Université de Montréal

On some Density Theorems in Number Theory and Group Theory

par

Mohammad Bardestani

Département de mathématiques et de statistique

Faculté des arts et des sciences

Thèse présentée à la Faculté des études supérieures

en vue de l'obtention du grade de

Philosophi Doctor (Ph.D.)
en Mathmatiques

October 2011

© Mohammad Bardestani, 2011

Université de Montréal

Faculté des études supérieures

Cette thèse intitulée

On some Density Theorems in Number Theory and Group Theory

présentée par

Mohammad Bardestani

a été évaluée par un jury composé des personnes suivantes :

Abraham Broer

(président-rapporteur)

Andrew Granville

(directeur de recherche)

Hershy Kisilevsky

(membre du jury)

Emmanuel Kowalski

(examinateur externe)

Pierre Bastien

(représentant du doyen de la FES)

Thèse acceptée le:

30 Octobre 2012

RÉSUMÉ

Gowers [31], dans son article sur les matrices quasi-aléatoires, étudie la question, posée par Babai et Sós, de l'existence d'une constante $c > 0$ telle que tout groupe fini possède un sous-ensemble sans produit de taille supérieure ou égale à $c|G|$. En prouvant que, pour tout nombre premier p assez grand, le groupe $\mathrm{PSL}_2(\mathbb{F}_p)$ (d'ordre noté n) ne possède aucun sous-ensemble sans produit de taille $cn^{8/9}$, il y répond par la négative.

Nous allons considérer le problème dans le cas des groupes compacts finis, et plus particulièrement des groupes profinis $\mathrm{SL}_k(\mathbb{Z}_p)$ et $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$. La première partie de cette thèse est dédiée à l'obtention de bornes inférieures et supérieures exponentielles pour la mesure suprémale des ensembles sans produit. La preuve nécessite d'établir préalablement une borne inférieure sur la dimension des représentations non-triviales des groupes finis $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ et $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$. Notre théorème prolonge le travail de Landazuri et Seitz [49], qui considèrent le degré minimal des représentations pour les groupes de Chevalley sur les corps finis, tout en offrant une preuve plus simple que la leur.

La seconde partie de la thèse à trait à la théorie algébrique des nombres. Un polynôme monogène f est un polynôme unitaire irréductible à coefficients entiers qui endengre un corps de nombres monogène. Pour un nombre premier q donné, nous allons montrer, en utilisant le théorème de densité de Tchebotariov, que la densité des nombres premiers p tels que $t^q - p$ soit monogène est supérieure ou égale à $(q-1)/q$. Nous allons également démontrer que, quand $q = 3$, la densité des nombres premiers p tels que $\mathbb{Q}(\sqrt[3]{p})$ soit non monogène est supérieure ou égale à $1/9$.

Mots clés: groupes profinis, représentations complexes, opérateur de Hilbert-Schmidt, décomposition en valeurs singuliéres, théorème de densité de Chebotarev, corps monogénique, équation de Thue.

ABSTRACT

Gowers [31] in his paper on quasirandom groups studies a question of Babai and Sós asking whether there exists a constant $c > 0$ such that every finite group G has a product-free subset of size at least $c|G|$. Answering the question negatively, he proves that for sufficiently large prime p, the group $\mathrm{PSL}_2(\mathbb{F}_p)$ has no product-free subset of size $\geq cn^{8/9}$, where n is the order of $\mathrm{PSL}_2(\mathbb{F}_p)$.

We will consider the problem for compact groups and in particular for the profinite groups $\mathrm{SL}_k(\mathbb{Z}_p)$ and $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$. In Part I of this thesis, we obtain lower and upper exponential bounds for the supremal measure of the product-free sets. The proof involves establishing a lower bound for the dimension of non-trivial representations of the finite groups $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ and $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$. Indeed, our theorem extends and simplifies previous work of Landazuri and Seitz [49], where they consider the minimal degree of representations for Chevalley groups over a finite field.

In Part II of this thesis, we move to algebraic number theory. A monogenic polynomial f is a monic irreducible polynomial with integer coefficients which produces a monogenic number field. For a given prime q, using the Chebotarev density theorem, we will show the density of primes p, such that $t^q - p$ is monogenic, is greater than or equal to $(q-1)/q$. We will also prove that, when $q = 3$, the density of primes p, which $\mathbb{Q}(\sqrt[3]{p})$ is non-monogenic, is at least $1/9$.

Keywords. Profinite group, Complex representation, Hilbert-Schmidt operator, Singular value decomposition, Chebotarev density theorem, Monogenic field, Thue equation.

Dedicated to professor Mehrdad Shahshahani who has inspired and encouraged me to study mathematics.

CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENT

In the last five years I received a lot of help from many people, without whom I could not have written this thesis. I am greatly indebted to my advisor Andrew Granville. I would like to use this opportunity to thank for his efforts. I consider it very fortunate, that I could learn from him. I learned additive combinatorics and of course analytic number theory from him. His course in Pretentious analytic number theory was one of the most interesting course I have taken in my life. He showed me how one can go beyond the history of analytic number theory, and give a different perspective of such an old theory.

I owe a lot to Hershy Kisilevsky. I learned algebraic number theory and class field theory from him, and later I had many fruitful discussions with him on different aspects of my work. I thank him for his continued interest and encouragement.

I wish to thank Adrian Iovita. I learned algebraic geometry from him. His course in Étale Cohomology is a model for me to learn how an expert could explain one of the hardest subject in mathematics to students.

I would also like to thank Abraham Broer for many helpful discussions and for all the help.

I am very grateful to my friend Keivan Mallahi-Karai for letting me work with him and also sharing his amazing insight with me.

It is very hard to truly thank all professors in the math department. I wish to specially thank Eyal Goren, Henri Darmon , Chantal David, Matilde Lalin, John Voight, Marlène Frigon, Iosif Polterovich and Octavian Cornea.

My special thanks to my friends François Charette, Dimitri Dias, Kevin Henriot, Aziz Raymond Elmahdaoui and Mostafa Nasri. Thank you very much for all of your help.

I would not be able to do math without my true friends, and it is a privilege for me to thank them. I wish to thank, Marzieh Mehdizadeh, Bahare Mirza-Hossein, Jim Parks, Farzad Aryan, Daniel Fiorilli, Dimitris Koukoulopoulos, Mariah Hamel, Mat Rogers, Fai Chandee, Ke Gong, Shabnam Akhtari, Igor Wigman, Youness Lamzouri and Tristan Freiberg. I would like to thank all the good people of the Math department at the Université de Montréal for creating a warm, supportive environment.

I am grateful for financial support from the Institut des sciences mathématiques in Montréal.

It is impossible to express how much I am indebted to my lovely wife Najmeh. I would not be able to do anything without her. Thank you for all you've done from the bottom of my heart. All I have done in my life had a simple reason: to make my family proud. I hope I could make them proud and I wish to thank them, my father and my mother, thank you.

Chapter 1

INTRODUCTION

In this chapter we will give a general sketch of our thesis. We will mainly focus on general ideas and present the results of the thesis, which are divided into two main chapters. The first one concerns density results in additive combinatorics on compact groups, and the other one studies the distribution of monogenicity of a family of polynomials. We will also set some notations and definitions.

1.1. Product-free sets in groups

Additive combinatorics has been investigated extensively over the last decade and now consists of a variety of tools from graph theory, group theory, number theory, algebraic geometry and many other methods in mathematics. Amazingly, in the last decade, computer science has also contributed in this branch of mathematics, and raised many important questions that turn out to be challenging for mathematicians. For instance "expander graphs" are highly connected sparse finite graphs. One might interpret these graphs as networks that transmit information very fast but in the same time that are very economical, meaning that they do not have many cables. It is important for computer scientists to design such a network. Various deep mathematical theories have been used to give explicit constructions of expander graphs, including the Kazhdan property (T) from representation theory of semisimple Lie groups, the Ramanujan Conjecture (proved by Deligne) from the theory of automorphic forms, and more. Lubotzky's survey paper [51] is an excellent reference for the theory of expander graphs.

Another aspect of additive combinatorics is the multiplicative (or additive) structure of groups. To single out one example, let us mention a famous theorem of Schur, which states that for any k, there exists $N = N(k)$ such that for any partition of the set $\{1, \dots, N\}$ into k subsets, there exist numbers x, y, z in the same subset (where $x = y$ is allowed) such that $x + y = z$. One approach to prove Schur's theorem, is to use "Ramsey theory" which is a graph theoretical concept (See [50], Chapter 8). It is very interesting to observe how different sets of ideas can be put together and prove this beautiful theorem.

In contrast to Schur's theorem, one might ask for which subsets A of the positive integers, the equation $x + y = z$ does not have any solutions in A. These sets are called "product-free" sets. More formally:

Definition 1.1.1. *For a given group G, a subset $A \subseteq G$ is called a* **product-free** *set if there are no solutions to the equation $xy = z$, with $x, y, z \in A$.*

Remark 1.1.1. *We use "multiplicative structure" typically in the non-commutative setting and "additive structure" in the commutating setting. Indeed we defined product-free sets for multiplicative groups, however the same definition holds for additive groups. In that case product-free sets are called "***sum-free***" sets. But in this thesis, for simplicity, the multiplicative notation will be used even when working in the additive case.*

More intuitively, a subset $A \subseteq G$ is product-free if

$$A^2 \cap A = \emptyset,$$

where

$$A^2 = \{xy : x, y \in A\}.$$

First remark to point out, regarding to this definition, is that if a subset $A \subseteq G$ has any group structure inside, then A can not be a product-free set. In other words, a product-free set is very rigid. Indeed this phenomenon turns out to be a source of many investigations in additive combinatorics. To illustrate this point, let us mention an observation. Let G be a finite group of order n, and let A be a subset of G. Suppose that $|A| > n/2$. Let us denote

$$A^{-1} := \{a^{-1} : a \in G\}.$$

For every $g \in G$ we have

$$|gA^{-1} \cap A| = |gA^{-1}| + |A| - |gA^{-1} \cup A| > n/2 + n/2 - n = 0,$$

hence for some $a_1, a_2 \in A$ we have $ga_1^{-1} = a_2$. Therefore $g = a_1a_2 \in AA$ which implies that $A^2 = G$.

From this, one can ask if for some group G of order n, there exists a product-free set of size exactly $n/2$.

Example 1.1.1. *The set of quadratic non-residue modulo prime p is an example of a product-free set in the multiplicative group $\mathbb{F}_p^*$ of size $(p-1)/2$.*

Then almost immediately the following questions arise:

Question 1. *How big is the largest product-free subset of G?*

Question 2. *How many product-free subsets of G are there?*

Both of these questions have been considered by many mathematicians from different point of views. In this thesis, we mainly concentrate on Question 1.

Question 2 was motivated by a conjecture of Cameron and Erdös [10], where they conjectured that the number of sum-free subsets of $\{1, 2, \cdots, n\}$ is $O(2^{n/2})$. Alon [1], Calkin [9], and Erdös and Granville (unpublished) proved independently that the number of sum-free subsets of $\{1, 2, \cdots, n\}$ is

$$2^{n/2+o(n)}.$$

The Cameron and Erdös conjecture was eventually proven by Ben Green [38].

Back to Question 1, we fix some definitions and notations.

Definition 1.1.2. *For a given finite group G, let $\alpha(G)$ denote the size of the largest product-free set in G, and the "***product-free density***" is defined by*

$$\mathrm{pf}(G) := \frac{\alpha(G)}{|G|}. \tag{1.1.1}$$

To clarify our definition, let us remark one more time that we defined this notation for multiplicative groups, however the same definition holds for additive groups. In that case product-free density is called "**sum-free density**". But in this thesis, for simplicity, the multiplicative notation will be used even when working in the additive case.

Lemma 1.1.1. *For $n \geq 2$,*

$$\begin{aligned} &\alpha(\mathbb{Z}/(n\mathbb{Z})) = n/2, && \text{if } n \text{ is even,} \\ &\alpha(\mathbb{Z}/(n\mathbb{Z})) \geq \lfloor (n+1)/3 \rfloor && \text{if } n \text{ is odd.} \end{aligned} \tag{1.1.2}$$

Proof: First notice that for any given group G, if $A \subseteq G$ is a product-free set, then for any $a \in A$ we have $aA \cap A = \emptyset$, hence

$$|G| \geq |A| + |aA| = 2|A|.$$

Therefore $\mathrm{pf}(G) \leq 1/2$. Now we approximate $\alpha(\mathbb{Z}/(n\mathbb{Z}))$. If n is even, take

$$A = \{1, 3, 5, \ldots, n-1\}.$$

Then A is a product-free set since for $x, y \in A$, we have that $x + y$ is even, while the elements of A are odd. For an odd n, take

$$A = \{k, k+1, \ldots, 2k-1\} = \{k + j : 0 \leq j \leq k-1\},$$

where $k := \lfloor (n+1)/3 \rfloor$. For $x, y \in A$ we have

$$2k - 1 < 2k \leq x + y \leq 4k - 2 < n + k,$$

so in this case also, A is a product-free set. □

Notice that if $n \geq 3$ is odd then

$$\lfloor (n+1)/3 \rfloor \geq 2n/7.$$

So from Lemma 1.1.1 we have

Corollary 1.1.1. *For $n \geq 2$ we have*

$$\mathrm{pf}(\mathbb{Z}/(n\mathbb{Z})) \geq 2/7. \tag{1.1.3}$$

We remark that this inequality is sharp, since Rhemtulla and Street [58] proved that

$$\mathrm{pf}(\underbrace{\mathbb{Z}/(7\mathbb{Z}) \times \cdots \times \mathbb{Z}/(7\mathbb{Z})}_{m}) = \frac{2}{7},$$

for all m.

Moving to general groups, we remark that the following simple observation is very useful.

Lemma 1.1.2. *Let H be a proper normal subgroup of G then*

$$\mathrm{pf}(G) \geq \mathrm{pf}(G/H).$$

Proof: Consider the natural projection $\pi : G \longrightarrow G/H$. Let A be a product-free subset in G/H, then $\pi^{-1}(A)$ is a product-free set in G. So we have

$$\alpha(G) \geq |\pi^{-1}(A)| = |A||\ker \pi| = |A||H|.$$

So if we take $A \subset G/H$ to be a maximal product-free set, then

$$\mathrm{pf}(G) = \frac{\alpha(G)}{|G|} \geq \frac{|A||H|}{|G|} = \frac{|A|}{[G:H]} = \mathrm{pf}(G/H).$$

□

Example 1.1.2. *For any non-trivial abelian group G of even order, notice that we have a surjective homomorphism*

$$G \longrightarrow \mathbb{Z}/(2\mathbb{Z}),$$

therefore

$$\mathrm{pf}(G) = \frac{1}{2}.$$

From the fundamental theorem of finite abelian groups, we know that any finite abelian group G is isomorphic to a direct sum of finite cyclic groups. More precisely

$$G \cong \mathbb{Z}/(n_1\mathbb{Z}) \oplus \mathbb{Z}/(n_2\mathbb{Z}) \oplus \cdots \oplus \mathbb{Z}/(n_k\mathbb{Z}),$$

for some integers $n_i \in \mathbb{N}$. So we obtain

Corollary 1.1.2. *For any non-trivial abelian group G, we have*

$$\mathrm{pf}(G) \geq 2/7.$$

For abelian groups, we also have a geometric picture that heuristically gives us a product-free set of density $1/3$. From the circle

$$S^1 = \{e^{2\pi i\theta} : 0 \leq \theta \leq 1\},$$

take a sector

$$A := \{e^{2\pi i\theta} : 1/3 \leq \theta < 2/3\}.$$

Then A is product-free set (See Figure 1.1). Note that the cyclic group $\mathbb{Z}/(n\mathbb{Z})$

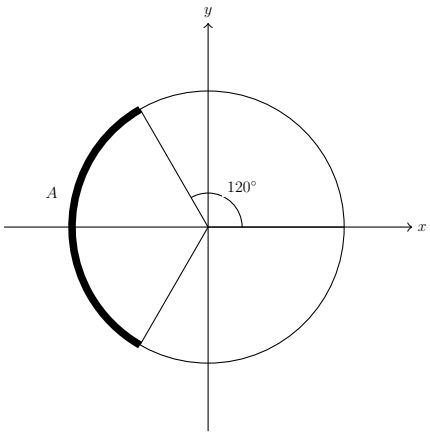


FIGURE 1.1. Product-free set in S^1

can be arranged into the circle by considering the group of nth roots of unity, and then in $\mathbb{Z}/(n\mathbb{Z})$ we get a product-free set of density roughly 1/3. As mentioned earlier, any abelian group is the product of cyclic groups, then basically in any abelian group we can get a product-free set of density roughly 1/3. Green and Ruzsa (See Theorem 1.5 [39]), used Fourier analysis methods to prove this.

If something can be proven for abelian groups, then it is often possible to generalize it to solvable groups. To be more precise, let us recall a definition of solvable groups.

Let G be a non-trivial group. Recall that the commutator of $x, y \in G$ is

$$[x, y] := xyx^{-1}y^{-1}.$$

The group G' generated by the commutators in G is called the commutator or first derived subgroup of G. Notice that G' is a normal subgroup of G and G/G' is an abelian group. The second derived subgroup of G is $G^{(2)} := (G')'$; the third is $G^{(3)} := (G^{(2)})'$; and so on. So we have the following normal series

$$G \supseteq G' \supseteq G^{(2)} \supseteq G^{(3)} \supseteq \cdots .$$

Definition 1.1.3. *A group G is called* **solvable** *if $G^{(k)} = 1$ for some k.*

Example 1.1.3. *The following groups are solvable.*

1. *Abelian groups.*
2. *p-groups. Indeed any nilpotent group is solvable.*

Solvable groups indeed are those groups that are constructed from an "abelian tower".

Corollary 1.1.3. *If G is a solvable group then*

$$\mathrm{pf}(G) \geq 2/7.$$

Proof: Since G is solvable, then G' is a pure normal subgroup of G since otherwise $G^{(k)} = G$ for all k which is a contradiction to the definition of solvable groups. But G/G' is an abelian group then by Lemma 1.1.2 we have

$$\mathrm{pf}(G) \geq \mathrm{pf}(G/G') \geq 2/7.$$

□

Another way to construct a product-free set is to take a pure subgroup of G, and consider one of its non-trivial cosets. More precisely.

Lemma 1.1.3. *Let H be a subgroup of index $k \geq 2$ and let $A = xH$ be a non-trivial coset of H. Then A is a product-free set.*

Proof: We have

$$(xh_1)(xh_2) = (xh_3) \Longleftrightarrow x = h_1^{-1}h_3h_2^{-1} \in H, \tag{1.1.4}$$

which is a contradiction, since $x \notin H$. □

Therefore, to construct a big product-free set, we need to find a subgroup with small index. From the classification of finite simple groups it can be shown that every finite simple group of order n has a subgroup of index at most $Cn^{3/7}$ and hence a product-free set of size at least $cn^{4/7}$.

These examples motivated Babai and Sós [3] to ask:

Question 3 (Babai and Sós)**.** *Does there exist a constant $c > 0$ such that every group of order n has a product-free set of size $> cn$?*

As we saw earlier, Babai and Sós' question is true for solvable groups. So if one wants to give a negative answer to this question, then one needs to look at those groups that are as non-abelian as possible. For instance, simple groups might be a good candidate for a counterexample.

The special linear group of degree n over a field F is the set of n by n matrices with determinant 1. More formally

Definition 1.1.4.

$$\mathrm{SL}_n(F) := \{A \in M_n(F) : \det(A) = 1\}. \tag{1.1.5}$$

It is clear that $\mathrm{SL}_n(F)$ is not a simple group since $\pm I$ is in its center. Instead we can look at the projective special linear group defined by

$$\mathrm{PSL}_n(F) := \mathrm{SL}_n(F)/\{\pm I\}.$$

For the finite field $\mathbb{F}$, the group $\mathrm{PSL}_n(\mathbb{F})$ is a finite simple group, except for $n = 2$ and $\mathbb{F} = \mathbb{F}_2$ or $\mathbb{F}_3$.

Gowers in his remarkable paper on quasirandom groups [31], gives a negative answer to Question 3 and proves that for sufficiently large prime p, the group $\mathrm{PSL}_2(\mathbb{F}_p)$ has no product-free subset of size $cn^{8/9}$, where n is the order of $\mathrm{PSL}_2(\mathbb{F}_p)$. Gowers' theorem, apart from its intrinsic interest, has important applications. Indeed Nikolov and Pyber [55], by using Gowers' theorem, have obtained improved versions of recent theorems of Helfgott [41] and of Shalev [65] concerning product decompositions of finite simple groups. Gowers method, which is known as Gowers' trick, has also appeared in several other papers, namely [64, 62].

Behind Gowers' result lies the fact that $\mathrm{PSL}_2(\mathbb{F}_p)$ has no nontrivial irreducible representation in low dimensions. The same property has been used by Lubotzky, Phillips and Sarnak [52] to show that the Ramanujan graphs are expanders. Indeed, finding a lower bound for the dimension of non-trivial representations of a group has many applications in number theory and additive combinatorics. Sarnak and Xue in their remarkable paper [61], exploited this and introduced the concept of high multiplicity of non-trivial eigenvalues. This concept then became ubiquitous in number theory and additive combinatorics. For instance, in order to show that $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ is an expander family, with respect to an appropriate generating set, Bourgain and Gamburd [7, 8] needed this bound and obtained a lower bound for the degree of all faithful representations of $\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))$.

Let us very briefly explain how representation theory will participate in this sort of question. We consider a more general setting. For subsets A, B, C of a

group G, we would like to know when the following equation is verified:

$$xy = z, \qquad x \in A, y \in B, z \in C. \tag{1.1.6}$$

Notation 1. *Let us denote the vector space of all functions from G to $\mathbb{C}$ by $\mathbb{C}^G$. Sometimes it is more appropriate to denote this space by $L^2(G)$, since then Fourier analysis can be applied to G.*

For any two functions $f_1, f_2 \in \mathbb{C}^G$, the convolution is defined as follows:

$$f_1 * f_2(y) = \sum_{x \in G} f_1(x) f_2(x^{-1}y) = \sum_{x \in G} f_1(yx^{-1}) f_2(x).$$

Therefore to show that $xy = z$ has a solution, one needs to show that for some $z \in C$,

$$1_A * 1_B(z) = \sum_{\substack{xy=z \\ x \in A, y \in B, z \in C}} 1 \neq 0. \tag{1.1.7}$$

So if one can show that the support of the function $1_A * 1_B$ is a big set, then we can perhaps show that there is a solution for the equation $xy = z$. So let assume that A and B are reasonably big sets in a group G, then we would like to show that AB fills up almost all of the group G. A usual method of attack is to prove that $1_A * 1_B$ is an almost constant function. So we seek the following strategy: **we need to show that $1_A * 1_B$ has small variance**.

To be more precise, let us set some notations. Notice that $\mathbb{C}^G$ is an inner-product space. Indeed for $f_1, f_2 \in \mathbb{C}^G$, we define

$$\langle f_1, f_2 \rangle := \sum_{x \in G} f_1(x) \overline{f_2}(x). \tag{1.1.8}$$

Then we can define the L^2-norm on $\mathbb{C}^G$. For $f \in \mathbb{C}^G$, define

$$\|f\|_2^2 := \langle f, f \rangle = \sum_{x \in G} |f(x)|^2.$$

First, we compute the mean of $1_A * 1_B$.

Lemma 1.1.4.

$$\mathbb{E}(1_A * 1_B) = \frac{|A||B|}{|G|}.$$

Proof:

$$\mathbb{E}(1_A * 1_B) := \frac{1}{|G|}\sum_{x\in G} 1_A * 1_B(x) = \frac{1}{|G|}\sum_{x\in G}\left(\sum_{y\in G} 1_A(xy^{-1})1_B(y)\right)$$
$$= \frac{1}{|G|}\sum_{y\in G}\left(\sum_{x\in G} 1_A(xy^{-1})\right)1_B(y)$$
$$= \frac{|A||B|}{|G|}.$$

□

Set

$$\Sigma := \{x \in G : 1_A * 1_B(x) = 0\}.$$

Our aim is to show that Σ is a small set.

Lemma 1.1.5. *We have*

$$|\Sigma| \leq \left(\frac{|G|}{|A||B|}\right)^2 \|1_A * 1_B - \mathbb{E}(1_A * 1_B)\|_2^2 . \tag{1.1.9}$$

Proof:

$$\|1_A * 1_B - \mathbb{E}(1_A * 1_B)\|_2^2 = \sum_{x\in G}\left|1_A * 1_B(x) - \frac{|A||B|}{|G|}\right|^2$$
$$\geq \sum_{x\in \Sigma}\left|1_A * 1_B(x) - \frac{|A||B|}{|G|}\right|^2$$
$$= \left(\frac{|A||B|}{|G|}\right)^2 |\Sigma|.$$

□

Then if the variance $\|1_A * 1_B - \mathbb{E}(1_A * 1_B)\|_2$ is small, we can deduce that $|\Sigma|$ is small, which in particular implies that $C \not\subseteq \Sigma$, if C is big enough. We remark that

$$\|1_A * 1_B - \mathbb{E}(1_A * 1_B)\|_2 = \|(1_A - \mathbb{E}(1_A)) * 1_B\|_2 . \tag{1.1.10}$$

For technical reasons, it is easier to work with a "normalized function", where we normalize a function by subtracting its mean. More precisely we define:

Definition 1.1.5.

$$L_0^2(G) := \{f \in L^2(G) : \mathbb{E}(f) = 0\}.$$

Notice that $1_A - \mathbb{E}(1_A) \in L_0^2(G)$ since $\mathbb{E}(1_A - \mathbb{E}(1_A)) = 0$. We prefer to work with $1_A - \mathbb{E}(1_A)$ (or $1_B - \mathbb{E}(B)$) rather than 1_A.

Now the question changes to

Question 4. *Let $f_1, f_2 \in L^2(G)$, and assume that at least one of them belongs to $L_0^2(G)$. What can we say about $\|f_1 * f_2\|_2$?*

The first attempt to answer this question is to use the Cauchy-Schwarz inequality. Indeed, we have

Lemma 1.1.6. *Let $f_1, f_2 \in L^2(G)$ then*

$$\|f_1 * f_2\|_2 \leq |G|^{1/2} \|f_1\|_2 \|f_2\|_2. \tag{1.1.11}$$

Proof: From the Cauchy-Schwarz inequality we have

$$\begin{aligned}
\|f_1 * f_2\|_2 &= \left(\sum_{x \in G} |f_1 * f_2(x)|^2 \right)^{1/2} = \left(\sum_{x \in G} \left| \sum_{y \in G} f_1(xy^{-1}) f_2(y) \right|^2 \right)^{1/2} \\
&\leq \left(\sum_{x \in G} \left[\left(\sum_{y \in G} |f_1(xy^{-1})|^2 \right) \left(\sum_{y \in G} |f_2(y)|^2 \right) \right] \right)^{1/2} \\
&= |G|^{1/2} \|f_1\|_2 \|f_2\|_2.
\end{aligned}$$

□

But this inequality is not sharp enough to show that the variance is small. It turns out that when the minimal dimension of all non-trivial representations of G is big enough then the above inequality can be improved significantly.

Definition 1.1.6. *Let G be a finite group and let us define*

$$m(G) := \min_{\rho \neq 1} d_\rho,$$

where d_ρ denotes the dimension of an irreducible representation *ρ. Here we denote the trivial representation by* 1.

The following theorem gives an answer to Question 4.

Theorem 1.1.1 (Babai-Nikolov-Pyber)**.** *Let $f_1, f_2 \in L^2(G)$. If at least one of f_1, f_2 belongs to $L_0^2(G)$, then*

$$\|f_1 * f_2\|_2 \leq \left(\frac{|G|}{m(G)} \right)^{1/2} \|f_1\|_2 \|f_2\|_2. \tag{1.1.12}$$

From this theorem we can prove the following result:

Corollary 1.1.4 (Gowers [31]). *For a finite group G, let $A, B, C \subseteq G$ be so that*

$$|A||B||C| > \frac{|G|^3}{m(G)}.$$

Then $AB \cap C \neq \emptyset$. In particular if $|A| > |G|m(G)^{-1/3}$, then A is not a product-free set. Therefore

$$\mathrm{pf}(G) \leq m(G)^{-1/3}.$$

Proof: From (1.1.9) and Theorem 1.1.1 we have

$$\begin{aligned} |\Sigma| &\leq \left(\frac{|G|}{|A||B|}\right)^2 \|(1_A - \mathbb{E}(1_A)) * 1_B\|_2^2 \\ &\leq \left(\frac{|G|}{|A||B|}\right)^2 \frac{|G|}{m(G)} \|1_A - \mathbb{E}(1_A)\|_2^2 \|1_B\|_2^2 \\ &\leq \left(\frac{|G|}{|A||B|}\right)^2 \frac{|G|}{m(G)} |A||B| \\ &= \frac{|G|^3}{|A||B|m(G)} < |C|, \end{aligned} \tag{1.1.13}$$

by hypothesis, which implies that $C \not\subseteq \Sigma$. So $AB \cap C \neq \emptyset$. □

For $\mathrm{PSL}_2(\mathbb{F}_p)$, from a theorem due to Frobenius (See [17], Theorem 3.5.1), we have

$$m(\mathrm{PSL}_2(\mathbb{F}_p)) \geq (p-1)/2.$$

Clearly $|\mathrm{PSL}_2(\mathbb{F}_p)| \approx p^3$ and this shows that the minimal degree of non-trivial representations of $\mathrm{PSL}_2(\mathbb{F}_p)$ is roughly $|\mathrm{PSL}_2(\mathbb{F}_p)|^{1/3}$.

Corollary 1.1.5.

$$\mathrm{pf}(\mathrm{PSL}_2(\mathbb{F}_p)) \leq \left(\frac{2}{p-1}\right)^{1/3}.$$

One might consider a similar problem for compact groups. Indeed, a finite group should be seen as a compact group with the counting measure, so the next generalization of finite groups is compact groups with the normalized Haar measure.

Let G be a compact, Hausdorff, second countable topological group and μ denote the Haar measure on G, normalized so that $\mu(G) = 1$. Note that since G is compact, and hence unimodular, a left Haar measure is automatically right

invariant. Similar to the finite case, a measurable subset of A is said to be **product-free** if $A^2 \cap A = \emptyset$. We define the **product-free measure** by

Definition 1.1.7. *Let G be a compact group with normalized Haar measure μ. Define the product-free measure of G by*

$$\mathrm{pf}(G) = \sup\{\mu(A) : A \subseteq G \text{ is measurable }, A \cap A^2 = \emptyset\}.$$

Let $\mathrm{U}_n(\mathbb{C})$ be the unitary group on $\mathbb{C}^n$ defined by

$$\mathrm{U}_n(\mathbb{C}) := \{X \in M_n(\mathbb{C}) : XX^* = I_n, \},$$

where X^* is the complex conjugate of X. Notice that $\mathrm{U}_1(\mathbb{C}) = S^1$. Indeed, unitary groups have a very rich geometric structure. This geometric structure might produce some product-free sets (See Figure 1.1). We can make these groups simpler to study by considering unitary matrices with the determinant 1, and denote this group by $\mathrm{SU}_n(\mathbb{C})$, which is called the special unitary group. Gowers [31] asked if $\mathrm{pf}(\mathrm{SU}_n) < c^n$ for some $c < 1$. The available methods only give polynomial bounds for these groups.

