Representation Growth and the Congruence Subgroup Problem

Lachlan Potter

October 2021

A thesis submitted for the degree of Bachelor of Philosophy (Honours) - Science
of the Australian National University

Australian
National
University

For my loving parents

Declaration

The work in this thesis is my own except where otherwise stated.

Lachlan Potter

Acknowledgements

First of all I would like to thank my supervisor, Uri Onn for suggesting the topic of this thesis and for many enlightening discussions. The promise that I would learn a lot has been well and truly fulfilled. More broadly I would like to thank the fantastic lecturers at ANU, from whom I have learnt so much in these four short years.

Thank you to those who volunteered their time to read and give feedback on earlier versions of the thesis. Your comments both positive and negative helped make the thesis what it is.

Thank you to my family, who have always been supportive of whatever I choose to set my mind to. Thank you to my cousins for the Sunday afternoon online game sessions; they always brightened my day. I look forward to seeing you all in person again soon.

Thank you to my partner Chiara for helping me stay sane throughout the year, and thank you to our housemates Griffin and Laura for putting up with us.

Thank you to my friends, who have been a source of joy all year. It would not have been the same without you. A special thank you to Edmund for the countless car trips to bouldering. You're a real one.

Contents

Notation and terminology

Notation

Grp	The category of groups
$\varprojlim_{i \in I} S_i$	The limit over a system indexed by $i \in I$
$(g_i)_i$	a sequence indexed by $i \in I$
Top	The category of topological spaces
Ring	The category of rings
$\mathbb{Z}_p$	The ring of p-adic integers
$\widehat{G}$	The profinite completion of a group/ring G
1	The (multiplicative) identity element in a group/ring. Commonly the identity matrix
$\mathbb{Q}_p$	The field of p-adic numbers
$[G : H]$	The index of H in G
$\operatorname{rk} G$	See Definition 1.19
$d(G)$	See Definition 1.19
$\operatorname{Irr}(G)$	The set of irreducible representations/characters of G
$\operatorname{Irr}_n(G)$	The n-dimensional irreducible representations/characters of G
$\operatorname{Tr}(X)$	The trace of a matrix X
$R^\times$	The group of units of a ring R

$[\bullet, \bullet]$	The group commutator, or the Lie bracket in a Lie algebra
$\mathrm{Res}^G_H(\rho)$	The restricted representation of ρ from G to H
$\mathrm{Ind}^G_H(\rho)$	The induced representation of ρ from H to G
$\mathbb{C}[G]$	The complex group algebra of G
$\otimes_R$	The tensor product over R
$\otimes$	The tensor product over an implicit ring, or one of two tensor products of representations.
$\langle \bullet, \bullet \rangle$	An inner product
X^g	gXg^{-1} where X is a set with a G-action
$H \leq G$	H is a subgroup of G
$H \trianglelefteq G$	H is a normal subgroup of G or an ideal in the case of rings
ρ^g	$\rho^g(x) := \rho(gxg^{-1})$ where ρ is a representation/character
$\mathbb{F}_p$	The finite field on p elements, where p is prime
$\mathrm{char}\, k$	The characteristic of a field k
$\mathfrak{p}$	A prime ideal
$\mathcal{O}$	A ring of integers
$\mathcal{O}_k$	The ring of integers of a field k
$\mathcal{O}_\mathfrak{p}$	$\mathcal{O}$ localised away from $\mathfrak{p}$
$v_\mathfrak{p}$	The valuation associated to a prime ideal $\mathfrak{p}$
$\mathcal{O}_S$	$\mathcal{O}_S$ localised at primes corresponding to valuations in S
k_v	The completion of k with respect to a valuation v
$\mathcal{O}_v$	The completion of $\mathcal{O} \subset k$ with respect to a valuation v
$\mathbb{A}_k$	The adele ring associated to a global field k
$\mathbb{A}_{k,S}$	The restricted adele ring associated to a global field k and a set of valuations S

$G * H$	A central product of groups G and H. The image of $G \times H$ under an isogeny
$Z(G)$	The center of a group G
$\mathrm{Aut}(X)$	The automorphism group of an object X
$G(R)$	For an algebraic group G and ring R see Definition 1.64, with the exception of $R = \mathbb{F}_v$
$\twoheadrightarrow$	Surjective map
$\hookrightarrow$	Injective map
$\xrightarrow{\sim}$	Isomorphism
$r_n(G)$	The number of n-dimensional irreducible representations of G (up to isomorphism)
$R_n(G)$	$\sum_{i=1}^{n} r_i(G)$
$\widehat{r}_n(G)$	The number of finite n-dimensional irreducible representations of G (up to isomorphism)
$\widehat{R}_n(G)$	$\sum_{i=1}^{n} \widehat{r}_i(G)$
$\widehat{\mathrm{Irr}}(G)$	The finite irreducible representations/characters of G
$\widehat{\mathrm{Irr}}_n(G)$	The n-dimensional finite irreducible representations of G
$A_n(G)$	See Definition 2.16
$M_n(R)$	$n \times n$ matrices with elements in a ring (or ideal) R
$\widetilde{G(\mathcal{O}_S)}$	The congruence completion of $G(\mathcal{O}_S)$. See Definition 2.20
V	The set of valuations on a global field k or a vectorspace
V_f	The set of finite valuations on a global field k
V_∞	$V \setminus V_f$
Γ	$G(\mathcal{O}_S)$
C	The congruence kernel of Γ

$\mathfrak{m}_v$	The unique maximal ideal in $\mathcal{O}_v$
$\mathbb{F}_v$	$\mathcal{O}_v/\mathfrak{m}_v$
q_v	$\lvert\mathbb{F}_v\rvert$
p_v	$\operatorname{char}\mathbb{F}_v$
e_v	$\log_{p_v}(q_v)$
$G(\mathbb{F}_v)$	$\operatorname{im}(G(\mathcal{O}_v) \to G(\mathcal{O}_v/\mathfrak{m}_v)) \subset \mathrm{GL}_N(\mathbb{F}_v)$
δ_{ij}	1 if $i = j$, 0 otherwise
$\mathfrak{N}(R)$	The nilpotent radical of a ring R
0	The additive identity in a ring or abelian group
$N_n^{(v)}$	See Definition 3.12
$L^{(v)}$	See Definition 3.14
$L_n^{(v)}$	See Definition 3.14
$\mathcal{P}_1$	See Definition 3.16
$\mathcal{P}_2$	$V_f \setminus \mathcal{P}_1$
$L^{(v)}(H)$	See Definition 3.19
$L_n^{(v)}(H)$	See Definition 3.19
$\mathrm{Rep}(H)$	The set of representations/characters of H
$\mathrm{Rep}_n(H)$	The n-dimensional representations/characters of H
$K_n(H)$	See Definition 3.22
$\mathbb{N}$	$\{1, 2, 3, ...\}$
$R(\Phi)$	See Definition 3.37
$R_K(\Phi)$	See Definition 3.38
$n >> 0$	Placed next to statements that hold for sufficiently large n
C_l	The finite cyclic group of order l

$C_E(W)$	The centraliser of W in E, i.e. $\{e \in E : ew = we \,\forall\, w \in W\}$
$G \rtimes H$	Semidirect product of G and H
E^{p^m}	The (closed) subgroup of E generated by the p^m powers

Terminology

PRG	Polynomial representation growth
CSP	Congruence subgroup property
Topological generating set	A subset $X \subset G$ of a topological group such that the group generated by X is dense in G
Transversal	A choice of coset representatives
Monomial	See Definition 1.41
Local group	$G(\mathcal{O}_v)$, see Terminology 3.11
Global group	$G(\mathcal{O}_S)$
Perfect	G is perfect if $G = [G, G]$
Good primes	See Terminology 3.17
Bad primes	See Terminology 3.17
Lcm	Lowest common multiple
Schur index	See Corollary 3.43
SES	Short exact sequence

Chapter 0

Introduction

Given a group G one can define a sequence $(r_n(G))_{n\in\mathbb{N}}$, where $r_n(G)$ is the number of (isomorphism classes of) n-dimensional irreducible representations of G. The behaviour of this sequence for various groups G is an active area of research. In this thesis we will be interested in the asymptotics of this sequence, specifically the property of polynomial representation growth. A group G is said to have polynomial representation growth if there exists a $c > 0$ such that $r_n(G) \leq cn^c$. One reason to be interested in groups with polynomial representation growth is that they are exactly the groups for which the representation zeta function

$$\zeta_G(s) := \sum_{n=1}^{\infty} r_n(G)n^{-s},$$

has a domain of convergence (see [Klo12]). This potentially allows tools of complex analysis to be brought to bear on the representation theory of G. Special values of this function also have interpretations in other areas of mathematics.

The other main topic of interest is the congruence subgroup property. We introduce it by way of example. Consider $\mathrm{SL}_d(\mathbb{Z})$; the congruence subgroup property is a statement about the structure of its finite index normal subgroups. One way to find a finite index normal subgroup is to consider the kernel of the canonical homomorphism $\mathrm{SL}_d(\mathbb{Z}) \to \mathrm{SL}_d(\mathbb{Z}/m)$, defined by reducing the entries of a matrix modulo m. We call subgroups of this form principal congruence subgroups; as sets they look like

$$\{1 + mX \in \mathrm{SL}_d(\mathbb{Z}) : X \in M_d(\mathbb{Z})\}.$$

Normal subgroups containing a principal congruence subgroup are called congruence subgroups. The group $\mathrm{SL}_d(\mathbb{Z})$ is said to have the congruence subgroup

property if all finite index normal subgroups are congruence subgroups. Joint work of Bass, Lazard and Serre proved that $\mathrm{SL}_d(\mathbb{Z})$ has the congruence subgroup property for $d \geq 3$ [BLS64], however $\mathrm{SL}_2(\mathbb{Z})$ is known not to have the congruence subgroup property.

The congruence subgroup property can be made sense of if we replace SL_d by an algebraic group defined over a global field and $\mathbb{Z}$ by its ring of integers. We use a slight generalisation of this notion in the thesis. For full generality and details see Section 2.3.

In this thesis we follow the work of Alexander Lubotzky and Benjamin Martin in [LM04], which characterises groups with the congruence subgroup property as those with polynomial representation growth. The full characterisation holds in characteristic 0, while in positive characteristic they only prove that groups with the congruence subgroup property have polynomial representation growth. The full characterisation is conjectured to hold in positive characteristic. This is in contrast to other characterisations of the congruence subgroup property by subgroup growth [Lub95] and generation properties of the profinite completion [PR93], which are known to be false in positive characteristic.

In Chapter 1 we will briefly introduce the background concepts of profinite groups, representation theory, number theory and algebraic groups. The reader is encouraged to use this chapter as a reference, to be used when a concept is unknown to them. In particular, the reader familiar with a subset of these topics is encouraged to briefly skim or skip the relevant sections.

In Chapter 2 we will formally introduce the central notions of polynomial representation growth and the congruence subgroup property. In particular we discuss how the former behaves with respect to subgroups and quotients. We discuss the representation theory of profinite groups in detail, generalising results about finite groups to the profinite context. Finally we define the congruence subgroup property in full, address issues of choice and specialise our working definition to our specific scenario.

In Chapter 3 we prove the main Theorem 3.1, which states under mild hypotheses that a group with the congruence subgroup property has polynomial representation growth. In the following suppose G is a semisimple simply connected and connected algebraic group defined over a global field with ring of integers $\mathcal{O}$, and let $\mathcal{O}_v$ be the completion with respect to a valuation v. The congruence subgroup property allows us to establish a link between the finite representations of the global group $G(\mathcal{O})$ and the local groups $G(\mathcal{O}_v)$. The simple ideal structure of $\mathcal{O}_v$ makes the local groups much easier to study. The proof

can be viewed from this perspective as a local-global result, where results in the local case, $G(\mathcal{O}_v)$, are used to prove results in the global case, $G(\mathcal{O})$. We also take two detours into the representation theory of finite groups, where we explore the impact of changing the field over which a representation manifests. In the final section we record some results regarding the image growth of representations. The author makes a small contribution to the literature in the form of Proposition 3.46.

