were of the same order (namely: all of order d). I think that, in general, one can reduce the dimension of the torus underlying the equidistribution result of Proposition 2.20 by grouping together the terms $w_q^{m_i}$ that are of the same order in $(\mathbf{Z}/q\mathbf{Z})^\times$. This is rather tedious to write in the general setting, so I have chosen to explain this claim on an example which I hope will be quite convincing. Consider sums of the type

$$\mathrm{Q}(a,b,c,q,d) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax^4+bx^2+cx}{q}\right) \text{ for } a,b,c \in \mathbf{Z}/q\mathbf{Z}$$

and let us say that we are interested in the case $d=6$. If w_q denotes a generator of the unique subgroup of order 6 of $(\mathbf{Z}/q\mathbf{Z})^\times$ (which exists if we restrict to 6-admissible values of q), then w_q^2 and w_q^4 are both of order 3. The powers of w_q^2 and w_q^4 that occur in the equidistribution modulo 1 therefore stop at the same rank $(\varphi(3)-1)$ and the same coefficients $c_{j,k}$ give the relations between the larger powers and the smaller powers. Explicitly, the $c_{j,k}$ are defined by congruences:

$$X^k \equiv \sum_{j=0}^{\varphi(3)-1} c_{j,k} X^j \bmod \phi_3.$$

We will also use the coefficients $d_{j,k}$ defined by the congruences:

$$X^k \equiv \sum_{j=0}^{\varphi(6)-1} d_{j,k} X^j \bmod \phi_6$$

Following the method of proof of the Proposition 2.20 we arrive at the following rewriting:

$$\mathrm{Q}(a,b,c,q,d) = \sum_{k=0}^{6-1} \left[\prod_{j=0}^{\varphi(3)-1} e\left(\frac{a(w_q^4)^j}{q}\right)^{c_{j,k}}\right] \left[\prod_{j=0}^{\varphi(3)-1} e\left(\frac{b(w_q^2)^j}{q}\right)^{c_{j,k}}\right] \left[\prod_{j=0}^{\varphi(6)-1} e\left(\frac{cw_q^j}{q}\right)^{d_{j,k}}\right] \tag{2.22}$$

Viewing the above expression as the evaluation of a Laurent polynomial in 6 variables in

$$e\left(\frac{a(w_q^4)^0}{q}\right), e\left(\frac{a(w_q^4)^1}{q}\right), e\left(\frac{b(w_q^2)^0}{q}\right), e\left(\frac{b(w_q^2)^1}{q}\right), e\left(\frac{cw_q^0}{q}\right), e\left(\frac{cw_q^1}{q}\right)$$

we then show that the sums $\mathrm{Q}(a,b,c,q,d)$ become equidistributed in the image of this Laurent polynomial when a,b,c range over $\mathbf{Z}/q\mathbf{Z}$ and q tends to $+\infty$. This result comes from the uniform distribution in $(\mathbf{S}^1)^6$ of the sets:

$$\left\{\left(e\left(\frac{a(w_q^4)^0}{q}\right), e\left(\frac{a(w_q^4)^1}{q}\right), e\left(\frac{b(w_q^2)^0}{q}\right), e\left(\frac{b(w_q^2)^1}{q}\right), e\left(\frac{cw_q^0}{q}\right), e\left(\frac{cw_q^1}{q}\right)\right);\ (a,b,c)\in(\mathbf{Z}/q\mathbf{Z})^3\right\}$$

as q goes to infinity. But in fact, we can bring down the dimension of the torus underlying the equidistribution phenomenon by grouping the terms in w_q^2 and w_q^4. Indeed, these two elements being of the same order, we used the same cyclotomic polynomial (here ϕ_3) to reduce the number of powers of these elements that we have to keep. So we have the same sequence of $c_{j,k}$ for these terms, as we see in the equality (2.22) above. So we can write:

$$\mathrm{Q}(a,b,c,q,d) = \sum_{k=0}^{6-1} \left[\prod_{j=0}^{\varphi(3)-1} e\left(\frac{a(w_q^4)^j + b(w_q^2)^j}{q}\right)^{c_{j,k}}\right] \left[\prod_{j=0}^{\varphi(6)-1} e\left(\frac{cw_q^j}{q}\right)^{d_{j,k}}\right]$$

and this time we see $\mathrm{Q}(a,b,c,q,d)$ as the image of the vector

$$\left(e\left(\frac{a(w_q^4)^0 + b(w_q^2)^0}{q}\right), e\left(\frac{a(w_q^4)^1 + b(w_q^2)^1}{q}\right), e\left(\frac{cw_q^0}{q}\right), e\left(\frac{cw_q^1}{q}\right)\right) \in (\mathbf{S}^1)^4$$

by a Laurent polynomial. Moreover, the sets

$$\left\{\left(e\left(\frac{a(w_q^4)^0 + b(w_q^2)^0}{q}\right), e\left(\frac{a(w_q^4)^1 + b(w_q^2)^1}{q}\right), e\left(\frac{cw_q^0}{q}\right), e\left(\frac{cw_q^1}{q}\right)\right);\ (a,b,c)\in(\mathbf{Z}/q\mathbf{Z})^3\right\}$$

become uniformly distributed in $(\mathbf{S}^1)^4$. To show this, we apply once again Weyl's criterion to prove the uniform distribution modulo 1 of the arguments inside the exponentials. Let $\mathbf{y} = (y_0, \ldots, y_3) \in \mathbf{Z}^4 \backslash \{0\}$. Let $f(X) := y_0 + y_1 X$ and $g(X) := y_2 + y_3 X$. We want to show that

$$\frac{1}{q^3} \sum_{a,b,c \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{af(w_q^4) + bf(w_q^2) + cg(w_q)}{q}\right) \underset{q \to +\infty}{\longrightarrow} 0$$

Now splitting the sum in terms of a, b and c turns it into:

$$\frac{1}{q} \sum_{a \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{af(w_q^4)}{q}\right) \times \frac{1}{q} \sum_{b \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{bf(w_q^2)}{q}\right) \times \frac{1}{q} \sum_{c \in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{cg(w_q)}{q}\right)$$

and either f is non-zero, in which case the first two terms tend to 0, or g is non-zero, in which case it is the last term that tends to 0. In either case, the product tends to 0 because each term has a modulus less than or equal to 1.
Let us note in passing that the same phenomenon as in the Proposition 2.12 appears: we can fix a and let b vary, or conversely, it will always tend towards 0, as long as we leave a free parameter before w_q^2 or w_q^4.

To summarize the general fact illustrated by this example, we can say that if several m_i are such that the corresponding d_i are equal, i.e. such that the $w_q^{m_i}$ have the same order, then they can be grouped together to reduce the dimension of the underlying torus, and the equidistribution result will remain true with a slightly simpler Laurent polynomial and fewer variables. Moreover, among these m_i that we group, we can choose to fix an arbitrary number of the corresponding a_i, as long as we let one vary freely, equidistribution will hold. Somewhat informally, we can therefore group the $w_q^{m_i}$ by "teams" according to their order, and we need at least one free a_i parameter per team, the others being allowed to be fixed arbitrarily without changing the uniform distribution result.

2.A. Some extra cases where a geometric description of the region of equidistribution can be obtained

As in Example 2.23, we consider the sums

$$\mathrm{G}_q(a,b,d) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax^2+bx}{q}\right) \text{ with } a,b\in\mathbf{Z}/q\mathbf{Z}.$$

When d is of the form $2r$ with r being a positive odd integer, we can obtain a geometric description of the region of equidistribution of the sets $\mathcal{G}_q(-,-,d) := \left\{\mathrm{G}_q(a,b,d);\ (a,b)\in(\mathbf{Z}/q\mathbf{Z})^2\right\}$. This means that we are able to describe the region of equidistribution in more concrete terms than as the image of some multi-dimensional torus via some Laurent polynomial. We also obtain such a concrete description in the case where $d=2^\beta$, with $\beta\geqslant 2$.

2.A.1. Sums associated with $\mathbf{m}=(2,1)$ and d of the form $2r$ with r odd

In order to state the result, we will need the following notation.

Definition 2.25. *Let r be a positive odd integer. We still denote by g_r the Laurent polynomial defined at Definition 2.6. Then we define the following Laurent polynomial:*

$$\begin{array}{rccc} g_r\oplus g_r & : & (\mathbf{S}^1)^{2\varphi(r)} & \to & \mathbf{C} \\ & & (z_j)_{0\leqslant j\leqslant 2\varphi(r)-1} & \mapsto & g_r(z_0,\dots,z_{\varphi(r)-1})+g_r(z_{\varphi(r)},\dots,z_{2\varphi(r)-1}) \end{array}$$

Let us stress that since the image of g_r has been geometrically interpreted in some cases (see Lemma 2.9 and Proposition 2.10), the image of $g_r\oplus g_r$ also admits a concrete geometric description in those cases, in terms of hypocycloids and Minkowski sums of hypocycloids.

With this notation, we can prove the following proposition.

Proposition 2.26. *Let r be a positive odd integer. Consider the sets*

$$\mathcal{G}_q(-,-,2r) := \left\{ \mathrm{G}_q(a,b,2r) := \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^{2r}=1}} e\left(\frac{ax^2+bx}{q}\right);\ a,b\in\mathbf{Z}/q\mathbf{Z} \right\}$$

for $2r$-admissible values of q. Then, as q goes to infinity, the sets $\mathcal{G}_q(-,-,2r)$ become equidistributed in the image of $(\mathbf{S}^1)^{2\varphi(r)}$ via $g_r\oplus g_r$ with respect to the pushforward measure of the probability Haar measure on $(\mathbf{S}^1)^{2\varphi(r)}$.

Proof. Let q be a $2r$-admissible integer, and let $a,b\in\mathbf{Z}/q\mathbf{Z}$.

1. *Reordering the terms.*
   As in the previous proofs, we let $w_q\in(\mathbf{Z}/q\mathbf{Z})^\times$ denote a generator of the unique subgroup of order $2r$ of $(\mathbf{Z}/q\mathbf{Z})^\times$, and we rewrite $\mathrm{G}_q(a,b,2r)$ in terms of this generator. This gives:

   $$\mathrm{G}_q(a,b,2r) = \sum_{k=0}^{2r-1} e\left(\frac{aw_q^{2k}+bw_q^k}{q}\right).$$

   Then, we split the sum into two parts, depending on the parity of k:

   $$\begin{aligned} \mathrm{G}_q(a,b,2r) &= \sum_{\substack{k=0\\ k\text{ even}}}^{2r-1} e\left(\frac{aw_q^{2k}+bw_q^k}{q}\right) + \sum_{\substack{k=0\\ k\text{ odd}}}^{2r-1} e\left(\frac{aw_q^{2k}+bw_q^k}{q}\right) \\ &= \sum_{m=0}^{r-1} e\left(\frac{aw_q^{4m}+bw_q^{2m}}{q}\right) + \sum_{m=0}^{r-1} e\left(\frac{aw_q^{4m+2}+bw_q^{2m+1}}{q}\right) \\ &=: \mathrm{G}_{\text{even}} + \mathrm{G}_{\text{odd}}. \end{aligned}$$

2. *Each term ($\mathrm{G}_{\mathrm{even}}$ and $\mathrm{G}_{\mathrm{odd}}$) belongs to the image of g_r.*

   For all $m \in \{0, \dots, r-1\}$, we perform the reduction modulo ϕ_r of X^m and denote the coefficients that appear by $c_{j,m}$ as in Definition 2.6:

$$X^m = \sum_{j=0}^{\varphi(r)-1} c_{j,m} X^j \bmod \phi_r.$$

   Then we reduce modulo q and evaluate at w_q^4 and w_q^2 (which are both elements of $(\mathbf{Z}/q\mathbf{Z})^\times$ of order r, so that Lemma 2.14 applies). This gives:

$$\begin{cases} w_q^{4m} = \sum_{j=0}^{\varphi(r)-1} c_{j,m} w_q^{4j} \\ w_q^{2m} = \sum_{j=0}^{\varphi(r)-1} c_{j,m} w_q^{2j}. \end{cases}$$

   Note that this step relies crucially on the fact that r is odd, otherwise w_q^4 would have an order which is half of that of w_q^2.

   We deduce that

$$\mathrm{G}_{\mathrm{even}} = \sum_{m=0}^{r-1} \prod_{j=0}^{\varphi(r)-1} e\left(\frac{a w_q^{4j} + b w_q^{2j}}{q}\right)^{c_{j,m}} \text{ et } \mathrm{G}_{\mathrm{odd}} = \sum_{m=0}^{r-1} \prod_{j=0}^{\varphi(r)-1} e\left(\frac{a w_q^{4j+2} + b w_q^{2j+1}}{q}\right)^{c_{j,m}}$$

   Therefore, if we introduce the notations

$$y_j := e\left(\frac{a w_q^{4j} + b w_q^{2j}}{q}\right) \text{ and } z_j := e\left(\frac{a w_q^{4j+2} + b w_q^{2j+1}}{q}\right),$$

   and

$$\mathbf{y} = (y_j)_{0 \leqslant j < \varphi(r)} \text{ and } \mathbf{z} = (z_j)_{0 \leqslant j < \varphi(r)},$$

   we have

$$\mathrm{G}_q(a, b, 2r) = \mathrm{G}_{\mathrm{even}} + \mathrm{G}_{\mathrm{odd}} = g_r(\mathbf{y}) + g_r(\mathbf{z}) = (g_r \oplus g_r)(\mathbf{y}, \mathbf{z})$$

   Therefore, $\mathrm{G}_q(a, b, 2r)$ belongs to the image of $g_r \oplus g_r$.

3. *Equidistribution of $\mathcal{G}_q(-, -, 2r)$ as q goes to infinity.*
   In order to prove that there is equidistribution with respect to the pushforward measure announced in the statement, we need to prove that the sets

$$\left\{ \left(\left(e\left(\frac{a w_q^{4j} + b w_q^{2j}}{q}\right)\right)_{0 \leqslant j < \varphi(r)}, \left(e\left(\frac{a w_q^{4j+2} + b w_q^{2j+1}}{q}\right)\right)_{0 \leqslant j < \varphi(r)} \right) ;\ (a, b) \in (\mathbf{Z}/q\mathbf{Z})^2 \right\}$$

   becomes equidistributed in $(\mathbf{S}^1)^{2\varphi(r)}$.
   Now, when j ranges over $\{0, \dots, \varphi(r) - 1\}$, $2j$ ranges over the even integers between 0 and $2\varphi(r) - 2$, whereas $2j + 1$ ranges over the odd integers between 1 and $2\varphi(r) - 1$. Thus, by reordering the components, it is equivalent to prove that the following sets become equidistributed in $(\mathbf{S}^1)^{2\varphi(r)}$:

$$\left\{ \left(e\left(\frac{a w_q^{2k} + b w_q^{k}}{q}\right)\right)_{0 \leqslant k \leqslant 2\varphi(r)-1} ;\ (a, b) \in (\mathbf{Z}/q\mathbf{Z})^2 \right\}.$$

   We do that using Weyl's criterion. Let $\mathbf{y} \in \mathbf{Z}^{2\varphi(r)} \setminus \{0\}$. Denoting by $\theta_q(a, b)$ the vector

$$\left(\frac{a w_q^{2k} + b w_q^{k}}{q}\right)_{0 \leqslant k < 2\varphi(r)} \in (\mathbf{R}/\mathbf{Z})^{2\varphi(r)}$$

we want to prove that the following exponential sum

$$\frac{1}{q^2}\sum_{a,b\in\mathbf{Z}/q\mathbf{Z}} e(\theta_q(a,b)\cdot\mathbf{y})$$

converges to 0 as q goes to infinity. If we write the coordinates of $\mathbf{y}$ as follows

$$\mathbf{y}=\begin{pmatrix} y_0 \\ \vdots \\ y_{2\varphi(r)-1}\end{pmatrix}$$

then we have

$$\frac{1}{q^2}\sum_{a,b\in\mathbf{Z}/q\mathbf{Z}} e(\theta_q(a,b)\cdot\mathbf{y}) = \frac{1}{q^2}\sum_{a,b\in\mathbf{Z}/q\mathbf{Z}} e\left(\frac{af(w_q^2)+bf(w_q)}{q}\right),$$

where

$$f := y_0 + y_1X + y_2X^2 + \cdots + y_{2\varphi(r)-1}X^{2\varphi(r)-1} \in \mathbf{Z}[X]\setminus\{0\}.$$

Now since $\psi_q\colon (a,b)\mapsto e\left(\frac{af(w_q^2)+bf(w_q)}{q}\right)$ is an additive character of $(\mathbf{Z}/q\mathbf{Z})^2$, we have, by orthogonality of characters,

$$\frac{1}{q^2}\sum_{a,b\in\mathbf{Z}/q\mathbf{Z}} e\left(\frac{af(w_q^2)+bf(w_q)}{q}\right) = \mathbb{1}_{\psi_q=\text{triv.}} \tag{2.23}$$

Moreover, ψ_q is the trivial character if and only if $f(w_q^2)$ and $f(w_q)$ are equal to 0 modulo q. Indeed, the group homomorphism

$$\widehat{\mathbf{Z}/q\mathbf{Z}}\times\widehat{\mathbf{Z}/q\mathbf{Z}} \;\to\; \widehat{(\mathbf{Z}/q\mathbf{Z})^2}$$

which maps (χ_1,χ_2) to the character of $(\mathbf{Z}/q\mathbf{Z})^2$:

$$(a,b)\mapsto\chi_1(a)\chi_2(b)$$

is an isomorphism. Thus, ψ_q is trivial if and only if the additive characters modulo q

$$a\mapsto e\left(\frac{f(w_q^2)}{q}a\right) \text{ and } b\mapsto e\left(\frac{f(w_q)}{q}b\right)$$

are both trivial. Therefore, in order to conclude, it suffices to show that there are only finitely many $2r$-admissible values of q such that $f(w_q)$ and $f(w_q^2)$ are simultaneously equal to zero modulo q. This is what we prove below. The main idea of the proof is to try to reduce to a situation similar to the one encountered in the proof of Lemma 2.15, which is why we try to reduce to polynomials of degree strictly less than $\varphi(r)$.

(a) *ϕ_r and ϕ_{2r} do not simultaneously divide $f(X)$.*
Indeed, ϕ_r and ϕ_{2r} are two distinct irreducible polynomials in $\mathbf{Q}[X]$, so if they both divided $f(X)$, then their product would divide $f(X)$ as well. Since f is non-zero, this would imply

$$\deg(f)\geqslant\deg(\phi_r)+\deg(\phi_{2r})=2\varphi(r),$$

contradicting the fact that $\deg(f)\leqslant 2\varphi(r)-1$.

(b) *Reduction to the case of polynomials of degree strictly less than $\varphi(r)$ through euclidean division.*

Since ϕ_r and ϕ_{2r} are monic polynomials in $\mathbf{Z}[X]$, the polynomials that appear in the euclidean divisions below still belong to $\mathbf{Z}[X]$:

$$\begin{cases} f(X) = \phi_r(X)Q_r(X) + R_r(X), & 0 \leqslant \deg(R_r) < \varphi(r) \\ f(X) = \phi_{2r}(X)Q_{2r}(X) + R_{2r}(X), & 0 \leqslant \deg(R_{2r}) < \varphi(2r) = \varphi(r) \end{cases}$$

Then we reduce these equalities modulo q and evaluate the first one at w_q^2, and the second one at w_q. As w_q has multiplicative order equal to $2r$, the term $\overline{\phi}_{2r}(w_q)$ is equal to zero in $\mathbf{Z}/q\mathbf{Z}$ thanks to Lemma 2.14. Similarly, the term $\overline{\phi}_r(w_q^2)$ is equal to zero in $\mathbf{Z}/q\mathbf{Z}$, because w_q^2 has order r. Thus,

$$f(w_q^2) \equiv 0 \bmod q \quad \text{and} \quad f(w_q) \equiv 0 \bmod q \tag{2.24}$$

if and only if

$$R_r(w_q^2) \equiv 0 \bmod q \quad \text{and} \quad R_{2r}(w_q) \equiv 0 \bmod q. \tag{2.25}$$

Now, thanks to step (a) above, at least one of the two polynomials R_r and R_{2r} is non-zero, so we can apply the argument of the proof of Lemma 2.15 (based on a Bézout relation between R_r and ϕ_r, respectively R_{2r} and ϕ_{2r}) to conclude that there are only finitely many q such that (2.25) is satisfied. Thanks to the equivalence with (2.24), this shows that the sum (2.23) is eventually equal to zero, and this finishes the proof.

□

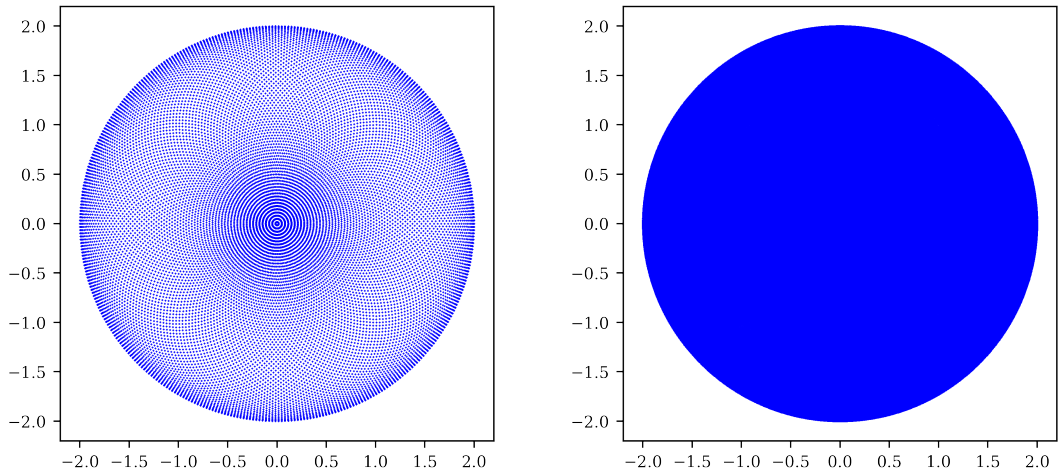
Example 2.27. • If we take $d = 2 = 2 \times 1$, then the sets $\mathcal{G}_q(-,-,2)$ become equidistributed in the image of $g_1 \oplus g_1$. Now, since $\phi_1 = X - 1$, it is easy to show that

$$\begin{array}{rccc} g_1 & : & \mathbf{S}^1 & \to & \mathbf{C} \\ & & z & \mapsto & z \end{array}$$

hence

$$\begin{array}{rccc} g_1 \oplus g_1 & : & (\mathbf{S}^1)^2 & \to & \mathbf{C} \\ & & (z_1, z_2) & \mapsto & z_1 + z_2 \end{array}$$

Thus, the image of $g_1 \oplus g_1$ is the closed disk with center 0 and radius 2.

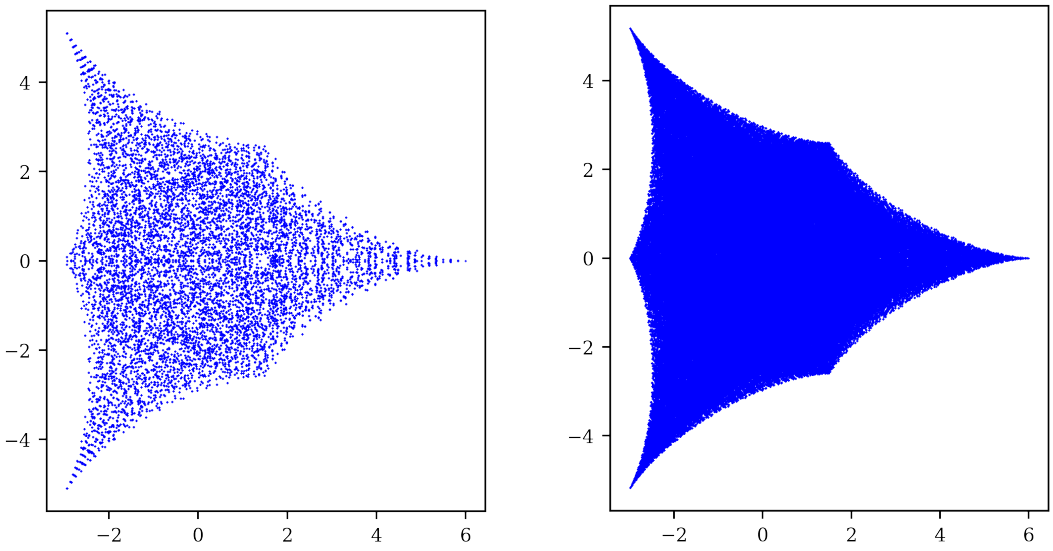


(a) $q = 193$ (b) $q = 709$

Figure 2.13: The sets $\mathcal{G}_q(-,-,2)$ for two 2-admissible values of q.

- If we take $d = 6 = 2\times 3$, Proposition 2.26 tells us that the sets $\mathcal{G}_q(-,-,6)$ become equidistributed in the image of $g_3 \oplus g_3$, that is: in $\mathbb{H}_3 + \mathbb{H}_3$ thanks to Lemma 2.9. Equidistribution holds with respect to the pushforward measure of the Haar measure on $(\mathbf{S}^1)^4$ via

$$\begin{array}{rccc} g_3 \oplus g_3 & : & (\mathbf{S}^1)^4 & \to & \mathbf{C} \\ & & (z_0, \ldots, z_3) & \mapsto & z_0 + z_1 + \frac{1}{z_0 z_1} + z_2 + z_3 + \frac{1}{z_2 z_3} \end{array}$$



(a) $q = 229$ (b) $q = 1021$

Figure 2.14: The sets $\mathcal{G}_q(-,-,6)$ for two 6-admissible values of q.

Proposition 2.26 covers the cases where $d = 2r$ for odd values of r. It remains to study what happens when d is of the form $2^\beta r$ with $\beta \geqslant 2$ and r odd. We were not able to find a concrete geometric description of the image of the Laurent polynomial in all of those remaining cases, but the next section presents what we obtained in the case where d is a power of 2.

2.A.2. Sums associated with $\mathbf{m} = (2,1)$ and d of the form 2^β with $\beta \geqslant 2$

We have the following geometric description of the region of equidistribution for the sums $\mathrm{G}_q\left(a, b, 2^\beta\right)$.

Proposition 2.28. *Let $\beta \in \mathbf{Z}_{\geqslant 2}$ and let $d := 2^\beta$. The sets $\mathcal{G}_q(-,-,d)$ become equidistributed in the Minkowski sum*

$$\sum_{j=0}^{2^{\beta-2}-1} \mathbb{H}_4 = \underbrace{\mathbb{H}_4 + \cdots + \mathbb{H}_4}_{2^{\beta-2}\ terms}$$

with respect to the pushforward measure of the Haar measure on $(\mathbf{S}^1)^{3\times 2^{\beta-2}}$ via $h_4 \oplus \cdots \oplus h_4$, where

$$\begin{array}{rccc} h_4 & : & (\mathbf{S}^1)^3 & \to & \mathbf{C} \\ & & (z_1, z_2, z_3) & \mapsto & z_1 + z_2 + z_3 + \frac{1}{z_1 z_2 z_3} \end{array}$$

As usual, equidistribution holds as q goes to infinity among the d-admissible integers.

Proof. Let q be a d-admissible integer and let $a, b \in \mathbf{Z}/q\mathbf{Z}$.

1. *Reordering the terms.*

Denoting by w_q a generator of the subgroup of order d of $(\mathbf{Z}/q\mathbf{Z})^\times$, we have:

$$\begin{aligned}\mathrm{G}_q(a,b,d) &= \sum_{k=0}^{d-1} e\left(\frac{aw_q^{2k}+bw_q^k}{q}\right)\\ &= \sum_{j=0}^{2^{\beta-2}-1} \sum_{\substack{k=0\\ k\equiv j \bmod 2^{\beta-2}}}^{d-1} e\left(\frac{aw_q^{2k}+bw_q^k}{q}\right)\\ &= \sum_{j=0}^{2^{\beta-2}-1} \underbrace{\sum_{m=0}^{3} e\left(\frac{aw_q^{2(j+m2^{\beta-2})}+bw_q^{j+m2^{\beta-2}}}{q}\right)}_{=:\mathrm{G}_j}\end{aligned}$$

2. *Each G_j belongs to $\mathbb{H}_4$.*
Let $j \in \{0,\dots,2^{\beta-2}-1\}$. In order to prove that G_j belongs to $\mathbb{H}_4$, we prove that the term corresponding to $m=3$ is equal to the inverse of the product of the terms associated with $m=0,1,2$. It is sufficient to show that the following equalities hold in $\mathbf{Z}/q\mathbf{Z}$:

$$\begin{cases} w_q^{2(j+0\times 2^{\beta-2})} + w_q^{2(j+1\times 2^{\beta-2})} + w_q^{2(j+2\times 2^{\beta-2})} = -w_q^{2(j+3\times 2^{\beta-2})} \\ w_q^{j+0\times 2^{\beta-2}} + w_q^{j+1\times 2^{\beta-2}} + w_q^{j+2\times 2^{\beta-2}} = -w_q^{j+3\times 2^{\beta-2}}. \end{cases}$$

These are equivalent to:

$$\begin{cases} 1 + w_q^{2^{\beta-1}} + w_q^{2^\beta} = -w_q^{3\times 2^{\beta-1}} \\ 1 + w_q^{2^{\beta-2}} + w_q^{2^{\beta-1}} = -w_q^{3\times 2^{\beta-2}} \end{cases}$$

because one can simplify the first equality by w_q^{2j} and the second one by w_q^j (these are both invertible modulo q since w_q is invertible). Now, both equalities hold because as w_q has order $d=2^\beta$, $w_q^{2^{\beta-1}}$ has order 2, hence $w_q^{2^{\beta-1}}=-1$. Thus, each G_j belongs to the image of h_4, which is the hypocycloid $\mathbb{H}_4$ thanks to Lemma 2.9.

3. *Equidistribution of $\mathcal{G}_q(-,-,d)$ as q goes to infinity.*

To conclude the proof, it remains to show that the exponential that are mapped to $\mathrm{G}_q(a,b,d)$ via $h_4\oplus\cdots\oplus h_4$ become equidistributed in $(\mathbf{S}^1)^{3\times 2^{\beta-2}}$. Precisely, the previous step showed that

$$\begin{aligned}\mathrm{G}(a,b,q,d) &= \sum_{j=0}^{2^{\beta-2}-1} \mathrm{G}_j\\ &= \sum_{j=0}^{2^{\beta-2}-1} h_4\left(e\left(\frac{aw_q^{2j}+bw_q^j}{q}\right), e\left(\frac{aw_q^{2(j+2^{\beta-2})}+bw_q^{j+2^{\beta-2}}}{q}\right), e\left(\frac{aw_q^{2(j+2^{\beta-1})}+bw_q^{j+2^{\beta-1}}}{q}\right)\right)\end{aligned}$$

hence it remains to prove that the sets

$$\left\{ \left(e\left(\frac{aw_q^{2(j+m2^{\beta-2})}+bw_q^{j+m2^{\beta-2}}}{q}\right)\right)_{0\leqslant j\leqslant 2^{\beta-2}-1,\ m\in\{0,1,2\}} \ ;\ (a,b)\in(\mathbf{Z}/q\mathbf{Z})^2 \right\}$$

become equidistributed in $(\mathbf{S}^1)^{3\times 2^{\beta-2}}$ as q goes to infinity among the d-admissible integers. By reordering the factors (instead of regrouping them by congruence classes) this amounts to showing the uniform distribution modulo 1 of the following subsets of $(\mathbf{R}/\mathbf{Z})^{3\times 2^{\beta-2}}$:

$$\left\{\left(\frac{aw_q^{2k}+bw_q^k}{q}\right)_{0\leqslant k<3\times 2^{\beta-2}}\ ;\ (a,b)\in(\mathbf{Z}/q\mathbf{Z})^2\right\}$$

Through Weyl's criterion, it is equivalent to show that if $f\in\mathbf{Z}[X]\setminus\{0\}$ is a polynomial of degree less than or equal to $3\times 2^{\beta-2}-1$, then we have

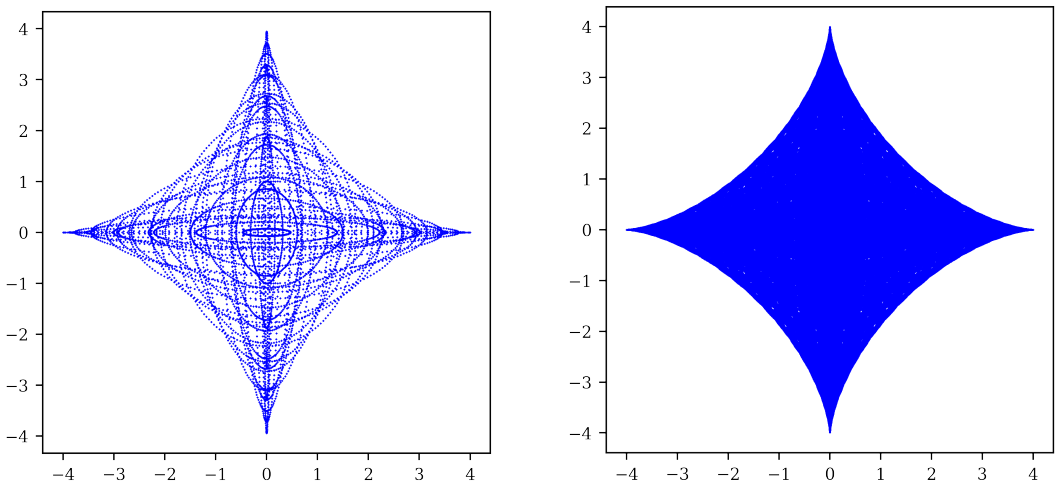
$$\frac{1}{q^2}\sum_{a,b\in\mathbf{Z}/q\mathbf{Z}} e\left(\frac{af(w_q^2)+bf(w_q)}{q}\right) \underset{\substack{q\to\infty\\ q\ d\text{-adm}}}{\longrightarrow} 0$$

By the same argument as in the proof of Proposition 2.26, one can prove that there are only finitely many d-admissibles integers q such that $f(\tilde{w}_q^2)$ and $f(\tilde{w}_q)$ are both equal to zero modulo q. Indeed, the key argument of the proof was the fact that ϕ_d and $\phi_{d/2}$ cannot simultaneously divide f, and this is still the case here, since

$$\deg(\phi_d\phi_{d/2})=\varphi(2^\beta)+\varphi(2^{\beta-1})=3\times 2^{\beta-2}>\deg(f).$$

□

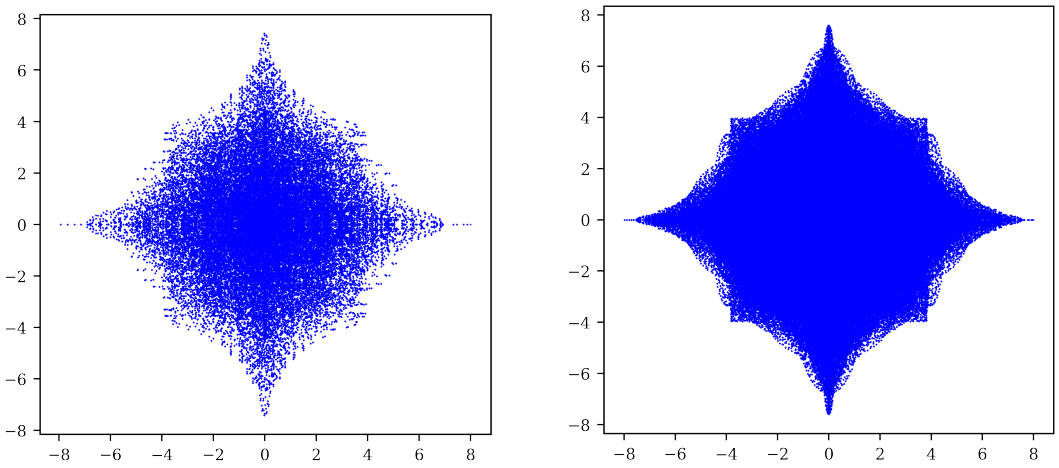
Example 2.29. • First we illustrate the equidistribution of the sets $\mathcal{G}_q(-,-,4)$ in $\mathbb{H}_4$:



(a) $q=173$ (b) $q=1193$

Figure 2.15: The sets $\mathcal{G}_q(-,-,4)$ for two 4-admissible values of q.

• Second, we illustrate the equidistribution of the sets $\mathcal{G}_q(-,-,8)$ in $\mathbb{H}_4+\mathbb{H}_4$:



(a) $q = 577$ (b) $q = 1777$

Figure 2.16: The sets $\mathcal{G}_q(-,-,8)$ for two 8-admissible values of q.

Proposition 2.26 and Proposition 2.28 do not cover all possible values of d, so there is still work to do to gain a better geometric understanding of the region of equidistribution for sums of the type $\mathrm{G}_q(a,b,d)$ when d is an arbitrary positive integer.

2.B. On the discrepancy in Myerson's lemma

In this appendix, we give a non-trivial upper bound for the discrepancy associated with the equidistribution result known as Myerson's lemma:

Lemma 2.30 ([32, Lemma 6.2]). *The sets*

$$\left\{\frac{a}{q}\left(1, w_q, w_q^2, \dots, w_q^{\varphi(d)-1}\right);\ a \in \mathbf{Z}/q\mathbf{Z}\right\}$$

become equidistributed modulo 1 *as* q *goes to infinity among the* d*-admissible integers.*

Proof. The proof of this lemma is an immediate consequence of Weyl's criterion and of the exponential sum estimate of Lemma 2.15. □

In our study of the discrepancy, we will restrict to prime moduli p for our approach to work. We prove that the discrepancy is bounded above, up to multiplicative constants, by an explicit negative power of p.

I wish to thank Gérald Tenenbaum for suggesting me to try to apply Erdös-Turán inequality to turn the fast decay of the Weyl sums into good discrepancy estimates. I also wish to thank Igor Shparlinski for the unpublished note he sent me which contained useful ideas.

We will also come back to these questions regarding the discrepancy in our equidistribution results in a more general setting in Chapter 5.

2.B.1. A short refresher on resultants

Let A be an integral domain, and let $f = a_m X^m + \cdots + a_0$ and $g = b_n X^n + \cdots + b_0$ be two polynomials with coefficients in A and such that $a_m \neq 0$ and $b_n \neq 0$.
Let $K := \mathrm{Frac}(A)$, and let F be the K-linear map:

$$\begin{array}{rccc} F & : & K_{n-1}[X] \times K_{m-1}[X] & \to & K_{n+m-1}[X] \\ & & (u, v) & \mapsto & uf + vg \end{array}$$

Definition 2.31. *Let* $\mathcal{B}$ *be the basis* $((X^{n-1}, 0), \dots, (1, 0), (0, X^{m-1}), \dots, (0, 1))$ *of* $K_{n-1}[X] \times K_{m-1}[X]$ *and let* $\mathcal{C}$ *be the basis* $(X^{n+m-1}, \dots, 1)$ *of* $K_{n+m-1}[X]$*. Then the Sylvester matrix of* f *and* g *is the matrix* $\mathrm{M}_{\mathcal{B},\mathcal{C}}(F) \in \mathcal{M}_{n+m}(A)$*. The determinant of this matrix is called the resultant of* f *anf* g*, and is denoted by* $\mathrm{Res}(f, g)$*. Since the Sylvester matrix has coefficients in* A*, the resultant of* f *and* g *is an element of* A*.*

One interest of the resultant is that it is an element of A, which can be computed with the sole knowledge of the coefficients of f and g, but it detects common roots of f and g in some extension of K. Indeed, we have the following proposition:

Proposition 2.32. *The following are equivalent:*

1. *The polynomials* f *and* g *have a common irreducible factor of degree* $\geqslant 1$ *in* $K[X]$
2. *There exists a field extension* L/K *in which* f *and* g *have a common root*
3. $\mathrm{Res}(f, g) = 0$.

2.B.2. A lemma essentially due to I. Shparlinski

Definition 2.33. *For $\mathbf{m} = (m_0, \dots, m_{n-1}) \in \mathbf{Z}^n$, we denote by*

- $\|\mathbf{m}\|_2 := \sqrt{\sum_{j=0}^{n-1} m_j^2}$ *its classical ℓ^2-norm,*
- $f_{\mathbf{m}} := \sum_{j=0}^{n-1} m_j X^j \in \mathbf{Z}[X]$ *the polynomial whose coefficients are the entries of $\mathbf{m}$.*

Lemma 2.34. *Let $d \geqslant 1$, and let $\mathbf{m} = \big(m_0, \dots, m_{\varphi(d)-1}\big) \in \mathbf{Z}^{\varphi(d)} \setminus \{0\}$. For all $p \equiv 1 \bmod d$, let w_p denote a primitive d^{th} root of unity in $\mathbf{F}_p$. Then we have the following implication:*
if $f_{\mathbf{m}}(w_p) \equiv 0 \bmod p$, then $\|\mathbf{m}\|_2 \geqslant C_d \times p^{\frac{1}{\varphi(d)}}$, where C_d is a constant depending only on d.

Proof. Let us denote by $k := \max\{0 \leqslant j < \varphi(d),\ m_j \neq 0\}$ (so that $f_{\mathbf{m}}$ has degree exactly k). The Sylvester matrix of ϕ_d and $f_{\mathbf{m}}$ consists of k columns containing the coefficients of ϕ_d plus some zero entries, followed by $\varphi(d)$ columns containing the coefficients of $f_{\mathbf{m}}$ plus some zero entries. Thus, if we apply Hadamard's bound to the determinant of this matrix (which states that the absolute value of the determinant is bounded above by the product of the ℓ^2-norms of the columns), we obtain the following:

$$|\mathrm{Res}(\phi_d, f_{\mathbf{m}})| \leqslant B_d^k \|\mathbf{m}\|_2^{\varphi(d)} \leqslant B_d^{\varphi(d)-1} \|\mathbf{m}\|_2^{\varphi(d)} \tag{2.26}$$

where $B_d = \sqrt{\sum_{j=0}^{\varphi(d)} a_j^2}$ if $\phi_d = \sum_{j=0}^{\varphi(d)} a_j X^j$ (so this constant depends only on d, and can be made more explicit when ϕ_d is well-known, for instance when d is prime). We found the idea of using Hadamard's bound in [9, Theorem 7], where it was used for the same purpose of giving estimates on resultants.

Now, if $f_{\mathbf{m}}(w_p) \equiv 0 \bmod p$ then since we also know that $\phi_d(w_p) \equiv 0 \bmod p$, we obtain that $\mathrm{Res}(\phi_d, f_{\mathbf{m}}) \equiv 0 \bmod p$ thanks to Proposition 2.32 applied in the field $\mathbf{F}_p$. Moreover, as $f_{\mathbf{m}}$ is non-zero and has degree $< \varphi(d)$, it is coprime with ϕ_d. Therefore, thanks to Proposition 2.32 (this time applied in the field $\mathbf{Q}$): $\mathrm{Res}(\phi_d, f_{\mathbf{m}}) \neq 0$. Also, $\mathrm{Res}(\phi_d, f_{\mathbf{m}})$ is an integer since ϕ_d and $f_{\mathbf{m}}$ have integer coefficients. Thus, $\mathrm{Res}(\phi_d, f_{\mathbf{m}})$ is a non-zero integer which is divisible by p, hence $|\mathrm{Res}(\phi_d, f_{\mathbf{m}})| \geqslant p$. Combining this with (2.26) gives the inequality

$$p \leqslant B_d^{\varphi(d)-1} \|\mathbf{m}\|_2^{\varphi(d)}$$

from which the result follows. We thank Igor Shparlinski for communicating to us a note which made use of this argument of reduction modulo p of a non-zero resultant. □

2.B.3. Application to the control of the discrepancy in Myerson's lemma

In the proof of Lemma 2.15, the Weyl sums coming from the application of Weyl's criterion not only *converge* to zero, but are *eventually equal to* 0. Gérald Tenenbaum suggested to us that this very strong convergence towards zero should enable us to deduce a non-trivial estimate on the decay of the discrepancy, via Erdös-Turán-Koksma inequality. In the remainder of this appendix, we follow his suggestion and prove a non-trivial upper bound on the discrepancy. But before that, let us introduce the necessary notations.

Definition 2.35. *Let $d \geqslant 1$ be an integer, and let $\mathbf{x}_1, \dots, \mathbf{x}_N \in (\mathbf{R}/\mathbf{Z})^d$. We define the discrepancy of $\mathbf{x}_1, \dots, \mathbf{x}_N$ as follows:*

$$D(\mathbf{x}_1, \dots, \mathbf{x}_N) := \sup_{I \in \mathscr{I}} \left| \frac{1}{N} \sum_{j=1}^{N} \mathbb{1}_I(\mathbf{x}_j) - \lambda_d(I) \right|$$

where $\mathscr{I}$ denotes the set of products of intervals $[a_1, b_1] \times \cdots \times [a_d, b_d]$ of $(\mathbf{R}/\mathbf{Z})^d$ and λ_d denotes the probability Haar measure on $(\mathbf{R}/\mathbf{Z})^d$.

It is well known that a sequence $(\mathbf{x}_j)_{j \geqslant 1}$ becomes equidistributed modulo 1 if and only if $D(\mathbf{x}_1, \ldots, \mathbf{x}_N)$ converges to zero as N goes to infinity. The Erdös-Turán-Koksma inequality gives an upper bound which allows one to evaluate the decay of the discrepancy in terms of the Weyl sums. We state it almost as in [28, Lemma 3.4] (see also [29, Theorem 1.21]).

Lemma 2.36 (Erdös-Turán-Koksma)**.** *Let $d \geqslant 1$ be an integer. There exists a constant C such that for any $N \geqslant 1$, for any $\mathbf{x}_1, \ldots, \mathbf{x}_N \in (\mathbf{R}/\mathbf{Z})^d$, and any $H > 0$,*

$$D(\mathbf{x}_1, \ldots, \mathbf{x}_N) \leqslant C \left(\frac{1}{H} + \sum_{\substack{\mathbf{m} \in \mathbf{Z}^d \\ 0 < \|\mathbf{m}\|_\infty < H}} \frac{1}{r(\mathbf{m})} \left| \frac{1}{N} \sum_{j=1}^{N} e\left(\mathbf{m} \cdot \mathbf{x}_j\right) \right| \right)$$

where $r(\mathbf{m}) = \prod_{i=1}^{d} \max(1, |m_i|)$.

In the setting of Lemma 2.15 above, we will apply this estimate with $N = p$ and the sequence

$$\mathbf{x}_0(p), \mathbf{x}_1(p), \ldots, \mathbf{x}_{p-1}(p)$$

where

$$\mathbf{x}_a(p) = \left(\frac{a w_p^0}{p}, \frac{a w_p^1}{p}, \ldots, \frac{a w_p^{\varphi(d)-1}}{p} \right) \in (\mathbf{R}/\mathbf{Z})^{\varphi(d)}$$

for all $a \in \{0, \ldots, p-1\}$.

Definition 2.37. *We denote the discrepancy of the $\mathbf{x}_a(p)$ as follows:*

$$D_p := D(\mathbf{x}_0(p), \mathbf{x}_1(p), \ldots, \mathbf{x}_{p-1}(p)) = \sup_{I \in \mathscr{I}} \left| \frac{1}{p} \sum_{a=0}^{p-1} \mathbb{1}_I(\mathbf{x}_a(p)) - \lambda_{\varphi(d)}(I) \right|$$

where $\mathscr{I}$ denotes the set of products of intervals as in Definition 2.35 and $\lambda_{\varphi(d)}$ denotes the probability Haar measure on $(\mathbf{R}/\mathbf{Z})^{\varphi(d)}$.

Proposition 2.38. *For all $d \geqslant 1$, we have that for all $p \equiv 1 \bmod d$,*

$$D_p \ll_d p^{-\frac{1}{\varphi(d)}}$$

Proof. By Lemma 2.36, we have that for all $p \equiv 1 \bmod d$, for all $H > 0$,

$$D_p \leqslant C \left(\frac{1}{H} + \sum_{\substack{\mathbf{m} \in \mathbf{Z}^{\varphi(d)} \\ 0 < \|\mathbf{m}\|_\infty < H}} \frac{1}{r(\mathbf{m})} \left| \frac{1}{p} \sum_{a=0}^{p-1} e\left(\mathbf{m} \cdot \mathbf{x}_a(p)\right) \right| \right), \tag{2.27}$$

where C is a constant which depends only on d. Now let C_d be a constant as in Lemma 2.34 and choose H as

$$H := \frac{C_d}{\sqrt{\varphi(d)}} p^{\frac{1}{\varphi(d)}}.$$

If $\mathbf{m} \in \mathbf{Z}^{\varphi(d)}$ is such that $0 < \|m\|_\infty < H$, then $0 < \|\mathbf{m}\|_2 \leqslant \sqrt{\varphi(d)} \|\mathbf{m}\|_\infty < C_d \times p^{\frac{1}{\varphi(d)}}$. Thus, by Lemma 2.34, we have $f_{\mathbf{m}}(w_p) \not\equiv 0 \bmod p$, and this implies that the Weyl sum

$$\frac{1}{p} \sum_{a=0}^{p-1} e\left(\mathbf{m} \cdot \mathbf{x}_a(p)\right)$$

is equal to zero by orthogonality, because this sum is actually equal to

$$\frac{1}{p}\sum_{a=0}^{p-1} e\left(\frac{f_{\mathbf{m}}(w_p)}{p}a\right).$$

Thus, the second term on the right-hand side of (2.27) is equal to zero with this choice of H, so we obtain

$$D_p \leqslant \frac{C}{H} \leqslant \frac{C\sqrt{\varphi(d)}}{C_d} p^{-\frac{1}{\varphi(d)}} \ll_d p^{-\frac{1}{\varphi(d)}}$$

□

Remark 2.39. Actually Lemma 2.15 also holds more generally for classes modulo p^α for any $\alpha \geqslant 1$. However, it is not clear whether the approach used here can give good bounds on the discrepancy in the case $\alpha \geqslant 2$. Indeed, we used properties of the resultant, and I do not know whether the resultant still satisfies the properties we used when the base ring is $\mathbf{Z}/p^\alpha\mathbf{Z}$ (which is not even an integral domain).

Remark 2.40. In his note, I. Shparlinski was studying a much more general case where d is not fixed, but is allowed to grow with p. If one can obtain the kind of estimate of the end of the proof of Proposition 2.38 with a relatively good understanding of the dependancy with respect to d, this could lead to a range of growth of d with respect to p, for which Myerson's lemma would still hold. This would have consequences on equidistribution of exponential sums indexed by subgroups whose cardinality *grows with* p, that is sums of the type:

$$\sum_{\substack{x\in\mathbf{F}_p \\ x^{d(p)}=1}} e\left(\frac{ax}{p}\right), \quad a \in \mathbf{F}_p$$

where $d(p)$ should probably satisfy a condition preventing it from growing too fast with respect to p.

Chapter 3

Restricting the parameters to range over small subgroups

In this chapter, we prove that in the results of Chapter 2, it is possible to impose strong restrictions on the set of parameters and still obtain equidistribution. More precisely, we show that one can restrict the parameters indexing our families of exponential sums to range over small subgroups of $(\mathbf{Z}/q\mathbf{Z})^\times$, instead of allowing them to range over the whole additive group $\mathbf{Z}/q\mathbf{Z}$. Our main result (Theorem 3.13, which corresponds to Theorem A of [103]) is indeed concerned with sets of sums of the form

$$\left\{ \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right);\ (a_1,\dots,a_n)\in H_q^{(1)}\times\cdots\times H_q^{(n)}\right\}, \tag{3.1}$$

where the $H_q^{(i)}$ are sufficiently large (in a sense which will be more precisely stated) subgroups of $(\mathbf{Z}/q\mathbf{Z})^\times$. These extensions make use of very strong estimates on exponential sums over multiplicative subgroups, which were proved to be connected to deep sum-product theorems in additive combinatorics.

Contents

3.1. Motivation

The proofs of Proposition 2.12 and Proposition 2.20 relied crucialy on Lemma 2.15 (Myerson's lemma). We made the choice to state this lemma in terms of exponential sums, because there are several slightly different results on equidistribution modulo 1 which can be deduced from this single fact on exponential sums. However, in [32, Lemma 6.2], Myerson's lemma is stated directly as an equidistribution result, and it asserts that if w_q denotes a primitive d-th root of unity modulo q, then the subsets of $(\mathbf{R}/\mathbf{Z})^{\varphi(d)}$

$$\left\{\frac{a}{q}\left(1,w_q,\dots,w_q^{\varphi(d)-1}\right);\ a\in\mathbf{Z}/q\mathbf{Z}\right\}$$

become equidistributed modulo 1 as q goes to infinity among the d-admissible integers.

The striking fact about the proof is that when applying Weyl's criterion, they do not only get convergence towards zero, but they obtain Weyl sums which are *eventually equal to zero*, thanks to the

orthogonality of characters (this is the content of Lemma 2.15). Since the convergence towards zero is so strong, it is natural to ask whether the liberty of the parameter a can be restricted while keeping the equidistribution property. For instance, one could want to study the question of the equidistribution modulo 1 of the sets

$$\left\{\frac{a}{q}\left(1, w_q, \dots, w_q^{\varphi(d)-1}\right);\ a \in (\mathbf{Z}/q\mathbf{Z})^\times\right\}.$$

Then, the sums involved when applying Weyl's criterion are controlled by the following lemma:

Lemma 3.1. *Let $d \geqslant 1$ be an integer, and let $f \in \mathbf{Z}[X] \setminus \{0\}$ be a polynomial of degree strictly less than $\varphi(d)$. Then there exists a rank n_f such that for all d-admissible integer q, for any element w_q of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$:*

$$\left|\sum_{a\in(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{af(w_q)}{q}\right)\right| \leqslant 1.$$

Proof. As in the proof of Lemma 2.15, we start by choosing a Bézout relation between ϕ_d and f:

$$a(X)\phi_d(X) + b(X)f(X) = n \tag{3.2}$$

where $a, b \in \mathbf{Z}[X]$ and $n \geqslant 1$. Now, let $q = p^\alpha$ be a d-admissible integer such that $q > n^2$, and let w_q be as in the statement. We have:

$$\sum_{a\in(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{af(w_q)}{q}\right) = \sum_{a\in\mathbf{Z}/q\mathbf{Z}} e\left(\frac{af(w_q)}{q}\right) - \sum_{a\in(\mathbf{Z}/q\mathbf{Z})\setminus(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{af(w_q)}{q}\right).$$

Now, we know from Lemma 2.15 that the complete sum $\sum_{a\in\mathbf{Z}/q\mathbf{Z}} e\left(\frac{af(w_q)}{q}\right)$ is eventually equal to zero. More precisely, the proof shows that as soon as $q > n$, the complete sum is equal to zero. Since we are assuming that $q > n^2$, this condition is satisfied, hence:

$$\sum_{a\in(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{af(w_q)}{q}\right) = -\sum_{a\in(\mathbf{Z}/q\mathbf{Z})\setminus(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{af(w_q)}{q}\right).$$

Now, we have:

$$\begin{aligned}\sum_{a\in(\mathbf{Z}/q\mathbf{Z})\setminus(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{af(w_q)}{q}\right) &= \sum_{\substack{a=0\\(a,q)\neq 1}}^{q-1} e\left(\frac{af(w_q)}{q}\right) = \sum_{\substack{a=0\\p|a}}^{q-1} e\left(\frac{af(w_q)}{q}\right)\\ &= \sum_{m=0}^{p^{\alpha-1}-1} e\left(\frac{pmf(w_q)}{p^\alpha}\right) = \sum_{m=0}^{p^{\alpha-1}-1} e\left(\frac{mf(w_q)}{p^{\alpha-1}}\right),\end{aligned}$$

Let us distinguish between the two following cases:

- If $\alpha = 1$, then
$$\sum_{m=0}^{p^{\alpha-1}-1} e\left(\frac{mf(w_q)}{p^{\alpha-1}}\right) = 1,$$
so that
$$\sum_{a\in(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{af(w_q)}{q}\right) = -1.$$
- If $\alpha \geqslant 2$, then we handle the sum
$$\sum_{m=0}^{p^{\alpha-1}-1} e\left(\frac{mf(w_q)}{p^{\alpha-1}}\right)$$

as in the proof of Lemma 2.15, that is: using the orthogonality of characters of $\mathbf{Z}/p^{\alpha-1}\mathbf{Z}$. Indeed, we recognize the sum over all $\mathbf{Z}/p^{\alpha-1}\mathbf{Z}$ of the values of the additive character:

$$m \mapsto e\left(\frac{f(w_q)}{p^{\alpha-1}}m\right)$$

and so the orthogonality of characters tells us that:

$$\sum_{m=0}^{p^{\alpha-1}-1} e\left(\frac{f(w_q)}{p^{\alpha-1}}m\right) = \begin{cases} 0 & \text{if } p^{\alpha-1} \nmid f(w_q) \\ p^{\alpha-1} & \text{if } p^{\alpha-1} \mid f(w_q) \end{cases} \tag{3.3}$$

Now, as in the proof of Lemma 2.15, we can use the relation

$$a(\tilde{w}_q)\phi_d(\tilde{w}_q) + b(\tilde{w}_q)f(\tilde{w}_q) \equiv n \bmod q \tag{3.4}$$

deduced from (3.2), where $\tilde{w}_q$ denotes any lift of w_q in $\mathbf{Z}$. Then thanks to Lemma 2.14, we have that $q = p^\alpha$ divides $\phi_d(\tilde{w}_q)$, so $\phi_d(\tilde{w}_q)$ is a fortiori divisible by $p^{\alpha-1}$.

Thus, if we assume for a contradiction that $p^{\alpha-1}$ divides $f(\tilde{w}_q)$, then $p^{\alpha-1}$ would divide n, but this is impossible. Indeed, $q = p^\alpha > n^2$, so $p^{\alpha/2} > n$, and since $\alpha \geqslant 2$, we have $p^{\alpha-1} \geqslant p^{\alpha/2}$, which implies that $p^{\alpha-1} > n$.
Therefore, $p^{\alpha-1}$ does not divide $f(\tilde{w}_q)$, and the sum:

$$\sum_{m=0}^{p^{\alpha-1}-1} e\left(\frac{mf(\tilde{w}_q)}{p^{\alpha-1}}\right)$$

is equal to zero by orthogonality.

Conclusion: We proved that we can take for instance the integer n_f of the statement to be n^2 (where n comes from (3.2)), and that for all d-admissible integer $q = p^\alpha > n_f$, we have:

$$\left|\sum_{a\in(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{af(w_q)}{q}\right)\right| = \begin{cases} 1 & \text{if } \alpha = 1 \\ 0 & \text{if } \alpha \geqslant 2 \end{cases}$$

This shows that in any case, if $q \in \mathcal{A}_d$ is strictly larger than n_f, then: $\left|\sum_{a\in(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{af(w_q)}{q}\right)\right| \leqslant 1$. □

Now if we use Weyl's criterion, we see that the bound proved in this Lemma 3.1 establishes the equidistribution modulo 1 of the sets

$$\left\{\frac{a}{q}\left(1, w_q, \ldots, w_q^{\varphi(d)-1}\right);\ a \in (\mathbf{Z}/q\mathbf{Z})^\times\right\}.$$

More generally, using Lemma 3.1 instead of Lemma 2.15 in the proofs of propositions 2.12 and 2.20 allows one to prove the equidistribution modulo 1 of the sets

$$\left\{\mathbf{x}(a_1, \ldots, a_n, q);\ (a_1, \ldots, a_n) \in \left((\mathbf{Z}/q\mathbf{Z})^\times\right)^n\right\}$$

instead of that of the sets (2.18):

$$\left\{\mathbf{x}(a_1, \ldots, a_n, q);\ (a_1, \ldots, a_n) \in (\mathbf{Z}/q\mathbf{Z})^n\right\}.$$

It follows from this improvement that the equidistribution results of propositions 2.12 and 2.20 still hold if we only let the parameters vary in $(\mathbf{Z}/q\mathbf{Z})^\times$ instead of $\mathbf{Z}/q\mathbf{Z}$. This gives equidistribution results for sets of the form

$$\left\{ \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right);\ (a_1,\dots,a_n)\in\left((\mathbf{Z}/q\mathbf{Z})^\times\right)^n \right\}$$

We do not give a precise statement at this point because these results will be superseded in the two next sections. Nethertheless, this serves as a motivation for further improvements, because if there is equidistribution when the parameters vary in all $\mathbf{Z}/q\mathbf{Z}$, but also when they only vary in $(\mathbf{Z}/q\mathbf{Z})^\times$, we can wonder how strong can the restrictions be before these sets no longer become equidistributed. This is why we asked ourselves the question: what happens if the parameters a_i are only allowed to range over subgroups H_q of $(\mathbf{Z}/q\mathbf{Z})^\times$? Of course if $H_q=\{1\}$, there is no hope, but what if $|H_q|$ tends to infinity as q goes to infinity? Is it sufficient to ensure the equidistribution of

$$\left\{ \sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{ax}{q}\right);\ a\in H_q \right\} \tag{3.5}$$

for instance? This is the type of question we are going to address in the two next sections.

3.2. Subgroups of cardinality at least $\sqrt{q}$

In this section, we use estimates on Gauss sums (the necessary facts on these are recalled in Appendix 3.A) to prove an exponential sum estimate which enables us to deduce the equidistribution modulo 1 of the sets

$$\left\{ \frac{a}{q}\left(1,w_q,\dots,w_q^{\varphi(d)-1}\right);\ a\in H_q \right\} \tag{3.6}$$

as soon as the subgroups H_q are satisfy the growth condition:

$$\frac{\sqrt{q}}{|H_q|}\underset{q\to\infty}{\longrightarrow}0. \tag{3.7}$$

In other words, equidistribution is guaranteed provided the cardinality of the subgroup H_q grow faster than $\sqrt{q}$, in the sense of condition (3.7). Via the same step of *reduction to a statement on equidistribution modulo* 1 as in the proof of Proposition 2.12, this kind of result allows us to deduce equidistribution theorems for sets of exponential sums of type (3.5), or generalizations of these.

Exponential sum estimates. The key exponential sum estimate is given in the following lemma.

Lemma 3.2. *Let $d\geqslant 1$ and let $f\in\mathbf{Z}[X]\setminus\{0\}$ be a polynomial of degree strictly less than $\varphi(d)$. For all d-admissible integer q, we choose a subgroup H_q of $(\mathbf{Z}/q\mathbf{Z})^\times$ and an element w_q of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$. Then:*
there exists a rank N_f (depending on f) such that for all q in $\mathcal{A}_d$ such that $q>N_f$,

$$\left|\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right)\right| \ll_f \sqrt{q}$$

Remark 3.3. The bound given in this lemma is non-trivial when the subgroup H_q of $(\mathbf{Z}/q\mathbf{Z})^\times$ is sufficiently large, namely when $|H_q|$ is larger than $\sqrt{q}$ (up to the hidden constant in the notation $\ll_f$).

Before moving forward to the full proof, let us give a brief overview of it, to underline where there is a subtlety.