A special class of compact groups that will be studied in this thesis are **profinite groups**, which are defined as the *projective limit* of finite groups. Using their close connection to finite groups, we can establish exponential lower and upper bounds for the product-free measure. Indeed, profinite groups are topological groups that are compact and totally disconnected. These groups appear naturally once we want to study a sequence of finite groups that can be patched together. An example to keep in mind is the ring of p-adic integers that is defined by

$$\mathbb{Z}_p := \left\{(x_n) \in \prod(\mathbb{Z}/(p^n\mathbb{Z})) : x_{n+1} \equiv x_n \pmod{p^n}\right\}.$$

Analytically, this ring is a "completion" of the ring of integers with respect to prime ideal (p). So these several interpretations of profinite groups make their theory very rich. Roughly speaking, understanding properties of profinite groups often reduces to finite quotients. This idea will be essential when we will study their representations.

1.1.1. Statement of our theorems for product-free sets

Let us now turn to our contribution in this thesis. This is joint work with Keivan Mallahi-Karai.

For the finite Chevalley group defined over a finite field, say $\mathbf{G}(\mathbb{F}_q)$, Landazuri and Seitz [49], in their important paper, gave a complete list of minimal degrees of non-trivial representations of $\mathbf{G}(\mathbb{F}_q)$. However, it seems that the similar question has not been considered for $\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))$.

Remark. *It is possible to use the theory of simple Lie algebras over $\mathbb{C}$ to construct simple groups of matrices over any field. This was discovered by Claude Chevalley [15]. Very briefly, for a given simple Lie algebra, one can study its automorphisms. The Chevalley group is a subgroup of this automorphism group. The generators of the Chevalley group are constructed with the help of a basis of the Lie algebra called a Chevalley basis . However in this thesis we only consider the following cases of Chevalley groups: projective special linear groups $\mathrm{PSL}_n(\mathbb{F}_p)$, or projective special sympletic groups $\mathrm{PSp}_{2k}(\mathbb{F}_p)$, and their extensions to $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ and $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$. However, we believe that some of these results can be extended to Chevalley groups because of their connections to simple Lie algebras. To see more about the Chevalley groups we refer the reader to [11, 12, 13, 66].*

Let us first set some definitions. For a ring R, we define the special linear group, denoted by $\mathrm{SL}_k(R)$, by

$$\mathrm{SL}_k(R) := \{X \in M_k(R) : \det X = 1\}. \tag{1.1.14}$$

Now let J denote the $2k$ by $2k$ matrix defined by

$$J := \begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix}.$$

The symplectic group is defined as follows:

$$\mathrm{Sp}_{2k}(R) := \left\{A \in M_{2k}(R) : AJA^t = J\right\}. \tag{1.1.15}$$

In this thesis, we will study lower bounds for the minimal degree of the non-trivial representations of all the groups $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ and $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$ (which are the

same as the minimal degree of the non-trivial continuous representations of the profinite groups $\mathrm{SL}_k(\mathbb{Z}_p)$ and $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$). Let us extend Definition 1.1.6 to general groups (not necessarily finite groups).

Definition 1.1.8. *For a given group G the* minimal degree *of non-trivial representations is defined by*

$$m(G) := \min_{\rho \neq 1} d_\rho, \tag{1.1.16}$$

where the minimum is taken over all non-trivial representations of G, and d_ρ denotes the degree of the representation ρ. We will also denote

$$m_f(G) := \min_{\ker \rho = \{1\}} d_\rho,$$

where the minimum is taken over the set of all faithful *representations, where a faithful representation is an injective representation.*

Remark 1.1.2. *For compact groups, we impose the natural restriction that all representations are continuous.*

Remark 1.1.3. *In what follows p always denote an odd prime.*

Our first theorem gives a minimal degree of all non-trivial representations of some classical groups. This indeed extends and simplifies previous work of Landazuri and Seitz, where they consider the minimal degree of representations for Chevalley groups over a finite field.

Theorem 1.1.2. *In the table below, the third column gives a lower bound for the degree of any non-trivial representations of the group $\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))$ where $\mathbf{G}$ is one of the groups listed in the first column. In other words,*

$$m(\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))) \geq h(\mathbf{G}, p).$$

Similarly, the forth column gives a lower bound for the degree of any faithful representation of $\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))$. In other words:

$$m_f(\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))) \geq h_f(\mathbf{G}, p, n).$$

Then we have the following table

		minimal degree of non-trivial representations	*minimal degree of faithful representations*
$\mathbf{G}$	k	$\geq h(\mathbf{G}, p)$	$\geq h_f(\mathbf{G}, p, n)$
$\mathbf{SL}_2$	2	$\geq \frac{1}{2}(p-1)$	$\geq \frac{1}{2}\varphi(p^n)$
$\mathbf{SL}_k$	≥ 3	$\geq p^{k-1} - p^{k-2}$	$\geq (p^n - p^{n-1})p^{(k-2)n}$
$\mathbf{Sp}_{2k}$	≥ 2	$\geq \frac{1}{2}(p-1)p^{k-1}$	$\geq \frac{1}{2}(p^n - p^{n-1})p^{(k-1)n}$

Remark 1.1.4. *Bourgain and Gamburd [7], using a theorem of Clifford, found the following lower bound for* $m_f(\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))$*:*

$$m_f(\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))) \geq \frac{p^{n-2}(p^2-1)}{2}. \tag{1.1.17}$$

Even though our bound is slightly weaker than the one obtained in [7], it is asymptotically equivalent. Our method is also more elementary and can be applied to other classes of Chevalley groups. For instance for $\mathrm{SO}^+_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$*, the group of orthogonal matrices with the determinant* 1*, we can also show that*

$$m_f(\mathrm{SO}^+_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))) \geq \varphi(p^n)p^{(2k-4)n}.$$

As any finite dimensional representation of a profinite group factors through a finite quotient, we have:

Theorem 1.1.3. *Let* $\mathbf{G}$ *be one of the groups listed in the table above and* $\mathbf{G}(\mathbb{Z}_p)$ *denote the compact group of p-adic points of* $\mathbf{G}$*. Then the minimal degree of all non-trivial continuous representations of* $\mathbf{G}(\mathbb{Z}_p)$ *is bounded below by* $h(\mathbf{G}, p)$*. In other words*

$$m(\mathbf{G}(\mathbb{Z}_p)) \geq h(\mathbf{G}, p).$$

Moreover, we will consider Babai and Sós's question for the profinite groups $\mathrm{SL}_k(\mathbb{Z}_p)$ and $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$. In this context, using representation bounds, we can get an upper bound for the measure of the product-free sets in $\mathrm{SL}_k(\mathbb{Z}_p)$ and $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$. Using the spectral theory of compact operators we will prove an extension of Theorem 1.1.1 to compact groups.

Remark 1.1.5. *In this thesis, all topological groups considered will be Hausdorff and second countable. By a representation of these groups we mean a continuous complex representation.*

Theorem 1.1.4 (Mixing inequality)**.** *Let G be a compact topological group such that any non-trivial representation of G has dimension at least $m(G)$. Let $f_1, f_2 \in L^2(G)$ and suppose that at least one of f_1, f_2 belongs to $L^2_0(G)$, which is the space of functions with zero mean. Then*

$$\|f_1 * f_2\|_2 \leq \sqrt{\frac{1}{m(G)}}\|f_1\|_2\|f_2\|_2. \tag{1.1.18}$$

This theorem has an immediate corollary.

Corollary 1.1.6. *Let G be a compact topological group such that any non-trivial representation of G has dimension at least $m(G)$. Let $A, B \subseteq G$ be two measurable sets then*

$$\|1_A * 1_B - \mu(A)\mu(B)\|_2 \leq \sqrt{\frac{\mu(A)\mu(B)}{m(G)}} \tag{1.1.19}$$

For compact groups we can therefore deduce the following:

Theorem 1.1.5. *Suppose G is a compact topological group such that any non-trivial representation of G has dimension at least $m(G)$. If $A, B, C \subseteq G$ such that*

$$\mu(A)\mu(B)\mu(C) > \frac{1}{m(G)},$$

then the set $AB \cap C$ has a positive measure. Moreover, if

$$m(G)\mu(A)\mu(B)\mu(C) \geq \frac{1}{\eta^2},$$

then

$$\mu\{(x, y, z) \in A \times B \times C : xy = z\} \geq (1 - \eta)\mu(A)\mu(B)\mu(C). \tag{1.1.20}$$

By Theorem 1.1.3 and Theorem 1.1.5 we get the following result:

Corollary 1.1.7. *The product-free measure of the profinite groups $\mathbf{G}(\mathbb{Z}_p)$ for the groups $\mathbf{G}$, given in Theorem 1.1.2, is bounded from above by:*

$$\mathrm{pf}(\mathbf{G}(\mathbb{Z}_p)) \leq h(\mathbf{G}, p)^{-1/3}.$$

These upper bounds in particular imply that:

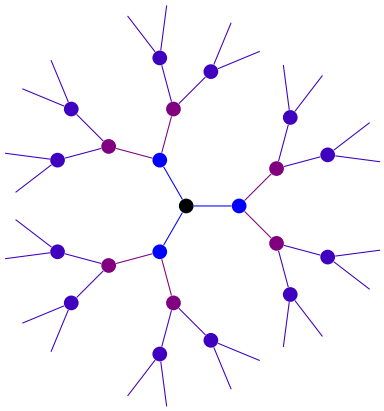
Corollary 1.1.8. *If A is a measurable subset of the groups $G = \mathbf{G}(\mathbb{Z}_p)$ with $\mu(A) > h(\mathbf{G}, p)^{-1/3}$, then $A^3 = G$.*

Proof: For every $g \in \mathbf{G}(\mathbb{Z}_p)$, set $B = A$ and $C = gA^{-1}$. Since

$$\mu(A)\mu(B)\mu(C) = \mu(A)^3 > h(\mathbf{G}, p),$$

then by Theorem 1.1.3 and Theorem 1.1.5, $AB \cap C \neq \emptyset$. If $x \in AB \cap C$ then $x = ga_3^{-1} = a_1a_2$ for $a_1, a_2, a_3 \in A$ which proves the claim. □

Let T_{k+1} be an *infinite regular tree* of degree $k+1$. The automorphism group $Aut(T_{k+1})$ of T_{k+1} is the group of isometries of the vertex set of T_{k+1} with respect to the discrete metric d, where $d(u, v)$ is the smallest number of edges on a path in T_{k+1} connecting u and v. In other words, by an automorphism of T_{k+1} we mean a permutation of the set of vertices of T_{k+1} that preserves adjacency.



Definition 1.1.9. *For a sequence $x_n \in Aut(T_{k+1})$, we define*

$$x_n \longrightarrow x,$$

if for any $v \in T_{k+1}$, there exits n_v so that for all $n \geq n_v$, we have $x_n(v) = x(v)$. With this topology, called pointwise convergence topology, one can show that $Aut(T_{k+1})$ is a locally compact topological group. We fix a vertex O of T_{k+1} to which we may occasionally refer as the root. Let A_{k+1} be the stabilizer of O in $Aut(T_{k+1})$. It can be shown that A_{k+1} is a compact group. In fact, every $x \in A_{k+1}$ fixes O and thereby permutes the set of all $(k+1)k^{j-1}$ vertices of distance j from O, for every $j \geq 1$. This induces a homomorphism

$$\sigma_j : A_{k+1} \longrightarrow \Sigma_{(k+1)k^{j-1}},$$

where Σ_m denotes the symmetric group on $\{1, 2, \ldots, m\}$. We can now define the following "congruence subgroups" and then provide a system of fundamental

open sets around the identity automorphism:

$$\mathcal{C}_j = \{x \in A_{k+1} : \sigma_j(x) = id\}.$$

Then

$$A_{k+1} = \varprojlim A_{k+1}/\mathcal{C}_j. \tag{1.1.21}$$

For more details we refer to Section 2.6 or Bass and Lubotzky's book [4]. We will obtain lower and upper bounds for the product-free measure for the group A_{k+1}^+ defined as

Definition 1.1.10. *An automorphism $x \in A_{k+1}$ is called positive if $\sigma_j(x)$ is an even permutation for all $j \geq 1$. The group of all positive automorphisms is denoted by A_{k+1}^+.*

We will prove:

Theorem 1.1.6. *For all $k \geq 6$ we have*

$$\frac{1}{k+1} \leq \mathrm{pf}(A_{k+1}^+) \leq \frac{1}{(k-1)^{1/3}}, \tag{1.1.22}$$

1.2. The density of monogenic number fields

In this section, which involves more algebraic number theory techniques, we study certain arithmetic properties of number fields.

By a number field, we mean a finite extension of the field of rational numbers. Historically, algebraic number theory is about arithmetic properties of integral polynomials. For instance, for a given integral irreducible polynomial $f(x)$, one might be interested to find the density of those primes p, so that $f(x) \pmod p$ is irreducible over $\mathbb{F}_p[x]$. Another example would be to compute the density of primes p so that $f(x) \pmod p$ splits over $\mathbb{F}_p[x]$. Let us, before going any further, set some notations.

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n, and assume that

$$\alpha_1, \alpha_2, \ldots, \alpha_n,$$

are roots of $f(x)$ in its splitting field denoted by E_f. The Galois group of $f(x)$ is often denoted by $\mathrm{Gal}_f := \mathrm{Gal}(E_f/\mathbb{Q})$. Notice that the Galois group of $f(x)$

permutes the roots of the polynomial. The discriminant is defined as follows:

$$\mathrm{Disc}_f = \Delta^2 = \left(\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) \right)^2, \tag{1.2.1}$$

where

$$\Delta = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j).$$

Since $f(x)$ is a monic integral polynomial, Δ is an algebraic integer that is a root of a monic integral polynomial. For $\sigma \in \mathrm{Gal}_f$ we have

$$\sigma(\Delta) = \mathrm{sgn}(\sigma)\Delta.$$

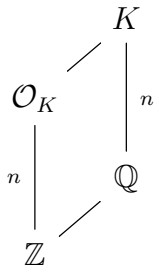
Hence for all $\sigma \in \mathrm{Gal}_f$ we get

$$\sigma(\mathrm{Disc}_f) = \mathrm{Disc}_f.$$

This implies that $\mathrm{Disc}_f \in \mathbb{Z}$, since it is a rational integer. Clearly $\mathrm{Disc}_f = 0$ means that $f(x)$ is not separable, i.e., $\alpha_i = \alpha_j$, for some $i \neq j$. Therefore we just consider separable polynomials.

Similarly we can define the discriminant for number fields. Let $K/\mathbb{Q}$ be a number field of degree n. The ring of integers of K is defined by

$$\mathcal{O}_K := \{x \in K : x \text{ is an algebraic integer over } K\}.$$



One can show that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. Then linear algebra can be invoked to define some concepts. Let A be a ring, E a free A-module of finite rank and let u be an endomorphism of E. If a base $\{e_i\}$ of E has been chosen and if (a_{ij}) is the matrix for u with respect to this base, then the trace of u is defined by

$$Tr(u) = \sum_i a_{ii}.$$

Notice that this quantity is independent of the choice of base.

Definition 1.2.1. *For an algebraic integer $\beta \in \mathcal{O}_K$, the trace of β, denoted by $\mathrm{Tr}_{K/\mathbb{Q}}(\beta)$, is defined by the trace of the linear transformation*

$$\begin{aligned} \mathcal{O}_K &\longrightarrow \mathcal{O}_K \\ x &\longmapsto \beta x. \end{aligned} \tag{1.2.2}$$

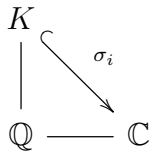
Notice that $\mathrm{Tr}_{K/\mathbb{Q}}(\beta)$ is a rational integer, since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module. We define the discriminant of K by

Definition 1.2.2. *Let $\beta_1, \ldots, \beta_n$ be an integral basis for $\mathcal{O}_K$. We define*

$$\mathrm{Disc}(K) := \det(\mathrm{Tr}_{K/\mathbb{Q}}(\beta_i\beta_j)). \tag{1.2.3}$$

Remark 1.2.1. *More generally, let $\mathcal{O}$ be a free $\mathbb{Z}$-module, then the discriminant of $\mathcal{O}$ can be defined similarly to Definition 1.2.2.*

There is another way to define the discriminant. Since the degree of K over $\mathbb{Q}$ is n, then there are exactly n embeddings of K into $\mathbb{C}$.



Let us denote them by $\sigma_1, \ldots, \sigma_n$. It is a standard fact in algebraic number theory that for $x \in K$,

$$\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_l \sigma_l(x).$$

Therefore,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\beta_i\beta_j) = \sum_l \sigma_l(\beta_i\beta_j) = \sum_l \sigma_l(\beta_i)\sigma_l(\beta_j).$$

Put

$$A := \begin{pmatrix} \sigma_1(\beta_1) & \ldots & \sigma_1(\beta_n) \\ \vdots & & \vdots \\ \sigma_n(\beta_1) & \ldots & \sigma_n(\beta_n) \end{pmatrix},$$

then we have the following matrix equality

$$(\mathrm{Tr}_{K/\mathbb{Q}}(\beta_i\beta_j)) = AA^T.$$

Hence we showed

Lemma 1.2.1.

$$\mathrm{Disc}(K) = \det \begin{pmatrix} \sigma_1(\beta_1) & \dots & \sigma_1(\beta_n) \\ \vdots & & \vdots \\ \sigma_n(\beta_1) & \dots & \sigma_n(\beta_n) \end{pmatrix}^2 . \tag{1.2.4}$$

For a given monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ we can associate a number field. Let α be a root of $f(x)$, we can consider $K := \mathbb{Q}(\alpha)$. So one might ask about the discriminant of $K = \mathbb{Q}(\alpha)$ and its relation to the discriminant of $f(x)$. Since $f(x)$ is a monic integral polynomial then α is an algebraic integer. So

$$\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K.$$

Lemma 1.2.2. *For an irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$, with an algebraic integer root α, we have*

$$\mathrm{Disc}(\mathbb{Z}[\alpha]) = \mathrm{Disc}_f.$$

Proof: Since $\beta_1 = 1, \beta_2 = \alpha, \beta_3 = \alpha^2, \dots, \beta_n = \alpha^{n-1}$ is an integral basis for $\mathbb{Z}[\alpha]$, then

$$\begin{pmatrix} \sigma_1(\beta_1) & \dots & \sigma_1(\beta_n) \\ \vdots & & \vdots \\ \sigma_n(\beta_1) & \dots & \sigma_n(\beta_n) \end{pmatrix},$$

is a Vandermonde matrix, hence

$$\mathrm{Disc}(\mathbb{Z}[\alpha]) = \left(\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) \right)^2 = \mathrm{Disc}_f,$$

where

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n).$$

□

We recall the elementary divisor theorem. For proof see [60] Theorem 1, section 1.5.

Theorem 1.2.1. *Let $\mathcal{O}$ be a free $\mathbb{Z}$-module of rank n. And let $\mathcal{M}$ be a free $\mathbb{Z}$-submodule of $\mathcal{O}$ with rank n. Then there exists a basis $\{\beta_1, \dots, \beta_n\}$ for $\mathcal{O}$, and non-zero integers $a_1, \dots, a_n$, so that*

- $a_i \mid a_{i+1}$.
- $\{a_1\beta_1, \ldots, a_n\beta_n\}$ *is a basis for* $\mathcal{M}$.

From this important theorem we can deduce

Theorem 1.2.2. *Let* α *be a root of a monic, irreducible integral polynomial* $f(x)$*, and suppose* $K := \mathbb{Q}(\alpha)$*, then*

$$\mathrm{Disc}_f = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \mathrm{Disc}(K),$$

Proof: Let $\{\beta_1, \ldots, \beta_n\}$ be a basis for $\mathcal{O}_K$ so that $\{a_1\beta_1, \ldots, a_n\beta_n\}$ is a basis for $\mathbb{Z}[\alpha]$. From Theorem 1.2.1 such a basis exists. By Lemma 1.2.2 we know $\mathrm{Disc}_f = \mathrm{Disc}([\mathbb{Z}[\alpha]])$. Notice that

$$\begin{aligned}
\mathrm{Disc}(\mathbb{Z}[\alpha]) &= \det(\mathrm{Tr}_{K/\mathbb{Q}}(a_i a_j \beta_i \beta_j)) \\
&= (a_1 \ldots a_n)^2 \det(\mathrm{Tr}_{K/\mathbb{Q}}(\beta_i \beta_j)) \\
&= (a_1 \ldots a_n)^2 \mathrm{Disc}(K).
\end{aligned}$$

Remark that

$$\left(\prod_i a_i\right)^2 = [\mathcal{O}_K : \mathbb{Z}[\alpha]].$$

□

The discriminant is one of the main tools in algebraic number theory. It reveals many arithmetic properties of $f(x)$. For instance one can show that when the discriminant of a given polynomial of degree n is square-free then its Galois group is isomorphic to S_n, the symmetric group of n elements. This would convince us to ask how it is possible that a random integral polynomial has a square-free discriminant. Recall that the **height** of an integral polynomial $f(x)$ is the maximum of the absolute value of all its coefficients.

Definition 1.2.3. *Call an irreducible monic integral polynomial* $f(x) \in \mathbb{Z}[x]$ **essential** *if*

$$\mathrm{Disc}_f = \mathrm{Disc}(K),$$

where $K = \mathbb{Q}(\alpha)$*, and* α *is a root of* $f(x)$*.*

The following conjecture is due to Hendrik Lenstra [2].

Conjecture 1 (Lenstra)**.** *Let $n \geq 2$. The probability that a random irreducible monic integral polynomial of degree n and height $\leq X$ is essential should tend to $6/\pi^2$ as $X \to \infty$.*

Notice that from Theorem 1.2.2 we have

$$\mathrm{Disc}_f = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \mathrm{Disc}(K).$$

So if Disc_f is square-free then $\mathrm{Disc}_f = \mathrm{Disc}(K)$, which means that f is essential. Moreover, from this, we deduce that

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1,$$

hence

$$\mathbb{Z}[\alpha] = \mathcal{O}_K.$$

This motivates the following definition.

Definition 1.2.4. *Let K be an algebraic number field of degree n and $\mathcal{O}_K$ its ring of integers. K is called* **monogenic** *if there exists an element $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

Notice that when $f(x)$ is essential then, by the definition, $\mathrm{Disc}_f = \mathrm{Disc}(K)$ therefore by Theorem 1.2.2 we have $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$ which implies that

$$\mathcal{O}_K = \mathbb{Z}[\alpha],$$

therefore K is monogenic.

It is a classical problem in algebraic number theory to identify if a number field K is monogenic or not. In the 1960s, Hasse [40] asked if one could give an arithmetic characterization of monogenic number fields. The quadratic and cyclotomic number fields are monogenic, but this is not the case in general. Dedekind [18] was the first who noticed this by giving an example of a cubic field generated by a root of $t^3 - t^2 - 2t - 8$.

Definition 1.2.5. *Let $f(t) \in \mathbb{Z}[t]$ be a monic irreducible polynomial. $f(t)$ is called monogenic if $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $K = \mathbb{Q}(\alpha)$ and α is a root of $f(t)$.*

Let us mention some remarks. The discriminant of a polynomial is itself a polynomial in several variables. For instance the discriminant of cubic polynomial

$ax^3 + bx^2 + cx + d$ is

$$F(a, b, c, d) := 18abcd + b^2c^2 - 4b^3d - 4ac^3 - 27a^2d^2.$$

Then it is interesting to count the number of $|a|, |b|, |c|, |d| \leq T$, so that $F(a, b, c, d)$ is square-free. This question seems very hard for general degrees. For small degrees however, this has been done by several mathematicians [44, 37]. For a given polynomial $f(x, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, assuming *abc*-conjecture, Poonen [56] in his striking paper, by generalizing a fundamental work of Granville [33], computed the density of $\mathbf{x} \in \mathbb{Z}^n$ such that $f(\mathbf{x})$ is square-free (See [56] (Theorem 3.2)). Let us recall the *abc*-conjecture.

Conjecture 2 (Oesterlé and Masser)**.** *For any given $\epsilon > 0$ there exists a constant k_ϵ such that if a, b and c, are coprime positive integers for which*

$$a + b = c,$$

then

$$c \leq k_\epsilon \left(\prod_{\substack{p \text{ prime} \\ p|abc}} p \right)^{1+\epsilon}.$$

To see more about this interesting conjecture see Granville and Tucker's paper [35]. As far as I know, there are not many results regarding the probability of a randomly chosen polynomial of degree n having square-free discriminant. One might also ask about the density of monogenic number fields when they are sorted by their discriminants. More formally

$$\lim_{X \to \infty} \frac{\#\{K : K \text{ monogenic} : |\mathrm{Disc}(K)| \leq X\}}{\#\{K : |\mathrm{Disc}(K)| \leq X\}}?$$

For cubic and quartic fields, this question has been studied by Bhargava and Shankar [6], Theorem 4.1, where we refer the reader to their paper since it requires some background to state their results precisely.

In Chapter 5 we have used the Chebotarev density theorem to study the distribution of a family of monogenic polynomials. In order to fix notations, let us review some concepts and definitions. Let $K/\mathbb{Q}$ be a finite Galois extension of

degree l with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ and discriminant D. For a prime p, and a prime $\mathfrak{p}$ above p, we can speak about the decomposition group, i.e.,

$$D_{\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Denote $\kappa(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$, then we have a well defined surjective homomorphism

$$\begin{aligned} D_{\mathfrak{p}} &\longrightarrow \mathrm{Gal}(\kappa(\mathfrak{p})/\mathbb{F}_p) \\ \sigma &\longrightarrow \bar{\sigma}, \end{aligned} \tag{1.2.5}$$

where

$$\bar{\sigma}(x + \mathfrak{p}) = \sigma(x) + \mathfrak{p}.$$

The kernel of this homomorphism is called the inertia subgroup, denoted by $I_{\mathfrak{p}}$, which measures the ramification degree. Indeed for a prime p coprime to D, from a well-known fact in the realm of algebraic number theory, we have that p is unramified in K, and the map defined by (1.2.5) is an isomorphism. Since $\mathrm{Gal}(\kappa(\mathfrak{p})/\mathbb{F}_p)$ is a cyclic group generated by the Frobenius element, denoted by Frob_p, i.e., $\mathrm{Frob}_p(\lambda) = \lambda^p$, then there is a unique element in the Galois group, denoted by $\sigma_{\mathfrak{p}}$ such that $\overline{\sigma_{\mathfrak{p}}} = \mathrm{Frob}_p$.

$\sigma_{\mathfrak{p}}$ is also called the Frobenius element, and one can show that this element is unique up to conjugation. Indeed, for a different prime $\mathfrak{p}'$ above p, we observe that $\sigma_{\mathfrak{p}}$ and $\sigma_{\mathfrak{p}'}$ are conjugate, and therefore when we study our objects, considering them in a conjugacy class, it is more convenient to write σ_p instead of $\sigma_{\mathfrak{p}}$. It is very important to notice that a prime p splits completely if and only if $\sigma_p = id$.

For an integer n, let a be coprime to n. By Dirichlet's theorem in primes for arithmetic progressions, we have

$$\pi(x, n, a) := \#\{p \leq x : p \equiv a \pmod{n}\} \sim \frac{\pi(x)}{\varphi(n)}. \tag{1.2.6}$$

The Chebotarev density theorem is a generalization of the Dirichlet's theorem. Let $\mathcal{C} \subseteq \mathrm{Gal}(K/\mathbb{Q})$ be a subset stable under conjugation, i.e., $\tau\mathcal{C}\tau^{-1} \subseteq \mathcal{C}$. The Chebotarev density theorem says that

$$\pi_{\mathcal{C}}(x) := \#\{p \leq x : \sigma_p \in \mathcal{C}\} \sim \frac{|\mathcal{C}|}{[K : \mathbb{Q}]}\pi(x). \tag{1.2.7}$$

Let us pick an example to show that how Dirichlet's theorem can be recovered by the Chebotarev density theorem. Taken $K = \mathbb{Q}(\zeta_n)$, one can see that p splits completely in K if and only if $p \equiv 1 \pmod{n}$, hence for $\mathcal{C} = id$, the set of primes that split completely is the same as the set of primes p for which $p \equiv 1 \pmod{n}$. Notice that $[K : \mathbb{Q}] = \varphi(n)$. Therefore

$$\#\{p \leq x : p \equiv 1 \pmod{n}\} = \#\{p \leq x : \sigma_p = id\} \sim \frac{\pi(x)}{\varphi(n)}, \tag{1.2.8}$$

thus recovering Dirichlet's theorem. Let us mention an application of the Chebotarev density theorem whose proof will be presented in Chapter 4. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n with discriminant $D \neq 0$. For a prime number p, coprime to D, we define

Definition 1.2.6. *$X_p(f)$:= the degree of the splitting field of $f(x) \pmod{p}$.*

We consider the average of this random variable.

$$\mu_n(f) := \lim_{t\to\infty} \left(\frac{1}{\pi(t)} \sum_{\substack{p\leq t \\ \gcd(p,D)=1}} X_p(f) \right), \tag{1.2.9}$$

if it exists. We will use the Chebotarev density theorem to prove

Theorem 1.2.3. *Assume that Galois group of $f(x)$ is the symmetric group S_n, where n is the degree of $f(x)$. Then*

$$\mu_n(f) = C\sqrt{\frac{n}{\log n}} + O\left(\frac{\sqrt{n}\log\log n}{\log n}\right), \tag{1.2.10}$$

where

$$C = 2\sqrt{\left(2\int_0^\infty \log\log\left(\frac{e}{1-e^t}\right) dt\right)}. \tag{1.2.11}$$

1.2.1. Statement of our theorems for monogenic fields

In this section we present our theorems on monogenic number fields. Our first theorem is the following.

Theorem 1.2.4. *Let p and q be prime numbers, where $q \geq 3$. Consider the polynomial*

$$f_p(t) := t^q - p.$$

Then, we have

$$\liminf_{x\to\infty}\frac{1}{\pi(x)}\#\{p\le x : f_p(t) \ \textit{is monogenic}\ \}\ge\frac{q-1}{q},$$

where $\pi(x)$ denotes the number of primes less than x.

The idea is to find a congruence condition on p such that $f_p(t)=t^q-p$ is monogenic. This condition on p reads as $p^{q-1}\not\equiv 1 \pmod{q^2}$. Then we use the Chebotarev density theorem to count these primes. We will also present an elementary method to count these primes by using Dirichlet's theorem on primes in arithmetic progressions.

When $q=3$, using a description of an integral basis for a pure cubic field (Theorem 5.1.1), and an explicit computation, we notice that the index form (see Lemma 5.1.1) of $\mathbb{Q}(\sqrt[3]{hk^2})$ is represented by hx^3-ky^3 when $h^2\not\equiv k^2 \pmod 9$ and $(hx^3-ky^3)/9$ for $h^2\equiv k^2 \pmod 9$. Thus $\mathbb{Q}(\sqrt[3]{hk^2})$ being monogenic is equivalent to integral solubility of

$$\begin{cases} hx^3+ky^3=1 & \text{if } h^2\not\equiv k^2 \pmod 9;\\ hx^3+ky^3=9 & \text{if } h^2\equiv k^2 \pmod 9. \end{cases} \tag{1.2.12}$$

In particular when p is a prime, $\mathbb{Q}(\sqrt[3]{p})$ is monogenic for $p\equiv\pm2,\pm5 \pmod 9$. For $p\equiv\pm1 \pmod 9$ we obtain the following equation

$$px^3+y^3=9. \tag{1.2.13}$$

By counting those primes $p\equiv\pm1 \pmod 9$ where 9 is not a cube in $\mathbb{F}_p$, we will find a lower bound for the density of non-monogenic cubic fields $\mathbb{Q}(\sqrt[3]{p})$. Notice that when $p\equiv-1 \pmod 9$, then 9 is a cube in $\mathbb{F}_p$. Therefore we restrict ourself by considering primes of the form $p\equiv1 \pmod 9$, and computing the density of these primes where 9 is not a cube modulo them. Let $K=\mathbb{Q}(\zeta_9,\sqrt[3]{9})$, where ζ_9 is a primitive 9'th root of unity. Since a prime p splits completely in K if and only if $p\equiv1 \pmod 9$ and $9^{\frac{p-1}{3}}\equiv1 \pmod p$. Then by applying the Chebotarev density theorem, we get

Theorem 1.2.5. *The density of primes $p\equiv1 \pmod 9$ such that the following Thue's equation*

$$px^3+y^3=9,$$

does not have any solution in integers x, y*, is at least* $1/9$*. This set of primes produces non-monogenic cubic fields* $\mathbb{Q}(\sqrt[3]{p})$*.*

We can also describe these primes by the following

Theorem 1.2.6. $\mathbb{Q}(\sqrt[3]{p})$ *is non-monogenic for those primes* $p \equiv 1 \pmod 9$ *which can be represented by* $7x^2 + 3xy + 9y^2$*.*

We will also remark some other connections to a phenomenon called *Euler-Kronecker constant.*

Part I: Additive combinatorics and product-free sets

Chapter 2

PRELIMINARIES FOR CHAPTER 3

In this chapter, we will cover some background for Chapter 3.