In Chapter 4 we prove Theorem 4.1, a partial converse to Theorem 3.1. The theme of the proof is that groups without the congruence subgroup property have a minimum complexity, from which we can construct enough representations to disprove polynomial representation growth. A conspicuous feature of the proof is that it uses image growth results established in Chapter 3, whose main project runs exactly converse to Chapter 4.

Chapter 1

Background

1.1 Profinite groups

1.1.1 Definition and examples

A slogan to remember is that "a profinite widget is a single widget that packages the information of a system of finite widgets".

To unpack this slogan we begin by defining a system of widgets.

Definition 1.1. A system of groups (G_i, ϕ_{ji}) is a functor from some partially ordered set I to **Grp**. In particular $\phi_{ji} : G_i \to G_j$ when $i \leq j$ in I, and $\phi_{kj} \circ \phi_{ji} = \phi_{ki}$ whenever $i \leq j \leq k$.

Remark 1.2. Concretely this amounts to a subcategory of **Grp** such that there is at most one map between any two objects. To define a system of sets or rings switch **Grp** with the category of choice.

Now we introduce the object that packages the information of a system.

Definition 1.3. The (categorical) limit over a system of sets (S_i, ϕ_{ji}) is defined as

$$\varprojlim_{i \in I} S_i := \left\{ (s_i) \in \prod_{i \in I} S_i : i \leq j \implies \phi_{ji}(s_i) = s_j \right\}.$$

The elements of this set are referred to informally as compatible sequences. This definition is often referred to as a projective or inverse limit in the literature.

The limit comes implicitly with projection maps $\pi_i : \varprojlim_{i \in I} S_i \to S_i$. The sense in which a limit packages the information in a system is captured by the following universal property.

Fact 1.4. For any set S and compatible maps $\{\phi_i : S \to S_i \,|\, i \in I\}$ in the sense that $\phi_{ji} \circ \phi_i = \phi_j$ for all $i \leq j$, there exists a unique map $\phi : S \to \varprojlim_{i \in I} S_i$ that is compatible in the sense that $\phi_i = \pi_i \circ \phi$.

The construction and universal property of the limit generalise to **Grp** and **Top**. In **Grp** all maps are group homomorphisms, and the group operation on the limit is defined coordinate-wise. In **Top** all maps are continuous, and the limit is given the topology induced as a subset of the product. Typically this construction will work when the objects in the category are sets with added structure, though we will only need it for the categories of **Grp**, **Top** and **Ring**.

Definition 1.5. A topological group is profinite if it is the (categorical) limit over a system of finite groups (G_i, ϕ_{ji}).

$$G = \left\{ (g_i)_i \in \prod_{i \in I} G_i : \phi_{ji}(g_i) = g_j \right\},$$

where the finite groups G_i are given the discrete topology.

Results and definitions for finite groups are often readily generalised to profinite groups. An example is the following.

Definition 1.6. A pro-p (resp. pronilpotent) group is a profinite group that is a limit over a system of finite p-groups (resp. finite nilpotent groups).

To bring this definition down to earth we give some examples. Finite groups and infinite products of finite groups are simple examples of profinite groups. The following example however captures more of the general behaviour and is considered by many as the quintessential example of a profinite group.

Example 1.7. The p-adic integers, $\mathbb{Z}_p$ are a profinite (in fact pro-p) group. They are the limit over the following system of finite groups:

$$\cdots \to \mathbb{Z}/p^k \to \cdots \to \mathbb{Z}/p^3 \to \mathbb{Z}/p^2 \to \mathbb{Z}/p,$$

where the map between any two adjacent groups is the canonical reduction map.

The p-adics are also defined as the set of "power series in p" with the logical addition and topology induced by the p-adic norm

$$\mathbb{Z}_p := \left\{ \sum_{i=0}^{\infty} a_i p^i : a_i \in \{0, 1, 2, ..., p-1\} \right\}.$$

One can reconcile these two definitions by taking truncations of these power series as a family of compatible maps $\pi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i$, then proving that $\mathbb{Z}_p$ satisfies the universal property. Furthermore the profinite topology on $\mathbb{Z}_p$ is equivalent to the topology induced by the p-adic norm on $\mathbb{Z}_p$.

Given that $\mathbb{Z}/p^k$ is a ring, not just a group, $\mathbb{Z}_p$ is also an example of a profinite ring.

Joke 1.8. p-adic integers are $\lim_{n\to\infty}(1+1/n)^n$ $\mathbb{Z}_p$ $\mathbb{Z}$.

1.1.2 Topological properties

So far the topology on profinite groups has been treated as an afterthought, however it is critically important. In fact there is a purely topological characterisation of profinite groups.

Theorem 1.9. *A topological group is profinite if and only if it is compact and totally disconnected.*

Proof Sketch. See [RV13, Theorem 1-14] for a full proof.

First one notices that the limit is a closed subset of a product of finite discrete spaces, which is compact, Hausdorff and totally disconnected. Therefore any profinite group is compact and totally disconnected.

For the converse one constructs the profinite completion (See Definition 1.14) of a compact totally disconnected group G and uses the topological conditions (and a lot of work) to show that the canonical map $G \to \widehat{G}$ is indeed an isomorphism of topological groups. □

This topological characterisation is actually useful in proving things about the category of profinite groups.

Proposition 1.10. *The category of profinite groups is closed under products, closed subgroups and quotients by closed normal subgroups. The profinite topology agrees with the product/subspace/quotient topology in each case.*

Proof sketch. Given two profinite groups, the product is simply the limit over the "disjoint union" of the two systems.

See [RV13, Theorem 1-18] for the treatment of subgroups and quotients. □

When dealing with profinite groups (and topological groups more generally) it is natural to require subgroups to be topologically closed. As such from this point on any subgroup of a profinite group will be closed, unless otherwise stated.

The open subgroups of a profinite group have a nice characterisation.

Lemma 1.11. *The open subgroups of a profinite group are exactly the closed subgroups of finite index.*

Proof. See [RV13, Theorem 1-18]. Of note is that the proof is simply a combination of facts about topological groups paired with the topological characterisation of profinite groups. □

Furthermore the open subgroups completely determine the topology.

Lemma 1.12. *[RV13, Lemma 1-17]. The open normal subgroups are a basis around 1 for the topology of any profinite group.*

Remark 1.13. A basis around 1 for a topological group completely defines the topology because it can be transported (via the group multiplication) to give a basis at any point.

1.1.3 Profinite completion

A construction we will use extensively in this thesis is the profinite completion.

Definition 1.14. Given some group G, we define the profinite completion $\widehat{G}$ to be the limit over the system of finite quotients G/N (given the discrete topology) along with the maps $G/N \to G/M$ whenever $N \subset M$. We denote this

$$\widehat{G} := \varprojlim_{[G:N]<\infty} G/N.$$

This construction will be important to us because we will often care only about the finite quotients of a group. This construction packages that information nicely for us as a universal property, which we develop now.

Lemma 1.15. *There is a natural map*

$$\eta : G \to \widehat{G},\ g \mapsto (gN)_N.$$

The image of η is dense in $\widehat{G}$, and if G is profinite, then η is an isomorphism.

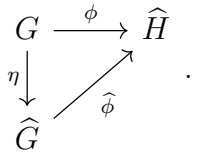
Proof Sketch. See the proof of [RV13, Lemma 1-15] for details.

The idea is to use the coarseness of the topology on $\widehat{G}$ to prove that the image of η is dense. Then if G is profinite it is compact and so η must be surjective.

Using total disconnectedness it follows by some elementary (but involved) topology to show that if G is profinite then $\ker \eta$ is trivial. □

We can now state the universal property of $\widehat{G}$.

Fact 1.16. For any group homomorphism $\phi : G \to \widehat{H}$ where $\widehat{H}$ is a profinite group, there is a unique continuous group homomorphism $\widehat{\phi} : \widehat{G} \to \widehat{H}$ such that the following diagram commutes.



We will use this construction later to study the finite representations of groups, but for now we zoom in on a particular type of profinite group.

1.1.4 p-adic analytic groups

One particular type of profinite group that will come up mostly in the final chapter of the thesis are p-adic analytic groups. This is a large topic that one could write books on (and indeed we cite one of them), so we will only give the barest detail necessary to understand the thesis.

We will informally define p-adic analytic groups as "groups that locally look like $(\mathbb{Z}_p)^n$". Recall that $\mathbb{Z}_p$ is the unit ball in $\mathbb{Q}_p$, which makes p-adic analytic groups the analogues of Lie groups for the field $\mathbb{Q}_p$. We will not rigorously define them this way, but a treatment can be found in [DDSMS03, Chapter 8]. We will instead use some of their various equivalent characterisations. See [DDSMS03, Interlude A].

Definition 1.17. Let G be a pro-p group. The following are equivalent:

(a) G is p-adic analytic;

(b) G has finite rank;

(c) $[G : G^{p^k}]$ grows polynomially in k;

(d) G is isomorphic to a closed subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$.

Remark 1.18. $\mathrm{GL}_n(\mathbb{Z}_p)$ inherits a topology from $(\mathbb{Z}_p)^n$ in much the same way that $\mathrm{GL}_n(\mathbb{R})$ has the structure of a Lie group. See [DDSMS03, Section 5.1] for details.

To make sense of (b) we must define the rank of a profinite group.

Definition 1.19. The rank of a profinite group G is defined to be

$$\operatorname{rk} G := \sup\{d(H) : H \leq G\},$$

where $d(H)$ is the minimal cardinality of a topological generating set for H.

1.2 Representation theory

Everything in this section can be found in [Ser77, Chapters 1-3] and [Isa94, Chapters 4-5]. We set up conventions that will be used later in the thesis and stress parts of the theory that will be of particular use to us.

1.2.1 General definitions

Representation theory can broadly be thought of as a method of "linearising" mathematical objects. The motivating principal is that questions about linear algebra are often far easier to answer than questions about other mathematical objects. In group theory this amounts to studying groups via their actions on vector spaces.

Definition 1.20. A representation of a group G in a vector space V is simply a group homomorphism $\rho : G \to \mathrm{GL}(V)$. Whenever G has a topology we require ρ to be continuous. We will sometimes refer to a representation as a tuple (ρ, V) and sometimes only as one of ρ or V when the other is clear from context.

In this section we will discuss the representation theory of finite groups over finite-dimensional complex vector spaces specifically, though in the thesis we will use many of these constructions for infinite groups. All representations in this thesis will be in finite-dimensional vector spaces and over the complex numbers unless otherwise stated.

A perk of working with finite groups is that representations can always be decomposed into direct sums of irreducible representations.

Definition 1.21. A representation of a group G is irreducible (an irrep or an irreducible) if it does not admit a nontrivial G-invariant subspace.

Notation 1.22. We write $\mathrm{Irr}(G)$ for the set of irreps of G up to isomorphism and $\mathrm{Irr}_n(G)$ for the set of irreps of dimension n.

While the full data of a representation is nice to have, a lot of it is captured by a much smaller piece of data known as a character.

Definition 1.23. Given a representation (ρ, V) the associated character is simply the **function**

$$\chi : G \to \mathbb{C},\ g \mapsto \mathrm{Tr}(\rho(g)).$$

If ρ is irreducible we call χ an irreducible character.

Characters are generally **not** group homomorphisms. Due to properties of the trace, characters are constant on conjugacy classes of G. Such functions are called **class functions**. The character theory for representations of finite groups is well trodden, we give a summary of the basic results below

Theorem 1.24. *[Ser77, Theorems 4,6] The irreducible characters of G form an orthonormal basis for the class functions on G with respect to the following inner product:*

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

The decomposition a character into irreducible characters corresponds exactly to the decomposition of the representation into irreducibles.

Terminology 1.25. Given the tight correspondence between representations and characters we will often play fast and loose with the distinction between a character and a representation. The correct interpretations should always be clear from context.

The case of one-dimensional representations is particularly important. When a representation is one-dimensional the character and representation effectively coincide, since $\mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times \subset \mathbb{C}$. In this case the character **is** a group homomorphisms into $\mathbb{C}^\times$. Every one-dimensional representation of a group G factors through the abelianisation $G/[G,G]$. In particular G admits exactly $[G : [G,G]]$ one-dimensional representations. [Ser77, Theorem 9 and Corollary 2].

The representation theory of a group can be linked to the representation theory of its subgroups via the operations of restriction and induction.