Overview of the proof of Lemma 3.2. The approach is the one described in the introduction of [79], but generalized to $(\mathbf{Z}/q\mathbf{Z})^\times$ instead of $\mathbf{F}_p^\times$. The first idea is to decompose the map:

$$\begin{array}{rccc} \psi_{f(w_q)} & : & (\mathbf{Z}/q\mathbf{Z})^\times & \to & \mathbf{C} \\ & & a & \mapsto & e\left(\frac{f(w_q)a}{q}\right) \end{array}$$

in the orthonormal basis of $\mathbf{Maps}((\mathbf{Z}/q\mathbf{Z})^\times, \mathbf{C})$ made of the multiplicative characters modulo q. Indeed, the $\mathbf{C}$-vector space of the maps from $(\mathbf{Z}/q\mathbf{Z})^\times$ to $\mathbf{C}$ can be endowed with the following hermitian product:

$$\forall f, g\colon (\mathbf{Z}/q\mathbf{Z})^\times \to \mathbf{C}, \quad \langle f, g\rangle := \frac{1}{\varphi(q)} \sum_{x\in(\mathbf{Z}/q\mathbf{Z})^\times} f(x)\overline{g(x)},$$

and it can be shown that the multiplicative characters modulo q form an orthonormal basis of this hermitian space. Therefore, for any map $\varphi\colon (\mathbf{Z}/q\mathbf{Z})^\times \to \mathbf{C}$, we have:

$$\varphi = \sum_\chi \langle \varphi, \chi\rangle \chi$$

where χ runs over the group of multiplicative characters modulo q. In particular, for $\varphi = \psi_{f(w_q)}$, we obtain:

$$\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right) = \sum_{a\in H_q} \psi_{f(w_q)}(a) = \sum_{a\in H_q}\sum_\chi \langle \psi_{f(w_q)}, \chi\rangle \chi(a)$$

Now, $\langle \psi_{f(w_q)}, \chi\rangle$ is almost a Gauss sum (see Appendix 3.A for the notation $\tau(\text{-},\text{-})$ for Gauss sums). Indeed,

$$\langle \psi_{f(w_q)}, \chi\rangle = \frac{1}{\varphi(q)} \sum_{x\in(\mathbf{Z}/q\mathbf{Z})^\times} \psi_{f(w_q)}(x)\overline{\chi(x)} = \frac{1}{\varphi(q)} \tau\left(\overline{\chi}, \psi_{f(w_q)}\right),$$

hence

$$\begin{aligned} \sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right) &= \sum_{a\in H_q}\sum_\chi \frac{1}{\varphi(q)} \tau\left(\overline{\chi}, \psi_{f(w_q)}\right) \chi(a) \\ &= \frac{1}{\varphi(q)} \sum_\chi \tau\left(\overline{\chi}, \psi_{f(w_q)}\right) \sum_{a\in H_q} \chi(a). \end{aligned}$$

Now, among the multiplicative characters modulo q, all those who induce (by restriction) a non-trivial character of H_q have no contribution. Indeed, for such characters, the inner sum is zero by orthogonality of the multiplicative characters of H_q. Thus,

$$\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right) = \frac{1}{\varphi(q)} \sum_{\chi_{|H_q}=1} \tau\left(\overline{\chi}, \psi_{f(w_q)}\right) \sum_{a\in H_q} \chi(a)$$

where the first sum is indexed by the multiplicative characters modulo q which are trivial on H_q. For such characters, the inner sum $\sum_{a\in H_q} \chi(a)$ is simply equal to $|H_q|$ (its number of terms).
Therefore,

$$\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right) = \frac{|H_q|}{\varphi(q)} \sum_{\chi_{|H_q}=1} \tau\left(\overline{\chi}, \psi_{f(w_q)}\right) = \frac{|H_q|}{\varphi(q)} \sum_{\chi_{|H_q}=1} \tau\left(\chi, \psi_{f(w_q)}\right) \tag{3.8}$$

Note that this last sum has $\varphi(q)/|H_q|$ terms. Indeed, more generally if G is a finite abelian group and H is a subgroup of G, then any character of H can be extended to a character of G. In other words, the restriction morphism:

$$\begin{array}{ccc} \widehat{G} & \to & \widehat{H} \\ \chi & \mapsto & \chi_{|H} \end{array}$$

is surjective. In our setting, $G = (\mathbf{Z}/q\mathbf{Z})^\times$ and $H = H_q$, and the surjectivity of the restriction morphism allows us to compute the cardinality of its kernel, which is exactly the number of χ modulo q satisfying $\chi_{|H_q} = 1$. Finally, by the triangle inequality, we have:

$$\left| \sum_{a \in H_q} e\left(\frac{af(w_q)}{q}\right) \right| \leqslant \frac{|H_q|}{\varphi(q)} \sum_{\chi_{|H_q}=1} |\tau\left(\chi, \psi_{f(w_q)}\right)| \tag{3.9}$$

The end of the proof consists in proving that we can apply this classical bound on Gauss sums (up to some multiplicative constant which does not cause any issue):

$$|\tau\left(\chi, \psi_{f(w_q)}\right)| \leqslant \sqrt{q}. \tag{3.10}$$

Indeed, if we could apply this bound for all χ, inequality (3.9) would immediately give:

$$\left| \sum_{a \in H_q} e\left(\frac{af(w_q)}{q}\right) \right| \leqslant \frac{|H_q|}{\varphi(q)} \sum_{\chi_{|H_q}=1} |\tau\left(\chi, \psi_{f(w_q)}\right)| \leqslant \frac{|H_q|}{\varphi(q)} \sqrt{q} \underbrace{\sum_{\chi_{|H_q}=1} 1}_{\varphi(q)/|H_q|} = \sqrt{q}$$

However, if χ is not primitive, or if $f(w_q)$ is not coprime with q, or both, there could be some "bad collision" between the non-primitivity of χ and that of $\psi_{f(w_q)}$, leading to a Gauss sum with modulus larger than $\sqrt{q}$. For instance if χ is the principal character modulo q and $f(w_q) \equiv 0 \bmod q$, then

$$\tau\left(\chi, \psi_{f(w_q)}\right) = \sum_{x \in (\mathbf{Z}/q\mathbf{Z})^\times} 1 = \varphi(q) = p^{\alpha-1}(p-1),$$

which is larger than $\sqrt{q} = p^{\alpha/2}$. Actually, we already know that this cannot happen for large values of q because we saw in the proof of Lemma 2.15 that there are only finitely many q such that $f(w_q) \equiv 0 \bmod q$. But we need to prove that the other possible "bad collisions" do not cause an issue, in order to apply inequality (3.10) (up to some multiplicative constant) and to conclude the proof. This is what remains to do in the detailed proof. □

The crucial control of the p-adic valuation. As we will see in the proof of the necessary Gauss sums estimates, it is not sufficient to know that $f(w_q)$ is non-zero modulo $q = p^\alpha$, we will actually need to know something more precise about the p-adic valuation of $f(w_q)$. This is the content of the following very important proposition.

Proposition 3.4. *Let $d \geqslant 1$ and let $f \in \mathbf{Z}[X] \setminus \{0\}$ be a polynomial of degree strictly less than $\varphi(d)$. For all d-admissible integers q, we choose an element w_q of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$. Then there exist two constants $C_f, n_f \geqslant 1$ such that for all $q = p^\alpha \in \mathcal{A}_d$ such that $q > n_f$,*

(a) $f(w_q) \not\equiv 0 \bmod q$

(b) $p^{v_p(f(w_q))} \leqslant C_f$.

Remark 3.5. Since $f(w_q) \not\equiv 0 \bmod q$ in point (a), it makes sense to speak about the p-adic valuation of $f(w_q)$ in point (b), as it does not depend on the choice of an integer $\tilde{w}_q$ representing the class w_q.

Proof. The first part of the proof is actually what we already did in the proof of Lemma 2.15, following closely the arguments of [32, Lemma 6.2]. Let us reproduce briefly the proof to facilitate the reading and have all notations on the same page.
First, we use the fact that there exist two polynomials $a, b \in \mathbf{Z}[X]$ and an integer $n \geqslant 1$ such that

$$a(X)\phi_d(X) + b(X)f(X) = n, \tag{3.11}$$

since f and ϕ_d are coprime in the euclidean domain $\mathbf{Q}[X]$. Now, let $q = p^\alpha$ be a d-admissible integer. Reducing equation (3.11) modulo q and evaluating it at w_q leads to

$$\overline{a}(w_q)\overline{\phi}_d(w_q) + \overline{b}(w_q)\overline{f}(w_q) \equiv n \bmod p^\alpha$$

hence

$$\overline{b}(w_q)\overline{f}(w_q) \equiv n \bmod p^\alpha \tag{3.12}$$

by Lemma 2.14. Now, if $q = p^\alpha > n$, then n is non-zero modulo q, hence $\overline{f}(w_q) \not\equiv 0 \bmod q$. This shows that $n_f := n$ is a suitable constant for assertion (a).

Another way of phrasing what we just proved is that as soon as $q > n$, the p-adic valuation of $f(w_q)$ is strictly less than α. Let us denote by $\gamma < \alpha$ the p-adic valuation of $f(w_q)$. Then, if we reduce the congruence (3.12) modulo p^γ, we get $n \equiv 0 \bmod p^\gamma$. Thus,

$$\gamma = v_p(f(w_q)) \leqslant v_p(n),$$

hence

$$p^{v_p(f(w_q))} \leqslant p^{v_p(n)} \leqslant n.$$

Therefore, we proved that with the choice $C_f := n$, assertion (b) holds. □

We can finally complete the proof of Lemma 3.2.

Proof of Lemma 3.2. In the overview of the proof, we arrived at the following inequality:

$$\left|\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right)\right| \leqslant \frac{|H_q|}{\varphi(q)} \sum_{\chi_{|H_q}=1} |\tau\left(\chi, \psi_{f(w_q)}\right)|. \tag{3.13}$$

Our next task consists in finding upper bounds for the absolute values of the Gauss sums $\tau\left(\chi, \psi_{f(w_q)}\right)$. We distinguish between the principal character χ_0 and the others.

- *Contribution of the principal character χ_0 in (3.13).*

  Since $\chi_0(a) = 1$ if $(a, q) = 1$ and $\chi_0(a) = 0$ otherwise, we have that $\tau\left(\chi_0, \psi_{f(w_q)}\right)$ is equal to the sum:

  $$\sum_{x\in(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{f(w_q)x}{q}\right)$$

  Now, thanks to Lemma 3.1 we know that there exists a rank n_f such that for all $q > n_f$:

  $$|\tau\left(\chi_0, \psi_{f(w_q)}\right)| \leqslant 1. \tag{3.14}$$

- *Contribution of the characters $\chi \neq \chi_0$ in (3.13).*

  These are handled using the following lemma.

  Lemma 3.6. *Let $d \geqslant 1$ be an integer, and let $f \in \mathbf{Z}[X] \setminus \{0\}$ be a polynomial of degree strictly less than $\varphi(d)$. There exist two constants C_f and m_f, larger than or equal to 1, such that for all d-admissible integer q strictly larger than m_f, for any element w_q of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$ and for any non-principal Dirichlet character χ modulo q,*

  $$\left|\tau(\chi, \psi_{f(w_q)})\right| \leqslant C_f\sqrt{q}.$$

  Proof. As in the proof of Myerson's lemma (Lemma 2.15), we fix a Bézout relation between ϕ_d and f:

  $$a(X)\phi_d(X) + b(X)f(X) = n \tag{3.15}$$

where $a, b \in \mathbf{Z}[X]$ and $n \geqslant 1$. Let $q = p^\alpha$ be a d-admissible integer such that $q > n$. We denote by w_q an element of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$, and since we assumed that $q > n$, we know from the proof of Lemma 2.15 that $f(w_q) \not\equiv 0 \bmod q$. This allows us to speak about the p-adic valuation of the class $f(w_q)$, as it does not depend on the choice of a representative $\tilde{w}_q$ of w_q in $\mathbf{Z}$.
Let χ be a non-principal multiplicative character modulo q, and denote by p^β its conductor (with $0 < \beta \leqslant \alpha$). In other words, χ is induced by a primitive character modulo p^β. Thanks to Corollary 3.20 of Appendix 3.A, we have:

$$\left|\tau\left(\chi, \psi_{f(w_q)}\right)\right| = \begin{cases} p^{\alpha-\beta/2} & \text{if } v_p(f(w_q)) = \alpha - \beta \\ 0 & \text{otherwise.} \end{cases}$$

In particular, the Gauss sum $\tau\left(\chi, \psi_{f(w_q)}\right)$ is non-zero if and only if $\beta = \alpha - v_p(f(w_q))$. In this case, we have:

$$\left|\tau\left(\chi, \psi_{f(w_q)}\right)\right| = p^{\alpha - \frac{\alpha - v_p(f(w_q))}{2}} = p^{\frac{\alpha + v_p(f(w_q))}{2}} = p^{\frac{v_p(f(w_q))}{2}}\sqrt{q} \tag{3.16}$$

Now, we saw in the proof of Proposition 3.4 that

$$\gamma = v_p(f(w_q)) \leqslant v_p(n).$$

Using this last inequality in (3.16) yields:

$$\left|\tau\left(\chi, \psi_{f(w_q)}\right)\right| = p^{\frac{v_p(n)}{2}}\sqrt{q}$$

and since $p^{\frac{v_p(n)}{2}} \leqslant \sqrt{n}$ we get: $\left|\tau\left(\chi, \psi_{f(w_q)}\right)\right| = \sqrt{n}\sqrt{q}$. Thus, $m_f := n$ and $C_f := \sqrt{n}$ are suitable constants for which the statement holds. □

We deduce from Lemma 3.6 that for all $q > m_f$:

$$\sum_{\substack{\chi_{|H_q}=1 \\ \chi \neq \chi_0}} \left|\tau\left(\chi, \psi_{f(w_q)}\right)\right| \leqslant C_f\sqrt{q}\left|\left\{\chi \neq \chi_0 \mid \chi_{|H_q} = 1\right\}\right| = C_f\sqrt{q}\left(\frac{\varphi(q)}{|H_q|} - 1\right) \tag{3.17}$$

- *Conclusion:* If we put $N_f := \max(n_f, m_f)$ we have that for all $q > N_f$, both inequalities (3.14) and (3.17) hold. Thanks to (3.13), this gives

$$\left|\sum_{a \in H_q} e\left(\frac{af(w_q)}{q}\right)\right| \leqslant \frac{|H_q|}{\varphi(q)}\left[C_f\sqrt{q}\left(\frac{\varphi(q)}{|H_q|} - 1\right) + 1\right] \leqslant C_f\sqrt{q},$$

and this concludes the proof of Lemma 3.2.

□

Remark 3.7. A closer look at the proofs of Lemma 3.1 and Lemma 3.6 reveals that one can take N_f to be n^2 and C_f to be $\sqrt{n}$, with the integer n coming from any Bézout relation between f and ϕ_d:

$$a(X)\phi_d(X) + b(X)f(X) = n$$

where $a, b \in \mathbf{Z}[X]$ and $n \geqslant 1$.

Remark 3.8. In the proof of Lemma 3.6, we actually saw that $|\tau\left(\chi, \psi_{f(w_q)}\right)|$ is non-zero if and only if the conductor of χ is p^β with $\beta = \alpha - v_p(f(w_q))$. Therefore, in the sum

$$\sum_{\substack{\chi_{|H_q}=1 \\ \chi \neq \chi_0}} \left|\tau\left(\chi, \psi_{f(w_q)}\right)\right|$$

only the characters χ with conductor equal to $p^{\alpha-v_p(f(w_q))}$ give a non-zero contribution, and this non-zero contribution is bounded by $C_f\sqrt{q}$. Thus, the upper bound (3.17) might be improved by counting precisely the number of characters χ having a prescribed conductor **and** satisfying $\chi_{|H_q}=1$. However, this seems to be difficult.

Besides, in the case where $\alpha=1$ and p goes to infinity, the bound is tight. Indeed, p eventually becomes strictly larger than the integer n from the Bézout relation, so that the congruence (3.12) immediately gives that $v_p(f(w_p))=0$. Then the condition $\beta=\alpha-v_p(f(w_p))$ is just requiring that χ is primitive, but modulo p, all non-principal characters are primitive.

Consequences on equidistribution of exponential sums. The above discussion has consequences in our problem of interest, that is: equidistribution of sums of the form

$$\sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times\\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right)$$

where the parameters a_i range over some specific subsets of $\mathbf{Z}/q\mathbf{Z}$. Precisely, Lemma 3.2 allows us to prove that the equidistribution results of Proposition 2.12 and 2.20 still hold if we restrict the parameters a_i to range over sufficiently large subgroups of $(\mathbf{Z}/q\mathbf{Z})^\times$, in a sense which matches the condition

$$\frac{\sqrt{q}}{|H_q|}\underset{q\to\infty}{\longrightarrow}0$$

in the case of the simplest sums

$$\sum_{x^d=1} e\left(\frac{ax}{q}\right).$$

Indeed, we have the following theorem:

Theorem 3.9. *Let $d\geqslant 1$ be an integer and let $\mathbf{m}=(m_1,\dots,m_n)\in\mathbf{Z}^n$. For all d-admissible integer q, we fix subgroups $H_q^{(1)},\dots,H_q^{(n)}$ of $(\mathbf{Z}/q\mathbf{Z})^\times$. Then we have the following equidistribution results:*

(a) The general case.
If the subgroups $H_q^{(1)},\dots,H_q^{(n)}$ satisfy the growth condition:

$$\forall i\in\{1,\dots,n\},\quad \frac{\sqrt{q}}{|H_q^{(i)}|}\underset{q\to\infty}{\longrightarrow}0, \tag{3.18}$$

then the sets

$$\left\{\sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times\\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right);\ (a_1,\dots,a_n)\in H_q^{(1)}\times\cdots\times H_q^{(n)}\right\}, \tag{3.19}$$

become equidistributed in the image of the Laurent polynomial $f_{d,\mathbf{m}}$ (Definition 2.19) with respect to the pushforward measure via $f_{d,\mathbf{m}}$ of the probability Haar measure λ on $(\mathbf{S}^1)^{\varphi(d_1)+\cdots+\varphi(d_n)}$, as q goes to infinity among the d-admissible integers. In other words, if we denote by $\mathcal{I}_{d,\mathbf{m}}$ the image of $f_{d,\mathbf{m}}$ and by $\mu:=(f_{d,\mathbf{m}})_*\lambda$, then for all continuous function $F\colon\mathcal{I}_{d,\mathbf{m}}\to\mathbf{C}$,

$$\frac{1}{\prod_{i=1}^n|H_q^{(i)}|}\sum_{a_1\in H_q^{(1)}}\cdots\sum_{a_n\in H_q^{(n)}}F\left(\sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times\\ x^d=1}} e\left(\frac{a_1x^{m_1}+\cdots+a_nx^{m_n}}{q}\right)\right)\underset{\substack{q\to\infty\\ q\in\mathcal{A}_d}}{\longrightarrow}\int_{\mathcal{I}_{d,\mathbf{m}}}F\mathrm{d}\mu.$$

(b) When $\mathbf{m}$ is coprime with d.
Let $s \in \{1, \dots, n\}$ and let $\{i_1, \dots, i_s\} \subseteq \{1, \dots, n\}$. We fix $n - s$ integers a_i for $i \in \{1, \dots, n\} \setminus \{i_1, \dots, i_s\}$. Then if the growth condition

$$\frac{q^{s/2}}{\prod_{1 \leqslant j \leqslant s} \left| H_q^{(i_j)} \right|} \underset{q \to \infty}{\longrightarrow} 0 \tag{3.20}$$

is satisfied, the sets of sums

$$\left\{ \sum_{\substack{x \in (\mathbf{Z}/q\mathbf{Z})^\times \\ x^d = 1}} e\left(\frac{a_1 x^{m_1} + \cdots + a_n x^{m_n}}{q} \right);\ (a_{i_1}, \dots, a_{i_s}) \in H_q^{(i_1)} \times \cdots \times H_q^{(i_s)} \right\}$$

become equidistributed in the image of the Laurent polynomial g_d (Definition 2.6) with respect to the pushforward measure via g_d of the probability Haar measure on $(\mathbf{S}^1)^{\varphi(d)}$, as q goes to infinity among the d-admissible integers.

In particular, the case of the sums

$$\mathrm{S}_q(a, d) = \sum_{\substack{x \in (\mathbf{Z}/q\mathbf{Z})^\times \\ x^d = 1}} e\left(\frac{ax}{q} \right)$$

corresponds to $\mathbf{m} = (1)$, which is coprime with d, so that case (b) of the above theorem asserts that the sets $\{\mathrm{S}_q(a, d);\ a \in H_q\}$ become equidistributed in the image of g_d with respect to the suitable pushforward measure, as soon as H_q is a subgroup of $(\mathbf{Z}/q\mathbf{Z})^\times$ such that $\sqrt{q}/|H_q| \underset{q \to \infty}{\longrightarrow} 0$.

Remark 3.10. Condition (3.20) is a weaker requirement than condition (3.18). Instead of asking for an individual control of the growth of each $H_q^{(i)}$, we just ask that they satisfy $\sqrt{q}/|H_q| \underset{q \to \infty}{\longrightarrow} 0$ "multiplicatively on average".

Proof of case (a) *of Theorem 3.9.* The reduction step is the same as in the proof of Proposition 2.20, except that one needs to put $Y_{\mathbf{m},q} = H_q^{(1)} \times \cdots \times H_q^{(n)}$ instead of $(\mathbf{Z}/q\mathbf{Z})^n$. This reduces the proof to the equidistribution modulo 1 of the following subsets of $(\mathbf{R}/\mathbf{Z})^{\varphi(d_1)+\cdots+\varphi(d_n)}$:

$$\left\{ \overbrace{\left(\left(\frac{a_1 (w_q^{m_1})^j}{q} \right)_{0 \leqslant j < \varphi(d_1)}, \dots, \left(\frac{a_n (w_q^{m_n})^j}{q} \right)_{0 \leqslant j < \varphi(d_n)} \right)}^{=: \mathbf{x}(a_1, \dots, a_n, q)};\quad (a_1, \dots, a_n) \in H_q^{(1)} \times \cdots \times H_q^{(n)} \right\},$$

as q goes to infinity among the d-admissible integers. To prove this, we apply Weyl's criterion, so we let $\mathbf{y} = (y_0, \dots, y_{\varphi(d_1)+\cdots+\varphi(d_n)-1}) \in \mathbf{Z}^{\varphi(d_1)+\cdots+\varphi(d_n)} \setminus \{0\}$ and we want to show the following convergence towards zero:

$$\frac{1}{\prod_{i=1}^n |H_q^{(i)}|} \times \sum_{\substack{a_1 \in H_q^{(1)} \\ \vdots \\ a_n \in H_q^{(n)}}} e\left(\mathbf{x}(a_1, \dots, a_n, q) \cdot \mathbf{y} \right) \underset{\substack{q \to \infty \\ q \in \mathcal{A}_d}}{\longrightarrow} 0. \tag{3.21}$$

As in the proof of Proposition 2.20, let us denote by $\mathbf{y}_1$ the vector extracted from $\mathbf{y}$ by taking the first $\varphi(d_1)$ entries, $\mathbf{y}_2$ the vector formed by the next $\varphi(d_2)$ entries and so on:

$$\mathbf{y}_1 = (y_0, \dots, y_{\varphi(d_1)-1}), \quad \mathbf{y}_2 = (y_{\varphi(d_1)}, \dots, y_{\varphi(d_1)+\varphi(d_2)-1}) \quad \mathbf{y}_3 = \cdots$$

so that $\mathbf{y} = (\mathbf{y}_1, \dots, \mathbf{y}_n)$. Similarly,

$$\mathbf{x}_1(a_1,q) := \left(\frac{a_1(w_q^{m_1})^j}{q}\right)_{0\leqslant j<\varphi(d_1)}, \ldots, \ \mathbf{x}_n(a_n,q) := \left(\frac{a_n(w_q^{m_n})^j}{q}\right)_{0\leqslant j<\varphi(d_n)}.$$

Then we have

$$\frac{1}{\prod_{i=1}^n |H_q^{(i)}|} \times \sum_{\substack{a_1\in H_q^{(1)}\\ \vdots \\ a_n\in H_q^{(n)}}} e\left(\mathbf{x}(a_1,\ldots,a_n,q)\cdot\mathbf{y}\right) = \prod_{i=1}^n \left[\frac{1}{|H_q^{(i)}|}\sum_{a_i\in H_q^{(i)}} e(\mathbf{x}_i(a_i,q)\cdot\mathbf{y}_i)\right]. \tag{3.22}$$

Now, since $\mathbf{y}\neq 0$, there exists at least one index $i\in\{1,\ldots,n\}$ such that $\mathbf{y}_i\neq 0$. For such an i, write

$$\frac{1}{|H_q^{(i)}|}\sum_{a_i\in H_q^{(i)}} e(\mathbf{x}_i(a_i,q)\cdot\mathbf{y}_i) = \frac{1}{|H_q^{(i)}|}\sum_{a\in H_q^{(i)}} e\left(\frac{af_i(w_q^{m_i})}{q}\right), \tag{3.23}$$

where f_i is the polynomial associated with $\mathbf{y}_i = \left(y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})},\ldots,y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})+\varphi(d_i)-1}\right)$ as follows: $f_i = y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})} + y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})+1}X + \cdots + y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})+\varphi(d_i)-1}X^{\varphi(d_i)-1}$. This is a non-zero polynomial with integer coefficients and with degree strictly less than $\varphi(d_i)$, and $w_q^{m_i}$ is an element of order d_i in $(\mathbf{Z}/q\mathbf{Z})^\times$. Thus, we can apply Lemma 3.2 which states that there exists a rank N_{f_i} such that for all $q>N_{f_i}$ such that q is d-admissible,

$$\left|\sum_{a\in H_q^{(i)}} e\left(\frac{af_i(w_q^{m_i})}{q}\right)\right| \ll_{f_i} \sqrt{q},$$

and this suffices to prove the convergence of (3.23) towards zero, thanks to assumption (3.18). As all the other factors of (3.22) have absolute value bounded above by 1, the whole product converges to zero, and this concludes the proof. □

Proof of case (b) *of Theorem* 3.9. With the same reduction step as in Proposition 2.12 (replacing the set of parameters $Y_{\mathbf{m},q} = (\mathbf{Z}/q\mathbf{Z})^s$ by $Y_{\mathbf{m},q} = H_q^{(i_1)}\times\cdots\times H_q^{(i_s)}$) one proves that the statement is implied by the equidistribution modulo 1 of the sets of $\varphi(d)$-tuples

$$\left\{\overbrace{\left(\frac{a_1(w_q^{m_1})^0+\cdots+a_n(w_q^{m_n})^0}{q},\ldots,\frac{a_1(w_q^{m_1})^{\varphi(d)-1}+\cdots+a_n(w_q^{m_n})^{\varphi(d)-1}}{q}\right)}^{=:\mathbf{x}(a_{i_1},\ldots,a_{i_s},q)};\right.$$
$$\left.(a_{i_1},\ldots,a_{i_s})\in H_q^{(i_1)}\times\cdots\times H_q^{(i_s)}\right\},$$

By Weyl's criterion, these sets become equidistributed if and only if for any $\mathbf{y} := \left(y_0,\ldots,y_{\varphi(d)-1}\right)\in \mathbf{Z}^{\varphi(d)}\setminus\{0\}$ we have the following convergence towards zero:

$$\frac{1}{\prod_{j=1}^s |H_q^{(i_j)}|}\times\left(\sum_{(a_{i_1},\ldots,a_{i_s})\in H_q^{(i_1)}\times\cdots\times H_q^{(i_s)}} e\left(\mathbf{x}(a_{i_1},\ldots,a_{i_s},q)\cdot\mathbf{y}\right)\right) \underset{\substack{q\to\infty\\ q\in\mathcal{A}_d}}{\longrightarrow} 0$$

But the left-hand side can be rewritten as:

$$\prod_{i\in\{i_1,\ldots,i_s\}}\left[\frac{1}{|H_q^{(i)}|}\sum_{a_i\in H_q^{(i)}} e\left(\frac{a_if(w_q^{m_i})}{q}\right)\right]\times\prod_{i\notin\{i_1,\ldots,i_s\}} e\left(\frac{a_if(w_q^{m_i})}{q}\right) \tag{3.24}$$

where f is the polynomial $y_0 + y_1 X + \cdots + y_{\varphi(d)-1} X^{\varphi(d)-1}$.

Now for all $i \in \{i_1, \dots, i_s\}$, the element $w_q^{m_i}$ is still of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$ because $(m_i, d) = 1$. Also, $f \in \mathbf{Z}[X] \setminus \{0\}$ and $\deg f < \varphi(d)$. Therefore, the assumptions of Lemma 3.2 are satisfied, and we can find an integer N_f such that for all $q > N_f$ such that q is d-admissible, we have:

$$\frac{1}{|H_q^{(i)}|} \left| \sum_{a_i \in H_q^{(i)}} e\left(\frac{a_i f(w_q^{m_i})}{q}\right) \right| \ll_f \frac{\sqrt{q}}{|H_q^{(i)}|}$$

for all $i \in \{i_1, \dots, i_s\}$. Thus, the first product in (3.24) can be bounded above as follows:

$$\left| \prod_{i \in \{i_1, \dots, i_s\}} \left[\frac{1}{|H_q^{(i)}|} \sum_{a_i \in H_q^{(i)}} e\left(\frac{a_i f(w_q^{m_i})}{q}\right) \right] \right| \ll_f \frac{q^{s/2}}{\prod_{j=1}^{s} \left| H_q^{(i_j)} \right|},$$

so it tends to zero as q goes to infinity thanks to assumption (3.20). As the remaining factors in (3.24) have absolute value equal to 1, this concludes the proof. □

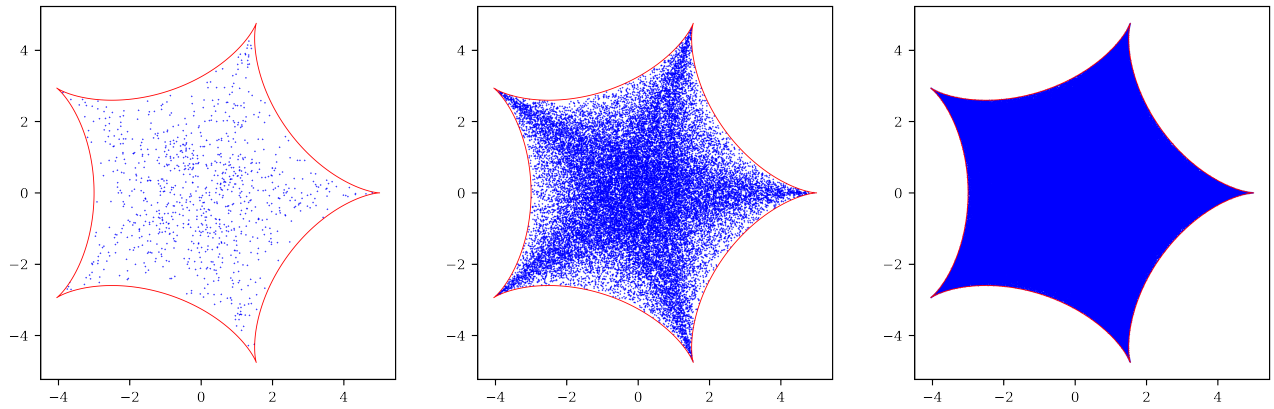
Illustration of Theorem 3.9 (b). In Figure 2.5, we were interested in the distribution of Kloosterman sums restricted to the subgroup of order 5:

$$\mathrm{K}_q(a, b, 5) := \sum_{\substack{x \in (\mathbf{Z}/q\mathbf{Z})^\times \\ x^5 = 1}} e\left(\frac{ax + bx^{-1}}{q}\right).$$

More precisely, [16, Theorem 7] asserts that the sets $\mathcal{K}_q(-,-,5) = \{\mathrm{K}_q(a,b,5);\ (a,b) \in (\mathbf{Z}/q\mathbf{Z})^2\}$ become equidistributed in the region $\mathbb{H}_5$ delimited by the 5-cusp hypocycloid, with respect to the pushforward measure via g_5 of the Haar measure on $\mathbb{T}^4$. Theorem 3.9 (b) strengthens this result by showing that one can impose restrictions on the set of parameters, and still obtain equidistribution. Namely, we proved that it suffices that the parameters a and b range over multiplicative subgroups $H_q^{(1)}$ and $H_q^{(2)}$ whose cardinality grows faster than $\sqrt{q}$ "multiplicatively on average" in the sense of (3.20). One can also fix one of the two parameters, and let the other one vary in a subgroup H_q, and again, equidistribution is ensured provided $\sqrt{q}/|H_q| \underset{q\to\infty}{\longrightarrow} 0$. This is what the following pictures illustrate. We consider the following sets of Kloosterman sums restricted to the subgroup of order 5:

$$\left\{ \sum_{\substack{x \in (\mathbf{Z}/q\mathbf{Z})^\times \\ x^5 = 1}} e\left(\frac{ax + x^{-1}}{q}\right);\ a \in H_q \right\} \tag{3.25}$$

for different 5-admissible values of q and the indicated choice of subgroups H_q (which are uniquely determined by their cardinality, since $(\mathbf{Z}/q\mathbf{Z})^\times$ is cyclic). We chose $|H_q|$ in such a way that $\sqrt{q}/|H_q|$ becomes very small.



(a) $q = 1901$
$|H_q| = 950$
$\sqrt{q}/|H_q| \simeq 0.046$

(b) $q = 421^2$
$|H_q| = 29470$
$\sqrt{q}/|H_q| \simeq 0.014$

(c) $q = 971^2$
$|H_q| = 941870$
$\sqrt{q}/|H_q| \simeq 0.001$

Figure 3.1: The sets of the form (3.25) for three 5-admissible integers q and for the indicated choice of subgroups H_q.

3.3. On crossing the $\sqrt{q}$ barrier

Theorem 3.9 is an improvement of propositions 2.12 and 2.20 because equidistribution is proved even though the parameters are restricted to range over "small" subsets of the whole ring $\mathbf{Z}/q\mathbf{Z}$. Precisely, it allows them to range over multiplicative subgroups $|H_q|$ satisfying

$$\frac{\sqrt{q}}{|H_q|} \underset{q\to\infty}{\longrightarrow} 0. \tag{3.26}$$

In particular, $|H_q| \gg_\varepsilon q^{1/2+\varepsilon}$ for some $\varepsilon > 0$ is sufficient to obtain equidistribution.

The proof relies mostly on Lemma 3.2, which is an exponential sum estimate for sums over a multiplicative subgroup of $(\mathbf{Z}/q\mathbf{Z})^\times$. If we forget for a moment about the dependence in q of $f(w_q)$ in this lemma, which adds a little extra difficulty, we can say that it is actually concerned with sums of the type

$$\sum_{x\in H_q} e\left(\frac{ax}{q}\right).$$

for fixed $a \in \mathbf{Z}/q\mathbf{Z}$ and H_q being a subgroup of $(\mathbf{Z}/q\mathbf{Z})^\times$. Equidistribution results with parameters varying in the subgroup will depend on non-trivial estimates for the absolute value of the sum above. For instance, we would like to obtain a power saving, that is: an estimate of the form

$$\left|\sum_{x\in H_q} e\left(\frac{ax}{q}\right)\right| \ll \frac{|H_q|}{q^\varepsilon}.$$

for some $\varepsilon > 0$. Moreover, one could wish for some uniformity with respect to a and hence seek for estimates of the form

$$\max_{a\in(\mathbf{Z}/q\mathbf{Z})^\times}\left|\sum_{x\in H_q} e\left(\frac{ax}{q}\right)\right| \ll \frac{|H_q|}{q^\varepsilon}. \tag{3.27}$$

It turns out that this question has been extensively studied and is at the intersection of many areas of mathematics. In [79], Pär Kurlberg gives a brief exposition of the history of the question and of some important achievements, before giving a detailed overview of the most recent progress and their connection with additive combinatorics. He focuses mainly on the case where $q = p$ is a prime number and starts by showing how a standard completion method allows one to get a power saving of the form (3.27) as soon as $|H_p| \gg_\varepsilon p^{1/2+\varepsilon}$.

The completion method. In this paragraph, we only consider exponential sums modulo prime numbers p, and H_p will always denote a subgroup of the multiplicative group $\mathbf{F}_p^\times$. What we call "completion method" is the approach described in the introduction of [79] that we already applied in the overview of the proof of Lemma 3.2. It turns sums over the subgroup H_p into sums over all $\mathbf{F}_p^\times$ by testing the condition $x \in H_p$ using multiplicative characters. The first step is to decompose the map:

$$\begin{array}{rccc} \psi_a & : & \mathbf{F}_p^\times & \to & \mathbf{C} \\ & & x & \mapsto & e\left(\frac{ax}{q}\right) \end{array}$$

in the orthonormal basis of $\mathbf{Maps}(\mathbf{F}_p^\times, \mathbf{C})$ made of the multiplicative characters modulo p. This gives

$$\sum_{x \in H_p} e\left(\frac{ax}{p}\right) = \sum_{x \in H_p} \sum_{\chi} \langle \psi_a, \chi \rangle \chi(x)$$

Now, $\langle \psi_a, \chi \rangle$ can be related to a Gauss sum as follows (see Appendix 3.A for the notation $\tau(\text{-},\text{-})$ for Gauss sums):

$$\langle \psi_a, \chi \rangle = \frac{1}{\varphi(p)} \sum_{y \in \mathbf{F}_p^\times} \psi_a(y) \overline{\chi(y)} = \frac{1}{p-1} \tau\left(\overline{\chi}, \psi_a\right),$$

hence

$$\sum_{x \in H_p} e\left(\frac{ax}{q}\right) = \frac{1}{p-1} \sum_{\chi} \tau\left(\overline{\chi}, \psi_a\right) \sum_{x \in H_p} \chi(x).$$

Now, among the multiplicative characters modulo p, all those who induce (by restriction) a non-trivial character of H_p have no contribution. Indeed, for such characters, the inner sum is zero by orthogonality of the multiplicative characters of H_p. On the other hand, for the trivial characters of H_p, the inner sum is just equal to its number of terms, that is: $|H_p|$. We deduce that

$$\sum_{x \in H_p} e\left(\frac{ax}{q}\right) = \frac{|H_p|}{p-1} \sum_{\chi_{|H_p}=1} \tau\left(\overline{\chi}, \psi_a\right)$$

Finally, if χ is the principal character χ_0 modulo p, we have $\tau\left(\overline{\chi_0}, \psi_a\right) = \tau\left(\overline{\chi_0}, \psi_a\right) = -1$ for all $a \in \mathbf{F}_p^\times$. If χ is not the principal character modulo p, then $\tau\left(\overline{\chi}, \psi_a\right)$ is a Gauss sum associated with a non-trivial additive character of $\mathbf{F}_p$ (provided $a \in \mathbf{F}_p^\times$) and a non trivial multiplicative character modulo p, hence $|\tau\left(\overline{\chi}, \psi_a\right)| = \sqrt{p}$. As the number of multiplicative characters modulo p satisfying $\chi_{|H_p} = 1$ is equal to $\frac{p-1}{|H_p|}$, we deduce that

$$\left| \sum_{x \in H_p} e\left(\frac{ax}{q}\right) \right| < \sqrt{p}.$$

This shows that we have a power saving of the form (3.27) as soon as $|H_p| \gg_\varepsilon p^{1/2+\varepsilon}$ for some $\varepsilon > 0$.

Going below $p^{1/2+\varepsilon}$. Crossing this $\sqrt{p}$ barrier is by no means easy, and the first achievement is due to Shparlinski in [97], where a power saving of the form (3.27) is obtained for subgroups satisfying $|H_p| \gg_\varepsilon p^{3/7+\varepsilon}$. Indeed, Shparlinski [97, Theorem 2] shows that if $g \in \mathbf{F}_p^\times$ is an element of order τ, then

$$\max_{(a,p)=1} \left| \sum_{x=1}^{\tau} e\left(\frac{ag^x}{p}\right) \right| \leqslant 2\tau^{5/12} p^{1/4}. \tag{3.28}$$

This upper bound relies on considerations on the 4-th moment and estimates for the number of points on curves given by an equation of the form $x^n + y^n = \lambda$ over finite fields, which were studied in [43]. Once we have the above estimate, it is easy to derive the needed power saving for subgroups of

cardinality $\gg_\varepsilon p^{3/7+\varepsilon}$. For such a subgroup H_p, it suffices to take a generator g, whose order τ then satisfies $\tau \gg p^{3/7+\varepsilon}$, and to apply (3.28) to get:

$$\frac{1}{|H_p|}\max_{a\in\mathbf{F}_p^\times}\left|\sum_{x\in H_p} e\left(\frac{ax}{p}\right)\right| \leqslant \frac{2|H_p|^{5/12}p^{1/4}}{|H_p|} = \frac{2p^{1/4}}{|H_p|^{7/12}} \ll_\varepsilon \frac{1}{p^{\frac{7}{12}\varepsilon}}.$$

Some significative improvements were made by Heath-Brown and Konyagin in [49], using a variation of Stepanov's polynomial method to handle the point-counting on the underlying curves over finite fields. This allowed them to consider the range $|H_p| \gg_\varepsilon p^{1/3+\varepsilon}$. The best known bound using these tools from analytic number theory is due to Konyagin [67], where subgroups satisfying $|H_p| \gg_\varepsilon p^{1/4+\varepsilon}$ are allowed. However, the story does not end there, thanks to a fruitful interplay between additive combinatorics and exponential sums!

A triumph for additive combinatorics. The previous discussion shows that obtaining a power saving of the form (3.27) for smaller and smaller subgroups required (quoting Green's lecture notes [47]) "quite sophisticated number-theoretical arguments" (as we have seen, it involved for instance Stepanov's polynomial method to handle the point counting on certain curves over finite fields). Thus, Theorem 3.11 below "is something of a triumph for additive combinatorics". It states that one can replace the growth condition (3.26) by the following one:

$$|H_q| \geqslant q^\delta$$

for any fixed $\delta > 0$, which represents a huge improvement!

This theorem is the achievement of a series of article, mainly by Bourgain, Chang, Glibichuk and Konyagin, in which very strong estimates on sums of additive characters modulo q over subgroups of $(\mathbf{Z}/q\mathbf{Z})^\times$ were proved for different forms of factorization of q. The case where q is prime is proved in [13], while the case of prime powers with bounded exponent is settled in [12]. This series of works culminated with the following theorem, which treats the general case, and includes in particular the case of small primes raised to high powers.

Theorem 3.11 (Bourgain). *For any $\delta > 0$, there exists $\varepsilon = \varepsilon(\delta) > 0$ such that for any integer $q \geqslant 2$, and any subgroup H of $(\mathbf{Z}/q\mathbf{Z})^\times$ such that $|H| \geqslant q^\delta$,*

$$\max_{a\in(\mathbf{Z}/q\mathbf{Z})^\times}\left|\sum_{x\in H} e\left(\frac{ax}{q}\right)\right| \leqslant C\frac{|H|}{q^\varepsilon} \tag{3.29}$$

where C is a constant depending at most on δ.

Proof. See [11, Theorem]. □

3.4. Subgroups of cardinality at least q^δ

In this section, we show that Bourgain's estimate allows us to push further the restriction of the liberty of the parameters in Theorem 3.9. We prove that the result still holds if the parameters are restricted to range over very small subgroups of $(\mathbf{Z}/q\mathbf{Z})^\times$, namely subgroups whose cardinality grows as fast as an arbitrary small power of q.

Exponential sum estimate. Lemma 2.15 was about estimates for

$$\sum_{a\in\mathbf{Z}/q\mathbf{Z}} e\left(\frac{af(w_q)}{q}\right)$$

(and actually showed that these are eventually equal to zero), while Lemma 3.2 provided an estimate for

$$\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right)$$

which was non-trivial as soon as H_q was substantially larger than $\sqrt{q}$, and which allowed us to extend our equidistribution results to sets of exponential sums with parameters varying in sufficiently large subgroups of $(\mathbf{Z}/q\mathbf{Z})^\times$ (the condition is essentially $|H_q|/\sqrt{q} \underset{q\to\infty}{\longrightarrow} \infty$). Bourgain's estimate (Theorem 3.11) allows us to go further in our reduction of the admissible cardinality of the subgroups, via the following proposition, which can be seen as an improvement of Lemma 2.15 and Lemma 3.2.

Proposition 3.12. *Let $d \geqslant 1$ and let $f \in \mathbf{Z}[X] \setminus \{0\}$ be a polynomial of degree strictly less than $\varphi(d)$. Let $\delta > 0$. Then, there exists $\varepsilon = \varepsilon(\delta) > 0$, depending only on δ, such that for all d-admissible integer q larger than some constant N_f depending only on f, for all subgroup H_q of $(\mathbf{Z}/q\mathbf{Z})^\times$ satisfying $|H_q| \geqslant q^\delta$, and for any element w_q of order d inside $(\mathbf{Z}/q\mathbf{Z})^\times$, we have*

$$\left|\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right)\right| \ll_{f,\delta} \frac{|H_q|}{q^\varepsilon}. \tag{3.30}$$

Proof. Let $q = p^\alpha$ be a d-admissible integer, and let H_q and w_q be as in the statement. Let $\tilde{w}_q$ be any lift in $\mathbf{Z}$ of the class w_q. Assume further that $q > n_f$ for any constant n_f as in Proposition 3.4. This ensures that $f(w_q) \not\equiv 0 \bmod q$, but $f(w_q)$ could still be non-invertible if q is a non-trivial prime power. This is why one cannot directly apply Bourgain's theorem to the sum on the left-hand side of (3.30). In order to reduce to a situation where Bourgain's theorem applies, let us introduce the notation β_q for the p-adic valuation of $f(\tilde{w}_q)$, and write $f(\tilde{w}_q) := p^{\beta_q} r_q$. By Proposition 3.4 (a), we know that $\beta_q < \alpha$. Then we have:

$$\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right) = \sum_{a\in H_q} e\left(\frac{ar_q}{p^{\alpha-\beta_q}}\right) \tag{3.31}$$

Now, each of the terms $e\left(\frac{ar_q}{p^{\alpha-\beta_q}}\right)$ only depends on the class of a modulo $p^{\alpha-\beta_q}$. Let us denote by $q' := p^{\alpha-\beta_q}$ and by π the group homomorphism $(\mathbf{Z}/q\mathbf{Z})^\times \to (\mathbf{Z}/q'\mathbf{Z})^\times$ induced by the reduction modulo q'. The latter induces a group homomorphism $\tilde{\pi}\colon H_q \to \pi(H_q) =: H'_q$. We denote by $k := |\ker\tilde{\pi}|$. Then we have the following equality

$$\sum_{a\in H_q} e\left(\frac{ar_q}{p^{\alpha-\beta_q}}\right) = k\sum_{a\in H'_q} e\left(\frac{ar_q}{q'}\right)$$

Indeed, any element of H'_q has exactly k pre-images in H_q under the reduction modulo q'.
Since $\ker\tilde{\pi} \subseteq \ker\pi$, we have that $k \leqslant |\ker\pi| = p^{\beta_q}$. Therefore:

$$\left|\sum_{a\in H_q} e\left(\frac{ar_q}{p^{\alpha-\beta_q}}\right)\right| \leqslant p^{\beta_q}\left|\sum_{a\in H'_q} e\left(\frac{ar_q}{q'}\right)\right| \tag{3.32}$$

In order to apply Theorem 3.11 to the sum on the right-hand side, we first need to check that the subgroup H'_q of $(\mathbf{Z}/q'\mathbf{Z})^\times$ is large in the following sense: $|H'_q| \geqslant (q')^{\delta'}$ for some $\delta' > 0$. Thanks to the first isomorphism theorem, we have:

$$|H'_q| = \frac{|H_q|}{k} \geqslant \frac{|H_q|}{p^{\beta_q}}$$

and by assumption $|H_q| \geqslant q^\delta$, therefore:

$$|H'_q| \geqslant \frac{q^\delta}{p^{\beta_q}} = \frac{p^{\alpha\delta}}{p^{\beta_q}} = \frac{p^{(\alpha-\beta_q)\delta}}{p^{\beta_q(1-\delta)}} = \frac{(q')^\delta}{\left(p^{\beta_q}\right)^{1-\delta}}.$$

Now, since $q > n_f$, we have that $p^{\beta_q} \leqslant C_f$ thanks to Proposition 3.4 (b), where C_f is a positive constant depending only on f. Thus,

$$|H'_q| \geqslant \frac{(q')^\delta}{C_f^{1-\delta}}$$

Finally, since $C_f^{1-\delta}$ is a constant and q' tends to infinity as q goes to infinity, we obtain that $\frac{(q')^{\frac{\delta}{2}}}{C_f^{1-\delta}}$ eventually becomes greater than 1 as q becomes large, so that:

$$|H'_q| \geqslant (q')^{\frac{\delta}{2}} \tag{3.33}$$

for all q large enough, say larger than some constant N_f which only depends on f. The fact that q' tends to infinity as q tends to infinity is a consequence of the inequality:

$$q' = p^{\alpha-\beta_q} = \frac{q}{p^{\beta_q}} \geqslant \frac{q}{C_f}.$$

Thanks to (3.33), Theorem 3.11 applies to the sum on the right-hand side of (3.32), because we also have that r_q is invertible modulo q'. So there exists a constant $\varepsilon = \varepsilon(\delta/2) > 0$ and a constant C depending at most on δ such that:

$$\left|\sum_{a\in H'_q} e\left(\frac{ar_q}{q'}\right)\right| \leqslant C\frac{|H'_q|}{(q')^\varepsilon}$$

Thanks to (3.31) and (3.32), this implies the following upper bound:

$$\left|\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right)\right| \leqslant C\frac{p^{\beta_q}|H'_q|}{(q')^\varepsilon}$$

Now we use the fact that $|H'_q| \leqslant |H_q|$ to obtain the following inequality:

$$C\frac{p^{\beta_q}|H'_q|}{(q')^\varepsilon} \leqslant C\frac{p^{\beta_q}|H_q|}{\left(p^{\alpha-\beta_q}\right)^\varepsilon} = C\frac{|H_q|p^{\beta_q(1+\varepsilon)}}{q^\varepsilon}.$$

Finally, we use again the fact that $p^{\beta_q} \leqslant C_f$, which gives us the conclusion of the proof:

$$\left|\sum_{a\in H_q} e\left(\frac{af(w_q)}{q}\right)\right| \leqslant CC_f^{1+\varepsilon}\frac{|H_q|}{q^\varepsilon} \ll_{f,\delta} \frac{|H_q|}{q^\varepsilon}.$$

□

Consequence on equidistribution of exponential sums. By replacing the use of Lemma 3.2 by the exponential sum estimate of Proposition 3.12, we are able to generalize Theorem 3.9 by allowing the parameters to range over even smaller subgroup. Precisely, we obtain the following statement.

Theorem 3.13. *Let $d \geqslant 1$ be an integer and let $\mathbf{m} = (m_1, \dots, m_n) \in \mathbf{Z}^n$. For all d-admissible integer q, we fix subgroups $H_q^{(1)}, \dots, H_q^{(n)}$ of $(\mathbf{Z}/q\mathbf{Z})^\times$. Then we have the following equidistribution results:*

(a) The general case.
If there exists $\delta > 0$ such that the subgroups $H_q^{(1)}, \dots, H_q^{(n)}$ satisfy the growth condition:

$$\forall i \in \{1, \dots, n\}, \quad |H_q^{(i)}| \geqslant q^\delta, \tag{3.34}$$

then the sets

$$\left\{\sum_{\substack{x\in(\mathbf{Z}/q\mathbf{Z})^\times \\ x^d=1}} e\left(\frac{a_1x^{m_1} + \cdots + a_nx^{m_n}}{q}\right);\ (a_1, \dots, a_n) \in H_q^{(1)} \times \cdots \times H_q^{(n)}\right\}, \tag{3.35}$$

become equidistributed in the image of the Laurent polynomial $f_{d,\mathbf{m}}$ (Definition 2.19) with respect to the pushforward measure via $f_{d,\mathbf{m}}$ of the probability Haar measure λ on $(\mathbf{S}^1)^{\varphi(d_1)+\cdots+\varphi(d_n)}$, as q goes to infinity among the d-admissible integers.

(b) When $\mathbf{m}$ is coprime with d.
Let $s \in \{1,\dots,n\}$ and let $\{i_1,\dots,i_s\} \subseteq \{1,\dots,n\}$. We fix $n-s$ integers a_i for $i \in \{1,\dots,n\} \setminus \{i_1,\dots,i_s\}$. Then if their exists $\delta > 0$ such that

$$\prod_{1 \leqslant j \leqslant s} \left| H_q^{(i_j)} \right| \geqslant q^{\delta} \tag{3.36}$$

is satisfied, the sets of sums

$$\left\{ \sum_{\substack{x \in (\mathbf{Z}/q\mathbf{Z})^\times \\ x^d = 1}} e\left(\frac{a_1 x^{m_1} + \cdots + a_n x^{m_n}}{q} \right);\ (a_{i_1},\dots,a_{i_s}) \in H_q^{(i_1)} \times \cdots \times H_q^{(i_s)} \right\}$$

become equidistributed in the image of the Laurent polynomial g_d (Definition 2.6) with respect to the pushforward measure via g_d of the probability Haar measure on $(\mathbf{S}^1)^{\varphi(d)}$, as q goes to infinity among the d-admissible integers.

For instance, if one takes $\mathbf{m} = (1,-1)$, the second case of this theorem states that the sets

$$\left\{ \mathrm{K}_q(a,b,d);\ (a,b) \in H_q^{(1)} \times H_q^{(2)} \right\} \tag{3.37}$$

satisfy the same equidistribution result as the sets of Figure 2.5, as soon as the $H_q^{(i)}$ are subgroups of $(\mathbf{Z}/q\mathbf{Z})^\times$ such that

$$|H_q^{(1)}||H_q^{(2)}| \geqslant q^{\delta} \tag{3.38}$$

for some $\delta > 0$. In other words, restricting the parameters a, b to large enough multiplicative (in the sense of (3.38)) subgroups does not introduce any bias in the distribution of the restricted Kloosterman sums, and still ensures equidistribution with respect to the same measure as in Theorem 2.5.

The above statement improves a lot Theorem 3.9 because in the latter, condition (3.20) said that we could only prove equidistribution under the condition

$$\frac{q}{|H_q^{(1)}||H_q^{(2)}|} \underset{q \to \infty}{\longrightarrow} 0$$

so essentially this is the conclusion given by Theorem 3.13 when $\delta > 1$, but this theorem actually allows any value of $\delta > 0$, hence much smaller subgroups can be taken as sets of parameters.

Proof of case (a) *of Theorem* 3.13. The beginning of the proof is the same as the proof of Theorem 3.9 (a). If we denote by $\mathbf{y}$ any non-zero vector with integer entries (which is needed in the application of Weyl's criterion), we perform the same splitting as $\mathbf{y} = (\mathbf{y}_1,\dots,\mathbf{y}_n)$ and $\mathbf{x} = (\mathbf{x}_1,\dots,\mathbf{x}_n)$ as in the mentioned proof, and we want to show that the product

$$\prod_{i=1}^{n} \left[\frac{1}{|H_q^{(i)}|} \sum_{a_i \in H_q^{(i)}} e(\mathbf{x}_i(a_i,q) \cdot \mathbf{y}_i) \right] \tag{3.39}$$

converges to zero as q goes to infinity. Now, we have that there exists at least one index $i \in \{1,\dots,n\}$ such that $\mathbf{y}_i \neq 0$. For such an i, write

$$\frac{1}{|H_q^{(i)}|} \sum_{a_i \in H_q^{(i)}} e(\mathbf{x}_i(a_i,q) \cdot \mathbf{y}_i) = \frac{1}{|H_q^{(i)}|} \sum_{a \in H_q^{(i)}} e\left(\frac{a f_i(w_q^{m_i})}{q} \right), \tag{3.40}$$

where f_i is the polynomial associated with $\mathbf{y}_i = \left(y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})}, \ldots, y_{\varphi(d_1)+\cdots+\varphi(d_{i-1})+\varphi(d_i)-1}\right)$ as in the proof of Theorem 3.9 (a). This is a non-zero polynomial with integer coefficients and with degree strictly less than $\varphi(d_i)$, and $w_q^{m_i}$ is an element of order d_i in $(\mathbf{Z}/q\mathbf{Z})^\times$. Besides, the cardinality of $H_q^{(i)}$ satisfies the growth assumption (3.34). Thus, we can apply Proposition 3.12, which states that there exists $\varepsilon = \varepsilon(\delta) > 0$ and a rank N_{f_i} such that for all $q > N_{f_i}$ such that q is d-admissible,

$$\left| \sum_{a \in H_q^{(i)}} e\left(\frac{a f_i(w_q^{m_i})}{q}\right) \right| \ll_{f_i} \frac{|H_q^{(i)}|}{q^\varepsilon}$$

This estimate allows us to conclude on the convergence of the product (3.39) and this finishes the proof. □

Proof of case (b) *of Theorem* 3.13. Thanks to the same arguments as in the proof of Theorem 3.9 (b), it suffices to show that the following quantity

$$\prod_{i \in \{i_1,\ldots,i_s\}} \left[\frac{1}{|H_q^{(i)}|} \sum_{a_i \in H_q^{(i)}} e\left(\frac{a_i f(w_q^{m_i})}{q}\right) \right] \times \prod_{i \notin \{i_1,\ldots,i_s\}} e\left(\frac{a_i f(w_q^{m_i})}{q}\right) \tag{3.41}$$

converges to zero as q goes to infinity among the d-admissible integers (we recall that f is the polynomial $y_0 + y_1 X + \cdots + y_{\varphi(d)-1} X^{\varphi(d)-1}$ associated with the vector $\mathbf{y} \in \mathbf{Z}^{\varphi(d)}$, whose apparition comes from the application of Weyl's criterion).

Now, if we assume for a contradiction that for all $i \in \{i_1, \ldots, i_s\}$ we have

$$|H_q^{(i)}| < q^{\delta/s}$$

then this would contradict assumption (3.36). Thus, their exists $i \in \{i_1, \ldots, i_s\}$ such that

$$|H_q^{(i)}| \geqslant q^{\delta/s}$$

Let us stress that of course, this i may change as q varies. Then we can apply Proposition 3.12 to this specific i, and deduce that if q is larger than some constant N_f, depending only on f but not on i (because Proposition 3.12 allows *any* primitive d-th root in its statement), we have:

$$\frac{1}{|H_q^{(i)}|} \left| \sum_{a_i \in H_q^{(i)}} e\left(\frac{a_i f(w_q^{m_i})}{q}\right) \right| \ll_f \frac{1}{q^\varepsilon}$$

where $\varepsilon = \varepsilon(\delta/s)$ in the notations of the proposition. Thus the absolute value of (3.41) can be bounded above as follows for all $q > N_f$:

$$\left| \prod_{i \in \{i_1,\ldots,i_s\}} \left[\frac{1}{|H_q^{(i)}|} \sum_{a_i \in H_q^{(i)}} e\left(\frac{a_i f(w_q^{m_i})}{q}\right) \right] \times \prod_{i \notin \{i_1,\ldots,i_s\}} e\left(\frac{a_i f(w_q^{m_i})}{q}\right) \right| \ll_f \frac{1}{q^\varepsilon},$$

so it tends to zero as q goes to infinity, and this finishes the proof. □

Remark 3.14. As a very special case, the estimate of Theorem 3.11 allows one us to deduce a generalization of Myerson's lemma, which asserts that the sets

$$\left\{ \frac{a}{q} \left(1, w_q, \ldots, w_q^{\varphi(d)-1}\right) ;\ a \in \mathbf{Z}/q\mathbf{Z} \right\}, \tag{3.42}$$

where w_q is a primitive d-th root of unity modulo q, become equidistributed modulo 1 as q goes to infinity among the d-admissible integers (see Lemma 2.30 of Chapter 2).

Precisely, it gives a generalization of the equidistribution of the sets of type (3.42) to sets of the form

$$\left\{\frac{a}{q}\left(1, w_q, \dots, w_q^{\varphi(d)-1}\right);\ a \in H_q\right\}, \tag{3.43}$$

where H_q is a large enough subgroup of $(\mathbf{Z}/q\mathbf{Z})^\times$:

Corollary 3.15. *Let $d \geqslant 1$ and let $\delta > 0$. For all $q \in \mathcal{A}_d$, let w_q be an element of order d in $(\mathbf{Z}/q\mathbf{Z})^\times$. For each of these values of q, we also fix a subgroup H_q of $(\mathbf{Z}/q\mathbf{Z})^\times$. If the following growth condition is satisfied:*

$$|H_q| \geqslant q^\delta,$$

then the sets (3.43) become equidistributed modulo 1 as q tends to infinity among the d-admissible integers.

Proof. This is a direct consequence of Weyl's equidistribution criterion and the estimate of Proposition 3.12. □

3.A. On Gauss sums modulo prime powers

In this section, we quote some results on the absolute value of Gauss sums associated with possibly non-primitive Dirichlet characters. These estimates on Gauss sums have played a central role in the argument to prove Lemma 3.12. Since we are working with sums modulo prime powers, and not necessarily modulo primes, some subtleties arise from the non-primitivity of the characters involved, and we thought it would be useful to include a few facts in an appendix. Indeed, if χ is a Dirichlet character modulo m and ψ_a an additive character modulo m, there are two independent periodicity properties that come into play: the non-primitivity of χ and the non-primitivity of ψ_a if a is not coprime with m.

We begin by reviewing a few facts about Dirichlet characters, the reader is also referred to [54, chapter 3] and [85, chapter 9].
Let $m \geqslant 2$ be an integer. A Dirichlet character modulo m is a function $\chi\colon \mathbf{Z} \to \mathbf{C}$ such that:

$$|\chi(i)| = \begin{cases} 1 & \text{if } (i,m) = 1 \\ 0 & \text{otherwise,} \end{cases}$$

and for all $i, j \in \mathbf{Z}$, $\chi(ij) = \chi(i)\chi(j)$.

In other words, it is a function on $\mathbf{Z}$ obtained by extending a multiplicative character of the group $(\mathbf{Z}/m\mathbf{Z})^\times$ to the whole additive group $\mathbf{Z}/m\mathbf{Z}$ by setting its value at 0 when evaluated at residue classes not coprime with m, and then composing by the canonical map $\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$.
If n divides m, then we have a canonical ring homorphism

$$\pi_{m,n}\colon \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$$

so that if χ is a Dirichlet character modulo n, then $\chi \circ \pi_{m,n}$ is a Dirichlet character modulo m. If a Dirichlet character modulo m is obtained in this way for n a *proper* divisor of m, then we say that χ is *not primitive* and that it is *induced* by a character modulo n. Otherwise, it is called *primitive*.

- If m is an integer larger than or equal to 2, the additive characters modulo m will be denoted by ψ_a for $a \in \mathbf{Z}/m\mathbf{Z}$, where:

$$\begin{array}{rccc} \psi_a & : & \mathbf{Z}/m\mathbf{Z} & \to & \mathbf{C}^\times \\ & & x & \mapsto & e\left(\frac{ax}{m}\right) \end{array}$$

- If χ is Dirichlet character modulo m and ψ is an additive character modulo m, we denote their attached Gauss sum by:

$$\tau(\chi, \psi) := \sum_{x \in \mathbf{Z}/m\mathbf{Z}} \chi(x)\psi(x)$$

  Equivalently, one could also define the Gauss sum by summing over the units modulo m, since χ takes the value 0 outside of this set.

- If $\psi = \psi_1$, we simply denote by $\tau(\chi)$ the associated Gauss sum, that is:

$$\tau(\chi) := \sum_{x \in \mathbf{Z}/m\mathbf{Z}} \chi(x) e\left(\frac{x}{m}\right)$$

- The principal Dirichlet character modulo m is denoted by χ_0. For all $a \in \mathbf{Z}$ we have: $\chi_0(a) = 1$ if a and m are coprime, and $\chi_0(a) = 0$ otherwise.

Lemma 3.16 ([85, theorem 9.12 page 290]). *Let χ be a non-principal character modulo m. Assume that χ is induced by the primitive character $\chi^\star$ modulo $m^\star$. Then for all $a \in \mathbf{Z}$, if we denote by $d := (m, a)$ we have:*

$$\tau(\chi,\psi_a)=\begin{cases}0 \text{ if } d \text{ does not divide } \frac{m}{m^\star}\\ \overline{\chi}^\star\left(\frac{a}{d}\right)\chi^\star\left(\frac{m}{dm^\star}\right)\mu\left(\frac{m}{dm^\star}\right)\frac{\varphi(m)}{\varphi(m/d)}\tau(\chi^\star) \text{ if } d \text{ divides } \frac{m}{m^\star}\end{cases} \tag{3.44}$$

In particular, if χ is primitive (that is $m=m^\star$ and $\chi=\chi^\star$), we obtain:

$$\tau(\chi,\psi_a)=\tau(\chi)\overline{\chi}(a) \tag{3.45}$$

Remark 3.17. Equality (3.45) above also holds when χ is not primitive in the particular case where $(a,m)=1$. Indeed, in that case it follows from the fact that $x\mapsto ax$ permutes $\mathbf{Z}/m\mathbf{Z}$, since $a\in(\mathbf{Z}/m\mathbf{Z})^\times$.