2.1. Bipartite graphs and Gowers' trick

In this section we will sketch Gowers' idea for counting the number of solutions to the equation $xy = z$. This method will then be developed further in Chapter 3.

We denote the vector space of all functions from G to $\mathbb{C}$ by $\mathbb{C}^G$. Let us recall that $\mathbb{C}^G$ is an inner-product space. Indeed, for $f_1, f_2 \in \mathbb{C}^G$ we define

$$\langle f_1, f_2 \rangle := \sum_{x \in G} f_1(x)\overline{f_2}(x), \tag{2.1.1}$$

and the L_2-norm on $\mathbb{C}^G = L^2(G)$ is defined by

$$\|f\|_2^2 := \langle f, f \rangle = \sum_{x \in G} |f(x)|^2.$$

Remark 2.1.1. *We will use the notation $\mathbb{C}^G$ when we wish to see it as a vector space. However, sometimes $\mathbb{C}^G$ is denoted by $L^2(G)$ when we want to emphasize its functional analytic properties.*

Our aim in this section is to prove the following theorem in detail, which is indeed a special case of Theorem 1.1.1. We will then mention how this can be modified to compact groups.

Theorem 2.1.1 (Gowers [31])**.** *Let G be a finite group of order n, all of whose non-trivial representations have dimension greater than or equal to $m(G)$. Let A*

be a subset of G and let $f \in L^2(G)$ be a function so that $\sum_{x\in G} f(x) = 0$, then

$$\|1_A * f\|_2 \leq \left(\frac{n|A|}{m(G)}\right)^{1/2} \|f\|_2 = \left(\frac{|G|}{m(G)}\right)^{1/2} \|1_A\|_2 \|f\|_2.$$

The convolution operator over a finite dimensional vector space can be understood by the language of graph theory and of course by functional analysis. Gowers' approach was to consider the graph theoretical interpretation, by relating the trace of biadjacency matrix of a bipartite graph to the number of edges.

Definition 2.1.1. *For a finite group G of order n, consider subset A of G. We define the following bipartite graph,* **denoted by** *$\mathcal{G}$. The vertex set of $\mathcal{G}$ consists of two copies of G, and $\{x, y\} \in E(\mathcal{G})$, if and only if for some $a \in A$, $y = ax$.*

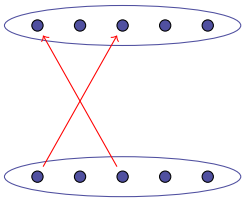


FIGURE 2.1. Bipartite Graph

Then each vertex of $\mathcal{G}$ is of degree $|A|$, and the number of edges in $\mathcal{G}$ is $n|A|$. Let us recall the definition of the **biadjacency matrix** of a bipartite graph. Let $G = \{x_1, x_2, \ldots, x_n\}$, then by our definition $\{x_i, x_j\} \in E(\mathcal{G})$ if and only if $x_j = ax_i$ for some $a \in A$. In other words $\{x_i, x_j\} \in E(\mathcal{G})$ if and only if $1_A(x_j x_i^{-1}) = 1$. Then the biadjacency matrix of the graph $\mathcal{G}$, denoted again by $\mathcal{G}$, simply is

$$\mathcal{G} := \begin{pmatrix} 1_A(x_1x_1^{-1}) & 1_A(x_2x_2^{-1}) & \ldots & 1_A(x_1x_n^{-1}) \\ 1_A(x_2x_1^{-1}) & 1_A(x_2x_2^{-1}) & \ldots & 1_A(x_2x_n^{-1}) \\ 1_A(x_3x_1^{-1}) & 1_A(x_3x_2^{-1}) & \ldots & 1_A(x_3x_n^{-1}) \\ \vdots & \vdots & \ldots & \vdots \\ 1_A(x_nx_1^{-1}) & 1_A(x_nx_2^{-1}) & \ldots & 1_A(x_nx_n^{-1}) \end{pmatrix}.$$

We define the *convolution operator*.

Definition 2.1.2. *Consider the following operator*

$$\begin{aligned} \alpha : \mathbb{C}^G &\longrightarrow \mathbb{C}^G \\ f &\longmapsto \alpha(f), \end{aligned} \tag{2.1.2}$$

where

$$(\alpha f)(y) := \sum_{\substack{x\in G\\ \{x,y\}\in E(\mathcal{G})}} f(x) = \sum_{x\in G} 1_A(yx^{-1})f(x) = (1_A * f)(y).$$

We also recall the definition of the norm of an operator.

Definition 2.1.3. *For the operator α, the norm of α is defined by*

$$\|\alpha\|_{op} := \sup_{0\neq f\in L^2(G)} \frac{\|\alpha f\|_2}{||f||_2}.$$

Since in Theorem 2.1.1, $\sum_{x\in G} f(x) = 0$, we restrict ourself to this subspace.

Definition 2.1.4.

$$L_0^2(G) := \left\{ f \in L^2(G) : \sum_{x\in G} f(x) = 0 \right\} = \left\{ f \in L^2(G) : \langle f, 1_G\rangle = 0 \right\}.$$

Indeed we have

Lemma 2.1.1. *Let $f \in L_0^2(G)$, then $\alpha f \in L_0^2(G)$. Hence the following map is well defined.*

$$\alpha|_{L_0^2(G)} : L_0^2(G) \longrightarrow L_0^2(G).$$

Proof: For $f \in L_0^2(G)$ we get

$$\begin{aligned}\sum_{y\in G}(\alpha f)(y) &= \sum_{y\in G}\sum_{x\in G} 1_A(yx^{-1})f(x)\\ &= \sum_{x\in G}\sum_{y\in G} 1_A(yx^{-1})f(x)\\ &= |A|\sum_{x\in G} f(x) = 0.\end{aligned} \tag{2.1.3}$$

□

Therefore, to prove Theorem 2.1.1 we need to prove the following inequality

$$\|\alpha|_{L_0^2(G)}\|_{op} := \sup_{0\neq f\in L_0^2(G)} \frac{\|\alpha f\|_2}{\|f\|_2} = \sup_{0\neq f\in L_0^2(G)} \frac{\|1_A * f\|_2}{\|f\|_2} \leq \left(\frac{|G|}{m(G)}\right)^{1/2} \|1_A\|_2. \tag{2.1.4}$$

Let δ_x be the characteristic function of the set $\{x\}$, then $\{\delta_x\}_{x\in G}$ is an orthonormal basis of $\mathbb{C}^G$. The following lemma is easy to prove.

Lemma 2.1.2. *The matrix of α with respect to this basis is the biadjacency matrix of the bipartite graph $\mathcal{G}$.*

Proof: Let $G = \{x_1, \ldots, x_n\}$, then to find for instance the first column of the matrix associated to the operator α we need to write $\alpha\delta_{x_1}$ with respect to the basis $\{\delta_{x_j}\}$. We have

$$\begin{aligned} \alpha\delta_{x_1} &= \sum_{j=1}^{n} (\alpha\delta_{x_1})(x_j)\delta_{x_j} \\ &= \sum_{j=1}^{n} (1_A * \delta_{x_1})(x_j)\delta_{x_j} \\ &= \sum_{j=1}^{n} 1_A(x_j x_1^{-1})\delta_{x_j}. \end{aligned} \tag{2.1.5}$$

Hence the first column of α with respect to this basis is the column vector

$$\begin{pmatrix} 1_A(x_1x_1^{-1}) \\ 1_A(x_2x_1^{-1}) \\ \vdots \\ 1_A(x_jx_1^{-1}) \\ \vdots \\ 1_A(x_nx_1^{-1}) \end{pmatrix},$$

which is exactly the first column of the biadjacency matrix of $\mathcal{G}$. □

Since $A \subseteq G$ is not necessarily a symmetric set, i.e., $A \neq A^{-1}$, the matrix representation of the operator α is not necessarily a symmetric matrix. In other words, the biadjacency matrix of the bipartite graph $\mathcal{G}$ can be a non-symmetric matrix.

Now let us recall an important theorem in linear algebra: let T be a symmetric operator on an inner product space V. Then by the *spectral theorem* one can find an orthonormal basis for V, say $\{v_1, v_2, \ldots, v_n\}$, so that the matrix of T with respect to this basis is a diagonal matrix. Perhaps it is appropriate to mention that this is equivalent to saying that any quadratic form can be diagonalized orthogonally. When T is not symmetric however, we have the following theorem.

Theorem 2.1.2 (Singular value decomposition)**.** *Let V be an inner product space with norm denoted by $|.|$, and let T be* **any linear map** *on V. Then there exist two orthonormal bases $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ such that the matrix of T*

with respect to these bases is

$$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}, \tag{2.1.6}$$

where $\lambda_1 \geq \cdots \geq \lambda_n \geq 0$. *Moreover*

$$\|T\|_{op} := \sup_{v \neq 0} \frac{|T(v)|}{|v|} = \lambda_1.$$

Proof: Let v be a non-zero vector such that $|T(v)|/|v|$ is maximized. Now suppose that w is any vector orthogonal to v. We claim that $T(w)$ is also orthogonal to $T(v)$. To prove this claim let ε be a small real number. Then

$$\begin{aligned} |T(v+\varepsilon w)|^2 &= \langle T(v)+\varepsilon T(w), T(v)+\varepsilon T(w)\rangle \\ &= |T(v)|^2 + 2\varepsilon \Re(\langle T(v), T(w)\rangle) + \varepsilon^2 |T(w)|^2. \end{aligned} \tag{2.1.7}$$

Moreover since v is orthogonal to w,

$$|v+\varepsilon w|^2 = |v|^2 + \varepsilon^2 |w|^2,$$

as $\langle v, w\rangle = 0$. Since v was chosen so that $|T(v)|/|v|$ to be maximized then we have

$$\frac{|T(v+\varepsilon w)|^2}{|v+\varepsilon w|^2} \leq \frac{|T(v)|^2}{|v|^2}, \tag{2.1.8}$$

therefore

$$\frac{|T(v+\varepsilon w)|^2}{|T(v)|^2} \leq \frac{|v+\varepsilon w|^2}{|v|^2}.$$

From this inequality and (2.1.7) we have

$$\frac{2\varepsilon \Re(\langle T(v), T(w)\rangle)}{|T(v)|^2} + \frac{\varepsilon^2 |T(w)|^2}{|T(v)|^2} \leq \frac{\varepsilon^2 |w|^2}{|v|^2}. \tag{2.1.9}$$

But this implies that $\Re(\langle T(v), T(w)\rangle) = 0$, since otherwise ε can be chosen so small with the same sign as $\Re(\langle T(v), T(w)\rangle)$, such that (2.1.9) is not fulfilled. We also have $\Im(\langle T(v), T(w)\rangle) = 0$, by choosing iw and repeating the above argument.

Therefore we will get a linear transformation from the orthogonal complement of $\langle v\rangle$ to the orthogonal complement of $\langle T(v)\rangle$.

$$T' : \langle v\rangle^{\perp} \longrightarrow \langle T(v)\rangle^{\perp}.$$

By induction, T' has a matrix of the required form. Now set

$$\begin{aligned} v_1 &:= v/|v|, \\ w_1 &:= T(v)/|T(v)| = T(v_1)/|T(v_1)|, \\ \lambda_1 &:= |T(v_1)|, \end{aligned} \tag{2.1.10}$$

then $T(v_1) = \lambda_1 w_1$, which proves the theorem. □

Remark 2.1.2. *As shown in the proof, we have*

$$\lambda_2 = \max_{0 \neq w \in \langle v_1 \rangle^\perp} \frac{|T(w)|}{|w|} = \|T|_{\langle v_1 \rangle^\perp}\|_{op}.$$

This remark will be invoked afterward.

For the vector space $\mathbb{C}^G$ with norm $\|\cdot\|_2$ and operator α, defined in (2.1.2), we will apply Theorem 2.1.2 to get two orthonormal bases for $\mathbb{C}^G$ so that, with respect to these bases, α is a diagonal matrix with the diagonal elements

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0,$$

so that

$$\|\alpha\|_{op} = \lambda_1.$$

Remark 2.1.3. *With the same notation as Theorem 2.1.2, λ_i^2's are the eigenvalues of $\alpha\alpha^*$. We will, by abuse of notation, call λ_i the "***eigenvalues***" of α.*

The eigenvalues of α will give some information about the number of edges of the bipartite graph $\mathcal{G}$. More precisely, we have

Lemma 2.1.3. *For the bipartite graph $\mathcal{G}$, with biadjacency matrix also denoted by $\mathcal{G}$, we have*

$$n|A| = |E(\mathcal{G})| = Tr(\mathcal{G}\mathcal{G}^T) = \sum_{i=1}^{n} \lambda_i^2,$$

where n is the order of G.

Proof: We have

$$Tr(\mathcal{G}\mathcal{G}^T) = \sum_{y \in G} \sum_{x \in G} 1_A(yx^{-1}) = n|A| = |E(\mathcal{G})|.$$

To show that $Tr(\mathcal{G}\mathcal{G}^T) = \sum_{i=1}^{n} \lambda_i^2$, by Theorem 2.1.2 we can find two orthogonal matrices, say Σ_1 and Σ_2, such that

$$\Sigma_1 \mathcal{G} \Sigma_2 = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}.$$

Therefore

$$Tr\left(\mathcal{G}\mathcal{G}^T\right) = Tr\left(\left(\Sigma_1 \mathcal{G} \Sigma_2\right)\left(\Sigma_1 \mathcal{G} \Sigma_2\right)^T\right) = \sum_i \lambda_i^2.$$

□

From Theorem 2.1.2 we see that $\|\alpha\|_{op} = \lambda_1$. In the following lemma we will find a graph interpretation of the norm of α.

Lemma 2.1.4. *We have*

$$\|\alpha\|_{op} = \lambda_1 = |A|,$$

moreover the multiplicity of the eigenvalue λ_1 is one, i.e.,

$$\lambda_1 > \lambda_2 \geq \lambda_3 \cdots \geq \lambda_n \geq 0.$$

Remark 2.1.4. *It is worth mentioning that for a k-regular graph X one can show that*

- $\lambda_1 = k$.
- λ_1 *has multiplicity* 1, *if and only if X is connected.*

Proof of Lemma 2.1.4: For two complex numbers a, b notice that

$$0 \leq |a - b|^2 = |a|^2 + |b|^2 - a\bar{b} - \bar{a}b,$$

then

$$(a\bar{b} + \bar{a}b) \leq |a|^2 + |b|^2. \tag{2.1.11}$$

For any $f \in \mathbb{C}^G$, from the above inequality we have

$$\begin{aligned}
\|\alpha f\|_2^2 &= \sum_{y\in G} |(\alpha f)(y)|^2 = \sum_{y\in G} |(1_A * f)(y)|^2 = \sum_{y\in G} \left|\sum_{x\in G} 1_A(yx^{-1})f(x)\right|^2 \\
&= \sum_{y\in G} \left(\sum_{x\in G} 1_A(yx^{-1})f(x)\right)\left(\sum_{z\in G} 1_A(yz^{-1})\overline{f(z)}\right) \\
&= \sum_{x,z\in G} f(x)\overline{f(z)} \sum_{y\in G} 1_A(yx^{-1})1_A(yz^{-1}) \qquad (2.1.12)\\
&\leq \frac{1}{2}\sum_{x,z\in G} \left(|f(x)|^2 + |f(z)|^2\right) \sum_{y\in G} 1_A(yx^{-1})1_A(yz^{-1}) \\
&= \sum_{x\in G} |f(x)|^2 \sum_{z\in G}\sum_{y\in G} 1_A(yx^{-1})1_A(yz^{-1}).
\end{aligned}$$

But

$$\sum_{z\in G}\sum_{y\in G} 1_A(yx^{-1})1_A(yz^{-1}) = |A|^2,$$

therefore for any $0 \neq f \in \mathbb{C}^G$ we have

$$\frac{\|\alpha f\|_2}{\|f\|_2} \leq |A|.$$

This implies that

$$\|\alpha\|_{op} \leq |A|.$$

Now, for the constant function $1_G(g) \equiv 1$, we have

$$\begin{aligned}
\|\alpha 1_G\|_2 &= \sqrt{|G|}|A|, \\
\|1_G\|_2 &= \sqrt{|G|},
\end{aligned} \qquad (2.1.13)$$

hence

$$\frac{\|\alpha 1_G\|_2}{\|1_G\|_2} = |A|.$$

From this we deduce that $\|\alpha\|_{op} = |A|$. To show that the multiplicity of λ_1 is 1, notice that when $a \neq b$ we have

$$(a\bar{b} + \bar{a}b) < |a|^2 + |b|^2.$$

which gives a strict inequality in (2.1.12). □

We use this lemma along with Theorem 2.1.2 to prove the following important corollary which will play an essential role in the proof of Theorem 2.1.1.

Corollary 2.1.1. *Let λ_2 be the second largest eigenvalue of α, then the following set is a linear subspace of $\mathbb{C}^G$*

$$W := \left\{ f \in \mathbb{C}^G : \sum_{x \in G} f(x) = 0, \quad \textit{and} \quad \frac{\|\alpha f\|_2}{\|f\|_2} = \lambda_2 \right\}.$$

Proof: From Theorem 2.1.2 and Lemma 2.1.4, we obtain an orthogonal basis $f_1, \ldots, f_n$ of $\mathbb{C}^G$, with $f_1 = 1_G$, such that $\alpha f_1, \ldots, \alpha f_n$ are orthogonal and

$$\lambda_i = \frac{\|\alpha f_i\|_2}{\|f_i\|_2}.$$

Also, as we saw in the proof of Theorem 2.1.2, we have

$$\alpha : \langle 1_G \rangle^{\perp} \longrightarrow \langle \alpha 1_G \rangle^{\perp},$$

hence $W \subseteq \langle 1_G \rangle^{\perp}$. Moreover by Remark 2.1.2 we also have

$$\lambda_2 = \max_{0 \neq f \in \langle 1_G \rangle^{\perp}} \frac{\|\alpha f\|_2}{\|f\|_2} = \|\alpha|_{L_0^2(G)}\|_{op}. \tag{2.1.14}$$

W is obviously closed under scalar multiplication, then we just need to show that W is closed under addition. If $v_1, v_2 \in W$ (v_1, v_2 are functions), then by (2.1.14) we have

$$\|\alpha(v_1 \pm v_2)\|_2 \leq \lambda_2 \|v_1 \pm v_2\|_2. \tag{2.1.15}$$

Moreover, by the parallelogram law we have

$$\begin{aligned} \|\alpha(v_1 + v_2)\|_2^2 + \|\alpha(v_1 - v_2)\|_2^2 &= 2\|\alpha(v_1)\|_2^2 + 2\|\alpha(v_2)\|_2^2 \\ &= \lambda_2(2\|v_1\|_2^2 + 2\|v_2\|_2^2) \\ &= \lambda_2(\|v_1 + v_2\|_2^2 + \|v_1 - v_2\|_2^2). \end{aligned} \tag{2.1.16}$$

Then from (2.1.15) and (2.1.16) we have

$$\|\alpha(v_1 \pm v_2)\|_2 = \lambda_2 \|v_1 \pm v_2\|_2,$$

which shows that W is a subspace. □

Now let

$$\lambda_2 = \lambda_3 = \cdots = \lambda_l,$$

then we show that l is big if G does not have any non-trivial representation with small degree. The idea is to define a non-trivial action of G on W, which induce

a non-trivial representation and then use the fact that the group G does not have small representations.

Lemma 2.1.5. *For $g \in G$ and $f \in \mathbb{C}^G$, define $T_g f \in \mathbb{C}^G$ by*

$$T_g f(x) := f(xg).$$

This action of G on $\mathbb{C}^G$ has the following properties:

1) $\|T_g f\|_2 = \|f\|_2$.

2) $\|\alpha(T_g f)\|_2 = \|\alpha f\|_2$.

3) $\mathbb{E}(T_g f) = \mathbb{E}(f)$.

Proof: For 1), we have

$$\|T_g(f)\|_2^2 = \sum_{x\in G} |f(xg)|^2 = \sum_{x\in G} |f(x)|^2 = \|f\|_2^2.$$

To prove 2) we remark that

$$\begin{aligned}(\alpha(T_g f))(y) = (1_A * T_g f)(y) &= \sum_{x\in G} 1_A(yx^{-1}) f(xg) \\ &= \sum_{x\in G} 1_A(yg(xg)^{-1}) f(xg) \qquad (2.1.17)\\ &= T_g(\alpha f)(y).\end{aligned}$$

Then $\alpha(T_g f) = T_g(\alpha f)$, therefore by 1) we can show 2). To prove the last property notice that

$$\sum_{x\in G} T_g f(x) = \sum_{x\in G} f(xg) = \sum_{x\in G} f(x). \qquad (2.1.18)$$

Hence we have 3) as well. □

By Lemma 2.1.5 we deduce that G acts on W, however we need to show that this action in non-trivial.

Lemma 2.1.6. *G acts non-trivially on W.*

Proof: Since any non-zero function f in W is a non-constant function, there exists $g \in G$ such that $T_g f \neq f$. So G acts non-trivially on W. □

Proof of Theorem 2.1.1: From Lemma 2.1.3 we have

$$\sum_{i=1}^{n} \lambda_i^2 = |G||A|.$$

With the notation of Corollary 2.1.1, let

$$\lambda_2 = \lambda_3 = \cdots = \lambda_l,$$

then

$$l\lambda_2^2 \leq |G||A|. \tag{2.1.19}$$

But G acts non-trivially on W by Lemma 2.1.6. Hence from this action we get a non-trivial representation of G, so

$$l = \dim W \geq m(G).$$

Therefore by (2.1.19) we have

$$\lambda_2^2 \leq \frac{|G||A|}{l} \leq \frac{|G||A|}{m(G)},$$

but as mentioned in (2.1.14)

$$\lambda_2 = \|\alpha|_{L_0^2(G)}\|_{op},$$

so

$$\|\alpha|_{L_0^2(G)}\|_{op} \leq \left(\frac{|G||A|}{m(G)}\right)^{1/2}.$$

□

As we saw, the main idea in Gowers' proof was to estimate $\|\alpha f\|$ when the average of f is zero. So one might ask a more general question. For given compact group G, let us define

$$L_0^2(G) := \left\{h \in L^2(G) : \int_G h \, d\mu = 0\right\}.$$

Notice that $L_0^2(G)$ is a Hilbert subspace of $L^2(G)$. Let $f_1, f_2 \in L^2(G)$ and at least one of f_1, f_2 belongs to $L_0^2(G)$. What can we say about $\|f_1 * f_2\|_2$?

To answer to this question we step back and look at what we have done for finite groups, from a more abstract point of view. One of the main identities that appears in Gowers' proof was

$$\|\mathcal{G}\|_{HS} := Tr(\mathcal{G}\mathcal{G}^T) = \sum \lambda_i^2. \tag{2.1.20}$$

From functional analysis, we know that any *Hilbert-Schmidt operator* has a property similar to (2.1.20). Moreover, we used the singular value decomposition

to diagonalize the convolution operator α. Fortunately when an operator over a Hilbert space is compact, we have the singular value decomposition. So we should see when our convolution operator is compact. We consider the following kernel

$$K(x,y) := f_1(xy^{-1}).$$

Since G is a compact group, we have $K(x,y) \in L^2(G \times G)$. For this kernel, we define the following integral operator

$$\begin{aligned} \Phi_K : L^2(G) &\longrightarrow L^2(G) \\ h &\longmapsto \Phi_K(h), \end{aligned} \tag{2.1.21}$$

where

$$\Phi_K(h)(x) := \int_G K(x,y)h(y)d\mu(y) = \int_G f_1(xy^{-1})h(y)d\mu(y) = (f_1 * h)(x). \tag{2.1.22}$$

We should remark that the operator Φ_K indeed should be compared with the definition of α (See (2.1.2)). Therefore, to evaluate $\|f_1 * f_2\|_2$ when $f_2 \in L^2_0(G)$, we need to compute the norm of $\|\Phi_K|_{L^2_0(G)}\|_{op}$, since

$$\|\Phi_K|_{L^2_0(G)}\|_{op} := \max_{0 \neq f \in L^2_0(G)} \frac{\|\Phi(f)\|_2}{\|f\|_2}.$$

In Chapter 3 we will consider these operators and answer the question we asked about the size of $\|f_1 * f_2\|_2$. To sketch the idea, first notice that Φ_K is a Hilbert-Schmidt operator, and hence is a compact operator. We will then use singular value decomposition theorem, which is valid for compact operators, to write the spectrum of $\Phi_K|_{L^2_0(G)}$, say

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq 0.$$

From the singular value decomposition we will have

$$\lambda_1 = \|\Phi_K|_{L^2_0(G)}\|_{op}.$$

λ_1^2 is indeed an eigenvalue of the self adjoint operator $\Phi_K|_{L^2_0(G)}\Phi_K^*|_{L^2_0(G)}$. We will see, using representation theory, that the multiplicity of λ_1^2 in the spectrum is big if the compact group G does not have a small dimensional representation.

2.2. The Peter-Weyl theorem and product-free sets

In this section we will give another approach to approximate the product-free measure of compact groups. By using the famous *Peter-Weyl theorem* we will prove the following theorem.

Theorem 2.2.1. *Let G be a compact group. With the notation used in Definition 1.1.8, let $A \subseteq G$ be a measurable set so that $\mu(A)^3 > 1/m(G)$. Then $A^3 = G$.*

This theorem is essentially due to Emmanuel Breuillard, who reproved Gowers' theorem 1.1.4 for finite groups. However his method can be modified to be used for compact groups. Indeed this method clearly shows how representation theory comes to play in the context of "group expansion". The main idea is to show that, for any element $g \in G$

$$1_A * 1_A * 1_A(g) = \mu\{(x, y, z) \in G^3 : xyz = g\} \neq 0,$$

where μ is the normalized Haar measure. Set $f := 1_A * 1_A * 1_A$. It is standard in number theory and additive combinatorics, to look at the Fourier coefficients of a function which gives much information about the original function. Indeed we will write f with regard to its Fourier expansion, and will derive a contradiction if $f(g) = 0$ for some $g \in G$. However, in order to prove the above theorem, we need to recall some facts from Fourier analysis on compact groups. The main tool that we will use in this section is Parseval's theorem; the compact groups case is due to Peter and Weyl. To give a better illustration of the Peter-Weyl theorem, we start from finite groups, and gradually we will move to compact groups. For more details on Fourier analysis over finite groups see [68]. First we recall some basic definitions.

Definition 2.2.1. *Let V be a finite dimensional $\mathbb{C}$-vector space of dimension n. For a given finite group G, a* **linear representation** *is an homomorphism from G to the group of invertible transformations of V. In other words*

$$\rho : G \longrightarrow \mathrm{GL}(V),$$

is a group homomorphism. n is called the dimension *of the representation ρ.*

Remark 2.2.1. *When ρ is given, we say that V is a representation space of G (or even simply, by abuse of language, a representation of G).*

Let us give some examples:

Example 2.2.1. *The first example is the classic Dirichlet characters. For an integer n, a Dirichlet character modulo n is a group homomorphism from $(\mathbb{Z}/(n\mathbb{Z}))^*$ to $\mathbb{C}^*$. These are all one dimensional representations.*

Another example is the *regular representation.*

Example 2.2.2. *Let G be a finite group. Let V be a $\mathbb{C}$-vector space with basis*

$$\{e_g\}_{g\in G}.$$

For $s \in G$, let ρ_s be a linear transformation that maps e_g to e_{sg}. From this we get a representation of dimension $|G|$. This representation is called the regular representation and detects much of the group theoretical structure of G.

We pick another example.

Example 2.2.3. *Let S_3 be the symmetric group with three elements. Also let V be a $\mathbb{C}$-vector space with basis*

$$\{e_1, e_2, e_3\}.$$

For any $\sigma \in S_3$, let ρ_σ be a linear transformation that maps e_i to $e_{\sigma(i)}$. More precisely, for $v = a_1e_1 + a_2e_2 + a_3e_3$ we have

$$\rho_\sigma(v) = a_1e_{\sigma(1)} + a_2e_{\sigma(2)} + a_3e_{\sigma(3)}.$$

This provides a representation of dimension 3. Notice that the following set is invariant under the action of S_3.

$$W = \{v \in \mathbb{C}^3 : a_1 = a_2 = a_3\}.$$

In particular V has an S_3-invariant subspace.

From the examples above we see that the representation V can be sometimes decomposed into smaller representations. When this cannot happen we say that the representation is **irreducible**.

Definition 2.2.2. *Let (ρ, V) be a representation of a finite group G. ρ is called irreducible when V does not have any invariant subspace under the G-action.*

Of course any one dimensional representation is irreducible. One can show that all of the irreducible representations of a finite abelian group are one dimensional.

Example 2.2.4. *In this example we determine all of the irreducible representations of* $\mathbb{Z}/(n\mathbb{Z})$. *For* $h = 0, \ldots, n-1$ *we define*

$$\begin{aligned} \chi_h : \mathbb{Z}/(n\mathbb{Z}) &\longrightarrow \mathbb{C}^* \\ k &\longrightarrow e^{\frac{2\pi i h k}{n}}. \end{aligned} \tag{2.2.1}$$

These representations are all the irreducible representations of $\mathbb{Z}/(n\mathbb{Z})$. *The set of all of these representations will be denoted by* $\widehat{\mathbb{Z}/(n\mathbb{Z})}$.

These representations indeed, gives us the Fourier analysis on $\mathbb{Z}/(n\mathbb{Z})$. Let us recall it, since this would gives a better understanding of the Peter-Weyl theorem.

Let $f \in L^2(\mathbb{Z}/(n\mathbb{Z}))$ be a function, then the Fourier coefficient of f with respect to a representation $\chi \in \widehat{\mathbb{Z}/(n\mathbb{Z})}$ is defined by

$$\widehat{f}(\chi) := \langle f, \chi \rangle = \sum_{k \pmod n} f(k)\overline{\chi(k)}.$$

Notice that $\widehat{f}$ is an element of $L^2(\widehat{\mathbb{Z}/(n\mathbb{Z})})$. We have the following theorem, known as Fourier inversion.

Theorem 2.2.2 (Fourier inversion for $\mathbb{Z}/(n\mathbb{Z})$)**.**

$$f(g) = \frac{1}{n} \sum_{\chi \in \widehat{\mathbb{Z}/(n\mathbb{Z})}} \widehat{f}(\chi)\chi(g). \tag{2.2.2}$$

Also we have the following theorem, which is sometimes called Plancherel's formula.