Definition 1.26. If $H \leq G$ and (ρ, V) is a representation of G then $\mathrm{Res}^G_H(\rho)$ (sometimes denoted $\rho|_H$) is simply the representation $(\rho|_H, V)$.

Definition 1.27. If $H \leq G$ and (ρ, V) is a representation of H then $\mathrm{Ind}^G_H(\rho)$ is a representation of G on the vector space $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$, where G acts by

$$\mathrm{Ind}^G_H(\rho)(g)(x \otimes v) := gx \otimes v.$$

The above definition is very convenient for establishing the theory. The following construction is equivalent, but will be useful for computations. Take a transversal $g_1, ..., g_r$ of H in G, then consider the vector space

$$\bigoplus_{i=1}^{r} g_i V = \left\{ \sum_{i=1}^{r} g_i v_i : v_i \in V \right\}.$$

Writing $gg_i = g_j h$ for all i we let $g \in G$ act on this vector space by

$$\mathrm{Ind}_H^G(g) g_i v_i := g_j \rho(h) v_i.$$

In particular g acts by first sending the i-th factor to the j-th, then acting by h according to ρ. Given this definition it is clear to see that induction scales dimension by the index of the subgroup.

Notation 1.28. We will apply Ind_H^G and Res_H^G to characters as well as representations. This should be clear from context.

Remark 1.29. These constructions work for infinite groups if $[G : H] < \infty$.

Res_H^G and Ind_H^G are not inverses, but they are adjoint in the following way.

Theorem 1.30 (Frobenius Reciprocity)**.** *[Ser77, Theorem 13] If ψ is a character of a representation on H and χ a character of a representation of G then*

$$\langle \psi, \mathrm{Res}_H^G \chi \rangle = \langle \mathrm{Ind}_H^G \psi, \chi \rangle,$$

where the inner products are as described in 1.24 on the relevant space of class functions.

One fact which we save now for use much later in the thesis is regarding the kernel of induced representations. Certainly $\ker(\mathrm{Res}_H^G(\rho)) = \ker(\rho) \cap H$. For induced representations we have the following.

Lemma 1.31. $\ker(\mathrm{Ind}_H^G(\rho)) = \bigcap_{g \in G} (\ker(\rho))^g$*, in particular*

$$[H : \ker \rho] \leq \frac{[G : \ker(\mathrm{Ind}_H^G(\rho))]}{[G : H]}.$$

Proof. This is [Isa94, Lemma (5.11)], the inequality comes easily from the fact that $\ker \rho \supset \bigcap_{g \in G} (\ker(\rho))^g$. □

The last thing we need before leaving the purview of a first course in representation theory is a result on the representation theory of products.

Definition 1.32. If (ρ_1, V_1) and (ρ_2, V_2) are representations of G_1 and G_2 respectively then $\rho_1 \otimes \rho_2$ is a representation of $G_1 \times G_2$ on the vector space $V_1 \otimes V_2$ given by the action

$$(g_1, g_2) \cdot (v_1 \otimes v_2) = g_1 v_1 \otimes g_2 v_2.$$

Theorem 1.33. *[Ser77, Theorem 10] The irreducible representations of a product of finite groups $G_1 \times G_2$ are exactly the representations of the form $\rho_1 \otimes \rho_2$ where ρ_i is an irreducible representation of G_i.*

Remark 1.34. This is a different representation to that of the tensor product of two representations of the same group G. Though we use the same notation, the construction will be clear from context. It will almost always be the one outlined above.

1.2.2 Clifford theory

While the operations of induction and restriction give us a way to move between representations of a group G and a finite index subgroup H, the correspondence is not always easy to describe. There may be distinct irreps of H that induce to the same irrep of G, furthermore the induction of an irrep of H may split into a sum of distinct irreps of G. The same issues are the case with restriction. We aim for a better understanding of this question in the case that H is normal in G.

In this case conjugation gives an action of G on the representations of H, and thus the characters. There is a meaningful symmetry with respect to this action when restricting irreps of G to H.

Theorem 1.35. *[Isa94, Theorem 6.2] Suppose H is normal in G. Suppose χ is a character of an irreducible representation of G, and let $\rho \leq \mathrm{Res}^G_H(\chi)$ be the character of an irreducible component of the representation restricted to H.*

If $g_1, ..., g_t$ is a transversal for H in G, then

$$\mathrm{Res}^G_H(\chi) = e \sum_{i=1}^{[G:H]} \rho^{g_i},$$

where $e = \langle \mathrm{Res}^G_H(\chi), \rho \rangle$ and $\rho^{g_i}(h) := \rho(g_i h g_i^{-1})$.

Given the correspondence between characters and representations, this describes the structure of an irreducible representation restricted to a normal subgroup.

Remark 1.36. There is an unimportant but fascinating analogy between the decomposition of representations restricted to normal subgroups, and the way primes split in Galois extensions of number fields. In the representation theory case all conjugate representations occur an equal number of times in the decomposition, while in the number theory case all primes in the decomposition have the same ramification index and inertial degree. In some sense the action of G by conjugation corresponds to the action of the Galois group of the field extension.

While this is a nice result, it still does not do very much to tease apart the relationship between representations of G and H. It turns out we can further exploit the action of G on the characters of H to construct an intermediate subgroup $H \trianglelefteq T \trianglelefteq G$, for which the correspondence between characters of T and G is transparent.

We are abuse notation by writing $\mathrm{Irr}(G)$ to denote the irreducible characters of G.

Theorem 1.37. *[Isa94, Theorem 6.11] Suppose $H \trianglelefteq G$. Let $\rho \in \mathrm{Irr}(H)$ be an irreducible character. Define the inertial subgroup T of G corresponding to ρ as*

$$T := \{g \in G : \rho(ghg^{-1}) = \rho(h)\, \forall h \in H\}.$$

Now let

$$A = \{\psi \in \mathrm{Irr}(T) : \langle \mathrm{Res}^T_H(\psi), \rho\rangle \neq 0\}$$

$$B = \{\chi \in \mathrm{Irr}(G) : \langle \mathrm{Res}^G_H(\chi), \rho\rangle \neq 0\}.$$

Then $\psi \mapsto \mathrm{Ind}^G_T(\psi)$ is a bijection from A to B.

So, given any irrep of H, there is some inertial subgroup $H \trianglelefteq T \trianglelefteq G$ such that the irreducibles of G and T, whose restriction contain a copy of ρ, are in bijection with one another via induction.

Remark 1.38. Lovers of the analogy to number theory can view the inertial subgroup as a result in the spirit of the decomposition and inertial fields. See [Ste12, Chapter 8].

1.2.3 Representations of nilpotent groups

A useful application of the results of Clifford theory are results regarding the representation theory of nilpotent groups.

Definition 1.39. A finite group is nilpotent if its lower central series terminates. That is for some n we have

$$G =: G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\},$$

where $G_{i+1} = [G, G_i]$.

Example 1.40. p-groups are nilpotent.

Nilpotent groups can be viewed as a generalisation of abelian groups. Given that all irreducible representations of abelian groups are one-dimensional, we can expect the representation theory of nilpotent groups to have a one-dimensional flavour to it. The way in which we describe this one-dimensionality is through the concept of monomiality.

Definition 1.41. A group G is monomial if all irreducible representations of G are induced from one-dimensional representations. Similarly we define a monomial representation to be one that is induced from a one-dimensional representation, and a monomial matrix to be a matrix with at most one nonzero entry in each row and column.

The definition of a monomial matrix is no accident. If χ is a one-dimensional representation of H and one takes a basis B of $\mathrm{Ind}_H^G(\chi)$ respecting the direct sum decomposition, the matrices $\mathrm{Ind}_H^G(\chi)(g)$ with respect to B are monomial.

Theorem 1.42. *[Isa94, Corollary 6.14] Nilpotent groups are monomial.*

We will take a particular interest in monomial representations, as they are both easy to count and construct.

1.3 Number theory

1.3.1 Valuations and completions

This thesis will leverage heavily the theory of valuations and completions of global fields. For the sake of brevity we give what is hopefully a fulfilling sketch of the ideas without proofs, followed by a concrete example also without proofs. Details can be found in [Neu13, Chapter II Sections 1-5].

Definition 1.43. A global field is a finite field extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$.

For global fields k we will be interested in valuations on k, which can be thought of as multiplicative norms.

Definition 1.44. A valuation on a global field k is a function

$$|\cdot| : k \to \mathbb{R}_{\geq 0},$$

satisfying:

- $|x| \geq 0$ and $|x| = 0 \iff x = 0$;
- $|xy| = |x||y|$;
- $|x + y| \leq |x| + |y|$.

Any valuation on k turns it into a metric space, and we say that two valuations are **equivalent** if they induce the same topology on k. We ignore any valuations that induce the discrete topology.

One way to construct a valuation on a global field is to take an embedding $\sigma : k \to \mathbb{C}$, followed by the standard norm on $\mathbb{C}$. This is only possible if $\operatorname{char} k = 0$. We call such valuations **archimedean**.

Another way to construct valuations on k is to consider prime ideals $\mathfrak{p}$ in the ring of integers $\mathcal{O}$ of k. Since $\mathcal{O}$ is a Dedekind domain the localisation $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring, meaning it has a unique maximal ideal and the maximal ideal is principal.

A consequence of this is that if π generates the maximal ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p} \lhd \mathcal{O}_\mathfrak{p}$, then every $x \in k^*$ has a unique expression as $x = u\pi^n$ with $u \in \mathcal{O}_\mathfrak{p}^\times$ and $n \in \mathbb{Z}$ [Ste12, Theorem 2.17]. We define the valuation $v_\mathfrak{p}$ associated to $\mathfrak{p}$ as

$$v_\mathfrak{p} : k \to \mathbb{R},\ v_\mathfrak{p}(x) := \begin{cases} r^n, & \text{if } x = u\pi^n \\ 0, & \text{if } x = 0, \end{cases}$$

where $0 < r < 1$. Intuitively if you lie in high powers of the maximal ideal you have small norm. We call such valuations **non-archimedean**.

Remark 1.45. In the finite characteristic case there are also valuations which arise from the valuation on $\mathbb{F}_p(t)$ that counts the relative degree of the numerator and denominator of a rational function. These valuations are considered archimedean, though there is no associated prime ideal. The following analysis will not apply to valuations of this type.

Archimedean valuations satisfy the strong triangle inequality, meaning that

$$|x+y| \leq \max\{|x|, |y|\}.$$

Many texts use this as a characterising property of non-archimedean valuations. This allows us to characterise many subsets of the ring $\mathcal{O}_\mathfrak{p}$ geometrically:

$$\begin{aligned}\mathcal{O}_\mathfrak{p} &= \{x \in k : v_\mathfrak{p}(x) \leq 1\},\\ \mathfrak{p}\mathcal{O}_\mathfrak{p} &= \{x \in k : v_\mathfrak{p}(x) < 1\},\\ \mathcal{O}_\mathfrak{p}^\times &= \{x \in k : v_\mathfrak{p}(x) = 1\}.\end{aligned}$$

As the terminology would suggest, all valuations on a global field are either archimedean or non-archimedean.

Remark 1.46. If we localise $\mathcal{O}$ at a finite set of primes S we get a ring $\mathcal{O}_S$ of S-integers as defined in Section 3.1. The non-archimedean valuations on this ring are exactly the non-archimedean valuations on $\mathcal{O}$ after removing the valuations corresponding to primes in S.

Given any non-archimedean valuation v on k, we can complete k with respect to the induced metric by taking as elements Cauchy sequences up to an equivalence relation (as one would complete a metric space). The completion is naturally a field. This should not be surprising because valuations are defined to behave well with respect to both the addition and multiplication on k. We denote such a completion by k_v and refer to such fields as **local fields**. A way to remember this is that the completion of the ring of integers $\mathcal{O}_v \subset k_v$ is a local ring.

One can also complete with respect to an archimedean metric, which always yields $\mathbb{R}$ or $\mathbb{C}$. [Neu13, Chapter II Theorem 4.2].

Notation 1.47. The localisation of $\mathcal{O}$ at a specific prime will always be written $\mathcal{O}_\mathfrak{p}$, while the completion of $\mathcal{O}$ with respect to the corresponding valuation will be written $\mathcal{O}_{v_\mathfrak{p}}$. If the prime itself is unimportant or unspecified we simplify the latter to $\mathcal{O}_v$. Given the close correspondence between primes $\mathfrak{p}$ and valuations v we will use the more explicit notation whenever there is danger of confusion.