When $\psi_a=\psi_1$, the statement takes a much simpler form, since only the non-primitivity of χ plays a role.

Lemma 3.18 ([54, lemma 3.1 page 48])**.** *Let χ be a non-principal Dirichlet character modulo m. Assume that χ is induced by the primitive character $\chi^\star$ modulo $m^\star$. Then:*

$$\tau(\chi)=\mu\left(\frac{m}{m^\star}\right)\chi^\star\left(\frac{m}{m^\star}\right)\tau(\chi^\star)$$

Moreover, if χ is primitive then:

$$|\tau(\chi)|=\sqrt{m}$$

Remark 3.19.

- When m is a prime number p, all the non-principal characters modulo m are primitive. Therefore the second assertion always holds for non-principal Dirichlet characters modulo a prime.
- Another case which will be interesting for us is the one where m is a non-trivial prime power. Let us say that $m=p^\alpha$ with $\alpha\geqslant 2$. Then, if χ is a non-primitive and non-principal character modulo m, its conductor $m^\star$ divides m, hence it is of the form p^β for some $0<\beta<\alpha$ (the inequalities are strict because $\beta=0$ would correspond to $\chi=\chi_0$ and $\beta=\alpha$ would correspond to χ primitive). Then p divides $m/m^\star=p^{\alpha-\beta}$, so $(m/m^\star,m^\star)>1$. We deduce that $\chi^\star\left(\frac{m}{m^\star}\right)=0$ because $\chi^\star$ is a character modulo $m^\star$. Thus, $\tau(\chi)=0$ as soon as χ is not primitive (and is not the principal character modulo m).

This last remark tells us that when m is a prime power, the sums $\tau(\chi)$ are either zero or associated with a primitive Dirichlet character χ, in which case $|\tau(\chi)|=\sqrt{m}$. However, the situation is not as simple when the additive character can be any ψ_a. In this case, the specialization of lemma 3.16 to the case of sums modulo prime powers gives the following corollary:

Corollary 3.20. *Let p be a prime number and $\alpha\geqslant 1$ be an integer. Let χ be a non-principal Dirichlet character modulo p^α, induced by the primitive character $\chi^\star$ modulo p^β for some $0<\beta\leqslant\alpha$. For all $a\in\mathbf{Z}$, we have $\tau(\chi,\psi_a)\neq 0$ if and only if the p-adic valuation of a equals $\alpha-\beta$, in which case we have:*

$$\tau(\chi,\psi_a)=\overline{\chi}^\star\left(\frac{a}{p^{\alpha-\beta}}\right)p^{\alpha-\beta}\tau(\chi^\star)$$

In particular:

$$|\tau(\chi,\psi_a)|=\begin{cases}p^{\alpha-\frac{\beta}{2}} \text{ if } v_p(a)=\alpha-\beta\\ 0 \text{ otherwise}\end{cases}$$

Proof. We apply lemma 3.16 with $m=p^\alpha$ and $m^\star=p^\beta$. We still denote by $d:=(a,m)$. Then d is a power of p, say $d=p^\gamma$.

- If $\gamma>\alpha-\beta$: then d does not divide $m/m^\star$ so the Gauss sum $\tau(\chi,\psi_a)$ is zero.

- If $\gamma \leqslant \alpha - \beta$: then d divides $m/m^\star$, hence:

$$\begin{aligned}\tau(\chi, \psi_a) &= \overline{\chi}^\star\left(\frac{a}{p^\gamma}\right)\chi^\star\left(p^{\alpha-\beta-\gamma}\right)\mu\left(p^{\alpha-\beta-\gamma}\right)\frac{\varphi(p^\alpha)}{\varphi(p^{\alpha-\gamma})}\tau(\chi^\star)\\ &= \overline{\chi}^\star\left(\frac{a}{p^\gamma}\right)\chi^\star\left(p^{\alpha-\beta-\gamma}\right)\mu\left(p^{\alpha-\beta-\gamma}\right)\frac{(p-1)p^{\alpha-1}}{(p-1)p^{\alpha-\gamma-1}}\tau(\chi^\star)\\ &= \overline{\chi}^\star\left(\frac{a}{p^\gamma}\right)\chi^\star\left(p^{\alpha-\beta-\gamma}\right)\mu\left(p^{\alpha-\beta-\gamma}\right)p^\gamma\tau(\chi^\star)\end{aligned}$$

  Now, as soon as $\gamma < \alpha - \beta$, we have $\chi^\star(p^{\alpha-\beta-\gamma}) = 0$ because then p divides $p^{\alpha-\beta-\gamma}$ and $\chi^\star$ is a Dirichlet character modulo p^β. This shows that $\tau(\chi, \psi_a)$ is non-zero if and only if $\gamma = \alpha - \beta$, that is: $d = (a, p^\alpha) = p^{\alpha-\beta}$, which is equivalent to $v_p(a) = \alpha - \beta$ since $\beta > 0$ (here we use the fact that χ is not the principal character modulo p^α). In this case, we have:

$$\begin{aligned}\tau(\chi, \psi_a) &= \overline{\chi}^\star\left(\frac{a}{p^{\alpha-\beta}}\right)\chi^\star(1)\,\mu(1)\,p^{\alpha-\beta}\tau(\chi^\star)\\ &= \overline{\chi}^\star\left(\frac{a}{p^{\alpha-\beta}}\right)p^{\alpha-\beta}\tau(\chi^\star)\end{aligned}$$

  Finally, $|\tau(\chi^\star)| = p^{\beta/2}$ thanks to the second part of lemma 3.18 since $\chi^\star$ is a primitive character modulo p^β. The assertion on $|\tau(\chi, \psi_a)|$ follows from that.

□

Remark 3.21. This last corollary can also be found in [5, section 1.6] with a self-contained proof which does not rely on the more general case we stated in Lemma 3.16.

3.B. Some complements on Bourgain-Glibichuk-Konyagin's estimate

I thank Élise Goujard and Pascal Autissier for asking me the question of the optimality of the growth condition in Bourgain's estimate. This question encouraged me to gain a better understanding of the state of the art and led to the writing of this appendix.

In the case of prime moduli, Bourgain-Glibichuk-Konyagin's estimate asserts that for any $\delta > 0$, there exists $\varepsilon = \varepsilon(\delta) > 0$ such that for all p, for all subgroup G of $\mathbf{F}_p^\times$ satisfying

$$|G| \geqslant p^\delta \tag{3.46}$$

we have

$$\max_{a\in\mathbf{F}_p^\times} \left|\sum_{x\in G} e\left(\frac{ax}{p}\right)\right| \ll_\delta \frac{|G|}{p^\varepsilon}.$$

In particular,

$$\max_{a\in\mathbf{F}_p^\times} \left|\sum_{x\in G} e\left(\frac{ax}{p}\right)\right| \underset{p\to\infty}{=} o\left(|G|\right), \tag{3.47}$$

but this only holds for large enough subgroups, in the sense of condition (3.46). In this section, we address the question of the optimality of this growth condition. In other words, is there a hope to obtain (3.47) for subgroups whose cardinality is less than any power of p? In [68], the following theorem explains that there is no hope for subgroups whose cardinality is at most a constant times $\log(p)$. This does not completely answer our question, but still, this tells us that subgroups that are too small (even though their cardinality goes to infinity) cannot satisfy (3.47).

Theorem 3.22 ([68, Theorem 1.8]). *For all $u > 0$, there exist $p(u)$ and $\eta(u) > 0$ such that for all $p \geqslant p(u)$, if G is a subgroup of $\mathbf{F}_p^\times$ satisfying*

$$|G| \leqslant u\log(p),$$

then

$$\max_{a\in\mathbf{F}_p^\times} \left|\sum_{x\in G} e\left(\frac{ax}{p}\right)\right| > \eta(u)|G|.$$

In this section we give the proof of this theorem, following the arguments of *loc. cit.* and expanding some details.

Notation. For any prime p and any subgroup G of $\mathbf{F}_p^\times$, we denote by

$$M_p(G) := \max_{a\in\mathbf{F}_p^\times} \left|\sum_{x\in G} e\left(\frac{ax}{p}\right)\right|$$

and by $D_p(a, G)$ the discrepancy of the set $\left\{\left\{\frac{ax}{p}\right\},\ x \in G\right\}$:

$$D_p(a,G) := \sup_{I\in\mathscr{I}} \left|\frac{\#\left\{x\in G,\ \left\{\frac{ax}{p}\right\}\in I\right\}}{|G|} - \lambda(I)\right|$$

We start by stating and proving some preparatory lemmas for the proof of Theorem 3.22.

A consequence of Erdös-Turán inequality.

Lemma 3.23 ([68, p.7 and 8]). *For all prime p, for all subgroup G of $\mathbf{F}_p^\times$, for all $\eta \in \left[\frac{1}{p}, 1\right[$, if*

$$\frac{M_p(G)}{|G|} \leqslant \eta$$

then for all $a \in \mathbf{F}_p^\times$,

$$D_p(a, G) \leqslant 6\eta \left(\ln\left(\eta^{-1}\right) + 1\right).$$

Proof. Thanks to Erdös-Turán inequality [29, Theorem 1.21], for any sequence $z_1, \ldots, z_N$ of elements of $\mathbf{R}/\mathbf{Z}$, we have that for all $H \geqslant 1$ and all $N \geqslant 1$, the discrepancy of the sequence is bounded above by

$$\frac{3}{2}\left(\frac{2}{H+1} + \sum_{0<|m|\leqslant H} \frac{1}{|m|}\left|\frac{1}{N}\sum_{n=1}^{N} e(mz_n)\right|\right)$$

Applying this inequality to the finite sequence of the points of the set

$$\left\{\left\{\frac{ax}{p}\right\},\ x \in G\right\}$$

one obtains

$$D_p(a, G) \leqslant \frac{3}{H+1} + \frac{3}{2}\sum_{0<|m|\leqslant H} \frac{1}{|m|}\left|\frac{1}{|G|}\sum_{x\in G} e\left(m\frac{ax}{p}\right)\right|.$$

Now if $H < p$, then for all $0 < |m| \leqslant H$, ma is invertible modulo p, so

$$\left|\sum_{x\in G} e\left(m\frac{ax}{p}\right)\right| \leqslant M_p(G),$$

from which we deduce

$$\begin{aligned} D_p(a, G) &\leqslant \frac{3}{H+1} + \frac{3M_p(G)}{2|G|}\sum_{0<|m|\leqslant H}\frac{1}{|m|} \\ &= \frac{3}{H+1} + \frac{3M_p(G)}{|G|}\sum_{m=1}^{H}\frac{1}{m} \\ &\leqslant \frac{3}{H+1} + \frac{3M_p(G)}{|G|}(1+\ln(H)) \end{aligned}$$

Now, assume that

$$\frac{M_p(G)}{|G|} \leqslant \eta \tag{3.48}$$

for some $\eta \in \left[\frac{1}{p}, 1\right[$. Then we can take

$$H := \left\lfloor \frac{1}{\eta\left(\ln\left(\eta^{-1}\right)+1\right)} \right\rfloor$$

It satisfies $1 \leqslant H < p$, so we can use this value of H in the estimate of $D_p(a, G)$ previously obtained, namely:

$$D_p(a, G) \leqslant \frac{3}{H+1} + \frac{3M_p(G)}{|G|}(1+\ln(H)).$$

Then,

- First, we have
$$\frac{3}{H+1} \leqslant 3\eta\left(\ln\left(\eta^{-1}\right)+1\right)$$
using $\frac{1}{\lfloor x\rfloor+1} \leqslant \frac{1}{x}$.
- Second, we have
$$1+\ln(H) \leqslant 1+\ln\left(\frac{\eta^{-1}}{1+\ln\left(\eta^{-1}\right)}\right) \leqslant 1+\ln\left(\eta^{-1}\right)$$
using $\lfloor x\rfloor \leqslant x$.

Therefore, remembering that we assumed that (3.48) holds, we conclude that

$$D_p(a,G) \leqslant 6\eta\left(\ln\left(\eta^{-1}\right)+1\right).$$

□

We now turn to a second preparatory lemma, which belongs to the field of diophantine approximation.

Dirichlet's simultaneous approximation theorem. We will introduce the result as a corollary of the following slightly more general theorem:

Theorem 3.24 ([95, Theorem 1.E]). *Let $(\alpha_{i,j})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m}$ be nm real numbers, and let $Q>1$ be an integer. Then there exist integers $a_1,\dots,a_m,b_1,\dots,b_m$ such that*

$$1 \leqslant \max(|a_1|,\dots,|a_m|) < Q^{n/m}$$

and for all $i\in\{1,\dots,n\}$,

$$\left|\left(a_1\alpha_{i,1}+\cdots+a_m\alpha_{i,m}\right)-b_i\right| \leqslant \frac{1}{Q}.$$

Moreover, in the remark following the statement of this theorem in [95], it is written that one may drop the condition that Q is an integer, using a theorem of Blichfeldt [95, Theorem 2.A]. Taking this remark into account and $m=1$ in the previous theorem, one obtains the following corollary, which is the actual version that we will use in the proof of Theorem 3.22.

Corollary 3.25 (Dirichlet's simultaneous approximation theorem). *Let $\alpha_1,\dots,\alpha_n$ be n real numbers, and let $Q>1$ (not necessarily an integer). Then there exist integers $a,b_1,\dots,b_n$ such that*

$$1 \leqslant |a| < Q^n \tag{3.49}$$

and for all $i\in\{1,\dots,n\}$,

$$|a\alpha_i - b_i| \leqslant \frac{1}{Q}.$$

Remark 3.26. Up to replacing a by $-a$ and b_i by $-b_i$, we can always assume that a satisfies $1\leqslant a<Q^n$. In other words, the conclusion of Corollary 3.25 is still true if we remove the absolute value in (3.49).

In the case where Q is an integer, the above corollary can be proved using only the pigeonhole principle. However, in the proof of Theorem 3.22, we use the version where Q is not an integer, so we really need to include this more general statement.

Proof of Corollary 3.25 when Q is an integer. We consider, for $0\leqslant c<Q^n$, the Q^n points in $[0,1]^n$:

$$\mathbf{x}_c := \begin{pmatrix} \{c\alpha_1\} \\ \vdots \\ \{c\alpha_n\} \end{pmatrix}$$

(where $\{\beta\}$ denotes the fractional part of a real number β). We denote by $\mathbf{1}$ the point

$$\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

of $[0,1]^n$. Then the set $\mathcal{X} := \{\mathbf{x}_c,\ 0 \leqslant c < Q^n\} \cup \{\mathbf{1}\}$ is made of $Q^n + 1$ points in $[0,1]^n$. Now we split the unit cube $[0,1]^n$ into Q^n smaller cubes of side $1/Q$, in the most natural way. By the pigeonhole principle, there must exist two points of $\mathcal{X}$ which belong to the same cube of side $1/Q$.

- If one of these points is $\mathbf{1}$, this means that there exists $c \in \{0, \dots, Q^n - 1\}$ such that $\mathbf{x}_c$ belong to the cube of side $1/Q$ containing $\mathbf{1}$. Of course, it cannot be the point $\mathbf{x}_0$, which is at the opposite corner of the unit cube $[0,1]^n$, hence too far away. Therefore, c belongs to $\{1, \dots, Q^n - 1\}$, and the fact that $\mathbf{x}_c$ belongs to the small cube containing $\mathbf{1}$ precisely means that there exist integers $b_1, \dots, b_n$ such that for all $i \in \{1, \dots, n\}$,

  $$b_i - 1/Q \leqslant c\alpha_i \leqslant b_i$$

  because the fractional parts of the $c\alpha_i$ are all close to 1. We get the conclusion by taking $a = c$.

- Otherwise, we have two points $\mathbf{x}_c$ and $\mathbf{x}_d$ belonging to the same cube of side $1/Q$, associated with c and d satisfying $0 \leqslant c < d < Q^n$. This implies that for all $i \in \{1, \dots, n\}$,

  $$|\{d\alpha_i\} - \{c\alpha_i\}| \leqslant 1/Q$$

  Now we use the fact that $\beta = \lfloor \beta \rfloor + \{\beta\}$ for any real number β, to see that

  $$|\{d\alpha_i\} - \{c\alpha_i\}| = |(d-c)\alpha_i - b_i|,$$

  where $b_i = \lfloor d\alpha_i \rfloor - \lfloor c\alpha_i \rfloor \in \mathbf{Z}$. This concludes the proof by taking $a = d - c$.

□

Before actually proving the main theorem of this section, we thought that a short preview of the strategy might be useful.

Strategy of the proof of Theorem 3.22. As far as I understand, the proof is guided by the following ideas.

1. If the subgroup G of $\mathbf{F}_p^\times$ is "small" (in the sense that $|G| \leqslant u \log(p)$), then

   - One can find some $a \in \mathbf{F}_p^\times$ such that most of the fractional parts $\left\{\frac{ax}{p}\right\}$ for $x \in G$ belong to some "short" interval. This is essentially the pigeonhole principle, since there are many a in $\mathbf{F}_p^\times$ compared to the size of the subgroup. The quantitative version of this informal description of this step is provided by Dirichlet's simultaneous approximation theorem.
   - The previous step allows one to deduce a lower bound for the discrepancy $D_p(a, G)$ of the set $\left\{\left\{\frac{ax}{p}\right\},\ x \in G\right\}$, which is natural because we chose a so that most of the fractional parts belong to a short interval, so we are in some sense "far from equidistribution".

   So informally:

   $$|G| \text{ small} \implies \text{lower bound for } D_p(a, G) \text{ for some } a \in \mathbf{F}_p^\times$$

2. On the other hand, if the exponential sums over G:

   $$\sum_{x \in G} e\left(\frac{bx}{p}\right)$$

are "small", in the sense that $M_p(G) = o(|G|)$, then it follows from Erdös-Turán inequality (in the form of Lemma 3.23) that the discrepancy $D_p(a, G)$ is also small. So informally

$$\left|\sum_{x\in G} e\left(\frac{bx}{p}\right)\right| \text{ small for all } b \in \mathbf{F}_p^\times \implies \text{ upper bound for } D_p(a,G) \text{ for all } a \in \mathbf{F}_p^\times$$

Thus, we see that $|G|$ being small and the exponential sums over G being small can lead to contradictory inequalities, so that both cannot happen at the same time. This will prove that if $|G|$ is too small, then the exponential sums over G cannot all be too small. Of course, this was just an informal overview of the proof, but now we need to turn the word "small" into quantitative estimates in order to make the argument work.

Proof of Theorem 3.22. Let p be a prime number, and let G be a subgroup of $\mathbf{F}_p^\times$. Let us denote by $t := |G|$ and let X denote any subset of G, with cardinality $T \leqslant t$ (to be adjusted later in the proof). Let $x_1, \dots, x_T \in \{1, \dots, p-1\}$ be the unique lifts of the elements of X. For all $i \in \{1, \dots, T\}$, we let

$$\alpha_i := \frac{x_i}{p}.$$

Then we apply Corollary 3.25 to the real numbers $\alpha_1, \dots, \alpha_T$, with $Q := p^{1/T}$. This gives the existence of integers $a, b_1, \dots, b_T$ such that

$$1 \leqslant a < p$$

and for all $i \in \{1, \dots, T\}$,

$$|a\alpha_i - b_i| \leqslant p^{-1/T}.$$

This implies that for all $i \in \{1, \dots, T\}$,

$$d\left(\frac{ax_i}{p}, \mathbf{Z}\right) \leqslant p^{-1/T}.$$

We deduce that there exists an interval $[\alpha, \beta[\subset [0,1[$ with $\beta - \alpha \leqslant p^{-1/T}$ and a subset Y of X, with $|Y| \geqslant T/2$, such that for all $y \in Y$:

$$\left\{\frac{ay}{p}\right\} \in [\alpha, \beta[.$$

We deduce the following lower bound for the discrepancy of the set $\left\{\left\{\frac{ax}{p}\right\},\ x \in G\right\}$:

$$\begin{aligned} D_p(a,G) &:= \sup_{I\in\mathscr{I}} \left|\frac{\#\left\{x\in G,\ \left\{\frac{ax}{p}\right\}\in I\right\}}{|G|} - \lambda(I)\right| \\ &\geqslant \left|\frac{\#\left\{x\in G,\ \left\{\frac{ax}{p}\right\}\in [\alpha,\beta[\right\}}{|G|} - (\beta-\alpha)\right| \\ &\geqslant \frac{\#\left\{x\in G,\ \left\{\frac{ax}{p}\right\}\in [\alpha,\beta[\right\}}{|G|} - (\beta-\alpha) \\ &\geqslant \frac{|Y|}{t} - p^{-1/T} \geqslant \frac{T}{2t} - p^{-1/T}. \end{aligned}$$

- If $t \leqslant \log(p)$, we take T to be equal to t (that is: X is equal to the whole subgroup G). Then

$$D_p(a,G) \geqslant \frac{1}{2} - \exp(-\frac{\log p}{t}) \geqslant \frac{1}{2} - \frac{1}{\mathrm{e}}.$$

- Otherwise, we have $\log p < t \leqslant u \log p$, so $u > 1$. Then we take T to be equal to $\lfloor \frac{\log p}{3u} \rfloor$. For all p large enough, say larger than some $j(u)$ which can be explicited, we have $\frac{\log p}{3u} \geqslant 1$, and the following inequality holds:
$$\lfloor \frac{\log p}{3u} \rfloor > \frac{\log p}{6u}$$
because for all $x \geqslant 1$, $\lfloor x \rfloor \geqslant x/2$. Therefore, we have the following lower bound for the discrepancy $D_p(a, G)$:
$$\begin{aligned} D_p(a, G) &\geqslant \frac{\log p}{12ut} - \exp\left(-\frac{\log p}{\lfloor \frac{\log p}{3u} \rfloor}\right) \\ &\geqslant \frac{1}{12u^2} - e^{-3u} > 0. \end{aligned}$$

Thus, for all $u > 0$, there exist $j(u)$ and $c(u) > 0$ such that for all $p \geqslant j(u)$ the discrepancy $D_p(a, G)$ satisfies
$$D_p(a, G) \geqslant c(u) \tag{3.50}$$
for any subgroup G of $\mathbf{F}_p^\times$ such that $|G| \leqslant u \log(p)$ and for a suitable $a \in \mathbf{F}_p^\times$. Indeed, it suffices to take
$$c(u) := \begin{cases} \frac{1}{2} - \frac{1}{\mathrm{e}} & \text{if } u \leqslant 1 \\ \frac{1}{12u^2} - e^{-3u} & \text{if } u > 1. \end{cases}$$
Now let $\eta := \eta(u) \in]0, 1[$ be such that $6\eta\left(\ln\left(\eta^{-1}\right) + 1\right) < c(u)$. Suppose that there exists $p \geqslant p(u) := \max\left(j(u), \frac{1}{\eta(u)}\right)$ and a subgroup G of $\mathbf{F}_p^\times$ such that $|G| \leqslant u \log(p)$ and
$$\frac{M_p(G)}{|G|} \leqslant \eta.$$
On one hand, since $p \geqslant j(u)$, we can apply (3.50). On the other hand, the condition $p \geqslant \frac{1}{\eta}$ ensures that we are in the conditions of application of Lemma 3.23. Therefore,
$$c(u) \leqslant D_p(a, G) \leqslant 6\eta\left(\ln\left(\eta^{-1}\right) + 1\right)$$
for a suitable $a \in \mathbf{F}_p^\times$, which gives a contradiction with our choice of η. Thus, for all $p \geqslant p(u)$, for all subgroup G of $\mathbf{F}_p^\times$ such that $|G| \leqslant u \log(p)$, we have
$$M_p(G) > \eta |G|.$$
This concludes the proof. □

Remark 3.27. The obstruction to equidistribution of Theorem 3.22 may be sharp! Indeed, a conjecture of Montgomery, Vaughan and Wooley, stated in [84], implies the equidistribution modulo 1 of the $\{x/p;\ x \in G\}$ as soon as the multiplicative subgroup G satisfies
$$\frac{|G|}{\log p} \underset{p \to \infty}{\longrightarrow} +\infty.$$
Indeed, the conjecture is the following (we state it as in [14], because it is written in a form which is more relevant here):
Conjecture.
$$\max_{a \in \mathbf{F}_p^\times} \left| \sum_{x \in G} e\left(\frac{ax}{p}\right) \right| < \min\left(p^{1/2}, C(\log p)^{1/2} |G|^{1/2}\right).$$
This conjecture is also cited in [99], where it is not really used, but where it is said that it could be interesting to study whether it could have some implications in the study of Artin's conjecture on primitive roots (which states that for a given non-square integer $a \neq -1$, there is a positive proportion of primes such that $a \pmod p$ generates the cyclic group $\mathbf{F}_p^\times$).

Chapter 4

Equidistribution of exponential sums indexed by the roots of a polynomial

The two previous chapters consisted of a study of exponential sums over subgroups of fixed cardinality, which can also be described as sums indexed by the roots of unity in some finite fields. In this chapter, we extend these equidistribution results to the case of exponential sums indexed by the roots of an arbitrary monic polynomial $g \in \mathbf{Z}[X]$, such as

$$\sum_{\substack{x \in \mathbf{F}_q \\ g(x) \equiv 0 \,(\mathrm{mod}\, q)}} e\left(\frac{ax}{q}\right).$$

Under some natural conditions on the prime numbers q (which already appeared in the previous chapters in the form of the condition $p \equiv 1 \,(\mathrm{mod}\, d)$), we show that these sums become equidistributed in $\mathbf{C}$ with respect to a measure μ_g which is related to the module of additive relations between the complex roots of g. The study of this module of additive relations can be approached via the representation theory of the Galois group of the polynomial g. This chapter is part of the article [77], which is a joint work with E. Kowalski.
We gathered some needed facts on the duality of compact abelian groups in Appendix 4.A. We also assume some familiarity with the terminology of ramification in the number field setting, but the necessary definitions are recalled in Appendix 4.B for completeness.

Contents

4.1. A better setting for the previous results on sums indexed by a subgroup of fixed cardinality

In this first section, we recall the method of proof we used in Chapter 2 and explain some of its limitations. Then we introduce the important change of point of view brought by E. Kowalski, which overcomes the difficulties of the previous method and opens the door to new generalizations.

4.1.1. Definition of the new random variables

For any field K, we denote by $\mu_d(K)$ the set of d-th roots of unity in K, and we put $\boldsymbol{\mu}_d := \mu_d(\mathbf{C})$.
In Chapter 2, and in the previous references [32] and [44], the sums under consideration were

$$\mathrm{S}_q(a,d) := \sum_{x \in \mu_d(\mathbf{F}_q)} e\left(\frac{ax}{q}\right) \tag{4.1}$$

for prime numbers $q \equiv 1 \pmod d$ (and generalizations of these modulo prime powers). More precisely, the uniform distribution of the sets

$$\{\mathrm{S}_q(a,d);\ a \in \mathbf{F}_q\}$$

was investigated as q goes to infinity. The proof went along the following lines: we chose for each q a primitive d-th root of unity modulo q, which we denoted by w_q, and then wrote the sum $S_q(a,d)$ as

$$\sum_{k=0}^{d-1} e\left(\frac{aw_q^k}{q}\right).$$

Then we studied the equidistribution by proving that the tuples

$$\left(e\left(\frac{aw_q^k}{q}\right)\right)_{0 \leqslant k \leqslant \varphi(d)-1} \in (\mathbf{S}^1)^{\varphi(d)} \tag{4.2}$$

become equidistributed in $(\mathbf{S}^1)^{\varphi(d)}$, as a varies in $\mathbf{F}_q$ and q goes to infinity, and that the other terms of the sum (those involving higher powers of w_q) can be expressed as Laurent polynomials in these $\varphi(d)$ variables.
This first approach relies a lot on the choice of the primitive root w_q and on the natural ordering of the roots of unity that comes with it. For that reason, it does not seem clear how to extend the method to handle sums such as

$$\sum_{\substack{x \in \mathbf{F}_q \\ g(x) \equiv 0 \pmod q}} e\left(\frac{ax}{q}\right)$$

for any fixed polynomial $g \in \mathbf{Z}[X]$.

Question: *How can we get around the issue of ordering the roots?*

A first idea would be to replace the ordered tuple

$$\left(e\left(\frac{aw_q^k}{q}\right)\right)_{0 \leqslant k \leqslant d-1} \in (\mathbf{S}^1)^{d} \tag{4.3}$$

by the map

$$\begin{array}{rccc} V_q(a) & : & \mu_d(\mathbf{F}_q) & \to & \mathbf{S}^1 \\ & & x & \mapsto & e\left(\frac{ax}{q}\right) \end{array} \tag{4.4}$$

Then, the equidistribution result we are aiming at naturally leads to introducing the random variables

$$\begin{array}{rccc} V_q & : & \mathbf{F}_q & \to & \mathrm{C}(\mu_d(\mathbf{F}_q), \mathbf{S}^1) \\ & & a & \mapsto & V_q(a) \end{array}$$

where $\mathbf{F}_q$ is seen as a probability space with the normalized counting measure, and $\mathrm{C}(\mu_d(\mathbf{F}_q), \mathbf{S}^1)$ denotes the set of (continuous) maps from $\mu_d(\mathbf{F}_q)$ to $\mathbf{S}^1$.
However, there is still an issue because the random variables V_q do not take values in the same space (although $\mathrm{C}(\mu_d(\mathbf{F}_q), \mathbf{S}^1) \simeq (\mathbf{S}^1)^d$ for any $q \equiv 1 \,(\mathrm{mod}\, d)$). Indeed, we cannot speak about the convergence in law of the sequence $(V_q)_{q \equiv 1 \,(\mathrm{mod}\, d)}$. Instead, we would like to define random variables $U_q \colon \mathbf{F}_q \to C(\boldsymbol{\mu}_d, \mathbf{S}^1)$ where $\boldsymbol{\mu}_d$ is always the same set of roots of unity in $\mathbf{C}$ for any q, while keeping track of the arithmetic meaning of taking in fact roots of unity in different finite fields.
In order to do this, it is convenient to use some algebraic number theory and to work with ideals of the cyclotomic field $K := \mathbf{Q}(\boldsymbol{\mu}_d)$. We denote by $\mathcal{O}_K$ the ring of integers of K and we introduce two notions of d-admissible ideals, which will play the role of the condition $q \equiv 1 \,(\mathrm{mod}\, d)$.

Definition 4.1. *Let us define*

- $\mathcal{R}_d$ *to be the set of prime ideals of* $\mathcal{O}_K$ *with residual degree equal to* 1*, and*
- $\mathcal{S}_d$ *to be the set of prime ideals of* $\mathcal{O}_K$ *which are unramified and have residual degree* 1 *(equivalently: the ideals which lie above a prime* $q \in \mathbf{Z}$ *which is totally split in* K*).*

The restriction to prime ideals living in $\mathcal{R}_d$ allows us to define random variables with values in the same space. Indeed, for each prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ with residual degree 1 (lying above q, say), the natural map $\iota_{\mathfrak{p}} \colon \mathbf{F}_q \to \mathcal{O}_K/\mathfrak{p}$ is an isomorphism, so if we denote by $\tau_{\mathfrak{p}} \colon \mathcal{O}_K/\mathfrak{p} \to \mathbf{F}_q$ its inverse, we have the following composition of maps

$$\boldsymbol{\mu}_d \hookrightarrow \mathcal{O}_K \overset{\varpi_{\mathfrak{p}}}{\to} \mathcal{O}_K/\mathfrak{p} \overset{\tau_{\mathfrak{p}}}{\to} \mathbf{F}_q$$

where $\varpi_{\mathfrak{p}}$ denotes the reduction modulo $\mathfrak{p}$ from $\mathcal{O}_K$ to $\mathcal{O}_K/\mathfrak{p}$.

Remark 4.2. If we further assume that q is totally split in K (that is: $\mathfrak{p} \in \mathcal{S}_d$), the above composition induces a bijection between $\boldsymbol{\mu}_d$ and $\mu_d(\mathbf{F}_q)$ (this is proved at Proposition 4.31 in a more general context). This fact will be useful to derive equidistribution results concerning exponential sums, but the assumption $\mathfrak{p} \in \mathcal{R}_d$ is already sufficient to define the suitable random variables and prove an equidistribution result.

We now have all the elements to define the random variables which will replace the ordered tuple (4.3).

Definition 4.3. *For all* $\mathfrak{p} \in \mathcal{R}_d$ *we define a random variable* $U_{\mathfrak{p}}$ *on the probability space* $\mathcal{O}_K/\mathfrak{p}$ *(endowed with the discrete* σ*-algebra and the normalized counting measure) as follows:*

$$\begin{array}{rccc} U_{\mathfrak{p}} & : & \mathcal{O}_K/\mathfrak{p} & \to & \mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1) \\ & & a & \mapsto & U_{\mathfrak{p}}(a) \end{array}$$

where

$$\begin{array}{rccc} U_{\mathfrak{p}}(a) & : & \boldsymbol{\mu}_d & \to & \mathbf{S}^1 \\ & & x & \mapsto & e\left(\frac{\tau_{\mathfrak{p}}(a\varpi_{\mathfrak{p}}(x))}{q}\right). \end{array}$$

Remark 4.4. Since $\mathfrak{p}$ has residual degree 1, the prime q in the definition of $U_{\mathfrak{p}}(a)$ is the norm $\|\mathfrak{p}\|$ of the ideal $\mathfrak{p}$ (that is: the cardinality of the residue field $\mathcal{O}_K/\mathfrak{p}$). Thus we can define $U_{\mathfrak{p}}$ only in terms of the ideal $\mathfrak{p}$, by writing

$$U_{\mathfrak{p}}(a)(x) = e\left(\frac{\tau_{\mathfrak{p}}(a\varpi_{\mathfrak{p}}(x))}{\|\mathfrak{p}\|}\right).$$

Our next step consists in proving the convergence in law of the random variables $U_{\mathfrak{p}}$, as $\|\mathfrak{p}\|$ goes to infinity. This step corresponds to the uniform distribution statement for the tuples (4.2) which was handled in earlier references by the use of Myerson's lemma. Once the convergence of the random variables $U_{\mathfrak{p}}$ is proved, the compatibility between convergence in law and continuous mappings allows one to deduce easily the convergence in law of the random variables

$$\begin{array}{rccc} \mathrm{S}_{\mathfrak{p}} & : & \mathcal{O}_K/\mathfrak{p} & \to & \mathbf{C} \\ & & a & \mapsto & \sum_{x\in\boldsymbol{\mu}_d} e\left(\frac{\tau_{\mathfrak{p}}(a\varpi_{\mathfrak{p}}(x))}{\|\mathfrak{p}\|}\right) \end{array}$$

Finally, to recover the previous results about sums of type (4.1), it remains to prove that $\tau_{\mathfrak{p}} \circ \varpi_{\mathfrak{p}}$ induces a bijection between $\boldsymbol{\mu}_d$ and $\mu_d(\mathbf{F}_q)$. This holds under the stronger assumption that $\mathfrak{p} \in \mathcal{S}_d$, and will be proved in Proposition 4.31 in greater generality. This number field approach can actually be generalized to explain uniform distribution phenomena for exponential sums indexed by $\mathrm{Z}_g(\mathbf{F}_q)$ for any monic polynomial $g \in \mathbf{Z}[X]$. Moreover, it also extends to sums indexed by the roots of g modulo prime powers.

4.1.2. Some preparation for the convergence of the new random variables

As we will see, the object which governs the limiting distribution of the sequence of random variables $(U_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{R}_d}$ is the module of additive relations with coefficients in $\mathbf{Z}$ between the elements of $\boldsymbol{\mu}_d$. We introduce that object and set some extra notations in the following definition.

Definition 4.5. *Let $d \geqslant 1$ be an integer. We denote by $\mathrm{C}(\boldsymbol{\mu}_d, X)$ the set of maps from $\boldsymbol{\mu}_d$ to any set X. Moreover,*

- *R_d denotes the submodule of $\mathrm{C}(\boldsymbol{\mu}_d, \mathbf{Z})$ of additive relations between the elements of $\boldsymbol{\mu}_d$:*

$$\mathrm{R}_d := \left\{ \alpha \colon \boldsymbol{\mu}_d \to \mathbf{Z},\ \sum_{x\in\boldsymbol{\mu}_d} \alpha(x)x = 0 \right\},$$

- *H_d denotes the subgroup of $\mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1)$ which is "dual" to R_d in the following sense:*

$$\mathrm{H}_d := \left\{ f \in \mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1),\ \forall \alpha \in \mathrm{R}_d,\ \prod_{x\in\boldsymbol{\mu}_d} f(x)^{\alpha(x)} = 1 \right\}$$

Remark 4.6. As H_d is a closed subgroup of the compact abelian group $\mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1)$, it is a compact abelian group, hence has a unique probability Haar measure. Therefore, it makes sense to speak about uniformly distributed random variables on H_d in the sense of Appendix 4.A.

Now, to prove the desired convergence in law, we will apply Weyl's criterion in the form of Theorem 4.71. In order to do that, we need a good understanding of the characters of the groups $\mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1)$ and H_d. Since $\mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1)$ is nothing more than an unordered version of $(\mathbf{S}^1)^d$, its characters are described by a small variation of Proposition 4.72 of the Appendix. More precisely, we have the following definition and proposition.

Definition 4.7. *For all $\alpha : \boldsymbol{\mu}_d \to \mathbf{Z}$, we denote by η_α the following character of $\mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1)$:*

$$\begin{array}{rccc} \eta_\alpha & : & \mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1) & \to & \mathbf{S}^1 \\ & & f & \mapsto & \displaystyle\prod_{x\in\boldsymbol{\mu}_d} f(x)^{\alpha(x)} \end{array}$$

Proposition 4.8. *The map*

$$\begin{array}{rccc} \eta & : & \mathrm{C}(\boldsymbol{\mu}_d, \mathbf{Z}) & \to & \widehat{\mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1)} \\ & & \alpha & \mapsto & \eta_\alpha \end{array} \tag{4.5}$$

is an isomorphism of abelian groups.

Proof. Since $\mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1) \simeq (\mathbf{S}^1)^d$ via the choice of a primitive root of unity, the surjectivity statement is a small variation on Proposition 4.72. For the injectivity, assume that α is not the zero map and let $x_0 \in \boldsymbol{\mu}_d$ be such that $\alpha(x_0) = m \in \mathbf{Z} \setminus \{0\}$. Then take $f : \boldsymbol{\mu}_d \to \mathbf{S}^1$ such that $f(x_0) \in \mathbf{S}^1 \setminus \boldsymbol{\mu}_m$ and for all $x \in \boldsymbol{\mu}_d \setminus \{x_0\}$, $f(x) = 1$. Then

$$\eta_\alpha(f) = \prod_{x \in \boldsymbol{\mu}_d} f(x)^{\alpha(x)} = f(x_0)^m \neq 1$$

since $f(x_0)$ is not an m-th root of unity. Therefore, $(\alpha \neq 0 \implies \eta_\alpha \neq 1)$, which proves the injectivity. □

Proposition 4.9. *Let $\alpha \in \mathrm{C}(\boldsymbol{\mu}_d, \mathbf{Z})$. The character η_α is trivial on H_d if and only if $\alpha \in \mathrm{R}_d$.*

Proof. We keep the notation η for the isomorphism (4.5). Then by definition of H_d, we have

$$\mathrm{H}_d = \left\{ f \in \mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1),\ \forall \chi \in \eta(\mathrm{R}_d),\ \chi(f) = 1 \right\} = \eta(\mathrm{R}_d)^\perp$$

with the notation "$^\perp$" from Definition 4.69. Thus,

$$\eta_\alpha \text{ is trivial on } \mathrm{H}_d \iff \eta_\alpha \in \mathrm{H}_d^\perp \iff \eta_\alpha \in \left(\eta(\mathrm{R}_d)^\perp\right)^\perp = \eta(\mathrm{R}_d) \iff \alpha \in \mathrm{R}_d$$

thanks to Proposition 4.70 on "the orthogonal of the orthogonal" and to the injectivity of η. □

4.1.3. Convergence in law of the new random variables

The analogue of the result of Chapter 2 about the equidistribution of the tuples (4.2) in a subtorus of $(\mathbf{S}^1)^d$ is the following proposition. It is the central result, as the equidistribution result for exponential sums follows easily (as we will see below) by definition of the pushforward measure.

Proposition 4.10. *The random variables $(U_\mathfrak{p})_{\mathfrak{p} \in \mathcal{R}_d}$ defined at Definition 4.3 converge in law as $\|\mathfrak{p}\| \to \infty$ to a uniformly distributed random variable on H_d.*

Proof.

- First, let us prove that the random variables $U_\mathfrak{p}$ take values in H_d. Let us fix $a \in \mathcal{O}_K/\mathfrak{p}$ and prove that $U_\mathfrak{p}(a) \in \mathrm{H}_d$. It suffices to prove that for all $\alpha \in \mathrm{R}_d$, $\eta_\alpha(U_\mathfrak{p}(a)) = 1$. It is indeed the case, as

$$\eta_\alpha(U_\mathfrak{p}(a)) = \prod_{x \in \boldsymbol{\mu}_d} e\left(\frac{\tau_\mathfrak{p}(a\varpi_\mathfrak{p}(x))}{\|\mathfrak{p}\|}\right)^{\alpha(x)} = e\left(\frac{\tau_\mathfrak{p}(a\varpi_\mathfrak{p}(\sum_{x \in \boldsymbol{\mu}_d} \alpha(x)x))}{\|\mathfrak{p}\|}\right)$$

  and $\sum_{x \in \boldsymbol{\mu}_d} \alpha(x)x = 0$ because $\alpha \in \mathrm{R}_d$. This proves that for all $a \in \mathcal{O}_K/\mathfrak{p}$, $U_\mathfrak{p}(a) \in \mathrm{H}_d$.

- Now, let us prove the convergence in law stated in the proposition. As H_d is a compact abelian group, we can apply the generalized Weyl Criterion for equidistribution: it is enough to check that, for all non-trivial characters η of H_d, we have

$$\mathbb{E}(\eta(U_\mathfrak{p})) \to 0$$

  as $\|\mathfrak{p}\| \to +\infty$. Now, any character of H_d can be extended to a character of the whole group $\mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1)$, so it can be written as η_α for some $\alpha \in \mathrm{C}(\boldsymbol{\mu}_d, \mathbf{Z})$ (thanks to Theorem 4.68). Moreover, η_α is trivial on H_d if and only if $\alpha \in \mathrm{R}_d$ thanks to Proposition 4.9. Therefore, we take $\alpha \notin \mathrm{R}_d$ and we want to show that

$$\mathbb{E}(\eta_\alpha(U_\mathfrak{p})) \to 0.$$

  We have

$$\mathbb{E}(\eta_\alpha(U_\mathfrak{p})) = \frac{1}{\|\mathfrak{p}\|} \sum_{a \in \mathcal{O}_K/\mathfrak{p}} \eta_\alpha(U_\mathfrak{p}(a)) = \frac{1}{\|\mathfrak{p}\|} \sum_{a \in \mathcal{O}_K/\mathfrak{p}} \prod_{x \in \boldsymbol{\mu}_d} (U_\mathfrak{p}(a)(x))^{\alpha(x)} = \frac{1}{\|\mathfrak{p}\|} \sum_{a \in \mathcal{O}_K/\mathfrak{p}} \prod_{x \in \boldsymbol{\mu}_d} e\left(\frac{\tau_\mathfrak{p}(a\varpi_\mathfrak{p}(x))}{\|\mathfrak{p}\|}\right)^{\alpha(x)}.$$

Therefore, if we introduce the notation $S_\alpha := \sum_{x \in \boldsymbol{\mu}_d} \alpha(x) x$, we have

$$\mathbb{E}(\eta_\alpha(U_\mathfrak{p})) = \frac{1}{\|\mathfrak{p}\|} \sum_{a \in \mathcal{O}_K/\mathfrak{p}} e\left(\frac{\tau_\mathfrak{p}(a \varpi_\mathfrak{p}(S_\alpha))}{\|\mathfrak{p}\|}\right) = \frac{1}{\|\mathfrak{p}\|} \sum_{b \in \mathbf{Z}/\|\mathfrak{p}\|\mathbf{Z}} e\left(\frac{\tau_\mathfrak{p}(\varpi_\mathfrak{p}(S_\alpha))}{\|\mathfrak{p}\|} b\right)$$

(the last equality is obtained via the change of variables $b = \tau_\mathfrak{p}(a)$). By orthogonality of the additive characters modulo $\|\mathfrak{p}\|$, we obtain

$$\mathbb{E}(\eta_\alpha(U_\mathfrak{p})) = \mathbb{1}_{\tau_\mathfrak{p}(\varpi_\mathfrak{p}(S_\alpha))=0} = \mathbb{1}_{\varpi_\mathfrak{p}(S_\alpha)=0}$$

since $\tau_\mathfrak{p}$ is an isomorphism. Now since $\alpha \notin \mathrm{R}_d$, we have that the ideal $S_\alpha \mathcal{O}_K$ is a *non-zero* ideal of the Dedekind ring $\mathcal{O}_K$, so there are only finitely many prime ideals in $\mathcal{O}_K$ that contain it. Thus, for all but finitely many $\mathfrak{p}$ we have $\varpi_\mathfrak{p}(S_\alpha) \neq 0$ i.e. $\mathbb{1}_{\varpi_\mathfrak{p}(S_\alpha)=0} = 0$. This shows that for all $\mathfrak{p} \in \mathcal{R}_d$ such that $\|\mathfrak{p}\|$ is large enough, $\mathbb{E}(\eta(U_\mathfrak{p})) = 0$. In particular,

$$\mathbb{E}(\eta(U_\mathfrak{p})) \underset{\substack{\|\mathfrak{p}\| \to \infty \\ \mathfrak{p} \in \mathcal{R}_d}}{\longrightarrow} 0.$$

□

4.1.4. Recovering the result of Chapter 2

The previous proposition immediately gives the following corollary:

Corollary 4.11. *The random variables*

$$\begin{array}{rccc} \mathrm{S}_\mathfrak{p} & : & \mathcal{O}_K/\mathfrak{p} & \to & \mathbf{C} \\ & & a & \mapsto & \displaystyle\sum_{x \in \boldsymbol{\mu}_d} e\left(\frac{\tau_\mathfrak{p}(a \varpi_\mathfrak{p}(x))}{\|\mathfrak{p}\|}\right) \end{array}$$

converge in law as $\|\mathfrak{p}\| \to \infty$ (and $\mathfrak{p} \in \mathcal{R}_d$) to a random variable $\sigma(U)$ where U is a uniformly distributed random variable on H_d and $\sigma \colon \mathrm{C}(\boldsymbol{\mu}_d, \mathbf{S}^1) \to \mathbf{C}$, $f \mapsto \sum_{x \in \boldsymbol{\mu}_d} f(x)$.

Proof. This is just because if a sequence (X_n) of random variables converges in law to X, then for any continuous map F, we have that $(F(X_n))$ converges in law to $F(X)$. Here the continuous map is σ and the convergence in law before composition with σ is given by Proposition 4.10. □

Remark 4.12. However, in order to recover a statement in the spirit of Chapter 2, we would rather not have these homomorphisms $\tau_\mathfrak{p}$ and $\varpi_\mathfrak{p}$ and replace $\boldsymbol{\mu}_d$ by $\mu_d(\mathbf{F}_q)$ for primes $q \equiv 1 \pmod d$. The reason why we can obtain such a statement comes from the following fact.

Proposition 4.13 ([87, Corollary 10.4])**.** *A prime $q \neq 2$ is totally split in $K = \mathbf{Q}(\boldsymbol{\mu}_d)$ if and only if $q \equiv 1 \pmod d$.*

In particular, if $q \equiv 1 \pmod d$ and if $\mathfrak{p} \mid q$, then $\mathfrak{p} \in \mathcal{R}_d$ so that we have some hope that the equidistribution result of Corollary 4.11 may be related to the results of Chapter 2. Let us prove that this is indeed the case:

Corollary 4.14. *For any prime $q \neq 2$ such that $q \equiv 1 \pmod d$, define (as in Chapter 2)*

$$\mathrm{S}_q(b, d) := \sum_{x \in \mu_d(\mathbf{F}_q)} e\left(\frac{bx}{q}\right) \quad \text{for all } b \in \mathbf{F}_q$$

Then the set $\{\mathrm{S}_q(b, d);\ b \in \mathbf{F}_q\}$ become equidistributed in $\sigma(\mathrm{H}_d)$ with respect to the pushforward measure $\sigma_*(\mu_{\mathrm{H}_d})$, where μ_{H_d} denotes the probability Haar measure on H_d.

Proof. If $q \equiv 1 \,(\mathrm{mod}\, d)$, then Proposition 4.13 tells us that *any* prime ideal above q belongs to $\mathcal{R}_d$. So for each q, we let $\mathfrak{p}$ be such an ideal. Then thanks to Corollary 4.11, we know that the random variables $\mathrm{S}_\mathfrak{p}$ converge in law, as $\|\mathfrak{p}\|$ goes to infinity, to a random variable $\sigma(U)$ as in the statement. In other words, the sets

$$\{\mathrm{S}_\mathfrak{p}(a); a \in \mathcal{O}_K/\mathfrak{p}\}$$

become equidistributed with respect to the measure $\sigma_*(\mu_{\mathrm{H}_d})$. Now, we have that for all $a \in \mathcal{O}_K/\mathfrak{p}$,

$$\mathrm{S}_\mathfrak{p}(a) = \sum_{x \in \boldsymbol{\mu}_d} e\left(\frac{\tau_\mathfrak{p}(a)\tau_\mathfrak{p}(\varpi_\mathfrak{p}(x))}{\|\mathfrak{p}\|}\right)$$

and we would like to perform the change of variable $y = \tau_\mathfrak{p}(\varpi_\mathfrak{p}(x))$ in order to relate these sums to sums over $\mu_d(\mathbf{F}_q)$. In fact, it is true that under the assumption $q \equiv 1 \,(\mathrm{mod}\, d)$, $\tau_\mathfrak{p} \circ \varpi_\mathfrak{p}$ induces a bijection between $\boldsymbol{\mu}_d$ and $\mu_d(\mathbf{F}_q)$. This will be proved at Proposition 4.31 in a more general setting. This part of the proof really makes use of the fact that q is totally split in K, as it requires the assumption that $\mathfrak{p}$ is unramified, and not only has residual degree 1.
Once we know this, we immediately get the following lemma and the conclusion follows.

Lemma 4.15. *If $q \equiv 1 \,(\mathrm{mod}\, d)$ and $\mathfrak{p}$ is an ideal of $\mathcal{O}_K$ lying above q, then*

$$\{\mathrm{S}_\mathfrak{p}(a); a \in \mathcal{O}_K/\mathfrak{p}\} = \{\mathrm{S}_q(b, d);\ b \in \mathbf{F}_q\}\,.$$

□

Remark 4.16. Proposition 4.31 requires the extra assumption that $q \nmid \mathrm{disc}(g)$, but in the case of $g = X^d - 1$, we have $|\mathrm{disc}(g)| = d^d$ so that the condition $q \equiv 1 \,(\mathrm{mod}\, d)$, which we use to ensure that q is totally split in K, actually also ensures the condition on the non-divisibility of the discriminant.

Now, it remains to check that the measure $\sigma_*(\mu_{\mathrm{H}_d})$ in Corollary 4.14 is indeed the same as the push-forward measure which appears in Proposition 2.12. To simplify a little, we will only deal with the case where d is prime, and check that the measure $\sigma_*(\mu_{\mathrm{H}_d})$ is indeed the same as the one of Theorem 2.5, that is: the pushforward measure, via the Laurent polynomial

$$X_1 + \cdots + X_{d-1} + \frac{1}{X_1 \ldots X_{d-1}},$$

of the Haar probability measure on $(\mathbf{S}^1)^{d-1}$. For a prime number d, let us fix a primitive d–th root of unity ζ. Then $\boldsymbol{\mu}_d = \left\{\zeta^j;\ 0 \leqslant j \leqslant d-1\right\}$ and we have

$$\mathrm{R}_d = \left\{\alpha \colon \boldsymbol{\mu}_d \to \mathbf{Z},\ \sum_{j=0}^{d-1} \alpha(\zeta^j)\zeta^j = 0\right\}$$

which corresponds, under the isomorphism of $\mathbf{Z}$-modules

$$\begin{array}{ccc} \mathbf{Z}^d & \to & \mathbf{Z}_{d-1}[X] \\ (a_0 \ldots, a_{d-1}) & \mapsto & \sum_{j=0}^{d-1} a_j X^j \end{array}$$

to

$$\{P \in \mathbf{Z}_{d-1}[X];\ P(\zeta) = 0\} = \{P \in \mathbf{Z}_{d-1}[X];\ \phi_d \text{ divides } P\}\,.$$

Now since we assumed that d is prime, ϕ_d is monic of degree $d-1$, so that the multiples of ϕ_d which belong to $\mathbf{Z}_{d-1}[X]$ are exactly the polynomials of the form $\lambda\phi_d(X) = \lambda(1 + X + \cdots + X^{d-1})$ for some integer λ. Going back to R_d, this means that R_d is the $\mathbf{Z}$-module of constant maps $\alpha \colon \boldsymbol{\mu}_d \to \mathbf{Z}$. Therefore,

$$\begin{aligned} \mathrm{H}_d &= \left\{f \colon \boldsymbol{\mu}_d \to \mathbf{S}^1;\ \forall \lambda \in \mathbf{Z},\ \prod_{x \in \boldsymbol{\mu}_d} f(x)^\lambda = 1\right\} \\ &= \left\{f \colon \boldsymbol{\mu}_d \to \mathbf{S}^1;\ \prod_{x \in \boldsymbol{\mu}_d} f(x) = 1\right\}. \end{aligned}$$

We have a group isomorphism between H_d and the group $\mathrm{H}'_d := \left\{g\colon \boldsymbol{\mu}_d \setminus \{1\} \mapsto \mathbf{S}^1\right\}$ given by

$$\begin{array}{rccc} \Phi & : & \mathrm{H}_d & \to & \mathrm{H}'_d \\ & & f & \mapsto & f_{|\boldsymbol{\mu}_d\setminus\{1\}} \end{array}$$

and whose inverse is obtained by associating to $g \in \mathrm{H}'_d$ its continuation at 1 defined in the only possible way to create an element of H_d:

$$g(1) := \prod_{x\in\boldsymbol{\mu}_d\setminus\{1\}} g(x)^{-1}.$$

As H'_d is isomorphic to $(\mathbf{S}^1)^{d-1}$, the Haar measure on H'_d is just the product of the uniform measure on $\mathbf{S}^1$. Since Φ is an isomorphism of topological groups, this implies that $\mu_{\mathrm{H}_d} = \Phi_*^{-1}(\mu_{\mathrm{H}'_d})$, hence $\sigma_*(\mu_{\mathrm{H}_d}) = \sigma_*\left(\Phi_*^{-1}(\mu_{\mathrm{H}'_d})\right)$. In other words, for any measurable subset A of $\mathbf{C}$, we have

$$\begin{aligned} \sigma_*(\mu_{\mathrm{H}_d})(A) &= \mu_{\mathrm{H}'_d}\left(\Phi\left(\sigma^{-1}(A)\right)\right) \\ &= \mu_{\mathrm{H}'_d}\left(\left\{g\in\mathrm{H}'_d;\ \sum_{x\in\boldsymbol{\mu}_d\setminus\{1\}} g(x) + \prod_{x\in\boldsymbol{\mu}_d\setminus\{1\}} g(x)^{-1} \in A\right\}\right) \end{aligned}$$

Thus, we recover that the measure $\sigma_*(\mu_{\mathrm{H}_d})$ is indeed the pushforward measure via the Laurent polynomial

$$(z_1,\dots,z_{d-1}) \mapsto z_1 + \cdots + z_{d-1} + \frac{1}{z_1\dots z_{d-1}}$$

of the Haar measure on $(\mathbf{S}^1)^{d-1}$.

4.2. Generalization to exponential sums restricted to the roots of a fixed polynomial

The number field approach of the previous section shows that we can recover the previous results on sums over subgroups of fixed cardinality, but it also has the advantage of opening the door to many generalizations. Indeed, since the method no longer relies on the fact that we are working with roots of unity and that we can choose a primitive root, it is more likely to extend to the case of roots of arbitrary polynomials. We present those generalizations in this section.

4.2.1. Algebraic number theory prerequisites I

Since we also want to consider exponential sums modulo prime powers, and not only primes, we need to start with a short section on "residue rings" instead of the more usual residue fields.

Lemma 4.17. *Let A be a Dedekind domain, K its fraction field, L/K a finite and separable extension, and let B be the integral closure of A in L. Let p be a prime ideal in A and let $\mathfrak{p}$ be a prime ideal in B lying above p, with ramification index e. Let $n \geqslant 1$.*
Then we have

$$\mathfrak{p}^n \cap A = p^{\lceil n/e\rceil}$$

where $\lceil n/e\rceil$ denotes the smallest integer larger than or equal to n/e.

Proof. (inspired by the answers on Stack Exchange available at https://math.stackexchange.com/questions/1526463/prime-ideals-in-extensions-of-dedekind-domains and https://math.stackexchange.com/questions/2577145/intersection-of-powers-of-prime-ideals-with-subring).
Since A and B are Dedekind domains, the localizations A_p and $B_{\mathfrak{p}}$ are discrete valuation rings. If we denote by v_p and $v_{\mathfrak{p}}$ the corresponding *normalized* discrete valuations, then we have $(v_{\mathfrak{p}})_{|A} = ev_p$

because the $\mathfrak{p}$-adic valuation of p is equal to e by definition of the ramification index. Therefore, for all $x \in B$, we have:

$$\begin{aligned} x \in \mathfrak{p}^n \cap A &\iff x \in A \text{ and } v_{\mathfrak{p}}(x) \geqslant n \iff x \in A \text{ and } ev_p(x) \geqslant n \\ &\iff x \in A \text{ and } v_p(x) \geqslant n/e \underset{(\star)}{\iff} x \in A \text{ and } v_p(x) \geqslant \lceil n/e \rceil \\ &\iff x \in p^{\lceil n/e \rceil} \end{aligned}$$

where the equivalence $(\star)$ comes from the fact that $v_p(x)$ is an integer. □

Corollary 4.18. *Let $K/\mathbf{Q}$ be a number field, let p be a prime number, and $\mathfrak{p}$ be a prime ideal of K which lies above p. Assume that the extension is unramified at $\mathfrak{p}$. Then the natural ring homomorphism*

$$\mathbf{Z}/p^n\mathbf{Z} \to \mathcal{O}_K/\mathfrak{p}^n$$

is injective.

Proof. The kernel of $\mathbf{Z} \to \mathcal{O}_K/\mathfrak{p}^n$ is $\mathfrak{p}^n \cap \mathbf{Z}$, and the latter is exactly $p^n\mathbf{Z}$ thanks to Lemma 4.17. □

Corollary 4.19. *Under the assumptions of the preceding corollary, assume further that the residual degree $f_{\mathfrak{p}}$ is equal to 1. Then for any $n \geqslant 1$, the natural ring homomorphism*

$$\iota_{\mathfrak{p}^n} : \mathbf{Z}/p^n\mathbf{Z} \to \mathcal{O}_K/\mathfrak{p}^n$$

is an isomorphism.

Proof. Recall that one can define the norm of an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ as the index of $\mathfrak{a}$ in $\mathcal{O}_K$. We will denote it by $\|\mathfrak{a}\|$

$$\|\mathfrak{a}\| := |\mathcal{O}_K/\mathfrak{a}|,$$

and that this norm is multiplicative (see e.g. [81, Theorem 22 (a)]). Thus,

$$|\mathcal{O}_K/\mathfrak{p}^n| = \|\mathfrak{p}^n\| = \|\mathfrak{p}\|^n = |\mathcal{O}_K/\mathfrak{p}|^n = \left(p^{f_{\mathfrak{p}}}\right)^n = p^n$$

using the fact that $f_{\mathfrak{p}} = 1$. Therefore, the map in the statement is a map between two sets having the same number of elements, and it is injective thanks to Corollary 4.18, so it is a bijection. □

Remark 4.20. When the residual degree $f_{\mathfrak{p}}$ is equal to 1, the natural homomorphism $\mathbf{Z}/p\mathbf{Z} \to \mathcal{O}_K/\mathfrak{p}$ is an isomorphism, so the prime p equals the norm $\|\mathfrak{p}\|$ of the ideal $\mathfrak{p}$.

Remark 4.21. If p is totally split in K then for all $\mathfrak{p} \mid p$, the assumptions of Corollary 4.19 are fulfilled.

Definition 4.22. *Under the assumptions of Corollary 4.19, we denote by $\tau_{\mathfrak{p}^n} : \mathcal{O}_K/\mathfrak{p}^n \to \mathbf{Z}/p^n\mathbf{Z} = \mathbf{Z}/\|\mathfrak{p}\|^n\mathbf{Z}$ the inverse of $\iota_{\mathfrak{p}^n}$.*

We can now set the definitions which will give an appropriate framework to handle exponential sums over the roots of some polynomial.

4.2.2. Definition and convergence in law of the suitable random variables

Let $g \in \mathbf{Z}[X]$ be a *monic* polynomial of degree $d \geqslant 1$.

Definition 4.23. *We will use the following notations:*

- *Z_g denotes the set of roots of g in $\mathbf{C}$,*
- *$K_g := \mathbf{Q}(\mathrm{Z}_g)$ denotes the splitting field of g, and $\mathbf{O}_g$ the ring of integers of K_g,*
- *for any ideal $\mathfrak{a}$ of $\mathbf{O}_g$, we denote by $\varpi_{\mathfrak{a}} : \mathbf{O}_g \to \mathbf{O}_g/\mathfrak{a}$ the canonical surjection,*
- *$\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ is the compact abelian group of (continuous) maps from Z_g to the unit circle $\mathbf{S}^1$,*

Important note: Since all results in this chapter only depend on Z_g, we can assume without loss of generality that the polynomial g is *separable*. We will do so in the remainder of the chapter.

We will also need a notion of "admissible ideals" in order to be able to define the random variables of interest to us.

Definition 4.24. *Let us define $\mathcal{S}_g$ as the set of prime ideal $\mathfrak{p}$ of $\mathbf{O}_g$ which lie above a prime $q \in \mathbf{Z}$ which is totally split in K_g. Equivalently (because $K_g/\mathbf{Q}$ is Galois), those are the ideals which are unramified and of residual degree equal to 1.*

We can now define a sequence of random variables indexed by powers of prime ideals in $\mathcal{S}_g$.

Definition 4.25. *Define the random variables $U_{\mathfrak{p}^n}$ for all $\mathfrak{p} \in \mathcal{S}_g$ and $n \geqslant 1$ as follows:*

$$\begin{array}{rccc} U_{\mathfrak{p}^n} & : & \mathbf{O}_g/\mathfrak{p}^n & \to & \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1) \\ & & a & \mapsto & U_{\mathfrak{p}^n}(a) \end{array}$$

where

$$\begin{array}{rccc} U_{\mathfrak{p}^n}(a) & : & \mathrm{Z}_g & \to & \mathbf{S}^1 \\ & & x & \mapsto & e\left(\frac{\tau_{\mathfrak{p}^n}(a\varpi_{\mathfrak{p}^n}(x))}{\|\mathfrak{p}\|^n}\right) \end{array}$$

where $\tau_{\mathfrak{p}^n}$ is the isomorphism of Definition 4.22.

Note that $\mathrm{Z}_g \subset \mathbf{O}_g$ because g is a monic polynomial in $\mathbf{Z}[X]$, therefore the term $\varpi_{\mathfrak{p}^n}(x)$ in the definition of $U_{\mathfrak{p}^n}(a)$ makes sense.