Theorem 2.2.3 (Parseval's theorem for $\mathbb{Z}/(n\mathbb{Z})$)**.** *For a function* $f \in L^2(\mathbb{Z}/(n\mathbb{Z}))$ *we have*

$$\|f\|_2^2 = \frac{1}{n}\|\widehat{f}\|_2^2.$$

Now let G be a finite group, and let $f \in L^2(G)$. For any irreducible representation (ρ, V_ρ) of G we can similarly define the Fourier coefficient.

$$\widehat{f}(\rho) := \sum_{g \in G} f(g)\rho(g).$$

Let us emphasize the difference when G is a an abelian group. Indeed, when G is abelian, ρ is one dimensional, so the Fourier coefficient is a complex number. But for a general group, ρ is not necessary one dimensional, so $\widehat{f}(\rho)$ is a linear transformation of V_ρ. The Fourier inversion formula now reads:

Theorem 2.2.4 (Fourier inversion for finite groups)**.** *Let $f \in L^2(G)$ then*

$$f(g) = \frac{1}{|G|} \sum_{\rho} d_\rho Tr_{V_\rho} \left(\widehat{f}(\rho)\rho(g^{-1}) \right), \tag{2.2.3}$$

where the sum is over all the irreducible representations (ρ, V_ρ) of dimension d_ρ.

Moreover we have Parseval's identity.

Theorem 2.2.5 (Parseval's theorem for finite groups)**.** *Let $f \in L^2(G)$ then*

$$\|f\|_2^2 = \frac{1}{|G|} \sum_{\rho} d_\rho Tr_{V_\rho} \left(\widehat{f}(\rho)\widehat{f}(\rho)^* \right), \tag{2.2.4}$$

where $\widehat{f}(\rho)^*$ is the conjugate transpose of the matrix $\widehat{f}(\rho)$.

Let us go further and consider the circle group. For S^1 one can observe that the irreducible finite-dimensional representations are 1-dimensional, hence are given by additive characters. The exponential functions $x \longmapsto e^{nix}$, where n is an integer, are examples of all additive characters. For a function $f \in L^2(S^1)$, define the Fourier coefficient of f by

$$c_n := \frac{1}{2\pi} \int_{S^1} f(x) e^{-inx} dx.$$

Then by Parseval's theorem we have

$$\frac{1}{2\pi} \int_{S^1} |f(x)|^2 = \sum_{n \in \mathbb{Z}} |c_n|^2.$$

the Peter-Weyl's theorem is indeed a vast generalization of Parseval's theorem. As we saw for finite groups and for S^1, by Parseval's theorem the L^2-norm of a function can be expressed by the L^2-norm of its Fourier transform.

We define a finite-dimensional representation of a topological group G on a finite-dimensional complex vector space $V = \mathbb{C}^n$ to be a continuous homomorphism ρ of G into $\mathrm{GL}_n(\mathbb{C})$. The continuity condition means that in any basis of V the matrix entries of $\rho(g)$ are continuous for $g \in G$. It is equivalent to say that $g \longmapsto \rho(g)v$ is a continuous function from G into V for each v in V. Indeed we have

Theorem 2.2.6 (Peter-Weyl)**.** *If G is a compact group, then the linear span of all matrix coefficients for all finite-dimensional irreducible unitary representations of G is dense in $L^2(G)$.*

For more details, we refer the reader to an excellent reference with many examples [48]. Let us set some notations. Let $f \in L^2(G)$ be a square integrable function with respect to the normalized Haar measure μ, meaning that $\mu(G) = 1$. For a continuous representation ρ, define the Fourier transform of f by

$$\widehat{f}(\rho) := \int_G f(g)\rho(g)d\mu(g). \tag{2.2.5}$$

From the Peter-Weyl's theorem, we have the following well known theorems.

Theorem 2.2.7 (Fourier inversion formula for compact groups)**.** *Let G be a compact group and let $f \in L^2(G)$. Then*

$$f(g) = \sum_{\rho} d_\rho \langle \widehat{f}(\rho), \rho(g) \rangle_{HS}, \tag{2.2.6}$$

where the sum is over all the continuous irreducible representations. Moreover, the Hilbert-Schmidt inner product, denoted by $\langle . \rangle_{HS}$ is defined by

$$\langle A, B \rangle_{HS} := Tr(AB^*),$$

where B^* is the complex conjugate.

Remark 2.2.2. *Here we consider all representations to be unitary, which can be done by Weyl's unitary trick since G is a compact group.*

Notice that

$$\|AB\|_{HS} \leq \|A\|_{HS}\|B\|_{HS}. \tag{2.2.7}$$

We also have

Theorem 2.2.8 (The Parseval-Plancherel theorem)**.** *For a compact group G, let $f \in L^2(G)$. Then*

$$\|f\|_2^2 = \sum_{\rho} d_\rho \|\widehat{f}(\rho)\|_{HS}^2, \tag{2.2.8}$$

where the sum is over all the continuous irreducible representations.

Consider the function 1_A, then from Plancherel's theorem, we can deduce the following

Lemma 2.2.1. *For any non-trivial continuous irreducible representation π, we have*

$$\mu(A) \geq m(G)\|\widehat{1_A}(\pi)\|_{HS}^2.$$

Proof: Notice that $\|1_A\|_2^2 = \mu(A)$, so by Plancherel's theorem we have

$$\mu(A) = \sum_{\rho \in \widehat{G}} d_\rho \|\widehat{1_A}(\rho)\|_{HS}^2 \geq d_\pi \|\widehat{1_A}(\pi)\|_{HS}^2 \geq m(G)\|\widehat{1_A}(\pi)\|_{HS}^2.$$

□

Now we prove Theorem 2.2.1.

Proof of Theorem 2.2.1. To prove Theorem 2.2.1, we will consider f to be $1_A * 1_A * 1_A$. Then we will show that $f(g) \neq 0$ for any $g \in G$. This in particular implies that $g \in A^3$, and hence $G = A^3$. Suppose $f(g) = 0$ for some $g \in G$. We will derive a contradiction. Notice that

$$\widehat{f}(\rho) = \widehat{1_A}(\rho)^3, \tag{2.2.9}$$

hence from the Fourier inversion formula we have

$$\begin{aligned} 0 = f(g) &= \sum_{\rho \in \widehat{G}} d_\rho \langle \widehat{1_A}(\rho)^3, \rho(g) \rangle_{HS} \\ &= \mu(A)^3 + \sum_{\rho \neq 1} d_\rho \langle \widehat{1_A}(\rho)^3, \rho(g) \rangle_{HS}. \end{aligned}$$

Therefore

$$\begin{aligned} \mu(A)^3 &= \left| \sum_{\rho \neq 1} d_\rho \langle \widehat{1_A}(\rho)^3, \rho(g) \rangle_{HS} \right| \\ &\leq \sum_{\rho \neq 1} d_\rho \left| \langle \widehat{1_A}(\rho)^3, \rho(g) \rangle_{HS} \right| \\ &= \sum_{\rho \neq 1} d_\rho \left| \langle \widehat{1_A}(\rho)^2, \rho(g) \widehat{1_A}(\rho)^* \rangle_{HS} \right|. \end{aligned} \tag{2.2.10}$$

Notice that $\|\rho(g)\widehat{1_A}(\rho)^*\|_{HS} = \|\widehat{1_A}(\rho)\|_{HS}$ since $\rho(g)$ is an unitary matrix, therefore from (2.2.10) we have

$$\begin{aligned}
\mu(A)^3 &\leq \sum_{\rho\neq 1} d_\rho \left|\langle \widehat{1_A}(\rho)^2, \rho(g)\widehat{1_A}(\rho)^*\rangle_{HS}\right| \\
&\leq \sum_{\rho\neq 1} d_\rho \|\widehat{1_A}(\rho)^2\|_{HS}\|\rho(g)\widehat{1_A}(\rho)^*\|_{HS} \quad \text{(by Cauchy-Schwarz)} \\
&\leq \sum_{\rho\neq 1} d_\rho \|\widehat{1_A}(\rho)\|_{HS}^3 \\
&\leq \sqrt{\frac{\mu(A)}{m(G)}} \sum_{\rho\in\widehat{G}} d_\rho \|\widehat{1_A}(\rho)\|_{HS}^2 \qquad \text{(by Lemma 2.2.1)} \\
&= \sqrt{\frac{\mu(A)}{m(G)}}\mu(A).
\end{aligned}$$

Hence

$$\mu(A)^3 \leq \sqrt{\frac{\mu(A)}{m(G)}}\mu(A) \Longrightarrow \mu(A)^3 \leq \frac{1}{m(G)}, \tag{2.2.11}$$

which is a contradiction. □

Then by Theorem 1.1.2 we can prove Corollary 1.1.8.

2.3. Minimal degree of non-trivial representations of finite groups

As we saw in Gowers' proof, to show that the multiplicity of the second eigenvalue is high, one needs to show that the minimal degree of any non-trivial representation of a given group G is big. These groups are called "quasirandom group" by Gowers [31]. This concept is highly related to the nature of the group. For instance, for a given group G, let ρ be a one dimensional representation, then this representation factors through G/G', where G' is the commutator subgroup. Conversely, any representation of G/G' gives a representation of G. Since G/G' is an abelian group, then G/G' has exactly $[G : G']$ one dimensional representations. Hence we have

Lemma 2.3.1. *The number of one-dimensional representations of G, is $[G : G']$.*

Therefore if a group G is perfect, meaning that $G = G'$, all of its non-trivial representations have dimension bigger or equal than 2. For a finite non-abelian simple group G of order n however, Jordan showed that every non-trivial representation of G has dimension at least $\sqrt{\log n}/2$. This was rediscovered by Gowers as well (See [31], Theorem 4.7).

Frobenius wrote down the character table of $\mathrm{SL}_2(\mathbb{F}_p)$, and then proved that any non-trivial representation of this group has dimension at least $(p-1)/2$. How can one get such bound without finding the character table? We will describe a method which we call the "eigenvalue multiplicity principle". The idea is very simple. For an $n \times n$ complex matrix A, n is obviously greater than or equal to the number of distinct eigenvalues. Let us describe how this simple observation gives us a bound for the minimal degree of a non-trivial representation.

To illustrate this principle we first consider a hypothetical situation. After words we will come back to more concrete examples.

Lemma 2.3.2. *Suppose that G is finite group, and let*

$$\rho : G \longrightarrow GL_d(\mathbb{C}),$$

be a non-trivial representation. For an element $g \in G$ of order p, let us assume that

$$\rho_g := \rho(g) \neq I,$$

where I is the identity matrix in $\mathrm{GL}_d(\mathbb{C})$. Moreover assume that g is conjugate to g^t, for all integers $1 \leq t \leq p-1$. Then $d \geq p-1$.

Proof: Since the order of g is p and ρ_g is not the identity matrix, then at least one of the eigenvalues of ρ_g is $\zeta_p^m := e^{\frac{2\pi i m}{p}}$, where $\gcd(m,p) = 1$.

Notice that ζ_p^{tm} is an eigenvalue of $\rho_{g^t} = \rho_g^t$. But g is conjugate to g^t, hence ρ_g is also conjugate to ρ_{g^t}. Any two conjugate matrices have the same set of eigenvalues. Hence ζ_p^{mt} is also an eigenvalue of ρ_g. From this we get $p-1$ different eigenvalues, so $d \geq p-1$. □

Now let us look at an example. Take the symmetric group of n-elements, where $n \geq 5$. The commutator subgroup of S_n is A_n, which has index 2. Therefore S_n has only two one dimensional representations. One is the trivial representation

and the other one is the sign representation, which assigns to each element of $\sigma \in S_n$ its sign $sgn(\sigma)$.

Lemma 2.3.3. *For $n \geq 5$, let*

$$\rho : S_n \longrightarrow \mathrm{GL}_d(\mathbb{C}),$$

be an irreducible representation of dimension greater than or equal to 2. Then ρ is a faithful representation, meaning that ρ is an injective homomorphism.

S_n acts on $\mathbb{C}^n$ by permuting the coordinates. More precisely, for $\sigma \in S_n$ and $v = a_1e_1 + \cdots + a_ne_n$, we define

$$\sigma.v := a_1e_{\sigma(1)} + \cdots + a_ne_{\sigma(n)}. \tag{2.3.1}$$

This does not give us an irreducible representation. Notice that the subspace W defined by

$$W = \{v \in \mathbb{C}^n : a_1 = a_2 = \cdots = a_n\},$$

is fixed by S_n. However, W is irreducible (it has dimension 1), and one can show that the complement,

$$W^{\perp} := \left\{ v \in \mathbb{C}^n : \sum_i a_i = 0 \right\},$$

is an irreducible representation of degree $n-1$. Frobenius and Schur have studied representation theory of the symmetric group. Indeed in modern language there is a correspondence between the set of irreducible representation of S_n and "Specht Modules". Using this correspondence one can show that, for $n \geq 6$, the minimal degree of non-trivial representations of the simple group A_n is $n-1$.

Here we just consider S_p, when p is a prime greater than 5, and use the eigenvalue multiplicity principle to show that the degree of any irreducible representation of S_p, beside the trivial one and the sign representation, is at least $p-1$. First we prove the following lemma.

Lemma 2.3.4. *For $n \geq 5$, let H be a normal subgroup of S_n such that*

$$H \cap A_n = \{id\},$$

where A_n is the alternating group on n letters. Then H is the trivial subgroup.

PROOF. First we show that H has at most two elements. Suppose $id \neq \sigma \in H$, therefore $\operatorname{sgn}(\sigma) = -1$, since $H \cap A_n = \{id\}$. Hence

$$\sigma^2 \in H \cap A_n = \{id\} \Longrightarrow \sigma = \sigma^{-1}.$$

Let $\tau \in H$ be an another element of H different from σ and id, then

$$\sigma\tau \in H \cap A_n = \{id\} \Longrightarrow \tau = \sigma^{-1} = \sigma,$$

which is a contradiction. Therefore $H = \{id, \sigma\}$. But H is a normal subgroup, therefore for any $\eta \in S_n$ we have

$$\eta\sigma = \sigma\eta,$$

so σ belongs to the center of S_n. It is well known that the center of S_n is trivial, hence H is a trivial subgroup. □

From this lemma we can prove Lemma 2.3.3.

Proof of Lemma 2.3.3: Note that $\ker\rho \trianglelefteq S_n$, therefore $\ker\rho \cap A_n \trianglelefteq A_n$. But A_n is a simple group for $n \geq 5$. Hence $\ker\rho = A_n$ or ρ is faithful. Let

$$\ker\rho = A_n,$$

then we have the following representation of $S_n/A_n \cong \mathbb{Z}/(2\mathbb{Z})$,

$$\begin{aligned} \tilde{\rho} : S_n/A_n &\longrightarrow \mathrm{GL}_d(\mathbb{C}) \\ \sigma A_n &\longmapsto \rho(\sigma). \end{aligned} \tag{2.3.2}$$

Notice that an invariant subspace of $\mathbb{C}^d$ under the action of $\tilde{\rho}$, remains invariant under the action of ρ. So $\tilde{\rho}$ is an irreducible representation of dimension greater than or equal to 2. But this is a contradiction, since $\mathbb{Z}/(2\mathbb{Z})$ has only two one dimensional irreducible representations. □

Theorem 2.3.1. *For a prime $p \geq 5$, let*

$$\rho : S_p \longrightarrow \mathrm{GL}_d(\mathbb{C}),$$

be an irreducible representation of dimension greater than or equal to 2, then $d \geq p - 1$.

Proof: Take the permutation

$$g = (1, 2, \ldots, p-1, p).$$

By Lemma 2.3.3, ρ is faithful therefore

$$\rho_g \neq I.$$

For $1 \leq t \leq p-1$, notice that g and g^t have the same cyclic structure so g is conjugate to g^t, for all integers $1 \leq t \leq p-1$. Moreover the order of g is p. Then by Lemma 2.3.2 we deduce $d \geq p-1$. □

In this argument, we just picked one eigenvalue, and then produced many other eigenvalues from it. In our proof for the minimal degree of non-trivial representations of $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$, we manipulate this argument, and instead of picking just one eigenvalue, we pick many eigenvalues. To do this, we will consider the root functions. We postpone this argument to Chapter 3.

2.4. Some remarks on compact operators

In this thesis, we always consider our Hilbert space to be *separable*, meaning that it has a countable basis, or equivalently has a countable dense subset. A typical example would be $L^2(G)$, when G is a compact group.

Let X, Y be normed spaces. An operator T from X to Y is called *bounded* if there is a number M so that for any $x \in X$ we have

$$\|T(x)\|_Y \leq M\|x\|_X.$$

Definition 2.4.1. *The vector space of all bounded linear operators from X to Y, will be denoted by $B(X, Y)$.*

In linear algebra, we mostly work with finite matrices. Compact operators are the natural generalization of matrices.

Definition 2.4.2. *A linear transformation $T \in B(X, Y)$ is* **compact**, *if for any bounded sequence $\{x_n\}$ in X, the sequence $\{T(x_n)\}$ in Y contains a convergent subsequence.*

To illustrate this definition, let us give some examples. An operator $T \in B(X,Y)$, is called a *finite rank* operator when its image is a finite dimensional vector space. Let T be a finite rank operator with image $Z = Im(T)$. Now, for any bounded sequence $\{x_n\}$ in X, the sequence $\{T(x_n)\}$ is bounded in Z, so by the Bolzano-Weierstrass theorem this sequence must contain a convergent subsequence. Hence T is compact. This in particular implies the following lemma.

Lemma 2.4.1. *Let X be a Banach space. Let $\{T_k\}$ be a sequence of bounded, finite rank operators which converges to $T \in B(X)$, then T is compact.*

When $\mathcal{H}$ is a Hilbert space, the converse of the above theorem is also valid.

Lemma 2.4.2. *Let $T \in B(\mathcal{H})$ be a compact operator, then there is a sequence of finite rank operators $\{T_k\}$ which converges to T in $B(\mathcal{H})$.*

This indeed would justify our attempt to study compact operators for our problem. Notice that, when $T \in B(\mathcal{H})$ is compact, $T_k \longrightarrow T$, where T_k are finite rank. Therefore $T_k^* \longrightarrow T^*$. Hence T^* is also a compact operator. Another interesting property of compact operators is closedness that they form an ideal in $B(\mathcal{H})$. This means that for two bounded operators S, T, if at least one of them is compact, ST is compact.

Now we consider a specific family of compact operators, which are called **Hilbert-Schmidt** operators.

Lemma 2.4.3. *Let $\mathcal{H}$ be a Hilbert space with norm denoted by $\|\cdot\|$. Let $T \in B(\mathcal{H})$ be a bounded operator, and assume $\{e_i\}$, and $\{e_i'\}$ are two orthonormal basis for $\mathcal{H}$, then*

$$\sum \|T(e_i)\|^2 = \sum \|T(e_i')\|^2. \tag{2.4.1}$$

Proof: By Parseval's identity

$$\|T(e_i)\|^2 = \sum_j |\langle T(e_i), e_j' \rangle|^2,$$

and

$$\|T^*(e_j')\|^2 = \sum_i |\langle e_i, T^*(e_j') \rangle|^2.$$

Therefore

$$\begin{aligned}\sum \|T(e_i)\|^2 &= \sum_i \sum_j |\langle T(e_i), e'_j\rangle|^2 \\ &= \sum_j \sum_i |\langle e_i, T^*(e'_j)\rangle|^2 \\ &= \sum \|T^*(e'_i)\|^2 \\ &= \sum \|T(e'_i)\|^2.\end{aligned} \tag{2.4.2}$$

□

With this theorem for $T \in B(\mathcal{H})$ we can define a norm which is called **Hilbert-Schmidt norm**.

Definition 2.4.3. *An operator $T \in B(\mathcal{H})$ is called a* **Hilbert-Schmidt** *operator when for some orthonormal basis $\{e_i\}$, hence for any orthonormal basis, we have*

$$\sum \|T(e_i)\|^2 < \infty.$$

For these operators, the **Hilbert-Schmidt norm** *is defined by*

$$\|T\|_{HS}^2 = \sum \|T(e_i)\|^2.$$

To justify this definition we remark that for a finite matrix A, we have

$$\|A\|_{HS}^2 = Tr(AA^*) = \sum \lambda_i^2,$$

where A^* is the complex conjugate of A and λ_i^2 are the eigenvalues of AA^* (See Theorem 2.1.2). We should mention that the usual norm of an operator is defined by

$$\|T\|_{op} := \sup_{0 \neq x \in \mathcal{H}} \frac{\|T(x)\|}{\|x\|} = \sup_{\substack{x \in \mathcal{H} \\ \|x\|=1}} \|T(x)\|.$$

The following lemma which will be needed for Chapter 3.

Lemma 2.4.4. *For any $T, S \in B(\mathcal{H})$, we have*

$$\|TS\|_{HS} \leq \|T\|_{HS}\|S\|_{HS}.$$

Proof: For any operators $T, S \in B(\mathcal{H})$, and an orthonormal basis $\{e_i\}$, we have

$$\|TS\|_{HS}^2 = \sum \|TS(e_i)\|^2 \leq \|T\|_{op}^2 \sum \|S(e_i)\|^2 = \|T\|_{op}^2 \|S\|_{HS}^2. \tag{2.4.3}$$

Now let e_1 be a unit vector, then by extending this to an orthonormal basis $\{e_i\}$ we observe that

$$\|T(e_1)\| \leq \|T\|_{HS},$$

therefore

$$\|T\|_{op} \leq \|T\|_{HS}.$$

From this and (2.4.3), we have the required inequality. □

Moreover the following properties of Hilbert-Schmidt operators.

Lemma 2.4.5. *Let $\mathcal{H}$ be a separable Hilbert space and let $T \in B(\mathcal{H})$ then*

a) T is Hilbert-Schmidt if and only if T^* is Hilbert-Schmidt.

b) If either S or T is Hilbert-Schmidt, then ST is Hilbert-Schmidt.

c) If T is Hilbert-Schmidt then it is compact.

In Chapter 3 we will give some other properties of Hilbert-Schmidt operators.

2.5. Profinite groups

In this section, we will spend some time to explain some basic properties of profinite groups. Historically, the notion of profinite groups first appeared in the theory of Galois correspondence. Indeed let E/F be a finite Galois extension, and assume that $H \subseteq \mathrm{Gal}(E/F)$. Then $\mathrm{Gal}(E/L) = H$, where L is the fixed field of H. But when E/F is an infinite Galois extension, this is not necessarily true. Krull was the first to put a topology, called the "Krull topology", on $\mathrm{Gal}(E/F)$. This topology is Hausdorff, compact and totally disconnected. With this topology one can show that $\mathrm{Gal}(E/L) = \overline{H}$, where $\overline{H}$ is the closure of H. The Krull topology is essential in the theory of Galois Cohomology.

Another example of profinite group is the ring of p-adic integers, denoted by $\mathbb{Z}_p$. Let us recall that

$$\mathbb{Z}_p := \left\{(x_n) \in \prod(\mathbb{Z}/(p^n\mathbb{Z})) : x_{n+1} \equiv x_n \pmod{p^n}\right\}.$$

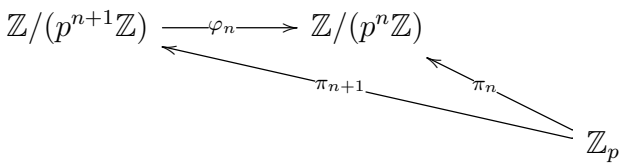
Abstractly we have reduction maps

$$\varphi_n : \mathbb{Z}/(p^{n+1}\mathbb{Z}) \longrightarrow \mathbb{Z}/(p^n\mathbb{Z}), \tag{2.5.1}$$

and then

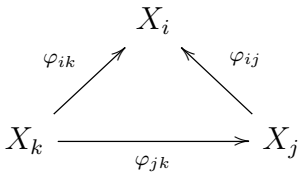
$$\mathbb{Z}_p := \left\{ x = (x_n) \in \prod (\mathbb{Z}/(p^n\mathbb{Z})) : \varphi_{n+1}\pi_{n+1}(x) = \pi_n(x) \right\},$$

where π_n is projection map.



Put the discrete topology on $\mathbb{Z}/(p^n\mathbb{Z})$, then by Tychonoff's theorem $\prod \mathbb{Z}/(p^n\mathbb{Z})$ is compact. Using this, one can that $\mathbb{Z}_p$ is a compact ring. This motivates us to consider the following concepts. A directed set is a partially ordered set I such that for all $i_1, i_2 \in I$ there is an element $j \in I$ for which $i_1 \leq j$ and $i_2 \leq j$.

Definition 2.5.1. *An inverse system (X_i, φ_{ij}) of topological spaces indexed by a directed set I consists of a family $(X_i)_{i\in I}$ of topological spaces and a family $\varphi_{ij} : X_j \longrightarrow X_j$, for $i \leq j$, of continuous maps such that φ_{ii} is the identity map Id_{X_i}, for each i and $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ whenever $i \leq j \leq k$.*

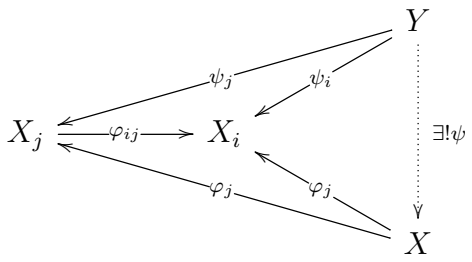


The sets for which no other topology is specified will be regarded as topological spaces with the discrete topology. If each X_i is a topological group and each φ_{ij} is a continuous homomorphism, then (X_i, φ_{ij}) is called an inverse system of topological groups; an inverse system of topological rings is defined similarly.

Example 2.5.1. *Assume $I = \mathbb{N}$ and let p be a prime. Let $G_i = \mathbb{Z}/(p^i\mathbb{Z})$ for each i, and for $i \leq j$ let $\varphi_{ij} : G_j \longrightarrow G_i$ be the reduction homomorphism. Then (G_i, φ_{ij}) is an inverse system of finite rings.*

Definition 2.5.2. *An inverse limit (or projective limit) (X, φ_i) of an inverse system (X_i, φ_{ij}) of topological spaces (resp. groups, rings) is a topological space (resp. group, ring) X together with a compatible family $\varphi_i : X \longrightarrow X_i$ of continuous maps (resp. continuous homomorphisms) with the following universal property: whenever $\psi_i : Y \longrightarrow X_i$ is a compatible family of continuous maps from*

a space Y (resp. of continuous homomorphisms from a group or a ring Y), there is a unique continuous map (resp. continuous homomorphism) $\psi : Y \longrightarrow X$ such that $\varphi_i \psi = \psi_i$ for each i.



(2.5.2)

Now let (X_i, φ_{ij}) be an inverse system, then the inverse limit of this inverse system, denoted by $\varprojlim X_i$, exists. To define this, we simply mimic the construction of $\mathbb{Z}_p$.

$$\varprojlim X_i := \left\{ x = (x_i) \in \prod X_i : \varphi_{ij}\pi_j(x) = \pi_i(x) \right\}. \tag{2.5.3}$$

Here π_i stands for the projection map. A topological space is called totally disconnected when the connected component of each element has only one element.

Lemma 2.5.1. *Let (X_i, φ_{ij}) be an inverse system, with inverse limit $X := \varprojlim X_i$, then*

1) If each X_i is Hausdorff, so is X.

2) If each X_i is compact and Hausdorff, so is X.

3) If each X_i is totally disconnected, so is X.

Therefore if all X_i are discrete then X is Hausdorff, compact and totally disconnected.

Definition 2.5.3. *A topological group G is called profinite when G is Hausdorff, compact and totally disconnected.*

One can show that any profinite group is an inverse limit of finite groups. To emphasize the vital role of profinite groups, let us mention that

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{\substack{E/\mathbb{Q} \\ \text{finite, Galois}}} \mathrm{Gal}(E/\mathbb{Q}).$$

This relation is very important, since by this one can reduce any continuous representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to a linear representation of a finite quotient. In Chapter 3, inspired by these arguments, we will give some other properties of

profinite groups which are relevant to our work. We will work with continuous representations of the profinite group $\mathrm{SL}_k(\mathbb{Z}_p)$.

2.6. Regular trees

This section is devoted to the automorphism group of regular trees. A tree is a connected non-empty graph without circuits. For instance the following diagram is a 3-regular tree. Another way to visualize a regular tree is to look at the Cayley

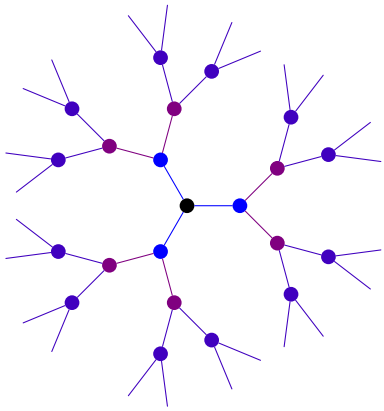


Figure 2.2. Rooted tree

graph of the free group F_n.

Trees have been source of many important contributions in mathematics. We pick an example merely to show its importance. Ihara [45] in 1966 proved that every torsion-free subgroup G of $\mathrm{SL}_2(\mathbb{Q}_p)$ is a free group. Serre [63] reproved this theorem using trees. Serre's idea was to connect this group to a tree via the fundamental group of a topological space. Indeed he showed that G act freely ("without fixed points") on a tree X. The idea is roughly that G is the universal cover of X/G, hence G may then be identified with the fundamental group $\pi_1(X/G)$ of the quotient graph X/G, a group which is obviously free. In this thesis we are more interested in the automorphism group of a tree. Let us set up some notations for this group.

Let T_{k+1} be a regular tree of degree $k+1$. The automorphism group $Aut(T_{k+1})$ of T_{k+1} is the group of isometries of the vertex set of T_{k+1} with respect to the discrete metric d, where $d(x, y)$ is the smallest number of edges on a path in T_{k+1} connecting x and y. In other words, by an automorphism of T_{k+1} we mean a

permutation of the set of vertices of T_{k+1} that preserves adjacency. Notice that $Aut(T_{k+1})$ acts transitively on T_{k+1}. For a sequence $\sigma_n \in Aut(T_{k+1})$, we define

$$\sigma_n \longrightarrow \sigma,$$

if for any $x \in T_{k+1}$, there exists n_x so that for all $n \geq n_x$, we have $\sigma_n(x) = \sigma(x)$. With this topology, called pointwise convergence topology, one can show that $Aut(T_{k+1})$ is a locally compact topological group. We can define this topology via a subbasis for the topology. We fix a vertex O of T_{k+1} which we may occasionally refer as the root. Let A_{k+1} be the stabilizer of O in $Aut(T_{k+1})$. For any $x \in T_{k+1}$, there is a an element $\sigma \in Aut(T_{k+1})$, so that $\sigma_x(O) = x$, therefore

$$\sigma_x A_{k+1} \sigma_y, \quad x, y \in T_{k+1},$$

is a subbasis of the topology.