1.3.2 Example: the p-adics

We now aim to make this theory more concrete by working through an example.

Consider $k = \mathbb{Q}$, its ring of integers is $\mathcal{O} = \mathbb{Z}$. Let p be a prime number, then let $(p) \triangleleft \mathbb{Z}$. We wish to construct the non-archimedean valuation $v_{(p)} = |\cdot|_p$ (we will use both notations as convenient) associated to $(p) \triangleleft \mathbb{Z}$. First we note that

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : b \notin (p) \right\}.$$

In words these are the rational numbers with no factors of p in the denominator. Writing any nonzero rational number $x \in \mathbb{Q}^\times$ in reduced form we have that $x = \frac{a}{b}p^n$ where a and b are coprime to p, and $n \in \mathbb{Z}$. This means $\frac{a}{b} \in (\mathbb{Z}_{(p)})^\times$. Let $0 < r < 1$, then we define $v_p(x) = r^n$.

We have the following geometric characterisations:

$$\begin{aligned}
\mathbb{Z}_{(p)} &= \left\{ \frac{a}{b} \in \mathbb{Q} : b \notin (p) \right\} = \{x \in \mathbb{Q} : |x|_p \leq 1\}, \\
p\mathbb{Z}_{(p)} &= \left\{ \frac{a}{b} \in \mathbb{Q} : b \notin (p) \text{ and } a \in (p) \right\} = \{x \in \mathbb{Q} : |x|_p < 1\}, \\
(\mathbb{Z}_{(p)})^\times &= \left\{ \frac{a}{b} \in \mathbb{Q} : a, b \notin (p) \right\} = \{x \in \mathbb{Q} : |x|_p = 1\}.
\end{aligned}$$

We now denote the completion with respect to $|\cdot|_p$ of $\mathbb{Q}$ by $\mathbb{Q}_p$ and $\mathbb{Z}$ by $\mathbb{Z}_p$. In the notation of the previous subsection these are $\mathbb{Q}_{v_{(p)}}$ and $\mathbb{Z}_{v_{(p)}}$. Currently these are sets containing Cauchy sequences up to an equivalence relation, but we have seen $\mathbb{Z}_p$ before in Example 1.7. We now reconcile the two definitions by explaining how to get a Cauchy sequence from a power series in p.

Suppose we have some $\sum_{i=0}^{\infty} a_i p^i$ with $a_i \in \{0, 1, ..., p-1\}$. Construct a sequence (x_n) by

$$x_n := \sum_{i=0}^{n} a_i p^i.$$

This sequence is clearly a sequence in $\mathbb{Z}$ which is Cauchy in $|\cdot|_p$. Similarly if we have a Laurent series $\sum_{i=-N}^{\infty} a_i p^i$ in p, we get a sequence in $\mathbb{Q}$ which is Cauchy in $|\cdot|_p$. This gives us a realisation of $\mathbb{Q}_p$ as

$$\mathbb{Q}_p := \left\{ \sum_{i=-N}^{\infty} a_i p^i : N \in \mathbb{N},\ a_i \in \{0, 1, ..., p-1\} \right\}.$$

with the natural addition and multiplication.

If $\operatorname{char} k = 0$ with v a non-archimedean valuation, then k_v is a field extension of $\mathbb{Q}_p$, and $\mathcal{O}_v \cong \mathbb{Z}_p^n$ as $\mathbb{Z}_p$-modules, for some p. Generally if v corresponds to a prime ideal then $\mathcal{O}_v$ is a profinite ring. [Neu13, Proposition (4.5)].

1.3.3 Adeles

The last thing to mention in this section, which will come up briefly in the thesis are the adele and restricted adele rings. An adele ring is best thought of as a ring that packages the information contained in all completions of a global field k.

Definition 1.48. Let k be a global field and V the set of valuations on k (up to equivalence). The adele ring associated to k is defined as the restricted product

$$\mathbb{A}_k = \left\{ (x_v) \in \prod_{v \in V} k_v : x_v \in \mathcal{O}_v \text{ for all but finitely many } v \in V \right\}.$$

The addition and multiplication in this ring are defined coordinate-wise. The topology is defined by declaring sets of the form $\prod_{v \in V} U_v$, where U_v is open in k_v and $U_v = \mathcal{O}_v$ for all but finitely many v to be a basis.

The fact that we have not defined $\mathcal{O}_v$ when v does not have an associated prime ideal is not a problem, since there are only finitely many such valuations.

If $S \subset V$ (usually finite) then we define the restricted adeles.

Definition 1.49.

$$\mathbb{A}_{k,S} = \left\{ (x_v) \in \prod_{v \in V \setminus S} k_v : x_v \in \mathcal{O}_v \text{ for all but finitely many } v \in V \right\}.$$

It inherits a topological ring structure in exactly the same way as $\mathbb{A}_k$.

Remark 1.50. The canonical maps $\mathcal{O} \to \mathcal{O}_v$ make $\mathbb{A}_k$ an $\mathcal{O}$-algebra.

Joke 1.51. One can find some fantastic visualisations of $\mathbb{A}_{\mathbb{Q}}$ if one searches "hello adele" in Google.

1.4 Algebraic groups

1.4.1 Over an algebraically closed field

In this section we will provide the bare minimum background on algebraic groups, so that the reader may understand the rest of the thesis.

For any algebraically closed field K we can give $M_n(K)$ the Zariski topology by identifying it with K^{n^2}. The reader yet unacquainted with the Zariski topology is invited to familiarise themselves by reading [Hum12, Chapter 1].

Definition 1.52. An algebraic group $G(K)$ (often called a linear algebraic group) over K is a Zariski closed subgroup of $\mathrm{GL}_n(K)$, where $\mathrm{GL}_n(K)$ is given the structure of affine variety via the inclusion into $\mathrm{SL}_{n+1}(K)$

$$g \mapsto \begin{pmatrix} g & 0 \\ 0 & (\det g)^{-1} \end{pmatrix},$$

the image being a Zariski closed subset of $\mathrm{SL}_{n+1}(K)$.

In practice this is as a subgroup of $\mathrm{GL}_n(K)$ defined by polynomial equations in the entries.

Examples 1.53. Inside $\mathrm{GL}_n(K)$, the following are examples of algebraic groups:

- $\mathrm{GL}_n(K)$;
- $\mathrm{SL}_n(K)$;
- Upper triangular matrices;
- Diagonal matrices.

Another class of examples come from taking all invertible matrices that preserve a given bilinear form. Examples of these are $O_n(K)$ and $\mathrm{Sp}_{2n}(K)$.

Now we will begin defining the types of algebraic groups we are particularly interested in, and their classification.

Definition 1.54. A connected algebraic group is called semisimple if it has no nontrivial, closed, connected solvable subgroups.

In general when one sees the term semisimple, it means that the object is somehow built out of simple objects.

Definition 1.55. A connected algebraic group is simple if it is non-abelian and has no proper, nontrivial, connected normal subgroups.

A consequence of this definition is that every closed, proper, normal subgroup of a connected simple algebraic group is finite and central.

We are still yet to justify our definition of semisimple. We do so with the following theorem.

Theorem 1.56. *A semisimple algebraic group $G(K)$ is isomorphic to a central product of simple algebraic groups*

$$G(K) \cong S_1(K) * \cdots * S_l(K),$$

where the factors S_i are unique up to reordering.

In particular $G(K)$ is a quotient of $S_1(K) \times \cdots \times S_l(K)$ by some (finite) central subgroup. Central quotients will occur often, so it will be useful to have the following definition.

Definition 1.57. An isogeny is a map that quotients an algebraic group by some finite central subgroup.

We can now state a powerful classification theorem.

Theorem 1.58. *Every simple algebraic group belongs to exactly one of the following Lie types:*

$$A_n\ (n \geq 1),\ B_n\ (n \geq 2),\ C_n\ (n \geq 3),\ D_n\ (n \geq 4),\ E_6,\ E_7,\ E_8,\ F_4,\ G_2.$$

Furthermore for every Lie type H there is a group G_{sc}, which we call ***simply connected****, with the property that any simple algebraic group of Lie type H is the image of G_{sc} under an isogeny.*

The simply connected terminology makes sense if one views an isogeny as a covering space map. In this sense G_{sc} is the universal cover of all groups of a fixed Lie type.

A few words on this theorem are in order before we give some examples. Of note is that the theorem is independent of our choice of algebraically closed field K. The proof leverages the fact that one can define the Lie algebra $L = L(G)$ of an algebraic group. If G is simple the action of conjugation on $L(G)$ embeds $G/Z(G)$ into $\mathrm{Aut}(L)$. Therefore once $L(G)$ is known, G is determined up to an isogeny. There is of course a *lot* of detail being skimmed over here, but the familiar reader will notice the similarity to the classification theory for Lie groups.

Examples 1.59. Examples of simply connected simple algebraic groups are:

- $\mathrm{SL}_n(K)$ is simply connected of type A_{n-1};
- $\mathrm{Sp}_{2n}(K)$ is simply connected of type C_n.

Examples 1.60. Examples of simple algebraic groups are:

- $\mathrm{SO}_n(K)$ is simple of type $B_{(n-1)/2}$ or $D_{n/2}$ depending on the parity of n. Its simply connected double cover (for $n \neq 2$) is the spin group $\mathrm{Spin}(n)$;
- $\mathrm{PSL}_n(K)$ is simple of type C_n. The isogeny $\mathrm{SL}_n(K) \twoheadrightarrow \mathrm{PSL}_n(K)$ has kernel consisting of scalar matrices with determinant 1, so elements of the kernel correspond to n-th roots of unity in K. If K is algebraically closed and characteristic 0 this will be of size n.

The last thing we need to do is generalise the notion of simply connected to semisimple groups.

Definition 1.61. A semisimple algebraic group is simply connected if it is the finite product of simply connected algebraic groups.

Now due to Theorem 1.58 we have that every semisimple algebraic group is the image under an isogeny of a unique simply connected semisimple group.

1.4.2 Changing the ring of definition and the Lie algebra

We will often want to work with algebraic groups over non-algebraically closed fields and their rings of integers. In this subsection we will set up the framework with which to do this.

The observant reader will note times in the previous section where we simply wrote G rather than $G(K)$ to denote an algebraic group. While this is not strictly correct, it points towards the theory we are about to develop. It is often beneficial to view G as a subfunctor of GL_n, which can take in certain rings and spit out the relevant groups. Given any algebraic group $G(K)$ over K we can construct such a subfunctor, which we will also call an algebraic group. We will denote this by $G \leq \mathrm{GL}_n$ to maintain a level of distinction. Whenever discussing simplicity or simply connectedness of G we will always mean $G(K)$. This point of view will allow us to make sense of the correct generalisation of $\mathrm{SL}_n(\mathbb{Z})$.

The first thing to notice is that the defining equations of an algebraic group $G(K)$ have coefficients in K. These coefficients present a fundamental restriction on the types of rings A over which we can make sense of $G(A)$.

Definition 1.62. Given some subring $R \subset K$ and an algebraic group over K, $G(K) \leq \mathrm{GL}_n(K)$, we say that G is defined over R if there exists a set of defining equations for $G(K)$ with coefficients in R.

Example 1.63. The algebraic group $\mathrm{SL}_n(\mathbb{C})$ is defined over $\mathbb{Z} \subset \mathbb{C}$, since the coefficients of the determinant consist only of ± 1.

Now we define the subfunctor $G \leq \mathrm{GL}_n$ associated to an algebraic group $G(K)$ defined over $R \subset K$.

Definition 1.64. Let $G(K) \leq \mathrm{GL}_n(K)$ be an algebraic group defined over a subring $R \subset K$. Let $f_1, ..., f_r \in R[x_1, .., x_{n^2}]$ be a set of defining equations for G.