Finally, the limiting distribution of these random variables will be governed by the additive relations between the roots of g. Thus, the suitable analogue of Definition 4.5 is given by the following one:

Definition 4.26. *Let $g \in \mathbf{Z}[X]$.*

- R_g *denotes the submodule of* $\mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$ *of additive relations between the roots of g:*

$$\mathrm{R}_g := \left\{ \alpha \colon \mathrm{Z}_g \to \mathbf{Z},\ \sum_{x \in \mathrm{Z}_g} \alpha(x)x = 0 \right\}.$$

- H_g *denotes the subgroup of* $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ *which is "dual" to* R_g *in the following sense:*

$$\mathrm{H}_g := \left\{ f \in \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1),\ \forall \alpha \in \mathrm{R}_g,\ \prod_{x \in \mathrm{Z}_g} f(x)^{\alpha(x)} = 1 \right\}$$

Definition 4.7 and propositions 4.8 and 4.9 transpose to this setting as follows (the proofs are near copies of the corresponding ones when g was taken to be the polynomial $X^d - 1$).

Definition 4.27. *For all $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$, we denote by η_α the following character of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$:*

$$\begin{array}{rccc} \eta_\alpha & : & \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1) & \to & \mathbf{S}^1 \\ & & f & \mapsto & \displaystyle\prod_{x \in \mathrm{Z}_g} f(x)^{\alpha(x)} \end{array}$$

Proposition 4.28. *The map*

$$\begin{array}{rccc} \eta & : & \mathrm{C}(\mathrm{Z}_g, \mathbf{Z}) & \to & \widehat{\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)} \\ & & \alpha & \mapsto & \eta_\alpha \end{array}$$

is an isomorphism of abelian groups.

Proposition 4.29. *Let $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$. The character η_α is trivial on H_g if and only if $\alpha \in \mathrm{R}_g$.*

Then, a proof very close to that of Proposition 4.10 gives the following statement:

Theorem 4.30. *The sequence $(U_{\mathfrak{p}^n})_{\mathfrak{p}\in\mathcal{S}_g,n\geqslant 1}$ converges in law, as $\|\mathfrak{p}\|^n$ goes to infinity, to a random variable U uniformly distributed on H_g. Note that $\|\mathfrak{p}\|^n \to \infty$ includes the case where $\mathfrak{p}$ if a fixed prime ideal and only n goes to infinity.*

In other words, the limiting distribution is described as the Haar measure on the orthogonal of the module of additive relations between the roots of g.

Proof.

- First, let us prove that the random variables $U_{\mathfrak{p}^n}$ take values in H_g. Let us fix $a \in \mathbf{O}_g/\mathfrak{p}^n$ and prove that $U_{\mathfrak{p}^n}(a) \in \mathrm{H}_g$. It suffices to prove that for all $\alpha \in \mathrm{R}_g$, $\eta_\alpha(U_{\mathfrak{p}^n}(a)) = 1$. It is indeed the case, as

$$\eta_\alpha(U_{\mathfrak{p}^n}(a)) = \prod_{x\in \mathrm{Z}_g} e\left(\frac{\tau_{\mathfrak{p}^n}(a\varpi_{\mathfrak{p}^n}(x))}{\|\mathfrak{p}\|^n}\right)^{\alpha(x)} = e\left(\frac{\tau_{\mathfrak{p}^n}(a\varpi_{\mathfrak{p}^n}(\sum_{x\in \mathrm{Z}_g}\alpha(x)x))}{\|\mathfrak{p}\|^n}\right)$$

  and $\sum_{x\in \mathrm{Z}_g}\alpha(x)x = 0$ because $\alpha \in \mathrm{R}_g$. This proves that for all $a \in \mathbf{O}_g/\mathfrak{p}^n$, $U_{\mathfrak{p}^n}(a) \in \mathrm{H}_g$.

- Now, let us prove the convergence in law stated in the proposition. As H_g is a compact abelian group, we can apply the generalized Weyl Criterion for equidistribution: it is enough to check that, for all non-trivial characters η of H_g, we have

$$\mathbb{E}(\eta(U_{\mathfrak{p}^n})) \to 0$$

  as $\|\mathfrak{p}\|^n \to +\infty$. Now, any character of H_g can be extended to a character of the whole group $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ thanks to the Theorem 4.68 of the appendix, so it can be written as η_α for some $\alpha \in \mathrm{C}(\mathrm{Z}_g; \mathbf{Z})$. Moreover, η_α is trivial on H_g if and only if $\alpha \in \mathrm{R}_g$ (thanks to Proposition 4.29). Therefore, we take $\alpha \notin \mathrm{R}_g$ and we want to show that

$$\mathbb{E}(\eta_\alpha(U_{\mathfrak{p}^n})) \to 0.$$

  We have

$$\begin{aligned}\mathbb{E}(\eta_\alpha(U_{\mathfrak{p}^n})) &= \frac{1}{\|\mathfrak{p}\|^n}\sum_{a\in\mathbf{O}_g/\mathfrak{p}^n} e\Big(\frac{\tau_{\mathfrak{p}^n}(a)}{\|\mathfrak{p}\|^n}\tau_{\mathfrak{p}^n}\Big(\varpi_{\mathfrak{p}^n}\Big(\sum_{x\in \mathrm{Z}_g}\alpha(x)x\Big)\Big)\Big)\\ &= \frac{1}{\|\mathfrak{p}\|^n}\sum_{b\in\mathbf{Z}/\|\mathfrak{p}\|^n\mathbf{Z}} e\Big(\frac{b}{\|\mathfrak{p}\|^n}\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha))\Big)\end{aligned}$$

  where we denoted

$$S_\alpha := \sum_{x\in \mathrm{Z}_g}\alpha(x)x$$

  (it is a non-zero element of $\mathbf{O}_g$ because $\alpha \notin \mathrm{R}_g$). By orthogonality of the additive characters modulo $\|\mathfrak{p}\|^n$, we have

$$\mathbb{E}(\eta_\alpha(U_{\mathfrak{p}^n})) = 1 \iff \tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha)) = 0 \iff \varpi_{\mathfrak{p}^n}(S_\alpha) = 0 \iff S_\alpha \in \mathfrak{p}^n,$$

  and $\mathbb{E}(\eta_\alpha(U_{\mathfrak{p}^n}))$ equals 0 otherwise. Now, the condition $S_\alpha \in \mathfrak{p}^n$ implies that $\|\mathfrak{p}\|^n$ divides the non-zero integer $\mathrm{N}_{K_g/\mathbf{Q}}(S_\alpha)$, so that it cannot be satisfied for $\|\mathfrak{p}\|^n$ large enough. This shows that $\mathbb{E}(\eta_\alpha(U_{\mathfrak{p}^n}))$ not only converges to zero as $\|\mathfrak{p}\|^n$ tends to infinity, but is actually eventually equal to 0.

□

4.2.3. Algebraic number theory prerequisites II

Next, we want to derive from Theorem 4.30 a statement on the equidistribution of sums indexed by the roots of a polynomial modulo prime powers. In order to do this, we need a few extra facts from algebraic number theory. The aim of this section is to obtain the following proposition, a special case of which has already been used without proof in the proof of Corollary 4.14.

Proposition 4.31. *Let $g \in \mathbf{Z}[X]$ be a monic and separable polynomial. Let q be a prime number which does not divide the discriminant of g. If q is totally split in K_g, then for all $\mathfrak{p} \mid q$ and all $n \geqslant 1$, the composition*

$$\mathrm{Z}_g \hookrightarrow \mathbf{O}_g \overset{\varpi_{\mathfrak{p}^n}}{\to} \mathbf{O}_g/\mathfrak{p}^n \overset{\tau_{\mathfrak{p}^n}}{\to} \mathbf{Z}/q^n\mathbf{Z}$$

yields a bijection between Z_g and $\mathrm{Z}_g(\mathbf{Z}/q^n\mathbf{Z}) := \{x \in \mathbf{Z}/q^n\mathbf{Z};\ g(x) \equiv 0 \bmod q^n\}$.

The reason why we need this result is that we want to relate the random variables of Definition 4.25 (which are defined in the number field setting), to the more elementary random variables

$$\begin{array}{ccc} \mathbf{Z}/q^n\mathbf{Z} & \to & \mathrm{C}(\mathrm{Z}_g(\mathbf{Z}/q^n\mathbf{Z}), \mathbf{S}^1) \\ a & \mapsto & V_{q^n}(a) \end{array}$$

where

$$\begin{array}{ccccc} V_{q^n}(a) & : & \mathrm{Z}_g(\mathbf{Z}/q^n\mathbf{Z}) & \to & \mathbf{S}^1 \\ & & x & \mapsto & e\left(\frac{ax}{q^n}\right) \end{array}$$

This is why we need to look more closely at what happens to the roots of g after the identifications through $\varpi_{\mathfrak{p}^n}$ and $\tau_{\mathfrak{p}^n}$.

In order to prove the previous proposition, we will need the following famous theorem:

Theorem 4.32 (Dedekind, see [20] or [81, Theorem 27])**.** *Let K be a number field of degree n over $\mathbf{Q}$, and $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$. Let $f(T)$ be the minimal polynomial of α in $\mathbf{Z}[T]$. For any prime q not dividing $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$, write*

$$f(T) \equiv \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g} \,(\mathrm{mod}\, q)$$

where the π_i are distinct monic irreducible polynomials in $\mathbf{F}_q[T]$. Then $q\mathcal{O}_K$ factors into prime ideals as

$$q\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where $\mathfrak{p}_i = \langle q, \tilde{\pi}_i(\alpha)\rangle$ is the ideal generated by q and $\tilde{\pi}_i(\alpha)$ ($\tilde{\pi}_i$ denotes any polynomial in $\mathbf{Z}[T]$ which reduces to π_i modulo q). Besides, $\|\mathfrak{p}_i\| = q^{\deg(\pi_i)}$.

Remark 4.33. In fact, we have the relation

$$\mathrm{disc}(\mathbf{Z}[\alpha]) = \mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = [\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 d_K$$

where d_K denotes the absolute discriminant of the number field K (that is: the discriminant of any $\mathbf{Z}$-basis of $\mathcal{O}_K$). Thus, if q does not divide $\mathrm{disc}(\mathbf{Z}[\alpha])$ it does not divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$, so the theorem applies. It is usually more convenient to use this divisibility condition, because it does not require any knowledge of the full ring $\mathcal{O}_K$.

Now, since we want to apply this theorem to $K_g = \mathbf{Q}(\mathrm{Z}_g)$, which is generated by *all* the roots of g, we will also need the following theorem to go from the extensions $\mathbf{Q}(\alpha)$ generated by a single root of g to the extension K_g.

Theorem 4.34 ([81, Theorem 31])**.** *Let K be a number field, and let L and M be two finite extensions of K. Let $\mathfrak{p}$ be a prime ideal of K. Then $\mathfrak{p}$ splits completely in L and M if and only if it splits completely in their compositum LM.*

Remark 4.35. Actually, [81, Theorem 31] only states the direction " $\Longrightarrow$ " but the converse is easier by multiplicativity of the ramification index and residual degree in extensions (if they are both equal to 1 in the largest extension, they are equal to 1 in the subextensions).

Combining the last two theorems allows us to obtain the following lemma.

Lemma 4.36. *Let $g \in \mathbf{Z}[X]$ be a monic and separable polynomial of degree $d \geqslant 1$. Then for all prime numbers q not dividing* $\mathrm{disc}(g)$*, we have*

$$q \text{ is totally split in } K_g \iff \overline{g} \text{ splits into distinct linear factors in } \mathbf{F}_q[X]$$

In this lemma and its proof, $\overline{f}$ denotes the reduction modulo q of a polynomial $f \in \mathbf{Z}[X]$.

Proof. Let q be a prime number not dividing the discriminant of g and let $\alpha \in \mathrm{Z}_g$. Denote by μ_α the minimal polynomial of α over $\mathbf{Q}$, which belongs to $\mathbf{Z}[X]$ and is one of the factors of g. Then

$$\mathrm{disc}(\mu_\alpha) \mid \mathrm{disc}(g).$$

Indeed, it is a general fact that for two polynomial $P, Q \in \mathbf{Z}[X]$, we have (up to a sign):

$$\mathrm{disc}(PQ) = \mathrm{disc}(P)\mathrm{disc}(Q)\mathrm{Res}(P,Q)^2 \tag{4.6}$$

Therefore, the assumption on q ensures that q does not divide $\mathrm{disc}(\mu_\alpha) = \mathrm{disc}(\mathbf{Z}[\alpha])$, so we can apply Theorem 4.32 at q to the extension $\mathbf{Q}(\alpha)/\mathbf{Q}$: it tells us that the ramification of q in $\mathbf{Q}(\alpha)$ is exactly given by the factorization of $\overline{\mu}_\alpha$ modulo q. In particular, q is totally split in $\mathbf{Q}(\alpha)$ if and only if $\overline{\mu}_\alpha$ splits into distinct linear factors mod q.
Now, the irreducible factors of g are the μ_α, and g has no square factor, because we assumed that it is separable. Moreover, the assumption that q does not divide $\mathrm{disc}(g)$ ensures that g remains separable after reduction modulo q. Thus, we have that $\overline{g}$ splits into distinct linear factors mod q if and only if for all $\alpha \in \mathrm{Z}_g$, $\overline{\mu}_\alpha$ splits into distinct linear factors mod q.
Thus, we have proved that $\overline{g}$ splits into distinct linear factors modulo q if and only if for all $\alpha \in \mathrm{Z}_g$, the prime q is totally split in $\mathbf{Q}(\alpha)$, and thanks to Theorem 4.34, this is equivalent to q being totally split in K_g. □

Remark 4.37 (inpired by the answer here)**.** There is an elementary way to prove that if P, Q are two monic polynomials with coefficients in $\mathbf{Z}$, then $\mathrm{disc}(P) \mid \mathrm{disc}(PQ)$, without knowing the notion of resultant of two polynomials used in equation (4.6) above. Indeed, if we denote by $\alpha_1, \dots, \alpha_m$ the (not necessarily distinct) roots of P in $\mathbf{C}$ and by $\beta_1, \dots, \beta_n$ those of Q, then (up to a sign)

$$\mathrm{disc}(PQ) = \prod_{1 \leqslant i \neq j \leqslant m} (\alpha_i - \alpha_j) \prod_{1 \leqslant k \neq \ell \leqslant n} (\beta_k - \beta_\ell) \prod_{\substack{1 \leqslant r \leqslant m \\ 1 \leqslant s \leqslant n}} (\alpha_r - \beta_s).$$

The first two factors are respectively equal (again, up to a sign convention) to $\mathrm{disc}(P)$ and $\mathrm{disc}(Q)$, while the last factor can be expressed in terms of the resultant of P and Q once we know the expression of the resultant in terms of the roots. However, without speaking about resultants, we can prove the this last factor is an integer. Indeed, if we consider the polynomial

$$F(Y_1, \dots, Y_n) := \prod_{\substack{1 \leqslant r \leqslant m \\ 1 \leqslant s \leqslant n}} (X_r - Y_s),$$

it belongs to $A[Y_1, \dots, Y_n]$, where $A = \mathbf{Z}[X_1, \dots, X_m]$, and it is a symmetric polynomial, so there exists a polynomial $G \in A[Y_1, \dots, Y_n]$ such that $F(Y_1, \dots, Y_n) = G(\sigma_1, \dots, \sigma_n)$ where $\sigma_i = \sigma_i(Y_1, \dots, Y_n)$ is the i-th elementary symmetric polynomial. Then $\sigma_i(\beta_1, \dots, \beta_n)$ is (up to a sign) equal to a coefficient of Q, hence is an integer. Thus,

$$F(\beta_1, \dots, \beta_n) = \prod_{\substack{1 \leqslant r \leqslant m \\ 1 \leqslant s \leqslant n}} (X_r - \beta_s)$$

belongs to $\mathbf{Z}[X_1, \dots, X_m]$, and is a symmetric polynomial, hence by a similar argument we conclude that its evaluation at $\alpha_1, \dots, \alpha_m$ is an integer, and this concludes the proof.

Remark 4.38. Can we remove the assumption $q \nmid \mathrm{disc}(g)$ in Lemma 4.36? The answer is no! For instance, if one takes $g := X^3 - X^2 - 2X - 8$ (the "Dedekind's polynomial" mentioned in [20]), then $\mathrm{disc}(g) = -2^2 \cdot 503$, so that 2 divides the discriminant of g. On one hand, we have that $\overline{g} \equiv X^2(X+1) \pmod 2$, so $\overline{g}$ does not split into distinct linear factor modulo 2. On the other hand, 2 is totally split in K_g (using `PARI-GP`).

We now have all the ingredients to finish the proof of the main proposition of this section.

Proof of Proposition 4.31. Let q be a prime which does not divide the discriminant of g, and which is totally split in K_g. Let $\mathfrak{p} \mid q$ and let $n \geqslant 1$.

- First, the last arrow in the statement ($\mathbf{O}_g/\mathfrak{p}^n \to \mathbf{Z}/q^n\mathbf{Z}$) is an isomorphism thanks to Corollary 4.19, and we claim that it induces a bijection between $\mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)$ and $\mathrm{Z}_g(\mathbf{Z}/q^n\mathbf{Z})$. Indeed, if $\alpha \in \mathbf{O}_g$ is such that $g(\alpha) \equiv 0 \bmod \mathfrak{p}^n$, then:

  - First, thanks to Corollary 4.19, there exists an integer x (unique modulo $q^n\mathbf{Z}$) such that $x \equiv \alpha \bmod \mathfrak{p}^n$.
  - Second, this integer satisfies $g(x) \equiv g(\alpha) \equiv 0 \bmod \mathfrak{p}^n$, which means that $g(x) \in \mathfrak{p}^n \cap \mathbf{Z} = q^n\mathbf{Z}$ thanks to Lemma 4.17. In other words $g(x) \equiv 0 \bmod q^n$.

  This proves that for any $\overline{\alpha} \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)$ there exists a unique $\overline{x} \in \mathbf{Z}/q^n\mathbf{Z}$ such that $x \equiv \alpha \bmod \mathfrak{p}^n$, and that this $\overline{x}$ is a root of g modulo q^n. This proves that the natural isomorphism between $\mathbf{Z}/q^n\mathbf{Z}$ and $\mathbf{O}_g/\mathfrak{p}^n$ induces a bijection between $\mathrm{Z}_g(\mathbf{Z}/q^n\mathbf{Z})$ and $\mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)$. Thus, it just remains to prove that the natural map $\mathrm{Z}_g \to \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)$ is a bijection.

- Thanks to Lemma 4.36, the assumptions on q ensure that $\overline{g}$ splits in $\mathbf{F}_q$ with *simple* roots. Thus, the previous point shows that the polynomial g also split in $\mathbf{O}_g/\mathfrak{p}$ with simple roots.

  Now, let $\overline{\alpha} \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)$ be the reduction modulo $\mathfrak{p}^n$ of some $\alpha \in \mathbf{O}_g$.

  Then we have
  $$\begin{cases} g(\alpha) \equiv 0 \bmod \mathfrak{p}^n \\ g'(\alpha) \not\equiv 0 \bmod \mathfrak{p}. \end{cases}$$

  Therefore, by Hensel's lemma, there exists a unique $\widehat{\alpha}$ in the $\mathfrak{p}$-adic completion $\widehat{\mathbf{O}_g}$ of $\mathbf{O}_g$ such that
  $$\begin{cases} g(\widehat{\alpha}) = 0 \\ \widehat{\alpha} \equiv \alpha \bmod \mathfrak{p}^n. \end{cases}$$

  Now, we have by assumption that g has d distinct roots in $\mathbf{O}_g \subseteq \widehat{\mathbf{O}_g}$, and it cannot have more roots than its degree, so $\widehat{\alpha}$ actually belongs to $\mathbf{O}_g$. This proves that the natural map $\mathrm{Z}_g \to \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)$ is a bijection.

□

Remark 4.39. The proof of this proposition is a natural extension of what we did in the case of the polynomial $X^d - 1$ in Chapter 2. Indeed, in Lemma 2.14, a completion argument and an application of Hensel's lemma were also needed.

4.2.4. Equidistribution of exponential sums restricted to the roots of a polynomial

Now that we did all the sanity checks in the previous section, Theorem 4.30 has the following easy corollary.

Corollary 4.40. (1) *For a taken uniformly at random in $\mathbf{O}_g/\mathfrak{p}^n$ with $\mathfrak{p} \in \mathcal{S}_g$ not dividing the discriminant of g, the sums*

$$\sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)} e\Big(\frac{\tau_{\mathfrak{p}^n}(ax)}{\|\mathfrak{p}\|^n}\Big)$$

become equidistributed in $\mathbf{C}$ as $\|\mathfrak{p}\|^n \to +\infty$ with limiting measure μ_g given by the law of $\sigma(U)$, where $\sigma\colon \mathrm{C}(\mathrm{Z}_g, \mathbf{C}) \to \mathbf{C}$ is the linear form defined by

$$f \mapsto \sum_{x \in \mathrm{Z}_g} f(x).$$

(2) *Similarly, for q prime totally split in K_g and not dividing the discriminant of g, the sums*

$$\sum_{\substack{x \in \mathbf{Z}/q^n\mathbf{Z} \\ g(x) \equiv 0 \,(\mathrm{mod}\, q^n)}} e\Big(\frac{bx}{q^n}\Big)$$

for $b \in \mathbf{Z}/q^n\mathbf{Z}$ become equidistributed in $\mathbf{C}$ as $q^n \to +\infty$ with the same limit.

Proof. (1) The first statement is a direct application of Theorem 4.30 and of the composition principle for convergence in law, since σ is continuous (when $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ has its product topology). Indeed, the random variables

$$\begin{array}{rccc} \mathrm{S}_{\mathfrak{p}^n} & : & \mathbf{O}_g/\mathfrak{p}^n & \to & \mathbf{C} \\ & & a & \mapsto & \sum_{x \in \mathrm{Z}_g} U_{\mathfrak{p}^n}(a)(x) \end{array}$$

are exactly $\sigma(U_{\mathfrak{p}^n})$. Moreover, thanks to Proposition 4.31 (more precisely from the fact that $\varpi_{\mathfrak{p}^n}$ induces a bijection between Z_g and $\mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)$) we have that

$$\mathrm{S}_{\mathfrak{p}^n}(a) = \sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)} e\Big(\frac{\tau_{\mathfrak{p}^n}(ax)}{\|\mathfrak{p}\|^n}\Big)$$

so the statement follows.
(2) For any prime number q which is totally split in K_g, there exists a prime ideal $\mathfrak{p} \in \mathcal{S}_g$ above q. Moreover, the canonical isomorphism $\tau_{\mathfrak{p}^n}$ between the residue rings $\mathbf{O}_g/\mathfrak{p}^n$ and $\mathbf{Z}/q^n\mathbf{Z}$ induces a bijection between $\mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}^n)$ and $\mathrm{Z}_g(\mathbf{Z}/q^n\mathbf{Z})$. Therefore, $\mathrm{S}_{\mathfrak{p}^n}$ and the random variable

$$\begin{array}{rccc} \widetilde{\mathrm{S}}_{q^n} & : & \mathbf{Z}/q^n\mathbf{Z} & \to & \mathbf{C} \\ & & b & \mapsto & \displaystyle\sum_{\substack{x \in \mathbf{Z}/q^n\mathbf{Z} \\ g(x) \equiv 0 \,(\mathrm{mod}\, q^n)}} e\Big(\frac{bx}{q^n}\Big) \end{array}$$

share the same law, so that point (1) provides the equidistribution result (2). □

Remark 4.41. In [77], we included the condition that $\mathfrak{p}$ must not divide the discriminant of the polynomial g in the definition of $\mathcal{S}_g$, in order to avoid repeating this assumption in many statements. However, it is worth noting that the uniform distribution of the unitary random variables (Theorem 4.30) holds *without* this restriction. The assumption that $\mathfrak{p}$ must not divide the discriminant of g only comes into play once we want to deduce corollaries on exponential sums over $\mathrm{Z}_g(\mathbf{F}_q)$, because we need Proposition 4.31.

Remark 4.42. In [77], we define $\mathcal{S}_g$ as the set of prime ideals $\mathfrak{p} \in \mathbf{O}_g$ such that $\mathfrak{p}$ does not divide the discriminant of g and $\mathfrak{p}$ has residual degree 1, and we claim that such primes are unramified primes in $\mathbf{O}_g$. This is not completely straightforward, so let us give some details here. Indeed, our assumption is that $\mathfrak{p}$ does not divide the discriminant *of the polynomial* g, and the classical theorem of algebraic number theory rather says that the primes which do not divide the discriminant *of the number field* K_g are unramified. Thus, we need to spell out more precisely what is the relation between the fact that a prime divides the discriminant of g and the fact that it divides the discriminant of its splitting field K_g. As far as I know, there is no divisibility relation of the type "$\mathrm{disc}(g)$ divides $\mathrm{disc}(K_g)$" or "$\mathrm{disc}(K_g)$ divides $\mathrm{disc}(g)$". However, there is an inclusion between their sets of prime factors, given by the following lemma:

Lemma 4.43. *If $\mathfrak{p}$ divides the discriminant of K_g, then $\mathfrak{p}$ divides the discriminant of the polynomial g.*

Proof. Let $\mathfrak{p} \subseteq \mathbf{O}_g$ be a prime ideal that divides the discriminant of g. As the splitting field K_g is the compositum of the extensions $\mathbf{Q}(z)$ for $z \in \mathrm{Z}_g$, [50, Theorem 85] tells us that $\mathfrak{p}$ must divide the discriminant of one of the extensions $\mathbf{Q}(z)/\mathbf{Q}$. By Remark 4.33, this implies that $\mathfrak{p}$ divides the discriminant of $\mathbf{Z}[z]$, which equals the discriminant of the minimal polynomial of z over $\mathbf{Q}$, which is an irreducible factor of g. Thus, $\mathfrak{p}$ divides the discriminant of g. □

Taking the contrapositive, we deduce that indeed, our condition ensures in particular that the prime ideals which do not divide the discriminant of g are unramified in K_g.

Note that the previous lemma does not imply that $\mathrm{disc}(K_g)$ divides $\mathrm{disc}(g)$, because of the powers of the prime ideals which may appear in each factorization. Moreover, the converse of this lemma does not hold, as one can check by considering Dedekind's polynomial $X^3 - X^2 - 2X - 8$ of Remark 4.38. For this choice of polynomial g, one has $\mathrm{disc}(g) = -2^2 \cdot 503$ while $\mathrm{disc}(K_g) = -503^3$ (using `PARI-GP`).

Remark 4.44. Since the linear map

$$\begin{array}{ccc} \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1) & \to & \mathbf{C} \\ f & \mapsto & \sum_{x \in \mathrm{Z}_g} f(x) \end{array}$$

is continuous and bounded and the random variables $U_{\mathfrak{p}}$ converge in law to U, we have that

$$\mathbb{E}(\sigma(U_{\mathfrak{p}})) \underset{\|\mathfrak{p}\| \to +\infty}{\longrightarrow} \mathbb{E}(\sigma(U)).$$

Now,

$$\begin{aligned} \mathbb{E}(\sigma(U_{\mathfrak{p}})) &= \frac{1}{\|\mathfrak{p}\|} \sum_{a \in \mathbf{O}_g/\mathfrak{p}} \sigma(U_{\mathfrak{p}}(a)) = \frac{1}{\|\mathfrak{p}\|} \sum_{a \in \mathbf{O}_g/\mathfrak{p}} \sum_{x \in \mathrm{Z}_g} U_{\mathfrak{p}}(a)(x) \\ &= \frac{1}{\|\mathfrak{p}\|} \sum_{a \in \mathbf{O}_g/\mathfrak{p}} \sum_{x \in \mathrm{Z}_g} e\left(\frac{\tau_{\mathfrak{p}}(a\varpi_{\mathfrak{p}}(x))}{\|\mathfrak{p}\|}\right) \\ &= \sum_{x \in \mathrm{Z}_g} \frac{1}{\|\mathfrak{p}\|} \sum_{a \in \mathbf{O}_g/\mathfrak{p}} e\left(\frac{\tau_{\mathfrak{p}}(\varpi_{\mathfrak{p}}(x))}{\|\mathfrak{p}\|} \tau_{\mathfrak{p}}(a)\right) \\ &= \sum_{x \in \mathrm{Z}_g} \underbrace{\frac{1}{\|\mathfrak{p}\|} \sum_{b \in \mathbf{Z}/\|\mathfrak{p}\|\mathbf{Z}} e\left(\frac{\tau_{\mathfrak{p}}(\varpi_{\mathfrak{p}}(x))}{\|\mathfrak{p}\|} b\right)}_{\mathbb{1}_{\varpi_{\mathfrak{p}}(x)=0}} \end{aligned} \tag{4.7}$$

and for all $\mathfrak{p}$ such that $\|\mathfrak{p}\|$ is large enough, $\varpi_{\mathfrak{p}}(x) = 0$ if and only if $x = 0$, so that eventually we have

$$\mathbb{E}(\sigma(U_{\mathfrak{p}})) = \begin{cases} 0 \text{ if } 0 \notin \mathrm{Z}_g \\ 1 \text{ if } 0 \in \mathrm{Z}_g. \end{cases} \tag{4.8}$$

As a consequence,

$$\mathbb{E}(\sigma(U)) = \begin{cases} 0 \text{ if } 0 \notin \mathrm{Z}_g \\ 1 \text{ if } 0 \in \mathrm{Z}_g. \end{cases}$$

In view of (4.7) and (4.8), and using Proposition 4.31 to identify those sums with sums over $\mathrm{Z}_g(\mathbf{F}_q)$, this shows that if $0 \notin \mathrm{Z}_g$, then *on average over* $b \in \mathbf{F}_q$, the sums

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{bx}{q}\right)$$

equal 0 as q tends to infinity (among the prime numbers q which do not divide the discriminant of g and are totally split in K_g).

A natural question one may ask is the horizontal analogue: does the same result hold if we fix a non-zero integer b and average over primes q? We will come back to this question (and its relation to famous conjectures regarding the uniform distribution of roots of polynomials) in the final chapter of this thesis, where some research perspectives are sketched.

4.2.5. Sparse equidistribution

As in the case of the sums $\mathrm{S}_p(a,d)$ of Chapter 2 and 3, we can get equidistribution of sparser sets of sums, by changing the probability space in the definition of the random variables $U_{\mathfrak{p}^n}$ (Definition 4.25). Indeed, if for all prime ideal $\mathfrak{p} \subset \mathcal{S}_g$ and all $n \geqslant 1$, we choose a subgroup $H_{\mathfrak{p}^n}$ of the multiplicative group $(\mathbf{O}_g/\mathfrak{p}^n)^\times$ and redefine the random variables

$$\begin{array}{rccc} U_{\mathfrak{p}^n} & : & H_{\mathfrak{p}^n} & \to & \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1) \\ & & a & \mapsto & U_{\mathfrak{p}^n}(a) \end{array}$$

then under some growth conditions on the cardinality of $H_{\mathfrak{p}^n}$, the convergence in law of Theorem 4.30 still holds. Indeed, a proposition analogous to Proposition 3.4 allows us to apply the main theorem of [11] on exponential sums over small multiplicative subgroups.

Proposition 4.45. *Let $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$ be such that $\alpha \notin \mathrm{R}_g$ and let $S_\alpha := \sum_{x \in \mathrm{Z}_g} \alpha(x)x$ (which is non-zero by definition of R_g).*
There exist two constants $n_\alpha, C_\alpha \geqslant 1$ such that for all $\mathfrak{p} \in \mathcal{S}_g$ (lying above q, say) and for all $n \geqslant 1$, if $\|\mathfrak{p}\|^n > n_\alpha$, then

(a) $\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha)) \not\equiv 0 \,(\mathrm{mod}\, q^n)$

(b) $q^{v_q(\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha)))} \leqslant C_\alpha$.

Proof. (a) Since $\tau_{\mathfrak{p}^n}$ is an isomorphism, we have that $\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha)) \equiv 0 \,(\mathrm{mod}\, q^n)$ if and only if $\varpi_{\mathfrak{p}^n}(S_\alpha) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}^n)$, that is: if and only if $S_\alpha \in \mathfrak{p}^n$. Now we have seen in the proof of Theorem 4.30 that the fact that $S_\alpha \in \mathfrak{p}^n$ implies that $\|\mathfrak{p}\|^n$ divides the non-zero integer $\mathrm{N}_{K_g/\mathbf{Q}}(S_\alpha)$. Therefore, it suffices to take $n_\alpha := |\mathrm{N}_{K_g/\mathbf{Q}}(S_\alpha)|$ to ensure that (a) holds for all $\mathfrak{p}$ and n such that $\|\mathfrak{p}\|^n > n_\alpha$.

(b) Now we assume that $\|\mathfrak{p}\|^n > n_\alpha$, so that the q-adic valuation of $\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha))$ is well defined. We denote it by $\gamma \in \{0, \dots, n-1\}$, so that we can write

$$\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha)) \equiv q^\gamma m \,(\mathrm{mod}\, q^n)$$

where $(m,q) = 1$. Applying $\iota_{\mathfrak{p}^n}$ (the inverse of $\tau_{\mathfrak{p}^n}$) to this equality gives

$$\varpi_{\mathfrak{p}^n}(S_\alpha) \equiv q^\gamma m \,(\mathrm{mod}\, \mathfrak{p}^n)$$

from which it is easy to see that $\gamma = v_{\mathfrak{p}}(S_\alpha)$. Therefore, we have

$$q^\gamma = q^{v_q(\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha)))} = q^{v_{\mathfrak{p}}(S_\alpha)}$$

and the right-hand side is bounded above by

$$C_\alpha := \max\left\{ \|\mathfrak{p}\|^{v_{\mathfrak{p}}(S_\alpha)} ;\ \mathfrak{p} \in \mathcal{S}_g \text{ such that } \mathfrak{p} \mid S_\alpha \mathbf{O}_g \right\}$$

which is the maximum of a finite set because $S_\alpha \neq 0$.

□

Thanks to this control of the q-adic valuation, we can reduce to a setting where Bourgain's theorem (Theorem 3.11) can be applied, and prove the convergence in law of the random variables $U_{\mathfrak{p}^n}$ when defined on the probability spaces $H_{\mathfrak{p}^n}$ which are multiplicative subgroups of cardinality larger than $(\|\mathfrak{p}\|^n)^\delta$ for some positive real number delta.
Namely, we have the following refinement of Theorem 4.30:

Theorem 4.46. *For each $\mathfrak{p} \in \mathcal{S}_g$ and $n \geqslant 1$, we fix a multiplicative subgroup $H_{\mathfrak{p}^n}$ of $(\mathbf{O}_g/\mathfrak{p}^n)^\times$ and define the random variables $U_{\mathfrak{p}^n}$ as before, but on this smaller probability space:*

$$\begin{array}{rccc} U_{\mathfrak{p}^n} & : & H_{\mathfrak{p}^n} & \to & \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1) \\ & & a & \mapsto & U_{\mathfrak{p}^n}(a) \end{array}$$

Then, if there exists $\delta > 0$ such that for all $\mathfrak{p}$ and n,

$$|H_{\mathfrak{p}^n}| \geqslant (\|\mathfrak{p}\|^n)^\delta,$$

the random variables $U_{\mathfrak{p}^n}$ converge in law to a uniformly distributed random variable U on H_g, as $\|\mathfrak{p}\|^n$ tends to infinity.

Proof. The Weyl sums appearing in the application of Weyl's equidistribution criterion are in this case

$$\frac{1}{|H_{\mathfrak{p}^n}|} \sum_{a \in H_{\mathfrak{p}^n}} e\left(\frac{\tau_{\mathfrak{p}^n}(a\varpi_{\mathfrak{p}^n}(S_\alpha))}{\|\mathfrak{p}\|^n}\right)$$

and we want to prove that they converge to zero as $\|\mathfrak{p}\|^n$ tends to infinity, for any fixed $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$ such that $\alpha \notin \mathrm{R}_g$ (this condition reflects the fact that we only need to consider *non-trivial* characters of H_g). Making the change of variables $b = \tau_{\mathfrak{p}^n}(a)$, we can write these sums as

$$\frac{1}{|H_{\|\mathfrak{p}\|^n}|} \sum_{b \in H_{\|\mathfrak{p}\|^n}} e\left(\frac{\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha))}{\|\mathfrak{p}\|^n} b\right)$$

where $H_{\|\mathfrak{p}\|^n}$ denotes the multiplicative subgroup $\tau_{\mathfrak{p}^n}(H_{\mathfrak{p}^n})$ of $(\mathbf{Z}/\|\mathfrak{p}\|^n \mathbf{Z})^\times$. As in the proof of Proposition 3.12, we cannot directly apply Theorem 3.11 because we do not know if $\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha))$ is invertible modulo $\|\mathfrak{p}\|^n$. However, we know that it is non-zero, and that it is not divisible by high powers of $\|\mathfrak{p}\|$, so that it is not far from being invertible. The precise meaning of this "not far from being invertible" is given by the control of the q-adic valuation of Proposition 4.45. Then, the rest of the proof is exactly the same as the proof of Proposition 3.12, with $f(w_q)$ replaced by $\tau_{\mathfrak{p}^n}(\varpi_{\mathfrak{p}^n}(S_\alpha))$ and n_f, C_f by n_α, C_α. □

Corollary 4.47. *Let $g \in \mathbf{Z}[X]$ be a monic and separable polynomial of degree $d \geqslant 1$. For all $q \in \mathcal{S}_g$ not dividing the discriminant of g and all $n \geqslant 1$, suppose we are given a subgroup H_{q^n} of the multiplicative group $(\mathbf{Z}/q^n\mathbf{Z})^\times$. If there exists $\delta > 0$ such that for all q and n,*

$$|H_{q^n}| \geqslant q^{n\delta},$$

then the sums

$$\sum_{\substack{x \in \mathbf{Z}/q^n\mathbf{Z} \\ g(x) \equiv 0 \,(\mathrm{mod}\, q^n)}} e\left(\frac{bx}{q^n}\right)$$

parametrized by $b \in H_{q^n}$, become equidistributed in $\mathbf{C}$ as q^n goes to infinity, with respect to the same measure as in Corollary 4.40 (2).

Remark 4.48. A natural question one may ask is: can we replace subgroups H_{q^n} of $(\mathbf{Z}/q^n\mathbf{Z})^\times$ by arbitrary subsets A_{q^n} of $\mathbf{Z}/q^n\mathbf{Z}$, and under which condition do we still have equidistribution of the sets of sums

$$\left\{ \sum_{\substack{x \in \mathbf{Z}/q^n\mathbf{Z} \\ g(x) \equiv 0 \,(\mathrm{mod}\, q^n)}} e\left(\frac{bx}{q^n}\right),\ b \in A_{q^n} \right\} \tag{4.9}$$

with respect to the same measure? This question is addressed in Section 4 of [77], where we give a partial answer to that question. Under a certain condition on the polynomial g, we prove that there is

an equivalence between the uniform distribution of the sets (4.9) and the *uniform equidistribution* of the fractional parts[1] of the elements of A_{q^n}, which corresponds to the convergence to zero of

$$\max_{\substack{h\in\mathbf{Z}/q^n\mathbf{Z}\\ h\neq 0}} \frac{1}{|A_{q^n}|}\left|\sum_{a\in A_{q^n}} e\left(\frac{ah}{q^n}\right)\right|.$$

In particular, if $n=1$ and we take A_q to be $\{0,\dots,(q-1)/2\}$, then it is easy to see that the fractional parts of the elements of A_q are not uniformly equidistributed, so that we can find polynomials g for which the sums in (4.9) do not become equidistributed with respect to the measure μ_g of Corollary 4.40 (2).

4.3. Some explicit determinations of the module of additive relations

4.3.1. A general approach

A fruitful idea to study this type of question was developped by Girstmair in [45, 46], and we describe here the general idea in the case where the ground field is $\mathbf{Q}$. This section also owes a lot to E. Kowalski's treatment in [74, section 4.7.3].
Given a separable polynomial $g\in\mathbf{Q}[X]$ (g will even be in $\mathbf{Z}[X]$ in the applications we have in mind), we denote by Z_g its set of complex roots, and by $K_g:=\mathbf{Q}(\mathrm{Z}_g)$ the splitting field of g over $\mathbf{Q}$. We also denote by $\mathbf{Q}^{\mathrm{Z}_g}$ the set of maps from Z_g to $\mathbf{Q}$, and by G the Galois group of the field extension $K_g/\mathbf{Q}$. Then G acts on Z_g, and this gives rise to the *permutation representation* of G on $\mathbf{Q}^{\mathrm{Z}_g}$. Precisely, given an element $\alpha\in\mathbf{Q}^{\mathrm{Z}_g}$ (that is: a map $\alpha\colon \mathrm{Z}_g\to\mathbf{Q}$), the action of an element $\sigma\in G$ on α is given by

$$(\sigma,\alpha)\mapsto \alpha\circ\sigma^{-1}$$

In other words, if we write

$$\alpha=\sum_{x\in\mathrm{Z}_g}\alpha(x)\delta_x$$

where $\delta_x(y)=1$ if $y=x$ and equals 0 otherwise, the action of σ on α is simply its natural action on the roots,

$$\sigma\cdot\alpha=\sum_{x\in\mathrm{Z}_g}\alpha(x)\delta_{\sigma(x)}.$$

We have the evaluation map from $\mathbf{Q}^{\mathrm{Z}_g}$ to $\mathrm{Span}_{\mathbf{Q}}(\mathrm{Z}_g)\subseteq\mathbf{Q}(\mathrm{Z}_g)$:

$$\mathrm{ev}\colon \alpha\mapsto\sum_{x\in\mathrm{Z}_g}\alpha(x)x$$

which is easily seen to be a morphism of G-representations when the $\mathbf{Q}(\mathrm{Z}_g)$ on the right-hand side has the natural Galois action. Therefore, as the kernel of the evaluation, the vector space of $\mathbf{Q}$-linear relations between the roots of g :

$$\mathrm{R}_{g,\mathbf{Q}}:=\left\{\alpha\colon \mathrm{Z}_g\to\mathbf{Q},\ \sum_{x\in\mathrm{Z}_g}\alpha(x)x=0\right\}$$

is a subrepresentation of $\mathbf{Q}^{\mathrm{Z}_g}$. Thus, in order to determine $\mathrm{R}_{g,\mathbf{Q}}$, it can be helpful to determine the decomposition of $\mathbf{Q}^{\mathrm{Z}_g}$ as a direct sum of irreducible subrepresentations.

[1] If $a\in\mathbf{Z}/q^n\mathbf{Z}$, the fractional part $\left\{\frac{\tilde{a}}{q^n}\right\}$ of the rational number $\tilde{a}/q^n$ does not depend on the lift $\tilde{a}\in\mathbf{Z}$ which represents the residue class a. This is what we call the "fractional part of a".

4.3.2. The case of roots of unity

Although we already recovered the results of Chapter 2 in section 4.1.4 by determining the module of additive relation with integral coefficients R_g, let us illustrate how the point of view of representations can be used in this simple case.

For a prime number ℓ, consider the polynomial $g := X^\ell - 1$. Then $\mathrm{Z}_g = \boldsymbol{\mu}_\ell = \{\zeta^j;\ 0 \leqslant j \leqslant \ell - 1\}$ where $\zeta = \exp(2i\pi/\ell)$, and the splitting field of g is $K_g = \mathbf{Q}(\zeta)$. It has degree $\ell - 1$ over $\mathbf{Q}$, and we have the homomorphism of $\mathrm{Gal}\,(\mathbf{Q}(\zeta)/\mathbf{Q})$-representations:

$$\mathrm{ev} : \mathbf{Q}^{\mathrm{Z}_g} \to \mathbf{Q}(\zeta)$$

This homomorphism is surjective because $\mathbf{Q}(\zeta) = \mathbf{Q}[\zeta] = \mathrm{Span}_{\mathbf{Q}}(\mathrm{Z}_g)$. Therefore, by the rank-nullity theorem, we have

$$\dim(\ker(\mathrm{ev})) = \dim(\mathbf{Q}^{\mathrm{Z_g}}) - \dim(\mathbf{Q}(\zeta)) = \ell - (\ell - 1) = 1 \tag{4.10}$$

But as we explained above, the kernel of the evaluation map is nothing but the module of $\mathbf{Q}$-linear relations between the roots of g. Thus, $\mathrm{R}_{g,\mathbf{Q}}$ has dimension 1 over $\mathbf{Q}$. Moreover, we know that the sum of the elements of $\boldsymbol{\mu}_\ell$ equals 0, so that the constant map $\mathbb{1}$ (which maps all the elements of Z_g to 1) is an element of $\mathrm{R}_{g,\mathbf{Q}}$. From this we conclude that

$$\mathrm{R}_{g,\mathbf{Q}} = \mathbf{Q}\mathbb{1} = \{\alpha \colon \boldsymbol{\mu}_\ell \to \mathbf{Q} \text{ such that } \alpha \text{ is constant}\}$$

In particular, this implies that the modulo of $\mathbf{Z}$-linear relations, which we denoted by R_g in the previous sections, is actually a free $\mathbf{Z}$-module of rank 1, generated by the constant map equal to 1.

Remark 4.49. In the general case where $g = X^d - 1$ for d not necessarily prime, the surjectivity of the evaluation map is still true, and equation (4.10) gives that the dimension of $\mathrm{R}_{g,\mathbf{Q}}$ equals $d - \varphi(d)$.

4.3.3. The case of primitive roots of unity

If we consider the polynomial $g := \phi_\ell$ (the ℓ-th cyclotomic polynomial) for some prime number ℓ, then we have again $K_g = \mathbf{Q}(\zeta)$ with the notation above, and this time Z_g just consists of the *primitive* ℓ-th roots of unity. Therefore, $\mathbf{Q}^{\mathrm{Z}_g}$ and K_g have the same dimension $\ell - 1$ over $\mathbf{Q}$. Moreover, the linear map $\mathrm{ev}\colon \mathbf{Q}^{\mathrm{Z}_g} \to K_g$ is still surjective because the primitive ℓ-th roots of unity form a $\mathbf{Q}$-basis of $\mathbf{Q}(\zeta)$[2]. Therefore, the rank-nullity theorem implies that the dimension of the space of $\mathbf{Q}$-linear relations between the roots of g equals 0. In particular, the module of additive relations R_g is trivial in this case! In view of Corollary 4.40 (2), this translates into the fact that the sums

$$\mathrm{S}_q^\star(a, \ell) := \sum_{x \in \mu_\ell^\star(\mathbf{F}_q)} e\left(\frac{ax}{q}\right) \tag{4.11}$$

become equidistributed with respect to the measure on $\mathbf{C}$ which is the law of $\ell - 1$ independent random variables, each uniformly distributed on $\mathbf{S}^1$.

[2]More generally, one can prove that the primitive d-th roots of unity are linearly independent over $\mathbf{Q}$ if and only if d is squarefree, see [55, Satz 3] or https://math.stackexchange.com/questions/87290/basis-of-primitive-nth-roots-in-a-cyclotomic-extension?noredirect=1&lq=1

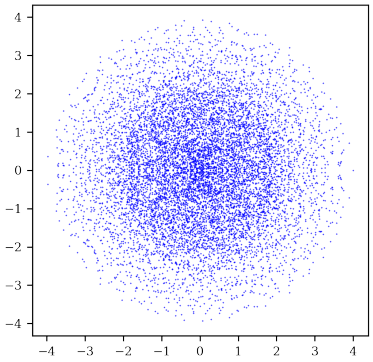


Figure 4.1: The sums $\mathrm{S}_q^\star(a,d)$ for $d=5$, $q=10151$ and a varying in $\mathbf{F}_q$.

These last two examples only relied on arguments on the dimensions of $\mathbf{Q}^{\mathrm{Z}_g}$ and K_g, but did not involve any more involved notions of representations. In the following section, we present some special cases where the decomposition into irreducible subrepresentations plays a role in the study of the additive relations.

4.3.4. The case where $\mathrm{Gal}\,(K_g/\mathbf{Q}) \simeq \mathfrak{S}_d$

In this section, we assume that the Galois group of $K_g/\mathbf{Q}$ is isomorphic to $\mathfrak{S}_d$, meaning that any permutation of the roots of g can be realized by the action of an element of $\mathrm{Gal}\,(K_g/\mathbf{Q})$. In this case, we have the following decomposition as a direct sum of subrepresentations:

$$\mathbf{Q}^{\mathrm{Z}_g} = V \oplus W,$$

where $V = \mathbf{Q}\mathbb{1}$ is the 1-dimensional subspace spanned by the constant function equal to 1 and

$$W := \left\{ \alpha \in \mathbf{Q}^{\mathrm{Z}_g};\ \sum_{x\in \mathrm{Z}_g} \alpha(x) = 0 \right\}.$$

As V is 1-dimensional, it is an irreducible subrepresentation, and clearly the action of $\mathrm{Gal}\,(K_g/\mathbf{Q})$ is trivial on V (i.e. for all $\alpha \in V$, for all $\sigma \in \mathrm{Gal}\,(K_g/\mathbf{Q})$, $\sigma\cdot\alpha = \alpha$). This implies that the character of this subrepresentation is constant equal to 1:

$$\forall \sigma \in \mathrm{Gal}\,(K_g/\mathbf{Q})\,,\ \chi_V(\sigma) = 1.$$

On the other hand, the character of W can be determined from the knowledge of the character of the full permutation representation on $\mathbf{Q}^{\mathrm{Z}_g}$ (because $\mathbf{Q}^{\mathrm{Z}_g} = V \oplus W$ implies that $\chi_{\mathbf{Q}^{\mathrm{Z}_g}} = \chi_V + \chi_W$). Gladly, the character of the permutation representation is quite accessible! Indeed, it is not hard to prove that the character of any permutation representation associated with an action of a finite group G on a finite set X is given by:

$$\chi\colon \sigma \mapsto |X^\sigma|$$

where X^σ denotes the set $\{x \in X, \sigma\cdot x = x\}$ (the set of points fixed by σ). This implies that the character of W is given by:

$$\chi_W\colon \sigma \in \mathrm{Gal}\,(K_g/\mathbf{Q}) \mapsto |\mathrm{Z}_g^\sigma| - 1 = \#\{x \in \mathrm{Z}_g \ \mid\ \sigma(x) = x\} - 1$$

From this, one can deduce that W is irreducible, because it is *absolutely irreducible*, meaning that it is irreducible even after tensorization with $\mathbf{C}$. Indeed, over $\mathbf{C}$, the irreducibility can be proved by computing the inner product

$$\langle \chi_W, \chi_W \rangle := \frac{1}{d!} \sum_{\sigma \in \mathrm{Gal}(K_g/\mathbf{Q})} |\chi_W(\sigma)|^2$$

and showing that it equals 1 (see [74, Corollary 4.3.14]). Replacing $\chi_W(\sigma)$ by its explicit expression determined above and expanding the square, one obtains:

$$\langle \chi_W, \chi_W \rangle = \left(\frac{1}{d!} \sum_{\sigma \in \mathrm{Gal}(K_g/\mathbf{Q})} |\mathrm{Z}_g^\sigma|^2 \right) - 2 \left(\frac{1}{d!} \sum_{\sigma \in \mathrm{Gal}(K_g/\mathbf{Q})} |\mathrm{Z}_g^\sigma| \right) + 1.$$

Thanks to Burnside's lemma, the term $\frac{1}{d!} \sum_{\sigma \in \mathrm{Gal}(\mathrm{K}_g/\mathbf{Q})} |\mathrm{Z}_g^\sigma|$ equals the number of orbits of Z_g under the action of $\mathrm{Gal}\,(K_g/\mathbf{Q})$, so it is equal to 1 as the action is transitive. On the other hand, the term with $|\mathrm{Z}_g^\sigma|^2$ counts the number of orbits of $\mathrm{Z}_g \times \mathrm{Z}_g$ under the diagonal action of the Galois group. The key argument to conclude is the fact there are two orbits (namely the diagonal $\{(x,x), x \in \mathrm{Z}_g\}$ and its complement), and this is due to that fact that the action of the Galois group is *doubly transitive*. This proves that $\langle \chi_W, \chi_W \rangle = 1$, hence the irreducibility of W.

Finally, the subrepresentations V and W are not isomorphic over $\mathbf{C}$ because they do not have the same character for instance.

Let us explain how this decomposition of $\mathbf{Q}^{\mathrm{Z}_g}$ into two non-isomorphic subrepresentations can help us understanding the additive relations between the roots of g. As we said before, the vector space of $\mathbf{Q}$-linear relations is a subrepresentation of $\mathbf{Q}^{\mathrm{Z}_g} = V \oplus W$. It follows from the uniqueness of isotypic components (see e.g. [74, Proposition 2.7.9 (2)]) that

$$\mathrm{R}_{g,\mathbf{Q}} = \{0\} \text{ or } V \text{ or } W \text{ or } \mathbf{Q}^{\mathrm{Z}_g} \tag{4.12}$$

In the proof of the following proposition, which is due to Girstmair, we will see that the last two cases actually do not occur (we follow the proof of Kowalski's book).

Proposition 4.50 (Girstmair, [74, Proposition 4.7.12])**.** *Let $g \in \mathbf{Z}[X]$ be a separable polynomial of degree $d \geqslant 1$ such that its Galois group $\mathrm{Gal}\,(K_g/\mathbf{Q})$ is isomorphic to $\mathfrak{S}_d$. Then R_g is either $\{0\}$ or the free $\mathbf{Z}$-module generated by the constant function equal to 1.*

In other words, either the coefficient of X^{d-1} in $g(X)$ is zero, in which case the sum of the roots of g equals 0 and it is the only (up to multiplicative constants) additive relation between the roots, or the coefficient of X^{d-1} is non-zero and there are no non-trivial additive relations between the roots. Note that as soon as there exists a polynomial with Galois group $\mathfrak{S}_d$, then both cases occur because a simple change of variables can cancel the coefficient of X^{d-1} without affecting the splitting field.

Proof. Thanks to the above discussion, it suffices to rule out the last two possibilities in (4.12) to obtain the conclusion. Assume for a contradiction that $W \subseteq \mathrm{R}_{g,\mathbf{Q}}$. Fixing two distinct roots of g, say x and y, define the map $\alpha\colon \mathrm{Z}_g \to \mathbf{Q}$ by $\alpha(x) = 1$, $\alpha(y) = -1$ and for all $z \in \mathrm{Z}_g \setminus \{x,y\}$, $\alpha(z) = 0$. Then by definition we have that $\alpha \in W$, which (as we assumed) is contained in $\mathrm{R}_{g,\mathbf{Q}}$, so $\alpha \in \mathrm{R}_{g,\mathbf{Q}}$. This means that

$$\alpha(x)x + \alpha(y)y + \sum_{z_i n \mathrm{Z}_g \setminus \{x,y\}} \alpha(z)z = 0,$$

i.e. $x = y$, and this is a contradiction. □

Corollary 4.51. *Let $g \in \mathbf{Z}[X]$ be a monic and separable polynomial of degree $d \geqslant 1$ such that its Galois group $\mathrm{Gal}\,(K_g/\mathbf{Q})$ is isomorphic to $\mathfrak{S}_d$. Then the exponential sums*

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{ax}{q}\right)$$

for q totally split in K_g and not dividing the discriminant of g, and a varying in $\mathbf{F}_q$, become equidistributed in $\mathbf{C}$ with respect to a measure μ_g which is either

(1) *the law of the sum of d-independent and identically distributed Steinhaus random variables (this occurs if and only if the coefficient of X^{d-1} of $g(X)$ is non-zero).*

(2) *or the pushforward measure via the Laurent polynomial*

$$z_1 + \cdots + z_{d-1} + \frac{1}{z_1 \dots z_{d-1}}$$

of the uniform measure on $(\mathbf{S}^1)^{d-1}$ *(and this occurs if and only if the coefficient of* X^{d-1} *of* $g(X)$ *equals zero).*

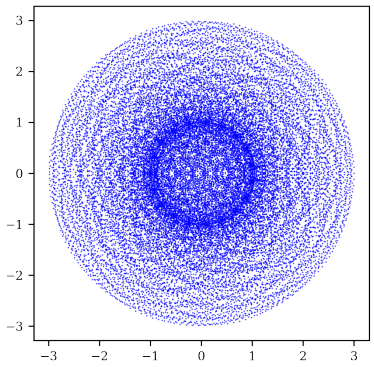
Proof. This is Corollary 4.40 combined with an explicit determination of the law of the random variable U, which is provided by the explicit determination of the module of additive relation of Proposition 4.50. □

In order to give an illustration of this result, one needs to find polynomials with Galois group $\mathfrak{S}_d$. Hilbert proved, as a consequence of his irreducibility theorem that such polynomials exist for any $d \geqslant 1$.

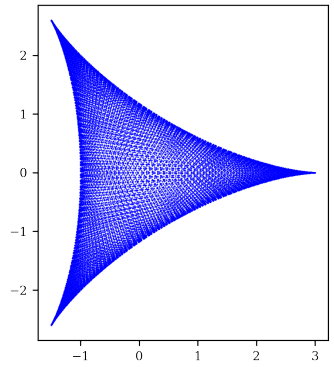
Moreover, for irreducible polynomials of degree 3, there is a very simple criterion to determine whether the Galois group of a polynomial is $\mathfrak{S}_3$ or not:

Proposition 4.52 ([21, Theorem 2.1])**.** *Let* $g \in \mathbf{Q}[X]$ *be an irreducible polynomial of degree* 3*. If* $\mathrm{disc}(g)$ *is a square in* $\mathbf{Q}$*, then* $\mathrm{Gal}\,(K_g/\mathbf{Q})$ *is isomorphic to* $\mathfrak{A}_3$*, otherwise it is isomorphic to* $\mathfrak{S}_3$*.*

In the picture below, we chose two irreducible polynomials of degree 3 and checked that their Galois group is the full symmetric group using this criterion. In the case of the polynomial X^3+2X^2+3, there are no non-trivial additive relations between the zeros of g (because the sum of the roots is non-zero, as one can see from the coefficient of X^2), whereas in the case of the polynomial $X^3 + X + 3$, there is clearly the relation given by the sum of the roots which equals zero (because the coefficient of X^2 is zero). Thus, these two polynomials illustrate the two possibilities in Corollary 4.51. We see that the difference between their module of additive relations translates into different limiting measures μ_g for the associated sums of additive characters.



(a) $g = X^3 + 2X^2 + 3$ and $q = 30113$.



(b) $g = X^3 + X + 3$ and $q = 30223$.

Figure 4.2: The sums $\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{ax}{q}\right)$ as a varies in $\mathbf{F}_q$, for two two different polynomials g of degree 3.

Remark 4.53. Although it may look very specific to prescribe the Galois group as we did, it is actually the typical case to have the full symmetric group as Galois group. Indeed, if we denote by $E_d(H)$ the number of monic polynomials $g(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbf{Z}[X]$ such that $\max\{|a_0|, \dots, |a_{d-1}|\} \leqslant H$ and $\mathrm{Gal}\,(K_g/\mathbf{Q})$ is not isomorphic to $\mathfrak{S}_d$, then

$$E_d(H) \underset{H \to +\infty}{=} o\left(H^d\right).$$

This is a consequence of Hilbert's irreducibility theorem. As the total number of polynomials of the form $X^d + a_{d-1}X^{d-1} + \cdots + a_0$ with $\max\{|a_0|, \dots, |a_{d-1}|\} \leqslant H$ equals $(2H+1)^d$, this implies that

asymptotically, 100% of monic polynomials of degree d with integer coefficients have their Galois group isomorphic to $\mathfrak{S}_d$.
Moreover, one can easily find a lower bound for $E_d(H)$, since all polynomials with $a_0 = 0$ will admit 0 as a rational root, so the Galois group of their splitting field over $\mathbf{Q}$ will be a subgroup of $\mathfrak{S}_{d-1}$, hence will not be maximal. Therefore, $E_d(H) \gg H^{d-1}$. In 1936, van der Waerden [105] conjectured that the latter was the correct order of magnitude, meaning that the upper bound

$$E_d(H) \ll H^{d-1}$$

should also hold. 86 years later, Bhargava proved this conjecture in a preprint of October 2022: [6][3]. This gives a strong quantitative sense to the sentence "most polynomials of degree d with integer coefficient have Galois group $\mathfrak{S}_d$".
Now that van der Waerden's conjecure has been proved, we can derive without much effort a quantitative bound for the proportion of polynomials falling in each case of Corollary 4.51. Indeed, the number of polynomials $g(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ having the sums of their roots equal to zero is $\ll H^{d-1}$ because one needs a_{d-1} to be zero. Therefore, the number of polynomials which do not fall in the first case of Corollary 4.51 (either because their Galois group is not $\mathfrak{S}_d$ or because the sums of their roots equals 0) is $\ll H^{d-1}$. Thus, writing again

$$g(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$$

we have

$$\frac{\#\left\{g(X) \;\middle|\; \max_{0\leqslant i<d}|a_i| \leqslant H \text{ and } g \text{ does not fall in case (1) of Corollary 4.51}\right\}}{(2H+1)^d} \ll 1/H.$$

4.3.5. The case where $\mathrm{Gal}\,(K_g/\mathbf{Q}) \simeq W_d$

This section is inspired by [74, Exercise 4.7.13]. Assume that $d = 2n$ is an even integer, and denote by $X := \{-n, \ldots, -1, 1, \ldots, n\}$ and by $\mathfrak{S}_d$ the set of bijective maps from X to X. We define the group W_d as follows:

$$W_d := \{\sigma \in \mathfrak{S}_d \;\mid\; \sigma(-j) = -\sigma(j) \text{ for all } j \in X\}$$

In other words, it is the set of σ which permute the set of pairs $\{-j, j\}$. In *loc. cit.*, it is shown that the Galois group of an irreducible *palindromic*[4] polynomial of degree d can be seen as a subgroup of W_d. If the Galois group is the full group W_d, then one can determine the decomposition into irreducible subrepresentations of the permutation representation induced by the action of W_d on the roots, and the result is the following:

$$\mathbf{Q}^{\mathrm{Z}_g} = V_1 \oplus V_2 \oplus V_3.$$

Here, $V_1 = \mathbf{Q}\mathbb{1}$ is the 1-dimensional linear subspace spanned by the constant map equal to 1,

$$V_2 = \left\{\alpha \in \mathbf{Q}^{\mathrm{Z}_g} \;\middle|\; \text{for all } x \in \mathrm{Z}_g,\ \alpha(1/x) = \alpha(x) \text{ and } \sum_{x\in\mathrm{Z}_g} \alpha(x) = 0\right\}$$

and

$$V_3 = \left\{\alpha \in \mathbf{Q}^{\mathrm{Z}_g} \;\middle|\; \text{for all } x \in \mathrm{Z}_g,\ \alpha(1/x) = -\alpha(x)\right\}.$$

As in the previous section, one can show that this is a decomposition into absolutely irreducible subrepresentations, and deduce that $\mathrm{R}_{g,\mathbf{Q}}$ can only be a direct sum of some of the representations V_1, V_2 and V_3. In fact, if g is an irreducible palindromic polynomial with Galois group W_d, one can

[3] I thank my journalist friend Clémentine Laurens for bringing that to my attention! You can click here to read her article for *Le Monde*.

[4] A polynomial g is said to be palindromic if its coefficients form a palindrome, which is equivalent to the fact that $X^{\deg(g)}g(1/X) = g(X)$.

prove that the inclusions $V_2 \subseteq \mathrm{R}_{g,\mathbf{Q}}$ and $V_3 \subseteq \mathrm{R}_{g,\mathbf{Q}}$ both lead to contradictions (under the assumption that $n \geqslant 2$ so that $d \geqslant 4$), so the only possibilities are

$$\mathrm{R}_{g,\mathbf{Q}} = \{0\} \text{ or } \mathbf{Q}\mathbb{1}.$$

We refer to [71, Proposition 2.4] for more details.