Lemma 2.6.1. *A_{k+1} is compact.*

Proof: Let $\{\sigma_n\}$ be a sequence in A_{k+1}. Let $\{x_0 = O, x_1, x_2, \ldots\}$ be the set of vertices of the tree T_{k+1}. Notice that $\sigma_n(O) = O$. Since σ_n is an isometry, for any k the following set is a finite set

$$\{\sigma_n(x_k)\}.$$

Therefore for a subsequence, say a_{1n}, we have

$$\sigma_{a_{11}}(x_1) = \sigma_{a_{12}}(x_1) = \cdots = \sigma_{a_{1n}}(x_1) = \cdots .$$

Now we look at the finite set $\{\sigma_{a_{1n}}(x_2)\}$. There is a subsequence of a_{1n}, denoted by a_{2n}, so that

$$\sigma_{a_{21}}(x_2) = \sigma_{a_{22}}(x_2) = \cdots = \sigma_{a_{2n}}(x_2) = \cdots .$$

We construct these subsequences inductively and define

$$\sigma(x_i) := \sigma_{a_{ii}}(x_i).$$

Then $\sigma_{a_{nn}} \longrightarrow \sigma$. □

It turns out that A_{k+1} is a profinite group. In fact, every $\sigma \in A_{k+1}$ fixes O and thereby permutes the set of all $(k+1)k^{j-1}$ vertices of distance j from O, for every $j \geq 1$. This induces a homomorphism

$$\varphi_j : A_{k+1} \longrightarrow S_{(k+1)k^{j-1}},$$

where S_m denotes the symmetric group on $\{1, 2, \ldots, m\}$. We can now define the following "congruence subgroups" that provide a system of fundamental open sets around the identity automorphism:

$$C_j = \{\sigma \in A_{k+1} : \varphi_j(\sigma) = id\}.$$

We have

$$A_{k+1} = \varprojlim A_{k+1}/C_j. \tag{2.6.1}$$

We will speak more about this group in Chapter 3.

Chapter 3

PRODUCT-FREE SUBSETS OF PROFINITE GROUPS

Authors: Mohammad Bardestani, Keivan Mallahi-Karai.

In this chapter we will prove our theorems which were stated in Section 1.1.1. This chapter is organized as follows: In Section 3.1 we will recall some definitions and set the notations. Moreover in this section we will establish some elementary properties of the product-free measure. In Section 3.2 we gather some facts about the representation theory of profinite groups. In Section 3.3 we will prove Theorem 1.1.2. Gowers' proof [31] uses the language of quasirandom graphs. We will translate his argument to direct arguments in functional analysis involving Hilbert-Schmidt operators which is more suitable for compact groups. This is done in Section 3.4. In Section 3.5 we will prove Theorems 1.1.5, 1.1.6.

3.1. Product-free measure

For a profinite group

$$G = \varprojlim G_i,$$

the Haar measure can be easily described as a "limit" of counting measures. More precisely, for an open set $U \subseteq G$ we have,

$$\mu(U) = \lim_i \frac{|\phi_i(U)|}{|G_i|}, \tag{3.1.1}$$

where

$$\phi_i : G \longrightarrow G_i,$$

is the continuous projection (See Definition 2.5.2).

Moving to product-free measure, let us recall its definition. Let G be a compact group with normalized Haar measure μ. We recall the definition of the product-free measure of G.

$$\mathrm{pf}(G) := \sup\{\mu(A) : A \subseteq G \text{ is measurable }, A \cap A^2 = \emptyset\}.$$

First note that $\mathrm{pf}(G) \leq 1/2$. This follows from the fact that if $A \cap A^2 = \emptyset$ then for each $x \in A$, the sets A and xA are disjoint and have the same Haar measure. When G is a non-trivial group then one can also easily see that $\mathrm{pf}(G) > 0$ as we now show: Let G be a compact group. It is known that the topology of G is given by a bi-invariant metric (see Corollary A4.19 in [43].) Let d_G be such a metric and $D = \mathrm{diam}(G)$ be the diameter of G which is defined by

$$\dim(G) = \sup\{d_G(x, y) : x, y \in G\}.$$

Let us also denote $f(r) = \mu(B(x, r))$ (note that the bi-invariance of d_G implies that the volume of the ball is independent of its center.) Then we have

Proposition 3.1.1.

$$\mathrm{pf}(G) \geq f(D/3) > 0.$$

Proof: Choose $y, z \in G$ such that $d_G(y, z) = D$ and let $x = z^{-1}y$. We have,

$$d_G(x, x^2) = d_G(1, x) = d_G(z, zx) = d_G(z, y) = D. \tag{3.1.2}$$

For $u, v \in B(x, D/3)$ we have

$$d_G(uv, x^2) \leq d_G(uv, ux) + d_G(ux, x^2) = d_G(v, x) + d_G(u, x) < \frac{2D}{3}.$$

Then $uv \in B(x^2, 2D/3)$ and hence $uv \notin B(x, D/3)$ since otherwise we would have

$$d_G(x, x^2) \leq d_G(x, uv) + d_G(uv, x^2) < \frac{D}{3} + \frac{2D}{3} = D,$$

which contradicts (3.1.2). This shows that $B(x, D/3)$ is a product-free set. □

We would also like to remark that one can give an alternative definition by replacing $A \cap A^2 = \emptyset$ with $\mu(A \cap A^2) = 0$. However, these turn out to be equivalent:

Proposition 3.1.2. *Suppose G is an infinite compact group with Haar measure μ. Define*

$$\mathrm{pf}_0(G) = \sup\{\mu(A) : A \subseteq G \text{ is measurable }, \mu(A \cap A^2) = 0.\}$$

Then $\mathrm{pf}_0(G) = \mathrm{pf}(G)$.

Proof: It is clear that $\mathrm{pf}(G) \leq \mathrm{pf}_0(G)$. To prove the inverse inequality, let A be a measurable set with $\mu(A \cap A^2) = 0$. Then $B = A - (A \cap A^2) \subseteq A$ has the same measure as A and $B \cap B^2 \subseteq B \cap A^2 = \emptyset$. This shows that $\mathrm{pf}(G) \leq \mathrm{pf}_0(G)$. □

3.2. Complex representations of profinite groups

In this section we will gather some facts about profinite groups that will be used later. Our final aim in this section is to show that any non-trivial complex continuous representation of $\mathrm{SL}_k(\mathbb{Z}_p)$ (respectively $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$) factors through a non-trivial representation of $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ (respectively $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$) for some n (See Corollary 3.2.1). In the next section we will find a lower bound for such a representation.

We call a family $\mathcal{I}$ of normal subgroups of an arbitrary group G a filter base if for all $K_1, K_2 \in \mathcal{I}$ there is a subgroup $K_3 \in \mathcal{I}$ which is contained in $K_1 \cap K_2$. Now let G be a topological group and $\mathcal{I}$ a filter base of closed normal subgroups, and for $K, L \in \mathcal{I}$ define $K \preceq L$ if and only if L is a subgroup of K. Thus $\mathcal{I}$ is a directed set with respect to the order $\preceq$ and the surjective homomorphisms $q_{KL} : G/L \longrightarrow G/K$, defined for $K \preceq L$, make the groups G/K into an inverse system. Write

$$\widehat{G} = \varprojlim(G/K).$$

There is a continuous homomorphism

$$\theta : G \longrightarrow \widehat{G}$$

with kernel $\bigcap_{K\in\mathcal{I}} K$, whose image is dense in $\widehat{G}$. We have the following

Proposition 3.2.1 (See [69], proposition 1.2.2)**.** *If G is compact then θ is surjective; if G is compact and $\bigcap_{K\in\mathcal{I}} K = \{id\}$ then θ is an isomorphism of topological groups.*

Moreover we have,

Proposition 3.2.2 (See [69], proposition 1.2.1)**.** *Let (G, φ_n) be an inverse limit of an inverse system (G_n) of compact Hausdorff topological groups and let L be an open normal subgroup of G. Then $\ker \varphi_n \leq L$ for some n.*

For the profinite group $\mathrm{SL}_k(\mathbb{Z}_p)$ consider the following surjective homomorphism

$$0 \longrightarrow K_n \longrightarrow \mathrm{SL}_k(\mathbb{Z}_p) \xrightarrow{\varphi_n} \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow 0,$$

where φ_n is induced by the canonical surjective homomorphism $\mathbb{Z}_p \longrightarrow \mathbb{Z}/(p^n\mathbb{Z})$. Clearly the set $\mathcal{I}$ of K_n is a filter base and $\bigcap K_n = I$, therefore by Proposition 3.2.1 we have

$$\mathrm{SL}_k(\mathbb{Z}_p) = \varprojlim \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})).$$

Similarly

$$\mathrm{Sp}_{2n}(\mathbb{Z}_p) = \varprojlim \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})).$$

The following proposition is a standard fact in Galois representation, however for the sake of completeness we will prove it.

Proposition 3.2.3. *Let G be a profinite group, and assume $\rho : G \longrightarrow \mathrm{GL}_m(\mathbb{C})$ is a continuous representation. Then the kernel of ρ is an open subgroup, hence $\mathrm{Im}(\rho)$ is a finite subgroup of $\mathrm{GL}_m(\mathbb{C})$.*

Proof: First we show that there exists a neighborhood of the identity element in $\mathrm{GL}_m(\mathbb{C})$ that does not contain any subgroup other than the trivial subgroup. Let

$$\exp : \mathfrak{g}l_m(\mathbb{C}) \longrightarrow \mathrm{GL}_m(\mathbb{C}),$$

be the exponential map of the Lie group $\mathrm{GL}_m(\mathbb{C})$, where $\mathfrak{g}l_m(\mathbb{C})$ is the Lie algebra of the Lie group $\mathrm{GL}_m(\mathbb{C})$. Let U_1 be an open neighborhood of $0 \in \mathfrak{g}l_m(\mathbb{C})$ on which the exponential map is a diffeomorphism. Set $U = (1/2)U_1$ (if it is necessary, we will take $U = (1/2^k)U_1$ for some k big enough). Let H be a non-trivial subgroup of $\mathrm{GL}_m(\mathbb{C})$ contained in $\exp(U)$. Then one can choose $X \in U$ such that $a = \exp(X) \in H$ and $2X \in U_1 \setminus U$. This shows that

$$a^2 = \exp(2X) \in \exp(U_1) \setminus \exp(U),$$

which is a contradiction since $a^2 \in H \subseteq \exp(U)$. Therefore U is a neighborhood of the identity element in $\mathrm{GL}_m(\mathbb{C})$ that does not contain any subgroup other than the trivial subgroup.

Then $V := \rho^{-1}(U)$ is an open subset of G containing the identity and from the properties of profinite groups, we know that V contains an open subgroup, say H. This implies that $\rho(H) = 1$ and hence $H \leq \ker \rho$. Therefore $\ker \rho$ is open thus $\mathrm{Im}(\rho)$ is finite. □

This result implies the following:

Corollary 3.2.1. *Let $\rho : \mathrm{SL}_k(\mathbb{Z}_p) \longrightarrow \mathrm{GL}_m(\mathbb{C})$ be a non-trivial representation. Then ρ factors through a non-trivial representation of $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ for some n.*

Proof: By Proposition 3.2.3, $\ker \rho$ is an open normal subgroup, therefore by Proposition 3.2.2 we have $K_n \leq \ker \rho$, for some n, where

$$0 \longrightarrow K_n \longrightarrow \mathrm{SL}_k(\mathbb{Z}_p) \xrightarrow{\varphi_n} \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow 0.$$

Therefore ρ factors through a non-trivial representation of

$$\bar{\rho} : \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow \mathrm{GL}_m(\mathbb{C}). \tag{3.2.1}$$

□

Theorem 3.2.1 is also valid for $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$.

3.3. Root functions

Our approach to obtain the minimal degree of all non-trivial representations of SL_k and Sp_{2k}, is to consider an appropriate abelian subgroup of these groups. Then by looking at its image under the given representation in $\mathrm{GL}_d(\mathbb{C})$ where d is the dimension of the representation, we will show that, these matrices have many different eigenvalues and then we will prove that the dimension of the representation is big. To make this idea precise, let us recall a basic fact from linear algebra.

Definition 3.3.1. *Let $\mathcal{S}$ be a family of matrices in $M_d(\mathbb{C})$. For a function*

$$r : \mathcal{S} \longrightarrow \mathbb{C},$$

define

$$V(r) := \{v \in \mathbb{C}^d : Sv = r(S)v \quad \textit{for all } S \in \mathcal{S}\}.$$

A map $r : \mathcal{S} \longrightarrow \mathbb{C}$ *will be called a* **root** *of* $\mathcal{S}$ *if* $V(r) \neq \{0\}$. *Moreover* $V(r)$ *is called a* **root subspace**.

The following proposition is a special case of Theorem 15 in section 9.5. of [42].

Proposition 3.3.1. *Let* $\mathcal{S}$ *be a commuting family of* $d \times d$ *unitary matrices. Then* $\mathcal{S}$ *has only a finite number of roots. If* $r_1, \ldots, r_t$ *are all the distinct roots of* $\mathcal{S}$ *then*

(1) $V(r_i)$ *is orthogonal to* $V(r_j)$ *for* $i \neq j$.

(2) $\mathbb{C}^d = V(r_1) \oplus \cdots \oplus V(r_t)$.

3.3.1. Root functions for the special linear groups

Let L be the abelian subgroup of $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ defined by

$$L = \left\{ \begin{pmatrix} I_{k-1} & x \\ 0 & 1 \end{pmatrix} : x \in (\mathbb{Z}/(p^n\mathbb{Z}))^{k-1} \right\},$$

where x is a column vector. Moreover let H be the subgroup of $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ consisting of matrices of the form

$$H = \left\{ \begin{pmatrix} \sigma & 0 \\ 0 & 1 \end{pmatrix} : \sigma \in \mathrm{SL}_{k-1}(\mathbb{Z}/(p^n\mathbb{Z})) \right\}.$$

It is easy to see that H normalizes L. Indeed we have

$$\begin{pmatrix} \sigma & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} I_{k-1} & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \sigma & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} I_{k-1} & \sigma x \\ 0 & 1 \end{pmatrix}. \tag{3.3.1}$$

Let

$$\rho : \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow \mathrm{GL}_d(\mathbb{C}), \tag{3.3.2}$$

be a non-trivial representation. Note that $\mathcal{S}_{\mathrm{SL}} := \rho(L)$ is an abelian group. Next proposition shows that H acts on the root functions and the root subspaces of $\mathcal{S}_{\mathrm{SL}}$.

Proposition 3.3.2. *Let r be one of the roots in the decomposition in Proposition 3.3.1 and let $h \in H$. For any $s = \rho(l) \in \mathcal{S}_{\mathrm{SL}}$, define*

$$r_h(s) := r(\rho(hlh^{-1})).$$

Then r_h is also a root for $\mathcal{S}_{\mathrm{SL}}$, and $V(r_h) = \rho(h^{-1})V(r)$.

Proof: First note that since H normalizes L, the map r_h is well-defined. For $w \in V(r)$ and $l \in L$, we have

$$\begin{aligned} \rho(l)(\rho(h^{-1})w) &= \rho(h^{-1})(\rho(hlh^{-1})w) \\ &= r(\rho(hlh^{-1}))\rho(h^{-1})w \\ &= r_h(\rho(l))(\rho(h^{-1})w). \end{aligned} \tag{3.3.3}$$

This shows that r_h is a root for $\mathcal{S}_{\mathrm{SL}}$, and $\rho(h^{-1})V(r) \subseteq V(r_h)$. To show the equality let $v \in V(r_h)$, then for any $l \in L$ we have

$$\rho(l)(\rho(h)v) = \rho(h)(\rho(h^{-1}lh)v) = r(\rho(l))(\rho(h)v),$$

so $\rho(h)V(r_h) \subseteq V(r)$. □

Consider the following matrices

$$e_i := \left(\begin{array}{ccccc|c} 1 & & & & & 0 \\ & 1 & & & & \vdots \\ & & \ddots & & & 1 \\ & & & 1 & & \vdots \\ & & & & 1 & 0 \\ \hline 0 & & & & 0 & 1 \end{array}\right) \rightarrow i\text{th row},$$

that are some elementary matrices. Notice that the values of the root functions are the eigenvalues of the matrices, so their values are roots of unity. We recall that $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ is generated by the elementary matrices ((by row-and-column reduction of integral matrices to compute elementary divisors), and all elementary matrices are conjugate to e_1. Therefore we have the following lemma.

Lemma 3.3.1. *If $\rho(e_1) = I$, then ρ is a trivial representation.*

Now let ρ be a faithful representation then we claim the following.

Lemma 3.3.2. *There exists a root r for $\mathcal{S}_{\mathrm{SL}}$, such that $r(\rho(e_1)) = \zeta$, where ζ is a primitive p^nth root of unity.*

PROOF. Let us denote the roots of $\mathcal{S}_{\mathrm{SL}}$ by $r_1, \ldots, r_t$. Assume that for all $1 \leq i \leq t$ we have $r_i(\rho(e_1)) = \zeta_{p^n}^{m_i}$, where $p \mid m_i$. Assuming this, we will show that $\rho(e_1^{p^{n-1}}) = I$, which is a contradiction since ρ is a faithful representation and the order of e_1 is p^n.

By Proposition 3.3.1 we have

$$\mathbb{C}^d = V(r_1) \oplus \cdots \oplus V(r_t).$$

For an arbitrary element $v \in \mathbb{C}^d$ write

$$v = v_1 + \cdots + v_t,$$

where $v_i \in V(r_i)$. Therefore for any integer m we have

$$\begin{aligned} (\rho(e_1))^m v &= r_1(\rho(e_1))^m v_1 + \cdots + r_t(\rho(e_1))^m v_t \\ &= \zeta_{p^n}^{m_1 m} v_1 + \cdots + \zeta_{p^n}^{m_t m} v_t. \end{aligned} \tag{3.3.4}$$

In particular for $m = p^{n-1}$ we have

$$\rho(e_1^{p^{n-1}})v = v_1 + \cdots + v_t = v.$$

Hence $\rho(e_1^{p^{n-1}}) = I$. □

Now we can prove Theorem 1.1.2 for $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$.

Proof of Theorem 1.1.2 for $m_f(\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})))$ when $k \geq 3$: Let

$$\rho : \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow \mathrm{GL}_d(\mathbb{C}),$$

be a faithful representation. First note that L, as an abstract group, is isomorphic to the direct sum of $k-1$ copies of the cyclic group $\mathbb{Z}/(p^n\mathbb{Z})$. Notice that $\{e_1, \ldots, e_{k-1}\}$ is the standard basis of L. We will occasionally deviate from our standard notation for the group operation and use additive notation for group operation on L, when this isomorphism is used. For instance, we will write $e_1 + e_2$ instead of $e_1 \cdot e_2$.

By Lemma 3.3.2 there is a root r for $\mathcal{S}_{\mathrm{SL}}$ such that $r(\rho(e_1)) = \zeta_{p^n}^{m_1}$, where $\gcd(m_1, p) = 1$. We also assume that for $2 \leq i \leq k-1$ we have $r(\rho(e_i)) = \zeta_{p^n}^{m_i}$

where $0 \leq m_i \leq p^n - 1$. For $t \in (\mathbb{Z}/(p^n\mathbb{Z}))^*$ and $x_2, \ldots, x_{k-1} \in \mathbb{Z}/(p^n\mathbb{Z})$ whose values will later be assigned, define

$$\alpha = \alpha(t, a_2, \cdots, a_{k-1}) = \left(\begin{array}{cccccc|c} t & a_2 & a_3 & \cdots & & a_{k-1} & 0 \\ 0 & t^{-1} & & & & & 0 \\ 0 & 0 & 1 & & & & 0 \\ \vdots & \vdots & & \ddots & & & \vdots \\ & & & & 1 & & \\ 0 & 0 & \cdots & & 0 & 1 & 0 \\ \hline 0 & 0 & \cdots & & 0 & 0 & 1 \end{array}\right) \in H.$$

Using (3.3.1), a simple computation shows that

$$\alpha e_1 \alpha^{-1} = te_1, \quad \alpha e_2 \alpha^{-1} = t^{-1}e_2 + a_2 e_1, \quad \alpha e_i \alpha^{-1} = e_i + a_i e_1 \quad (3 \leq i \leq k-1).$$

By Proposition 3.3.2, we have $r_{t,a_2,\cdots,a_{k-1}} := r_\alpha$ is a root and

$$\begin{aligned} r_\alpha(\rho(e_1)) &= r(\rho(\alpha e_1 \alpha^{-1})) = r(\rho(te_1)) = \zeta_{p^n}^{tm_1}, \\ r_\alpha(\rho(e_2)) &= r(\rho(\alpha e_2 \alpha^{-1})) = r(\rho(t^{-1}e_2 + a_2 e_1)) = \zeta_{p^n}^{t^{-1}m_2 + a_2 m_1}, \\ r_\alpha(\rho(e_i)) &= r(\rho(\alpha e_i \alpha^{-1})) = r(\rho(e_i + a_i e_1)) = \zeta_{p^n}^{m_i + a_i m_1} \quad (3 \leq i \leq k-1). \end{aligned} \tag{3.3.5}$$

Now, since $\gcd(m_1, p) = 1$, by varying the values of $t, a_2, \ldots, a_{k-1}$ we can get at least

$$\varphi(p^n)p^{(k-2)n} = (p^n - p^{n-1})p^{(k-2)n},$$

different roots. This shows that the dimension of the representation space has to be at least

$$(p^n - p^{n-1})p^{(k-2)n}.$$

□

Now let ρ be a non-trivial representation. Then we have

Lemma 3.3.3. *Let ρ be a non-trivial representation, then there exists a root r for $\mathcal{S}_{\mathrm{SL}}$, such that $r(\rho(e_1)) = \zeta_{p^n}^{m_1}$, where m_1 is non-zero in $\mathbb{Z}/(p^n\mathbb{Z})$.*

Proof: If for all roots we have $r_i(\rho(e_1)) = 1$, then similar to the proof of Lemma 3.3.2 we can deduce that $\rho(e_1) = I$. But by Lemma 3.3.1 we saw that if $\rho(e_1) = I$ then ρ is a trivial representation. That is a contradiction. □

Proof of Theorem 1.1.2 for $m\left(\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))\right)$ when $k \geq 3$: Let

$$\rho : \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow \mathrm{GL}_d(\mathbb{C}), \tag{3.3.6}$$

be a non-trivial representation. Since ρ is not a trivial representation then by Lemma 3.3.1, we deduce that $\rho(e_1) \neq I$. With the same notation we used in the previous proof, we obtain the following identities similar to (3.3.5).

$$\begin{aligned}
&r_\alpha(\rho(e_1)) = r(\rho(\alpha e_1 \alpha^{-1})) = r(\rho(te_1)) = \zeta_{p^n}^{tm_1},\\
&r_\alpha(\rho(e_2)) = r(\rho(\alpha e_2 \alpha^{-1})) = r(\rho(t^{-1}e_2 + a_2e_1)) = \zeta_{p^n}^{t^{-1}m_2 + a_2m_1},\\
&r_\alpha(\rho(e_i)) = r(\rho(\alpha e_i \alpha^{-1})) = r(\rho(e_i + a_ie_1)) = \zeta_{p^n}^{m_i + a_im_1} \quad (3 \leq i \leq k-1).
\end{aligned} \tag{3.3.7}$$

The only difference is that, here m_1 is non-zero in $\mathbb{Z}/(p^n\mathbb{Z})$, whereas in the previous proof it was coprime to p. So by varying the values of $t, a_2, \ldots, a_{k-1}$ we can get at least $p^{k-1} - p^{k-2}$ different roots. □

For $\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))$ this method does not work. Instead we present a different proof.

Proof of Theorem 1.1.2 for $m_f\left(\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))\right)$: Let

$$\rho : \mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow \mathrm{GL}_d(\mathbb{C}),$$

be a faithful representation and set

$$a := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Let $A := \rho(a) \neq I$. Since the order of a is p^n and ρ is faithful, then A has a non-trivial eigenvalue ζ which is a primitive p^nth root of unity, since otherwise

$$A^{p^{n-1}} = I,$$

which is a contradiction.

Notice that a is conjugate to a^m, where m is a square in $(\mathbb{Z}/(p^n\mathbb{Z}))^*$. Therefore A is conjugate to A^m. Hereafter m will be an arbitrary quadratic residue in $\mathbb{Z}/(p^n\mathbb{Z})$. This implies that A and A^m would have the same set of eigenvalues. But ζ^m is an eigenvalue of A^m. The number of square elements in $(\mathbb{Z}/(p^n\mathbb{Z}))^*$ is $\varphi(p^n)/2$. Therefore A has at least $\varphi(p^n)/2$ different eigenvalues. So

$$d \geq \frac{\varphi(p^n)}{2}.$$

□

For $m\,(\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z})))$, the same method gives the bound $(p-1)/2$.

3.3.2. Root functions for the symplectic groups

Let J denote the $2k \times 2k$ matrix

$$J := \begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix}.$$

The symplectic group is defined as follows

$$\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) := \left\{ A \in \mathrm{GL}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) : AJA^T = J \right\}.$$

Elements of this group can be describe by the following relation:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) \Longleftrightarrow \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha^T & -\beta^T \\ -\gamma^T & \delta^T \end{pmatrix} = I_{2k}.$$

In particular if $\sigma \in M_k(\mathbb{Z}/(p^n\mathbb{Z}))$ is a symmetric matrix then

$$\begin{pmatrix} I_k & \sigma \\ 0 & I_k \end{pmatrix} \in \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})).$$

It is known that the reduction map

$$\mathrm{Sp}_{2k}(\mathbb{Z}) \longrightarrow \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})),$$

is a surjective homomorphism (See [54], Theorem VII.21). Moreover $\mathrm{Sp}_{2k}(\mathbb{Z})$ is generated by (See [57] Section §5, Proposition 2, or [5], Chapter III)

$$\begin{pmatrix} I_k & \sigma \\ 0 & I_k \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix},$$

where σ is a symmetric matrix. But

$$\begin{pmatrix} I_k & I_k \\ 0 & I_k \end{pmatrix} \begin{pmatrix} I_k & 0 \\ -I_k & I_k \end{pmatrix} \begin{pmatrix} I_k & I_k \\ 0 & I_k \end{pmatrix} = \begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix}.$$

From these we have the following lemma.

Lemma 3.3.4. *The following matrices are a generating set for* $\mathrm{Sp}_{2k}(\mathbb{Z})$*, and hence a generating set for* $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$*,*

$$\begin{pmatrix} I_k & \sigma_1 \\ 0 & I_k \end{pmatrix}, \quad \begin{pmatrix} I_k & 0 \\ \sigma_2 & I_k \end{pmatrix},$$

where $\sigma_i^T = \sigma_i$ *for* $i = 1, 2$*.*

Notice that for a symmetric matrix $\sigma \in M_k(\mathbb{Z}/(p^n\mathbb{Z}))$, we have

$$\begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix} \begin{pmatrix} I_k & \sigma \\ 0 & I_k \end{pmatrix} \begin{pmatrix} 0 & -I_k \\ I_k & 0 \end{pmatrix} = \begin{pmatrix} I_k & 0 \\ -\sigma & I_k \end{pmatrix}.$$

Therefore

$$\begin{pmatrix} I_k & \sigma \\ 0 & I_k \end{pmatrix} \sim_{\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))} \begin{pmatrix} I_k & 0 \\ -\sigma & I_k \end{pmatrix},$$

where $\sim_{\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))}$ means that they are conjugate in $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$. Therefore if ρ is a representation of $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$, such that for all symmetric matrices $\sigma \in M_k\mathbb{Z}/(p^n\mathbb{Z})$, we have

$$\rho\left(\begin{pmatrix} I_k & \sigma \\ 0 & I_k \end{pmatrix}\right) = I,$$

then ρ is trivial.

Similar to $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$, we are looking for an abelian group in $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$, so that a big subgroup of $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$ acts on it. Take the following subgroup.

$$L_{\mathrm{Sp}} := \left\{ \begin{pmatrix} I_k & \sigma \\ 0 & I_k \end{pmatrix} : \sigma = \sigma^T \right\} \subseteq \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})).$$

Also define

$$H := \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \tilde{\alpha} \end{pmatrix} : \alpha \in \mathrm{GL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \right\} \subseteq \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})),$$

where $\tilde{\alpha} := (\alpha^T)^{-1}$. We remark that H acts by conjugation on L_{Sp}.

$$\begin{pmatrix} \alpha & 0 \\ 0 & \tilde{\alpha} \end{pmatrix} \begin{pmatrix} I_k & \sigma \\ 0 & I_k \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \tilde{\alpha} \end{pmatrix}^{-1} = \begin{pmatrix} I_k & \alpha\sigma\alpha^T \\ 0 & I_k \end{pmatrix}. \tag{3.3.8}$$

One can think of the action of H on L_{Sp}, as the action of $\mathrm{GL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ on quadratic forms. More precisely, for a symmetric matrix σ we have the following quadratic form

$$q_\sigma(x) := x\sigma x^T,$$

where x is a row matrix. Then the action of H on L_{Sp} would be the same as the action of α on q_σ. This interpretation will significantly simplify our calculations. Indeed, if for all row vectors we have $q_\sigma(x) = 0$ then we can conclude $\sigma = 0$, since σ is a symmetric matrix. Therefore to compute the action of H on L_{Sp}, we need to compute $q_\sigma(x\alpha)$. These computations will appear very soon. In the sequel we will use the following notations. For $1 \leq i, j \leq k$, E_{ij} will be denoted for the symmetric k by k matrix such that the (i, j) and (j, i) entries are 1 and all others are zero. We have

Lemma 3.3.5.

$$q_{E_{ij}} = \begin{cases} 2x_ix_j & i \neq j \\ x_i^2 & i = j \end{cases}. \tag{3.3.9}$$

Denote

$$G_{ij} := \begin{pmatrix} I_k & E_{ij} \\ 0 & I_k \end{pmatrix} \in L_{\mathrm{Sp}}.$$

We remark that if $i_1 \neq j_1$ and $i_2 \neq j_2$ then the quadratic form $2x_{i_1}x_{j_1}$ is equivalent to $2x_{i_2}x_{j_2}$. This in particular says that

$$G_{i_1j_1} \sim_H G_{i_2j_2},$$

where $\sim_H$ here means that those two matrices are conjugate under the action of H on L_{Sp}. Moreover since the quadratic form x_i^2 is equivalent to x_j^2 then

$$G_{ii} \sim_H G_{jj}.$$

Based on what we mentioned above, we have the following

Lemma 3.3.6. *Let ρ be a representation of $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$, so that*

$$\rho(G_{11}) = \rho(G_{12}) = I, \tag{3.3.10}$$

then ρ is a trivial representation.

Also for $a_i \in \mathbb{Z}/(p^n\mathbb{Z})$ and $t \in (\mathbb{Z}/(p^n\mathbb{Z}))^*$, define

$$\alpha = \alpha_{t,a_1,\ldots,a_{k-1}} := \begin{pmatrix} t & a_1 & a_2 & \cdots & a_{k-1} \\ 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathrm{GL}_k(\mathbb{Z}/(p^n\mathbb{Z})). \tag{3.3.11}$$

Hence

$$\overline{\alpha} := \begin{pmatrix} \alpha & 0 \\ 0 & \tilde{\alpha} \end{pmatrix} \in H.$$

For a row vector $x = (x_1, \cdots, x_k) \in (\mathbb{Z}/(p^n\mathbb{Z}))^k$, we have

$$x\alpha = (tx_1, a_1x_1 + x_2, a_2x_1 + x_3, \cdots, a_{k-1}x_1 + x_k). \tag{3.3.12}$$

So for $1 \le i, j \le k$,

$$q_{E_{ij}}(x\alpha) = x\left(\alpha E_{ij}\alpha^T\right)x^T. \tag{3.3.13}$$

From (3.3.12) and Lemma 3.3.5 we have

$$\begin{aligned} &q_{E_{11}}(x\alpha) = t^2x_1^2 \\ &q_{E_{1j}}(x\alpha) = 2ta_{j-1}x_1^2 + 2tx_1x_j && (2 \le j \le k) \\ &q_{E_{22}}(x\alpha) = a_1^2x_1^2 + 2a_1x_1x_2 + x_2^2 \\ &q_{E_{2j}}(x\alpha) = 2a_1a_{j-1}x_1^2 + 2a_1x_1x_j + 2a_{j-1}x_1x_2 + 2x_2x_j && (3 \le j \le k). \end{aligned} \tag{3.3.14}$$

From (3.3.8,3.3.13) and (3.3.14), we have the following identities which are crucial in our proof.