For any commutative unital R-algebra A we can naturally define the polynomials $\widetilde{f}_1, ..., \widetilde{f}_r \in A[x_1, ..., x_{n^2}]$ by mapping the coefficients into A. We define $G(A)$ as the solutions in A to $\widetilde{f}_1, ..., \widetilde{f}_r$, such that the inverse also has entries in A. For any map $\phi : A \to B$ of R-algebras we have an induced map $G(A) \to G(B)$ given by applying ϕ to the entries of a matrix. As such one can view G as a functor from R-algebras to **Grp**. We call this functor an algebraic group defined over R and denote it by $G \leq \mathrm{GL}_n$.

Remark 1.65. Note that if A is some intermediate ring $R \subset A \subset K$ then our definition above simplifies to $G(A) := \mathrm{GL}_n(A) \cap G(K)$.

Example 1.66. Suppose $G(K) \leq \mathrm{GL}_n(K)$ is defined over some number field $k \subset K$. Scaling the defining equations we see that $G(K)$ is defined over $\mathcal{O}$. This allows us to consider the points of G over any $\mathcal{O}$-algebra. In particular we can now make sense of $G(\mathcal{O}/I)$, $G(\mathcal{O}_S)$, $G(k_v)$, $G(\mathbb{A}_{k,S})$ and $G(\mathcal{O}_v)$.

The last thing we have to introduce is the Lie algebra associated to G. There is again a lot that could be said on this topic, so we attempt to give the minimum that will make the thesis understandable. We take the subfunctor point of view when defining the Lie algebra of an algebraic group.

Definition 1.67. If $G \leq \mathrm{GL}_n$ is an algebraic group defined over some ring R, then for any R-algebra A, the Lie algebra over A can be defined as the set

$$\ker(G(A[\varepsilon]/\varepsilon^2) \to G(A)) = \{1 + \varepsilon M \in G(A[\varepsilon]/\varepsilon^2) : M \in M_n(A)\}.$$

The map on groups is induced by the map $A[\varepsilon]/\varepsilon^2 \to A$, sending ε to 0.

We define addition on this Lie algebra as multiplication in the group or "addition of the ε components", given that

$$1 + \varepsilon(M + N) = (1 + \varepsilon M)(1 + \varepsilon N) \in G(A[\varepsilon]/\varepsilon^2).$$

The Lie bracket is a little tricker to define. If we take the group theoretic commutator of two elements we always get the identity, since the Lie algebra is commutative. However if we allow ourselves to work in the ring $A[\varepsilon_1, \varepsilon_2]/(\varepsilon_1^2, \varepsilon_2^2)$ we notice that

$$(1 + \varepsilon_1 M)(1 + \varepsilon_2 N)(1 + \varepsilon_1 M)^{-1}(1 + \varepsilon_2 N)^{-1} = 1 + \varepsilon_1\varepsilon_2(MN - NM).$$

As such the correct definition for the Lie bracket is to take "the commutator of the ε components", though it is harder to see why this should remain in the Lie algebra. A formal justification, along with other facts about the Lie algebra we leave to Waterhouse in [Wat12].

Chapter 2

Preliminaries

2.1 Polynomial representation growth

We define $r_n(G)$ to be the number n-dimensional irreducible representations of a group G. We will be concerned with the asymptotic behaviour of this sequence for various groups G.

Definition 2.1. A group G has polynomial representation growth (PRG) if there exists some $c > 0$ such that $r_n(G) \leq cn^c$ for all $n \in \mathbb{N}$.

Equivalently one can require there to exist $c, d > 0$ such that $r_n(G) \leq cn^d$. We will use both definitions in proofs depending on what is convenient.

Example 2.2. Assuming Theorem 3.1, $\mathrm{SL}_d(\mathbb{Z})$ for $d \geq 3$ has polynomial representation growth.

The concept of polynomial representation growth can be a difficult one to come up with interesting examples for. To be an interesting example a group must have infinitely many irreducible representations, but only finitely many of a fixed dimension. The latter condition is known as representation rigidity. There is, at the time of writing, no known classification of representation rigid groups.

In this section we will investigate how representation growth behaves on subgroups and quotients. On quotients we have an implication in one direction.

Lemma 2.3. *Suppose G and G' are groups with a surjective group homomorphism $\pi : G \twoheadrightarrow G'$. Then $r_n(G') \leq r_n(G)$, and so if G has PRG then so does G'.*

Proof. Given any irreducible representation $\rho : G' \to \mathrm{GL}_n(\mathbb{C})$ we can pull back along the surjection and construct a representation $\rho \circ \pi$ of G. This representation

is irreducible because $\operatorname{im}(\rho\circ\pi) = \operatorname{im}(\rho)$, so the two representations have the same invariant subspaces.

This function $(-)\circ\pi : \operatorname{Irr}_n(G') \to \operatorname{Irr}_n(G)$ is injective due to the surjectivity of π. Therefore $r_n(G') \leq r_n(G)$, which gives us the required result. □

It is often easier to bound representations of dimension at most n, rather than representations of dimension exactly n. To facilitate this we define the following.

Notation 2.4. Define $R_n(G) := \sum_{i=1}^{n} r_i(G)$ and note that $R_n(G)$ is polynomially bounded if and only if $r_n(G)$ is. The difficult direction follows from the string of inequalities

$$R_n(G) := \sum_{i=1}^{n} r_i(G) \leq \sum_{i=1}^{n} ci^c \leq \sum_{i=1}^{n} cn^c = cn^{c+1}.$$

For subgroups we have an if and only if result. Naturally induction and restriction make an appearance in the proof.

Lemma 2.5. *If $G' \leq G$ is finite index, then:*

$$R_n(G') \leq [G : G']R_{n[G:G']}(G) \text{ and } R_n(G) \leq [G : G']R_n(G').$$

Proof. We give a proof of the second inequality. A proof of the first can be found in [LM04, Lemma 2.2], it follows by a similar argument after switching the roles of restriction and induction.

Let $\tau \in \operatorname{Irr}_m(G)$ for $m \leq n$. Define $\psi(\tau)$ to be an irreducible component of $\operatorname{Res}^G_{G'}(\tau)$. As a consequence we have $\langle \psi(\tau), \operatorname{Res}^G_{G'}(\tau)\rangle_{G'} \neq 0$. This defines a map

$$\psi : \bigcup_{m=1}^{n} \operatorname{Irr}_m(G) \to \bigcup_{m=1}^{n} \operatorname{Irr}_m(G').$$

Now the plan is to show that all fibers of this map have cardinality at most $[G : G']$. Let τ be of minimal dimension in the fiber $\psi^{-1}(\psi(\tau))$. By Frobenius reciprocity, for any $\tau' \in \psi^{-1}(\psi(\tau))$ we have

$$\langle \operatorname{Ind}^G_{G'}(\psi(\tau)), \tau'\rangle_G = \langle \psi(\tau), \operatorname{Res}^G_{G'}(\tau')\rangle_{G'} \neq 0.$$

Therefore every element $\tau' \in \psi^{-1}(\psi(\tau))$ occurs in $\operatorname{Ind}^G_{G'}(\psi(\tau))$, so

$$\begin{aligned} |\psi^{-1}(\psi(\tau))| \cdot \dim \tau &\leq \dim \operatorname{Ind}^G_{G'}(\psi(\tau)) \\ &= [G : G'] \dim \psi(\tau) \\ &\leq [G : G'] \dim \tau. \end{aligned}$$

Hence $|\psi^{-1}(\psi(\tau))| \leq [G : G']$. Since $\psi^{-1}(\psi(\tau))$ was an arbitrary fiber this tells us that $R_n(G) \leq [G : G']R_n(G')$. □

We will use these inequalities extensively, but with respect to PRG we get the following Corollary.

Corollary 2.6. *If $G' \leq G$ is finite index, then G has PRG iff G' has PRG.*

For infinite groups there is a useful dichotomy to be drawn with respect to the cardinality of the image of a representation.

Definition 2.7. A representation (ρ, V) is finite (resp. infinite) if $\mathrm{im}\,(\rho)$ is finite (resp. infinite).

This is not to be confused with the concept of a finite-*dimensional* representation. All representations in this thesis are finite-dimensional.

Remark 2.8. Lemma 2.5 and Corollary 2.6 are true if we just consider the finite representations. This is because restriction and induction preserve the property of a representation being finite.

2.2 Representations and profinite groups

Any finite representation of a group must factor through some finite quotient. This is the first clue that profinite groups and profinite completions are going to have a large role to play when studying finite representations.

We now investigate representations of profinite groups. Recall that we consider only continuous representations of profinite groups.

Theorem 2.9. *Let H be a profinite group. If $\rho : H \to \mathrm{GL}_n(\mathbb{C})$ is a representation then $\rho(H)$ is finite.*

Proof. We can quotient by $N = \ker(\rho)$ to get a map $\rho' : H/N \hookrightarrow \mathrm{GL}_n(\mathbb{C})$. Since N is a closed normal subgroup H/N is still profinite. Therefore since H/N is compact and $\mathrm{GL}_n(\mathbb{C})$ is Hausdorff ρ' is a homeomorphism onto its image. Now $\rho'(H/N)$ is a compact subgroup of $\mathrm{GL}_n(\mathbb{C})$ and hence a Lie group. Since H/N is totally disconnected, the connected component of the identity of $\rho'(H/N)$ is trivial. Therefore $\rho'(H/N)$ is discrete. Compactness of $\rho'(H/N)$ then tells us that $\rho'(H/N) = \rho(H)$ is finite. □

This result tells us that the complex representation theory of a profinite group is completely controlled by its finite quotients. This should not be too surprising because a profinite group is essentially *defined* by its finite quotients. (Recall that a profinite group is isomorphic to its profinite completion). Motivated by this initial link and results to come later, we define the following notation.

Notation 2.10. Let $\widehat{r}_n(G)$, $\widehat{R}_n(G)$, $\widehat{\mathrm{Irr}}_n(G)$ and $\widehat{\mathrm{Irr}}(G)$ be defined for finite representations analogously to their un-hatted counterparts.

The next result will justify this choice of notation beyond doubt.

Lemma 2.11. *For a discrete group G, we have that $\widehat{r}_n(G) = r_n(\widehat{G}) = \widehat{r}_n(\widehat{G})$*

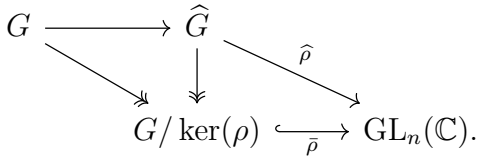
Proof. The second equality comes from Theorem 2.9.

To show $\widehat{r}_n(G) = r_n(\widehat{G})$ let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be an irrep of G with finite image. We can mod out by $\ker(\rho)$ to get a map

$$\bar{\rho} : G/\ker(\rho) \hookrightarrow \mathrm{GL}_n(\mathbb{C}).$$

Since the image is finite the kernel is finite index and we can construct the composition $\widehat{G} \twoheadrightarrow G/\ker(\rho) \hookrightarrow \mathrm{GL}_n(\mathbb{C})$, which gives us an irreducible representation $\widehat{\rho}$ of $\widehat{G}$.

This map from $\widehat{\mathrm{Irr}}_n(G) \to \mathrm{Irr}_n(\widehat{G})$ is bijective because the inverse can be constructed explicitly. Given a representation of $\widehat{G}$, precompose with $\eta : G \to \widehat{G}$ to get a representation of G. Checking that this is a two-sided inverse for our function amounts to commutativity of the following diagram:



The first triangle commutes by the universal property of the profinite completion. The second triangle commutes by the definition of $\widehat{\rho}$. □

Therefore we see that studying the finite representations of a discrete group G is equivalent to studying the representations of its profinite completion $\widehat{G}$. We continue this investigation by analysing the representations of a product of profinite groups.

Lemma 2.12. *For profinite groups G_1, G_2 every irrep of $G_1 \times G_2$ is $\rho_1 \otimes \rho_2$ where ρ_1 and ρ_2 are irreps of G_1 and G_2 respectively.*

Proof. Let $\rho : G_1 \times G_2 \to \mathrm{GL}_n(\mathbb{C})$ be an irrep. Since the product of profinite groups is profinite we know that the kernel $H = \ker(\rho)$ is a closed finite index normal subgroup, hence open by 1.11.