Thus, we have the following analogue of Corollary 4.51:

Corollary 4.54. *Let $g \in \mathbf{Z}[X]$ be a monic, irreducible and palindromic polynomial of even degree $d \geqslant 4$ such that its Galois group $\mathrm{Gal}(K_g/\mathbf{Q})$ is isomorphic to W_d. Then the exponential sums*

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{ax}{q}\right)$$

for q totally split in K_g and not dividing the discriminant of g, and a varying in $\mathbf{F}_q$, become equidistributed in $\mathbf{C}$ with respect to a measure μ_g which is either

(1) *the law of the sum of d-independent and identically distributed Steinhaus random variables (this occurs if and only if the coefficient of X^{d-1} of $g(X)$ is non-zero).*

(2) *or the pushforward measure via the Laurent polynomial*

$$z_1 + \cdots + z_{d-1} + \frac{1}{z_1 \dots z_{d-1}}$$

of the uniform measure on $(\mathbf{S}^1)^{d-1}$ (and this occurs if and only if the coefficient of X^{d-1} of $g(X)$ equals zero).

Remark 4.55. The $\mathbf{Q}$-linear relations between the roots of a polynomial with Galois group W_d have been studied in the paper [71]. Let us describe briefly the type of questions tackled in this article, to show the relevance of the study of linear relations in other problems of analytic number theory.
Among others, one motivation is the study of the Chebyshev bias, a particular case of which is the observation made by Chebyshev that for most x, there are more primes $p \leqslant x$ that are congruent to 3 modulo 4 than primes $p \leqslant x$ that are congruent to 1 modulo 4. Denoting by $\pi(x;4,3)$ and $\pi(x;4,1)$ the number of such primes, Chebyshev observed that for the first thousands values of x, one had the inequality

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

Actually, the first value of x for which $\pi(x;4,3) < \pi(x;4,1)$ is 26861. Littlewood proved that $\pi(x;4,1) < \pi(x;4,3)$ actually changes signs infinitely often, but still, the primes congruent to 3 modulo 4 seem to be ahead "most of the time" in their race against the primes congruent to 1 modulo 4. In the article [93], Rubinstein and Sarnak gave a conjectural explanation of this phenomenon. The first chapter of Alexandre Bailleul's Ph.D. thesis [3] gives a very detailed description of their approach. In a few words, they used explicit formulas to relate the prime counting functions involved in the problem to sums over the zeros of Dirichlet L-functions. To understand the oscillations inside these sums, one needs (in view of the Kronecker-Weyl theorem) to study the $\mathbf{Q}$-linear relations between the imaginary parts of the zeros. This led Rubinstein and Sarnak to introduce the *linear independence hypothesis*, and conditionally on this assumption (as well as the generalized Riemann hypothesis concerning the real part of the zeros) they proved that the set

$$\{x \geqslant 2 \ \mid \ \pi(x;4,1) < \pi(x;4,3)\}$$

admits a logarithmic density which is approximately $0.9959\ldots$ This gives an explanation to Chebyshev's observation, and it extends to arbitrary arithmetic progressions. It reveals that in the race between $\pi(x;q,a)$ against $\pi(x;q,b)$, there is a bias if a or b is a square modulo q and the other one is not. The non-squares are ahead more often than not in logarithmic density.

Motivated by the importance of the linear independence hypothesis, Kowalski studied in [71] another class of L-functions: that of L-functions of algebraic curves over finite fields. The following entry on Kowalski's blog gives a very accessible introduction to the ideas of that paper: https://blogs.ethz.ch/kowalski/2008/08/14/independence-of-zeros-of-l-functions-over-function-fields/.
The advantage of this setting is that the L-functions are polynomials (so they only have finitely many roots) instead of analytic functions which can have infinitely many zeros, and the Riemann hypothesis has been proved by Deligne for such L-functions. In this article, Kowalski proves that the linear independence between the zeros of the L-function associated with an hyperelliptic curve C is "typically" satisfied among the curves of a certain family. An estimate quantifies how rare are the exceptional curves in the given family whose L-functions fails to satisfy the linear independence hypothesis.

4.3.6. The Hilbert class polynomial

Another polynomial for which the module of additive relations can be determined is the Hilbert class polynomial $g := H_\Delta$, whose roots are the j-invariants of elliptic curves with CM by an imaginary quadratic order $\mathcal{O}$ of given discriminant Δ (see, e.g., [23, § 13, Prop. 13.2]). This means that we consider sums

$$\sum_{E \text{ with CM by } \mathcal{O}} e\Big(\frac{aj(E)}{q}\Big) \tag{4.13}$$

(summing over isomorphism classes of elliptic curves with CM by $\mathcal{O}$) for prime numbers q totally split in the ring class field corresponding to the order $\mathcal{O}$ (which, for $\Delta = -4m$ with $m \geqslant 1$ a fixed squarefree integer, means primes of the form $x^2 + my^2$, see the book of Cox [23] for details). From Proposition 4.30, and Corollary 4.40, we know that the asymptotic distribution of the sums (4.13), as q tends to infinity and a varies in $\mathbf{F}_q$, is governed by the additive relations between the roots of the Hilbert class polynomial (or in other words: the additive relations between j–invariants of elliptic curves with CM by $\mathcal{O}$). In fact, in the next proposition we prove that for all discriminants $\Delta \leqslant -9$, there are no non-trivial additive relations, so that the sums (4.13) equidistribute with respect to a measure which is the law of independent and identically distributed Steinhaus random variables.

Proposition 4.56. *Let Δ be a negative discriminant, that is: a negative integer such that $\Delta \equiv 0, 1 \pmod 4$. Let $\mathcal{O}$ be the unique imaginary quadratic order of discriminant Δ, with class number denoted by h. Let $j(\tau_1), \dots, j(\tau_h)$ be the singular moduli of discriminant Δ, where the imaginary quadratic integers τ_k belong to the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbf{Z})$ on the Poincaré upper half-plane $\mathbf{H}$.*
Then if $\Delta \leqslant -9$, the algebraic integers $j(\tau_1), \dots, j(\tau_h)$ are linearly independent over $\mathbf{Q}$.

Remark 4.57. From the point of view of elliptic curves, the $j(\tau_k)$ are exactly the different j-invariants of elliptic curves with CM by $\mathcal{O}$.

Proof. The proof relies on the following facts[5]:

(a) $\{j(\tau_1), \dots, j(\tau_h)\}$ is a Galois orbit over $\mathbf{Q}$. This comes from the fact that the Hilbert class polynomial H_Δ, which belongs to $\mathbf{Z}[X]$ and is irreducible over $\mathbf{Q}$, equals

$$\prod_{k=1}^{h} (X - j(\tau_k)).$$

See [23, §13] for a proof.

(b) We have an effective estimate of the absolute value of $j(\tau)$ in terms of the imaginary part of τ, due to Bilu, Masser and Zannier. Namely, if $\tau \in \mathbf{H}$ is in the standard fundamental domain, then

$$\Big| |j(\tau)| - e^{2\pi \mathrm{Im}(\tau)} \Big| \leqslant 2079,$$

see [8, Lemma 1].

[5] Many thanks to Emanuele Tron for giving the key ideas of the proof, leaving me only a few details to check.

(c) Finally, for any given negative discriminant, there is a unique so-called *dominant* singular modulus of discriminant Δ, which corresponds to a τ with imaginary part $\sqrt{|\Delta|}/2$, while all others are associated with complex number τ' with imaginary part less than or equal to $\sqrt{|\Delta|}/4$, see [2, Section 3.3]. As a consequence of the estimate above, the dominant singular modulus of discriminant Δ satisfies

$$|j(\tau)| \geqslant e^{\pi\sqrt{|\Delta|}} - 2079,$$

while all the other singular moduli of discriminant Δ satisfy

$$|j(\tau')| \leqslant e^{\pi\frac{\sqrt{|\Delta|}}{2}} + 2079.$$

Thanks to these facts combined with classical estimates for the class number of imaginary quadratic orders, we can now prove Proposition 4.56.

Assume that there exists a non-trivial linear relation over $\mathbf{Q}$:

$$\sum_{k=1}^{h} a_k j(\tau_k) = 0 \tag{4.14}$$

Then up to reordering the τ_k, we may assume that $|a_1| = \max_{1\leqslant k\leqslant h} |a_k|$, and after dividing by a_1, we may assume that $a_1 = 1$ and that for all $k \geqslant 2$ we have $|a_k| \leqslant 1$. Moreover, using the fact that $j(\tau_1)$ is a Galois conjugate over $\mathbf{Q}$ of the dominant singular modulus of discriminant Δ, we may assume that $j(\tau_1)$ is the dominant singular modulus. Then, isolating this term in (4.14) gives:

$$j(\tau_1) = -\sum_{k=2}^{h} a_k j(\tau_k).$$

Taking absolute values and using the estimates from point (c), we get:

$$\begin{aligned} e^{\pi\sqrt{|\Delta|}} - 2079 \leqslant |j(\tau_1)| &= \left|\sum_{k=2}^{h} a_k j(\tau_k)\right| \\ &\leqslant \sum_{k=2}^{h} |j(\tau_k)| \leqslant \left(e^{\pi\frac{\sqrt{|\Delta|}}{2}} + 2079\right) h. \end{aligned}$$

Finally, thanks to Dirichlet's analytic class number formula (see e.g. [19, Proposition 5.3.12] in the case $\Delta < -4$), we have

$$h = \frac{\sqrt{|\Delta|}}{\pi} L\left(1, \left(\frac{\Delta}{-}\right)\right),$$

where $\left(\frac{\Delta}{-}\right)$ is the Kronecker symbol. Besides, the value at 1 of the L-function is classically bounded above by $\log(|\Delta|) + 2$ (using summation by parts, see for instance [52, Chapter 12, Theorem 14.3]). Therefore,

$$e^{\pi\sqrt{|\Delta|}} - 2079 \leqslant \left(e^{\pi\frac{\sqrt{|\Delta|}}{2}} + 2079\right) \frac{\sqrt{|\Delta|}}{\pi} \left(\log(|\Delta|) + 2\right),$$

which is contradictory for all $|\Delta| \geqslant 9$. Thus, there is no non-trivial linear relation over $\mathbf{Q}$ between the singular moduli of a given discriminant $\Delta \leqslant -9$. □

Now let us state the corollary concerning the distribution of sums of type (4.13):

Corollary 4.58. *Fix a negative discriminant $\Delta \neq -3$ and denote by $\mathcal{O}$ the unique imaginary quadratic order of discriminant Δ, and by h its class number. As $q \to \infty$ among the primes totally split in the ring class field corresponding to the order $\mathcal{O}$, the sums*

$$\sum_{E \text{ with CM by } \mathcal{O}} e\left(\frac{aj(E)}{q}\right)$$

parametrized by $a \in \mathbf{F}_q$ become equidistributed in $\mathbf{C}$ with respect to the measure μ which is the law of the sum $X_1 + \cdots + X_h$ of h independent random variables, each uniformly distributed on the unit circle.

Proof. When $\Delta \leqslant -9$, Proposition 4.56 shows that the group of additive relations of the polynomial $g = H_\Delta$ is trivial. Therefore, its orthogonal H_g is the full group of functions from Z_g to $\mathbf{S}^1$ and the uniform distribution result is a particular case of Corollary 4.40. In the remaining cases, the class number is equal to 1, and the proof follows from the fact that the unique j-invariant of elliptic curve of discriminant Δ is a non-zero integer, as shown in the tables of [23, §12, section C]. □

Remark 4.59. In the case $\Delta = -3$, we have $j(E) = 0$ for the unique class of isomorphism of elliptic curves with CM by $\mathcal{O}$, so that the sums above are always equal to 1.

4.4. Allowing more general Laurent polynomials instead of ax

In this section, we generalize the previous equidistribution results regarding sums of the type

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{ax}{q}\right)$$

to allow more general Laurent polynomials inside the exponentials, just as we did in Chapter 2. In particular, this will allow us to obtain equidistribution results for

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{a(x+x^{-1})}{q}\right) \quad \text{or} \quad \sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{ax+bx^{-1}}{q}\right).$$

Once again, this relies on the uniform distribution of certain unitary random variables inside a subgroup of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ related to the relations between the roots of the polynomial g. Then, uniform distribution of the corresponding exponential sums follows immediately from composition with the linear form σ.

Proposition 4.60. *Let $v \in \mathbf{Z}[X, X^{-1}]$ be a non-constant Laurent polynomial. Assume that $0 \notin \mathrm{Z}_g$. Define random variables $W_{\mathfrak{p}^n}$ on $\mathbf{O}_g/\mathfrak{p}^n$ for $\mathfrak{p} \in \mathcal{S}_g$ which divides none of the roots of g and $n \geqslant 1$, with values in $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$, by*

$$W_{\mathfrak{p}^n}(a)(x) = e\Big(\frac{\tau_{\mathfrak{p}^n}(av(\varpi_{\mathfrak{p}^n}(x)))}{\|\mathfrak{p}\|^n}\Big).$$

The random variables $W_{\mathfrak{p}^n}$ converge in law as $\|\mathfrak{p}\|^n \to +\infty$ to the random function $W \colon \mathrm{Z}_g \to \mathbf{S}^1$ such that W is uniformly distributed on the subgroup orthogonal to the abelian group $\mathrm{R}_{g,v} \subset \mathrm{C}(\mathrm{Z}_g; \mathbf{Z})$ of additive relations between components of $(v(x))_{x \in \mathrm{Z}_g}$, namely

$$\mathrm{R}_{g,v} = \{\alpha \colon \mathrm{Z}_g \to \mathbf{Z} \mid \sum_{x \in \mathrm{Z}_g} \alpha(x)v(x) = 0\}.$$

Remark 4.61. Let us give some precisions about the condition "which divides none of the roots of g" in the assumptions above. For all $x \in \mathrm{Z}_g$, the ideal $x\mathbf{O}_g$ is a non-zero ideal of the Dedekind ring $\mathbf{O}_g$ (thanks to the assumption that $0 \notin \mathrm{Z}_g$). As such, it can be written as a finite product

$$x\mathbf{O}_g = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$$

of powers of prime ideals of $\mathbf{O}_g$, where the product is indexed by the (finitely many) prime ideals containing $x\mathbf{O}_g$. We say that $\mathfrak{p}$ *divides* x when $\mathfrak{p}$ appears in the factorization of the ideal $x\mathbf{O}_g$. Moreover, let us stress that the fact that $\mathfrak{p} \in \mathcal{S}_g$ does not ensure that $\mathfrak{p}$ divides none of the roots of g, so this extra condition is not superfluous. Indeed, if one considers for instance the polynomial $g := X^2+X+3$, then $\mathrm{disc}(g) = -11$, so $q = 3$ is a prime number which does not divide the discriminant of g. Therefore, 3 is totally split in K_g if and only if g splits into distinct linear factors in $\mathbf{F}_3$. But

$$g(X) \equiv X(X+1) \,(\mathrm{mod}\, 3)$$

So 0 is one of the roots of g modulo 3, which means that if $\mathfrak{p}$ is an ideal of K_g lying above the prime number 3, then one of the roots of g belongs to $\mathfrak{p}$ (although $\mathfrak{p} \in \mathcal{S}_g$ because it lies above 3, which is totally split!)

Remark 4.62. The assumptions that $\mathfrak{p}$ divides none of the roots of g is used in the proof, but is is even necessary to ensure that our random variables are well-defined. Indeed, in order to be able to write $v(\varpi_{\mathfrak{p}^n}(x))$, for a Laurent polynomial v, we need $\varpi_{\mathfrak{p}^n}(x)$ to be invertible in the ring $\mathbf{O}_g/\mathfrak{p}^n$. This is guaranteed by the fact that for all $x \in \mathrm{Z}_g$, we have that $x \notin \mathfrak{p}$. Indeed, $\mathbf{O}_g/\mathfrak{p}^n$ is a local ring with unique maximal ideal $\mathfrak{p}/\mathfrak{p}^n$ (because ideals of $\mathbf{O}_g/\mathfrak{p}^n$ correspond to ideals of $\mathbf{O}_g$ containing $\mathfrak{p}^n$, which are $\mathfrak{p}^n \subset \mathfrak{p}^{n-1} \subset \cdots \subset \mathfrak{p} \subset \mathbf{O}_g$), and in a local ring, all the elements which do not belong to the maximal ideal are units.

This small difficulty on the possibility of some primes dividing a root of g justifies the writing of the proof of Proposition 4.60, as it is not a completely immediate adaptation of the proof of Proposition 4.30. Indeed, the issue is that

$$S_{\alpha,v} := \sum_{x \in \mathrm{Z}_g} \alpha(x) v(x)$$

need not belong to $\mathbf{O}_g$ (it is an element of K_g, but the fact that we invert roots of the polynomial g in order to evaluate $v(x)$ can give us an element which no longer belongs to $\mathbf{O}_g$). Therefore, we need to be a little bit more cautious when applying the homomorphism properties of $\varpi_{\mathfrak{p}^n} \colon \mathbf{O}_g \to \mathbf{O}_g/\mathfrak{p}^n$, since it is only defined on $\mathbf{O}_g$. The key argument is the following:

Lemma 4.63. *Let $\mathfrak{p} \subset \mathbf{O}_g$ be an ideal which does not contain any root of g and let P denote the product*

$$\prod_{y \in \mathrm{Z}_g} y^m,$$

where $-m$ is the valuation of the Laurent polynomial v fo Proposition 4.60. Then $PS_{\alpha,v} \in \mathbf{O}_g$ and for all $n \geqslant 1$, we have

$$\varpi_{\mathfrak{p}^n}(PS_{\alpha,v}) = \sum_{x \in \mathrm{Z}_g} \alpha(x) v(\varpi_{\mathfrak{p}^n}(x)).$$

Proof. Indeed, if we write

$$v(X) = \sum_{i=-m}^{N} a_i X^i$$

then

$$\begin{aligned}
\varpi_{\mathfrak{p}^n}(PS_{\alpha,v}) &= \varpi_{\mathfrak{p}^n}\left(P \sum_{x \in \mathrm{Z}_g} \alpha(x) \sum_{i=-m}^{N} a_i x^i \right) \\
&= \varpi_{\mathfrak{p}^n}\left(\sum_{x \in \mathrm{Z}_g} \alpha(x) \sum_{i=-m}^{N} a_i \left(\prod_{y \in \mathrm{Z}_g \setminus \{x\}} y^m \right) x^{m+i} \right) \\
&= \sum_{x \in \mathrm{Z}_g} \alpha(x) \varpi_{\mathfrak{p}^n}\left(\prod_{y \in \mathrm{Z}_g \setminus \{x\}} y^m \right) \sum_{i=-m}^{N} a_i \varpi_{\mathfrak{p}^n}\left(x^{m+i}\right)
\end{aligned}$$

Next, we use the fact that for all $-m \leqslant i \leqslant N$, we have $\varpi_{\mathfrak{p}^n}(x^{m+i}) = \varpi_{\mathfrak{p}^n}(x)^{m+i}$ because $m+i \geqslant 0$ and $\varpi_{\mathfrak{p}^n}$ is a ring homomorphism. Now, $\varpi_{\mathfrak{p}^n}(x)^{m+i} = \varpi_{\mathfrak{p}^n}(x)^m \varpi_{\mathfrak{p}^n}(x)^i = \varpi_{\mathfrak{p}^n}(x^m)\varpi_{\mathfrak{p}^n}(x)^i$ and the right-hand side makes sense even for negative values of i because $\varpi_{\mathfrak{p}}(x) \in (\mathbf{O}_g/\mathfrak{p}^n)^\times$, thanks to the assumption that $\mathfrak{p}$ does not divide $x\mathbf{O}_g$. Therefore,

$$\begin{aligned}
\varpi_{\mathfrak{p}^n}(PS_{\alpha,v}) &= \sum_{x \in \mathrm{Z}_g} \alpha(x) \underbrace{\varpi_{\mathfrak{p}^n}\left(\prod_{y \in \mathrm{Z}_g \setminus \{x\}} y^m \right) \varpi_{\mathfrak{p}^n}(x^m)}_{\varpi_{\mathfrak{p}^n}(P)} \underbrace{\sum_{i=-m}^{N} a_i \varpi_{\mathfrak{p}^n}\left(x\right)^i}_{v(\varpi_{\mathfrak{p}^n}(x))} \\
&= \varpi_{\mathfrak{p}^n}(P) \sum_{x \in \mathrm{Z}_g} \alpha(x) v(\varpi_{\mathfrak{p}^n}(x)).
\end{aligned}$$

□

Proof of Proposition 4.60.

- Let us first prove that the random variable $W_{\mathfrak{p}^n}$ takes values in $\mathrm{R}_{g,v}^{\perp}$. We let $a \in \mathbf{O}_g/\mathfrak{p}^n$ and we take $\alpha \in \mathrm{R}_{g,v}$. We want to prove that

$$\eta_\alpha(W_{\mathfrak{p}^n}(a)) = 1.$$

But we have

$$\begin{aligned}\eta_\alpha(W_{\mathfrak{p}^n}(a)) &= \prod_{x\in \mathrm{Z}_g} W_{\mathfrak{p}^n}(a)(x)^{\alpha(x)} \\ &= e\left(\frac{\tau_{\mathfrak{p}^n}(a)}{\|\mathfrak{p}\|^n}\tau_{\mathfrak{p}^n}\left(\sum_{x\in \mathrm{Z}_g}\alpha(x)v(\varpi_{\mathfrak{p}^n}(x))\right)\right)\end{aligned}$$

Now thanks to Lemma 4.63 we have that

$$\sum_{x\in \mathrm{Z}_g}\alpha(x)v(\varpi_{\mathfrak{p}^n}(x)) = \varpi_{\mathfrak{p}^n}(PS_{\alpha,v})$$

and $S_{\alpha,v} = 0$ since $\alpha \in \mathrm{R}_{g,v}$. This gives the conclusion.

- Now, let us prove the convergence in law of the random variables $W_{\mathfrak{p}^n}$. We let η_α be a non-trivial character of $\mathrm{R}_{g,v}^{\perp}$, which means that $\alpha \notin \mathrm{R}_{g,v}$, and we want to prove that

$$\mathbb{E}\left(\eta_\alpha(W_{\mathfrak{p}^n})\right) \underset{\|\mathfrak{p}\|^n\to+\infty}{\longrightarrow} 0.$$

First, we write

$$\begin{aligned}\mathbb{E}\left(\eta_\alpha(W_{\mathfrak{p}^n})\right) &= \frac{1}{\|\mathfrak{p}\|^n}\sum_{a\in\mathbf{O}_g/\mathfrak{p}^n}\eta_\alpha(W_{\mathfrak{p}^n}(a)) \\ &= \frac{1}{\|\mathfrak{p}\|^n}\sum_{a\in\mathbf{O}_g/\mathfrak{p}^n} e\left(\frac{\tau_{\mathfrak{p}^n}(a)}{\|\mathfrak{p}\|^n}\tau_{\mathfrak{p}^n}\left(\sum_{x\in \mathrm{Z}_g}\alpha(x)v(\varpi_{\mathfrak{p}^n}(x))\right)\right)\end{aligned}$$

Next, we use again Lemma 4.63, which tells us that

$$\sum_{x\in \mathrm{Z}_g}\alpha(x)v(\varpi_{\mathfrak{p}}(x)) = \varpi_{\mathfrak{p}}(PS_{\alpha,v})$$

But now, $S_{\alpha,v} \neq 0$ thanks to the assumption that $\alpha \notin \mathrm{R}_{g,v}$, so that $PS_{\alpha,v} \neq 0$. Thus, $\mathrm{N}_{K_g/\mathbf{Q}}(PS_{\alpha,v})$ is a non-zero integer, and if $\varpi_{\mathfrak{p}^n}(PS_{\alpha,v}) = 0$ then $\|\mathfrak{p}\|^n$ divides it, so in particular $\|\mathfrak{p}\|^n \leqslant \mathrm{N}_{K_g/\mathbf{Q}}(PS_{\alpha,v})$. Therefore, as soon as $\|\mathfrak{p}\|^n > \mathrm{N}_{K_g/\mathbf{Q}}(PS_{\alpha,v})$, we have $\varpi_{\mathfrak{p}^n}(PS_{\alpha,v}) \neq 0$, hence $\sum_{x\in \mathrm{Z}_g}\alpha(x)v(\varpi_{\mathfrak{p}^n}(x)) \neq 0$, so that $\mathbb{E}\left(\eta_\alpha(W_{\mathfrak{p}^n})\right) = 0$ by orthogonality of characters.

□

For instance, if $v(x) = x + x^{-1}$, we have that W is uniformly distributed in the orthogonal of the group

$$\mathrm{R}_{g,v} = \left\{\alpha\colon \mathrm{Z}_g \to \mathbf{Z} \;\middle|\; \sum_{x\in \mathrm{Z}_g}\alpha(x)\left(x+\frac{1}{x}\right) = 0\right\}.$$

Corollary 4.64. *For q totally split in K_g and not dividing any root of g nor its discriminant, we have that the sums*

$$\sum_{x\in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{a(x+x^{-1})}{q}\right)$$

parametrized by $a \in \mathbf{F}_q$ become equidistributed with respect to a measure which is the law of $\sigma(W)$, with W as above.

Let us now turn our attention to the suitable setting to handle sums of the form

$$\sum_{x\in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{ax+bx^{-1}}{q}\right).$$

Proposition 4.65. *Let $k \geqslant 1$ be an integer and let $\mathbf{m} = (m_1, \dots, m_k) \in \mathbf{Z}^k$. For $\mathfrak{p} \in \mathcal{S}_g$ dividing none of the roots of g, and $n \geqslant 1$, define random variables $Y_{\mathfrak{p}^n}$ on the space $(\mathbf{O}_g/\mathfrak{p}^n)^k$ with uniform probability measure, with values in $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$, by*

$$Y_{\mathfrak{p}^n}(a_1, \dots, a_k)(x) = e\left(\frac{\tau_{\mathfrak{p}^n}\left(a_1\varpi_{\mathfrak{p}^n}(x)^{m_1} + \cdots + a_k\varpi_{\mathfrak{p}^n}(x)^{m_k}\right)}{\|\mathfrak{p}\|^n}\right).$$

The random variables $Y_{\mathfrak{p}^n}$ converge in law as $\|\mathfrak{p}\|^n \to +\infty$ to the random function $Y\colon \mathrm{Z}_g \to \mathbf{S}^1$ such that Y is uniformly distributed on the subgroup orthogonal to the abelian group

$$\mathrm{R}_{g,\mathbf{m}} := \{\alpha\colon \mathrm{Z}_g \to \mathbf{Z} \mid \sum_{x\in \mathrm{Z}_g} \alpha(x)x^{m_j} = 0 \text{ for } 1 \leqslant j \leqslant k\}$$

of common additive relations between powers of elements of Z_g.

Proof. For $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$, a computation shows that

$$\mathbb{E}(\eta_\alpha(Y_{\mathfrak{p}^n})) = \prod_{j=1}^{k} \frac{1}{\|\mathfrak{p}\|^n} \sum_{a_j\in \mathbf{O}_g/\mathfrak{p}^n} e\left(\frac{\tau_{\mathfrak{p}^n}(a_j)}{\|\mathfrak{p}\|^n}\tau_{\mathfrak{p}^n}\left(\sum_{x\in \mathrm{Z}_g} \alpha(x)\varpi_{\mathfrak{p}^n}(x)^{m_j}\right)\right)$$

Now thanks to the assumption that $\mathfrak{p}$ divides none of the roots of g, Lemma 4.63 applied to the Laurent polynomial X^{m_j} shows that $\sum_{x\in \mathrm{Z}_g} \alpha(x)\varpi_{\mathfrak{p}^n}(x)^{m_j}$ equals zero if $\sum_{x\in \mathrm{Z}_g} \alpha(x)x^{m_j} = 0$, which is the case for all j if we assume that $\alpha \in \mathrm{R}_{g,\mathbf{m}}$. This proves that the random variables $Y_{\mathfrak{p}^n}$ take values in the subgroup $\mathrm{R}_{g,\mathbf{m}}^{\perp}$ of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$.
On the other hand, if $\alpha \notin \mathrm{R}_{g,\mathbf{m}}$, then there exists a $j \in \{1, \dots, k\}$ such that $\sum_{x\in \mathrm{Z}_g} \alpha(x)x^{m_j} \neq 0$, and this implies that $\sum_{x\in \mathrm{Z}_g} \alpha(x)\varpi_{\mathfrak{p}^n}(x)^{m_j}$ is non-zero as soon as $\|\mathfrak{p}\|^n$ is sufficiently large. The factor corresponding to j in $\mathbb{E}(\eta_\alpha(Y_{\mathfrak{p}^n})$ is then equal to zero for all $\|\mathfrak{p}\|^n$ sufficiently large. This proves the desired uniform distribution. □

Example 4.66. Consider the case of $g = X^d - 1$ and the sums

$$\sum_{x\in \mu_d(\mathbf{F}_q)} e\left(\frac{a(x+x^{-1})}{q}\right) \tag{4.15}$$

with a varying in $\mathbf{F}_q$, and

$$\sum_{x\in \mu_d(\mathbf{F}_q)} e\left(\frac{ax+bx^{-1}}{q}\right), \tag{4.16}$$

with a and b varying in $\mathbf{F}_q$ for q totally split in K_g. Both satisfy equidistribution, but in general with different measures. For (4.15), we need to determine the functions α satisfying the relation

$$\sum_{x\in \boldsymbol{\mu}_d} \alpha(x)(x+x^{-1}) = 0,$$

and for (4.16), we need to solve

$$\sum_{x\in \boldsymbol{\mu}_d} \alpha(x)x = \sum_{x\in \boldsymbol{\mu}_d} \alpha(x)x^{-1} = 0.$$

This last case gives the same relations as in the end of section 4.1.4, since the second sum above is the complex-conjugate of the first. For instance, in the case $d = 3$, this means that the sums (4.16) will become equidistributed with respect to the measure on $\mathbf{C}$ which is the pushforward measure via

$$\begin{array}{ccc} \mathbf{S}^1 \times \mathbf{S}^1 & \to & \mathbf{C} \\ (y_1, y_2) & \mapsto & y_1 + y_2 + \frac{1}{y_1 y_2} \end{array}$$

of the uniform measure on $\mathbf{S}^1 \times \mathbf{S}^1$. This is illustrated in Figure 4.3 (b), since the image of the above map is the closed region delimited by a 3-cusp hypocycloid.
For (4.15), on the other hand, the relation is equivalent to

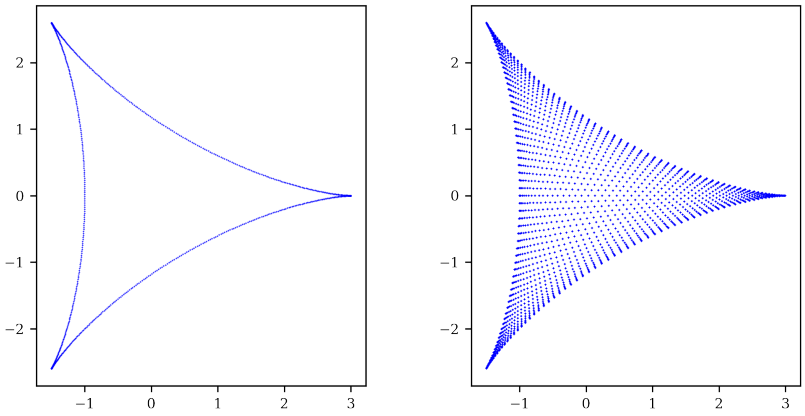
$$\sum_{x \in \boldsymbol{\mu}_d} (\alpha(x) + \alpha(x^{-1}))x = 0,$$

which means that $\beta \colon x \mapsto \alpha(x) + \alpha(x^{-1})$ belongs to the module of additive relations of the polynomial $X^d - 1$. If $d = \ell$ is a prime number, for instance, this means that β is constant.

In the case $\ell = 3$, the group $R_{X^{\ell}-1, x+x^{-1}}$ is generated by the constant function 1 and (say) the function on roots of unity of order ℓ which gives the sign of the imaginary part (with the imaginary part 0 mapped to 0). This implies that the sums (4.15) become equidistributed in the image of the map

$$\begin{array}{ccc} \mathbf{S}^1 & \to & \mathbf{C} \\ y & \mapsto & 2y + \frac{1}{y^2} \end{array}$$

with respect to the pushforward measure of the Haar measure on $\mathbf{S}^1$. Since the image of this map is precisely the 3-cusp hypocycloid (see Definition 2.3) this explains the picture obtained in Figure 4.3 (a).



(a) The sums of type (4.15) for $d = 3$, $q = 811$, and a varying in $\mathbf{F}_q$.

(b) The sums of type (4.16) for $d = 3$, $q = 109$, and a and b varying in $\mathbf{F}_q$.

Figure 4.3: Comparison between the regions of equidistribution for sums of type (4.15) and sums of type (4.16).

4.A. Duality of compact abelian groups and Weyl's criterion

Duality of compact abelian groups. Let G be a compact abelian group (Theorem 4.68 and Proposition 4.70 hold more generally for locally compact abelian groups, but we only need the compact case in the applications of this chapter).

Definition 4.67. *A character of G is a continuous group homomorphim from G to $\mathbf{S}^1$ (a more precise name would be "*continuous unitary character*"). We denote by $\widehat{G}$ the group of characters of G. It is called the dual of G.*

If H is a subgroup of G, then we can always restrict to H a character of G, and this gives an element of $\widehat{H}$. A consequence of Pontryagin duality is the fact that when H is closed, all characters of H are of this form!

Theorem 4.68 ([94, Theorem 2.1.4])**.** *If H be a closed subgroup of G then the restriction homomorphism*

$$\begin{array}{ccc} \widehat{G} & \to & \widehat{H} \\ \chi & \mapsto & \chi_{|H} \end{array}$$

is surjective. In other words, any character of H can be extended to a character defined on all G.

As in linear algebra, we can use the dual to define the *orthogonal* or *annihilator* of a subset of G as the set of characters which are trivial on it. There is also the dual notion of orthogonal of a subset of $\widehat{G}$, and we gather the two definitions below:

Definition 4.69 (Orthogonal of a subset)**.**

- *If A is a subset of G, we denote by $A^\perp := \left\{\chi \in \widehat{G};\ \forall x \in A, \chi(x) = 1\right\}$.*
- *If B is a subset of $\widehat{G}$, we denote by $B^\perp := \{x \in G;\ \forall \chi \in B, \chi(x) = 1\}$.*

Another consequence of Pontryagin duality is the following fact, which is reminiscent of what happens in finite dimensional vector spaces.

Proposition 4.70 ([94, Lemma 2.1.3])**.** *If H is a closed subgroup of G then $\left(H^\perp\right)^\perp = H$.*

Equidistribution and Weyl's criterion. If we have a sequence (X_n) of random variables defined on some probability spaces $(\Omega_n, \mathscr{F}_n, \mathbb{P}_n)$ and with values in the compact abelian group G, we say that the sequence converges in law to a uniformly distributed random variable on G if the distribution of X_n (which is the pushforward measure of $\mathbb{P}_n$ via X_n) converges weakly to the probability Haar measure μ_G on G.
In other words

$$X_n \xrightarrow{\text{law}} \mathcal{U}(G) \iff \int_{\Omega_n} f(X_n(\omega))\mathrm{d}\mathbb{P}_n(\omega) \underset{n\to\infty}{\longrightarrow} \int_G f(x)\mathrm{d}\mu_G(x)$$

for all continuous map $f\colon G \to \mathbf{C}$. Weyl's criterion states that it suffices to check this convergence for maps f which are characters of G. We state it below in the form of [75, Theorem B.6.3]:

Theorem 4.71 (Weyl's criterion)**.** *Let G be a compact abelian group. A sequence (X_n) of G-valued random variables converges in law to a uniformly distributed random variable on G if and only if for any non trivial character χ of G,*

$$\mathbb{E}(\chi(X_n)) \underset{n\to\infty}{\longrightarrow} 0.$$

Finally, the group $(\mathbf{S}^1)^d$ and its closed subgroups will be of particular interest for us, so we need a precise description of their characters.

Proposition 4.72 (Characters of $(\mathbf{S}^1)^d$)**.** *Let G be the compact group $(\mathbf{S}^1)^d$. The characters of G are exactly the maps*

$$\begin{array}{rccc} \chi_{\mathbf{m}} & : & G & \to & \mathbf{S}^1 \\ & & (z_1, \dots, z_d) & \mapsto & z_1^{m_1} \cdots z_d^{m_d} \end{array}$$

for $\mathbf{m} = (m_1, \dots, m_d) \in \mathbf{Z}^d$. Moreover, $\chi_{\mathbf{m}}$ is the trivial character if and only if $\mathbf{m} = (0, \dots, 0)$.

4.B. On ramification in number fields

Given a number field K (that is: a finite extension of the field $\mathbf{Q}$), we denote by $\mathcal{O}_K$ its *ring of integers*. By definition, it is the set

$$\{x \in K \mid \text{there exists a monic polynomial } P \in \mathbf{Z}[X] \text{ such that } P(x) = 0\}.$$

It can be shown that this subset is actually a subring of K. In general, this ring $\mathcal{O}_K$ is not a unique factorization domain, but it is always a *Dedekind ring*. This implies that even though unique factorization might fail at the level of elements of $\mathcal{O}_K$, there is an essentially unique factorization at the level of ideals of $\mathcal{O}_K$. Namely, for any non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$, there exist a finite set of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and positive integers $\alpha_1, \ldots, \alpha_r$ such that

$$\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \ldots \mathfrak{p}_r^{\alpha_r}.$$

This factorization is unique up to permutation of the $\mathfrak{p}_i$. The prime ideals which appear in this decomposition are precisely those which contain $\mathfrak{a}$. In particular, if p is a prime number in $\mathbf{Z}$, the ideal generated by p in $\mathcal{O}_K$ can be decomposed as a product of the form above. If $p\mathcal{O}_K \subseteq \mathfrak{p}$ (i.e. if $\mathfrak{p}$ appears at a non-zero power in the factorization of $p\mathcal{O}_K$ as a product of prime ideals), we say that $\mathfrak{p}$ *lies above* p, or that $\mathfrak{p}$ *divides* p and we denote this condition by $\mathfrak{p} \mid p$. We denote by $e_\mathfrak{p}$ the power at which the ideal $\mathfrak{p}$ appears in the factorization. With these notations, we have

$$p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e_\mathfrak{p}}.$$

Definition 4.73. *The integer $e_\mathfrak{p} \in \mathbf{Z}_{>0}$ is called the ramification index of p at $\mathfrak{p}$.*

When $\mathfrak{p} \mid p$, we have the following natural ring homomorphisms:

$$\mathbf{Z} \hookrightarrow \mathcal{O}_K \to \kappa(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$$

The composition factorizes through $\mathbf{Z}/p\mathbf{Z}$ and gives rise to the so-called *residual extension*:

$$\mathbf{F}_p \hookrightarrow \kappa(\mathfrak{p})$$

.

Definition 4.74. *The field $\kappa(\mathfrak{p})$ is called the residue field at $\mathfrak{p}$, and we denote by $f_\mathfrak{p}$ the residual degree, which is defined as $[\kappa(\mathfrak{p}) : \mathbf{F}_p]$ (the degree of the extension of residue fields).*

Finally, let us introduce some terminology regarding the numbers $e_\mathfrak{p}$ and $f_\mathfrak{p}$.

Definition 4.75.

- *If $e_\mathfrak{p} = 1$, we say that the extension $K/\mathbf{Q}$ is unramified at $\mathfrak{p}$, or that $\mathfrak{p}$ is unramified.*
- *If for all $\mathfrak{p} \mid p$, the extension $K/\mathbf{Q}$ is unramified at $\mathfrak{p}$, we say that the prime p is unramified.*
- *If for all $\mathfrak{p} \mid p$ we have $e_\mathfrak{p} = f_\mathfrak{p} = 1$, we say that p is totally split in K.*

An important result to have in mind is that when the extension $K/\mathbf{Q}$ is Galois, $\mathrm{Gal}(K/\mathbf{Q})$ acts transitively on the set of prime ideals $\mathfrak{p}$ dividing a given prime p. A consequence of this fact is that the numbers $e_\mathfrak{p}$ and $f_\mathfrak{p}$ do not depend on $\mathfrak{p}$, they are the same for *any* ideal $\mathfrak{p} \mid p$. As a consequence, in the Galois case, a prime p is totally split in K if and only if there exists a prime ideal $\mathfrak{p}$ dividing p such that $e_\mathfrak{p} = f_\mathfrak{p} = 1$.

Chapter 5

Discrepancy estimates

The aim of this chapter is to study the speed of the convergence in law of the random variables $U_{\mathfrak{p}}$ introduced in the previous chapter. In order to do this, we need to generalize the Erdös-Turán-Koksma inequality to *closed subgroups* of $(\mathbf{S}^1)^k$, since the random variables $U_{\mathfrak{p}}$ take values in a closed subgroup of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1) \simeq (\mathbf{S}^1)^{\deg g}$. Using the well-known classification of such subgroups, we propose a definition of the φ-discrepancy of a sequence which depends on the choice of an isomorphism φ with $(\mathbf{R}/\mathbf{Z})^d \oplus F$, where F is a finite abelian group. Then we prove that this discrepancy decays at least as fast as $\|\mathfrak{p}\|^{-\frac{1}{[K_g:\mathbf{Q}]}}$.

Contents

5.1. Erdös-Turán-Koksma inequality (classical form)

Let $(z_n)_{n\geqslant 1}$ be a sequence of elements of $\mathbb{T}^k = (\mathbf{R}/\mathbf{Z})^k$. We say that this sequence becomes equidistributed in $\mathbb{T}^k$ if for any continuous function $f\colon \mathbb{T}^k \to \mathbf{C}$, we have

$$\frac{1}{N}\sum_{n=1}^{N} f(z_n) \underset{N\to+\infty}{\longrightarrow} \int_{\mathbb{T}^k} f \mathrm{d}\lambda_k, \tag{5.1}$$

where λ_k denotes the probability Haar measure on the compact abelian group $\mathbb{T}^k$. Equivalently, (z_n) becomes equidistributed in $\mathbb{T}^k$ if for any "rectangle" $I := [a_1, b_1] \times \cdots \times [a_k, b_k] \subseteq (\mathbf{R}/\mathbf{Z})^k$ (with $0 \leqslant b_i - a_i \leqslant 1$), the right proportion of the terms (z_n) falls inside the rectangle (asymptotically), that is:

$$\frac{\#\{1 \leqslant n \leqslant N,\ z_n \in I\}}{N} \underset{N\to+\infty}{\longrightarrow} \prod_{j=1}^{k} (b_j - a_j)$$

The celebrated Weyl's criterion asserts that one can check the convergence (5.1) only on a certain class of functions: the trigonometric polynomials. In other words, (z_n) becomes equidistributed in $\mathbb{T}^k$ if and only if for all $\mathbf{m} \in \mathbf{Z}^k \setminus \{0\}$,

$$\frac{1}{N}\sum_{n=1}^{N} e(\mathbf{m}\cdot z_n) \underset{N\to+\infty}{\longrightarrow} 0.$$

We call the sums on the left-hand side the Weyl sums associated with this equidistribution problem.

Notation: in the remainder of this chapter, $\chi_{\mathbf{m}}$ denotes the character $e(\mathbf{m}\cdot(-))$ of $\mathbb{T}^k$. The dimension k will always be clear in the context.

The Erdös-Turán-Koksma inequality is a theorem which gives a control of the discrepancy of a sequence in $\mathbb{T}^k$ in terms of the Weyl sums. It allows one to deduce a "rate of equidistribution" from estimates on the decay of the absolute value of the Weyl sums. Before stating it, let us recall the definition of the discrepancy in this context.

Definition 5.1. *If $z = (z_n)_{n\geqslant 1}$ is a sequence of elements of $\mathbb{T}^k$, we define its discrepancy at the rank N as*

$$D_N(z) := \sup_{I\in\mathscr{I}_k} \left| \frac{\#\{1\leqslant n\leqslant N,\ z_n\in I\}}{N} - \lambda_k(I)\right|$$

where $\mathscr{I}_k$ denotes the set of rectangles $I = [a_1,b_1]\times\cdots\times[a_k,b_k]$ of $\mathbb{T}^k$.

We can now state the Erdös-Turán-Koksma inequality:

Theorem 5.2 ([29, Theorem 1.21])**.** *Let $z = (z_n)_{n\geqslant 1}$ be a sequence of elements of $\mathbb{T}^k$. Then for all $H \geqslant 1$ and all $N \geqslant 1$,*

$$D_N(z) \leqslant \left(\frac{3}{2}\right)^k \left(\frac{2}{H+1} + \sum_{\substack{\mathbf{m}\in\mathbf{Z}^k \\ 0<\|\mathbf{m}\|_\infty\leqslant H}} \frac{1}{r(\mathbf{m})}\left|\frac{1}{N}\sum_{n=1}^{N} e(\mathbf{m}\cdot z_n)\right| \right)$$

where $r(\mathbf{m}) = \prod_{j=1}^{k}\max(1,|m_j|)$ for $\mathbf{m} = (m_1,\dots,m_k)\in\mathbf{Z}^k$.

The main aim of this chapter is to prove an extension of this result which gives a control of the discrepancy of a sequence of elements in a closed subgroup $G\subseteq\mathbb{T}^k$ in terms of the Weyl sums, that is sums of the form

$$\frac{1}{N}\sum_{n=1}^{N}\chi(z_n)$$

where χ is a character of G. Our first step consists in the study of the structure of such closed subgroups. It is actually quite well understood, and we recall some facts in the next section, borrowing from [10].

5.2. Generalization to closed subgroups of $\mathbb{T}^k$

5.2.1. Structure of closed subgroups of $\mathbb{T}^k$

If G is a closed subgroup of $\mathbb{T}^k$, then it corresponds (via the canonical map $\mathbf{R}^k\to\mathbf{R}^k/\mathbf{Z}^k$) to a closed subgroup of $\mathbf{R}^k$ containing $\mathbf{Z}^k$, which we denote by G'. Thanks to [10, Chapter 7], there exists a basis $a_1,\dots,a_k$ of $\mathbf{R}^k$ such that

$$\begin{cases} \mathbf{Z}^k = \bigoplus_{i=1}^{k}\mathbf{Z}a_i \\ G' = \left(\bigoplus_{i=1}^{d}\mathbf{R}a_i\right)\oplus\left(\bigoplus_{i=d+1}^{k}\mathbf{Z}a_i'\right), \end{cases}$$

where each a_i' is equal to $\frac{1}{m_i}a_i$ for some integers m_i (the m_i are the invariant factors of some $\mathbf{Z}$-module, dual in some sense of the module G'). If we denote by $\mathcal{B}$ the basis $(a_1, \dots, a_d, a_{d+1}', \dots, a_k')$ of $\mathbf{R}^k$ and by $P := P_{\mathcal{B},\mathcal{C}}$ the change-of-basis matrix which takes the coordinates of a vector $x \in \mathbf{R}^k$ in the canonical basis and returns the vector of its coordinates in the basis $\mathcal{B}$, then P induces an isomorphism

$$\varphi_P \colon G \to \mathbb{T}^d \oplus \underbrace{\left(\bigoplus_{i=d+1}^{k} \mathbf{Z}/m_i\mathbf{Z} \right)}_{=:F} =: \mathbb{T}^d \oplus F. \tag{5.2}$$

Explicitly, we start from an element $\overline{x} \in G$, we lift it to an element x in $\mathbf{R}^k$, and we denote by $(x_1, \dots, x_k)$ its coordinates in the canonical basis of $\mathbf{R}^k$, then we multiply that vector by the matrix P, to obtain the vector $(y_1, \dots, y_k)$ made of the coordinates of x in the basis $\mathcal{B}$. Now, thanks to the explicit description of G' in the basis $\mathcal{B}$, we know that $y_1, \dots, y_d$ are real numbers and that $y_{d+1}, \dots, y_k$ are integers. Then we reduce the first d coordinates modulo 1, and the following coordinates y_i each modulo m_i. This describes the isomorphism φ_P.

Sections 5.2.2 and 5.2.3 of this chapter are devoted to proving Theorem 5.13, which generalizes Theorem 5.2 to the case of the group $\mathbb{T}^d \oplus F$, where F is any finite abelian group.

This will allow us to deduce an inequality of Erdös-Turán-Koksma type for sequences taking values inside any closed subgroup G of $\mathbb{T}^k$ (the inequality will depend in a relatively well-understood way of the choice of an isomorphism $G \to \mathbb{T}^d \oplus F$ as constructed in (5.2)).

Before proving Theorem 5.13, we need to define some convolution kernels and to study their properties from the point of view of Fourier analysis.

5.2.2. Construction of convolution kernels via Fourier analysis

We will take the following convention for the Fourier transform on $\mathbf{R}$: if $f \in L^1(\mathbf{R})$, we define its Fourier transform as

$$\widehat{f} \colon x \mapsto \int_{\mathbf{R}} f(t)e(-xt)\mathrm{d}t.$$

With this convention, the Fourier inversion formula takes the following form:

Proposition 5.3. *If $f \in L^1(\mathbf{R})$ and $\widehat{f} \in L^1(\mathbf{R})$, then*

$$f(t) = \widehat{\widehat{f}}(-t) = \int_{\mathbf{R}} \widehat{f}(x)e(tx)\mathrm{d}x.$$

In [29, section 1.2.2], the following function is introduced

$$H(z) := \left(\frac{\sin(\pi z)}{\pi}\right)^2 \left(\sum_{n \in \mathbf{Z}} \frac{\mathrm{sgn}(n)}{(z-n)^2} + \frac{2}{z} \right), \tag{5.3}$$

and the authors set

$$J(z) := \frac{1}{2}H'(z).$$

This quite complicated definition of J is useful in the proofs, but only the properties of $\widehat{J}$ stated in the lemma below will be needed to follow our proof, as we will rely on some facts stated in [29] without reproducing the full arguments.

Lemma 5.4 ([29, Lemma 1.23])**.** *The function J belongs to $L^1(\mathbf{R})$ and its Fourier transform is given by*

$$\widehat{J}(t) = \begin{cases} 1 & \text{if } t = 0 \\ \pi t(1-|t|)\cot(\pi t) + |t| & \text{if } 0 < |t| < 1 \\ 0 & \text{otherwise} \end{cases}$$

Moreover, $\widehat{J}$ is decreasing on $[0,1]$.

Remark 5.5. Note that there is a typo in [29, Lemma 1.23] (cos is written instead of cot).

On the other hand, the following function K is also introduced:

$$K(z) = \left(\frac{\sin(\pi z)}{\pi z}\right)^2$$

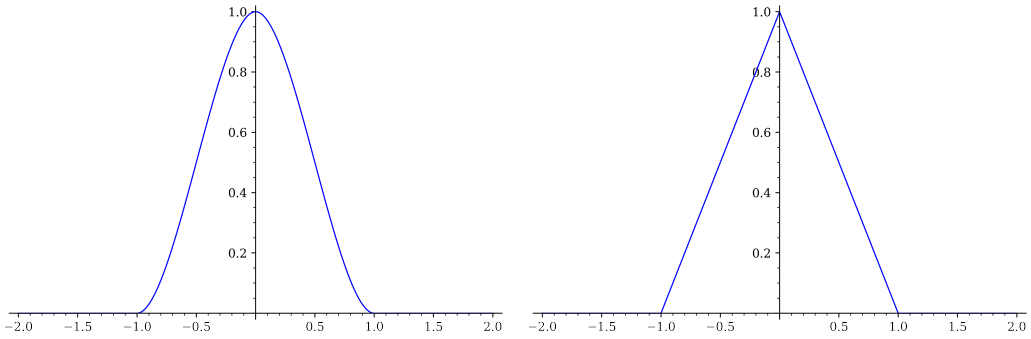
and its Fourier transform is the "triangle function". More precisely:

Lemma 5.6. *For all $t \in \mathbf{R}$, we have $\widehat{K}(t) = (1-|t|)\mathbb{1}_{|t|\leqslant 1}$.*

Proof. An elementary calculation shows that for all $z \in \mathbf{R}$ we have

$$K(z) = \int_{-1}^{1} (1-|t|)e(zt)\mathrm{d}t,$$

and then the result follows from Fourier inversion formula. □



(a) Plot of $\widehat{J}$ on $[-2,2]$ (b) Plot of $\widehat{K}$ on $[-2,2]$

The two functions $\widehat{J}$ and $\widehat{K}$ are then used to define the Fourier coefficients of two sequences of trigonometric polynomials:

Definition 5.7. *For all integers $H \geqslant 1$, we define the two following trigonometric polynomials of degree H:*

- $j_H(x) := \displaystyle\sum_{h=-H}^{H} \widehat{J}\left(\frac{h}{H+1}\right) e(hx)$
- $k_H(x) := \displaystyle\sum_{h=-H}^{H} \widehat{K}\left(\frac{h}{H+1}\right) e(hx)$

To gain some space, we will write $\widehat{J}_{H+1}(h)$ and $\widehat{K}_{H+1}(h)$ for $\widehat{J}\left(\frac{h}{H+1}\right)$ and $\widehat{K}\left(\frac{h}{H+1}\right)$.

Finally, we will need to calculate the convolution between 1-periodic functions, so we recall a few notations. For f and g two 1-periodic functions, define $f \star g$ as follows:

$$(f \star g)(x) = \int_{-1/2}^{1/2} f(x-t)g(t)\mathrm{d}t.$$

Similarly, if f is 1-periodic and μ is a 1-periodic measure on $\mathbf{R}$,

$$(f \star \mathrm{d}\mu)(x) = \int_{-1/2}^{1/2} f(x-t)\mathrm{d}\mu(t).$$

Finally, if $f\colon \mathbf{R} \to \mathbf{R}$, the total variation of f on $[a,b]$ is defined as

$$V_f([a,b]) := \sup \sum_{i=0}^{n-1} |f(x_{i+1}) - f(x_i)|,$$

where the supremum is taken over all partitions $a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b$ of $[a,b]$. This defines a measure V_f on $\mathbf{R}$, which is 1-periodic if the function f is 1-periodic. We say that f is of bounded variation on $[a,b]$ if $V_f([a,b]) < +\infty$.

The main theorem on approximation by convolutions, that we are going to use without proof, is the following result due to Vaaler (see [104, Theorem 19]).

Theorem 5.8 ([29, Theorem 1.25]). *Let f be a real function of bounded variation and period 1 satisfying $|2f(x_0) - f(x_0^-) - f(x_0^+)| \leqslant |f(x_0^-) - f(x_0^+)|$ for all $x_0 \in [0,1]$. Then the trigonometric polynomials $f \star j_H$ and $\mathrm{d}V_f \star k_H$ are at most of degree H and satisfy*

$$|f(x) - f \star j_H(x)| \leqslant \frac{1}{2H+2} \mathrm{d}V_f \star k_H(x)$$

for all $x \in \mathbf{R}$.

Applying this result to $f = \mathbb{1}_I$ for some interval of $\mathbf{R}$ of length $\leqslant 1$ gives the following corollary.

Corollary 5.9. *Let $I \subseteq \mathbf{R}$ be an interval of length $\lambda_1(I) \leqslant 1$. Then for all $H \geqslant 1$ and for all $x \in \mathbf{R}$,*

$$|\mathbb{1}_I(x) - \mathbb{1}_I \star j_H(x)| \leqslant \frac{1}{H+1} \sum_{h=-H}^{H} \widehat{K}_{H+1}(h) C_h e(hx)$$

where $C_h = \frac{1}{2}\int_0^1 e(-hx)\mathrm{d}V_{\mathbb{1}_I}(x)$ satisfies $|C_h| \leqslant 1$ for all h, and $C_0 = 1$.

Proof. It is an application of [29, Theorem 1.25] to the function $f = \mathbb{1}_I$. This particular case is stated at the beginning of the proof of [29, Corollary 1.26]. □

Remark 5.10. In this chapter, we only focus on the consequences of the analytic properties of the functions H, J, K above on Erdös-Turán-Koksma type inequalities, but Vaaler's article [104] gives other applications, such as one which is important in Selberg's large sieve. The extremality property satisfied by the entire function that we denoted by H in (5.3) is already a beautiful result on its own, see [104] for details.

5.2.3. An extension of Theorem 5.2 to direct sums of a torus with a finite abelian group

Let $d \geqslant 1$ and let F be a finite abelian group. We denote by Γ the group $\mathbb{T}^d \oplus F$. For any character $\chi_{\mathbf{m}}$ of $\mathbb{T}^d$ and any character ψ of F, we denote by $\chi_{\mathbf{m}} \otimes \psi$ the character of Γ defined by:

$$\begin{array}{ccc} \Gamma = \mathbb{T}^d \oplus F & \to & \mathbf{S}^1 \\ (x,y) & \mapsto & \chi_{\mathbf{m}}(x)\psi(y) \end{array}$$

Then the map

$$\begin{array}{ccc} \mathbf{Z}^d \times \widehat{F} & \to & \widehat{\Gamma} \\ (\mathbf{m}, \psi) & \mapsto & \chi_{\mathbf{m}} \otimes \psi \end{array}$$

is an isomorphism of groups. In other words, any character $\chi \in \widehat{\Gamma}$ can be written uniquely as $\chi_{\mathbf{m}} \otimes \psi$ for a certain $\mathbf{m} \in \mathbf{Z}^d$ and a certain $\psi \in \widehat{F}$.

Definition 5.11. *Let $\chi \in \widehat{\Gamma}$ and let $\mathbf{m} = (m_1, \ldots, m_d)$ and ψ be the unique elements of $\mathbf{Z}^d$ and $\widehat{F}$ such that $\chi = \chi_{\mathbf{m}} \otimes \psi$. Then we introduce the following quantities which measure the "size" of the character χ:*

- $T(\chi) := \|\mathbf{m}\|_\infty$
- $r(\chi) = \prod_{j=1}^{d} \max(1, |m_j|)$

Let us stress that these notions of "size" of a character only take into account the continuous part $\chi_{\mathbf{m}}$, without taking into the discrete part ψ into consideration.
Now, let us define the natural notion of discrepancy for a sequence with values in Γ.

Definition 5.12. *If $z = (z_n)_{n\geqslant 1}$ is a sequence of elements of $\Gamma = \mathbb{T}^d \oplus F$, we define its discrepancy as*

$$D_N(z) := \sup_{\substack{I\in\mathscr{I}_d \\ y\in F}} \left| \frac{\#\{1 \leqslant n \leqslant N,\ z_n \in I \times \{y\}\}}{N} - \frac{\lambda_d(I)}{|F|} \right|$$

where $\mathscr{I}_d$ denotes the set of rectangles $I = [a_1, b_1] \times \cdots \times [a_d, b_d]$ of $\mathbb{T}^d$.

A rather lengthy but simple adaptation of the proof of Theorem 5.2 gives the following extension of the Erdös-Turán-Koksma inequality.

Theorem 5.13. *Let $z = (z_n)_{n\geqslant 1}$ be a sequence of elements of $\Gamma = \mathbb{T}^d \oplus F$. Then for all $H \geqslant 1$ and all $N \geqslant 1$,*

$$D_N(z) \leqslant \left(\frac{3}{2}\right)^d \left(\frac{2}{H+1} + \frac{1}{|F|} \sum_{\substack{\chi\in\widehat{\Gamma}\setminus\{1\} \\ 0\leqslant T(\chi)\leqslant H}} \frac{1}{r(\chi)} \left| \frac{1}{N} \sum_{n=1}^{N} \chi(z_n) \right| \right)$$

Proof. The following proof is an adaptation of the proof of [29, Theorem 1.21].
For all $n \geqslant 1$, we write z_n as (x_n, y_n), where $x_n = \left(x_n^{(1)}, \ldots, x_n^{(d)}\right) \in \mathbb{T}^d$ and $y_n \in F$. Let us denote by $m := |F|$ and let us fix an element $y \in F$ and a rectangle

$$I = I_1 \times \cdots \times I_d = [a_1, b_1] \times \cdots \times [a_d, b_d] \in \mathscr{I}_d.$$

Then for all $H \geqslant 1$, we have

$$\begin{aligned}\sum_{n=1}^{N} \left(\mathbb{1}_I(x_n)\mathbb{1}_{\{y\}}(y_n)\right) - N\frac{\lambda_d(I)}{m} &= \sum_{n=1}^{N} \left[\left(\prod_{j=1}^{d} \mathbb{1}_{I_j}\left(x_n^{(j)}\right) \right) \mathbb{1}_{\{y\}}(y_n) - \left(\prod_{j=1}^{d} f_j\left(x_n^{(j)}\right) \right) \mathbb{1}_{\{y\}}(y_n) \right] \\ &\quad + \sum_{n=1}^{N} \left[\left(\prod_{j=1}^{d} f_j\left(x_n^{(j)}\right) \right) \mathbb{1}_{\{y\}}(y_n) - \frac{\lambda_d(I)}{m} \right],\end{aligned}$$

where $f_j\left(x_n^{(j)}\right) := \mathbb{1}_{I_j} \star j_H\left(x_n^{(j)}\right)$. Denote the first sum on the right-hand side by S_N and the second one by T_N.