Lemma 3.3.7.

$$\begin{aligned}
\overline{\alpha}G_{11}\overline{\alpha}^{-1} &= \begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix} G_{11} \begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix}^{-1} = G_{11}^{t^2} \\
\overline{\alpha}G_{1j}\overline{\alpha}^{-1} &= \begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix} G_{1j} \begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix}^{-1} = G_{11}^{2ta_{j-1}}G_{1j}^{t} \qquad (2 \le j \le k) \\
\overline{\alpha}G_{22}\overline{\alpha}^{-1} &= \begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix} G_{22} \begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix}^{-1} = G_{11}^{{a_1}^2}G_{12}^{a_1}G_{22} \\
\overline{\alpha}G_{2j}\overline{\alpha}^{-1} &= \begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix} G_{2j} \begin{pmatrix}\alpha & 0\\ 0 & \tilde{\alpha}\end{pmatrix}^{-1} = G_{11}^{2a_1a_{j-1}}G_{1j}^{a_1}G_{12}^{a_{j-1}}G_{2j} \qquad (3 \le j \le k).
\end{aligned} \tag{3.3.15}$$

Now let

$$\rho : \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow \mathrm{GL}_d(\mathbb{C}),$$

be a non-trivial representation. Set $\mathcal{S}_{\mathrm{Sp}} := \rho(L_{\mathrm{Sp}})$. Proof of the following proposition is similar to Proposition 3.3.2.

Proposition 3.3.3. *Let r be one of the roots in the decomposition in Proposition 3.3.1 and let $h \in H$. For any $s = \rho(l) \in \mathcal{S}_{\mathrm{Sp}}$, define*

$$r_h(s) := r(\rho(hlh^{-1})).$$

Then r_h is also a root for $\mathcal{S}_{\mathrm{Sp}}$, and $V(r_h) = \rho(h^{-1})V(r)$.

Similar to Lemma 3.3.2 we have

Lemma 3.3.8. *When ρ is a faithful representation, then there exists a root r for $\mathcal{S}_{\mathrm{Sp}}$, such that $r(\rho(G_{11})) = \zeta$, where ζ is a primitive p^nth root of unity.*

We are ready to prove Theorem 1.1.2 for $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$.

Proof of Theorem 1.1.2 for $m_f\left(\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))\right)$: Let

$$\rho : \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow \mathrm{GL}_d(\mathbb{C}), \tag{3.3.16}$$

be a faithful representation. Pick a root r for $\mathcal{S}_{\mathrm{Sp}}$ such that $r(\rho(G_{11})) = \zeta_{p^n}^m$, where $\gcd(m,p) = 1$. This root exists by Lemma 3.3.8. For this root let $r(\rho(G_{1j})) = \zeta_{p^n}^{m_j}$

for $2 \leq j \leq k$. With the same notation as in Proposition 3.3.3 and (3.3.15) we have

$$\begin{aligned} r_{\overline{\alpha}}(\rho(G_{11})) &= \zeta_{p^n}^{t^2 m} \\ r_{\overline{\alpha}}(\rho(G_{1j})) &= \zeta_{p^n}^{2a_{j-1}tm+tm_j}, \quad (2 \leq j \leq k). \end{aligned} \tag{3.3.17}$$

Notice that the number of different squares in $(\mathbb{Z}/(p^n\mathbb{Z}))^*$ is $\varphi(p^n)/2$. So by varying $t, a_1, \ldots, a_{k-1}$, we will obtain at least

$$\frac{\varphi(p^n)p^{(k-1)n}}{2},$$

different roots. □

Proof of Theorem 1.1.2 for $m\,(\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})))$: Now let

$$\rho : \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow \mathrm{GL}_d(\mathbb{C}), \tag{3.3.18}$$

be a non-trivial representation. We mentioned earlier that when ρ is not a trivial representation then either $\rho(G_{11}) \neq I$ or $\rho(G_{12}) \neq I$. So we split the proof into two cases.

Case I: Let $\rho(G_{11}) \neq I$. Then we will show that there is a root r for $\mathcal{S}_{\mathrm{Sp}}$ such that

$$r(\rho(G_{11})) = \zeta_{p^n}^m,$$

where $m \neq 0$ in $\mathbb{Z}/(p^n\mathbb{Z})$. Suppose that there is no such root. Let denote all the roots of $\mathcal{S}_{\mathrm{Sp}}$ by $r_1, r_2, \cdots, r_t$, and assume that for any i, we have $r_i(\rho(G_{11})) = 1$. By Proposition 3.3.1 we have

$$\mathbb{C}^d = V(r_1) \oplus \cdots \oplus V(r_t).$$

For an arbitrary element $v \in \mathbb{C}^d$ write

$$v = v_1 + \cdots + v_t,$$

where $v_i \in V(r_i)$. Therefore

$$\begin{aligned} (\rho(G_{11}))v &= r_1(\rho(G_{11}))v_1 + \cdots + r_t(\rho(G_{11}))v_t \\ &= v_1 + \cdots + v_t \\ &= v. \end{aligned} \tag{3.3.19}$$

So $\rho(G_{11}) = I$ which is a contradiction. Hence there is a root r for $\mathcal{S}_{\mathrm{Sp}}$ such that $r(\rho(G_{11})) = \zeta_{p^n}^m$, where $m \neq 0$ in $\mathbb{Z}/(p^n\mathbb{Z})$. For this root let $r(\rho(G_{1i})) = \zeta_{p^n}^{m_i}$ for $2 \leq i \leq k$. So (3.3.15) implies that

$$\begin{aligned} r_{\overline{\alpha}}(\rho(G_{11})) &= \zeta_{p^n}^{t^2 m} \\ r_{\overline{\alpha}}(\rho(G_{1j})) &= \zeta_{p^n}^{2a_{j-1}tm + tm_j}, \quad (2 \leq j \leq k). \end{aligned} \tag{3.3.20}$$

So by varying $t, a_1, \ldots, a_{k-1}$, we will obtain at least $\frac{1}{2}(p-1)p^{(k-1)}$ different roots.

Case II: Let $\rho(G_{11}) = I$. In this case then we have $\rho(G_{12}) \neq I$. Pick a root r for $\mathcal{S}_{\mathrm{Sp}}$ such that $r(\rho(G_{12})) = \zeta_{p^n}^m$, where $m \neq 0$ in $\mathbb{Z}/(p^n\mathbb{Z})$. Assume that for this root $r(\rho(G_{2j})) = \zeta_{p^n}^{m_i}$ for $2 \leq j \leq k$. Then by (3.3.15) we have

$$r_{\overline{\alpha}}(\rho(G_{12})) = r(\rho(G_{11}^{2ta_1}))r(\rho(G_{12}^t)) = r(\rho(G_{12}^t)) = \zeta_{p^n}^{tm}.$$

Also

$$r_{\overline{\alpha}}(\rho(G_{22})) = r(\rho(G_{11}^{a_1^2}))r(\rho(G_{12}^{a_1}))r(\rho(G_{22})) = r(\rho(G_{12}^{a_1}))r(\rho(G_{22})) = \zeta_{p^n}^{a_1 m} r(\rho(G_{22})).$$

Moreover for $3 \leq j \leq k$ we have

$$\begin{aligned} r_{\overline{\alpha}}(\rho(G_{2j})) &= r(\rho(G_{11}^{2a_1 a_{j-1}}))r(\rho(G_{12}^{a_{j-1}}))r(\rho(G_{1j}^{a_1}))r(\rho(G_{2j})) \\ &= \zeta_{p^n}^{a_{j-1} m} r(\rho(G_{1j}^{a_1}))r(\rho(G_{2j})). \end{aligned} \tag{3.3.21}$$

So by varying $t, a_1, \ldots, a_{k-1}$, we will obtain at least $(p-1)p^{(k-1)}$ different roots. Therefore the minimal degree of a non-trivial representation is $\frac{1}{2}(p-1)p^{(k-1)}$. □

From these theorem we can prove Theorem 1.1.3.

Proof of Theorem 1.1.3. Using Theorem 1.1.2 along with Corollary 3.2.1, we can establish Theorem 1.1.3. □

3.4. Hilbert-Schmidt operators and product-free sets

Our aim in this section is to give a proof for Theorem 1.1.4 and Corollary 1.1.6. We use several standard facts from functional analysis, however we are not trying to give a complete proof of these facts. The reader can consult with [59] for details. Let G be a compact, second countable, Hausdorff topological group with

a normalized Haar measure μ. For $f_1, f_2 \in L^2(G)$, the convolution $f_1 * f_2 \in L^2(G)$ is defined by

$$(f_1 * f_2)(x) := \int_G f_1(xy^{-1}) f_2(y)\, d\mu(y).$$

For any given $f_1, f_2 \in L^2(G)$, from the Cauchy-Schwartz inequality we have

$$\|f_1 * f_2\|_2 \leq \|f_1\|_2 \|f_2\|_2. \tag{3.4.1}$$

Our objective in this section is to prove a stronger form of this inequality. For finite groups, Gowers [31] applies the singular value decomposition to the adjacency matrix attached to a finite bipartite graph, to obtain a stronger inequality. In order to generalize this to all compact groups, we will invoke Hilbert-Schmidt integral operator along with the singular value decomposition. Assume $f_1 \in L^2_0(G)$. To prove Theorem 1.1.4 note that by subtracting the constant $c = \int_G f_2\, d\mu$ from f_2 and noticing that $f_1 * c = 0$, without loss of generality, we can assume that $f_2 \in L^2_0(G)$. We consider the following kernel

$$K(x, y) := f_1(xy^{-1}).$$

Since G is a compact group, then we have $K(x, y) \in L^2(G \times G)$. For this kernel, we define the following integral operator

$$\begin{aligned} \Phi_K : L^2(G) &\longrightarrow L^2(G) \\ h &\longmapsto \Phi_K(h), \end{aligned} \tag{3.4.2}$$

where

$$\Phi_K(h)(x) := \int_G K(x, y) h(y) d\mu(y) \in L^2(G). \tag{3.4.3}$$

It is clear that $\Phi_K(h)(x) = (f_1 * h)(x)$. In order to prove Theorem 1.1.4, we need to show that

$$\|\Phi_{K_{|_{L^2_0(G)}}}\|^2_{op} \leq \frac{1}{m(G)} \|f_1\|_2^2. \tag{3.4.4}$$

We first remark that Φ_K is a compact operator. Indeed, for $K \in L^2(G \times G)$, consider the operator Φ_K, as it defined in (3.4.3), which is called an integral operator with the kernel K. We have,

Lemma 3.4.1. *The integral operator $\Phi_K : L^2(G) \longrightarrow L^2(G)$ is a Hilbert-Schmidt operator and hence is compact. The norm of Φ_K is given by,*

$$\|\Phi_K\|_{HS} = \|K\|_{L^2(G\times G)}. \tag{3.4.5}$$

One can easily see that

$$\Phi_K^*(h)(y) = \int_G \overline{K(x,y)}h(x)d\mu(x).$$

Since G is not commutative, Φ_K is not necessarily a self adjoint operator.

Lemma 3.4.2 (singular value decomposition)**.** *Let $\mathcal{H}$ be a separable Hilbert space and $T \in B(\mathcal{H})$ be a compact operator (not necessary self adjoint). Then there exists two orthonormal sets $\{e_n\}$ and $\{e'_n\}$ in $\mathcal{H}$ such that*

$$T(e_i) = \lambda_i e'_i, \quad T^*(e'_i) = \lambda_i e_i, \qquad i = 1, 2, \dots$$

where

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq 0,$$

and for any $x \in \mathcal{H}$

$$T(x) = \sum_{i\geq 1} \lambda_i \langle x, e_i\rangle e'_i. \tag{3.4.6}$$

Moreover, by (3.4.6), we have $\|T\|_{op} = \lambda_1$.

Using these lemmas we will now prove:

Proof of Theorem 1.1.4: Consider the restriction operator

$$\Phi_1 := \Phi_{K_{|_{L^2_0(G)}}} : L^2_0(G) \longrightarrow L^2_0(G),$$

defined by (3.4.2) and apply the singular value decomposition to obtain orthonormal bases $\{e_n\}$ and $\{e'_n\}$ in $L^2_0(G)$ such that

$$\Phi_1(e_i) = \lambda_i e'_i,$$

where

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq 0.$$

For $\Phi_1^*\Phi_1$, which is a self-adjoint Hilbert-Schmidt operator, let V_1 be the eigenspace of $\Phi_1^*\Phi_1$ correspondence to λ_1^2. Since $\Phi_1^*\Phi_1$ is a compact operator then

$$\dim V_1 < \infty.$$

Let us remark that from the singular value decomposition we have

$$\|\Phi_1\|_{op} = \|\Phi_{K_{|L^2_0(G)}}\|_{op} = \lambda_1.$$

So we deduce

$$\begin{aligned}\|\Phi_1\|^2_{op} \dim V_1 = \lambda_1^2 \dim(V_1) &\leq \sum_{i=1}^{\infty} \lambda_i^2 \\ &\leq \|\Phi_K^* \Phi_K\|^2_{HS} \\ &\leq \|\Phi_K\|^2_{HS} = \|K\|^2_{L^2(G\times G)} \\ &= \int_G \int_G |f_1(xy^{-1})|^2 d\mu(y) d\mu(x) = \|f_1\|_2^2.\end{aligned}$$

We show that $\dim V_1 \geq m(G)$, and this would finish the proof. We will construct an action of G on V_1 by defining for every $h \in V_1$ and $g \in G$

$$T_g h(x) := h(xg).$$

We need to verify that,

$$T_g(\Phi_1^* \Phi_1(h)) = \Phi_1^* \Phi_1(T_g h). \tag{3.4.7}$$

Since G is compact and hence unimodular we have,

$$\begin{aligned}\Phi_1(T_g h)(x) &= \int_G f_1(xy^{-1}) h(yg) d\mu(y) \\ &= \int_G f_1(x(zg^{-1})^{-1}) h(z) d\mu(z) \\ &= \int_G f_1(xgz^{-1}) h(z) d\mu(z) \\ &= T_g(\Phi_1(h))(x).\end{aligned}$$

By acting Φ_1^* from the left we obtain (3.4.7). Since V_1 is a subspace of $L^2_0(G)$, it does not contain the constant function, and hence this linear action is non-trivial. This induces a non-trivial representation of G in the unitary group $U(V_1)$, thus $\dim V_1 \geq m(G)$. □

Proof of Corollary 1.1.6. Apply the inequality to $f_1 = 1_A$ and $f_2 = 1_B - \mu(B)$. □

Now we can proof Theorems 1.1.5.

Proof of Theorem 1.1.5: Let

$$S := \{y \in G : (1_A * 1_B)(y) = 0\}.$$

Thus

$$\begin{aligned}\mu(S)^{1/2}\mu(A)\mu(B) &= \left(\int_S |(1_A * 1_B)(y) - \mu(A)\mu(B)|^2 \, d\mu(y)\right)^{1/2} \\ &\leq \left(\int_G |(1_A * 1_B)(y) - \mu(A)\mu(B)|^2 \, d\mu(y)\right)^{1/2} \\ &= \|1_A * 1_B - \mu(A)\mu(B)\|_2.\end{aligned}$$

But via Corollary 1.1.6 we can deduce that

$$\mu(S)^{1/2}\mu(A)\mu(B) \leq \sqrt{\frac{\mu(A)\mu(B)}{m(G)}},$$

therefore

$$\mu(S) \leq \frac{1}{m(G)\mu(A)\mu(B)}.$$

This implies that $\mu(C \setminus S) > 0$, since otherwise we get

$$\mu(C)\mu(A)\mu(B) \leq \frac{1}{m(G)},$$

which is a contradiction. Hence there exists a set of positive measure of $y \in C$ so that $1_A * 1_B(y) \neq 0$, which means that $AB \cap C$ has positive measure.

For the second statement let define

$$\Sigma := \{(a, b, c) \in A \times B \times C : ab = c\}.$$

Notice that

$$\mu(\Sigma) = \langle 1_A * 1_B, 1_C\rangle = \langle 1_A * (1_B - \mu(B)), 1_C\rangle + \mu(A)\mu(B)\mu(C). \tag{3.4.8}$$

By Cauchy-Schwartz inequality we have

$$\begin{aligned}\langle 1_A * (1_B - \mu(B)), 1_C\rangle^2 &\leq \|1_A * (1_B - \mu(B))\|_2^2 \|1_C\|_2^2 \\ &= \|1_A * 1_B - \mu(A)\mu(B)\|_2^2 \mu(C) \\ &\leq \frac{\mu(A)\mu(B)\mu(C)}{m(G)}.\end{aligned}$$

Thus if

$$\frac{\mu(A)\mu(B)\mu(C)}{m(G)} \leq \eta^2\mu(A)^2\mu(B)^2\mu(C)^2,$$

which is fulfilled by our assumption, we deduce that

$$|\langle 1_A * (1_B - \mu(B)), 1_C \rangle| \leq \eta\mu(A)\mu(B)\mu(C),$$

thus

$$\mu(\Sigma) \geq \mu(A)\mu(B)\mu(C) - \eta\mu(A)\mu(B)\mu(C) = (1-\eta)\mu(A)\mu(B)\mu(C)$$

□

Remark 3.4.1. *One can also establish another inequality. For $f_1 = 1_A$ and $f_2 = 1_B - \mu(B)$, notice that*

$$\|f_2\|_2^2 = \mu(B)(1-\mu(B)).$$

Thus by Theorem 1.1.4 we have

$$\mu(G - AB)^{1/2}\mu(A)\mu(B) \leq \sqrt{\frac{1}{m(G)}}\mu(A)^{1/2}\left(\mu(B)(1-\mu(B))\right)^{1/2},$$

therefore

$$1 - \frac{1-\mu(B)}{m(G)\mu(A)\mu(B)} \leq \mu(AB).$$

3.5. Automorphisms of regular trees

The goal of this section is to obtain lower and upper bounds on the product-free measure of the group of positive automorphisms of a rooted regular tree. Let us recall the definition of the group of A_{k+1}^+ that appeared in the statement of Theorem 1.1.6.

Definition 3.5.1. *An automorphism $x \in A_{k+1}$ is called positive if $\sigma_j(x)$ is an even permutation for all $j \geq 1$. We will denote the group of all positive automorphisms by A_{k+1}^+.*

First, notice that A_{k+1}^+ is a closed subgroup of A_{k+1} and hence a profinite group. In fact, the group can also be represented by

$$A_{k+1}^+ = \varprojlim A_{k+1}^+ / \mathcal{C}_j^+, \tag{3.5.1}$$

where

$$\mathcal{C}_j^+ := \left\{ x \in A_{k+1}^+ : \sigma_j(x) = \mathrm{id} \right\}.$$

In what follows, let $\mathrm{Alt}_{k+1} \leq \Sigma_{k+1}$ denote the alternating group on $k+1$ symbols.

To prove Theorem 1.1.6, we first prove a lemma. Let us define the following set.

$$\mathcal{L} := \left\{(v_1, \ldots, v_{k+1}) \in \mathbb{F}_2^{k+1} : v_1 + \cdots + v_{k+1} = 0\right\}. \tag{3.5.2}$$

We have

Lemma 3.5.1. *Let $k \geq 6$ be an integer and let $\mathcal{L}$ be the group defined in (3.5.2). Moreover assume that*

$$\rho : \mathcal{L} \longrightarrow \mathrm{GL}_d(\mathbb{C}),$$

is a non-trivial representation of $\mathcal{L}$, such that

$$\rho(v_1, \ldots, v_{k+1}) = \rho(v_{i_1}, \ldots, v_{i_{k+1}}),$$

for any even permutation $(i_1, \ldots, i_{k+1})$ of the set $\{1, \ldots, k+1\}$. Then $d \geq k - \epsilon$ where $\epsilon = 0$ if k is even and $\epsilon = 1$ when k is odd.

Proof. We will show that ρ is faithful when $k+1$ is odd and $|\ker(\rho)| \leq 2$ when $k+1$ is even. For $0 \neq v \in \mathcal{L}$, define

$$I(v) := \{1 \leq i \leq k+1 : v_i = 1\}.$$

First we show that if for some $0 \neq v \in \ker(\rho)$ we have $|I(v)| = 2$, then the representation ρ is a trivial. To show this note that for every $w \in \mathcal{L}$ with $|I(w)| = 2$, we can find $\sigma \in \mathrm{Alt}_{k+1}$ such that $\sigma(v) = w$. Therefore by the property of ρ we can deduce that $\rho(w) = 0$. This implies that $\ker(\rho) = \mathcal{L}$, hence ρ should be a trivial representation.

Now assume that ρ is not a faithful representation and suppose $0 \neq v \in \ker(\rho)$ is chosen such that $|I(v)|$ is minimal. Since ρ is non-trivial then $|I(v)| = 2j > 2$. Without loss of generality assume that $v = (1, 1, \ldots, 1, 0, \ldots, 0)$ where the first $2j$ entries are equal to 1 and the rest are zero.

If $k+1$ is odd then we can consider the 3-cycle $\sigma = (1, 2, 2j+1) \in \mathrm{Alt}_{k+1}$. Now it is easy to see that $\sigma \cdot v - v$ has 1 in only two positions, hence $\sigma(v) - v \in \ker(\rho)$, with $|I(\sigma(v) - v)| = 2$. But this, as was shown above, implies that ρ is a trivial representation. So for odd $k+1$ we deduce that ρ is a faithful representation.

A similar argument can be made when $k+1$ is even and $|\ker(\rho)| > 2$. This show that ρ is faithful when $k+1$ is odd and $|\ker(\rho)| \leq 2$ when $k+1$ is even.

In either case $\rho(\mathcal{L})$ is isomorphic to $\mathbb{F}_2^{k-\epsilon}$. The set $\rho(\mathcal{L})$ can be simultaneously diagonalized with diagonal entries being ± 1. Now it is clear that $d \geq k-\epsilon$, where $\epsilon = 0$ if k is even and $\epsilon = 1$ when k is odd. $\square$

We will need the following fact from the representation theory of finite groups:

Theorem 3.5.1 (See [29] Exercise 5.5)**.** *For $k \geq 6$, the minimum dimension of non-trivial representations of* Alt_k *is $k-1$.*

From these lemmas, we will prove Theorem 1.1.6.

Proof of Theorem 1.1.6: For the lower bound, note that

$$\sigma_1 : A_{k+1}^+ \longrightarrow \mathrm{Alt}_{k+1},$$

is surjective. Let H be the subgroup of Alt_{k+1} consisting of those permutations that fix $k+1$. H is clearly isomorphic to Alt_k. Now, apply Lemma 1.1.3 to the subgroup $\sigma_1^{-1}(H)$ to obtain an open subgroup of index $k+1$ in A_{k+1}^+. This establishes the lower bound.

For the upper bound, we need to show that for the group A_{k+1}^+, the minimal degree of all non-trivial continuous representations is $k-1$. By (3.5.1) then we should prove that $F_j := A_{k+1}^+/\mathcal{C}_j^+$ does not have any non-trivial representation of dimension less than $k-1$.

For $j=1$, we will get $F_1 = \mathrm{Alt}_{k+1}$, and then by Theorem 3.5.1, for $k \geq 5$, all the non-trivial representations have dimension greater than or equal to k. For the sake of clarity and notational simplicity, we will present the argument for $j=2$. The argument readily extends to an arbitrary $j \geq 2$. Suppose ρ to be a non-trivial representation of F_2. It is easy to see that

$$F_2 \cong \mathrm{Alt}_{k+1} \ltimes \underbrace{(\Sigma_k \times \cdots \times \Sigma_k)^+}_{k+1},$$

where

$$\underbrace{(\Sigma_k \times \cdots \times \Sigma_k)^+}_{k+1} := \left\{ (\sigma_1, \ldots, \sigma_{k+1}) \in \underbrace{(\Sigma_k \times \cdots \times \Sigma_k)}_{k+1} : \prod_{i=1}^{k+1} \mathrm{sgn}(\sigma_i) = 1 \right\}.$$

and Alt_{k+1} acts by permuting the factors.

If the restriction of ρ to Alt_{k+1} is non-trivial then we are done by Theorem 3.5.1. Suppose that the restriction of ρ to Alt_{k+1} is trivial. Clearly

$$\underbrace{\mathrm{Alt}_k \times \cdots \times \mathrm{Alt}_k}_{k+1} \trianglelefteq \underbrace{(\Sigma_k \times \cdots \times \Sigma_k)^+}_{k+1},$$

Again, we can assume that the restriction of ρ to each one of the factors is trivial, since otherwise we can apply Theorem 3.5.1 to obtain the bound $k-1$.

Therefore let assume that ρ is trivial over $\underbrace{\mathrm{Alt}_k \times \cdots \times \mathrm{Alt}_k}_{k+1}$. So ρ factors through the quotient

$$\overbrace{(\Sigma_k \times \Sigma_k \times \cdots \times \Sigma_k)^+}^{k+1} / \underbrace{(\mathrm{Alt}_k \times \mathrm{Alt}_k \times \cdots \times \mathrm{Alt}_k)}_{k+1}.$$

For $(\sigma_1, \sigma_2, \ldots, \sigma_k, \sigma_{k+1}) \in \overbrace{(\Sigma_k \times \cdots \times \Sigma_k)^+}^{k+1}$, we recall that since the restriction of ρ to Alt_{k+1} is trivial we have

$$\rho(\sigma_1, \sigma_2, \ldots, \sigma_k, \sigma_{k+1}) = \rho(\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}, \sigma_{i_{k+1}}),$$

for any even permutation $(i_1, i_2, \ldots, i_k, i_{k+1})$ of the set $\{1, \ldots, k, k+1\}$. Notice that

$$\frac{\overbrace{(\Sigma_k \times \cdots \times \Sigma_k)^+}^{k+1}}{\underbrace{\mathrm{Alt}_k \times \cdots \times \mathrm{Alt}_k}_{k+1}} \cong \mathcal{L}, \tag{3.5.3}$$

where $\mathcal{L}$ was defined in (3.5.2). Therefore we obtain a non-trivial representation of $\mathcal{L}$ that satisfies in the conditions of Lemma 3.5.1, so we have

$$\dim \rho \geq k - \epsilon \geq k - 1.$$

For $j \geq 3$, the group F_j is isomorphic to an iterated semi-direct product of alternating groups as above and a similar argument establishes the lower bound on the degree of nontrivial representation. Applying Theorem 1.1.5 completes the proof. $\square$

3.6. Product-free measure of the ring of p-adic integers

It is possible to compute the exact value of product-free measure for connected abelian Lie groups. Let $\mathbb{T}^k$ denote the k-dimensional torus. Then,

Theorem 3.6.1. *For any $k \geq 1$ we have* $\mathrm{pf}(\mathbb{T}^k) = 1/3$.

Proof: The proof is similar to the proof given in [47] where only open sets A are considered. We will show that in fact there is no need to restrict to consider just the open sets. First we show that $\mathrm{pf}(\mathbb{T}^k) \leq 1/3$. Suppose that A is a product-free subset with $\mu(A) = 1/3 + \beta$ for some $\beta > 0$. We will show that there is an open product-free set U such that

$$\mu(U) \geq 1/3 + \beta/2.$$

We will write this part of the proof, which is valid for any compact group, using the multiplicative notation. First choose a compact set $K \subseteq A$ with $\mu(K) \geq 1/3 + \beta/2$. Clearly K is a product-free set and since K is compact $d(K, K^2) = \epsilon > 0$, where we use d as shorthand for $d_{\mathbb{T}^k}$. Let U_δ be the δ-neighborhood of K, i.e., the set of points $u \in \mathbb{T}^k$ such that $d(u, k) < \delta$ for some $k \in K$. We will show that for δ small enough U_δ will be a product-free set as well. Let $u_1, u_2, u_3 \in U_\delta$. So there exist $k_1, k_2, k_3 \in K$ such that $d(u_i, k_i) < \delta$ for $i = 1, 2, 3$. Using the invariance of d we have

$$\begin{aligned} d(u_2u_3, k_2k_3) &\leq d(u_2u_3, k_2u_3) + d(k_2u_3, k_2k_3) \\ &= d(u_2, k_2) + d(u_3, k_3) < 2\delta. \end{aligned}$$

From here we have

$$d(u_1, u_2u_3) \geq d(k_1, k_2k_3) - d(k_1, u_1) - d(k_2k_3, u_2u_3) \geq \epsilon - 3\delta.$$

So if we choose $\delta = \epsilon/4$ we will have $d(u_1, u_2u_3) > \epsilon/4$ which shows that

$$U_{\epsilon/4} \cap U_{\epsilon/4}^2 = \emptyset.$$

Notice that $K \subseteq U_{\epsilon/4}$, so

$$\mu(U_{\epsilon/4}) \geq 1/3 + \beta/2.$$

$U := U_{\epsilon/4}$ is the open set that we were looking for. Now let us assume that A is an open product-free subset of

$$\mathbb{T}^k = \mathbb{T}^1 \times \cdots \times \mathbb{T}^1,$$

with $\mu(A) = 1/3 + \beta$. Again, by possibly exchanging β with $\beta/2$, we can assume that A is a finite disjoint unions of boxes of the form: $I_1 \times I_2 \cdots \times I_k$ where I_j is an interval in the j-th copy of $\mathbb{T}^1$. Choose a large prime number p. Set $\zeta = \exp(2\pi i/p)$ and let

$$G_p \cong \mathbb{Z}/(p\mathbb{Z}) \times \cdots \times \mathbb{Z}/(p\mathbb{Z}),$$

be the elementary abelian p-group in $\mathbb{T}^k$ consisting of all elements of order p. Note that G_p contains p^k elements. Consider a box $I := I_1 \times I_2 \cdots \times I_k$ and let h_j be the length of I_j. It is easy to see that

$$|G_p \cap I| \geq (ph_1 - 1) \cdots (ph_k - 1) = p^k \mu(I) + O(p^{k-1}).$$

By adding up over all boxes we will get

$$|G_p \cap A| \geq p^k \mu(A) + O(p^{k-1}).$$

Since G_p is a finite p-group, by Green-Ruzsa theorem (see Theorem 3.6.2) we have $\mathrm{pf}(G_p) \leq 1/3 + 1/(3p)$. Since A is product-free we must have

$$(1/3 + \beta/2) + O(1/p) \leq 1/3 + 1/(3p),$$

which as $p \to \infty$ gives a contradiction. Hence $\mathrm{pf}(\mathbb{T}^k) \leq 1/3$. Set

$$B := \{e^{2\pi i\theta} : 1/3 \leq \theta \leq 2/3\},$$

then notice that

$$B \times \mathbb{T} \times \cdots \times \mathbb{T},$$

is a product-free set in $\mathbb{T}^k$ of density $1/3$. So we have $\mathrm{pf}(\mathbb{T}^k) = 1/3$. □

For finite abelian groups, the exact value of $\mathrm{pf}(G)$ is explicitly given by:

Theorem 3.6.2. *(Green-Ruzsa, cf. [39]) Suppose G is a finite abelian group of size n.*

(1) If n is divisible by a prime $p \equiv 2 \pmod 3$, then $\mathrm{pf}(G) = 1/3 + 1/(3p)$ where p is the smallest such p.

(2) Otherwise, if $3|n$, *then* $\mathrm{pf}(G) = 1/3$.

(3) Otherwise, $\mathrm{pf}(G) = 1/3 - 1/(3m)$ *where* m *is the largest order of any element of* G.