Now using the basis for the product topology there is some open normal of the form $H_1 \times H_2 \subset H$ that is finite index in $G_1 \times G_2$. Therefore ρ factors through the finite quotient

$$(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2).$$

Now $\bar{\rho} : (G_1/H_1) \times (G_2/H_2) \to \mathrm{GL}_n(\mathbb{C})$ is a representation of a product of finite groups, hence is of the form $\bar{\rho}_1 \otimes \bar{\rho}_2$ (Lemma 1.33). Pulling both of these representations back along the quotient maps tells us that $\rho \simeq \rho_1 \otimes \rho_2$, where ρ_i is an irreducible representation of G_i. □

Remark 2.13. The above statement holds for infinite products, provided every factor is profinite. The proof is the same. We will use this generality later on.

This proof is a classic example of how results for finite groups readily generalise to profinite groups. This result naturally has consequences for polynomial representation growth.

Corollary 2.14. *If G_i is a profinite group for $i \in \{1, ..., t\}$, then $G_1 \times \cdots \times G_t$ has PRG iff G_i has PRG for all $i \in \{1, ..., t\}$.*

Proof. Certainly if $G_1 \times \cdots \times G_t$ has PRG then G_i does, given the surjection $G_1 \times \cdots \times G_t \twoheadrightarrow G_i$ (Lemma 2.3).

Suppose the G_i have PRG such that $r_n(G_i) \leq c_i n^{c_i}$, then by Lemma 2.12

$$\begin{aligned} r_n(G_1 \times \cdots \times G_r) &= \sum_{n_1 \cdots n_t = n} r_{n_1}(G_1) \cdots r_{n_t}(G_t) \\ &\leq \sum_{n_1 \cdots n_t = n} c_1 n_1^{c_1} \cdots c_t n_t^{c_t} \\ &\leq \sum_{n_1 \cdots n_t = n} c_1 \cdots c_t n^{c_1 + \cdots + c_t} \\ &\leq c_1 \cdots c_t n^{c_1 + \cdots + c_t + t}. \end{aligned}$$

Therefore $G_1 \times \cdots \times G_t$ has PRG. □

We now turn our attention to monomial representations. We generalise results from Chapter 1 to the profinite context and explore their applications to polynomial representation growth.

Lemma 2.15. *Pronilpotent groups are monomial.*

Proof. Let σ be an irreducible representation of a pronilpotent group H. Let $H' := \ker(\sigma)$, Then σ gives rise to a representation $\bar{\sigma}$ of H/H'.

Since H is pronilpotent, H/H' is a finite nilpotent group. Therefore H/H' is monomial by Theorem 1.42, so $\bar{\sigma}$ is induced from a one-dimensional representation $\bar{\chi}$ of a subgroup Q/H' of index $\dim \sigma$ in H/H'.

Pulling back these representations we see that σ is induced from the one-dimensional representation given by the composition $Q \to Q/H' \xrightarrow{\bar{\chi}} \mathrm{GL}_1(\mathbb{C})$. A diagram that might help digest this is included below.

$$\begin{array}{ccccc} H & \twoheadrightarrow & H/H' & \xrightarrow{\bar{\sigma}} & \mathrm{GL}_{\dim(\sigma)}(\mathbb{C}) \\ {\scriptstyle [H:Q]=\dim\sigma}\uparrow & & \uparrow & & \vdots\,{\scriptstyle \mathrm{Ind}_Q^H} \\ Q & \twoheadrightarrow & Q/H' & \xrightarrow{\bar{\chi}} & \mathrm{GL}_1(\mathbb{C}). \end{array}$$

□

We will see this result come to life when applied to pro-p groups. Now we are ready to justify our claim that monomial representations of groups are easy to count.

Definition 2.16. $A_n(G) := \max\{[G' : [G', G']] \mid [G : G'] \leq n\}$.

This definition may at first be a little difficult to parse. It keeps track of the size of the abelianisation of G', when G' is of bounded index in G. There is no reason for this to be finite in general, in fact for any infinite abelian group $A_n(G)$ will be infinite for all n. Recall that the size of the abelianisation of G' counts the number of one-dimensional representations of G'. We can use this to say things about the representation growth of G, by counting the number of monomial representations.

Lemma 2.17. *If H is a profinite group, then $A_n(H) \leq nR_n(H)$.*

Proof. Let $m \leq n$ and $M \leq H$ with $[H : M] = m$ such that M has abelianisation of size $A_n(H)$. Therefore M admits exactly $A_n(H)$ one-dimensional irreps, so using Lemma 2.5 we have $A_n(H) = R_1(M) \leq mR_m(H) \leq nR_n(H)$, as required. □

This result will make an appearance in proving that a group does *not* have PRG. To show that $A_n(H)$ is large one needs to find a large abelian quotient of some finite index subgroup of H. We will see how this crops up in Chapter 4.

2.3 The congruence subgroup problem

2.3.1 Definitions

Let G and $\mathcal{O}_S$ be as in Section 3.1. Since G is defined over k we can scale the defining equations such that G is defined over $\mathcal{O}$. Recall the definition of $G(A)$ where A is an $\mathcal{O}$-algebra (Definition 1.64 and Example 1.66).

Definition 2.18. For nontrivial ideals $0 \neq I \triangleleft \mathcal{O}_S$ the kernels of the induced maps $G(\mathcal{O}_S) \to G(\mathcal{O}_S/I)$ are called principal congruence subgroups of $G(\mathcal{O}_S)$. As a set this looks like

$$\{1 + M \in G(\mathcal{O}_S) : M \in M_N(I)\}.$$

A congruence subgroup is a normal subgroup containing a principal congruence subgroup.

Remark 2.19. Notice that since $G(\mathcal{O}_S/I)$ is finite, all congruence subgroups are finite index.

Now that we have established what a congruence subgroup is, we define the congruence subgroup property. Recall that the profinite completion of $G(\mathcal{O}_S)$ is defined as

$$\widehat{G(\mathcal{O}_S)} = \varprojlim_{N \triangleleft G(\mathcal{O}_S),\, [G(\mathcal{O}_S):N] < \infty} G(\mathcal{O}_S)/N.$$

We define a similar notion as follows.

Definition 2.20. The congruence completion of $G(\mathcal{O}_S)$ is defined to be

$$\widetilde{G(\mathcal{O}_S)} := \varprojlim_{N} G(\mathcal{O}_S)/N,$$

where N ranges over all *congruence* subgroups.

Remark 2.21. Given an element $(gN)_N \in \widetilde{G(\mathcal{O}_S)}$, note that the elements of the sequence corresponding to principal congruence subgroups fully determine the entire sequence. As such we can view the congruence completion equivalently as the limit over all principal congruence subgroups. We do so in Corollary 2.32.

In general the congruence subgroup problem is the study of the kernel C of the map $\pi : \widehat{G(\mathcal{O}_S)} \twoheadrightarrow \widetilde{G(\mathcal{O}_S)}$. The map is defined by taking a sequence $(gN)_N$ and forgetting all entries that do not correspond to congruence subgroups. Specifically the congruence subgroup property is defined in the following way.

Definition 2.22 (CSP definition 1)**.** The group $G(\mathcal{O}_S)$ has the congruence subgroup property (CSP) if $C := \ker(\widehat{G(\mathcal{O}_S)} \overset{\pi}{\twoheadrightarrow} \widetilde{G(\mathcal{O}_S)})$ is finite. C is referred to as the *congruence kernel*. This information is often conveyed in the exact sequence

$$1 \to C \to \widehat{G(\mathcal{O}_S)} \overset{\pi}{\to} \widetilde{G(\mathcal{O}_S)} \to 1.$$

Remark 2.23. In the literature the congruence subgroup property is sometimes defined to mean that $C = \{1\}$ or that π is an isomorphism, while the notion we have defined as the congruence subgroup property is referred to as the *weak* congruence subgroup property. If $C = \{1\}$ then every finite index normal subgroup of $G(\mathcal{O}_S)$ is a congruence subgroup.

One way to think about $C := \ker(\pi)$ is that it measures how much the congruence subgroups fail to capture the structure of $\widehat{G(\mathcal{O}_S)}$. We will care about the structure of $\widehat{G(\mathcal{O}_S)}$ because it controls the finite representations of $G(\mathcal{O}_S)$.

2.3.2 Independence of choice

The astute reader will notice that our definition of the congruence kernel, and hence the CSP depends a priori on the choice of embedding $G \leq \mathrm{GL}_N$. Specifically if we take isomorphic $G \leq \mathrm{GL}_N$ and $G' \leq \mathrm{GL}_{N'}$, how do we know that the CSP only depends on the Lie type of G and not our choice of embedding? Even more alarmingly the definition of $G(\mathcal{O}_S)$ appears to depend on our choice of embedding. These are certainly issues that need to be addressed, though their resolutions take us a little too far from the main aim of the thesis. As such we will settle to give sketches of the resolutions to these problems.

Firstly, the group $G(\mathcal{O}_S)$ actually *does* depend on our choice of embedding. Our saving grace is the notion of commensurability. In short, given two embeddings $G \leq \mathrm{GL}_N$ and $G' \leq \mathrm{GL}_{N'}$, the associated groups $G(\mathcal{O}_S)$ and $G'(\mathcal{O}_S)$ can both be embedded in some larger group such that $[G(\mathcal{O}_S) : G(\mathcal{O}_S) \cap G'(\mathcal{O}_S)]$ and $[G'(\mathcal{O}_S) : G(\mathcal{O}_S) \cap G'(\mathcal{O}_S)]$ are finite; see [Mil06, Proposition 28.8] for details. Since the property of polynomial representation growth is stable between finite index subgroups, the statement that "$G(\mathcal{O}_S)$ has polynomial representation growth" is still completely well defined.

On the other hand, the congruence kernel C associated to $G(\mathcal{O}_S)$ is completely independent of the choice of embedding $G \leq \mathrm{GL}_N$. For details of the following sketch see [Rag76, pages 107-108]. The way to resolve this issue is a reformulation of the CSP that is more intrinsic to the algebraic group G than its embedding in some GL_N.

First take the profinite and congruence topologies on $\Gamma = G(\mathcal{O}_S)$, and extend them to topologies on $G(k)$. Completing $G(k)$ with respect to these topologies gives us groups $\widehat{G}(k)$ and $\widetilde{G}(k)$. Note that $\widehat{G}(k)$ is **not** the profinite completion of $G(k)$, but the closure of Γ inside $\widehat{G}(k)$ **is** $\widehat{\Gamma}$.

Since the topology on $\widehat{G}(k)$ is finer than the topology on $\widetilde{G}(k)$, the identity map on $G(k)$ induces a surjective map $\widehat{G}(k) \to \widetilde{G}(k)$. Certainly the restriction of this map to $\widehat{\Gamma}$ is the map π in the definition of the CSP. It turns out that the kernel of this map is actually contained in $\widehat{\Gamma}$ [Lub95, 2.2], and so the congruence subgroup problem can be phrased as the determination of C in the exact sequence:

$$1 \to C \to \widehat{G}(k) \to \widetilde{G}(k) \to 1.$$

From here if one takes two isomorphic embeddings $G \leq \mathrm{GL}_N$ and $G' \leq \mathrm{GL}_{N'}$ then there is an isomorphism of k-algebraic groups $G \to G'$. Due to the functoriality of taking the congruence kernel [Rag76, page 108 line 1], this induces an isomorphism between the a priori distinct congruence kernels. Therefore the CSP does not depend on the choice of embedding $G \leq \mathrm{GL}_N$.

2.3.3 A reworking of the congruence subgroup property

There is nothing wrong with Definition 2.22, it is the most widely applicable definition of the congruence subgroup property. However for the specific circumstances of G and $\mathcal{O}_S$ as in Section 3.1 there is a very useful equivalent definition that we will use throughout the thesis.