Estimation of $|S_N|$. Thanks to the triangle inequality and to Lemma 5.18 to control the inner difference of products, we have

$$\begin{aligned}|S_N| &\leqslant \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \left(\sum_{\emptyset\neq J\subseteq\{1,\ldots d\}} \prod_{j\notin J} \mathbb{1}_{I_j}\left(x_n^{(j)}\right) \prod_{j\in J} \left| f_j\left(x_n^{(j)}\right) - \mathbb{1}_{I_j}\left(x_n^{(j)}\right) \right| \right) \\ &\leqslant \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \left(\sum_{\emptyset\neq J\subseteq\{1,\ldots d\}} \prod_{j\in J} \left| f_j\left(x_n^{(j)}\right) - \mathbb{1}_{I_j}\left(x_n^{(j)}\right) \right| \right) \\ &= \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \left[\prod_{j=1}^{d} \left(1 + \left| f_j\left(x_n^{(j)}\right) - \mathbb{1}_{I_j}\left(x_n^{(j)}\right) \right| \right) - 1 \right]\end{aligned}$$

Now, thanks to Lemma 5.9, we have that for all $j \in \{1, \dots, d\}$,

$$\left| f_j\left(x_n^{(j)}\right) - \mathbb{1}_{I_j}\left(x_n^{(j)}\right) \right| \leqslant \frac{1}{H+1} \sum_{h_j=-H}^{H} \widehat{K}_{H+1}(h_j) C_{h_j} e\left(h_j x_n^{(j)}\right),$$

hence

$$\begin{aligned} |S_N| &\leqslant \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \left[\prod_{j=1}^{d} \left(1 + \frac{1}{H+1} \sum_{h_j=-H}^{H} \widehat{K}_{H+1}(h_j) C_{h_j} e\left(h_j x_n^{(j)}\right) \right) - 1 \right] \\ &= \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \left[\prod_{j=1}^{d} \left(1 + \frac{1}{H+1} + \frac{1}{H+1} \sum_{0<|h_j|\leqslant H} \widehat{K}_{H+1}(h_j) C_{h_j} e\left(h_j x_n^{(j)}\right) \right) - 1 \right], \end{aligned}$$

using the fact that $C_0 = \widehat{K}_{H+1}(0) = 1$. Then we develop the product, this gives the following upper bound:

$$\begin{aligned} |S_N| &\leqslant \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \left[\left(1 + \frac{1}{H+1} \right)^d - 1 \right] \\ &\quad + \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \left[\sum_{J \subsetneq \{1,\dots d\}} \left(\left(1 + \frac{1}{H+1} \right)^{|J|} \left(\frac{1}{H+1} \right)^{d-|J|} \prod_{j \notin J} \sum_{0<|h_j|\leqslant H} \widehat{K}_{H+1}(h_j) C_{h_j} e\left(h_j x_n^{(j)}\right) \right) \right] \end{aligned}$$

Now,

$$\prod_{j \notin J} \sum_{0<|h_j|\leqslant H} \widehat{K}_{H+1}(h_j) C_{h_j} e\left(h_j x_n^{(j)}\right) = \sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in \mathbf{Z}^d \\ 0<|h_j|\leqslant H \text{ if } j\notin J \\ h_j=0 \text{ if } j\in J}} \left(\prod_{j \notin J} \widehat{K}_{H+1}(h_j) C_{h_j} \right) e(\mathbf{h} \cdot x_n),$$

so the second sum in the previous upper bound of $|S_N|$ may be rewritten as follows:

$$\begin{aligned} &\sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \sum_{J \subsetneq \{1,\dots d\}} \left(1 + \frac{1}{H+1} \right)^{|J|} \left(\frac{1}{H+1} \right)^{d-|J|} \sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in \mathbf{Z}^d \\ 0<|h_j|\leqslant H \text{ if } j\notin J \\ h_j=0 \text{ if } j\in J}} \left(\prod_{j \notin J} \widehat{K}_{H+1}(h_j) C_{h_j} \right) e(\mathbf{h} \cdot x_n) \\ &= \sum_{J \subsetneq \{1,\dots d\}} \left(1 + \frac{1}{H+1} \right)^{|J|} \left(\frac{1}{H+1} \right)^{d-|J|} \sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in \mathbf{Z}^d \\ 0<|h_j|\leqslant H \text{ if } j\notin J \\ h_j=0 \text{ if } j\in J}} \left(\prod_{j \notin J} \widehat{K}_{H+1}(h_j) C_{h_j} \right) \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) e(\mathbf{h} \cdot x_n) \\ &= \sum_{\substack{\mathbf{h}\in \mathbf{Z}^d \\ 0<\|\mathbf{h}\|_\infty \leqslant H}} \left(1 + \frac{1}{H+1} \right)^{\alpha(\mathbf{h})} \left(\frac{1}{H+1} \right)^{d-\alpha(\mathbf{h})} \left(\prod_{\substack{1\leqslant j\leqslant d \\ h_j\neq 0}} \widehat{K}_{H+1}(h_j) C_{h_j} \right) \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) e(\mathbf{h} \cdot x_n). \end{aligned}$$

where $\alpha(\mathbf{h})$ denotes $\#\{1 \leqslant j \leqslant d,\ h_j = 0\}$. Finally, since

$$\left| \prod_{\substack{1\leqslant j\leqslant d \\ h_j\neq 0}} \widehat{K}_{H+1}(h_j) C_{h_j} \right| \leqslant 1,$$

we conclude that

$$|S_N| \leqslant \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \left[\left(1 + \frac{1}{H+1}\right)^d - 1 \right] + \sum_{\substack{\mathbf{h}\in\mathbf{Z}^d \\ 0<\|\mathbf{h}\|_\infty \leqslant H}} \left(1 + \frac{1}{H+1}\right)^{\alpha(\mathbf{h})} \left(\frac{1}{H+1}\right)^{d-\alpha(\mathbf{h})} \left| \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) e(\mathbf{h}\cdot x_n) \right|.$$

Estimation of $|T_N|$. Recall that

$$T_N = \sum_{n=1}^{N} \left[\left(\prod_{j=1}^{d} f_j\left(x_n^{(j)}\right) \right) \mathbb{1}_{\{y\}}(y_n) - \frac{\lambda_d(I)}{m} \right]$$

Replacing j_H by its definition allows one to rewrite $f_j\left(x_n^{(j)}\right)$ as

$$\sum_{h_j=-H}^{H} \widehat{\mathbb{1}}_{I_j}(h_j) \widehat{J}_{H+1}(h_j) e\left(h_j x_n^{(j)}\right).$$

Thus,

$$\begin{aligned} \prod_{j=1}^{d} f_j\left(x_n^{(j)}\right) &= \prod_{j=1}^{d} \sum_{h_j=-H}^{H} \widehat{\mathbb{1}}_{I_j}(h_j) \widehat{J}_{H+1}(h_j) e\left(h_j x_n^{(j)}\right) \\ &= \sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in\mathbf{Z}^d \\ 0\leqslant\|\mathbf{h}\|_\infty\leqslant H}} \left(\prod_{j=1}^{d} \widehat{\mathbb{1}}_{I_j}(h_j) \widehat{J}_{H+1}(h_j) \right) e(\mathbf{h}\cdot x_n). \end{aligned}$$

Now, for all $j \in \{1,\dots,d\}$, we have $\widehat{\mathbb{1}}_{I_j}(0) = \lambda_1(I_j)$ and $\widehat{J}_{H+1}(0) = 1$, so the term corresponding to $\mathbf{h} = 0$ in the previous sum is equal to the product of the $\lambda_1(I_j)$, that is: $\lambda_d(I)$. Thus:

$$T_N = \sum_{n=1}^{N} \left[\mathbb{1}_{\{y\}}(y_n) \left(\sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in\mathbf{Z}^d \\ 0<\|\mathbf{h}\|_\infty\leqslant H}} \left(\prod_{j=1}^{d} \widehat{\mathbb{1}}_{I_j}(h_j) \widehat{J}_{H+1}(h_j) \right) e(\mathbf{h}\cdot x_n) \right) + \lambda_d(I) \left(\mathbb{1}_{\{y\}}(y_n) - \frac{1}{m} \right) \right].$$

Thanks to the triangle inequality and to the inequality $\lambda_d(I) \leqslant 1$, we deduce:

$$\begin{aligned} |T_N| &\leqslant \left| \sum_{n=1}^{N} \left(\mathbb{1}_{\{y\}}(y_n) - \frac{1}{m} \right) \right| + \left| \sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in\mathbf{Z}^d \\ 0<\|\mathbf{h}\|_\infty\leqslant H}} \left(\prod_{j=1}^{d} \widehat{\mathbb{1}}_{I_j}(h_j) \widehat{J}_{H+1}(h_j) \right) \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) e(\mathbf{h}\cdot x_n) \right| \\ &\leqslant \left| \sum_{n=1}^{N} \left(\mathbb{1}_{\{y\}}(y_n) \right) - \frac{N}{m} \right| + \sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in\mathbf{Z}^d \\ 0<\|\mathbf{h}\|_\infty\leqslant H}} \left| \prod_{j=1}^{d} \widehat{\mathbb{1}}_{I_j}(h_j) \widehat{J}_{H+1}(h_j) \right| \left| \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) e(\mathbf{h}\cdot x_n) \right| \end{aligned}$$

Next, we use the upper bounds $\left|\widehat{J}_{H+1}(h_j)\right| \leqslant 1$ and

$$\left|\widehat{\mathbb{1}}_{I_j}(h_j)\right| \leqslant \begin{cases} \lambda_1(I_j) \leqslant 1 & \text{if } h_j = 0 \\ \frac{1}{\pi|h_j|} & \text{if } h_j \neq 0 \end{cases}$$

to obtain the estimate

$$|T_N| \leqslant \left| \sum_{n=1}^{N} \left(\mathbb{1}_{\{y\}}(y_n) \right) - \frac{N}{m} \right| + \sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in \mathbf{Z}^d \\ 0<\|\mathbf{h}\|_\infty \leqslant H}} \frac{1}{\pi^{d-\alpha(\mathbf{h})} r(\mathbf{h})} \left| \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) e(\mathbf{h}\cdot x_n) \right|.$$

(we recall here that $\alpha(\mathbf{h})$ denotes $\#\{1 \leqslant j \leqslant d,\ h_j = 0\}$, while $r(\mathbf{h}) = \prod_{j=1}^{d} \max(1, |h_j|)$).

Conclusion. We have

$$\left| \sum_{n=1}^{N} \left(\mathbb{1}_I(x_n) \mathbb{1}_{\{y\}}(y_n) \right) - N \frac{\lambda_d(I)}{m} \right| = |S_N + T_N| \leqslant |S_N| + |T_N|,$$

so if we use the two previous steps and divide by N, this gives

$$\begin{aligned} \left| \frac{\#\{1 \leqslant n \leqslant N,\ z_n \in I \times \{y\}\}}{N} - \frac{\lambda_d(I)}{m} \right| \leqslant & \left[\left(1 + \frac{1}{H+1} \right)^d - 1 \right] \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \\ & + \sum_{\substack{\mathbf{h}\in \mathbf{Z}^d \\ 0<\|\mathbf{h}\|_\infty \leqslant H}} \left(1 + \frac{1}{H+1} \right)^{\alpha(\mathbf{h})} \left(\frac{1}{H+1} \right)^{d-\alpha(\mathbf{h})} \left| \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) e(\mathbf{h}\cdot x_n) \right| \\ & + \left| \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) - \frac{1}{m} \right| \\ & + \sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in \mathbf{Z}^d \\ 0<\|\mathbf{h}\|_\infty \leqslant H}} \frac{1}{\pi^{d-\alpha(\mathbf{h})} r(\mathbf{h})} \left| \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) e(\mathbf{h}\cdot x_n) \right|. \end{aligned}$$

Finally, we use the inequality

$$\frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) \leqslant 1$$

as well as the two following upper bounds one can find at the bottom of [29, p. 22]:

$$\begin{cases} \left(1 + \frac{1}{H+1} \right)^d - 1 \leqslant \left(\frac{3}{2} \right)^d \frac{2}{H+1} \\ \\ \left(1 + \frac{1}{H+1} \right)^{\alpha(\mathbf{h})} \left(\frac{1}{H+1} \right)^{d-\alpha(\mathbf{h})} + \frac{1}{\pi^{d-\alpha(\mathbf{h})} r(\mathbf{h})} \leqslant \left(\frac{3}{2} \right)^d \frac{1}{r(\mathbf{h})}. \end{cases}$$

This gives

$$\begin{aligned} \left| \frac{\#\{1 \leqslant n \leqslant N,\ z_n \in I \times \{y\}\}}{N} - \frac{\lambda_d(I)}{m} \right| \leqslant & \left(\frac{3}{2} \right)^d \left(\frac{2}{H+1} + \sum_{\substack{\mathbf{h}=(h_1,\dots h_d)\in \mathbf{Z}^d \\ 0<\|\mathbf{h}\|_\infty \leqslant H}} \frac{1}{r(\mathbf{h})} \left| \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) e(\mathbf{h}\cdot x_n) \right| \right) \\ & + \left| \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\{y\}}(y_n) - \frac{1}{m} \right|. \end{aligned}$$

Then Theorem 5.13 follows from the trivial bound $1 \leqslant (3/2)^d$ and from writing

$$\mathbb{1}_{\{y\}}(y_n) = \frac{1}{m} \sum_{\psi \in \widehat{F}} \psi(y_n) \overline{\psi(y)}.$$

□

5.2.4. Discussion on the definition of the discrepancy in a subgroup of a torus

Let G be a closed subgroup of $\mathbb{T}^k$ and let $z = (z_n)_{n\geqslant 1}$ be a sequence of points in G. Once we know that (z_n) becomes equidistributed in G with respect to its Haar measure, one may ask: can we give a quantitative estimate of a certain notion of discrepancy in terms of the decay of the absolute value of the Weyl sums?

To answer this question, we must give a precise definition of the discrepancy in this context. There are two ideas we thought about:

Definition 5.14. *We define the discrepancy by intersecting rectangles of $\mathbb{T}^k$ (the large ambient group) with the closed subgroup G. More precisely, if we denote by $\mathscr{I}_k$ the set of reductions modulo $\mathbf{Z}^k$ of products $I = [a_1, b_1] \times \cdots \times [a_k, b_k]$ of intervals of length less than or equal to 1, we define the discrepancy of (z_n) at rank N as:*

$$D_N(z) := \sup_{I\in\mathscr{I}_k} \left| \frac{\#\{1 \leqslant n \leqslant N,\ z_n \in I\}}{N} - \mu_G(I \cap G) \right|$$

where μ_G denotes the Haar measure on G.

Advantage: this definition does not depend on any choice, and seems to be adapted to any subgroup G of $\mathbb{T}^k$.

Drawback: it seems difficult to understand the intersections $I \cap G$ well enough for any closed subgroup G, and understanding these intersections seems important to adapt the classical proofs of Theorem 5.2 to this setting.

Therefore, we thought about an alternative definition of the discrepancy, which is less intrinsic, but is easier to work with.

Definition 5.15. *One can fix an isomorphism of topological groups $\varphi\colon G \to \mathbb{T}^d \oplus F$, and then define a notion of "φ-discrepancy" using this isomorphism:*

$$D_N^{\varphi}(z) := \sup_{\substack{I\in\mathscr{I}_d \\ y\in F}} \left| \frac{\#\{1 \leqslant n \leqslant N,\ \varphi(z_n) \in I \times \{y\}\}}{N} - \frac{\lambda_d(I)}{|F|} \right|$$

Advantage: this definition allows us to use our Theorem 5.13 and still has an interpretation as a measure of the rate of convergence to the Haar measure on the subgroup G.

Drawback: it depends on the choice of an isomorphism.

An idea to obtain from this last definition an intrinsic notion of discrepancy would be to try to take an average, or even a supremum over all isomorphisms φ, and to define the discrepancy as $\sup_{\varphi} D_N^{\varphi}(z)$. However, as we will see below, the upper bounds we obtain depend on φ and I see no reason why they could be uniformly bounded.

In the next section, we use Definition 5.15 and prove an Erdös-Turán-Koksma inequality for any closed subgroup G of $\mathbb{T}^k$, relying on the choice of an isomorphim φ_P with some $\mathbb{T}^d \oplus F$ constructed as in Section 5.2.1, and on Theorem 5.13.

5.2.5. A version of Erdös-Turán-Koksma inequality for subgroups of a torus

Let G be a closed subgroup of $\mathbb{T}^k$, and let φ_P be an isomorphism as in Section 5.2.1, induced by the change-of-basis matrix P:

$$\varphi_P\colon G \to \mathbb{T}^d \oplus F,$$

where $F = \bigoplus_{i=d+1}^{k} \mathbf{Z}/m_i\mathbf{Z}$ for some positive integers m_i. Let $z = (z_n)_{n\geqslant 1}$ be a sequence of elements of G. We want to estimate its φ_P-discrepancy (Definition 5.15). Thanks to Theorem 5.13 applied to the sequence $(\varphi_P(z_n))_{n\geqslant 1}$, we have that for all $N \geqslant 1$ and for all $H \geqslant 1$,

$$D_N^{\varphi_P}(z) \leqslant \left(\frac{3}{2}\right)^d \left(\frac{2}{H+1} + \frac{1}{|F|} \sum_{\substack{\chi \\ 0\leqslant T(\chi)\leqslant H}} \frac{1}{r(\chi)} \left| \frac{1}{N} \sum_{n=1}^{N} \chi(\varphi_P(z_n)) \right| \right) \tag{5.4}$$

where the sum ranges over all non-trivial characters χ of $\mathbb{T}^d \oplus F$. These characters are of the form $\chi_{\mathbf{h}} \otimes \psi$, where $\psi \in \widehat{F}$ (see the beginning of section 5.2.3), and the condition $T(\chi) \leqslant H$ means that those which appear in the sum are the ones such that $\|\mathbf{h}\|_\infty \leqslant H$.

Now, the issue with the sum above is that it is indexed by characters of $\mathbb{T}^d \oplus F$, but we would like to view it as a sum over the characters of G, with some control of the "size" of those characters. Gladly, the isomorphism φ_P induces the following isomorphism between the dual groups:

$$\begin{array}{rccc} \widehat{\varphi_P} & : & \widehat{\mathbb{T}^d \oplus F} & \to & \widehat{G} \\ & & \chi & \mapsto & \chi \circ \varphi_P \end{array}$$

Thus, the sum on the right-hand side of (5.4) is easily turned into a sum over characters of G. The control of a certain notion of "size" is given by the following lemma. The idea is that any character of the closed subgroup $G \subseteq \mathbb{T}^k$ can be extended to a character of $\mathbb{T}^k$, and all such characters are of the form $e\left(\mathbf{h}' \cdot (-)\right)$ for some $\mathbf{h}' \in \mathbf{Z}^k$. We then control their size by controlling the ℓ^∞-norm of such an $\mathbf{h}'$.

Lemma 5.16. *If χ is a character of $\mathbb{T}^d \oplus F$ such that $0 \leqslant T(\chi) \leqslant H$, then there exists $\mathbf{h}' \in \mathbf{Z}^k$ such that $\|\mathbf{h}'\|_\infty \leqslant \left\|{}^tP\right\|_{\mathrm{op}} H$ and*

$$\widehat{\varphi_P}(\chi) = e\left(\mathbf{h}' \cdot (-)\right)_{|G}.$$

Here $\left\|{}^tP\right\|_{\mathrm{op}}$ denotes the operator norm (associated with the supremum norm on $\mathbf{R}^k$) of the matrix ${}^tP$.

Proof. Let $\chi = \chi_{\mathbf{h}} \otimes \psi$ be a character of $\mathbb{T}^d \oplus F$ such that $0 \leqslant T(\chi) \leqslant H$, meaning that $\|\mathbf{h}\|_\infty \leqslant H$. Since $F = \bigoplus_{i=d+1}^{k} \mathbf{Z}/m_i\mathbf{Z}$, we can write ψ as

$$\begin{array}{rccc} \bigotimes_{i=d+1}^{k} \psi_{\kappa_i} & : & \bigoplus_{i=d+1}^{k} \mathbf{Z}/m_i\mathbf{Z} & \to & \mathbf{S}^1 \\ & & (y_{d+1}, \dots, y_k) & \mapsto & \prod_{i=d+1}^{k} e\left(\frac{\kappa_i}{m_i} y_i\right) \end{array}$$

with $\kappa_i \in \{0, \dots, m_i - 1\}$ for all $i \in \{d+1, \dots, k\}$.

Let $z \in G$. We write $\varphi_P(z)$ as (x, y), where $x \in \mathbb{T}^d$ and $y = (y_{d+1}, \dots, y_k) \in F$. Then

$$\widehat{\varphi_P}(\chi)(z) = \chi(\varphi_P(z)) = \chi_{\mathbf{h}} \otimes \psi(\varphi_P(z)) = \chi_{\mathbf{h}}(x)\psi(y) = e(\mathbf{h} \cdot x) \prod_{i=d+1}^{k} e\left(\frac{\kappa_i}{m_i} y_i\right)$$

If we denote by $\mathbf{h}_\psi$ the vector of $\mathbf{Z}^d \oplus \frac{1}{m_{d+1}}\mathbf{Z} \oplus \cdots \oplus \frac{1}{m_k}\mathbf{Z}$

$$\begin{pmatrix} \mathbf{h} \\ \frac{\kappa_{d+1}}{m_{d+1}} \\ \vdots \\ \frac{\kappa_k}{m_k} \end{pmatrix}$$

we have

$$\widehat{\varphi_P}(\chi)(z) = e\left(\mathbf{h}_\psi \cdot \varphi_P(z)\right) = e\left(\mathbf{h}_\psi \cdot P\tilde{z}\right)$$

where $\tilde{z}$ is a lift in $\mathbf{R}^k$ of the element $z \in G \subseteq \mathbb{T}^k$. Next, we put the matrix P on the other side of the dot product, and this gives:

$$\widehat{\varphi_P}(\chi)(z) = e\left({}^tP\mathbf{h}_\psi \cdot \tilde{z}\right)$$

Now let $\mathbf{h}' := {}^tP\mathbf{h}_\psi$. Then, thanks to Lemma 5.19, the vector $\mathbf{h}'$ belongs to $\mathbf{Z}^k$, and satisfies

$$\left\|\mathbf{h}'\right\|_\infty \leqslant \left\|{}^tP\right\|_{\mathrm{op}} \left\|\mathbf{h}_\psi\right\|_\infty \leqslant \left\|{}^tP\right\|_{\mathrm{op}} H.$$

Moreover, we proved that for all $z \in G$, we have

$$\widehat{\varphi_P}(\chi)(z) = e\left(\mathbf{h}' \cdot \tilde{z}\right)$$

which concludes the proof. □

Going back to the φ_P-discrepancy of our sequence $(z_n)_{n\geqslant 1}$ in G, we have

$$D_N^{\varphi_P}((z_n)_{n\geqslant 1}) \leqslant \left(\frac{3}{2}\right)^d \left(\frac{2}{H+1} + \frac{1}{|F|} \sum_{\substack{\chi \\ 0\leqslant T(\chi)\leqslant H}} \frac{1}{r(\chi)} \left| \frac{1}{N} \sum_{n=1}^{N} \widehat{\varphi_P}(\chi)(z_n) \right| \right)$$

thanks to (5.4) and to the definition of $\widehat{\varphi_P}$. Now, as χ ranges over the non-trivial characters of $\mathbb{T}^d \oplus F$ satisfying $0 \leqslant T(\chi) \leqslant H$, $\widehat{\varphi_P}(\chi)$ ranges over a subset of

$$\widehat{G}_{\left\|{}^tP\right\|_{\mathrm{op}} H} := \left\{ \eta \in \widehat{G} \setminus \{1\} \;\middle|\; \exists \mathbf{h}' \in \mathbf{Z}^k, \begin{cases} \left\|\mathbf{h}'\right\|_\infty \leqslant \left\|{}^tP\right\|_{\mathrm{op}} H \\ \eta = e\left(\mathbf{h}' \cdot (-)\right)_{|G} \end{cases} \right\}.$$

This is the set of non-trivial characters of G which are the restriction to G of a character of $\mathbb{T}^k$ associated with an integral vector $\mathbf{h}'$ which satisfies $\left\|\mathbf{h}'\right\|_\infty \leqslant \left\|{}^tP\right\|_{\mathrm{op}} H$. Therefore,

$$D_N^{\varphi_P}((z_n)_{n\geqslant 1}) \leqslant \left(\frac{3}{2}\right)^d \left(\frac{2}{H+1} + \frac{1}{|F|} \sum_{\eta \in \widehat{G}_{\left\|{}^tP\right\|_{\mathrm{op}} H}} \frac{1}{r\left(\widehat{\varphi_P}^{-1}(\eta)\right)} \left| \frac{1}{N} \sum_{n=1}^{N} \eta(z_n) \right| \right)$$

Let us sum up what we proved in the following theorem:

Theorem 5.17. *Let G be a closed subgroup of $\mathbb{T}^k$ and let*

$$\varphi_P \colon G \to \mathbb{T}^d \oplus F$$

be an isomorphism as in Section 5.2.1, induced by a change-of-basis matrix P. As before, $d \leqslant k$ and $F = \bigoplus_{i=d+1}^k \mathbf{Z}/m_i\mathbf{Z}$ for some positive integers m_i. Let $z = (z_n)_{n\geqslant 1}$ be a sequence of points in G. We have the following Erdös-Turán-Koksma type inequality concerning the φ_P-discrepancy: for all $N \geqslant 1$ and all $H \geqslant 1$,

$$D_N^{\varphi_P}(z) \leqslant \left(\frac{3}{2}\right)^d \left(\frac{2}{H+1} + \frac{1}{|F|} \sum_{\eta \in \widehat{G}_{\left\|{}^tP\right\|_{\mathrm{op}} H}} \frac{1}{r\left(\widehat{\varphi_P}^{-1}(\eta)\right)} \left| \frac{1}{N} \sum_{n=1}^{N} \eta(z_n) \right| \right),$$

where

$$\widehat{G}_{\left\|{}^tP\right\|_{\mathrm{op}} H} := \left\{ \eta \in \widehat{G} \setminus \{1\} \;\middle|\; \exists \mathbf{h}' \in \mathbf{Z}^k, \begin{cases} \left\|\mathbf{h}'\right\|_\infty \leqslant \left\|{}^tP\right\|_{\mathrm{op}} H \\ \eta = e\left(\mathbf{h}' \cdot (-)\right)_{|G} \end{cases} \right\}.$$

5.2.6. Some technical lemmas

Here are two lemmas which are purely technical and would have made the discussions above more obscure had they been included in the previous sections.

Lemma 5.18. *If $a_1, \dots, a_d$ and $b_1, \dots, b_d \in \mathbf{C}$ then*

$$\left| \prod_{j=1}^{d} bj - \prod_{j=1}^{d} a_j \right| \leqslant \sum_{\varnothing \neq J \subseteq \{1,\dots d\}} \left(\prod_{j \notin J} |a_j| \prod_{j \in J} |b_j - a_j| \right)$$

Proof. A way to obtain it is to write $\prod_{j=1}^{d} b_j$ as $\prod_{j=1}^{d}(b_j - a_j) + a_j$ and to develop the product. Then the result follows from the triangle inequality. □

Lemma 5.19. *the vector ${}^tP\mathbf{h}_\psi$ in the proof of Lemma 5.16 belongs to $\mathbf{Z}^k$.*

Proof. The matrix P is the change-of-basis matrix which takes the coordinates of a vector in the canonical basis of $\mathbf{R}^k$ and returns its coordinates in the basis $\mathcal{B} = (a_1, \dots, a_d, a'_{d+1}, \dots, a'_k)$, where $a'_i = \frac{1}{m_i} a_i$ (see section 5.2.1). Let us denote by $\mathcal{C}$ the canonical basis of $\mathbf{R}^k$ and by $\mathcal{D}$ the basis $(a_1, \dots, a_d, a_{d+1}, \dots, a_k)$. Then

$$P = P_{\mathcal{B},\mathcal{C}} = P_{\mathcal{B},\mathcal{D}} P_{\mathcal{D},\mathcal{C}}.$$

Now, since $\mathcal{C}$ and $\mathcal{D}$ are two bases of the lattice $\mathbf{Z}^k$, we have that $P_{\mathcal{D},\mathcal{C}} \in \mathrm{GL}_k(\mathbf{Z})$. Moreover, $P_{\mathcal{B},\mathcal{D}} = \mathrm{diag}\,(1, \dots, 1, m_{d+1}, \dots, m_k)$. Therefore, since

$$\mathbf{h}_\psi = \begin{pmatrix} \mathbf{h} \\ \frac{\kappa_{d+1}}{m_{d+1}} \\ \vdots \\ \frac{\kappa_k}{m_k} \end{pmatrix}$$

it is clear that when multiplying by ${}^tP = {}^tP_{\mathcal{D},\mathcal{C}}\, {}^tP_{\mathcal{B},\mathcal{D}} = {}^tP_{\mathcal{D},\mathcal{C}} P_{\mathcal{B},\mathcal{D}}$, the denominators m_i cancel out, and we obtain an integer valued vector. □

5.3. Dependence with respect to choices of isomorphisms.

In Theorem 5.17, the definition of the discrepancy and the upper bound we obtain both depend on the isomorphim φ_P, and moreover the proof uses the fact that φ_P is induced by a matrix P. Now, one may ask what changes are needed in the proof to obtain an Erdös-Turán-Koksma inequality for the φ-discrepancy (Definition 5.15) for *any* choice of isomorphism of topological groups $G \to \mathbb{T}^d \oplus F$.

If $\varphi\colon G \to \mathbb{T}^d \oplus F$ is such an isomorphism and φ_P denotes a well-understood "matrix" isomorphism as in Section 5.2.1, then we can write $\varphi = \sigma \circ \varphi_P$, where σ is a continuous automorphism of $\mathbb{T}^d \oplus F$. So it remains to understand the group of automorphisms, and this is the aim of the following section. As we will see, these automorphisms are also induced by linear maps, so that we will be able to obtain estimates depending only on operator norms of matrices.

5.3.1. Automorphisms of $\mathbb{T}^d \oplus F$.

A continuous automorphism of $\mathbb{T}^d \oplus F$ is in particular a continuous endomorphism of that group. Therefore, it is of the form

$$\begin{array}{ccc} \mathbb{T}^d \oplus F & \to & \mathbb{T}^d \oplus F \\ (y, z) & \mapsto & (f(y,z), g(y,z)) \end{array}$$

where $f\colon \mathbb{T}^d \oplus F \to \mathbb{T}^d$ and $g\colon \mathbb{T}^d \oplus F \to F$ are continuous group homomorphisms. But now, one can write $f(y,z)$ as $\alpha(y) + \beta(z)$ where $\alpha\colon \mathbb{T}^d \to \mathbb{T}^d$ and $\beta\colon F \to \mathbb{T}^d$ are both continuous group homomorphisms. Indeed, it suffices to define $\alpha(y)$ as $f(y,0)$ and $\beta(z)$ as $f(0,z)$. Similarly, write

$g(y,z) = \gamma(y) + \delta(z)$ where $\gamma\colon \mathbb{T}^d \to F$ and $\delta\colon F \to F$. Thus, if σ is a continuous endomorphism of $\mathbb{T}^d \oplus F$, it can be represented by a matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

acting on $\mathbb{T}^d \oplus F$ as

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} y \\ z \end{pmatrix} = \begin{pmatrix} \alpha(y) + \beta(z) \\ \gamma(y) + \delta(z) \end{pmatrix}.$$

The aim of this section is to prove that all α, β, γ and δ can be described quite explicitly, mostly in terms of maps induced by linear maps.

A first observation one can make is the following:

Lemma 5.20. *If σ is a continuous endomorphism of $\mathbb{T}^d \oplus F$, then the component γ of the above matrix representation is trivial.*

Proof. The image of γ is a connected subgroup of the finite group F because γ is continuous and $\mathbb{T}^d$ is connected, therefore it must be the subgroup $\{0\}$. □

Now, if we further assume that σ is bijective, we can get more precise information on α, β and δ. Namely:

Lemma 5.21. *If σ is a continuous automorphism of $\mathbb{T}^d \oplus F$, then*

- *α is injective and $|\mathrm{coker}(\alpha)| \leqslant |F|$,*
- *δ is an automorphism of F.*

Proof.

- If α is not injective, let $y_1 \neq y_2 \in \mathbb{T}^d$ be such that $\alpha(y_1) = \alpha(y_2)$. Then

$$\sigma \begin{pmatrix} y_1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \begin{pmatrix} y_1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha(y_1) \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha(y_2) \\ 0 \end{pmatrix} = \sigma \begin{pmatrix} y_2 \\ 0 \end{pmatrix},$$

  hence σ is not injective. This proves that for σ to be an automorphism, it is necessary that α is injective. Now, the image of α is a subgroup of $\mathbb{T}^d$, and $\mathbb{T}^d$ is a disjoint union of classes modulo $\mathrm{Im}(\alpha)$:

$$\bigsqcup_{j=1}^{r} \mathrm{Im}(\alpha) + x_j,$$

  where $r = |\mathrm{coker}(\alpha)|$. So if σ is surjective, this means that any element of $\mathbb{T}^d$ is of the form $\alpha(y) + \beta(z)$ for some $y \in \mathbb{T}^d$ and some $z \in F$, and therefore β must reach all classes modulo α. This implies that F must have at least as many elements as there are classes modulo $\mathrm{Im}(\alpha)$.

- The second coordinate of $\sigma \begin{pmatrix} y \\ z \end{pmatrix}$ is simply given by $\delta(z)$, so δ needs to be surjective if we want σ to be an automorphism. Since $\delta\colon F \to F$, and F is finite, this is equivalent to saying that δ must be an automorphism.

□

Let us now explain why α, β and δ can in fact be written as maps induced by some matrix multiplications. For a vector $Y \in \mathbf{R}^d$, we denote by $(Y \bmod 1)$ the vector of $(\mathbf{R}/\mathbf{Z})^d$ obtained by reduction modulo 1 of each coordinate. Let us first view α as a map induced by a linear map.

Lemma 5.22. *Let $\alpha\colon \mathbb{T}^d \to \mathbb{T}^d$ be a continuous group homomorphism. Then there exists a matrix $A \in \mathrm{M}_d(\mathbf{Z})$ such that for all $y \in \mathbb{T}^d = (\mathbf{R}/\mathbf{Z})^d$,*

$$\alpha(y) = (AY \bmod 1),$$

where Y denotes any vector in $\mathbf{R}^d$ such that $(Y \bmod 1) = y$.

Proof. See [10, Chapter 7, §4]. □

Next, let us explain why β is also induced by the multiplication with a matrix.

Lemma 5.23. *Let*

$$F = \bigoplus_{j=d+1}^{k} \mathbf{Z}/m_j\mathbf{Z},$$

and let $\beta\colon F \to \mathbb{T}^d$ be a group homomorphism. Then there exist integers $\lambda_{i,j}$ (for $1 \leqslant i \leqslant d$ and $d+1 \leqslant j \leqslant k$) such that for all $z = (z_j)_{d+1\leqslant j\leqslant k} \in F$,

$$\beta(z) = \underbrace{\begin{pmatrix} \frac{\lambda_{1,d+1}}{m_{d+1}} & \cdots & \frac{\lambda_{1,k}}{m_k} \\ & \vdots & \\ \frac{\lambda_{d,d+1}}{m_{d+1}} & \cdots & \frac{\lambda_{d,k}}{m_k} \end{pmatrix}}_{=:B} \begin{pmatrix} z_{d+1} \\ \vdots \\ z_k \end{pmatrix} \bmod 1$$

Proof. A homomorphism $\beta\colon F \to \mathbb{T}^d$ is given by d homomorphisms

$$\beta_i\colon \bigoplus_{j=d+1}^{k} \mathbf{Z}/m_j\mathbf{Z} \to \mathbb{T}$$

for $i \in \{1, \dots, d\}$, and each of them can be decomposed as a sum of homomorphisms

$$\beta_{i,j}\colon \mathbf{Z}/m_j\mathbf{Z} \to \mathbb{T}$$

as follows:

$$\beta_i\left((z_j)_{d+1\leqslant j\leqslant k}\right) = \sum_{j=d+1}^{k} \beta_{i,j}(z_j)$$

(here we think of $\mathbb{T}$ as $\mathbf{R}/\mathbf{Z}$, hence the additive notation). Now each $\beta_{i,j}$ is an element of the dual of $\mathbf{Z}/m_j\mathbf{Z}$, so it acts as the multiplication by $\lambda_{i,j}/m_j$ for some integer $\lambda_{i,j} \in \{0, \dots, m_j - 1\}$. This gives the desired matrix representation of the statement. □

Finally, let us treat the case of $\delta\colon F \to F$:

Lemma 5.24. *If δ is an automorphism of the finite abelian group $F = \bigoplus_{j=d+1}^{k} \mathbf{Z}/m_j\mathbf{Z}$, then there exist integers $d_{i,j}$ (with $d+1 \leqslant i, j \leqslant k$) such that $0 \leqslant d_{i,j} < m_i$ and for all $z = (z_j)_{d+1\leqslant j\leqslant k} \in F$,*

$$\delta(z) = \underbrace{\begin{pmatrix} d_{d+1,d+1} & \cdots & d_{d+1,k} \\ & \vdots & \\ d_{k,d+1} & \cdots & d_{k,k} \end{pmatrix}}_{=:D} \begin{pmatrix} z_{d+1} \\ \vdots \\ z_k \end{pmatrix}$$

Proof. As in the previous proof, such an automorphism δ is given by a family $(\delta_{i,j})_{d+1\leqslant i,j\leqslant k}$ such that

$$\delta_{i,j}\colon \mathbf{Z}/m_j\mathbf{Z} \to \mathbf{Z}/m_i\mathbf{Z},$$

and each component of δ is given by $\delta_i := \sum_{j=d+1}^{k} \delta_{i,j}$. Now, a group homomorphism $f\colon \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ is of the form

$$\begin{array}{ccc} \mathbf{Z}/m\mathbf{Z} & \to & \mathbf{Z}/n\mathbf{Z} \\ k \bmod m & \mapsto & ak \bmod n \end{array}$$

for some integer $a \in \{1, \dots, n-1\}$, so we can write each $\delta_{i,j}$ as the multiplication by some integer $d_{i,j} \in \{0, \dots, m_i - 1\}$ (followed by reduction modulo m_i). We conclude that for all $z = (z_j)_{d+1\leqslant j\leqslant k} \in F$,

$$\delta(z) = \begin{pmatrix} \delta_{d+1}(z) \\ \vdots \\ \delta_k(z) \end{pmatrix} = \begin{pmatrix} \sum_{j=d+1}^{k} \delta_{d+1,j}(z_j) \\ \vdots \\ \sum_{j=d+1}^{k} \delta_{k,j}(z_j) \end{pmatrix} = \begin{pmatrix} d_{d+1,d+1} & \cdots & d_{d+1,k} \\ & \vdots & \\ d_{k,d+1} & \cdots & d_{k,k} \end{pmatrix} \begin{pmatrix} z_{d+1} \\ \vdots \\ z_k \end{pmatrix} =: Dz.$$

□

Conclusion. Any automorphism σ of $\mathbb{T}^d \times F$, where $F = \bigoplus_{i=d+1}^k \mathbf{Z}/m_i\mathbf{Z}$, is given by a matrix

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$$

where $A \in \mathrm{M}_d(\mathbf{Z})$, $D = (d_{i,j})_{d+1\leqslant i,j\leqslant k} \in \mathrm{M}_{k-d}(\mathbf{Z})$ and B is of the form

$$\begin{pmatrix} \frac{\lambda_{1,d+1}}{m_{d+1}} & \cdots & \frac{\lambda_{1,k}}{m_k} \\ & \vdots & \\ \frac{\lambda_{d,d+1}}{m_{d+1}} & \cdots & \frac{\lambda_{d,k}}{m_k} \end{pmatrix}$$

where the $\lambda_{i,j}$ are integers. Moreover we can choose $\lambda_{i,j}$ and $d_{i,j}$ such that for all i and j,

$$\begin{cases} 0 \leqslant \lambda_{i,j} < m_j \\ 0 \leqslant d_{i,j} < m_i. \end{cases}$$

Given an element $(y,z) = ((y_j),(z_j)) \in \mathbb{T}^d \oplus \left(\bigoplus_{i=d+1}^k \mathbf{Z}/m_i\mathbf{Z}\right)$, its image under σ is given by the matrix multiplication

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \begin{pmatrix} y \\ z \end{pmatrix}$$

and the appropriate reduction modulo 1 or modulo m_j on the suitable coordinates.

5.3.2. Generalization of Theorem 5.17 to any choice of isomorphism

We now let $\varphi\colon G \to \mathbb{T}^d \oplus F =: \Gamma$ be any isomorphism of topological groups. Then it can be written as $\varphi = \sigma \circ \varphi_P$ where σ is a continuous automorphism of Γ and φ_P is an explicit isomorphism induced by a matrix P as constructed in Section 5.2.1. Next, let $z = (z_n)_{n\geqslant 1}$ be a sequence with values in G, and consider the φ-discrepancy as defined in Definition 5.15. Then Theorem 5.13 applied to the sequence $\varphi(z_n)$ implies the following estimate:

$$D_N^{\varphi}(z) \leqslant \left(\frac{3}{2}\right)^d \left(\frac{2}{H+1} + \frac{1}{|F|} \sum_{\substack{\chi\in\widehat{\Gamma}\setminus\{1\} \\ 0\leqslant T(\chi)\leqslant H}} \frac{1}{r(\chi)} \left| \frac{1}{N} \sum_{n=1}^N \widehat{\varphi}(\chi)(z_n) \right| \right) \tag{5.5}$$

where $\widehat{\varphi}$ is the isomorphism $\widehat{\Gamma} \to \widehat{G}$ induced by φ.

The adaptation of Lemma 5.16 is as follows:

Lemma 5.25. *If $F = \bigoplus_{i=d+1}^k \mathbf{Z}/m_i\mathbf{Z}$, we denote by $\Sigma_F := \sum_{i=d+1}^k m_i$. If we represent the automorphism σ by a matrix*

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$$

as in the previous section, then for all $\chi \in \widehat{\Gamma}$ such that $T(\chi) \leqslant H$, there exists $\mathbf{h}' \in \mathbf{Z}^k \setminus \{0\}$ such that $\|\mathbf{h}'\|_\infty \leqslant \left\|{}^tP\right\|_{\mathrm{op}} \left(\left(\|{}^tA\|_{\mathrm{op}} + d\right) H + \Sigma_F\right)$ and

$$\widehat{\varphi}(\chi) = e\left(\mathbf{h}' \cdot (-)\right)_{|G}.$$

Proof. First, as in the proof of Lemma 5.16, we write χ as $\chi_{\mathbf{h}} \otimes \psi$ with $\|\mathbf{h}\|_\infty \leqslant H$ and $\psi = \bigotimes_{i=d+1}^k \psi_{\kappa_i} \in \widehat{F}$. For $z \in G$, we also keep the notation (x,y) for $\varphi_P(z)$ and introduce the notation (u,v) for $\varphi(z) = (\sigma\circ\varphi_P)(z) = \sigma(x,y)$. Then

$$\widehat{\varphi}(\chi)(z) = \chi(\varphi(z)) = \chi_{\mathbf{h}} \otimes \psi(\varphi(z)) = \chi_{\mathbf{h}}(u)\psi(v) = e(\mathbf{h}\cdot u) \prod_{i=d+1}^k e\left(\frac{\kappa_i}{m_i} v_i\right)$$

Denote by κ_ψ the element

$$\begin{pmatrix} \frac{\kappa_{d+1}}{m_{d+1}} \\ \vdots \\ \frac{\kappa_k}{m_k} \end{pmatrix}$$

of $\frac{1}{m_{d+1}}\mathbf{Z} \oplus \cdots \oplus \frac{1}{m_k}\mathbf{Z}$. Using the fact that

$$\begin{pmatrix} u \\ v \end{pmatrix} \equiv \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

(here $\equiv$ denotes an equality between the equivalence classes of these elements in $\mathbb{T}^d \oplus \left(\bigoplus_{i=d+1}^k \mathbf{Z}/m_i\mathbf{Z}\right)$), we get:

$$\widehat{\varphi}(\chi)(z) = e(\mathbf{h} \cdot (Ax + By))e(\kappa_\psi \cdot Dy).$$

Using the transpose matrices to isolate (x, y) on one side of the scalar product, we obtain

$$\widehat{\varphi}(\chi)(z) = e\left(\begin{pmatrix} {}^tA\mathbf{h} \\ {}^tB\mathbf{h} + {}^tD\kappa_\psi \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}\right).$$

Now, since $(x, y) = \varphi_P(z)$, we have

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv P\tilde{z},$$

where $\tilde{z}$ is a lift in $\mathbf{R}^k$ of the element $z \in G \subseteq \mathbb{T}^k$. We deduce that

$$\widehat{\varphi}(\chi)(z) = e\left({}^tP\begin{pmatrix} {}^tA\mathbf{h} \\ {}^tB\mathbf{h} + {}^tD\kappa_\psi \end{pmatrix} \cdot \tilde{z}\right)$$

To conclude, it remains to show that the vector

$$\mathbf{h}' := {}^tP\begin{pmatrix} {}^tA\mathbf{h} \\ {}^tB\mathbf{h} + {}^tD\kappa_\psi \end{pmatrix}$$

belongs to $\mathbf{Z}^k$ and that we can estimate its ℓ^∞-norm as in the statement of the lemma. The fact that $\mathbf{h}' \in \mathbf{Z}^k$ follows again from Lemma 5.19. Indeed, it is clear from the description of the matrix B in section 5.3.1 that the vector ${}^tB\mathbf{h}$ belongs to $\frac{1}{m_{d+1}}\mathbf{Z} \oplus \cdots \oplus \frac{1}{m_k}\mathbf{Z}$. The same holds for $D\kappa_\psi$, and so by Lemma 5.19, we know that ${}^tP$ cancels those denominators. Finally, we have:

$$\left\|\mathbf{h}'\right\|_\infty \leqslant \left\|{}^tP\right\|_{\mathrm{op}} \left\|\begin{pmatrix} {}^tA\mathbf{h} \\ {}^tB\mathbf{h} + D\kappa_\psi \end{pmatrix}\right\|_\infty \leqslant \left\|{}^tP\right\|_{\mathrm{op}} \left[\|{}^tA\mathbf{h}\|_\infty + \|{}^tB\mathbf{h}\|_\infty + \|{}^tD\kappa_\psi\|_\infty\right]$$

and

- $\|{}^tA\mathbf{h}\|_\infty \leqslant \|{}^tA\|_{\mathrm{op}}\|\mathbf{h}\|_\infty \leqslant \|{}^tA\|_{\mathrm{op}}H$,
- $\|{}^tB\mathbf{h}\|_\infty \leqslant \|{}^tB\|_{\mathrm{op}}\|\mathbf{h}\|_\infty \leqslant \left(\max_{d+1\leqslant j\leqslant k} \sum_{i=1}^d |B_{i,j}|\right)\|\mathbf{h}\|_\infty \leqslant d\|\mathbf{h}\|_\infty \leqslant dH$
- $\|{}^tD\kappa_\psi\|_\infty \leqslant \|{}^tD\|_{\mathrm{op}}\|\kappa_\psi\|_\infty \leqslant \left(\max_{d+1\leqslant j\leqslant k} \sum_{i=d+1}^k |d_{i,j}|\right)\|\kappa_\psi\|_\infty \leqslant \left(\sum_{i=d+1}^k m_i\right) \times 1 \leqslant \Sigma_F$.

and this concludes the proof. □

Corollary 5.26. *For any choice of isomorphism $\varphi\colon G \to \Gamma$, there exists a constant C_φ such that for all $\chi \in \widehat{\Gamma}$ such that $0 \leqslant T(\chi) \leqslant H$, there exists $\mathbf{h}' \in \mathbf{Z}^k$ such that*

$$\begin{cases} \|\mathbf{h}'\|_\infty \leqslant C_\varphi H \\ \widehat{\varphi}(\chi) = e(\mathbf{h}' \cdot (-))_{|G} \end{cases}$$

Once we have this corollary, we get a more general version of Theorem 5.17, where $D_N^{\varphi_P}$ can be replaced by D_N^{φ} for any choice of isomorphism φ. This gives the following statement:

Theorem 5.27. *Let G be a closed subgroup of $\mathbb{T}^k$ and let $\varphi\colon G \to \mathbb{T}^d \oplus F$ be an isomorphism of topological groups, where $d \leqslant k$ and $F = \bigoplus_{i=d+1}^{k} \mathbf{Z}/m_i\mathbf{Z}$ for some positive integers m_i. Then there exists a constant $C_\varphi > 0$ such that for any sequence $z = (z_n)_{n\geqslant 1}$ of points in G we have the following Erdös-Turán-Koksma type inequality: for all $N \geqslant 1$ and all $H \geqslant 1$,*

$$D_N^{\varphi}(z) \leqslant \left(\frac{3}{2}\right)^d \left(\frac{2}{H+1} + \frac{1}{|F|} \sum_{\eta \in \widehat{G}_{C_\varphi H}} \frac{1}{r\left(\widehat{\varphi}^{-1}(\eta)\right)} \left| \frac{1}{N} \sum_{n=1}^{N} \eta(z_n) \right| \right),$$

where

$$\widehat{G}_{C_\varphi H} := \left\{ \eta \in \widehat{G} \setminus \{1\} \;\middle|\; \exists \mathbf{h}' \in \mathbf{Z}^k, \begin{cases} \|\mathbf{h}'\|_\infty \leqslant C_\varphi H \\ \eta = e\left(\mathbf{h}' \cdot (-)\right)_{|G} \end{cases} \right\}.$$

5.4. Application to the discrepancy of the random variables of Chapter 4

Let us recall the setting of Chapter 4. We consider a fixed monic and separable polynomial $g \in \mathbf{Z}[X]$, say of degree $k \geqslant 1$. Denote by Z_g the set of roots of g in $\mathbf{C}$, by $K_g := \mathbf{Q}(\mathrm{Z}_g)$ the splitting field of g, and by $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ the compact group of maps from Z_g to the unit circle $\mathbf{S}^1$. Since the roots of g are all simple, $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ is isomorphic to $\mathbb{T}^k$.
Moreover, we denote by $\mathbf{O}_g$ the ring of integers of K_g. We defined in Definition 4.25 random variables $U_\mathfrak{p}$ for any prime ideal $\mathfrak{p} \subset \mathbf{O}_g$ which does not divide the discriminant of g and which has residual degree 1. Those random variables are defined on the probability space $\mathbf{O}_g/\mathfrak{p}$, with values in $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$. Actually, we also defined analogous random variables $U_{\mathfrak{p}^n}$ on the probability space $\mathbf{O}_g/\mathfrak{p}^n$, but for simplicity of exposition, we will just explain how we can deduce information on the discrepancy in the case $n = 1$.

The motivation for studying this question comes from the striking fact that the sums which appear in the application of Weyl's criterion in the proof of Theorem 4.30 (which states the convergence in law of the random variables $(U_\mathfrak{p})$ as $\|\mathfrak{p}\|$ tends to infinity) are *stationary*. During a seminar in Nancy, G. Tenenbaum suggested to me that this would probably translate into rather strong discrepancy estimates, via the use of the Erdös-Turán inequality or one of its generalizations. In order to achieve that goal, it remains to understand more precisely the rank after which the Weyl sums are stationary. This is the purpose of the following lemma. Recall that a character of the group $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ is of the form

$$\eta_\alpha\colon x \mapsto \prod_{x \in \mathrm{Z}_g} f(x)^{\alpha(x)}$$

for a unique $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$.

Lemma 5.28. *There exists a constant C_g, depending only on the polynomial g, such that for all $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$, if*

$$\|\alpha\|_\infty < C_g \|\mathfrak{p}\|^{\frac{1}{[K_g:\mathbf{Q}]}}$$

and η_α induces a non-trivial character of H_g, then the Weyl sum at rank $\mathfrak{p}$ associated with η_α is equal to zero:

$$\mathbb{E}(\eta_\alpha(U_\mathfrak{p})) = \frac{1}{\|\mathfrak{p}\|} \sum_{a \in \mathbf{O}_g/\mathfrak{p}} e\left(\frac{\tau_\mathfrak{p}(a\varpi_\mathfrak{p}(S_\alpha))}{\|\mathfrak{p}\|} \right) = 0.$$

Proof. Let $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$. The proof of Theorem 4.30 shows that

$$\mathbb{E}(\eta_\alpha(U_\mathfrak{p})) = \begin{cases} 1 & \text{if } S_\alpha \in \mathfrak{p} \\ 0 & \text{otherwise.} \end{cases}$$

If $\mathbb{E}(\eta_\alpha(U_\mathfrak{p})) = 1$, then $S_\alpha \in \mathfrak{p}$, so the ideal $S_\alpha \mathbf{O}_g$ is contained in the ideal $\mathfrak{p}$, hence $\|\mathfrak{p}\|$ divides $\|S_\alpha \mathbf{O}_g\| = \mathrm{N}_{K_g/\mathbf{Q}}(S_\alpha)$. Now, if we further assume that η_α is a *non-trivial* character of H_g, then this is equivalent to assuming that $\alpha \notin \mathrm{R}_g$ thanks to Proposition 4.29. This means that $S_\alpha \neq 0$. This implies that $\mathrm{N}_{K_g/\mathbf{Q}}(S_\alpha)$ is a non-zero integer (because $S_\alpha \in \mathbf{O}_g$) which is divisible by $\|\mathfrak{p}\|$, hence

$$\left|\mathrm{N}_{K_g/\mathbf{Q}}(S_\alpha)\right| \geqslant \|\mathfrak{p}\|. \tag{5.6}$$

On the other hand, we have

$$\begin{aligned}\mathrm{N}_{K_g/\mathbf{Q}}(S_\alpha) &= \prod_{\sigma \in \mathrm{Gal}(K_g/\mathbf{Q})} \sigma(S_\alpha) \\ &= \prod_{\sigma \in \mathrm{Gal}(K_g/\mathbf{Q})} \left(\sum_{x \in \mathrm{Z}_g} \alpha(x)\sigma(x) \right)\end{aligned}$$

Therefore, if we denote by

$$B_g := \prod_{\sigma \in \mathrm{Gal}(K_g/\mathbf{Q})} \max_{x \in \mathrm{Z}_g} |\sigma(x)|,$$

we have:

$$\left|\mathrm{N}_{K_g/\mathbf{Q}}(S_\alpha)\right| \leqslant B_g \left(\sum_{x \in \mathrm{Z}_g} |\alpha(x)| \right)^{[K_g:\mathbf{Q}]} = B_g \|\alpha\|_1^{[K_g:\mathbf{Q}]}.$$

Moreover, $\|\alpha\|_1 \leqslant k\|\alpha\|_\infty$, so that

$$\left|\mathrm{N}_{K_g/\mathbf{Q}}(S_\alpha)\right| \leqslant B_g k^{[K_g:\mathbf{Q}]} \|\alpha\|_\infty^{[K_g:\mathbf{Q}]}. \tag{5.7}$$

Combining (5.6) and (5.7) we deduce that

$$\|\alpha\|_\infty \geqslant \frac{1}{k} \left(\frac{\|\mathfrak{p}\|}{B_g} \right)^{\frac{1}{[K_g:\mathbf{Q}]}}.$$

This proves that there exists a constant $C_g := \frac{1}{k} B_g^{\frac{-1}{[K_g:\mathbf{Q}]}}$, depending only on g, such that for all $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z}) \setminus \mathrm{R}_g$, we have that if $\mathbb{E}(\eta_\alpha(U_\mathfrak{p})) = 1$ then

$$\|\alpha\|_\infty \geqslant C_g \|\mathfrak{p}\|^{\frac{1}{[K_g:\mathbf{Q}]}}.$$

Taking the contrapositive, this means that for all $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$ which does not belong to R_g, we have that if $\|\alpha\|_\infty < C_g \|\mathfrak{p}\|^{\frac{1}{[K_g:\mathbf{Q}]}}$, then $\mathbb{E}(\eta_\alpha(U_\mathfrak{p})) = 0$. □

This lemma gives us an explicit rank (in terms of $\|\alpha\|_\infty$) after which the Weyl sums associated with the character η_α equals 0. It tells us how large $\|\mathfrak{p}\|$ needs to be to have a sum equal to zero.

We now have almost all the tools to prove an estimate of the discrepancy in the equidistribution result of Theorem 4.30, it just remain to give a proper definition of the discrepancy in this setting!

Recall that the sequence $(U_\mathfrak{p})$ of Theorem 4.30 takes values in some closed subgroup H_g of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$. First, we can take an isomorphism between $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ and $(\mathbf{S}^1)^k$ (just by choosing an ordering of the roots of g), and so we can view H_g as a closed subgroup of $(\mathbf{S}^1)^k$. Moreover, we can just focus on the fractional parts of the arguments inside of the exponentials, and study their distribution rather than that of their image under the map e. This way, we can view the random variables $U_\mathfrak{p}$ as random variables taking values in a closed subgroup of $\mathbb{T} = \mathbf{R}/\mathbf{Z}$. Therefore, there exists an isomorphism of topological groups

$$\varphi \colon \mathrm{H}_g \to \mathbb{T}^d \times F$$

with $d \geqslant k = \deg(g)$ and F a finite abelian group. As we did in the previous sections, we then define a notion of φ-discrepancy which depends on the choice of such an isomorphism.

Definition 5.29. *We define the φ-discrepancy of the sequence $(U_{\mathfrak{p}})$ at rank $\mathfrak{p}$ as*

$$D_{\mathfrak{p}}^{\varphi} := \sup_{\substack{I\in\mathscr{I}_d\\ y\in F}} \left| \frac{\#\{a\in \mathbf{O}_g/\mathfrak{p},\ \varphi(U_{\mathfrak{p}}(a))\in I\times\{y\}\}}{\|\mathfrak{p}\|} - \frac{\lambda_d(I)}{|F|}\right|$$

where, as before, $\mathscr{I}_d$ denotes the set of rectangles of $\mathbb{T}^d$.

Combining the Erdös-Turán-Koksma type inequality of Theorem 5.17 with Lemma 5.28, we obtain the following upper bound for the discrepancy:

Theorem 5.30. *With the notations of the previous definition, we have:*

$$D_{\mathfrak{p}}^{\varphi} \ll_{g,\varphi} \frac{1}{\|\mathfrak{p}\|^{\frac{1}{[K_g:\mathbf{Q}]}}}$$

Proof. Thanks to Theorem 5.17, we have that for all $H\geqslant 1$, for all $\mathfrak{p}$ unramified of residual degree 1 in $\mathbf{O}_g$,

$$\begin{aligned} D_{\mathfrak{p}}^{\varphi} &\leqslant \left(\frac{3}{2}\right)^d \left(\frac{2}{H+1} + \frac{1}{|F|} \sum_{\chi\in\left(\widehat{\mathrm{H}_g}\right)_{C_\varphi H}} \frac{1}{r\left(\widehat{\varphi}^{-1}(\chi)\right)} \left| \frac{1}{\|\mathfrak{p}\|} \sum_{a\in\mathbf{O}_g/\mathfrak{p}} \chi(U_{\mathfrak{p}}(a))\right| \right) \\ &= \left(\frac{3}{2}\right)^d \left(\frac{2}{H+1} + \frac{1}{|F|} \sum_{\chi\in\left(\widehat{\mathrm{H}_g}\right)_{C_\varphi H}} \frac{1}{r\left(\widehat{\varphi}^{-1}(\chi)\right)} \left|\mathbb{E}\left(\chi(U_{\mathfrak{p}})\right)\right| \right) \end{aligned}$$

where

$$\left(\widehat{\mathrm{H}_g}\right)_{C_\varphi H} := \left\{ \chi\in\widehat{\mathrm{H}_g}\setminus\{1\} \ \middle|\ \exists \alpha\in \mathrm{C}(\mathrm{Z}_g,\mathbf{Z}),\quad \begin{cases} \|\alpha\|_\infty \leqslant C_\varphi H \\ \chi = (\eta_\alpha)_{|\mathrm{H}_g} \end{cases} \right\}.$$

Now, we are enclined by Lemma 5.28 to choose

$$H := \frac{C_g \|\mathfrak{p}\|^{\frac{1}{[K_g:\mathbf{Q}]}}}{C_\varphi} - 1.$$

Indeed, this ensures that all characters of H_g taken into account in the sum on the RHS are restrictions to H_g of some characters η_α associated with α's such that $\|\alpha\|_\infty < C_g \|\mathfrak{p}\|^{\frac{1}{[K_g:\mathbf{Q}]}}$. Therefore, by Lemma 5.28, the whole sum is equal to zero since $\mathbb{E}_{\mathfrak{p}}(\chi(U_{\mathfrak{p}})) = 0$ for all such χ.
Thus, we obtain the upper bound

$$D_{\mathfrak{p}}^{\varphi} \leqslant \left(\frac{3}{2}\right)^d \frac{2}{H+1} = \left(\frac{3}{2}\right)^d \frac{2C_\varphi}{C_g \|\mathfrak{p}\|^{\frac{1}{[K_g:\mathbf{Q}]}}}$$

In other words, once we fix an isomorphism $\varphi\colon \mathrm{H}_g \to \mathbb{T}^d\times F$, we have

$$D_{\mathfrak{p}}^{\varphi} \ll_{g,\varphi} \frac{1}{\|\mathfrak{p}\|^{\frac{1}{[K_g:\mathbf{Q}]}}}.$$

□

Remark 5.31. It is a bit disappointing that we could not obtain an upper bound for a certain notion of discrepancy which does not depend on the choice of an isomorphism between H_g and some $\mathbb{T}^d\oplus F$. However, it seems difficult with our approach to obtain a constant C_φ independent of φ in Corollary 5.26. Indeed, it seems to me that a linear map which induces an isomorphism between a closed subgroup G of $\mathbb{T}^k$ and $\mathbb{T}^d\oplus F$ can have arbitrarily large operator norm.

Chapter 6

Ultra-short sums of trace functions

The aim of this chapter is to give a detailed exposition of the results of Section 7 of the joint work [77] with E. Kowalski. These results concern short sums of trace functions of ℓ-adic sheaves on the affine line over a finite field. After a short section on short sums of multiplicative characters, which motivates the study of more general functions "of algebraic nature" defined on finite fields, the necessary background on trace functions is introduced in Section 6.2. Following the survey articles on the subject by Fouvry, Kowalski, Michel and Sawin, we define trace functions using the point of view of Galois representations, so that no prior knowledge on sheaves or ℓ-adic cohomology is needed. We use as a blackbox the Riemann hypothesis of Deligne, building on previous works on sums of products of trace functions, which determined concrete conditions on the Galois representations which ensure that it can be applied.

Contents

6.1. Motivation: sums of multiplicative characters

Let $g \in \mathbf{Z}[X]$ be a monic and separable polynomial. In Chapter 4 we presented equidistribution results for sums of additive characters of the type

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{ax}{q}\right).$$

parametrized by $a \in \mathbf{F}_q$. Or, in other words, for the family of sums

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \psi(x)$$

parametrized by *additive characters* $\psi \in \widehat{\mathbf{F}_q}$. In this short section, we explain how the method of proof can be adapted to prove equidistribution results for families of sums of the type

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \chi(x)$$

parametrized by *multiplicative characters* modulo q. More generally, we will be interested in the distribution of sums of the form

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \chi(v(x))$$

where χ is a varying multiplicative character of $\mathbf{F}_q$ and v is a fixed polynomial. In order to evaluate χ at $v(x)$ (at least for all q large enough), we add the assumption that $v(x) \neq 0$ for all $x \in \mathrm{Z}_g$. For instance, in the case where $v = X$, this amounts to requiring that $0 \notin \mathrm{Z}_g$.
For $\mathfrak{p} \in \mathcal{S}_g$, we now introduce the probability space $X_\mathfrak{p}$ of multiplicative characters $\chi\colon (\mathbf{O}_g/\mathfrak{p})^\times \to \mathbf{S}^1$, with the uniform probability measure. On this probability space, we will consider the random variables $\widetilde{U}_\mathfrak{p}$, taking values in the group $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$, and defined by

$$\widetilde{U}_\mathfrak{p}(\chi)(x) = \chi(v(\varpi_\mathfrak{p}(x))).$$

Proposition 6.1. *The random variables $\widetilde{U}_\mathfrak{p}$ converge in law as $\|\mathfrak{p}\| \to +\infty$ to the random function $\widetilde{U}\colon \mathrm{Z}_g \to \mathbf{S}^1$ such that $\widetilde{U}$ is uniformly distributed on the subgroup $\widetilde{\mathrm{H}}_{g,v} \subset \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ which is orthogonal to the abelian group $\widetilde{\mathrm{R}}_{g,v} \subset \mathrm{C}(\mathrm{Z}_g; \mathbf{Z})$ of multiplicative relations between values of v on Z_g, namely we have*

$$\widetilde{\mathrm{R}}_{g,v} = \{\alpha\colon \mathrm{Z}_g \to \mathbf{Z} \mid \prod_{x \in \mathrm{Z}_g} v(x)^{\alpha(x)} = 1\},$$

and

$$\widetilde{\mathrm{H}}_{g,v} = \{f \in \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1) \mid \text{ for all } \alpha \in \widetilde{\mathrm{R}}_{g,v}, \text{ we have } \prod_{x \in \mathrm{Z}_g} f(x)^{\alpha(x)} = 1\}.$$

In particular, as $q \to +\infty$ among primes totally split in K_g, the sums

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \chi(v(x))$$

converge in law to the image by the linear form σ of the Haar probability measure on $\widetilde{\mathrm{H}}_{g,v}$.

Proof. This is very close to the proof of Theorem 4.30, except that now

$$\mathbb{E}(\eta(\widetilde{U}_\mathfrak{p})) = \frac{1}{\|\mathfrak{p}\| - 1} \sum_{\chi \in X_\mathfrak{p}} \prod_{x \in \mathrm{Z}_g} \chi(v(\varpi_\mathfrak{p}(x)))^{\alpha(x)}$$

for a character η of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$ determined by the function α. This is

$$\mathbb{E}(\eta(\widetilde{U}_\mathfrak{p})) = \frac{1}{\|\mathfrak{p}\| - 1} \sum_{\chi \in X_\mathfrak{p}} \chi\Big(\varpi_\mathfrak{p}\Big(\prod_{x \in \mathrm{Z}_g} v(x)^{\alpha(x)}\Big)\Big)$$

and for the same reasons as before, if $\|\mathfrak{p}\|$ is large enough, $\varpi_\mathfrak{p}\Big(\prod_{x \in \mathrm{Z}_g} v(x)^{\alpha(x)}\Big)$ equals 1 if and only if $\prod_{x \in \mathrm{Z}_g} v(x)^{\alpha(x)}$ equals 1. Thus, by orthogonality of the multiplicative characters of $\mathbf{O}_g/\mathfrak{p}$, as soon as $\|\mathfrak{p}\|$ is large enough we have that $\mathbb{E}(\eta(\widetilde{U}_\mathfrak{p}))$ equals 1 if $\alpha \in \widetilde{\mathrm{R}}_{g,v}$ and equals 0 otherwise. Since *non-trivial* characters of $\widetilde{\mathrm{H}}_{g,v}$ correspond to $\alpha \notin \widetilde{\mathrm{R}}_{g,v}$, this finishes the proof thanks to Weyl's criterion. □

Example 6.2. (1) For $v = X$, the group $\mathrm{R}_{g,v}$ is simply the group of multiplicative relations between the roots of g. This group has already been studied in the literature. For instance, there are some interesting examples of applications in [71] and [74]. Another example which has been investigated in detail is that of the explicit polynomial g with Galois group the Weyl group of $\mathbf{E}_8$, which is of degree 240 but has all roots obtained multiplicatively from 8 of them (see [56]).
(2) For $v = X$ again, the case of $g = X^d - 1$ is quite degenerate. Indeed, for $q \equiv 1 \pmod{d}$ and a multiplicative character χ of $\mathbf{F}_q$, the sum

$$\sum_{x \in \mu_d(\mathbf{F}_q)} \chi(x)$$

is either d or 0, depending on whether the character χ is trivial on the d-th roots of unity or not. The former means that $\chi^{(q-1)/d} = 1$, and there are therefore $(q-1)/d$ such characters. Hence the sum is equal to d with probability $1/d$, and to 0 with probability $1 - 1/d$.
(3) If we consider the Hilbert class polynomial for elliptic curves with CM (as in Section 4.3.6), we are led to consider potential multiplicative relations between j-invariants. This seems to be a much more challenging problem than the additive case, and we do not have a precise answer at the moment (see, e.g., the papers of Bilu, Luca and Pizarro-Madariaga [7] and Fowler [42] for partial results).