Using a result of Green and Ruzsa [39] we will also compute the product-free measure of the ring of p-adic integers.

Theorem 3.6.3. *The product-free measure of the additive groups of* p*-adic integers* $\mathbb{Z}_p$ *and power series* $\mathbb{F}_p[[t]]$ *are respectively given by*

$$\mathrm{pf}(\mathbb{Z}_p) = \begin{cases} 1/3 + 1/(3p) & \text{if } p \equiv 2 \pmod 3 \\ 1/3 & \text{otherwise} \end{cases}.$$

$$\mathrm{pf}(\mathbb{F}_p[[t]]) = \begin{cases} 1/3 + 1/(3p) & \text{if } p \equiv 2 \pmod 3 \\ 1/3 & \text{if } p = 3 \\ 1/3 - 1/(3p) & \text{if } p \equiv 1 \pmod 3 \end{cases}. \tag{3.6.1}$$

Proof of Theorem 3.6.3: First we will give the proof for $\mathbb{Z}_p$. Let

$$\phi_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/(p^n\mathbb{Z}),$$

be reduction modulo p^n for $n \geq 1$. For $p \equiv 2 \pmod 3$, it is easy to verify that, if $S \subseteq \mathbb{Z}/(p\mathbb{Z})$ is a product-free set of density $1/3 + 1/(3p)$, provided by Green-Ruzsa theorem, then $\phi_1^{-1}(S) \subseteq \mathbb{Z}_p$ will be a set of the same density. Hence for $p \equiv 2 \pmod 3$ we have

$$\mathrm{pf}(\mathbb{Z}_p) \geq 1/3 + 1/(3p), \qquad p \equiv 2 \pmod 3.$$

For $p \equiv 1 \pmod 3$, consider the subset of $\mathbb{Z}/(p^n\mathbb{Z})$:

$$S_n = \left\{ \left\lfloor \frac{p^n+1}{3} \right\rfloor, \ldots, 2\left\lfloor \frac{p^n+1}{3} \right\rfloor - 1 \right\} \subseteq \mathbb{Z}/(p^n\mathbb{Z}).$$

By Lemma 1.1.3 we have

$$\mathrm{pf}(\mathbb{Z}_p) \geq \sup_{n\geq 1} \frac{|S_n|}{p^n} = \sup_{n\geq 1} \frac{\left\lfloor \frac{p^n+1}{3} \right\rfloor - 1}{p^n} = \frac{1}{3}.$$

Hence we have

$$\mathrm{pf}(\mathbb{Z}_p) \geq 1/3, \qquad p \equiv 1 \pmod 3.$$

For $p = 3$, by Green-Ruzsa theorem, we have a product-free set of density $1/3$, so

$$\mathrm{pf}(\mathbb{Z}_3) \geq 1/3.$$

On the other hand, suppose A is a measurable product-free subset of $\mathbb{Z}_p$ (or $\mathbb{F}_p[[t]]$) with $\mu(A)$ larger than the function given on the right side of (3.6.1), that we denote it by $f(p)$. Choose a compact subset $A_1 \subseteq A$ such that $\mu(A_1) = f(p)(1+\epsilon)$ for some $\epsilon > 0$. By (3.1.1) we have

$$\lim_{n\to\infty} \frac{\phi(A_1)}{p^n} = f(p)(1+\epsilon).$$

So there exists an integer m such that for all $n \geq m$, the set $\phi_n(A_1) \subseteq \mathbb{Z}/(p^n\mathbb{Z})$ has density larger that $f(p)(1+\epsilon/2)$. By the theorem of Green and Ruzsa, this implies that there exist $x_n, y_n, z_n \in A_1$ such that $\phi_n(x_n + y_n - z_n) = 0$. Since A_1 is compact, after passing to a subsequence, there exist $x, y, z \in A_1$ such that $x_n \to x, y_n \to y, z_n \to z$. Now, since $x_n + y_n - z_n \to 0$, we have $x + y = z$, which is a contradiction.

The proof for $\mathbb{F}_p[[t]]$ is similar. The only difference is that all of the finite quotients of $\mathbb{F}_p[[t]]$ are elementary p-groups. Hence when $p \equiv 1 \pmod 3$, it is the third condition in Green-Ruza theorem that applies. □

Acknowledgments:

We have benefited from some notes on Terence Tao's weblog as well as Emmanuel Breuillard's lecture notes on "Théorie des groupes approximatifs". We wish to thank them for providing these notes online. For many fruitful discussions, we wish to thank Andrew Granville. The first author was supported in part by Faculté des Études Supérieures et Postdoctorales de l'Université de Montréal. The second author would like to thank CRM in Montreal for the visit during which part of this joint work was done.

Part II: Algebraic number theory and monogenic fields

Chapter 4

PRELIMINARIES FOR CHAPTER 5

4.1. Average degree of splitting fields

In this section we will give an example, that illustrates how the Chebotarev density theorem appears in some arithmetic questions.

For $\sigma \in S_n$, let $\mathrm{ord}(\sigma)$ be the order of σ. The distribution of $\mathrm{ord}(\sigma)$ was studied by Erdös and Turán in a beautiful series of papers on "statistical group theory" [22, 23, 24, 25, 27, 26, 28]. Define the average order of elements of S_n to be

$$\mu_n := \frac{1}{n!} \sum_{\sigma \in S_n} \mathrm{ord}(\sigma). \tag{4.1.1}$$

Solving a conjecture of Erdös and Turán, Goh and Schmutz [30] proved that

$$\log(\mu_n) \sim C\sqrt{\frac{n}{\log n}} \qquad n \longrightarrow \infty, \tag{4.1.2}$$

where

$$C = 2\sqrt{\left(2\int_0^\infty \log\log\left(\frac{e}{1-e^t}\right) dt\right)}. \tag{4.1.3}$$

Stong in his paper [67] strengthens this theorem by providing an error term. He proved

$$\log(\mu_n) = C\sqrt{\frac{n}{\log n}} + O\left(\frac{\sqrt{n}\log\log n}{\log n}\right). \tag{4.1.4}$$

In this section we consider the following problem. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n with discriminant D. For a prime number p, coprime to D, let us denote $X_p(f)$ to be the degree of the splitting field of $f(x) \pmod p$.

We are interested in the following quantity

$$\mu_n(f) := \lim_{t\to\infty} \left(\frac{1}{\pi(t)} \sum_{\substack{p\leq t \\ \gcd(p,D)=1}} X_p(f) \right). \tag{4.1.5}$$

A motivation to study this quantity is a nice result of Dixon and Panario [20], where they fix a prime p and consider the distribution of the degree of the splitting field of certain family of polynomials in $\mathbb{F}_p[x]$. Let the Galois group of $f(x)$ be the symmetric group S_n. We will show that the degree of the splitting field of $f(x) \pmod p$ is the same as the order the Frobenius element in the Galois group. Then by using Stong's theorem and Chebotarev density theorem we will prove Theorem 1.2.3.

4.1.1. Dedekind's lemma

In this section we recall a fundamental lemma due to Dedekind. This lemma translates arithmetic properties of a polynomial into group theoretical properties of the Frobenius element in the Galois group of a polynomial.

Let $f(x)$ be a polynomial with coefficients in a field F. The discriminant of $f(x)$ is defined to be $D := D_f = \Delta_f^2$ where

$$\Delta_f = \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j),$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$ in some splitting field. The discriminant essentially tells us when we have a repeated root.

Now let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n with integer coefficients and let $E = E_f = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be its splitting field over $\mathbb{Q}$. Let $G_f = \mathrm{Gal}(E/\mathbb{Q})$ be the Galois group of $f(x)$. Suppose that p is a prime such that p does not divide the discriminant D of $f(x)$, in particular, we suppose that the roots of f are simple. Let $\bar{f}(x)$ be the reduction of $f(x)$ modulo p. Then the roots of $\bar{f}(x)$ are also simple. Let $A = A_f = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ and let $\mathfrak{p}$ be a prime ideal of A such that $\mathfrak{p} \cap \mathbb{Z} = (p)$. Such an ideal exists since A is integral over $\mathbb{Z}$.

For such a prime we can define a unique element in the Galois group of $f(x)$, which is called the Frobenius automorphism.

Lemma 4.1.1 (Dedekind)**.** *Let $f(x)$ be a monic irreducible polynomial with discriminant D, and assume p does not divide D, where p is a prime. Let E be the splitting field of $f(x)$. Then there exists an element $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(E/\mathbb{Q})$, unique up to conjugation, such that*

$$\sigma_{\mathfrak{p}}(a) \equiv a^p \mod \mathfrak{p},$$

for all $a \in A$. Moreover if $\bar{f}(x) = \phi_1(x) \cdots \phi_g(x)$, with $\phi_i(x)$ irreducible over $\mathbb{F}_p$ of degree n_i, then $\sigma_{\mathfrak{p}}$, when viewed as a permutation of the roots of $f(x)$, has a cycle decomposition $\sigma_1 \cdots \sigma_g$ with σ_i of length n_i.

We will follow closely John Labute's explanation of Tate's proof.

Proof (Tate): The field $E_{\bar{f}} = A/\mathfrak{p} = \mathbb{F}_p[\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n]$ is a splitting field for $\bar{f}(x)$, where $\bar{\alpha}$ is the residue class of α modulo $\mathfrak{p}$. The group $G_{\bar{f}} = \mathrm{Gal}(E_{\bar{f}}/\mathbb{F}_p)$ is cyclic generated by the Frob_p. Set

$$D_{\mathfrak{p}} = \{\sigma \in G_f | \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

This is a subgroup of G_f called the decomposition group at $\mathfrak{p}$. Every automorphism $\sigma \in D_{\mathfrak{p}}$ induces an automorphism $\bar{\sigma} \in G_{\bar{f}}$, given by $\bar{\sigma}(\bar{\alpha}) = \overline{\sigma(\alpha)}$. The homomorphism

$$\begin{aligned} \varphi : D_{\mathfrak{p}} &\longrightarrow G_{\bar{f}} \\ \sigma &\longmapsto \bar{\sigma}, \end{aligned} \tag{4.1.6}$$

is injective. We now show that it is surjective by showing that the fixed field of $\varphi(D_{\mathfrak{p}})$ has $\mathbb{F}_p$ as its fixed field.

Let $a \in A$. Then, by the Chinese Remainder Theorem, there is an element $\alpha \in A$ such that $\alpha \equiv a \pmod{\mathfrak{p}}$ and $\alpha \equiv 0 \pmod{\sigma^{-1}(\mathfrak{p})}$ for all $\sigma \in G_f \setminus D_{\mathfrak{p}}$. Then

$$g(x) = \prod_{\sigma \in G_f} (x - \sigma(\alpha)) \in \mathbb{Z}[x].$$

Notice that

$$\bar{g}(x) = x^m \prod_{\sigma \in D_{\mathfrak{p}}} (x - \bar{\sigma}(\bar{a})) \in \mathbb{F}_p[x],$$

for some m. It follows that the conjugates of $\bar{a}$ are all of the form $\bar{\sigma}(\bar{a})$ which implies that the fixed field of $\varphi(D_{\mathfrak{p}})$ is $\mathbb{F}_p$.

Therefore there is a unique element in G_f, denoted by $\sigma_{\mathfrak{p}}$, such that

$$\sigma_{\mathfrak{p}}(a) \equiv a^p \mod \mathfrak{p}.$$

□

This lemma will play an important role in our study of the distribution of the degree of the splitting field of $\bar{f}(x)$. The following lemma is easy to prove.

Lemma 4.1.2. *For $f(x) \in \mathbb{Z}[x]$, let $\bar{f}(x) = \phi_1(x) \cdots \phi_g(x)$, with $\phi_i(x)$ irreducible over $\mathbb{F}_p$ of degree n_i, then*

$$X_p(f) = \operatorname{lcm}(n_1, \dots, n_g). \tag{4.1.7}$$

By Lemma 4.1.1, the order of $\sigma_{\mathfrak{p}}$ is also

$$\operatorname{lcm}(n_1, \dots, n_g).$$

Therefore we have the following:

Corollary 4.1.1. *We have the following identity,*

$$X_p(f) = \operatorname{ord}(\sigma_{\mathfrak{p}}). \tag{4.1.8}$$

Now we can invoke Chebotarev's density theorem. If $f(x) \pmod p$ splits into distinct monic irreducible factors, with n_1 linear factors, n_2 quadratic factors, etc, then we say that $\lambda = (n_1, n_2, \dots)$ is the splitting type of $f(x)$ modulo p. For each splitting type λ we have

$$\sum_j j n_j = n. \tag{4.1.9}$$

Indeed λ is a partition of n, denoted by $\lambda \vdash n$. We have the same phenomenon in the symmetric group. The conjugacy classes of S_n correspond to the cycle structures of permutations; that is, two elements of S_n are conjugate in S_n if and only if they consist of the same number of disjoint cycles of the same length. For any permutation $\sigma \in S_n$, we know that we can write σ as a product of disjoint cycles. If σ splits into n_1 cycle of length one, n_2 transposition, etc. Then we say that $\lambda = (n_1, n_2, \dots)$ is the splitting type of σ. Therefore the conjugacy classes in S_n correspond to the partitions of n. For any partition $\lambda = (n_1, n_2, n_3, \dots, n_g)$,

i.e, $\sum_j jn_j = n$, the size of the conjugacy class of the permutation corresponding to λ is

$$\frac{n!}{1^{n_1}n_1!2^{n_2}n_2!\dots g^{n_g}n_g!} = n!\delta(\lambda) \tag{4.1.10}$$

where here $\delta(\lambda) = (1^{n_1}n_1!2^{n_2}n_2!\dots g^{n_g}n_g!)^{-1}$. By Dedekind's Lemma 4.1.1, we can say that the splitting type of $f(x) \pmod p$ is the same as the splitting type of $\sigma_{\mathfrak{p}}$. Therefore we have the following lemma

Lemma 4.1.3. *Assume that Galois group of $f(x)$ is the symmetric group S_n, where n is the degree of $f(x)$. For any partition $\lambda = (n_1, n_2, n_3, \dots, n_g)$ of n, by Chebotarev's density theorem we have*

$$\frac{\#\{p \le t : f(x) \pmod p \text{ has type } \lambda\}}{\pi(t)} \sim \delta(\lambda). \tag{4.1.11}$$

For a partition $\lambda = (n_1, n_2, \dots, n_g)$ of n, notice that the order of the element of S_n corresponding to λ is $\mathrm{lcm}(n_1, n_2, \dots, n_g)$, which will be denoted by $\mathrm{lcm}(\lambda)$. By Lemma 4.1.3 and Corollary 4.1.1 we have the following

Lemma 4.1.4.

$$\mu_n(f) = \sum_{\lambda \vdash n} \delta(\lambda)\mathrm{lcm}(\lambda). \tag{4.1.12}$$

Therefore we have

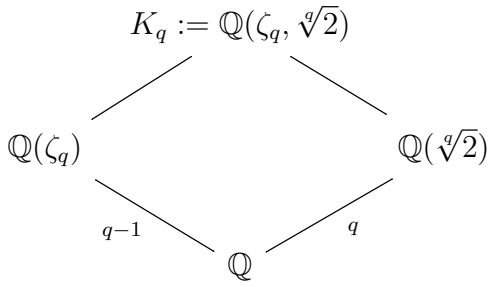
$$\begin{aligned}\sum_{\lambda\vdash n}\delta(\lambda)\mathrm{lcm}(\lambda) &= \frac{1}{n!}\sum_{\lambda\vdash n} n!\delta(\lambda)\mathrm{lcm}(\lambda)\\ &= \frac{1}{n!}\sum_{\sigma\in S_n}\mathrm{ord}(\sigma)\\ &= \mu_n,\end{aligned} \tag{4.1.13}$$

which by (4.1.4) proves Theorem 1.2.3.

4.2. Splitting of prime ideals in Kummer extensions

Consider the polynomial $f(x) = x^q - 2$ where q is an odd prime. Then the splitting field of $f(x)$ is $K_q := \mathbb{Q}(\zeta_q, \sqrt[q]{2})$. The following diagram will illustrate

this number field



In this diagram $\mathbb{Q}(\zeta_q)$ is a Galois extension over $\mathbb{Q}$, hence $N := \mathrm{Gal}(K_q/\mathbb{Q}(\zeta_q))$ is a normal subgroup of $G := \mathrm{Gal}(K_q/\mathbb{Q})$. Also $H := \mathrm{Gal}(K_q/\mathbb{Q}(\sqrt[q]{2}))$ is a subgroup of G. Let us recall the definition of the semidirect product.

Definition 4.2.1. *Let N and H be groups and let φ be a homomorphism from H into $Aut(N)$. Let denote $\cdot$ the (left) action of H on N determined by φ. Let G be the set of ordered pairs (n, h) with $n \in N$ and $h \in H$ and define the following multiplication on G:*

$$(n_1, h_1)(n_2, h_2) := (n_1 h_1 \cdot n_2, h_1 h_2).$$

With this operation G is a group, called the semidirect product of N and H, and denoted by $N \rtimes_\varphi H$.

Therefore $G \cong N \rtimes H$. Moreover we have $N \cong (\mathbb{Z}/(q\mathbb{Z})) = \mathbb{F}_q$ and $H \cong (\mathbb{Z}/(q\mathbb{Z}))^* = \mathbb{F}_q^* = Aut(\mathbb{F}_q)$. In other words

$$\mathrm{Gal}(K_q/\mathbb{Q}) \cong \mathbb{F}_q \rtimes Aut(\mathbb{F}_q).$$

Notice that the group $\mathbb{F}_q \rtimes Aut(\mathbb{F}_q)$ is isomorphic to $\mathrm{Aff}(\mathbb{F}_q)$, the group of all affine maps of $\mathbb{F}_q$. This group has natural matrix representation:

$$\mathrm{Aff}(\mathbb{F}_q) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}. \tag{4.2.1}$$

One can give an explicit isomorphism between the Galois group of $f(x) = x^q - 2$ and $\mathrm{Aff}(\mathbb{F}_q)$.

$$\begin{aligned} \Psi : \mathrm{Gal}(K_q/\mathbb{Q}) &\longrightarrow \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\} \\ \sigma &\longmapsto \begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & 1 \end{pmatrix}, \end{aligned} \tag{4.2.2}$$

where $\sigma(\zeta_q) = \zeta_q^{a(\sigma)}$, and $\sigma(\sqrt[q]{2}) = \zeta_q^{b(\sigma)}\sqrt[q]{2}$. By this explicit isomorphism we have

Lemma 4.2.1. *A prime p splits completely in K_q if and only if $p \equiv 1 \pmod q$ and $2^{\frac{p-1}{q}} \equiv 1 \pmod p$.*

There are several ways to show this, but in Chapter 5, we will consider the following method.

Proof: Let $p \equiv 1 \pmod q$ and $2^{\frac{p-1}{q}} \equiv 1 \pmod p$. With these conditions, by computing the discriminant of $f(x) = x^q - 2$, we can show that p is unramified in K_q. Let σ_p be the Artin symbol corresponding to the prime p, then we show that $\Psi(\sigma_p) = 1$, hence $\sigma_p = 1$. This shows that p splits completely. Since p is unramified, then by properties of the Artin symbol we have

$$\zeta_q^p = \sigma_p(\zeta_q) = \zeta_q^{a(\sigma_p)} \Longrightarrow a(\sigma_p) \equiv p \pmod q. \tag{4.2.3}$$

But $p \equiv 1 \pmod q$, so $a(\sigma_p) = 1$. Let $\mathfrak{p}$ be a prime in K_q above p, then

$$\zeta_q^{b(\sigma_p)} 2^{1/q} = \sigma_p(2^{1/q}) \equiv 2^{p/q} \pmod{\mathfrak{p}} \Longrightarrow 2^{1/q}\left(\zeta_q^{b(\sigma_p)} - 2^{(p-1)/q}\right) \in \mathfrak{p}. \tag{4.2.4}$$

Notice that p is unramified, so $2^{1/q} \notin \mathfrak{p}$, hence $\left(\zeta_q^{b(\sigma_p)} - 2^{(p-1)/q}\right) \in \mathfrak{p}$. Since $2^{\frac{p-1}{q}} \equiv 1 \pmod p$, then $\left(\zeta_q^{b(\sigma_p)} - 1\right) \in \mathfrak{p}$. But p is unramified, therefore $b(\sigma_p) = 0$. Hence $\Psi(\sigma_p) = 1$ so p splits completely.

Conversely, assume that p splits completely. Then σ_p is a trivial element. So $a(\sigma_p) = 1$, and $b(\sigma_p) = 0$. But

$$\zeta_q^p = \sigma_p(\zeta_q) = \zeta_q^{a(\sigma_p)} = \zeta_q \Longrightarrow p \equiv 1 \pmod q, \tag{4.2.5}$$

and

$$2^{1/q} = \zeta_q^{b(\sigma_p)} 2^{1/q} = \sigma_p(2^{1/q}) \equiv 2^{p/q} \pmod{\mathfrak{p}} \Longrightarrow 2^{1/q}\left(2^{(p-1)/q} - 1\right) \in \mathfrak{p}. \tag{4.2.6}$$

But $2^{1/q} \notin \mathfrak{p}$, therefore

$$\left(2^{(p-1)/q} - 1\right) \in \mathfrak{p} \cap \mathbb{Z} = (p) \Longrightarrow 2^{(p-1)/q} \equiv 1 \pmod{p}. \tag{4.2.7}$$

□

We would like to emphasize that this method will appear several times in Chapter 5.

Chapter 5

THE DENSITY OF A FAMILY OF MONOGENIC NUMBER FIELDS

Author: Mohammad Bardestani.

In this chapter we will prove our theorems which were stated in Section 1.2.1.

5.1. Monogenic fields and Diophantine equations

Generally speaking, we need to solve a Diophantine equation in order to show a number field is monogenic. It is useful to recall the following well-known statement.

Lemma 5.1.1. *Let K be a number field of degree n and $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ be linearly independent over $\mathbb{Q}$. Set $\mathcal{M} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Then*

$$Disc(\mathcal{M}) = (\mathcal{O}_K : \mathcal{M})^2 Disc(K).$$

In particular,

$$Disc(\alpha) = Ind(\alpha)^2 Disc(K),$$

if $\alpha \in \mathcal{O}_K$ and $K = \mathbb{Q}(\alpha)$, where $Ind(\alpha) = (\mathcal{O}_K : \mathbb{Z}[\alpha])$.

Choosing an integral basis for K and writing α with respect to this integral basis, one can see that $Ind(\alpha)$ is a homogeneous form. In this section, we will focus on cubic fields.

Let $K = \mathbb{Q}(\sqrt[3]{m})$, with $m \in \mathbb{Z}$ being a cube-free number, be a cubic field. We can assume that $m = hk^2$ with $h, k > 0$ and hk is square-free. The following theorem is due to Dedekind [19].

Theorem 5.1.1 (Dedekind). *If $K := \mathbb{Q}(\theta)$, where $\theta = \sqrt[3]{m}$, with m as given above, then*

(i) *For $m^2 \not\equiv 1 \pmod 9$, we have $Disc(K) = -27(hk)^2$, and the numbers*

$$\left\{1, \theta, \frac{\theta^2}{k}\right\}, \tag{5.1.1}$$

form an integral basis.

(ii) *For $m \equiv \pm 1 \pmod 9$, we have $Disc(K) = -3(hk)^2$, and the numbers*

$$\left\{1, \theta, \frac{k^2 \pm k^2\theta + \theta^2}{3k}\right\}, \tag{5.1.2}$$

form an integral basis.

Notice that this theorem shows $\mathbb{Q}(\sqrt[3]{p})$ is monogenic for primes $p \equiv \pm 2, \pm 5 \pmod 9$ which verifies Theorem 1.2.4 for $q = 3$. For $p \equiv \pm 1 \pmod 9$, by invoking Theorem 5.1.1 we obtain the following integral basis for $K = \mathbb{Q}(\sqrt[3]{p})$,

$$\left\{1, \theta, \frac{1 \pm \theta + \theta^2}{3}\right\},$$

where $\theta = \sqrt[3]{p}$. Let

$$\alpha = a + b\theta + c\frac{1 \pm \theta + \theta^2}{3} \in \mathcal{O}_K,$$

and assume α', α'' are its conjugates. It is easy to see

$$\begin{cases} \alpha - \alpha' = (\theta - \theta')\left(\left(b \pm \frac{c}{3}\right) - \frac{c\theta''}{3}\right) \\ \alpha - \alpha'' = (\theta - \theta'')\left(\left(b \pm \frac{c}{3}\right) - \frac{c\theta'}{3}\right) \\ \alpha' - \alpha'' = (\theta' - \theta'')\left(\left(b \pm \frac{c}{3}\right) - \frac{c\theta}{3}\right) \end{cases}, \tag{5.1.3}$$

where θ' and θ'' are the conjugates of θ. Therefore

$$\begin{aligned} Disc(\alpha) &= Disc(\theta)\left(\left(b \pm \frac{c}{3}\right)^3 - p\left(\frac{c}{3}\right)^3\right)^2 \\ &= -3^3p^2\left(\left(b \pm \frac{c}{3}\right)^3 - p\left(\frac{c}{3}\right)^3\right)^2 \\ &= -3p^2\left(3b^3 \pm 3b^2c + bc^2 + \frac{\pm 1 - p}{9}c^3\right)^2, \end{aligned}$$

thus

$$Ind(\alpha) = |3b^3 \pm 3b^2c + bc^2 + \frac{\pm 1 - p}{9}c^3|.$$

So to determine monogenicity of $\mathbb{Q}(\sqrt[3]{p})$, for primes of the form $p \equiv \pm 1 \pmod 9$, we need to find the integral solutions of

$$|3b^3 \pm 3b^2c + bc^2 + \frac{\pm 1 - p}{9}c^3| = 1. \tag{5.1.4}$$

Multiplying by 9 in (5.1.4) we obtain an equivalent equation

$$|(3b \pm c)^3 - pc^3| = 9, \tag{5.1.5}$$

which, for primes $p \equiv \pm 1 \pmod 9$, is equivalent to

$$px^3 + y^3 = 9.$$

Therefore we obtain

Lemma 5.1.2. *For $p \equiv \pm 1 \pmod 9$, $\mathbb{Q}(\sqrt[3]{p})$ being monogenic reduces to*

$$px^3 + y^3 = 9, \tag{5.1.6}$$

having an integral solution.

Remark 5.1.1. *Here, for simplicity, we found the index form of $\mathbb{Q}(\sqrt[3]{p})$, but the same computation gives us (1.2.12).*

Hence to construct a non-monogenic $\mathbb{Q}(\sqrt[3]{p})$, it would be enough to find a prime $p \equiv \pm 1 \pmod 9$, such that (5.1.6) does not have any integral solution. One can find some of those primes by studying the equation locally, for instance those primes p, such that 9 is not a cube modulo p. Notice that 9 is a cube if and only if 3 is a cube in $\mathbb{F}_p$. Therefore we will briefly study the number of solutions of $h(t) := t^3 - 3$ in a finite field $\mathbb{F}_p$, denoted by $N_p(h(t))$, for all primes $p \geq 5$.

Lemma 5.1.3.

$$N_p(h(t)) = \begin{cases} 1 & \text{if } p \equiv 2 \pmod 3 \\ 0 & \text{if } p = 7x^2 + 3xy + 9y^2 \\ 3 & \text{if } p = x^2 + xy + 61y^2 \end{cases}.$$

Let $E := \frac{\mathbb{Q}[t]}{(h(t))}$ be the cubic field defined by $h(t)$, with the splitting field L, which contains the quadratic field $K := \mathbb{Q}(\sqrt{-3})$. Let $\eta_1 = \sqrt[3]{3}, \eta_2, \eta_3$ be the

conjugates of $\sqrt[3]{3}$, then define

$$\Delta := \prod_{1 \le i < j \le 3} (\eta_j - \eta_i).$$

For a prime $p \geq 5$, consider the Frobenius automorphism associated to p, say $\sigma_p \in \mathrm{Gal}(L/\mathbb{Q})$; which is unique up to conjugation. Regarding σ_p as a permutation in S_3, we observe

$$\sigma_p(\Delta) = sgn(\sigma_p)\Delta.$$

Therefore σ_p being even implies that σ_p is a trivial element in $\mathrm{Gal}(K/\mathbb{Q})$, thus p splits completely in K. Also when σ_p is an odd permutation, σ_p is not an identity element, therefore p is inert in K. This shows $sgn(\sigma_p) = \left(\frac{p}{3}\right)$, where $\left(\frac{\cdot}{3}\right)$ denotes the Legandre symbol. Therefore $p \equiv 2 \pmod 3$ implies that σ_p is a transposition, thus $h(t) = 0$ has a unique solution in $\mathbb{F}_p$. For $p \equiv 1 \pmod 3$, σ_p is an even permutation, so $h(t) = 0$ has either zero or three solutions in $\mathbb{F}_p$. Hence for $p \equiv 1 \pmod 3$, if 3 is a cube in $\mathbb{F}_p$ we have $N_p(h(t)) = 3$, and if 3 is not a cube then $N_p(h(t)) = 0$.

One might find an alternative proof for this fact that $t^3 - 3$ has only one solution for $p \equiv 2 \pmod 3$, by looking at the homomorphism

$$\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$$
$$a \longrightarrow a^3,$$

and noticing that this an isomorphism. For $p \equiv 1 \pmod 3$, we have 3'th root of unity in $\mathbb{F}_p$, so one have either zero or three solutions. However the former method is more general, and can be applied for general polynomials.

Using the cubic residue symbol, one can show that for primes $p \geq 5$, p can be presented by $x^2 + xy + 61y^2$ if and only if $p \equiv 1 \pmod 3$ and 3 is a cubic residue modulo p. Indeed this was conjectured by Euler and proved by Gauss (see [16]).

Reduction theory of positive definite, integral binary quadratic form is easy to describe. For such a given form $f(x, y) = ax^2 + bxy + cy^2$, by $\mathrm{SL}_2(\mathbb{Z})$ change of variable we can obtain a simpler form $f'(x, y) = a'x^2 + b'xy + c'y^2$, where $|b'| \leq a' \leq c'$ and in case $|b'| = a'$, then $b' = a'$; and in case $a' = c'$, then $b' \geq 0$. The discriminant of $x^2 + xy + 61y^2$ is -243 which has the class number 3. More

precisely, using the reduction algorithm explained briefly, there are, up to $\mathrm{SL}_2(\mathbb{Z})$ change of variables, three binary quadratic form with discriminant -243. Namely $x^2+xy+61y^2, 7x^2\pm 3xy+9y^2$, which there are in the same genus. When $p\equiv 1 \pmod 3$, then p can be presented by only one of the form $x^2+xy+61y^2$ or $7x^2+3xy+9y^2$. Indeed we have the following

Lemma 5.1.4. *Let f_1, f_2 be two integral binary quadratic forms of the same discriminant which represent the same prime, say p. Then they are $\mathrm{GL}_2(\mathbb{Z})$-equivalent.*

Proof: Consider an integral binary quadratic form, say $f(x,y)=ax^2+bxy+cy^2$, that presents a prime p, then we can assume $f(x,y)=px^2+bxy+cy^2$. Consider

$$\gamma=\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}\in \mathrm{SL}_2(\mathbb{Z}),$$

then

$$\begin{aligned}\gamma.f(x,y):=f((x,y)\gamma) &= px^2+(2pm+b)xy+(c+bm+pm^2)y^2\\ &= px^2+b'xy+c'y^2.\end{aligned}$$

We can choose m such that

$$-p<2pm+b\leq p,$$

so we have shown that any integral binary quadratic form that represents a prime p is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $px^2+b'xy+c'y^2$, where $-p<b'\leq p$. Under $\mathrm{GL}_2(\mathbb{Z})$-equivalence, we can assume $0\leq b'\leq p$. This determines b' (and hence c') uniquely and finishes the proof. □

Lemma 5.1.3 shows $px^3+y^3=9$ does not have any integral solutions for those primes $p\equiv 1 \pmod 9$, which p can be represented by the quadratic form $7x^2+3xy+9y^2$, and hence Lemma 5.1.2 gives a proof for Theorem 1.2.6. Using the Chebotarev density theorem we can also count these primes and then prove Theorem 1.2.5. Let $K=\mathbb{Q}(\zeta_9,\sqrt[3]{9})$, where ζ_9 is a primitive 9'th root of unity. We will show

Lemma 5.1.5. *A prime p splits completely in K if and only if $p \equiv 1 \pmod 9$ and $9^{\frac{p-1}{3}} \equiv 1 \pmod p$.*

Since we will use the Chebotarev density theorem several times, let us recall it briefly. Let K be a number field and assume L/K is a Galois extension. To each prime ideal $\mathfrak{P}$ of K unramified in L there corresponds a certain conjugacy class $\mathcal{C}$ of $\mathrm{Gal}(L/K)$ consisting of the set of Frobenius automorphisms σ attached to the prime ideals $\mathcal{P}$ of L which lie over $\mathfrak{P}$. Denote this conjugacy class by the Artin symbol $\left(\frac{L/K}{\mathfrak{P}}\right)$. For a given conjugacy class $\mathcal{C}$ of $\mathrm{Gal}(L/K)$, let $\pi_{\mathcal{C}}(x)$ denote the number of prime ideals $\mathfrak{P}$ of K unramified in L such that $\left(\frac{L/K}{\mathfrak{P}}\right) \in \mathcal{C}$ and $N_{L/K}(\mathfrak{P}) \leq x$. By abuse of notation, the Frobenius automorphism is also represented by the Artin symbol.