Definition 2.24 (CSP definition 2)**.** The group $G(\mathcal{O}_S)$ has the congruence subgroup property (CSP) if $C := \ker(\widehat{G(\mathcal{O}_S)} \overset{\pi}{\twoheadrightarrow} G(\widehat{\mathcal{O}}_S))$ is finite. C is referred to as the *congruence kernel*. This information is often conveyed in the exact sequence

$$1 \to C \to \widehat{G(\mathcal{O}_S)} \overset{\pi}{\to} G(\widehat{\mathcal{O}}_S) \to 1.$$

Comparing Definitions 2.22 and 2.24 we see that to reconcile these definitions we need to establish an isomorphism between $\widehat{G(\mathcal{O}_S)}$ and $G(\widehat{\mathcal{O}}_S)$. Furthermore this isomorphism ought to be "nice enough" to justify using the symbol π in both definitions. We will establish this by exploring the structure of the group $G(\widehat{\mathcal{O}}_S)$. The first thing to note is that by definition $\widehat{\mathcal{O}}_S$ is the profinite completion of the ring $\mathcal{O}_S$. In particular

$$\widehat{\mathcal{O}}_S = \varprojlim_{I \lhd \mathcal{O}_S,\, [\mathcal{O}_S : I] < \infty} \mathcal{O}_S / I.$$

In the case of S-integers the finite index condition only rules out the zero ideal. The following lemma provides a useful way to think about $\widehat{\mathcal{O}}_S$.

Lemma 2.25. $\widehat{\mathcal{O}}_S \cong \prod_{v \in V_f \setminus S} \mathcal{O}_v$.

Proof sketch. The idea behind the above lemma is to use unique factorisation of prime ideals and the Chinese remainder theorem to construct a natural isomorphism between the two diagrams over which each side is the limit. Localisation removes exactly the primes in S from the final product. The isomorphism then follows from the universal properties of each object.

Concretely, take ideals $I \subset J$ and consider their prime factorisations

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \text{ and } J = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_s^{f_s}.$$

with $r \geq s$ and $e_i \geq f_i$. The Chinese remainder theorem gives us an isomorphism

$$\mathcal{O}_S/I \xrightarrow{\sim} \mathcal{O}_S/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_S/\mathfrak{p}_r^{e_r}.$$

By investigating how this map is actually constructed in the proof of the Chinese remainder theorem (that is, by taking the obvious map from $\mathcal{O}_S$ into the product and descending to the quotient) we see that the following naturality square commutes

$$\begin{array}{ccc} \mathcal{O}_S/I & \xrightarrow{\sim} & \mathcal{O}_S/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_S/\mathfrak{p}_r^{e_r} \\ \downarrow & & \downarrow \\ \mathcal{O}_S/J & \xrightarrow{\sim} & \mathcal{O}_S/\mathfrak{p}_1^{f_1} \times \cdots \times \mathcal{O}_S/\mathfrak{p}_s^{f_s}. \end{array}$$

This gives the desired natural isomorphism. □

As a sanity check $\widehat{\mathcal{O}}_S$ is profinite by definition, and $\prod_{v \in V_f \setminus S} \mathcal{O}_v$ is a product of profinite rings, hence profinite. This immediately lends itself to the following perspective on $G(\widehat{\mathcal{O}}_S)$.

Corollary 2.26. $G(\widehat{\mathcal{O}}_S) \cong \prod_{v \in V_f \setminus S} G(\mathcal{O}_v)$.

Proof. The proof is an easier version of the proof of Proposition 2.27. □

The fact that $\mathcal{O}_v$ is profinite tells us that $G(\mathcal{O}_v)$ is profinite. Therefore the above expresses $G(\widehat{\mathcal{O}}_S)$ as a product of profinite groups. This will be very useful for studying representations, as we can now apply Lemma 2.12 to this decomposition. This point of view will also naturally lead us to the study of the "local groups" $G(\mathcal{O}_v)$.

At this point there is a map $G(\mathcal{O}_S) \to G(\widehat{\mathcal{O}}_S)$ induced by the canonical map $\mathcal{O}_S \to \widehat{\mathcal{O}}_S$. In light of Corollary 2.26 we know that $G(\widehat{\mathcal{O}}_S)$ is profinite and so by the universal property of the profinite completion there is a map $\pi : \widehat{G(\mathcal{O}_S)} \to G(\widehat{\mathcal{O}}_S)$. We are yet to justify why this map is surjective, or why it deserves to be called π. The following exposition will give us a clearer picture of what is going on.

Proposition 2.27. $G(\widehat{\mathcal{O}}_S) \cong \varprojlim_{I \lhd \mathcal{O}_S,\, [\mathcal{O}_S : I] < \infty} G(\mathcal{O}_S/I)$.

Proof. Consider an element in $X \in G(\widehat{\mathcal{O}}_S)$. It is a matrix, with entries that are compatible sequences of elements in various quotients of $\mathcal{O}_S$. Specifically an entry of X looks like $(a^I)^I$, with $a^I \in \mathcal{O}_S/I$ and for any $I \subset J$ we have that $a^I \mapsto a^J$ under the quotient map $\mathcal{O}_S/I \twoheadrightarrow \mathcal{O}_S/J$. The entries of X must also satisfy the defining polynomial equations for G.

Similarly consider an element $Y \in \varprojlim_{I \lhd \mathcal{O}_S,\, [\mathcal{O}_S : I] < \infty} G(\mathcal{O}_S/I)$. This is by definition a sequence of matrices $(Y^I)^I$ with $Y^I \in G(\mathcal{O}_S/I)$ and for any $I \subset J$ we have that $Y^I \mapsto Y^J$ under the induced map $G(\mathcal{O}_S/I) \to G(\mathcal{O}_S/J)$, which is just given by reducing the entries modulo J. Every Y^I must also satisfy the defining polynomials of G.

Considering this we can see that there is an isomorphism that takes a sequence of matrices in $\varprojlim_{I \lhd \mathcal{O}_S,\, [\mathcal{O}_S : I] < \infty} G(\mathcal{O}_S/I)$ to a single matrix $X \in G(\widehat{\mathcal{O}}_S)$, whose entries are defined by the corresponding entries in the sequence of matrices. The defining equations of G are still clearly satisfied because the ring structure on $\widehat{\mathcal{O}}_S$ is defined coordinate-wise. For the symbolically inclined reader the definition using notation is provided below.

The isomorphism sends $Y \in \varprojlim_{I \lhd \mathcal{O}_S,\, [\mathcal{O}_S : I]} G(\mathcal{O}_S/I)$ to $X \in G(\widehat{\mathcal{O}}_S)$ where X is defined by:

$$(X_{ij})^I := (Y^I)_{ij}.$$

□

The missing piece now is surjectivity of the induced maps $G(\mathcal{O}_S) \to G(\mathcal{O}_S/I)$. The use of the following theorem will justify many of the constraints put on G and S in Section 3.1.

Definition 2.28. An algebraic group defined over a global field k is said to have the strong approximation property (with respect to S) if the inclusion $G(k) \hookrightarrow G(\mathbb{A}_{k,S})$ has dense image.

The concept behind the name is that when allowing the matrices to have entries in the much larger ring $\mathbb{A}_{k,S}$, we can still approximate all elements arbitrarily well by matrices with entries in k.

Theorem 2.29 (Strong Approximation)**.** *Let G be a connected, semisimple algebraic group defined over a global field k. Let S be a finite set of valuations of k. G has strong approximation with respect to S if and only if G is simply connected and $\prod_{v\in S} G(k_v)$ is non-compact.*

Proof. See [PRR93, Theorem 7.12] for the proof in characteristic 0 and [Pra77, Theorem A] in characteristic p. □

Remark 2.30. Here we use a lot of the mysterious constraints on G, k and S. If one wanted to use the techniques in this thesis to prove generalisations of the main Theorems 3.1 and 4.1, this would be the place to start. A lot of our approach relies on this particular reworking of the CSP.

Corollary 2.31. *If G has strong approximation with respect to S then for any ideal $I \lhd \mathcal{O}_S$ the induced map $\pi_I : G(\mathcal{O}_S) \to G(\mathcal{O}_S/I)$ is surjective.*

Proof. Consider the diagram

$$\begin{array}{ccc} G(k) & \longrightarrow & G(\mathbb{A}_{k,S}) \\ \uparrow & & \uparrow \\ G(\mathcal{O}_S) & \xrightarrow{i} & G(\widehat{\mathcal{O}}_S). \end{array}$$

Since $G(\widehat{\mathcal{O}}_S) \subset G(\mathbb{A}_{k,S})$ is open we have that the image of $G(\mathcal{O}_S) \to G(\widehat{\mathcal{O}}_S)$ is dense. Alternatively use [KNV11, Theorem 4.2].

Now let $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be any ideal of $\mathcal{O}_S$ and consider the following commutative diagram.

$$\begin{array}{ccc} G(\mathcal{O}_S) & \xrightarrow{i} & G(\widehat{\mathcal{O}}_S) \\ & \searrow^{\pi_I} & \downarrow \psi \\ & & G(\mathcal{O}_S/I). \end{array}$$

ψ is surjective as it is the composition

$$G(\widehat{\mathcal{O}}_S) \twoheadrightarrow \prod_{i=1}^{r} G(\mathcal{O}_{v_{\mathfrak{p}_i}}) \twoheadrightarrow \prod_{i=1}^{r} G(\mathcal{O}/\mathfrak{p}_i^{e_i}) \cong G(\mathcal{O}/\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = G(\mathcal{O}/I),$$

where $\mathcal{O}_{v_{\mathfrak{p}_i}}$ denotes completion with respect to the valuation corresponding to $\mathfrak{p}_i$ and *not* localisation at $\mathfrak{p}_i$. Surjectivity of the first map comes from Corollary 2.26, while the second comes from the condition we put on S using [KNV11, Proposition 4.1]. The isomorphism is simply the Chinese remainder theorem along with a Corollary 2.26 style proof.

Therefore $\mathrm{im}\,(\pi_I) = \mathrm{im}\,(\psi \circ i)$ must be dense, but since $G(\mathcal{O}_S/I)$ is discrete this implies that $\pi_I : G(\mathcal{O}_S) \to G(\mathcal{O}_S/I)$ is surjective. □

Applying this result with Proposition 2.27 gives us the following corollary.

Corollary 2.32.

$$G(\widehat{\mathcal{O}}_S) \cong \varprojlim_{I \lhd \mathcal{O}_S,\, [\mathcal{O}_S : I] < \infty} G(\mathcal{O}_S)/\ker(G(\mathcal{O}_S) \twoheadrightarrow G(\mathcal{O}_S/I)) \cong \widetilde{G(\mathcal{O}_S)}.$$

Namely definitions 2.22 and 2.24 agree.

We have reconciled the two definitions of CSP. The map π of Definition 2.24 is now clear. Take a compatible sequence of quotients in $\widehat{G(\mathcal{O}_S)}$, act as the identity on components corresponding to principal congruence subgroups, and forget those that do not. We recognise this as the π in Definition 2.22, so it must be surjective. Alternatively we are now in a position to give a different proof.

Lemma 2.33. *The map $\pi : \widehat{G(\mathcal{O}_S)} \to G(\widehat{\mathcal{O}}_S)$ as described above is surjective.*

Proof. By the previous proof the image of $G(\mathcal{O}_S)$ in $G(\widehat{\mathcal{O}}_S)$ is dense. Now considering the composition $G(\mathcal{O}_S) \to \widehat{G(\mathcal{O}_S)} \xrightarrow{\pi} G(\widehat{\mathcal{O}}_S)$ we see that $\mathrm{im}\,(\pi)$ contains a dense set. Furthermore $\mathrm{im}\,(\pi)$ is closed (as the image of a compact space in a Hausdorff space) and so π is surjective. □

We have now built up enough background to state Theorems 3.1 and 4.1. These two theorems are the main project of the thesis. Together they form an equivalence between polynomial representation growth and the congruence subgroup property. We spend Chapters 3 and 4 proving them.

Chapter 3

Groups with the CSP

3.1 Notation and goal

We now set out to fix some notation for the thesis.

- Let k be a global field and $\mathcal{O}$ be its ring of integers.
- Let $G \leq \mathrm{GL}_N$ be a semisimple, simply connected and connected algebraic group defined over k.
- Let V be the set of valuations on k.
- Write V_f for the finite valuations (the non-archimedean valuations corresponding to prime ideals) and V_∞ for all other valuations, so $V = V_f \sqcup V_\infty$.
- Fix a finite set S such that $V_\infty \subset S \subset V$ and such that $\prod_{v \in S} G(k_v)$ is non-compact (this ensures that strong approximation holds).
- Define $\mathcal{O}_S := \{x \in k : v(x) \leq 1 \, \forall \, v \in V \setminus S\}$, we call $\mathcal{O}_S$ the ring of S-integers. It is exactly $\mathcal{O}$ after localising at primes corresponding to valuations in S.
- Let $\Gamma = G(\mathcal{O}_S)$ and let $C := \ker(\widehat{G(\mathcal{O}_S)} \to G(\widehat{\mathcal{O}}_S))$ be the congruence kernel of Γ.