So far, we proved equidistribution results for ultra-short sums of the form

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} t_q(x)$$

for some functions $t_q \colon \mathbf{F}_q \to \mathbf{C}$ which had an algebraic nature (since they were additive of multiplicative characters). More examples of functions $\mathbf{F}_q \to \mathbf{C}$ of algebraic nature come from the theory of trace functions, a theory originally developed by Grothendieck and Deligne, which relies on the very deep formalism of ℓ-adic sheaves with respect to the étale topology. Thanks to the work of Katz and Laumon, and then Fouvry, Kowalski, Michel and Sawin, this formalism has been made more accessible, and for many applications to analytic number theory, the deepest results can be used as blackboxes. In the next section, we give a survey of the main facts one needs to work with trace functions.

6.2. An introduction to the theory of trace functions

6.2.1. The projective line over a field

Let us first recall some terminology from algebraic geometry. If A is a commutative ring, we denote by $\mathrm{Spec}(A)$ the set of prime ideals of A (i.e. ideals $\mathfrak{p}$ of A, not equal to A, such that the quotient $A/\mathfrak{p}$ is an integral domain).
For any ideal I of A, we denote by

$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(A);\ I \subseteq \mathfrak{p}\}.$$

By abuse of notation, if $I = (f)$ is a principal ideal, we denote $V(f)$ for $V(I)$. We also introduce the notation

$$D(f) := \mathrm{Spec}(A) \setminus V(f).$$

It can be shown that there exists a unique topology on $\mathrm{Spec}(A)$ such that the $V(I)$ form the family of closed sets. It is called the *Zariski topology*, and the $D(f)$ for $f \in A$ form a basis of open sets for this topology.

Example 6.3. If k is a field and $A = k[T]$, then $\mathrm{Spec}(A)$ consists of the zero ideal, which is a dense point for the Zariski topology and is called the generic point, and all the non-zero prime ideals, which are principal ideals of the form (π), where π is a monic irreducible polynomial with coefficients in k. These ideals being maximal, they are closed points of $\mathrm{Spec}(A)$. We can speak of the degree of a closed point by defining it as the degree of the extension $k[T]/(\pi)$, that is: the degree of the corresponding irreducible polynomial.

Definition 6.4. *We denote by* $\mathbf{A}^1_k$ *the topological space* $\mathrm{Spec}(k[T])$. *It is called the affine line over* k.

The above construction gives a way to associate to any commutative ring A a topological space, namely $\mathrm{Spec}(A)$. Now, to define a functor from the category of commutative rings to the category of topological spaces, we also need to associate to any ring homomorphism between two rings a continuous map between the corresponding topological spaces. It is done as follows: if $\phi\colon A \to B$ is a ring homomorphism, then we define

$$\begin{array}{ccccc} \mathrm{Spec}(\phi) & : & \mathrm{Spec}(B) & \to & \mathrm{Spec}(A) \\ & & \mathfrak{p} & \mapsto & \phi^{-1}(\mathfrak{p}) \end{array}$$

It can be checked that this map is continuous with respect to the Zariski topology, so that Spec defines a contravariant functor from the category of commutative rings to the category of topological spaces.

Example 6.5. if $S \subset A$ is a multiplicative set, one can build the localization of A with respect to S. It is a ring denoted by $S^{-1}A$ where we can make sense of fractions whose denominator belong to S. We have a canonical homomorphism $\phi\colon A \to S^{-1}A$, defined by $a \mapsto \frac{a}{1}$. Then $\mathrm{Spec}(\phi)$ is a homeomorphism from $\mathrm{Spec}(S^{-1}A)$ to $\{\mathfrak{p} \in \mathrm{Spec}(A);\ \mathfrak{p} \cap S = \emptyset\}$.
For instance, if $f \in A$ is not nilpotent and we take S to be $\{f^n;\ n \geqslant 0\}$, then $S^{-1}A$ is usually denoted by A_f and one can show that the map $\mathrm{Spec}(\phi)$ from above induces a homeomorphism between $\mathrm{Spec}(A_f)$ and $D(f)$, which is an elementary open subset of $\mathrm{Spec}(A)$ (thus, the terminology "localization" is well-suited).

Remark 6.6. Actually, the functor Spec as we defined it is not completely satisfactory, because many commutative rings have homeomorphic spectra. For instance, all fields correspond to the same topological space: the one with only one point. Indeed, they only admit $\{0\}$ as a prime ideal. To define a topological object which allows to distinguish between non-isomorphic commutative rings, one needs to add some extra-structure on $\mathrm{Spec}(A)$. Namely, one can endow it with a sheaf of rings $\mathcal{O}_{\mathrm{Spec}(A)}$ such that the stalk at each point is a local ring. With this structure of locally ringed topological space, $\mathrm{Spec}(A)$ becomes what is called an *affine scheme*, and this time the functor between the category of commutative rings to the category of affine schemes is an equivalence of categories. Although the structure sheaf is a very important part of the theory, we will not mention it in the sequel, and focus only on the topological part.

Let k be a field. We are going to define the projective line over k (as a topological space, without mentioning the whole scheme structure) $\mathbf{P}^1_k$ by glueing two copies of the affine line $\mathbf{A}^1_k = \mathrm{Spec}(k[T])$. To distinguish the two copies, we will denote them by $X = \mathrm{Spec}(k[x])$ and $Y = \mathrm{Spec}(k[y])$. We will glue them along the following glueing data: the open subsets are $U := D(x) \subset X$ and $V = D(y) \subset Y$ and the isomorphisms between U and V are the ones induced by the isomorphism of k-algebras

$$\begin{array}{ccc} k[x, x^{-1}] & \to & k[y, y^{-1}] \\ x & \mapsto & y^{-1} \\ x^{-1} & \mapsto & y \end{array}$$

Indeed, $D(x)$ is canonically homeomorphic to $\mathrm{Spec}(k[x]_x)$ (the spectrum of the localization of $k[x]$ with respect to the multiplicative set $\{x^n;\ n \geqslant 0\}$), and we have that $k[x]_x = k[x, x^{-1}]$, and similarly for $D(y)$.

Note that $D(x) = X \setminus \{(x)\}$ since $V(x) = \{\mathfrak{p} \in \mathrm{Spec}(k[x]);\ (x) \subseteq \mathfrak{p}\} = \{(x)\}$ because (x) is a maximal ideal. Therefore, the glueing is done on very large open sets: X and Y are identified along isomorphisms everywhere except at one point for each, which remain distinguishable.

Now, the points of degree 1 of X are in bijection with k, by associating with any $a \in k$ the degree one irreducible polynomial $x - a$. This is why we allow ourselves to denote by 0 the point (x) of X. We also denote by ∞ the point (y) of Y. This terminology is justified since everywhere outside of these two points, y is identified with $1/x$.

But the thing is that with this new abstract notion of point, the projective line $\mathbf{P}^1_k$ contains many more points that the points of degree 1. Indeed, the copy of $X = \mathrm{Spec}(k[x])$ inside $\mathbf{P}^1_k$ admits all the non-zero prime ideals (π) (generated by a monic irreducible polynomial $\pi \in k[x]$) as closed points. Thus, we can think of the closed points of X as classes of equivalence of valuations on $k(x)$: the ideal (π) corresponds to the (class of equivalence of the) valuation v_π on $k(x)$ defined by

$$v_\pi\left(\pi^n g(x)\right) = n$$

for all $g \in k[x]$ coprime with π, and extended to $k(x)$ by defining $v_\pi(f/g) = v_\pi(f) - v_\pi(g)$. The corresponding valuation ring is

$$\mathcal{O}_\pi := \left\{\frac{f}{g};\ f, g \in k[x],\ \pi \nmid g\right\},$$

its unique maximal ideal is

$$\mathfrak{p}_\pi := \left\{\frac{f}{g};\ f, g \in k[x],\ \pi \nmid g \text{ and } \pi \mid f\right\}$$

and the residue field $\kappa_\pi := \mathcal{O}_\pi/\mathfrak{p}_\pi$ is isomorphic to $k[x]/(\pi)$, which is a finite extension of k of degree $\deg(\pi)$.
Moreover, there is also the point ∞ coming from the other copy Y of $\mathbf{A}^1_k$, which corresponds to the ideal (y) of $k[y]$. Since y was identified with $1/x$ at all the other points, it is natural to define the corresponding valuation v_∞ as the valuation on $k(x)$ given by

$$v_\infty(f/g) = \deg(g) - \deg(f).$$

Its valuation ring is

$$\mathcal{O}_\infty := \left\{\frac{f}{g};\ f, g \in k[x], \deg(f) \leqslant \deg(g)\right\},$$

its unique maximal ideal is

$$\mathfrak{p}_\infty = \left\{\frac{f}{g};\ f, g \in k[x], \deg(f) < \deg(g)\right\}$$

and the residue field κ_∞ is isomorphic to k.

Definition 6.7. *Given a Zariski open subset $U \subseteq \mathbf{P}^1_k$, we denote by $U(k)$ the set of closed points of degree 1 of U. For instance, if $U \subseteq \mathbf{P}^1_k \setminus \{\infty\} = \mathbf{A}^1_k = \mathrm{Spec}(k[X])$, then $U(k)$ is the set of $x \in k$ such that the ideal generated by the polynomial $X - x$ belongs to U.*

6.2.2. Decomposition group and inertia subgroup at a point

Now, we let k be a finite field $\mathbf{F}_q$ for a prime number q. We define $K := \mathbf{F}_q(X)$, and we fix K^{sep} a separable closure of K which contains the algebraic closure $\overline{\mathbf{F}}_q$ of $\mathbf{F}_q$. The most appropriate setting to define trace functions is that of ℓ-adic sheaves with respect to the étale topology, but these notions are far beyond the understanding of the author. Quite conveniently, in some cases these objects have a more concrete interpretation in terms of Galois representations, so we will follow this path, guided by the survey papers [37, 39]. The reference [36] also helped the author's understanding.

More precisely, we will be interested in representations of the absolute Galois group of K: the group $\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$, which is defined as for finite extensions as the group of K-algebra automorphisms of K^{sep}. If we denote by Λ the set of finite Galois extensions L/K contained in K^{sep}, then their Galois groups together with the natural restriction maps allow us to define an inverse system of finite groups. One can then take the limit of this inverse system, and there is the natural restriction homomorphism

$$\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right) \to \varprojlim_{L \in \Lambda} \mathrm{Gal}\left(L/K\right)$$

which turns out to be an isomorphism. Therefore, any $\sigma \in \mathrm{Gal}\,(K^{\mathrm{sep}}/K)$ corresponds to a unique element

$$(\sigma_L)_{L\in\Lambda} \in \prod_{L\in\Lambda} \mathrm{Gal}\,(L/K)$$

which is compatible with the restriction maps, in the sense that whenever $L, M \in \Lambda$ and $L \subseteq M$, then the restriction of σ_M to L equals σ_L. It can be shown that $\mathrm{Gal}\,(K^{\mathrm{sep}}/K)$ inherits a topology from this isomorphism, which is called the Krull topology, and with respect to which it is a compact Hausdorff space. A basis of neighbourhoods of the identity is given by the subsets $\mathrm{Gal}\,(K^{\mathrm{sep}}/L)$ for $L \in \Lambda$, so that we can say that $\sigma, \tau \in \mathrm{Gal}\,(K^{\mathrm{sep}}/K)$ are close if and only if they coincide on a large finite Galois extension L/K. We refer to [87, Chapter IV] for a complete yet concise introduction to infinite Galois theory and profinite groups.

Given a closed point x in $\mathbf{P}^1_{\mathbf{F}_q}$ (which can be viewed an an equivalence class of valuations on K), we now wish to define two subgroups (defined up to conjugation) of $\mathrm{Gal}\,(K^{\mathrm{sep}}/K)$: the decomposition group at x and the inertia subgroup at x. We first define them on finite Galois extensions, before passing to the limit.

So let $L \in \Lambda$ and let $v_{x,L}$ be a valuation on L which extends the valuation v_x on K corresponding to the point $x \in \mathbf{P}^1_{\mathbf{F}_q}$. We can define the *decomposition group* at x as the following subgroup of $\mathrm{Gal}\,(L/K)$:

$$D_{x,L} := \{\sigma \in \mathrm{Gal}\,(L/K) \mid \ v_{x,L} \circ \sigma = v_{x,L}\ \}$$

Note that the choice of another extension $\widetilde{v}_{x,L}$ of v_x to L defines another decomposition group $\widetilde{D}_{x,L}$, but they belong to the same conjugacy class of $\mathrm{Gal}\,(L/K)$. This easily follows from the fact that $\mathrm{Gal}\,(L/K)$ acts transitively on the set of valuations which extend v_x to L (for a proof of this fact, see [87, Chapter II, §9]). Indeed, if $\sigma \in \mathrm{Gal}\,(L/K)$ is such that $\widetilde{v}_{x,L} = v_{x,L} \circ \sigma$, then we have $\widetilde{D}_{x,L} = \sigma^{-1} D_{x,L} \sigma$.

Now, once we fix a choice of $v_{x,L}$, we can define as usual the corresponding ring of integers

$$\mathcal{O}_{x,L} := \{f \in L \ \mid \ v_{x,L}(f) \geqslant 0\}$$

which has maximal ideal

$$\mathfrak{p}_{x,L} := \{f \in L \ \mid \ v_{x,L}(f) > 0\}$$

and residue field $\kappa_{x,L} := \mathcal{O}_{x,L}/\mathfrak{p}_{x,L}$. By definition, any $\sigma \in D_{x,L}$ preserves $\mathcal{O}_{x,L}$ and $\mathfrak{p}_{x,L}$, hence induces an automorphism $\overline{\sigma} \in \mathrm{Gal}\,(\kappa_{x,L}/\kappa_x)$. The *inertia subgroup* at x is defined as the kernel of the group homomorphism

$$\begin{array}{ccc} D_{x,L} & \to & \mathrm{Gal}\,(\kappa_{x,L}/\kappa_x) \\ \sigma & \mapsto & \overline{\sigma} \end{array}$$

In other words, we have

$$I_{x,L} := \{\sigma \in D_{x,L} \ \mid \text{ for all } f \in \mathcal{O}_{x,L},\ \sigma(f) \equiv f \,(\mathrm{mod}\, \mathfrak{p}_{x,L})\}$$

It is also easy to show that another choice of a valuation $\widetilde{v}_{x,L}$ gives an inertia subgroup $\widetilde{I}_{x,L}$ which is Galois conjugate to $I_{x,L}$. Indeed, if $\sigma \in \mathrm{Gal}\,(L/K)$ is such that $\widetilde{v}_{x,L} = v_{x,L} \circ \sigma$, then $\widetilde{I}_{x,L} = \sigma^{-1} I_{x,L} \sigma$. To sum up, we have the exact sequence

$$1 \to I_{x,L} \to D_{x,L} \to \mathrm{Gal}\,(\kappa_{x,L}/\kappa_x) \to 1. \tag{6.1}$$

Note that $\kappa_{x,L}/\kappa_x$ is a finite extension of a finite field, so $\mathrm{Gal}\,(\kappa_{x,L}/\kappa_x)$ is generated by the Frobenius automorphism:

$$u \mapsto u^{|\kappa_x|}.$$

Now, using Zorn's lemma, one can show that it is possible to make compatible choices of valuations $v_{x,L}$ for all $L \in \Lambda$, in the sense that if $L \subseteq M$, then the restriction of $v_{x,M}$ to L must be equal to $v_{x,L}$. This essentially amounts to construct a valuation $v_{\{x\}}$ on K^{sep} which extends v_x. Once we have made

these compatible choices of extended valuations, we can "pass to the limit" in (6.1), and the sequence remains exact thanks to [87, Chapter IV, Proposition (2.7)]:

$$1 \to \varprojlim_{L\in\Lambda} I_{x,L} \to \varprojlim_{L\in\Lambda} D_{x,L} \to \varprojlim_{L\in\Lambda} \mathrm{Gal}\left(\kappa_{x,L}/\kappa_x\right) \overset{(\star)}{\simeq} \mathrm{Gal}\left(\overline{\mathbf{F}}_q/\kappa_x\right) \to 1.$$

Remark 6.8. The isomorphism $(\star)$ is not an obvious fact, as it does not only rely on the fact that finite Galois extensions of the residue field κ_x are in one to one correspondence with finite unramified Galois extensions of the original field, see e.g. [17, Theorem 1 p.26 and the next corollary]. Indeed, this fact only applies to *complete* valued fields. Therefore, one actually needs to first view κ_x as the residue field of the completion $\widehat{K}$ of K at the place v_x, and then to deduce that for any finite extension λ/κ_x, there exists a finite unramified Galois extension $\widehat{L}/\widehat{K}$ with residue field isomorphic to λ thanks to *loc. cit.* Finally, one needs to explain that $\widehat{L}$ is actually the completion of a finite Galois extension L/K with respect to a valuation which extends v_x. This is a consequence of Krasner's lemma, see for instance [100, Corollary 11.19] in the section entitled "local extensions come from global extensions".

In view of the canonical isomorphism induced by the restriction map between $\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$ and $\varprojlim_{L\in\Lambda} \mathrm{Gal}\left(L/K\right)$, this tells us that if we define the decomposition group at x as

$$D_{\{x\}} := \left\{\sigma \in \mathrm{Gal}\left(K^{\mathrm{sep}}/K\right) \;\middle|\; \text{for all } L \in \Lambda,\ \sigma_{|L} \in D_{x,L}\right\}$$

and its inertia subgroup at x as follows:

$$I_{\{x\}} := \left\{\sigma \in \mathrm{Gal}\left(K^{\mathrm{sep}}/K\right) \;\middle|\; \text{for all } L \in \Lambda,\ \sigma_{|L} \in I_{x,L}\right\},$$

then they fit in the exact sequence

$$1 \to I_{\{x\}} \to D_{\{x\}} \to \mathrm{Gal}\left(\overline{\mathbf{F}}_q/\kappa_x\right) \to 1. \tag{6.2}$$

The *arithmetic Frobenius* of $\mathrm{Gal}\left(\overline{\mathbf{F}}_q/\kappa_x\right)$

$$\begin{array}{rccc} \mathrm{Frob}_{\kappa_x}^{\mathrm{arith}} & : & \overline{\mathbf{F}}_q & \to & \overline{\mathbf{F}}_q \\ & & u & \mapsto & u^{|\kappa_x|} \end{array}$$

satisfies that for all finite extension λ/κ_x, its restriction to λ is the Frobenius automorphism of $\mathrm{Gal}\left(\lambda/\kappa_x\right)$. We will rather work with the inverse of the arithmetic Frobenius:

Definition 6.9. *The inverse of* $\mathrm{Frob}_{\kappa_x}^{\mathrm{arith}}$ *is called the geometric Frobenius at* x*, and is denoted by* $\mathrm{Frob}_{\kappa_x}^{\mathrm{geom}}$.

Thanks to the exact sequence (6.2), we have that $D_{\{x\}}/I_{\{x\}} \simeq \mathrm{Gal}\left(\overline{\mathbf{F}}_q/\kappa_x\right)$, so that $\mathrm{Frob}_{\kappa_x}^{\mathrm{geom}}$ can be lifted to $D_{\{x\}}$ in several manners which differ by elements of $I_{\{x\}}$:

Definition 6.10. *We denote by* $\mathrm{Frob}_{\{x\}}$ *the left* $I_{\{x\}}$*-class of* $D_{\{x\}}$ *which corresponds to* $\mathrm{Frob}_{\kappa_x}^{\mathrm{geom}}$.

If we made another choice of a compatible system of valuations extending v_x to all finite Galois extensions of K, we would have defined another (possibly different) extension of v_x to K^{sep}. But as $\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$ acts transitively on the extensions of v_x to K^{sep} (see [87, Chapter II, Theorem 9.1]), all the objects $D_{\{x\}'}, I_{\{x\}'}$ and $\mathrm{Frob}_{\{x\}'}$ arising from this other construction would be $\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$-conjugates of $D_{\{x\}}, I_{\{x\}}$ and $\mathrm{Frob}_{\{x\}}$.

6.2.3. ℓ-adic Galois representations and their trace functions

Before speaking about ℓ-adic representations, let us introduce some vocabulary about representations of $\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$ in general, where $K := \mathbf{F}_q(X)$ as above. Given a representation

$$\rho\colon \mathrm{Gal}\left(K^{\mathrm{sep}}/K\right) \to \mathrm{GL}(V)$$

where V is a finite dimensional L-vector space for some arbitrary field L, we denote by

$$V^{I_{\{x\}}} := \left\{ v \in V \mid \rho(\sigma)(v) = v \text{ for all } \sigma \in I_{\{x\}} \right\}$$

the linear subspace of $I_{\{x\}}$-invariant vectors. One can show that this subspace is stable under the action of $D_{\{x\}}$ (this uses the fact that $I_{\{x\}}$ is a normal subgroup of $D_{\{x\}}$). Therefore, for any $\sigma \in D_{\{x\}}$, it makes sense to speak about the automorphism $\left(\sigma \mid V^{I_{\{x\}}}\right)$ which is induced by the action of $\rho(\sigma)$ on $V^{I_{\{x\}}}$.
Besides, if $\sigma' = \sigma \circ i$ for some $i \in I_{\{x\}}$, then by definition of $V^{I_{\{x\}}}$, we have

$$\left(\sigma' \mid V^{I_{\{x\}}}\right) = \left(\sigma \mid V^{I_{\{x\}}}\right)$$

Therefore, even though $\mathrm{Frob}_{\{x\}}$ is only defined up to an element of $I_{\{x\}}$, it makes sense to speak about *the* automorphism $\left(\mathrm{Frob}_{\{x\}} \mid V^{I_{\{x\}}}\right)$ induced on $V^{I_{\{x\}}}$. Finally, if we made another choice of extension of the valuation v_x to a valuation on K^{sep}, the corresponding groups $D_{\{x\}'}$ and $I_{\{x\}'}$ would be $\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$-conjugates to $D_{\{x\}}$ and $I_{\{x\}}$, which implies that

$$\mathrm{Tr}\left(\mathrm{Frob}_{\{x\}} \mid V^{I_{\{x\}}}\right) = \mathrm{Tr}\left(\mathrm{Frob}_{\{x\}'} \mid V^{I_{\{x\}'}}\right).$$

We refer to [36, Lemma 2.1.5] for more detailed proofs.

Definition 6.11 (Unramified representation)**.** *Given a representation $\rho\colon \mathrm{Gal}\left(K^{\mathrm{sep}}/K\right) \to \mathrm{GL}(V)$ as above and a closed point $x \in \mathbf{P}^1_{\mathbf{F}_q}$, we say that ρ is unramified (or lisse) at x if the inertia subgroup $I_{\{x\}}$ acts trivially on V (that is: if $V^{I_{\{x\}}} = V$).*
On the other hand, a point where ρ is ramified is called a singularity, and we will denote by $\mathrm{Sing}(\rho)$ the set of ramified points.

We can now turn our attention to a specific kind of representations, where V carries a topology and continuity plays a role in the definitions. Fix a prime number $\ell \neq q$, and an algebraic closure $\overline{\mathbf{Q}}_\ell$ of the field of ℓ-adic numbers. Even though the following definitions only use the language of representations, we will name the objects "ℓ-adic sheaves" to be consistent with the literature (we proceed as in [39]).

Definition 6.12 (ℓ-adic middle-extension sheaves)**.**

- *Let $U \subseteq \mathbf{P}^1_{\mathbf{F}_q}$ be a non-empty open subset. An ℓ-adic Galois representation lisse on U is a representation $(V_{\mathcal{F}}, \rho_{\mathcal{F}})$, where $V_{\mathcal{F}}$ is a finite dimensional $\overline{\mathbf{Q}}_\ell$-vector space and*

$$\rho_{\mathcal{F}}\colon \mathrm{Gal}\left(K^{\mathrm{sep}}/K\right) \to \mathrm{GL}(V_{\mathcal{F}})$$

  is a continuous representation of $\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$ which is unramified at every closed point $x \in U$. The dimension of $V_{\mathcal{F}}$ is called the rank of $\mathcal{F}$ and is denoted by $\mathrm{rk}(\mathcal{F})$.

- *An ℓ-adic middle extension sheaf is an ℓ-adic Galois representation $(V_{\mathcal{F}}, \rho_{\mathcal{F}})$ as above such that $\mathrm{Sing}(\rho_{\mathcal{F}})$ is finite. In other words, $(V_{\mathcal{F}}, \rho_{\mathcal{F}})$ must be unramified at all but finitely many points.*

Sometimes we will just say ℓ-adic sheaf to be brief, but we will only consider ℓ-adic middle-extension sheaves in the sense of the previous definition in this thesis.

Note that in this definition, the continuity of $\rho_{\mathcal{F}}$ refers to the profinite topology on the infinite Galois group $\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$ and to the unique normed vector space topology on the finite dimensional $\overline{\mathbf{Q}}_\ell$-vector space $\mathrm{GL}(V_{\mathcal{F}})$. We can finally state the definition of the trace function associated with an ℓ-adic sheaf. Recall that an element $x \in \mathbf{F}_q$ can be viewed as closed point of $\mathbf{P}^1_{\mathbf{F}_q}$ by identifying it with the ideal of $\mathbf{F}_q[X]$ generated by the irreducible degree 1 polynomial $X - x$ (see Definition 6.7, where we also introduce the notation $U(\mathbf{F}_q)$ for the closed points of degree 1 in a certain open subset U of $\mathbf{P}^1_{\mathbf{F}_q}$).

Definition 6.13. *Given an ℓ-adic sheaf lisse on U as in the previous definition, we define its associated trace function as the following map*

$$\begin{array}{rccc} t_{\mathcal{F}} & : & \mathbf{F}_q & \to & \overline{\mathbf{Q}}_\ell \\ & & x & \mapsto & \mathrm{Tr}\left(\mathrm{Frob}_{\{x\}} \mid V_{\mathcal{F}}^{I_{\{x\}}}\right) \end{array}$$

Remark 6.14. Actually, some references only define $t_{\mathcal{F}}$ on lisse points, that is: on $U(\mathbf{F}_q)$ and not on all $\mathbf{A}^1(\mathbf{F}_q) \simeq \mathbf{F}_q$. For a lisse point $x \in U(\mathbf{F}_q)$, we have that $I_{\{x\}}$ acts trivially on $V_{\mathcal{F}}$, so that $V_{\mathcal{F}}^{I_{\{x\}}} = V_{\mathcal{F}}$. Then the value of the trace function at x is defined as

$$\mathrm{Tr}\left(\mathrm{Frob}_{\{x\}} \mid V\right).$$

There are several possibilities to extend $t_{\mathcal{F}}$ to all $\mathbf{F}_q$. The choice we made in the previous definition is probably the most common, but for instance in [39, Remark 3.7] the simplest extension (extending by 0 outside of the lisse points) is also said to work for many analytic purposes.

Remark 6.15. From now on, we assume that we have fixed a field isomorphism $\iota\colon \overline{\mathbf{Q}}_\ell \to \mathbf{C}$ (the existence of such an isomorphism depends on the axiom of choice). This allows us to view trace functions as complex-valued functions (which is necessary if we want to say that additive and multiplicative characters are instances of trace functions). The fact that we are considering representations over $\overline{\mathbf{Q}}_\ell$ rather than $\mathbf{C}$ is crucial for the theory, and comes from their different topological nature, but the relevance of this choice will not appear clearly in this Chapter, as we are going to admit without proof some difficult statements.

6.2.4. Operations on trace functions

Classical transformations on representations can be applied to our specific kind of representations, and we will be interested in the effect of these operations on the attached trace functions. We just give some useful examples, which form a strict subset of the set of examples provided in [39].

Given two ℓ-adic sheaves $\mathcal{F}$ and $\mathcal{G}$ as in Definition 6.12, one can form:

- the direct sum sheaf $\mathcal{F} \oplus \mathcal{G}$, which is just defined as the usual direct sum of the corresponding representations $(V_{\mathcal{F}}, \rho_{\mathcal{F}})$ and $(V_{\mathcal{G}}, \rho_{\mathcal{G}})$. If $\mathcal{F}$ is lisse on U and $\mathcal{G}$ is lisse on U', then $\mathcal{F} \oplus \mathcal{G}$ is lisse at least on $U \cap U'$. Moreover, the rank of $\mathcal{F} \oplus \mathcal{G}$ equals the sum of the ranks, and on $U(\mathbf{F}_q) \cap U'(\mathbf{F}_q)$, we have
$$t_{\mathcal{F}\oplus\mathcal{G}}(x) = t_{\mathcal{F}}(x) + t_{\mathcal{G}}(x).$$
- the tensor product sheaf $\mathcal{F} \otimes \mathcal{G}$, which is defined as the usual tensor product of the representations $(V_{\mathcal{F}}, \rho_{\mathcal{F}})$ and $(V_{\mathcal{G}}, \rho_{\mathcal{G}})$. As in the previous case, this sheaf is lisse at least on $U \cap U'$, its rank is the product of the ranks, and on $U(\mathbf{F}_q) \cap U'(\mathbf{F}_q)$ we have
$$t_{\mathcal{F}\otimes\mathcal{G}}(x) = t_{\mathcal{F}}(x) t_{\mathcal{G}}(x).$$
- If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_q)$, then the map $x \mapsto \frac{ax+b}{cx+d}$ defines an automorphism of $\mathbf{P}^1(\mathbf{F}_q)$. Now if $\mathcal{F}$ is a lisse ℓ-adic sheaf on $\mathbf{P}^1_{\mathbf{F}_q}$, there is a construction of a *pullback sheaf* $[\gamma]^*\mathcal{F}$, whose trace function is given by
$$t_{[\gamma]^*\mathcal{F}}(x) = t_{\mathcal{F}}\left(\frac{ax+b}{cx+d}\right).$$
In particular, if $\gamma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, we will denote by $[+b]$ the corresponding automorphism of $\mathbf{P}^1(\mathbf{F}_q)$ and by $[+b]^*\mathcal{F}$ the corresponding pullback sheaf, which has trace function equal to $x \mapsto t_{\mathcal{F}}(x+b)$. Similarly, if $\gamma = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, we denote by $[\times a]$ the corresponding automorphism. The pullback sheaf $[\times a]^*\mathcal{F}$ then has trace function equal to $x \mapsto t_{\mathcal{F}}(ax)$.

We can also speak of isomorphic sheaves just by defining this notion as the isomorphism of the corresponding representations. Similarly, we can speak of irreducible representations (representations with no non-trivial subrepresentations) and isotypic representations (representations with all irreducible subrepresentations being isomorphic). For all these notions, we can add the word "geometric" before, and this will mean that we are restricting our representations to the geometric Galois group $\mathrm{Gal}\left(K^{\mathrm{sep}}/\overline{\mathbf{F}}_q(X)\right)$ (which is a subgroup of $\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$).

Definition 6.16.

- *We will say that two sheaves $\mathcal{F}$ and $\mathcal{G}$ are geometrically isomorphic if the corresponding representations $(V_{\mathcal{F}}, \rho_{\mathcal{F}})$ and $(V_{\mathcal{G}}, \rho_{\mathcal{G}})$ are isomorphic as representations of* $\mathrm{Gal}\left(K^{\mathrm{sep}}/\overline{\mathbf{F}}_q(X)\right)$.
- *We will say that a sheaf $\mathcal{F}$ is geometrically irreducible (reps. geometrically isotypic) if the corresponding representation is irreducible (resp. isotypic) as a representation of* $\mathrm{Gal}\left(K^{\mathrm{sep}}/\overline{\mathbf{F}}_q(X)\right)$.

6.2.5. Purity

We now turn to the important notion of weight of an ℓ-adic sheaf, which is an assumption concerning the modulus of the eigenvalues of the Frobenius automorphisms.

Definition 6.17. *Let $w \in \mathbf{Z}$. Let $\mathcal{F}$ be an ℓ-adic sheaf as in Definition 6.12, lisse on $U \subseteq \mathbf{P}^1_{\mathbf{F}_q}$. We say that $\mathcal{F}$ is pure of weight w if for all $x \in U$, the eigenvalues of $\left(\mathrm{Frob}_{\{x\}} \mid V_{\mathcal{F}}\right)$ are complex numbers of modulus $|\kappa_x|^{w/2}$.*

Let us stress that the eigenvalues of $\left(\mathrm{Frob}_{\{x\}} \mid V_{\mathcal{F}}\right)$ are the eigenvalues of $\rho_{\mathcal{F}}\left(\mathrm{Frob}_{\{x\}}\right) \in \mathrm{GL}(V_{\mathcal{F}})$, which is an automorphism of a $\overline{\mathbf{Q}}_\ell$-vector space. Therefore, they belong to $\overline{\mathbf{Q}}_\ell$, but when we speak of them as complex numbers of modulus $|\kappa_x|^{w/2}$, what we really mean is that there image under our fixed isomorphism $\iota\colon \overline{\mathbf{Q}}_\ell \to \mathbf{C}$ are such complex numbers. To be completely rigorous, we should speak about ι-pure sheaves of weight w.

Even though the definition only takes into account the unramified points, Deligne proved that the weights of the Frobenius eigenvalues at ramified points is well-controlled by the weights at the unramified points. Namely (see [39, Remark 3.12]): if $\mathcal{F}$ is an ℓ-adic sheaf lisse on U which is pure of weight w, then for any closed point $x \in \mathbf{P}^1_{\mathbf{F}_q}$, the eigenvalues of $\left(\mathrm{Frob}_{\{x\}} \mid V^{I_{\{x\}}}\right)$ have modulus less than or equal to $|\kappa_x|^{w/2}$.

6.2.6. Measuring the complexity of trace functions

Given a trace function, there are possibly many ℓ-adic representations which give the same trace functions. However, we would like to have a way to speak of the "simplest" representation giving rise to this given trace function. In order to do that, we need to define a quantity which measures the complexity of an ℓ-adic sheaf. It is the notion of *conductor* of a trace function, in the sense of Fouvry-Kowalski-Michel.

A first naive way to measure the complexity of a representation is its rank, but it turns out that this is not the suitable notion in applications. One also needs to take into account the number of singular points, which is assumed to be finite in our definition of an ℓ-adic middle extension sheaf (Definition 6.12). However, these two notions do not suffice, and there is a last quantity involved which is rather difficult to define: that of the Swan conductor $\mathrm{Swan}_x(\mathcal{F})$ at a singular point x. We will not define it (as I acknowledge not knowing the precise definition) but let us just say that it measures how wild is the ramification. As in the context of local fields, we can speak of tamely ramified points, as opposed to wildly ramified points, and the Swan conductor can be thought of as an analogue of the jumps in the ramification filtration of a local field. We refer to [65] for a complete introduction. Even though their definition is difficult, Swan conductors at singular points have been computed for many sheaves of interest in applications, so we have explicit values of the conductor of those sheaves, that can be used as blackboxes.

Definition 6.18 (Conductor of a trace function, see [38])**.** *Given an ℓ-adic middle-extension sheaf $\mathcal{F}$ on $\mathbf{P}^1_{\mathbf{F}_q}$, we define its conductor as:*

$$c(\mathcal{F}) := \mathrm{rk}(\mathcal{F}) + |\mathrm{Sing}(\rho_{\mathcal{F}})| + \sum_{x \in \mathrm{Sing}(\mathcal{F})} \mathrm{Swan}_x(\mathcal{F}).$$

6.2.7. Bounding trace functions

To prove uniform distribution results, we often need to bound exponential sums, and so we would like to have good upper bounds for the modulus of those very general exponential sums that arise as sums of trace functions. The best known general results follow from the Riemann hypothesis for varieties defined over finite fields, which is due to Deligne. This theorem involves very deep cohomological techniques that I am far from understanding, so let me just give some key steps which will hopefully explain the type of assumptions on $\mathcal{F}$ that are needed in order to apply the Riemann hypothesis.

The first step is the following cohomological interpretation of a sum of values of a trace function:

Theorem 6.19 (Grothendieck-Lefschetz trace formula, see e.g. [39, Theorem 4.1]). *Let $\mathcal{F}$ be an ℓ-adic sheaf lisse on $U \subseteq \mathbf{P}^1_{\mathbf{F}_q}$. There exists three finite dimensional ℓ-adic representations of $\mathrm{Gal}\left(\overline{\mathbf{F}}_q/\mathbf{F}_q\right)$:*

$$\mathrm{Gal}\left(\overline{\mathbf{F}}_q/\mathbf{F}_q\right) \to H^i_c(U \times \overline{\mathbf{F}}_q, \mathcal{F})$$

such that

$$\sum_{x \in U(\mathbf{F}_q)} t_{\mathcal{F}}(x) = \sum_{i=0}^{2} (-1)^i \mathrm{Tr}\left(\mathrm{Frob}_q \;\middle|\; H^i_c(U \times \overline{\mathbf{F}}_q, \mathcal{F})\right)$$

where Frob_q denotes the geometric Frobenius of $\mathrm{Gal}\left(\overline{\mathbf{F}}_q/\mathbf{F}_q\right)$.

The $\overline{\mathbf{Q}}_\ell$-vector spaces $H^i_c(U \times \overline{\mathbf{F}}_q, \mathcal{F})$ are called compactly supported étale cohomology groups, and as far as I understand, it is often easier in applications to understand the ones corresponding to $i = 0$ and $i = 2$. Indeed, as soon as $U \neq \mathbf{P}^1_{\mathbf{F}_q}$, we have $H^0_c(U \times \overline{\mathbf{F}}_q, \mathcal{F}) = 0$. Moreover, if $\mathcal{F}$ is geometrically irreducible or geometrically isotypic (with underlying geometrically irreducible representation being non-trivial) then we also have $H^2_c(U \times \overline{\mathbf{F}}_q, \mathcal{F}) = 0$ (see e.g. [39, §4.1] for statements of those facts). For instance, if we consider ℓ-adic sheaves on the affine line $\mathbf{A}^1_{\mathbf{F}_q}$ which are geometrically irreducible, then we are just left with one term in the Grothendieck-Lefschetz trace formula:

$$\sum_{x \in U(\mathbf{F}_q)} t_{\mathcal{F}}(x) = -\mathrm{Tr}\left(\mathrm{Frob}_q \;\middle|\; H^1_c(U \times \overline{\mathbf{F}}_q, \mathcal{F})\right).$$

Now, to estimate the term on the right-hand side, one needs to understand the dimension of the $\overline{\mathbf{Q}}_\ell$-vector space $H^1_c(U \times \overline{\mathbf{F}}_q, \mathcal{F})$ and the modulus of the eigenvalues of the geometric Frobenius acting on that space. The dimension can actually be bounded in terms of the conductor, see e.g. [39, §4.1]:

$$\sum_{i=0}^{2} \dim H^i_c(U \times \overline{\mathbf{F}}_q, \mathcal{F}) \ll c(\mathcal{F})^2.$$

However, the question of the size of the eigenvalues of the Frobenius is what is at the heart of the Riemann hypothesis, and required a tremendous amount of work to be fully proved.

Theorem 6.20 (Deligne, [26]). *If $\mathcal{F}$ is pure of weight 0, then the eigenvalues of Frob_q acting on $H^1_c(U \times \overline{\mathbf{F}}_q, \mathcal{F})$ are complex number of modulus $\leqslant \sqrt{q}$.*

All this sketchy discussion leads us to the following very concrete form of the Riemann hypothesis, which is applicable to our trace functions:

Corollary 6.21 (Applying the Riemann hypothesis to trace functions, [39, Corollary 4.7]). *Assume that $\mathcal{F}$ is an ℓ-adic middle extension sheaf lisse on $U \subset \mathbf{P}^1_{\mathbf{F}_q}$ (with $U \neq \mathbf{P}^1_{\mathbf{F}_q}$) which is pure of weight 0. Assume that $\mathcal{F}$ is geometrically isotypic (with underlying geometrically irreducible representation being non-trivial[1]), then*

$$\left|\sum_{x \in U(\mathbf{F}_q)} t_{\mathcal{F}}(x)\right| \ll c(\mathcal{F})^2 \sqrt{q}.$$

[1] meaning that there must not exist a 1 dimensional linear subspace V of $V_{\mathcal{F}}$ such that for all $\sigma \in \mathrm{Gal}\left(K^{\mathrm{sep}}/\overline{\mathbf{F}}_q(X)\right)$, $\rho_{\mathcal{F}}(\sigma)$ acts as the identity on V.

Remark 6.22. (1) Let us stress that the assumption "geometrically isotypic with no trivial component" is crucial to ensure the vanishing of the second étale cohomology group $H^2_c(U \times \overline{\mathbf{F}}_q, \mathcal{F})$. This type of assumption will play an important role in the main result of this Chapter (Theorem 6.27).

(2) Actually the isotypic assumption is not very restrictive, because any trace function can be decomposed as a sum of trace functions of geometrically isotypic sheaves. This is not at all obvious, as the representations involved are not necessarily arithmetically semi-simple (i.e. semi-simple as representations of $\mathrm{Gal}\,(K^{\mathrm{sep}}/K)$), but Deligne proved that they are *geometrically* semi-simple. Concretely, we can use the following consequence:

Proposition 6.23 ([39, Proposition 5.1]). *Let $\mathcal{F}$ be an ℓ-adic sheaf lisse on $U \subseteq \mathbf{P}^1_{\mathbf{F}_q}$ and pure of weight 0. Then there exist ℓ-adic sheaves $(\mathcal{F}_i)_{1\leqslant i\leqslant N}$, lisse on I, pure of weight 0, geometrically isotypic, such that*

- *$N \leqslant c(\mathcal{F})$,*
- *$c(\mathcal{F}_i) \leqslant c(\mathcal{F})$ for all $1 \leqslant i \leqslant N$,*
- *for all $x \in U(\mathbf{F}_q)$,*

$$t_{\mathcal{F}}(x) = \sum_{i=1}^{N} t_{\mathcal{F}_i}(x).$$

Thanks to this decomposition, in order to apply the Riemann hypothesis to $\mathcal{F}$, it suffices to check that the the geometric representation $\rho_{\mathcal{F}}$, i.e. the representation $\rho_{\mathcal{F}}$ viewed as a representation of $\mathrm{Gal}\,\big(\mathbf{F}_q(X)^{\mathrm{sep}}/\overline{\mathbf{F}}_q(X)\big)$, does not admit a geometrically irreducible subrepresentation which is the trivial one.

6.2.8. Additive and multiplicative characters as trace functions

Let us explain that this deep algebraic formalism actually encompasses the concrete examples of "functions $\mathbf{F}_q^{\times} \to \mathbf{C}$ of algebraic nature" that we already encountered, namely additive and multiplicative characters.

Artin-Schreier sheaf. Given an additive character $\psi\colon \mathbf{F}_q \to \mathbf{C}$, one can show that there exists an ℓ-adic middle extension sheaf $\mathcal{L}_\psi$, called an Artin-Schreier sheaf, with the following properties:

- $\mathrm{rk}(\mathcal{L}_\psi) = 1$,
- $\mathcal{L}_\psi$ is lisse on $\mathbf{P}^1_{\mathbf{F}_q} \setminus \{\infty\} = \mathbf{A}^1_{\mathbf{F}_q}$,
- $\mathcal{L}_\psi$ is pure of weight 0,
- $c(\mathcal{L}_\psi) = 3$ (the Swan conductor at ∞ is equal to 1),
- For all $x \in \mathbf{F}_q^{\times}$, $t_{\mathcal{L}_\psi}(x) = \psi(x)$.

Kummer sheaf. Given a multiplicative character $\chi\colon \mathbf{F}_q^{\times} \to \mathbf{C}$, it can be proved that there exists an ℓ-adic middle extension sheaf $\mathcal{L}_\chi$, called a Kummer sheaf, such that

- $\mathrm{rk}(\mathcal{L}_\chi) = 1$,
- $\mathcal{L}_\chi$ is lisse on $\mathbf{P}^1_{\mathbf{F}_q} \setminus \{0, \infty\}$,
- $\mathcal{L}_\chi$ is pure of weight 0,
- $c(\mathcal{L}_\chi) = 3$ (the Swan conductor at the two ramified points is equal to 0),
- For all $x \in \mathbf{F}_q^{\times}$, $t_{\mathcal{L}_\chi}(x) = \chi(x)$.

We refer to [54, Theorem 11.34] for a sketch of the proof of the existence of a rank 1 sheaf with the right trace function (without the computation of the conductor).

6.2.9. Monodromy groups

We have seen that if $\mathcal{F}$ is a middle-extension ℓ-adic sheaf lisse on some open subset $U \subseteq \mathbf{P}^1_{\mathbf{F}_q}$, then to any closed point $x \in U$ we can associate a Frobenius automorphism

$$\rho_{\mathcal{F}}(\mathrm{Frob}_{\{x\}}) = (\mathrm{Frob}_{\{x\}} \ \mid \ V_{\mathcal{F}}) \in \mathrm{GL}(V_{\mathcal{F}}).$$

Since different choices of extensions of valuations lead to different elements $\mathrm{Frob}_{\{x\}} \in \mathrm{Gal}\,(K^{\mathrm{sep}}/K)$, but all those elements are conjugates inside $\mathrm{Gal}\,(K^{\mathrm{sep}}/K)$, the conjugacy class of $\rho_{\mathcal{F}}(\mathrm{Frob}_{\{x\}})$ inside $\mathrm{GL}(V_{\mathcal{F}})$ does not depend on any choice. Thus, for all such x, we have a well defined element $\rho_{\mathcal{F}}(\mathrm{Frob}_{\{x\}}) \in \mathrm{GL}(V_{\mathcal{F}})^\sharp$. After taking an arbitrary basis of $V_{\mathcal{F}}$, we can identify $\rho_{\mathcal{F}}(\mathrm{Frob}_{\{x\}})$ with a conjugacy class in $\mathrm{GL}_r(\overline{\mathbf{Q}}_\ell)$. Finally, using our isomorphism $\iota\colon \overline{\mathbf{Q}}_\ell \to \mathbf{C}$, we can speak of the Frobenius conjugacy class $\iota(\rho_{\mathcal{F}}(\mathrm{Frob}_{\{x\}})) \in \mathrm{GL}_r(\mathbf{C})^\sharp$.

The work of Deligne and Katz allowed for major breakthroughs in the understanding of the distribution of trace functions. The main point is that they rather studied the uniform distribution of these conjugacy classes $\iota(\rho_{\mathcal{F}}(\mathrm{Frob}_{\{x\}}))$ inside $\mathrm{GL}_r(\mathbf{C})^\sharp$, before applying the trace and obtain as a corollary the uniform distribution of the trace functions. But there is actually one last subtlety that we did not talk about: it is the fact that the suitable space of conjugacy classes is not simply $\mathrm{GL}_r(\mathbf{C})^\sharp$, but rather the space of conjugacy classes of a maximal compact subgroup inside what is called the *monodromy group* associated with the sheaf $\mathcal{F}$. We now define these groups.

Definition 6.24. *let $\mathcal{F}$ be an ℓ-adic middle-extension sheaf on $\mathbf{P}^1_{\mathbf{F}_q}$, pure of weight 0. Recall that we denoted by $K := \mathbf{F}_q(X)$.*

- *The arithmetic monodromy group of $\mathcal{F}$ is the Zariski closure of $\iota(\rho_{\mathcal{F}}\,(\mathrm{Gal}\,(K^{\mathrm{sep}}/K)))$ inside $\mathrm{GL}_r(\mathbf{C})$.*
- *The geometric monodromy group of $\mathcal{F}$ is the Zariski closure of $\iota(\rho_{\mathcal{F}}(\mathrm{Gal}\,(K^{\mathrm{sep}}/\overline{\mathbf{F}}_q(X))))$ inside $\mathrm{GL}_r(\mathbf{C})$.*

They are respectively denoted by $G_{\mathcal{F},\mathrm{arith}}(\mathbf{C})$ and $G_{\mathcal{F},\mathrm{geom}}(\mathbf{C})$ and satisfy $G_{\mathcal{F},\mathrm{geom}}(\mathbf{C}) \subseteq G_{\mathcal{F},\mathrm{arith}}(\mathbf{C})$.

Let us explain what is the meaning of Zariski closure in this setting: there is a topology on $\mathbf{C}^{r^2+1}$ whose closed sets are those of the form

$$V(S) := \left\{((m_{i,j})_{1\leqslant i,j\leqslant r}, y) \in \mathbf{C}^{r^2+1} \ \mid \ \text{for all } f \in S,\ f\left((m_{i,j})_{1\leqslant i,j\leqslant r}, y\right) = 0\right\}$$

for subsets S of the polynomial ring $\mathbf{C}\left[(X_{i,j})_{1\leqslant i,j\leqslant r}, Y\right]$. We call this topology the Zariski topology, and $\mathrm{GL}_r(\mathbf{C})$ can be seen as a closed subset $\mathbf{C}^{r^2+1}$ via the map

$$\begin{array}{ccc} \mathrm{GL}_r(\mathbf{C}) & \to & \mathbf{C}^{r^2+1} \\ M = (m_{i,j}) & \mapsto & \left((m_{i,j})_{1\leqslant i,j\leqslant r}, \frac{1}{\det(M)}\right) \end{array}$$

which identifies $\mathrm{GL}_r(\mathbf{C})$ with the Zariski-closed subset $V(\{f\})$ where

$$f((X_{i,j})_{1\leqslant i,j\leqslant r}, Y) := \det((X_{i,j})_{1\leqslant i,j\leqslant r})Y - 1.$$

Therefore, we can speak of the Zariski topology on $\mathrm{GL}_r(\mathbf{C})$, whose closed sets are those given by polynomial equations via the embedding of $\mathrm{GL}_r(\mathbf{C})$ in $\mathbf{C}^{r^2+1}$. Then, the monodromy groups defined above are Zariski closures, meaning that they are the smallest Zariski closed subsets containing respectively $\iota(\rho_{\mathcal{F}}\,(\mathrm{Gal}\,(K^{\mathrm{sep}}/K)))$ and $\iota(\rho_{\mathcal{F}}\left(\mathrm{Gal}\left(K^{\mathrm{sep}}/\overline{\mathbf{F}}_q(X)\right)\right))$. As such, they are *linear algebraic groups* because they are subgroups of $\mathrm{GL}_r(\mathbf{C})$ *given by polynomial equations*. We refer to [74, §7.1] for a concise introduction to linear algebraic groups.

Remark 6.25. There is a different topology on $\mathrm{GL}_r(\mathbf{C})$ which is also called the Zariski topology: it is defined by viewing $\mathrm{GL}_r(\mathbf{C})$ as an open subset of $\mathbf{C}^{r^2}$, namely the set of points where the determinant is non-zero. However, it is not this Zariski topology that is used in the context of linear algebraic groups, because the matrix inversion is not a polynomial map if we make this choice instead of the one above.

In general, the determination of the monodromy group is a difficult problem. In many cases of interest in analytic number theory however, Katz determined the monodromy groups in several books (e.g. [59, 60, 61, 62]). His work provides many examples where the equidistribution of the Frobenius conjugacy classes is well-understood, and gives as corollaries beautiful equidistribution results regarding concrete trace functions.

6.3. Uniform distribution results for sums of trace functions over the roots of a fixed polynomial

Let us fix for all this section $g \in \mathbf{Z}[X]$ a monic and separable polynomial. We keep the notations $K_g, \mathbf{O}_g, \mathcal{S}_g$ from Chapter 4. In the latter, we studied exponential sums of the form

$$\sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} e\left(\frac{\tau_{\mathfrak{p}}(ax)}{\|\mathfrak{p}\|}\right)$$

where $\tau_{\mathfrak{p}}$ is just the inverse of the canonical isomorphism between $\mathbf{Z}/\|\mathfrak{p}\|\mathbf{Z}$ and $\mathbf{O}_g/\mathfrak{p}$ when $\mathfrak{p} \in \mathcal{S}_g$. On the other hand, in Section 6.1 we showed that the same techniques lead to equidistribution results for sums of the form

$$\sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} \chi(x)$$

where χ is a varying character of the multiplicative group $(\mathbf{O}_g/\mathfrak{p})^\times$. Thanks to Section 6.2.8, we see that we dealt with two instances of sums of trace functions over roots of a polynomial. Thus, it is natural to try to see whether similar results can be obtained for sums of the form

$$\sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} t_{\mathfrak{p}}(ax), \qquad \text{or} \qquad \sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} t_{\mathfrak{p}}(a+x),$$

(or other similar expressions) when $t_{\mathfrak{p}}$ is, for each $\mathfrak{p} \in \mathcal{S}_g$, a trace function over the finite field $\mathbf{O}_g/\mathfrak{p}$.

6.3.1. Definition of the unitary random variables

We thus assume that for each $\mathfrak{p} \in \mathcal{S}_g$, we are given an ℓ-adic middle-extension sheaf $\mathcal{F}_{\mathfrak{p}}$ on the affine line over $\mathbf{O}_g/\mathfrak{p}$. We assume that these sheaves are pure of weight 0, and have the same rank r, and moreover have bounded conductor in the sense of Definition 6.18. We also assume that they have the same geometric monodromy group, and that the arithmetic and the geometric monodromy groups are equal. Since we make this assumption, we can drop the subscript $\mathcal{F}_{\mathfrak{p}}$ in the notation of the monodromy groups, and just denote them as

$$G_{\mathrm{arith}}(\mathbf{C}) \quad \text{and} \quad G_{\mathrm{geom}}(\mathbf{C})$$

which are to be understood as the *common* monodromy groups of the sheaves $\mathcal{F}_{\mathfrak{p}}$.

Let $x \in \mathbf{O}_g/\mathfrak{p}$ be such that $\mathcal{F}_{\mathfrak{p}}$ is lisse at x. Then by definition, $\iota(\rho_{\mathcal{F}_{\mathfrak{p}}}(\mathrm{Frob}_{\{x\}})) \in G_{\mathrm{arith}}(\mathbf{C})$, and its conjugacy class only depends on x. Thanks to the assumption that the arithmetic and the geometric monodromy groups coincide, we can associate with x a unique conjugacy class $\vartheta_{\mathfrak{p}}(x) \in G_{\mathrm{geom}}(\mathbf{C})^\sharp$. It is represented by a matrix whose eigenvalues are all complex numbers of modulus 1 (due to the assumption that our sheaves are pure of weight 0). It can be shown in this context of linear algebraic groups that this matrix admits a Jordan-Chevalley multiplicative decomposition, so it may be written as a product of a diagonalizable matrix $\vartheta_{\mathfrak{p}}(x)^{\mathrm{ss}}$ (called the semi-simple part) by a unipotent one.

Since the eigenvalues have modulus 1, we can say that the semi-simple part $\vartheta_{\mathfrak{p}}(x)^{\mathrm{ss}}$ belongs to a certain compact subgroup of $G_{\mathrm{geom}}(\mathbf{C})$. But any such subgroup is $G_{\mathrm{geom}}(\mathbf{C})$-conjugate to a maximal compact subgroup, say $K_{\mathrm{geom}}(\mathbf{C})$. Therefore, we can associate to any $x \in \mathbf{O}_g/\mathfrak{p}$ such that $\mathcal{F}_{\mathfrak{p}}$ is lisse at x a unitary matrix which we denote by $\Theta_{\mathfrak{p}}(x) \in K_{\mathrm{geom}}(\mathbf{C})$, which is $G_{\mathrm{geom}}(\mathbf{C})$-conjugate to the semi-simple

part of the Frobenius automorphism $\iota(\rho_{\mathcal{F}_\mathfrak{p}}(\mathrm{Frob}_{\{x\}}))$.

If another choice of extension of valuation was made and led us to define $\mathrm{Frob}_{\{x\}'}$ instead of $\mathrm{Frob}_{\{x\}}$, then we have seen that these two automorphisms are $\mathrm{Gal}\,(K^{\mathrm{sep}}/K)$-conjugates, so that their images via the representation $\rho_{\mathcal{F}_\mathfrak{p}}$ and the isomorphism ι are two matrices which are $G_{\mathrm{geom}}(\mathbf{C})$-conjugates. However, it is not straightforward that when we find an element of $K_{\mathrm{geom}}(\mathbf{C})$ in the $G_{\mathrm{geom}}(\mathbf{C})$-conjugacy class of their semi-simple part, we obtain two elements of $K_{\mathrm{geom}}(\mathbf{C})$ which are $K_{\mathrm{geom}}(\mathbf{C})$-conjugates and not only $G_{\mathrm{geom}}(\mathbf{C})$-conjugates. It turns out that this is true, as explained in [63, §9.2.4]. This relies on the fact that $K_{\mathrm{geom}}(\mathbf{C})$-conjugacy classes are separated by the traces of finite dimensional representations of $K_{\mathrm{geom}}(\mathbf{C})$ (a consequence of the Peter-Weyl theorem) and that such representations of $K_{\mathrm{geom}}(\mathbf{C})$ are restrictions of representations of the whole algebraic group $G_{\mathrm{geom}}(\mathbf{C})$.

Thus, any $x \in \mathbf{O}_g/\mathfrak{p}$ such that $\mathcal{F}_\mathfrak{p}$ is lisse at x defines properly an element of $K_{\mathrm{geom}}(\mathbf{C})^\sharp$, which we still denote by $\Theta_\mathfrak{p}(x)$. Since we will be interested in sums of (additive or multiplicative) shifts, we need to be cautious with the fact that those shifts might reach non-lisse points. That is why we introduce the following sets:

$$A_\mathfrak{p} := \left\{a \in (\mathbf{O}_g/\mathfrak{p})^\times \;\middle|\; \text{for all } x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}),\ \mathcal{F}_\mathfrak{p} \text{ is lisse at } ax\right\}$$
$$B_\mathfrak{p} := \left\{a \in \mathbf{O}_g/\mathfrak{p} \;\middle|\; \text{for all } x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p}),\ \mathcal{F}_\mathfrak{p} \text{ is lisse at } a+x\right\}$$

Note that we always have $|B_\mathfrak{p}| \gg \|\mathfrak{p}\|$, and that if we further assume that $0 \notin \mathrm{Z}_g$, then we also have $|A_\mathfrak{p}| \gg \|\mathfrak{p}\|$.

Definition 6.26 (Unitary random variables)**.** *For $\mathfrak{p} \in \mathcal{S}_g$, we define random variables $U_\mathfrak{p}$ and $V_\mathfrak{p}$ on $A_\mathfrak{p}$ and $B_\mathfrak{p}$ respectively (with uniform probability measure), with values in the space $\mathrm{C}\left(\mathrm{Z}_g, K_{\mathrm{geom}}(\mathbf{C})^\sharp\right)$, by*

$$U_\mathfrak{p}(a)(x) = \Theta_\mathfrak{p}(ax), \qquad V_\mathfrak{p}(a)(x) = \Theta_\mathfrak{p}(a+x),$$

where $x \in \mathrm{Z}_g$ is viewed as an element of $\mathbf{O}_g/\mathfrak{p}$ through the canonical projection $\varpi_\mathfrak{p}$.

Note that this definition is a quite natural extension of Definition 4.25: in both cases we are viewing the terms of our exponential sums of interest as traces of certain "random" unitary elements, except that in Definition 4.25 we had 1×1 matrices, so we did not need to take the trace.

More precisely, since the trace function $t_\mathfrak{p}$ of $\mathcal{F}_\mathfrak{p}$ satisfies

$$t_\mathfrak{p}(x) = \mathrm{Tr}(\Theta_\mathfrak{p}(x))$$

for x lisse, we see that if one can prove that $(U_\mathfrak{p})$ and/or $(V_\mathfrak{p})$ has a limit, then the sums

$$\sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} t_\mathfrak{p}(ax), \qquad \text{and/or} \qquad \sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} t_\mathfrak{p}(a+x),$$

for a varying inn $A_\mathfrak{p}$ (respectively $B_\mathfrak{p}$) will become equidistributed according to the image of this limit distribution by the map

$$f \mapsto \sum_{x \in \mathrm{Z}_g} \mathrm{Tr}(f(x))$$

for $f\colon \mathrm{Z}_g \to K_{\mathrm{geom}}(\mathbf{C})^\sharp$.

6.3.2. Convergence in law of the unitary random variables

We will see that the proof of the uniform distribution of the random variables of Definition 6.26 relies a lot on estimates of "sums of products" of trace functions, which have been the object of a deep study in the article [38] by Fouvry, Kowalski and Michel. Relying on their notion of *bountiful* sheaves, we will prove the following (concrete examples of trace functions coming from bountiful sheaves will be given in the next section):

Theorem 6.27 ([77, Proposition 7.1]). *Assume that for all $\mathfrak{p} \in \mathcal{S}_g$, we are given an ℓ-adic middle-extension sheaf $\mathcal{F}_\mathfrak{p}$ on the affine line over the finite field $\mathbf{O}_g/\mathfrak{p}$. Assume that these sheaves all have the same rank r, are pure of weight 0, have the same geometric monodromy group $G_{\mathrm{geom}}(\mathbf{C})$, and that it coincides with their arithmetic monodromy group. Assume further that $\mathcal{F}_\mathfrak{p}$ is bountiful in the sense of [38] for all $\mathfrak{p}$ in $\mathcal{S}_g$ and that the conductor of $\mathcal{F}_\mathfrak{p}$ is bounded independently of $\mathfrak{p}$. Then:*
(1) *If $G_{\mathrm{geom}}(\mathbf{C}) = \mathrm{Sp}_r(\mathbf{C})$ then $(U_\mathfrak{p})$ and $(V_\mathfrak{p})$ converge in law as $\|\mathfrak{p}\| \to +\infty$, with limit uniform on $\mathrm{C}(\mathrm{Z}_g; \mathrm{USp}_r(\mathbf{C})^\sharp)$.*
(2) *If $G_{\mathrm{geom}}(\mathbf{C}) = \mathrm{SL}_r(\mathbf{C})$, and the special involution, if it exists, is not $y \mapsto -y$, then $(U_\mathfrak{p})$ and $(V_\mathfrak{p})$ converge in law with limit uniform on $\mathrm{C}(\mathrm{Z}_g; \mathrm{SU}_r(\mathbf{C})^\sharp)$.*
(3) *If $G_{\mathrm{geom}}(\mathbf{C}) = \mathrm{SL}_r(\mathbf{C})$ and $\mathcal{F}_\mathfrak{p}$ has special involution $y \mapsto -y$ for all $\mathfrak{p}$, then $(V_\mathfrak{p})$ converges in law as $\|\mathfrak{p}\| \to +\infty$ with limit uniform on $\mathrm{C}(\mathrm{Z}_g; \mathrm{SU}_r(\mathbf{C})^\sharp)$, and $(U_\mathfrak{p})$ converges in law with limit uniform on*

$$\{f\colon \mathrm{Z}_g \to \mathrm{SU}_r(\mathbf{C})^\sharp \mid f(x) = \overline{f(y)} \text{ if } x = -y\}.$$

In all cases, the convergence of $(V_\mathfrak{p})$ holds without additional assumptions, while for $(U_\mathfrak{p})$ we assume that $0 \notin \mathrm{Z}_g$.