Theorem 5.1.2 (Chebotarev density theorem, see[53])**.**

$$\lim_{x\to\infty} \pi_{\mathcal{C}}(x) = \frac{|\mathcal{C}|}{[L:K]}\pi(x). \tag{5.1.7}$$

Therefore

Proof of Theorem 1.2.5: Note that for $p \equiv 1 \pmod 9$, $9^{\frac{p-1}{3}} \equiv 1 \pmod p$ is equivalent to 9 being a cube in $\mathbb{F}_p$. Lemma 5.1.5 and the Chebotarev density theorem implies

$$\frac{1}{\pi(x)}\#\{p \leq x : p \equiv 1 \pmod 9, 9 \text{ is not a cube in } \mathbb{F}_p\} \xrightarrow[x\to\infty]{} \frac{1}{6} - \frac{1}{18} = \frac{1}{9}.$$

□

Let us denote ω the primitive cube root of unity. To prove Lemma 5.1.5, we need the following, which is easy to prove.

Lemma 5.1.6. *Let $K = \mathbb{Q}(\zeta_9, \sqrt[3]{9})$, then the following map is an isomorphism*

$$\begin{aligned} \psi : \mathrm{Gal}(K/\mathbb{Q}) &\longrightarrow \frac{\mathbb{Z}}{3\mathbb{Z}} \rtimes \left(\frac{\mathbb{Z}}{9\mathbb{Z}}\right)^* \\ \sigma &\longrightarrow (a(\sigma), b(\sigma)), \end{aligned}$$

where $\sigma(\sqrt[3]{9}) = \omega^{a(\sigma)}\sqrt[3]{9}$ and $\sigma(\zeta_9) = \zeta_9^{b(\sigma)}$.

This lemma implies

Proof of Lemma 5.1.5: Let p be an unramified prime in K and σ_p the Frobenius automorphism associated to p; which is unique up to conjugation. Then

$$\zeta_9^{b(\sigma_p)} = \sigma_p(\zeta_9) \equiv \zeta_9^p \pmod{\mathfrak{p}},$$

where $\mathfrak{p}$ is a prime above p. Since p is unramified we conclude that $b(\sigma_p) \equiv p \pmod 9$. The same reason implies for such a p,

$$\omega^{a(\sigma)} 9^{\frac{1}{3}} = \sigma_p(9^{\frac{1}{3}}) \equiv 9^{\frac{p}{3}} \pmod{\mathfrak{p}} \Longrightarrow (\omega^{a(\sigma)} - 9^{\frac{p-1}{3}}) \in \mathfrak{p}.$$

Let $p \equiv 1 \pmod 9$ and $9^{\frac{p-1}{3}} \equiv 1 \pmod p$. Notice that p is unramified since $\gcd(p, 3) = 1$, so

(i) $b(\sigma_p) \equiv p \equiv 1 \pmod 9$, thus $b(\sigma) = 1$.

(ii) $\omega^{a(\sigma)} - 9^{\frac{p-1}{3}} \in \mathfrak{p}$ which implies $\omega^{a(\sigma)} - 1 \in \mathfrak{p}$, hence $a(\sigma) = 0$.

Thus $\psi(\sigma_p) = (0, 1)$, therefore σ_p is the identity element. This means p splits completely. Conversely, if p splits completely then $a(\sigma) = 0$ and $b(\sigma) = 1$, which implies

(i) $\zeta_9 \equiv \zeta_9^p \pmod{\mathfrak{p}} \Longrightarrow p \equiv 1 \pmod 9$.

(ii) $9^{\frac{1}{3}} \equiv 9^{\frac{p}{3}} \pmod{\mathfrak{p}} \Longrightarrow \left(9^{\frac{p-1}{3}} - 1\right) \in \mathfrak{p} \cap \mathbb{Z} = (p)$.

This finishes the proof. □

Since $t^3 + 9$ is an irreducible polynomial then a famous conjecture due to Bunyakovsky says that there should be infinitely many prime of the form $t^3 + 9$ which are congruent to ± 1 modulo 9. These primes produce monogenic fields. This shows the difficulty of characterizing monogenic fields even for pure cubic extensions. Monogenicity of cyclic cubic fields has been studied by Dummit and Kisilevsky [21].

5.2. Eisenstein polynomials and Monogenic fields

Recall that a polynomial $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ is called an Eisenstein polynomial at a prime p when

(i) $p \mid a_i$ for all $0 \leq i \leq n - 1$,

(ii) $p^2 \nmid a_0$.

Let $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ be an Eisenstein polynomial at p, and let K be the field generated by a root of $f(t)$, say α, i.e., $K = \mathbb{Q}(\alpha)$. We will show that for any integers, $c_0, c_2, \ldots, c_{n-1}$,

$$N_{K/\mathbb{Q}}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) \equiv c_0^n \pmod{p}, \tag{5.2.1}$$

for which we deduce the following

Lemma 5.2.1. *suppose $K = \mathbb{Q}(\alpha)$, where α is a root of an Eisenstein polynomial at p, then*

$$p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]].$$

Proof: Let $p|[\mathcal{O}_K, \mathbb{Z}[\alpha]]$, therefore there exists an algebraic integer

$$\theta \in \mathcal{O}_K \setminus \mathbb{Z}[\alpha],$$

so that $p\theta \in \mathbb{Z}[\alpha]$. Hence for some integers $c_0, c_1, \ldots, c_{n-1}$ we have

$$p\theta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

so

$$p^n N_{K/\mathbb{Q}}(\theta) = N_{K/\mathbb{Q}}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) \equiv c_0^n \pmod{p},$$

which implies $p \mid c_0$. Note that $p \| N_{K/\mathbb{Q}}(\alpha)$, so this process and (5.2.1), imply $p \mid c_i$ for all i, which is a contradiction. □

Lemma 5.2.1 will allow us to find an arithmetic condition on p such that $f_p(t)$ produce a monogenic field. To prove Lemma 5.2.1, it remains to prove (5.2.1).

Proof of (5.2.1): Let E be the Galois closure of K, and assume $\mathfrak{P}$ is a prime in E above p. Since $p \mid a_i$, then $\alpha_i \in \mathfrak{P}$, where $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are the conjugates of α. Note that

$$N_{K/\mathbb{Q}}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = \prod_{i=1}^{n}(c_0 + c_1\alpha_i + \cdots + c_{n-1}\alpha_i^{n-1}),$$

This implies

$$N_{K/\mathbb{Q}}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) - c_0^n \in \mathfrak{P} \cap \mathbb{Z} = (p),$$

which proves the equation. □

In a monogenic field K, the field discriminant is equal to the discriminant of the minimal polynomial of α, where $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Also, by using the Dedekind's Theorem 5.2.1, it is easy to see how a prime splits, by looking at how the minimal polynomial of θ splits modulo primes. More precisely

Theorem 5.2.1 (Dedekind)**.** *Let K be a number field such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, for some α. Let $f(x)$ be the minimal polynomial of α and denote $\bar{f}$ the reduction of f modulo a prime p. Let*

$$\bar{f}(x) = P_1(x)^{e_1} \cdots P_g(x)^{e_g},$$

then

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Hence it is natural to see how prime splitting forces a number field to be non-monogenic. This idea was first noticed by Hensel. Indeed he constructed a family of C_3-extensions over $\mathbb{Q}$, such that 2 splits completely, and since in $\mathbb{F}_2[t]$ there are only two linear polynomials, he deduced that these fields are non-monogenic.

Hensel's idea can be extended easily to construct infinitely many non-monogenic Abelian number fields. Indeed let $l \equiv 1 \pmod{n}$ be a prime and assume $n \geq 3$. Denote the unique C_n-subfield of $\mathbb{Q}(\zeta_l)$ by $K_n(l)$. The same method used to prove Lemma 5.2.3 shows that a prime p splits completely in $K_n(l)$ if and only if $p \neq l$ and $t^n - p$ has a solution in $\mathbb{F}_l$. Therefore, for a prime $l \equiv 1 \pmod{n}$, if $t^n - 2$ has a solution in $\mathbb{F}_l$, then $K_n(l)$ cannot be non-monogenic. Notice that different l produces different C_n fields since the discriminant of $K_n(l)$ is a function of l. So we need to count, the number of prime $l \equiv 1 \pmod{n}$ such that 2 is a n'th power in $\mathbb{F}_l$. Consider the Kummer extension $\mathbb{Q}(\zeta_n, \sqrt[n]{2})$ and observing

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{2})/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/(n\mathbb{Z})) \rtimes (\mathbb{Z}/(n\mathbb{Z}))^*.$$

Lemma 5.2.2. *A prime p splits completely in $\mathbb{Q}(\zeta_n, \sqrt[n]{2})$ if and only if $p \equiv 1 \pmod{n}$ and $t^n - 2$ has a solution in $\mathbb{F}_p$.*

By the inequality $[\mathbb{Q}(\zeta_n, \sqrt[n]{2}) : \mathbb{Q}] \leq n\varphi(n)$ and the Chebotarev density theorem we obtain

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \{l \leq x : l \equiv 1 \pmod{n}, K_n(l) \text{ is non-monogenic}\} \geq \frac{1}{n\varphi(n)}.$$

Remark 5.2.1. *Let $K/\mathbb{Q}$ be a cyclic extension of prime degree $l \geq 5$. Gras [36] in her beautiful paper, using a result of Leopoldt, showed that K is non-monogenic unless $2l+1 = p$ is a prime and $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.*

Thus we have constructed infinitely many non-monogenic C_n-extension over $\mathbb{Q}$, such that 2 splits completely. For a given Abelian group

$$G = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_t},$$

choose a non-monogenic C_{n_i}-field, say K_{n_i}, for $1 \leq i \leq t$, with coprime discriminants. Put $K = K_{n_1} \cdots K_{n_t}$. Notice that 2 splits completely in K_{n_i}, therefore 2 splits completely in K, which shows that K is non-monogenic.

We can extend this idea further. For a prime number l, the field $K := \mathbb{Q}(\zeta_{l^2})$ is a Galois extension with cyclic Galois group $(\mathbb{Z}/(l^2\mathbb{Z}))^*$. Let η be its generator and put $H := \langle \eta^l \rangle$. Denote by K_l the fixed field of H, therefore $[K_l : \mathbb{Q}] = l$ and $\mathrm{Gal}(K/K_l) \cong H$.

Lemma 5.2.3. *p splits completely in K_l if and only if $p^{l-1} \equiv 1 \pmod{l^2}$.*

Proof: Assume a prime p splits completely in K_l, and let $\sigma_p := \left(\frac{K/\mathbb{Q}}{p}\right)$ be the Frobenius automorphism associated to p, then

$$\sigma_p|_{K_l} = \left(\frac{K/\mathbb{Q}}{p}\right)\Big|_{K_l} = \left(\frac{K_l/\mathbb{Q}}{p}\right) = id.$$

Therefore $\sigma_p \in \mathrm{Gal}(K/K_l) \cong H$. But $p \neq l$ is unramified in K, thus $\sigma_p(\zeta_{l^2}) = \zeta_{l^2}^p$, since $\sigma_p(\zeta_{l^2}) \equiv \zeta_{l^2}^p \pmod{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime in K above p. Under the canonical isomorphism

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \left(\frac{\mathbb{Z}}{l^2\mathbb{Z}}\right)^*,$$

we see that $p \in H = \langle \eta^l \rangle$, therefore for some integer t,

$$p \equiv \eta^{tl} \pmod{l^2} \Longrightarrow p^{l-1} \equiv 1 \pmod{l^2}.$$

Conversely, let

$$p^{l-1} \equiv 1 \pmod{l^2}.$$

Assume that $p \equiv \eta^t \pmod{l^2}$ for some integer t. Hence

$$1 \equiv p^{l-1} \equiv \eta^{t(l-1)} \pmod{l^2} \Longrightarrow l \mid t,$$

therefore $p \in H$ which implies that

$$\sigma_p \in \mathrm{Gal}(K/K_l).$$

This means $\left(\frac{K_l/\mathbb{Q}}{p}\right) = id$, hence p splits completely in K_l. □

Corollary 5.2.1. *Let l be a prime such that for some prime $p < l$, $p^{l-1} \equiv 1 \pmod{l^2}$ then K_l is non-monogenic.*

As an application of Lemma 5.2.3 and the Chebotarev density theorem, one can calculate the density of

$$\#\{p \leq x : p^{l-1} \not\equiv 1 \pmod{l^2}\},$$

which we will use to prove our main theorem.

Theorem 5.2.2. *With the notations of Lemma 5.2.3 we have*

$$\#\left\{p \leq x : p^{l-1} \not\equiv 1 \pmod{l^2}\right\} = \frac{l-1}{l}\pi(x)(1+o(1)).$$

Proof: Note that $\mathcal{C} = \mathrm{Gal}(K_l/\mathbb{Q}) - \{e\}$ is stable under conjugation, where e is the identity element in the Galois group, and $\mathcal{C}$ corresponds to the set of non-split primes by Lemma 5.2.3, therefore the Chebotarev density theorem implies our theorem. □

Remark 5.2.2. *As Professor Andrew Granville has pointed out to the author, Theorem 5.2.2 can also be proven by Dirichlet's theorem on primes in arithmetic progressions.*

We have all ingredients to prove Theorem 1.2.4.

Proof of Theorem 1.2.4: Let $K := E_{f_p} = \mathbb{Q}(\alpha)$ be the field obtained by adjoining a root of $f_p(x)$ to $\mathbb{Q}$. Since $f_p(x)$ is an Eisenstein polynomial at p, we have that

$$p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]].$$

It is easy to see that

$$|Disc(f_p)| = q^q p^{q-1},$$

therefore q might divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. For $p^{q-1} \not\equiv 1 \pmod{q^2}$ we see that

$$\begin{aligned} f_p(t+p) &= (t+p)^q - p \\ &= t^q + \binom{q}{1} p t^{q-1} + \cdots + \binom{q}{q-1} p^{q-1} t + (p^q - p), \end{aligned}$$

which implies $f_p(t+p)$ is an Eisenstein polynomial at the prime q so by Lemma 5.2.1 we obtain

$$q \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha - p]] = [\mathcal{O}_K : \mathbb{Z}[\alpha]],$$

therefore $f_p(t)$ is monogenic. Thus

$$\#\{p \le x : f_p(t) \text{ is monogenic}\} \ge \#\{p \le x : p^{q-1} \not\equiv 1 \pmod{q^2}\},$$

which combined with Theorem 5.2.2 proves our theorem. □

As was already mentioned, Theorem 1.2.4 can also also be proven without using the Chebotarev density theorem. Indeed, for $1 \le i \le q-1$, consider the following change of variable

$$f(t+i) = (t+i)^q - p = t^q + \sum_{j=1}^{q-1} \binom{q}{j} t^j i^{q-j} + (i^q - p),$$

so to obtain an Eisenstein polynomial at q, we need to have the conditions $p \equiv i^q \equiv i \pmod{q}$ and $p \not\equiv i^q \pmod{q^2}$ that also imply $p^{q-1} \not\equiv 1 \pmod{q^2}$. By the prime number theorem in arithmetic progressions, we get

$$\begin{aligned} &\lim_{x\to\infty} \frac{1}{\pi(x)} \{p \le x : p \equiv i \pmod{q}, p \not\equiv i^q \pmod{q^2}\} \\ &= \lim_{x\to\infty} \frac{1}{\pi(x)} \{p \le x : p \equiv i^q + qs \pmod{q^2}, 1 \le s \le q-1\} \\ &= \frac{q-1}{q(q-1)} = \frac{1}{q}. \end{aligned}$$

This also proves Theorem 1.2.4. However the Chebotarev density theorem would give a better error term.

It should be mentioned that the simple change of variable $x+1$ also gives interesting examples.

Example 5.2.1. *Let $m = 2^k$ be a power of 2, and assume $p \equiv 3 \pmod 4$ is a prime. Then $f(x) = x^m - p$ is an Eisenstein polynomial at p, with discriminant $-m^m p^{m-1}$. We now remark that*

$$k\binom{m}{k} = m\binom{m-1}{k-1},$$

which implies

$$f(x+1) = (x+1)^m - p = x^m + \sum_{j=1}^{m-1} \binom{m}{j} x^j + (1-p),$$

is an Eisenstein at 2, therefore

$$2 \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt[m]{p} - 1]] = [\mathcal{O}_K : \mathbb{Z}[\sqrt[m]{p}]].$$

So $\mathbb{Q}(\sqrt[2^k]{p})$ is a monogenic number field.

Eisenstein polynomials essentially give us a number field which contains a totally ramified prime. Indeed, by Lemma 5.2.1 and the Dedekind theorem (see [53], Proposition 8.3), we have the following well-known result.

Lemma 5.2.4. *Let $K = \mathbb{Q}(\alpha)$, where α is the root of an Eisenstein polynomial at a prime p. Then p is totally ramified in K.*

For primes p, q such that

$$p^{q-1} \not\equiv 1 \pmod{q^2},$$

p and q are totally ramified in the number field obtained by adjoining a root of $f_p(t) = t^q - p$, therefore $f_p(t)$'s generate a family of number fields which are totally ramified only at two primes.

5.3. Some final remarks

We can also fix a prime p and vary q in $t^q - p$. For example, when $p = 2$, we want to understand for which prime q, $t^q - 2$ is monogenic. We should therefore understand the distribution of primes q such that

$$2^{q-1} \not\equiv 1 \pmod{q^2}.$$

This is an interesting question, as it can be shown that if $2^{q-1} \not\equiv 1 \pmod{q^2}$, then the first case of Fermat's Last Theorem holds. Indeed, we expect that there

are only few primes q such that $2^{q-1} \equiv 1 \pmod{q^2}$. As far as I know, 1093 and 3511 are the only primes known to satisfy this relation. For a number field K, let $\zeta_K(s)$ be the Dedekind zeta function of K, and assume its Laurent expansion at $s = 1$ is

$$\zeta_K(s) = c_{-1}(s-1)^{-1} + c_0 + c_1(s-1) + \cdots \qquad (c_{-1} \neq 0).$$

Ihara [46] in his interesting paper defined an analogue to the Euler-Kronecker constant

$$\gamma_K = \frac{c_0}{c_{-1}},$$

which is the same as the usual Euler constant for $K = \mathbb{Q}$. Let K_q be the field we defined in Lemma 5.2.3 ($q = l$) and denote $\gamma_q := \gamma_{K_q}$. Assuming GRH, Ihara proved (see [46], Corollary 3)

Theorem 5.3.1 (Ihara)**.** *Assuming GRH, if* $\liminf \frac{\gamma_q}{q} = 0$*, then for each prime* p*, there are finitely many* q *such that*

$$p^{q-1} \equiv 1 \pmod{q^2}.$$

Therefore by considering these above assumptions we see, for a fixed p, most of the time $t^q - p$ is monogenic. These primes are called Wieferich primes. Motivated by Fermat's last theorem, Granville in his interesting paper [32] has studied these primes. Moreover, Granville and Soundararajan [34] in their remarkable paper related these primes to a conjecture of Erdös asking if every positive integer is the sum of a square-free number and a power of 2. It seems possible to use the effective Chebotarev density theorem, to obtain some averaging result for the distribution of q mentioned above.

For a given prime $q \geq 3$, it would be interesting to classify the monogenicity of $K_p := \mathbb{Q}(\zeta_q, \sqrt[q]{p})$ when $p(\neq q)$ varies. Note that a prime l splits completely in K_p if and only if $l \equiv 1 \pmod{q}$, and $p^{\frac{l-1}{q}} \equiv 1 \pmod{l}$. Therefore, by using Hensel's idea mentioned earlier, if the least prime in the arithmetic progression $n \equiv q \pmod{q}$ is less than $q(q-1)$, then there are infinitely many p such that K_p is non-monogenic, namely those p, for which $p^{\frac{l-1}{q}} \equiv 1 \pmod{l}$. Chang [14] considered this problem for $q = 3$ and proved that $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is essentially the only monogenic field among the family $\mathbb{Q}(\sqrt[3]{p}, \omega)$. However, it seems that for $q \geq 5$

the question is more delicate. Perhaps generalizing his methods might gives some characterization.

Acknowledgments:

I would like to thank Andrew Granville and Hershy Kisilevsky for their encouragements and advices. For many fruitful discussions, my thanks also to Carl Pomerance. I have benefited from some notes on Keith Conrad's web page. I wish to thank him for providing these notes online. Last, but not least, I would like to thank my friends François Charette and Daniel Fiorilli.

Bibliography

[1] N. Alon. Independent sets in regular graphs and sum-free subsets of finite groups. *Israel J. Math.*, 73(2):247–256, 1991.

[2] A. Ash, J. Brakenhoff, and T. Zarrabi. Equality of polynomial and field discriminants. *Experiment. Math.*, 16(3):367–374, 2007.

[3] L. Babai and V. T. Sós. Sidon sets in groups and induced subgraphs of Cayley graphs. *European J. Combin.*, 6(2):101–114, 1985.

[4] H. Bass and A. Lubotzky. *Tree lattices*, volume 176 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 2001. With appendices by Bass, L. Carbone, Lubotzky, G. Rosenberg and J. Tits.

[5] H. Bass, J. Milnor, and J.-P. Serre. Solution of the congruence subgroup problem for $\mathrm{SL}_n\,(n \geq 3)$ and $\mathrm{Sp}_{2n}\,(n \geq 2)$. *Inst. Hautes Études Sci. Publ. Math.*, (33):59–137, 1967.

[6] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. arXiv:1006.1002v2.

[7] J. Bourgain and A. Gamburd. Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. I. *J. Eur. Math. Soc. (JEMS)*, 10(4):987–1011, 2008.

[8] J. Bourgain and A. Gamburd. Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. II. *J. Eur. Math. Soc. (JEMS)*, 11(5):1057–1103, 2009. With an appendix by Bourgain.

[9] N. J. Calkin. On the number of sum-free sets. *Bull. London Math. Soc.*, 22(2):141–144, 1990.

[10] P. J. Cameron and P. Erdős. On the number of sets of integers with various properties. In *Number theory (Banff, AB, 1988)*, pages 61–79. de Gruyter,

Berlin, 1990.

[11] R. Carter, G. Segal, and I. Macdonald. *Lectures on Lie groups and Lie algebras*, volume 32 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1995. With a foreword by Martin Taylor.

[12] R. W. Carter. *Simple groups of Lie type*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1989. Reprint of the 1972 original, A Wiley-Interscience Publication.

[13] R. W. Carter. *Lie algebras of finite and affine type*, volume 96 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2005.

[14] M.-L. Chang. Non-monogeneity in a family of sextic fields. *J. Number Theory*, 97(2):252–268, 2002.

[15] C. Chevalley. Sur certains groupes simples. *Tôhoku Math. J. (2)*, 7:14–66, 1955.

[16] D. 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.

[17] G. Davidoff, P. Sarnak, and A. Valette. *Elementary number theory, group theory, and Ramanujan graphs*, volume 55 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2003.

[18] R. Dedekind. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Abh. Kgl. Ges. Wiss. Göttingen*, 23:1–23, 1878.

[19] R. Dedekind. Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern. *Journal für die reine und angewandte Mathematik*, 121:40–123, 1900.

[20] J. D. Dixon and D. Panario. The degree of the splitting field of a random polynomial over a finite field. *Electron. J. Combin.*, 11(1):Research Paper 70, 10 pp. (electronic), 2004.

[21] D. S. Dummit and H. Kisilevsky. Indices in cyclic cubic fields. In *Number theory and algebra*, pages 29–42. Academic Press, New York, 1977.

[22] P. Erdős and P. Turán. On some problems of a statistical group-theory. I. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 4:175–186 (1965), 1965.

[23] P. Erdős and P. Turán. On some problems of a statistical group-theory. II. *Acta math. Acad. Sci. Hungar.*, 18:151–163, 1967.

[24] P. Erdős and P. Turán. On some problems of a statistical group-theory. III. *Acta Math. Acad. Sci. Hungar.*, 18:309–320, 1967.

[25] P. Erdős and P. Turán. On some problems of a statistical group-theory. IV. *Acta Math. Acad. Sci. Hungar*, 19:413–435, 1968.

[26] P. Erdős and P. Turán. On some problems of a statistical group theory. VI. *J. Indian Math. Soc.*, 34(3-4):175–192 (1971), 1970.

[27] P. Erdős and P. Turán. On some problems of a statistical group theory. V. *Period. Math. Hungar.*, 1(1):5–13, 1971.

[28] P. Erdős and P. Turán. On some problems of a statistical group theory. VII. *Period. Math. Hungar.*, 2:149–163, 1972. Collection of articles dedicated to the memory of Alfréd Rényi, I.

[29] W. Fulton and J. Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[30] W. M. Y. Goh and E. Schmutz. The expected order of a random permutation. *Bull. London Math. Soc.*, 23(1):34–42, 1991.

[31] W. T. Gowers. Quasirandom groups. *Combin. Probab. Comput.*, 17(3):363–387, 2008.

[32] A. Granville. The Kummer-Wieferich-Skula approach to the first case of Fermat's last theorem. In *Advances in number theory (Kingston, ON, 1991)*, Oxford Sci. Publ., pages 479–497. Oxford Univ. Press, New York, 1993.

[33] A. Granville. *ABC* allows us to count squarefrees. *Internat. Math. Res. Notices*, (19):991–1009, 1998.

[34] A. Granville and K. Soundararajan. A binary additive problem of Erdős and the order of 2 mod p^2. *Ramanujan J.*, 2(1-2):283–298, 1998. Paul Erdős (1913–1996).

[35] A. Granville and T. J. Tucker. It's as easy as *abc*. *Notices Amer. Math. Soc.*, 49(10):1224–1231, 2002.

[36] M.-N. Gras. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbf{Q}$ de degré premier $l \geq 5$. *J. Number Theory*, 23(3):347–353, 1986.

[37] G. Greaves. Power-free values of binary forms. *Quart. J. Math. Oxford Ser. (2)*, 43(169):45–65, 1992.

[38] B. Green. The Cameron-Erdős conjecture. *Bull. London Math. Soc.*, 36(6):769–778, 2004.

[39] B. Green and I. Z. Ruzsa. Sum-free sets in abelian groups. *Israel J. Math.*, 147:157–188, 2005.

[40] H. Hasse. *Zahlentheorie*. Dritte berichtigte Auflage. Akademie-Verlag, Berlin, 1969.

[41] H. A. Helfgott. Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$. *J. Eur. Math. Soc. (JEMS)*, 13(3):761–851, 2011.

[42] K. Hoffman and R. Kunze. *Linear algebra*. Second edition. Prentice-Hall Inc., Englewood Cliffs, N.J., 1971.

[43] K. H. Hofmann and S. Morris. *The structure of compact groups*, volume 25 of *de Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin, augmented edition, 2006.

[44] C. Hooley. On the power free values of polynomials. *Mathematika*, 14:21–26, 1967.

[45] Y. Ihara. On discrete subgroups of the two by two projective linear group over p-adic fields. *J. Math. Soc. Japan*, 18:219–235, 1966.

[46] Y. Ihara. On the Euler-Kronecker constants of global fields and primes with small norms. In *Algebraic geometry and number theory*, volume 253 of *Progr. Math.*, pages 407–451. Birkhäuser Boston, Boston, MA, 2006.

[47] K. S. Kedlaya. Product-free subsets of groups. *Amer. Math. Monthly*, 105(10):900–906, 1998.

[48] A. W. Knapp. *Advanced real analysis*. Cornerstones. Birkhäuser Boston Inc., Boston, MA, 2005. Along with a companion volume ıt Basic real analysis.

[49] V. Landazuri and G. M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra*, 32:418–443, 1974.

[50] B. M. Landman and A. Robertson. *Ramsey theory on the integers*, volume 24 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2004.

[51] A. Lubotzky. Expander graphs in pure and applied mathematics. *Bull. Amer. Math. Soc. (N.S.)*, 49(1):113–162, 2012.

[52] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[53] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[54] M. Newman. *Integral matrices*. Academic Press, New York, 1972. Pure and Applied Mathematics, Vol. 45.

[55] N. Nikolov and L. Pyber. Product decompositions of quasirandom groups and a Jordan type theorem. *J. Eur. Math. Soc. (JEMS)*, 13(4):1063–1077, 2011.

[56] B. Poonen. Squarefree values of multivariable polynomials. *Duke Math. J.*, 118(2):353–373, 2003.

[57] N. S. Rege. On certain classical groups over Hasse domains. *Math. Z.*, 102:120–1257, 1967.

[58] A. H. Rhemtulla and A. P. Street. Maximal sum-free sets in finite abelian groups. *Bull. Austral. Math. Soc.*, 2:289–297, 1970.

[59] B. P. Rynne and M. A. Youngson. *Linear functional analysis*. Springer Undergraduate Mathematics Series. Springer-Verlag London Ltd., London, 2000.

[60] P. Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[61] P. Sarnak and X. X. Xue. Bounds for multiplicities of automorphic representations. *Duke Math. J.*, 64(1):207–227, 1991.

[62] G. Schul and A. Shalev. Words and mixing times in finite simple groups. *Groups Geom. Dyn.*, 5(2):509–527, 2011.

[63] J.-P. Serre. *Trees*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation.

[64] A. Shalev. Mixing and generation in simple groups. *J. Algebra*, 319(7):3075–3086, 2008.

[65] A. Shalev. Word maps, conjugacy classes, and a noncommutative Waring-type theorem. *Ann. of Math. (2)*, 170(3):1383–1416, 2009.

[66] R. Steinberg. *Lectures on Chevalley groups*. Yale University, New Haven, Conn., 1968. Notes prepared by John Faulkner and Robert Wilson.

[67] R. Stong. The average order of a permutation. *Electron. J. Combin.*, 5:Research Paper 41, 6 pp. (electronic), 1998.

[68] A. Terras. *Fourier analysis on finite groups and applications*, volume 43 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

[69] J. S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1998.