Proof of (1). We argue with $U_\mathfrak{p}$, as the case of $V_\mathfrak{p}$ is identical (one just needs to replace $[\times x]$ by $[+x]$ in the pullback sheaves below). By definition, the random variables $U_\mathfrak{p}$ take values in $\mathrm{C}\left(\mathrm{Z}_g, K_{\mathrm{geom}}(\mathbf{C})^\sharp\right)$, where $K_{\mathrm{geom}}(\mathbf{C})^\sharp$ is the space of conjugacy classes of a maximal compact subgroup $K_{\mathrm{geom}}(\mathbf{C})$ of the common geometric monodromy group $G_{\mathrm{geom}}(\mathbf{C})$ of the sheaves $\mathcal{F}_\mathfrak{p}$. Here, since we assume that the sheaves are of Sp_r-type, we have that

$$G_{\mathrm{geom}}(\mathbf{C}) = \mathrm{Sp}_r(\mathbf{C})$$

and a maximal compact subgroup is given by

$$K_{\mathrm{geom}}(\mathbf{C}) = \mathrm{USp}_r(\mathbf{C}) (= \mathrm{Sp}_r(\mathbf{C}) \cap \mathrm{U}_r(\mathbf{C})).$$

By definition of convergence in law, we want to show that for any continuous central function $f\colon \mathrm{C}\left(\mathrm{Z}_g, \mathrm{USp}_r(\mathbf{C})\right) \to \mathbf{C}$, we have

$$\frac{1}{|A_\mathfrak{p}|} \sum_{a \in A_\mathfrak{p}} f(U_\mathfrak{p}(a)) \underset{\|\mathfrak{p}\| \to +\infty}{\longrightarrow} \int_{\mathrm{USp}_r(\mathbf{C})} f \mathrm{d}\mu$$

where μ denotes the Haar probability measure on the compact group $\mathrm{USp}_r(\mathbf{C})$. Thanks to Peter-Weyl theorem (and in particular its consequence in the form of [96, Appendix A.1, Cor. 1]), it suffices to show that if $(\pi_x)_{x \in \mathrm{Z}_g}$ is a family of irreducible representations of $\mathrm{USp}_r(\mathbf{C})$, not all trivial, with characters $\chi_x = \mathrm{Tr}(\pi_x)$, we have

$$\frac{1}{|A_\mathfrak{p}|} \sum_{a \in A_\mathfrak{p}} \prod_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} \chi_x(\Theta_\mathfrak{p}(ax)) \underset{\|\mathfrak{p}\| \to +\infty}{\longrightarrow} 0. \tag{6.3}$$

The sum is, up to negligible amount coming from points where $\mathcal{F}_\mathfrak{p}$ is not lisse, the sum of the traces of Frobenius on the sheaf

$$\mathcal{G} := \bigotimes_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} \pi_x([\times x]^* \mathcal{F}_\mathfrak{p}),$$

or, from the point of view of representations, the sum of the traces of the representation

$$\rho_\mathcal{G} = \bigotimes_{x \in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} \widetilde{\pi}_x \circ \rho_{[\times x]^* \mathcal{F}_\mathfrak{p}}, \tag{6.4}$$

where $\widetilde{\pi}_x$ is a representation of $\mathrm{Sp}_r(\mathbf{C})$ which extends π_x. Therefore, proving the convergence (6.3) is equivalent to proving

$$\frac{1}{|A_\mathfrak{p}|} \sum_{a \in A_\mathfrak{p}} t_\mathcal{G}(a) \underset{\|\mathfrak{p}\| \to +\infty}{\longrightarrow} 0.$$

If we can apply the Riemann hypothesis to the sheaf $\mathcal{G}$ in the form of Corollary 6.21, then we obtain that

$$\frac{1}{|A_{\mathfrak{p}}|}\left|\sum_{a\in A_{\mathfrak{p}}} t_{\mathcal{G}}(a)\right| \ll \frac{c(\mathcal{G})^2\,\|\mathfrak{p}\|^{1/2}}{|A_{\mathfrak{p}}|}$$

and this finishes the proof since $c(\mathcal{G})$ is easily seen to be bounded independently of $\mathfrak{p}$ and the assumption that $0 \notin \mathrm{Z}_g$ ensures that $|A_{\mathfrak{p}}| \gg \|\mathfrak{p}\|$. So the question is: can we apply Corollary 6.21 to the sheaf $\mathcal{G}$?

Thanks to Corollary 6.21 and Proposition 6.23, it suffices to show that the representation $\rho_{\mathcal{G}}$ associated with the sheaf $\mathcal{G}$ has no trivial geometrically irreducible subrepresentation.

If we did not have the composition with the $\widetilde{\pi}_x$, we would be considering a sheaf of the form

$$\bigotimes_{x\in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})} [\times x]^*\mathcal{F}_{\mathfrak{p}},$$

and for such sheaves [38, Theorem 1.5] gives the conclusion (take $h = 0$ and the tuple γ to be $(x)_{x\in \mathrm{Z}_g(\mathbf{O}_g/\mathfrak{p})}$: the latter is normal in the sense of *loc. cit.* thanks to the separability of g, and since the sheaves are assumed to be bountiful, we get the conclusion). However, it remains to explain why the composition with the irreducible representations $\widetilde{\pi}_x$ does not create any issue. We isolate this part of the argument in Lemma 6.28 below.

The proof of (2) is the same, with $\mathrm{Sp}_r(\mathbf{C})$ replaced by $\mathrm{SL}_r(\mathbf{C})$.

For (3), we have to take into account the fact that if $x \in (\mathbf{O}_g/\mathfrak{p})^\times$, then $[\times(-x)]^*\mathcal{F}_{\mathfrak{p}}$ is isomorphic to the dual of $[\times x]^*\mathcal{F}_{\mathfrak{p}}$ (by definition of $y \mapsto -y$ being a special involution of the sheaf). This implies that $\Theta_{\mathfrak{p}}(-ax) = \overline{\Theta_{\mathfrak{p}}(ax)}$ for all $a \in A_{\mathfrak{p}}$ (resp. $B_{\mathfrak{p}}$), where the bar denotes the complex conjugate of the matrix. Indeed, for unitary representations, the dual representation is isomorphic to the conjugate representation, see e.g. [74, p. 150]. This shows that the random variables $U_{\mathfrak{p}}$ take values in the subgroup

$$\{f\colon \mathrm{Z}_g \to \mathrm{SU}_r(\mathbf{C}) \mid f(x) = \overline{f(y)} \text{ if } x = -y\}.$$

which is isomorphic to $\mathrm{C}(\mathrm{Z}_g/\{\pm 1\}, \mathrm{SU}_r(\mathbf{C}))$, where $\mathrm{Z}_g/\{\pm 1\}$ denotes the quotient of Z_g by the equivalence relation $\sim$ defined by:

$$x \sim y \iff x = y \text{ or } x = -y.$$

The end of the proof is the same as in the previous cases, with $\mathrm{C}(\mathrm{Z}_g/\{\pm 1\}, \mathrm{SU}_r(\mathbf{C})^\sharp)$ playing the role of $\mathrm{C}(\mathrm{Z}_g, \mathrm{SU}_r(\mathbf{C})^\sharp)$. The idea is that the only obstruction to the independence of shifts which is crucial in the proof of Lemma 6.28 was the possibility to have two opposite roots of g, but the quotient by the equivalence relation $\sim$ removed that issue. □

Lemma 6.28. *The multiplicity of the trivial representation as a geometrically irreducible representation of $\rho_{\mathcal{G}}$ (the representation introduced in equation (6.4) of the proof of Theorem 6.27) equals* 0.

Proof. Let us denote by k the field $\mathbf{O}_g/\mathfrak{p}$. To simplify notations, we will only prove this lemma in the case where two representations are involved in the tensor product, but there is no hidden difficulty when more factors are involved. So we assume that we are given a bountiful sheaf $\mathcal{F}_{\mathfrak{p}}$ on the affine line over k, two distinct points $x, y \in k$, and two representations π_x and π_y of a maximal compact subgroup $K_{\mathrm{geom}}(\mathbf{C})$ of the geometric monodromy group $G_{\mathrm{geom}}(\mathbf{C})$ of $\mathcal{F}_{\mathfrak{p}}$. We assume that π_x and π_y are irreducible representations, and that at least one of them is not the trivial one.

First, thanks to [59, §3.2] (see also the statement in [89, Cor. 3.3]), these representations extend to representations $\widetilde{\pi}_x$ and $\widetilde{\pi}_y$ of the whole Lie group $G_{\mathrm{geom}}(\mathbf{C})$ satisfying the same irreducibility assumptions. Then, we want to show that the representation

$$\lambda := \left(\widetilde{\pi}_x \circ \rho_{[\times x]^*\mathcal{F}_{\mathfrak{p}}}\right) \otimes \left(\widetilde{\pi}_y \circ \rho_{[\times y]^*\mathcal{F}_{\mathfrak{p}}}\right)$$

does not admit a non-zero vector which is invariant under the action of the geometric Galois group $\mathrm{Gal}\left(k(X)^{\mathrm{sep}}/\overline{k}(X)\right) =: \Pi_k^{\mathrm{geom}}$. Assume for a contradiction that such a vector exists. Then for all $\sigma \in \Pi_k^{\mathrm{geom}}$, we have $\lambda(\sigma)(x) = x$, that is

$$\left[\widetilde{\pi}_x\left(\rho_{[\times x]^*\mathcal{F}_{\mathfrak{p}}}(\sigma)\right) \otimes \widetilde{\pi}_y\left(\rho_{[\times y]^*\mathcal{F}_{\mathfrak{p}}}(\sigma)\right)\right](x) = x \tag{6.5}$$

where the tensor product inside the brackets is the tensor product of the endomorphisms $\widetilde{\pi}_x\left(\rho_{[\times x]^*\mathcal{F}_{\mathfrak{p}}}(\sigma)\right)$ and $\widetilde{\pi}_y\left(\rho_{[\times y]^*\mathcal{F}_{\mathfrak{p}}}(\sigma)\right)$ in the sense of Definition 6.36. Now, the bountiful property of $\mathcal{F}_{\mathfrak{p}}$ ensures that the image of the map

$$\begin{array}{ccc} \Pi_k^{\mathrm{geom}} & \to & G_{\mathrm{geom}}(\mathbf{C}) \times G_{\mathrm{geom}}(\mathbf{C}) \\ \sigma & \mapsto & \left(\rho_{[\times x]^*\mathcal{F}_{\mathfrak{p}}}(\sigma), \rho_{[\times y]^*\mathcal{F}_{\mathfrak{p}}}(\sigma)\right) \end{array}$$

is Zariski dense in $G_{\mathrm{geom}}(\mathbf{C}) \times G_{\mathrm{geom}}(\mathbf{C})$ (informally, this can be interpreted as an "independence of shifts"). This comes from the Goursat-Kolchin-Ribet criterion, as stated by Katz in [60, Proposition 1.8.2]. Therefore, we can deduce from (6.5) that for all $(g, h) \in G_{\mathrm{geom}}(\mathbf{C}) \times G_{\mathrm{geom}}(\mathbf{C})$,

$$\left[\widetilde{\pi}_x(g) \otimes \widetilde{\pi}_y(h)\right](x) = x.$$

This is equivalent to saying that the external product representation $\widetilde{\pi}_x \boxtimes \widetilde{\pi}_y$ (see Appendix 6.A) admits a non-zero invariant vector, which contradicts the fact that it is irreducible (thanks to Proposition 6.37) of dimension $\geqslant 2$.

□

Remark 6.29. For the general case, the fact that g is a separable polynomial ensures that the tuple $(x)_{x \in \mathbf{Z}_g}$ is *normal* in the sense of [38] because each x appears with multiplicity one. Thus, the bountiful property of $\mathcal{F}_{\mathfrak{p}}$ ensures the "independence of shifts": this gives us the fact that

$$\begin{array}{ccc} \Pi_k^{\mathrm{geom}} & \to & \prod_{x \in \mathbf{Z}_g} G_{\mathrm{geom}}(\mathbf{C}) \\ \sigma & \mapsto & \left(\rho_{[\times x]^*\mathcal{F}_{\mathfrak{p}}}(\sigma)\right)_{x \in \mathbf{Z}_g} \end{array}$$

has dense image and the remainder of the proof works in the same manner.

6.3.3. The example of Kloosterman sums

Let us illustrate cases (1) and (3) of the previous theorem with a concrete example: that of Kloosterman sums. They are defined as follows: For an integer $r \geqslant 2$, and an odd prime q,

$$\mathrm{Kl}_r(a, q) := \frac{(-1)^{r-1}}{q^{\frac{r-1}{2}}} \sum_{\substack{x_1, \ldots, x_r \in \mathbf{F}_q^\times \\ x_1 \cdots x_r = a}} e\left(\frac{x_1 + \cdots + x_r}{q}\right) \quad \text{for all } a \in \mathbf{F}_q^\times.$$

In the case $r = 2$, we recover the classical Kloosterman sums of Katz' equidistribution theorem of Section 1.3.2.

It was proved by Deligne that these sums are also trace functions. Namely, he proved in [25] the existence of an ℓ-adic middle-extension sheaf $\mathcal{K}\ell_r$ (called the Kloosterman sheaf) on $\mathbf{P}^1_{\mathbf{F}_q}$ such that (see [39, Theorem 4.4]):

- $\mathrm{rk}(\mathcal{K}\ell_r) = r$,
- $\mathcal{K}\ell_r$ is lisse on $\mathbf{P}^1_{\mathbf{F}_q} \setminus \{0, \infty\}$,
- $\mathcal{K}\ell_r$ is pure of weight 0
- $c(\mathcal{K}\ell_r) = r + 3$ (with Swan conductor 0 at 0 and 1 at ∞)
- for all $a \in \mathbf{F}_q^\times$,

$$t_{\mathcal{K}\ell_r}(a) = \mathrm{Kl}_r(a, q)$$

The Kloosterman sheaf was then studied in more detail by Katz in [59], where (among other things) he determined the monodromy groups.

Theorem 6.30 (Katz, see [90, Theorem 1.3] for this specific statement)**.** *For all $r \geqslant 2$, we have*

$$G_{\mathcal{K}\ell_r,\mathrm{geom}}(\mathbf{C}) = G_{\mathcal{K}\ell_r,\mathrm{arith}}(\mathbf{C}) = \begin{cases} \mathrm{SL}_r(\mathbf{C}) \text{ if } r \text{ is odd} \\ \mathrm{Sp}_r(\mathbf{C}) \text{ if } r \text{ is even.} \end{cases}$$

Finally, $\mathcal{K}\ell_r$ is bountiful thanks to the determination of the automorphism group of this sheaf, which is contained in [38, Proposition 3.6]. It has no special involution when r is even, and one special involution when r is odd, given by $y \mapsto -y$. All those facts are stated in [38, §3(b) and §3(c)] and proved further in the article.

Therefore, even rank Kloosterman sheaves satisfy the assumptions of Theorem 6.27 (1), while odd rank Kloosterman sheaves satisfy the assumptions of point (3).

Even rank Kloosterman sums. Assume that $r = 2g$ is even. Then thanks to case (1) of Theorem 6.27 applied to the bountiful sheaf $\mathcal{K}\ell_r$, we know that the corresponding random variables $U_{\mathfrak{p}}$ become equidistributed in $\mathrm{C}(\mathrm{Z}_g, \mathrm{USp}_r(\mathbf{C})^\sharp)$ as $\|\mathfrak{p}\|$ tends to infinity. Composing this convergence in law with the continuous mapping

$$\begin{array}{ccc} \mathrm{C}(\mathrm{Z}_g, \mathrm{USp}_r(\mathbf{C})^\sharp) & \to & \mathbf{C} \\ M & \mapsto & \sum_{x \in \mathrm{Z}_g} \mathrm{Tr}(M(x)) \end{array}$$

we obtain as a corollary the convergence in law of the random variables

$$\begin{array}{ccc} \mathbf{O}_g/\mathfrak{p} & \to & \mathbf{C} \\ a & \mapsto & \sum_{x \in \mathrm{Z}_g} \mathrm{Tr}(U_{\mathfrak{p}}(a)(x)) \end{array}$$

towards a random variable which is the sum of $\deg(g)$ independent random variables, each distributed as the trace of a uniform element of $\mathrm{USp}_r(\mathbf{C})^\sharp$. Now, unfolding the definition of the random variables $U_{\mathfrak{p}}$ and identifying $\mathbf{O}_g/\mathfrak{p}$ with $\mathbf{F}_q$ for the prime $q = \|\mathfrak{p}\|$, we see that this gives us the equidistribution of the sums

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_r(ax, q)$$

with respect to a measure which is the law of $\deg(g)$ independant random variables, each distributed as the trace of a uniform element in $\mathrm{USp}_r(\mathbf{C})^\sharp$. The distribution of those traces was studied by Katz in [59, Chapter 13]. In particular, when $r = 2$, he shows that they are uniformly distributed in $[-2, 2]$ with respect to the Sato-Tate measure

$$\mathrm{d}\mu_{\mathrm{ST}}(x) = \frac{1}{2\pi}\sqrt{4 - x^2}\mathrm{d}x.$$

This is a consequence of the fact that $\mathrm{USp}_2(\mathbf{C})$ is isomorphic to $\mathrm{SU}_2(\mathbf{C})$ and of the explicit determination of the Haar measure on the latter (we give a sketch of the proof of this last part in Proposition 6.34 below). Therefore, we have the following concrete corollary of Theorem 6.27:

Corollary 6.31. *Let $g \in \mathbf{Z}[X]$ be a monic polynomial of degree $d \geqslant 1$, and assume that $0 \notin \mathrm{Z}_g$. As q goes to infinity among the prime number totally split in K_g, the sums*

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_2(ax, q),$$

parametrized by $a \in \mathbf{F}_q$, become equidistributed in $\mathbf{C}$ with respect to a measure which is the law of d independant and identically distributed Sato-Tate random variables. The same holds for the sums

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_2(a + x, q)$$

without the assumption that $0 \notin \mathrm{Z}_g$.

Here is an illustration of this statement:

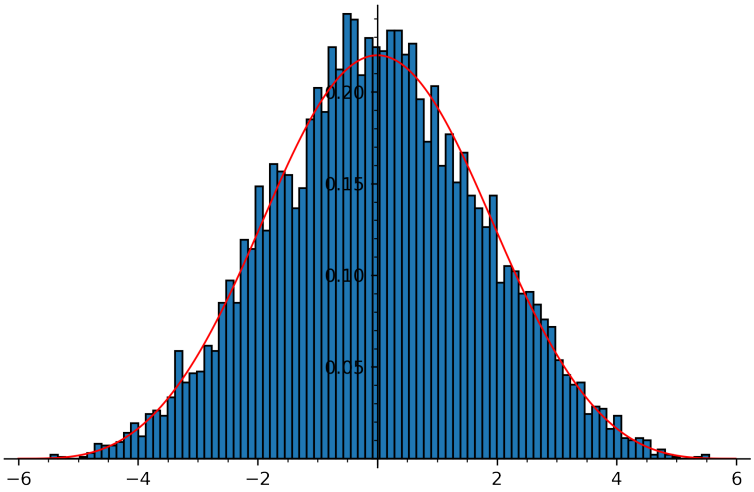


Figure 6.1: Distribution of the values of the sums $\sum_{x\in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_2(ax,q)$ as a varies in $\mathbf{F}_q$, for $g = X^3 - 9X - 1$ and $q = 8089$. The red curve is the probability density function of the random variable $X_1 + X_2 + X_3$ defined as the sum of three independent and identically distributed Sato–Tate random variables.

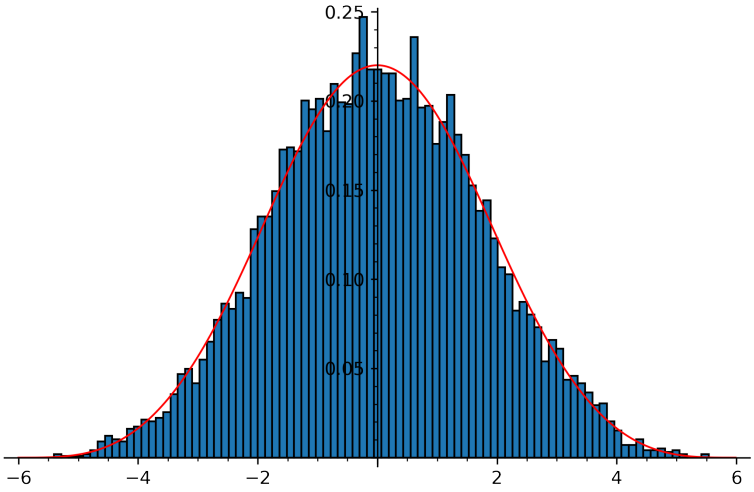


Figure 6.2: Distribution of the values of the sums $\sum_{x\in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_2(a+x,q)$ as a varies in $\mathbf{F}_q$, for $g = X^3 - 9X - 1$ and $q = 8089$. The red curve is the probability density function of the random variable $X_1 + X_2 + X_3$ defined as the sum of three independent and identically distributed Sato–Tate random variables.

Remark 6.32. This last corollary recovers Katz' equidistribution result in the form stated in the introduction (see Theorem 1.23). Indeed, it suffices to take the polynomial g to be $X - 1$.
Moreover, such sums of shifts of Kloosterman sums already appeared in analytic number theory, see e.g. [35, Proposition 3.2].

Odd rank Kloosterman sums. If r is odd, the Kloosterman sheaf $\mathcal{K}\ell_r$ satisfies the assumptions of case (3) of Theorem 6.27. Therefore, the convergence in law of the random variables $(V_\mathfrak{p})$ implies the uniform distribution of the sums

$$\sum_{x\in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_r(a+x,q)$$

as q goes to infinity and a varies in $\mathbf{F}_q$ (provided q splits completely in K_g). The theorem tells us that the limit measure is the law of the sum of $\deg(g)$ random variables, each distributed as the trace of a uniform matrix in $\mathrm{SU}_r(\mathbf{C})$. For $r = 3$, the pushforward measure of the Haar measure on $\mathrm{SU}_3(\mathbf{C})$ via the trace is determined in [57], and it is supported inside the 3-cusp hypocycloid that we already encountered several times along this thesis. The following figure[2] illustrates the limit distribution of individual Kloosterman sums $\mathrm{Kl}_3(a, q)$.

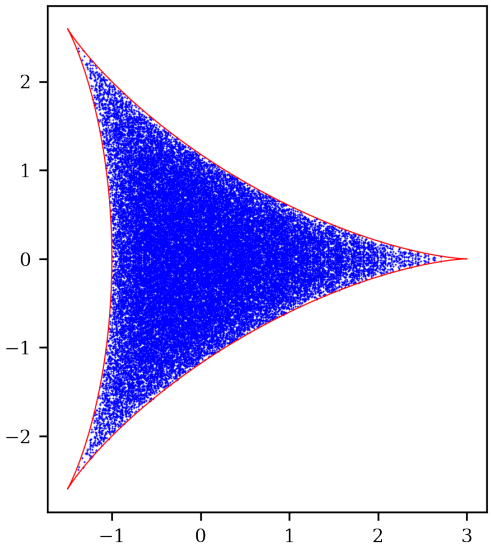


Figure 6.3: The sums $\mathrm{Kl}_3(a, q)$ for $q = 40009$ and a varying in $\mathbf{F}_q$

Remark 6.33. In Chapter 2, we encountered a measure on the 3-cusp hypocycloid $\mathbb{H}_3$ that was defined as the pushforward measure of the Haar measure on $\mathbf{S}^1 \times \mathbf{S}^1$ via the map

$$(z_1, z_2) \mapsto z_1 + z_2 + \frac{1}{z_1 z_2}.$$

(see e.g. Theorem 2.5 p.53). In terms of matrices in $\mathrm{SU}_3(\mathbf{C})$, this corresponds to considering the Haar measure on the maximal torus of diagonal matrices

$$\left\{ \begin{pmatrix} z_1 & 0 & 0 \\ 0 & z_2 & 0 \\ 0 & 0 & \overline{z_1}.\overline{z_2} \end{pmatrix} ;\ (z_1, z_2) \in \mathbf{S}^1 \times \mathbf{S}^1 \right\}$$

and then taking the pushforward measure via the trace. On the other hand, in the current chapter we have another measure on $\mathbb{H}_3$, which is defined as the pushforward of the Haar measure on the full group $\mathrm{SU}_3(\mathbf{C})$ (not only on its maximal torus). In this remark, we want to stress that even though hypocycloids appeared in earlier chapters, the measure with respect to which our exponential sums become equidistributed only happen to have the same support, but it is not the same.
Let us sketch the argument in the simpler case of $\mathrm{SU}_2(\mathbf{C})$. In that case, the measure on the 2-cusp hypocycloid $\mathbb{H}_2 = [-2, 2]$ that was relevant in the previous chapters was the pushforward of the Haar measure λ on $\mathbf{S}^1$ via the map:

$$f\colon z \mapsto z + \frac{1}{z} = z + \overline{z} = 2\mathrm{Re}(z).$$

Let us determine this measure explicitly: for any interval $[a, b] \subseteq [-2, 2]$, we have

[2] The computations of the values $\mathrm{Kl}_3(a, q)$ have been performed by Bill Allombert using `PARI-GP`: [101]. It took around 11 hours on 128 cores.

$$\int_{-2}^{2} \mathbb{1}_{[a,b]} \mathrm{d}f_*\lambda = \int_{\mathbf{S}^1} (\mathbb{1}_{[a,b]} \circ f)\ \mathrm{d}\lambda = \frac{1}{2\pi}\int_0^{2\pi} (\mathbb{1}_{[a,b]} \circ f)(\exp(i\theta))\mathrm{d}\theta$$
$$= \frac{1}{2\pi}\int_0^{2\pi} \mathbb{1}_{[a,b]}(2\cos\theta)\mathrm{d}\theta = \frac{1}{2\pi}\int_{-2}^{2} \mathbb{1}_{[a,b]}(x)\frac{\mathrm{d}x}{\sqrt{1-\left(\frac{x}{2}\right)^2}}.$$

Therefore, the measure on $[-2,2]$ has probability density function given by

$$x \mapsto \frac{1}{2\pi\sqrt{1-\left(\frac{x}{2}\right)^2}} \tag{6.6}$$

with respect to the Lebesgue measure on $[-2,2]$. On the other hand, the image by the trace of the Haar measure on $\mathrm{SU}_2(\mathbf{C})$ can be determined using the following classical result (see e.g. [34]):

Proposition 6.34. *Let μ_2 denote the Haar probability measure on $\mathrm{SU}_2(\mathbf{C})$. Then for any central*[3] *function $\varphi\colon \mathrm{SU}_2(\mathbf{C}) \to \mathbf{C}$ which is absolutely integrable, we have*

$$\int_{\mathrm{SU}_2(\mathbf{C})} \varphi \mathrm{d}\mu_2 = \frac{2}{\pi}\int_0^{\pi} \varphi\begin{pmatrix}\exp(i\theta) & 0\\ 0 & \exp(-i\theta)\end{pmatrix}\sin^2(\theta)\mathrm{d}\theta.$$

For any interval $[a,b] \subseteq [-2,2]$, we can apply this proposition to the function $\varphi = \mathbb{1}_{[a,b]} \circ \mathrm{Tr}$, and this gives that

$$\int_{\mathrm{SU}_2(\mathbf{C})} (\mathbb{1}_{[a,b]} \circ \mathrm{Tr})\ \mathrm{d}\mu_2 = \frac{2}{\pi}\int_0^{\pi} \mathbb{1}_{[a,b]}(2\cos\theta)\sin^2(\theta)\mathrm{d}\theta$$
$$= \frac{1}{\pi}\int_{-2}^{2} \mathbb{1}_{[a,b]}(y)\sqrt{1-\left(\frac{y}{2}\right)^2}\mathrm{d}y$$

Thus, the image by the trace of the Haar measure on $\mathrm{SU}_2(\mathbf{C})$ admits the following probability density function with respect to the Lebesgue measure on $[-2,2]$:

$$x \mapsto \frac{1}{\pi}\sqrt{1-\left(\frac{x}{2}\right)^2} \tag{6.7}$$

(we recognize the Sato-Tate measure, which governs the equidistribution of the classical Kloosterman sums $\mathrm{Kl}_2(a,q)$). Comparing (6.6) et (6.7) clearly shows that the two pushforward measures do not coincide.

Next, we illustrate Theorem 6.27 in the case of the sum of two Kloosterman sums, shifted additively by the two roots in $\mathbf{F}_q$ of the polynomial X^2+X+1. As expected, the picture suggests that these sums behave like a sum of two independent random variables, each following the law of the trace of a random matrix in $\mathrm{SU}_3(\mathbf{C})$ (because we can see that the sums will eventually fill in the Minkowski sum $\mathbb{H}_3+\mathbb{H}_3$, even though the length of the computations only allows us relatively small values of q).

[3] i.e. satisfying $\varphi(ghg^{-1}) = \varphi(h)$ for all $g,h \in \mathrm{SU}_2(\mathbf{C})$.

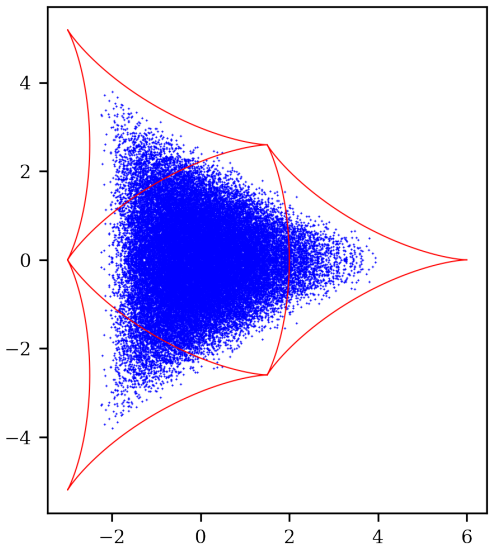


Figure 6.4: The sums $\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_3(a+x,q)$ for $q = 40009$, a varying in $\mathbf{F}_q$, and $g = X^2 + X + 1$.

Moreover, since $X^2 + X + 1$ does not admit two roots of opposite sign, the random variables $U_{\mathfrak{p}}$ also converge in law to the a random variable uniformly distributed in $\mathrm{C}(\mathrm{Z}_g, \mathrm{SU}_3(\mathbf{C})^\sharp)$, so that the same type of picture is obtained when we replace additive shifts by multiplicative shifts by the roots of g.

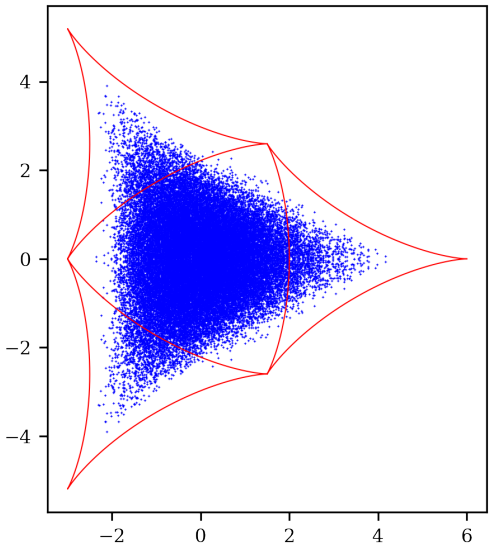


Figure 6.5: The sums $\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_3(ax,q)$ for $q = 40009$, a varying in $\mathbf{F}_q$, and $g = X^2 + X + 1$.

However, for other polynomials g, sums of multiplicative shifts can show a different asymptotic behaviour than sums of additive shifts. For instance, if we take g to be the polynomial $(X-1)(X+1)$, then in that case the random variables $U_{\mathfrak{p}}$ become equidistributed in the subgroup

$$\left\{ f \colon \{\pm 1\} \to \mathrm{SU}_3(\mathbf{C}) \mid f(-1) = \overline{f(1)} \right\}$$

which is isomorphic to $\mathrm{SU}_3(\mathbf{C})$, so it is only half-dimensional compared to the space where the random variable $V_{\mathfrak{p}}$ become equidistributed. The sums $\mathrm{Kl}_3(a,q) + \mathrm{Kl}_3(-a,q)$ are equal to $\mathrm{Kl}_3(a,q) + \overline{\mathrm{Kl}_3(a,q)}$, and they become equidistributed with respect to the measure which is the law of the random variable

$$\mathrm{Tr}(U) + \overline{\mathrm{Tr}(U)}$$

where U is uniformly distributed in $\mathrm{SU}_3(\mathbf{C})$. In particular, they are real-valued, so they certainly do not have the same limit measure as the corresponding sums of additive shifts $\mathrm{Kl}_3(a-1,q)+\mathrm{Kl}_3(a+1,q)$.

The following histogram illustrates what we obtain experimentally for the distribution of these real numbers for a large value of q.

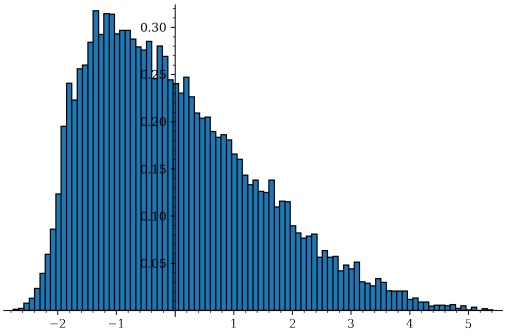


Figure 6.6: Distribution of the sums $\sum_{x\in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_3(ax,q)$ on the real line, for $q = 40009$, a varying in $\mathbf{F}_q$, and $g = (X-1)(X+1)$.

Remark 6.35. Examples of bountiful sheaves satisfying the assumptions of case (2) of Theorem 6.27 can also be found. A concrete example is given by sums of the form

$$t_q(x) = \frac{1}{\sqrt{q}} \sum_{y\in\mathbf{F}_q} \chi(h(y))e\left(\frac{xy}{q}\right),$$

where χ is a multiplicative character of $\mathbf{F}_q^\times$ and $h \in \mathbf{Z}[X]$ is a polynomial which must satisfy certain technical conditions. Indeed, such sums are trace functions associated with a sheaf whose automorphism group is not necessarily trivial depending on some properties of h (and we want the automorphism group to be trivial, as it is a crucial part of the definition of a bountiful sheaf). We refer to [38, Proposition 3.7] for a precise statement of the conditions on h which ensure the triviality of the automorphism group.

6.A. On tensor products of representations

In this appendix, we provide a brief summary on external and internal tensor products of representations, as both constructions are useful when working with products of trace functions.

First, let k be a field, and let V and W be two finite dimensional k-vector spaces. Given endomorphisms of V and W respectively, one can define an endomorphism of the vector space $V \otimes W$ as follows:

Definition 6.36. *For $A \in \mathrm{End}_k(V)$ and $B \in \mathrm{End}_k(W)$, we define*

$$A \otimes B \colon V \otimes W \to V \otimes W$$

on pure tensors by the formula $(A \otimes B)(v \otimes w) := A(v) \otimes B(w)$, and then extend it to the whole vector space $V \otimes W$ by k-linearity.

Now we let G be a group. We recall that a finite dimensional k-representation of G is a group homomorphism $\rho : G \to \mathrm{GL}(V)$, where V is a finite dimensional k-vector space. Given two representations of the same group G, say $\rho \colon G \to \mathrm{GL}(V)$ and $\sigma \colon G \to \mathrm{GL}(W)$, one can construct another representation $\rho \otimes \sigma$ of G, called the *internal tensor product* of ρ and σ, as follows:

$$\begin{array}{rccc} \rho \otimes \sigma \colon & G & \to & \mathrm{GL}(V \otimes W) \\ & g & \mapsto & \rho(g) \otimes \sigma(g). \end{array}$$

In other words, it is defined on pure tensors $v \otimes w \in V \otimes W$ by

$$(\rho \otimes \sigma)(g)(v \otimes w) = \rho(g)(v) \otimes \sigma(g)(w) \text{ for all } g \in G,$$

and is extended by k-linearity to $V \otimes W$.

On the other hand, there is also a construction of an *external tensor product* of representations. Given a representation $\rho \colon G \to \mathrm{GL}(V)$ of a group G and a representation $\sigma \colon H \to \mathrm{GL}(W)$ of another group H, one can define the external tensor product representation $\rho \boxtimes \sigma$ as the following representation of $G \times H$:

$$\begin{array}{rccc} \rho \boxtimes \sigma \colon & G \times H & \to & \mathrm{GL}(V \otimes W) \\ & (g, h) & \mapsto & \rho(g) \otimes \sigma(h). \end{array}$$

In other words, it is defined on pure tensors by

$$(\rho \boxtimes \sigma)(g, h)(v \otimes w) = \rho(g)(v) \otimes \sigma(h)(w) \text{ for all } g \in G, h \in H,$$

and extended by k-linearity to $V \otimes W$.

When the base field k is algebraically closed, it can be shown that this construction, if we start from irreducible representations ρ and σ, actually gives *all* irreducible representations of $G \times H$. Indeed, we have the following result:

Proposition 6.37 ([74, Prop. 2.3.23])**.** *Let k be an algebraically closed field, and let G and H be two groups.*
(1) If τ is a finite-dimensional irreducible representation of $G \times H$, then there exists two irreducible representations ρ of G and σ of H such that $\tau \simeq \rho \boxtimes \sigma$.
(2) Conversely, if ρ is an irreducible representation of G and σ is an irreducible representation of H, then $\rho \boxtimes \sigma$ is an irreducible representation of $G \times H$.

Research perspectives

Limiting growth condition for the equidistribution of subgroups of $\mathbf{F}_p^\times$

Given a subgroup G of $\mathbf{F}_p^\times$, one can view[4] the elements $\frac{x}{p}$ for $x \in G$ as elements of $\mathbf{R}/\mathbf{Z}$, and ask whether these elements become equidistributed in $\mathbf{R}/\mathbf{Z}$ as p goes to infinity. As we already mentioned in Remark 3.27 p.117, a conjecture of Montgomery, Vaughan and Wooley in [84] (also mentioned and stated in the survey [14]) implies that there is equidistribution as soon as

$$\frac{|G|}{\log(p)} \underset{p\to\infty}{\longrightarrow} +\infty$$

but, to my current knowledge, it has neither been proved nor disproved. In view of the discussion of Appendix 3.B, this conjecture is very strong, since subgroups that have a cardinality less than a constant times $\log(p)$ *do not* satisfy

$$\max_{a\in\mathbf{F}_p^\times} \left| \sum_{x\in G} e\left(\frac{ax}{p}\right) \right| \underset{p\to\infty}{=} o\left(|G|\right).$$

To my current knowledge, the best result in this direction is the fact that if $|G| \geqslant p^\delta$ for some $\delta > 0$ independent of p, then we have equidistribution: see e.g. [13, Theorem 6], or Bourgain's theorem as stated in this thesis in Theorem 3.11. However, there is still a gap to bridge between p^δ and $\log(p)$. Moreover, it could also be interesting to look for other subsets $A \subset \mathbf{F}_p$ (not necessarily multiplicative subgroups) which become equidistributed in $\mathbf{R}/\mathbf{Z}$. This would strengthen Corollary 4.40 by allowing us to prove the equidistribution of the exponential sums

$$\sum_{\substack{x\in\mathbf{F}_p \\ g(x)\equiv 0 \,(\mathrm{mod}\, p)}} e\Big(\frac{bx}{p}\Big) \tag{6.8}$$

with parameters b varying in the subset A of $\mathbf{F}_p$ instead of the whole group.

Additive and multiplicative relations between roots of polynomials

To make the limit measure in the equidistribution of the sums (6.8) of Corollary 4.40 more explicit, one needs to determine the module of additive relations between the roots of the polynomial g.
I am interested in finding examples of infinite families of polynomials with a given module of additive relations. As we saw in Chapter 4, some are already known, for instance when the Galois group of $K_g/\mathbf{Q}$ is maximal (which is the generic case), but I would like to investigate other possible Galois groups.

I am also interested in related inverse problems, such as: when is a polynomial (in a certain family, such as the cyclotomic polynomials) uniquely determined by its module of additive relations?

[4] simply because the fractional part of $\tilde{x}/p$ does not depend on the lift $\tilde{x} \in \mathbf{Z}$ of the residue class $x \,(\mathrm{mod}\, p)$.

Similarly, in Proposition 6.1 the equidistribution of the sums

$$\sum_{x\in \mathrm{Z}_g(\mathbf{F}_q)} \chi(x),$$

where χ varies over multiplicative characters of $\mathbf{F}_q$, is governed by the multiplicative relations among the roots of g. Therefore, I would also be interested in understanding more precisely how to apply the work of Girstmair [46], which gives a general approach based on the study of the rational representations of $\mathrm{Gal}(K_g/\mathbf{Q})$, to this type of questions.

Morover, this may have interactions with other problems in analytic number theory. For instance, in [71] and [18], multiplicative relations between roots of L-functions of algebraic curves over finite fields were already investigated using this approach. This type of results is motivated for instance by the study of the Chebyshev bias in the distribution of primes in arithmetic progression (or generalizations of this question), where the linear independence hypothesis regarding the zeros of Dirichlet L-functions plays a central role.

Horizontal problems

In Chapter 4, we studied random variables $U_{\mathfrak{p}}$ defined on $\mathbf{O}_g/\mathfrak{p}$ (with uniform probability measure) with values in $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$, defined as follows:

$$U_{\mathfrak{p}}(a)\colon x \in \mathrm{Z}_g \mapsto e\left(\frac{\tau_{\mathfrak{p}}(a\varpi_{\mathfrak{p}}(x))}{\|\mathfrak{p}\|}\right).$$

We proved at Theorem 4.30 that these random variables converge in law to a random variable U, uniformly distributed on the subgroup H_g of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$. This belonged to the class of *vertical* equidistribution problems, since for any $\mathfrak{p} \in \mathcal{S}_g$, we averaged over $a \in \mathbf{O}_g/\mathfrak{p}$.

The corresponding *horizontal* question would be to *fix a non-zero algebraic integer* $a \in \mathbf{O}_g$, and to consider the random variables U'_T, defined on the set $\mathcal{S}_g(T)$ of ideals $\mathfrak{p} \in \mathcal{S}_g$ such that $\|\mathfrak{p}\| \leqslant T$ (with uniform probability measure), with values in $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$, as follows

$$U'_T(\mathfrak{p})\colon x \in \mathrm{Z}_g \mapsto e\left(\frac{\tau_{\mathfrak{p}}(\varpi_{\mathfrak{p}}(ax))}{\|\mathfrak{p}\|}\right).$$

The question one may ask is: do the random variables U'_T converge in law as T goes to infinity, and if so, do they converge to the same limit U as the random variables $U_{\mathfrak{p}}$?

Let us see what this gives if we try to apply Weyl's criterion to this problem. For a character η of the group $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$,

$$\mathbb{E}\left(\eta(U'_T)\right) = \frac{1}{|\mathcal{S}_g(T)|}\sum_{\mathfrak{p}\in\mathcal{S}_g(T)} \eta(U'_T(\mathfrak{p}))$$

so if η is associated with $\alpha \in \mathrm{C}(\mathrm{Z}_g, \mathbf{Z})$, we can write

$$\mathbb{E}\left(\eta(U'_T)\right) = \frac{1}{|\mathcal{S}_g(T)|}\sum_{\mathfrak{p}\in\mathcal{S}_g(T)}\prod_{x\in\mathrm{Z}_g} e\left(\frac{\tau_{\mathfrak{p}}(\varpi_{\mathfrak{p}}(ax))}{\|\mathfrak{p}\|}\right)^{\alpha(x)} = \frac{1}{|\mathcal{S}_g(T)|}\sum_{\mathfrak{p}\in\mathcal{S}_g(T)} e\left(\frac{\tau_{\mathfrak{p}}(\varpi_{\mathfrak{p}}(aS_\alpha))}{\|\mathfrak{p}\|}\right)$$

where $S_\alpha = \sum_{x\in\mathrm{Z}_g}\alpha(x)x$. Therefore, the sum of the right-hand side is the type of Weyl sum which appears in the following problem:

Given a number field $K/\mathbf{Q}$ and an algebraic integer $\beta \in \mathcal{O}_K$, we can reduce it modulo $\mathfrak{p}$ for any prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, to obtain $\varpi_{\mathfrak{p}}(\beta)$. Now, if we further assume that $\mathfrak{p}$ has residual degree 1, then we can

identify canonically $\mathcal{O}_K/\mathfrak{p}$ with $\mathbf{Z}/\|\mathfrak{p}\|\mathbf{Z}$, to see $\varpi_{\mathfrak{p}}(\beta)$ as a residue class modulo $\|\mathfrak{p}\|$: this is what is denoted by $\tau_{\mathfrak{p}}(\varpi_{\mathfrak{p}}(\beta))$. Then we can wonder whether the fractional parts of

$$\frac{\tau_{\mathfrak{p}}(\varpi_{\mathfrak{p}}(\beta))}{\|\mathfrak{p}\|}$$

become equidistributed in $\mathbf{R}/\mathbf{Z}$ as $\mathfrak{p}$ varies among the prime ideals with residual degree 1 and $\|\mathfrak{p}\|$ goes to infinity. The application of Weyl's criterion in this setting would give sums of the form

$$\frac{1}{\mathcal{S}(T)}\sum_{\mathfrak{p}\in\mathcal{S}(T)} e\left(h\frac{\tau_{\mathfrak{p}}(\varpi_{\mathfrak{p}}(\beta))}{\|\mathfrak{p}\|}\right)$$

where $\mathcal{S}(T)$ denotes the set of prime ideals of $\mathcal{O}_K$ with residual degree 1 and satisfying $\|\mathfrak{p}\| \leqslant T$. This equidistribution question is investigated in [106] in the case of the reduction of a fixed algebraic integer β modulo arbitrary ideals with residual degree 1 (not necessarily prime). However, it is likely that the level of difficulty will rise when trying to restrict to prime ideals, just as in the case of the theorem of Duke-Friedlander-Iwaniec on roots of polynomial congruences (Theorem 1.12 of our introduction), which is only known for quadratic polynomials, while the analogous theorem of Hooley modulo arbitrary integers is proved for polynomials of arbitrary degree.

Moreover, we cannot hope that the random variables U'_T converge in law to U in all cases. For instance, assume that a is a fixed non-zero integer and that g admits a root $k \in \mathbf{Z}\setminus\{0\}$ (as it is the case with root $k = 1$ of the polynomial $g = X^d - 1$). Then for all $\mathfrak{p} \in \mathrm{Z}_g$,

$$U'_T(\mathfrak{p})(k) = e\left(\frac{ka}{\|\mathfrak{p}\|}\right),$$

so it converges to 1 as $\|\mathfrak{p}\|$ tends to infinity, which is not the behaviour of a random variable which converges in law to U. Thus, there are probably some assumptions on g that one needs to add in order to obtain the horizontal equidistribution (for instance, g probably needs to be irreducible).

Now, **if** the random variables U'_T converge in law to U, then since the linear map

$$\begin{array}{rccc}\sigma & : & \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1) & \to & \mathbf{C} \\ & & f & \mapsto & \sum_{x\in\mathrm{Z}_g} f(x)\end{array}$$

is continuous and bounded, we have that

$$\mathbb{E}(\sigma(U'_T)) \underset{T\to+\infty}{\longrightarrow} \mathbb{E}(\sigma(U)).$$

In particular, if $0 \notin \mathrm{Z}_g$, we have that $\mathbb{E}(\sigma(U)) = 0$ (see Remark 4.44) so that we would have

$$\mathbb{E}(\sigma(U'_T)) = \frac{1}{|\mathcal{S}_g(T)|}\sum_{\mathfrak{p}\in\mathcal{S}_g(T)}\left(\sum_{x\in\mathrm{Z}_g} e\left(\frac{\tau_{\mathfrak{p}}(\varpi_{\mathfrak{p}}(ax))}{\|\mathfrak{p}\|}\right)\right) \underset{T\to+\infty}{\longrightarrow} 0$$

Using Proposition 4.31 to relate the inner sums to sums over $\mathrm{Z}_g(\mathbf{F}_q)$, we see that the above limit is closely related[5] to sums of the type

$$\frac{1}{\pi(x)}\sum_{q\leqslant x}\sum_{y\in\mathrm{Z}_g(\mathbf{F}_q)} e\left(\frac{by}{q}\right)$$

which are exactly the type of sums that arise when one applies Weyl's criterion to tackle the problem of the uniform distribution modulo 1 of the roots of g modulo q, as q goes to infinity. Thus, the convergence in law of the random variables U'_T would imply a version of the equidistribution conjecture modulo totally split primes, on average over prime ideals over q.

[5] there is just an extra averaging over prime ideals over q.

Bibliography

[1] Lambert A'Campo. The circle method, applications to the partition function, and beyond. Undergraduate research project, available at https://sites.google.com/view/acampo/home.

[2] Bill Allombert, Yuri Bilu, and Amalia Pizarro-Madariaga. CM-points on straight lines. In *Analytic number theory*, pages 1–18. Springer, Cham, 2015.

[3] Alexandre Bailleul. Étude de la répartition des automorphismes de Frobenius dans les groupes de Galois. available at http://abailleul.perso.math.cnrs.fr/Manuscrit.pdf.

[4] Olga Balkanova and Dmitry Frolenkov. Sums of kloosterman sums in the prime geodesic theorem. https://arxiv.org/abs/1803.04206.

[5] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[6] Manjul Bhargava. Galois groups of random integer polynomials and van der Waerden's conjecture, 2022. https://arxiv.org/abs/2111.06507.

[7] Yuri Bilu, Florian Luca, and Amalia Pizarro-Madariaga. Rational products of singular moduli. *J. Number Theory*, 158:397–410, 2016.

[8] Yuri Bilu, David Masser, and Umberto Zannier. An effective "theorem of André" for CM-points on a plane curve. *Math. Proc. Cambridge Philos. Soc.*, 154(1):145–152, 2013.

[9] Yuval Bistritz and Alexander Lifshitz. Bounds for resultants of univariate and bivariate polynomials. *Linear Algebra Appl.*, 432(8):1995–2005, 2010.

[10] N. Bourbaki. *Éléments de mathématique. Topologie générale. Chapitres 5 à 10*. Hermann, Paris, 1974.

[11] J. Bourgain. Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary. *J. Anal. Math.*, 97:317–355, 2005.

[12] J. Bourgain and M.-C. Chang. Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors. *Geom. Funct. Anal.*, 16(2):327–366, 2006.

[13] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin. Estimates for the number of sums and products and for exponential sums in fields of prime order. *J. London Math. Soc. (2)*, 73(2):380–398, 2006.

[14] Jean Bourgain. Sum-product theorems and applications. In *Additive number theory*, pages 9–38. Springer, New York, 2010.

[15] Daniel Bump. *Automorphic forms and representations*, volume 55 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[16] Paula Burkhardt, Alice Zhuo-Yu Chan, Gabriel Currier, Stephan Ramon Garcia, Florian Luca, and Hong Suh. Visual properties of generalized Kloosterman sums. *J. Number Theory*, 160:237–253, 2016.

[17] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*. London Mathematical Society, London, 2010. Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965, Including a list of errata.

[18] Byungchul Cha, Daniel Fiorilli, and Florent Jouve. Independence of the zeros of elliptic curve L-functions over function fields. *Int. Math. Res. Not. IMRN*, (9):2614–2661, 2017.

[19] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[20] Keith Conrad. Factoring after Dedekind. available at https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf.

[21] Keith Conrad. Galois groups of cubics and quartics (not in characteristic 2). available at https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf.

[22] Barrie Cooper. *Almost Koszul duality and rational conformal field theory*. PhD Thesis, University of Bath, 2007.

[23] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[24] Cécile Dartyge and Greg Martin. Exponential sums with reducible polynomials. *Discrete Anal.*, pages Paper No. 15, 31, 2019.

[25] P. Deligne. Applications de la formule des traces aux sommes trigonométriques. In *Cohomologie étale*, volume 569 of *Lecture Notes in Math.*, pages 168–232. Springer, Berlin, 1977.

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

[27] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[28] Michael Drmota, Clemens Mullner, and Lukas Spiegelhofer. Primes as sums of fibonacci numbers. 2021. https://arxiv.org/abs/2109.04068.

[29] Michael Drmota and Robert F. Tichy. *Sequences, discrepancies and applications*, volume 1651 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.

[30] W. Duke. Hyperbolic distribution problems and half-integral weight Maass forms. *Invent. Math.*, 92(1):73–90, 1988.

[31] W. Duke, J. B. Friedlander, and H. Iwaniec. Equidistribution of roots of a quadratic congruence to prime moduli. *Ann. of Math. (2)*, 141(2):423–441, 1995.

[32] William Duke, Stephan Ramon Garcia, and Bob Lutz. The graphic nature of Gaussian periods. *Proc. Amer. Math. Soc.*, 143(5):1849–1863, 2015.

[33] Jordan S. Ellenberg, Philippe Michel, and Akshay Venkatesh. Linnik's ergodic method and the distribution of integer points on spheres. In *Automorphic representations and L-functions*, volume 22 of *Tata Inst. Fundam. Res. Stud. Math.*, pages 119–185. Tata Inst. Fund. Res., Mumbai, 2013.

[34] Jacques Faraut. *Analyse sur les groupes de Lie*. Éditions Calvage & Mounet.

[35] Étienne Fouvry, Satadal Ganguly, Emmanuel Kowalski, and Philippe Michel. Gaussian distribution for the divisor function and Hecke eigenvalues in arithmetic progressions. *Comment. Math. Helv.*, 89(4):979–1014, 2014.

[36] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. Trace functions over finite fields and applications. 2014. https://people.math.ethz.ch/~kowalski/elements.pdf.

[37] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. Trace functions over finite fields and their applications. In *Colloquium De Giorgi 2013 and 2014*, volume 5 of *Colloquia*, pages 7–35. Ed. Norm., Pisa, 2014.

[38] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. A study in sums of products. *Philos. Trans. Roy. Soc. A*, 373(2040):20140309, 26, 2015.

[39] Étienne Fouvry, Emmanuel Kowalski, Philippe Michel, and Will Sawin. Lectures on applied ℓ-adic cohomology. In *Analytic methods in arithmetic geometry*, volume 740 of *Contemp. Math.*, pages 113–195. Amer. Math. Soc., 2019.

[40] Etienne Fouvry and Philippe Michel. Sommes de modules de sommes d'exponentielles. *Pacific J. Math.*, 209(2):261–288, 2003.

[41] Etienne Fouvry and Philippe Michel. Corrigendum à l'article sommes de modules de sommes d'exponentielles. *Pacific J. Math.*, 225:199–200, 2006.

[42] Guy Fowler. Triples of singular moduli with rational product. *Int. J. Number Theory*, 16(10):2149–2166, 2020.

[43] A. García and J. F. Voloch. Fermat curves over finite fields. *J. Number Theory*, 30(3):345–356, 1988.

[44] Stephan Ramon Garcia, Trevor Hyde, and Bob Lutz. Gauss's hidden menagerie: from cyclotomy to supercharacters. *Notices Amer. Math. Soc.*, 62(8):878–888, 2015.

[45] Kurt Girstmair. Linear dependence of zeros of polynomials and construction of primitive elements. *Manuscripta Math.*, 39(1):81–97, 1982.

[46] Kurt Girstmair. Linear relations between roots of polynomials. *Acta Arith.*, 89(1):53–96, 1999.

[47] Ben Green. Sum-product phenomena in $\mathbb{F}_p$: a brief introduction. https://arxiv.org/abs/0904.2075.

[48] G. H. Hardy and S. Ramanujan. Asymptotic formulæin combinatory analysis [Proc. London Math. Soc. (2) **17** (1918), 75–115]. In *Collected papers of Srinivasa Ramanujan*, pages 276–309. AMS Chelsea Publ., Providence, RI, 2000.

[49] D. R. Heath-Brown and S. Konyagin. New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum. *Q. J. Math.*, 51(2):221–235, 2000.

[50] David Hilbert. *The theory of algebraic number fields*. Springer-Verlag, Berlin, 1998. Translated from the German and with a preface by Iain T. Adamson, With an introduction by Franz Lemmermeyer and Norbert Schappacher.

[51] C. Hooley. On the distribution of the roots of polynomial congruences. *Mathematika*, 11:39–49, 1964.

[52] Loo Keng Hua. *Introduction to number theory*. Springer-Verlag, Berlin-New York, 1982. Translated from the Chinese by Peter Shiu.

[53] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory.*, volume 84 of *Grad. Texts Math.* New York etc.: Springer-Verlag, 2nd ed. edition, 1990.

[54] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[55] Karsten Johnsen. Lineare Abhängigkeiten von Einheitswurzeln. *Elem. Math.*, 40(3):57–59, 1985.

[56] Florent Jouve, Emmanuel Kowalski, and David Zywina. An explicit integral polynomial whose splitting field has Galois group $W(E_8)$. *J. Théor. Nombres Bordeaux*, 20(3):761–782, 2008.

[57] N. Kaiser. Mean eigenvalues for simple, simply connected, compact Lie groups. *J. Phys. A*, 39(49):15287–15298, 2006.

[58] Nicholas M. Katz. *Sommes exponentielles*, volume 79 of *Astérisque*. Société Mathématique de France, Paris, 1980. Course taught at the University of Paris, Orsay, Fall 1979, With a preface by Luc Illusie, Notes written by Gérard Laumon, With an English summary.

[59] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

[60] Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1990.

[61] Nicholas M. Katz. *Moments, monodromy, and perversity: a Diophantine perspective*, volume 159 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2005.

[62] Nicholas M. Katz. *Convolution and equidistribution*, volume 180 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2012. Sato-Tate theorems for finite-field Mellin transforms.

[63] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.

[64] Dubi Kelmer. Distribution of twisted Kloosterman sums modulo prime powers. *Int. J. Number Theory*, 6(2):271–280, 2010.

[65] Lars Kindler and Kay Rülling. Introductory course on ℓ-adic sheaves and their ramification theory on curves, 2014. https://arxiv.org/abs/1409.6899.

[66] H. D. Kloosterman. On the Representation of Numbers in the Form $ax^2 + by^2 + cz^2 + dt^2$. *Proc. London Math. Soc. (2)*, 25:143–173, 1926.

[67] S. V. Konyagin. Estimates for trigonometric sums over subgroups and for Gauss sums. In *IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part III (Russian) (Tula, 2001)*, pages 86–114. Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002.

[68] Sergei Konyagin. Exponential sums over multiplicative groups in fields of prime order and related combinatorial problems. Lecture notes available at https://www.mathtube.org/sites/default/files/lecture-notes/Konyagin_Lectures.pdf.

[69] Emmanuel Kowalski. Exponential sums over finite fields: elementary methods. lecture notes available at https://people.math.ethz.ch/~kowalski/exponential-sums-elementary.pdf.

[70] Emmanuel Kowalski. *Un cours de théorie analytique des nombres*, volume 13 of *Cours Spécialisés [Specialized Courses]*. Société Mathématique de France, Paris, 2004.

[71] Emmanuel 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.

[72] Emmanuel Kowalski. Poincaré and analytic number theory. In *The scientific legacy of Poincaré*, volume 36 of *Hist. Math.*, pages 73–85. Amer. Math. Soc., Providence, RI, 2010.

[73] Emmanuel Kowalski. *Convolution and equidistribution: Sato-Tate theorems for finite fields Mellin transforms* [book review of mr2850079]. *Bull. Amer. Math. Soc. (N.S.)*, 51(1):141–149, 2014.

[74] Emmanuel Kowalski. *An introduction to the representation theory of groups*, volume 155 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2014.

[75] Emmanuel Kowalski. *An introduction to probabilistic number theory*, volume 192 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2021.

[76] Emmanuel Kowalski and William F. Sawin. Kloosterman paths and the shape of exponential sums. *Compos. Math.*, 152(7):1489–1516, 2016.

[77] Emmanuel Kowalski and Théo Untrau. Ultra-short sums of trace functions, 2023. https://arxiv.org/abs/2302.13670, to appear in *Acta Arith.*

[78] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974.

[79] Pär Kurlberg. Bounds on exponential sums over small multiplicative subgroups. In *Additive combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, pages 55–68. Amer. Math. Soc., Providence, RI, 2007.

[80] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[81] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, 2018. Second edition, With a foreword by Barry Mazur.

[82] Greg Martin and Scott Sitar. Erdös-Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples. *Mathematika*, 57(1):1–29, 2011.

[83] Djordje Milićević and Sichen Zhang. Distribution of Kloosterman paths to high prime power moduli, 2020. https://arxiv.org/abs/2005.08865.

[84] H. L. Montgomery, R. C. Vaughan, and T. D. Wooley. Some remarks on Gauss sums associated with kth powers. *Math. Proc. Cambridge Philos. Soc.*, 118(1):21–33, 1995.

[85] Hugh L. Montgomery and Robert C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[86] Gerald Myerson. A combinatorial problem in finite fields. II. *Quart. J. Math. Oxford Ser. (2)*, 31(122):219–231, 1980.

[87] Jürgen 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.

[88] H. Niederreiter and Walter Philipp. Berry-esseen bounds and a theorem of erdös and turán on uniform distribution mod 1. *Duke Math. J.*, 40:633–649, 1973.

[89] Corentin Perret-Gentil. *Probabilistic aspects of short sums of trace functions over finite fields*. PhD Thesis, ETH Zürich, 2016. https://corentinperretgentil.gitlab.io/static/documents/probabilistic-aspects-trace-functions.pdf.

[90] Corentin Perret-Gentil. Integral monodromy groups of Kloosterman sheaves. *Mathematika*, 64(3):652–678, 2018.

[91] Guillaume Ricotta and Emmanuel Royer. Kloosterman paths of prime powers moduli. *Comment. Math. Helv.*, 93(3):493–532, 2018.

[92] J. Rivat and G. Tenenbaum. Constantes d'Erdös-Turán. *Ramanujan J.*, 9(1-2):111–121, 2005.

[93] Michael Rubinstein and Peter Sarnak. Chebyshev's bias. *Experiment. Math.*, 3(3):173–197, 1994.

[94] Walter Rudin. *Fourier analysis on groups*. Interscience Tracts in Pure and Applied Mathematics, No. 12. Interscience Publishers (a division of John Wiley and Sons), New York-London, 1962.

[95] Wolfgang M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[96] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, second edition, 1989. With the collaboration of Willem Kuyk and John Labute.

[97] I. E. Shparlinskiĭ. Estimates for Gauss sums. *Mat. Zametki*, 50(1):122–130, 1991.

[98] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[99] Sankar Sitaraman. Note on Artin's conjecture on primitive roots. *Hardy-Ramanujan J.*, 44:136–142, 2021.

[100] Andrew V. Sutherland. Sato-Tate distributions. In *Analytic methods in arithmetic geometry*, volume 740 of *Contemp. Math.*, pages 197–248. Amer. Math. Soc., [Providence], RI, 2019.

[101] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.13.4*, 2022. available from http://pari.math.u-bordeaux.fr/.

[102] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2020. https://www.sagemath.org.

[103] Théo Untrau. Equidistribution of exponential sums indexed by a subgroup of fixed cardinality, 2021. https://arxiv.org/abs/2112.05441, to appear in *Math. Proc. Cambridge Philos. Soc.*

[104] Jeffrey D. Vaaler. Some extremal functions in Fourier analysis. *Bull. Amer. Math. Soc. (N.S.)*, 12(2):183–216, 1985.

[105] B. L. van der Waerden. Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt. *Monatsh. Math. Phys.*, 43(1):133–147, 1936.

[106] Chunlin Wang. Distribution of residues of an algebraic number modulo ideals of degree one, 2021. https://arxiv.org/abs/2108.05496.

[107] Hermann Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77(3):313–352, 1916.

[108] Alessandro Zaccagnini. Introduction to the circle method of Hardy, Ramanujan and Littlewood. Lectures at the Harish-Chandra Research Institute, available at https://people.dmi.unipr.it/alessandro.zaccagnini/psfiles/didattica/HRI.pdf.