We have now set up enough notation to state the main theorem of this chapter.

Theorem 3.1. *Let Γ be as above. Assume that if $\operatorname{char} k = 2$, then G contains no factors of type A_1 or C_m for any m. If Γ has the congruence subgroup property, then Γ has polynomial representation growth.*

The extra assumptions in the $\operatorname{char} k = 2$ case ensure that the Lie algebra of G is perfect. We record them here for later reference.

Assumption 3.2. If $\operatorname{char} k = 2$ then G contains no factors of type A_1 or C_m.

This is one half of the striking relationship between the congruence subgroup property and polynomial representation growth. Once proven, this will yield many interesting examples of groups with PRG. We now proceed to introduce more notation, which we will use in the rest of the thesis.

- Given $v \in V$ define k_v to be the completion of k with respect to v.
- For $v \in V_f$ let $\mathcal{O}_v$ be the valuation ring of k_v.
- Let $\mathfrak{m}_v$ be the unique maximal ideal $\mathfrak{m}_v \lhd \mathcal{O}_v$.
- Let $\mathbb{F}_v = \mathcal{O}_v/\mathfrak{m}_v$ denote the residue field.
- Define $q_v := |\mathbb{F}_v|$, $p_v := \operatorname{char}(\mathbb{F}_v)$ and $e_v := \log_{p_v}(q_v)$.
- Enlarge S using [KNV11, Proposition 4.1] to ensure that for all $v \in V_f \setminus S$ the maps $G(\mathcal{O}_v) \to G(\mathcal{O}_v/\mathfrak{m}_v^n)$ are surjective.
- Finally define $G(\mathbb{F}_v)$ to be the image of $G(\mathcal{O}_v)$ in $\mathrm{GL}_N(\mathbb{F}_v)$.

3.2 Some initial reductions

The aim of this section is to make three important reductions: from all representations of $G(\mathcal{O}_S)$ to just the finite ones; from semisimple G to simple G and from $\widehat{G(\mathcal{O}_S)}$ to $G(\widehat{\mathcal{O}}_S)$.

When Γ has the CSP it has polynomial representation growth if and only if its finite representations are polynomially bounded. We give a brief sketch of this reduction for the curious reader. See [LM04, Chapter 3] for details.

The idea in characteristic 0 is to first view $G(\mathcal{O}_S)$ as living inside a complex algebraic group H in a particular way. Then the CSP kicks in to say that infinite representations of $G(\mathcal{O}_S)$ "are algebraic representations of the associated complex algebraic group tensored with a finite representation of $G(\mathcal{O}_S)$, up to a finite index subgroup". The final step is to leverage the structure theory of semisimple complex algebraic groups, specifically their representation theory, to prove that the complex algebraic group H has PRG. The case of $\operatorname{char} k = p$ is a similar

story, except that if Γ has the CSP then there are *no* complex representations of algebraic groups to be accounted for.

With this in mind we spend the rest of this chapter (and indeed the thesis) focused solely on the finite representations of Γ. In light of Lemma 2.11 we know that the finite representation theory of Γ is equivalent to the representation theory of $\widehat{\Gamma}$. Thus we have reduced to proving the following.

Theorem 3.3. *Let Γ be as in Theorem 3.1. If Γ has the congruence subgroup property then $\widehat{\Gamma}$ has polynomial representation growth.*

The next reduction we make is to assume that G is simple.

Lemma 3.4. *Theorem 3.3 holds if and only if it holds with the added assumption that G is simple.*

Proof. Clearly if Theorem 3.3 holds, then it holds for simple G. Therefore suppose Theorem 3.3 holds with the added assumption that G is simple.

Let Γ be as in the statement of Theorem 3.3. Since G is semisimple and simply connected, it is a product of simple algebraic groups. Therefore we have $\Gamma = G_1(\mathcal{O}_S) \times \cdots \times G_r(\mathcal{O}_S)$, where the G_i are simple. Since taking the profinite completion commutes with taking products we have that

$$\widehat{\Gamma} \cong \widehat{G_1(\mathcal{O}_S)} \times \cdots \times \widehat{G_r(\mathcal{O}_S)}. \tag{3.1}$$

Now the map $\pi : \widehat{G(\mathcal{O}_S)} \to G(\widehat{\mathcal{O}}_S)$ is given by

$$\pi = \pi_1 \times \cdots \times \pi_r : \widehat{G_1(\mathcal{O}_S)} \times \cdots \times \widehat{G_r(\mathcal{O}_S)} \to G_1(\widehat{\mathcal{O}}_S) \times \cdots \times G_r(\widehat{\mathcal{O}}_S).$$

If Γ has CSP, then the $G_i(\mathcal{O}_S)$ do, because the following commutative diagram implies that $|\ker(\pi_i)| < |\ker(\pi)| < \infty$.

$$\begin{array}{ccc} \widehat{G_1(\mathcal{O}_S)} \times \cdots \times \widehat{G_r(\mathcal{O}_S)} & \xrightarrow{\pi} & G_1(\widehat{\mathcal{O}}_S) \times \cdots \times G_r(\widehat{\mathcal{O}}_S) \\ \uparrow & & \uparrow \\ \widehat{G_i(\mathcal{O}_S)} & \xrightarrow{\pi_i} & G_i(\widehat{\mathcal{O}}_S). \end{array}$$

Therefore applying Theorem 3.3 to $G_i(\mathcal{O}_S)$ in the simple case tells us that each of the $\widehat{G_i(\mathcal{O}_S)}$ have PRG. Since the $\widehat{G_i(\mathcal{O}_S)}$ are profinite, applying Corollary 2.14 with Equation 3.1 tells us that Γ has PRG, as required. □

So we may additionally assume that G is simple. The rest of the section will be dedicated to the reduction from $\widehat{G(\mathcal{O}_S)}$ to $G(\widehat{\mathcal{O}}_S)$. To do this it helps to know something about how Γ sits inside its profinite completion.

Lemma 3.5. *The map $\eta : \Gamma \to \widehat{\Gamma}$ is injective.*

Proof. The map $\eta : \Gamma \to \widehat{\Gamma}$ simply takes an element of Γ and maps it to the sequence of its images modulo every finite index normal subgroup. It suffices to prove that $\ker \eta = \{1\}$.

Suppose $\gamma \in \ker \eta$, then γ is trivial modulo every finite index normal subgroup. Consider the principal congruence subgroups corresponding to prime ideals. In particular γ must be trivial under every map $\pi_{\mathfrak{p}} : G(\mathcal{O}_S) \to G(\mathcal{O}_S/\mathfrak{p})$ where $\mathfrak{p} \triangleleft \mathcal{O}_S$ is prime. Recall that γ is a matrix and $\pi_{\mathfrak{p}}$ is given by reduction of the matrix entries mod $\mathfrak{p}$. If we take $\gamma_{ij} - \delta_{ij}$, this must be trivial in $\mathcal{O}_S/\mathfrak{p}$ and hence *in* $\mathfrak{p}$.

Now we apply [AM18, Proposition 1.8] to see that

$$\gamma_{ij} - \delta_{ij} \in \bigcap_{\mathfrak{p} \triangleleft \mathcal{O}_S} \mathfrak{p} = \mathfrak{N}(\mathcal{O}_S) = \{0\}.$$

We know that the nilpotent radical $\mathfrak{N}(\mathcal{O}_S)$ is $\{0\}$ because $\mathcal{O}_S$ includes into a field k, which has no nilpotent elements. Therefore $\gamma_{ij} = \delta_{ij}$, so γ is the identity matrix. Therefore $\ker(\eta) = \{1\}$ and the map $\eta : \Gamma \to \widehat{\Gamma}$ is injective. □

In light of this lemma we fix the following notation for this section.

Notation 3.6. For any subset $X \subset \Gamma$, take $\overline{X}$ to mean the closure of X in $\widehat{\Gamma}$.

This notation allows us to state some results very simply, but has the drawback of potential ambiguity. We now construct the finite index subgroup which allows this reduction to take place.

Lemma 3.7. *If Γ has the CSP then there exists some finite index subgroup $\Gamma_0 \leq \Gamma$ such that $C \cap \overline{\Gamma_0}$ is trivial.*

Proof. Since Γ has the CSP, C is finite, and hence $C \subset \widehat{\Gamma}$ is discrete. Since the open normal subgroups in $\widehat{\Gamma}$ form a basis for the topology at the identity there exists some open normal $N \leq \widehat{\Gamma}$ such that $N \cap C = \{1\}$. Note that N is closed by Lemma 1.11. We now need to use this N to find a finite index subgroup of Γ.

Take the normal subgroup $\Gamma_0 := N \cap \Gamma$. We will show it is finite index and that $\overline{\Gamma_0} \cap C = \{1\}$.

Take a transversal $\gamma_1, ..., \gamma_r \in \Gamma$ for N as a subgroup of $\widehat{\Gamma}$. This is possible because Γ is dense in $\widehat{\Gamma}$, and the cosets of N are open. Then $\widehat{\Gamma} = \bigcup_{i=1}^{r} \gamma_i N$.

Therefore

$$\begin{aligned}\bigcup_{i=1}^{r}\gamma_i\Gamma_0 = \bigcup_{i=1}^{r}\gamma_i(N\cap\Gamma) &= \bigcup_{i=1}^{r}\gamma_i N\cap\gamma_i\Gamma\\ &= \bigcup_{i=1}^{r}\gamma_i N\cap\Gamma\\ &= \left(\bigcup_{i=1}^{r}\gamma_i N\right)\cap\Gamma\\ &= \widehat{\Gamma}\cap\Gamma = \Gamma.\end{aligned}$$

So $[\Gamma:\Gamma_0]\leq r$ and we have shown that $\Gamma_0\leq\Gamma$ is finite index. Finally

$$\overline{\Gamma_0}\cap C = \overline{N\cap\Gamma}\cap C\subset\overline{N}\cap C = N\cap C = \{1\}.$$

□

If one would like to visualise this situation they can imagine Γ as a dense lattice in $\widehat{\Gamma}$. Once we find our huge (finite index) open subgroup, the intersection of that lattice with the open subgroup must be finite index in the lattice.

The final piece we need is the fact that $\overline{\Gamma_0}\cong\widehat{\Gamma}_0$. This is a completely general fact about profinite completions and does not use anything specific to Γ. As such we relegate the proof to Appendix A (Lemma A.1).

We are now ready to make the third and final reduction of this section.

Proposition 3.8. *If Γ has the CSP then $\widehat{G(\mathcal{O}_S)}$ has PRG if and only if $G(\widehat{\mathcal{O}}_S)$ does.*

Proof. Let Γ_0 be as in Lemma 3.7. Consider the commutative diagram

$$\begin{array}{ccccc}\Gamma & \hookrightarrow & \widehat{G(\mathcal{O}_S)} & & \\ \uparrow & & \uparrow & \searrow & \\ \Gamma_0 & \hookrightarrow & \overline{\Gamma_0} & \hookrightarrow & G(\widehat{\mathcal{O}_S}).\end{array}$$

Since $[\Gamma:\Gamma_0]<\infty$ the representation growths of Γ and Γ_0 are the same. We know that the map $\overline{\Gamma_0}\to G(\widehat{\mathcal{O}_S})$ is injective because of the condition that $\overline{\Gamma_0}\cap C=\{1\}$. Furthermore since $\overline{\Gamma_0}$ is finite index in $\widehat{G(\mathcal{O}_S)}$, and $\widehat{G(\mathcal{O}_S)}\twoheadrightarrow G(\widehat{\mathcal{O}_S})$ is surjective, this realises $\overline{\Gamma_0}$ as a finite index subgroup of $G(\widehat{\mathcal{O}_S})$. Therefore $\overline{\Gamma_0}$ has PRG if and only if $G(\widehat{\mathcal{O}_S})$ does.

Finally, applying Lemma 2.11 and A.1 for the equalities and Corollary 2.6 for the implications we get the following string of statements:

$r_n(\widehat{\Gamma}) = \widehat{r}_n(\Gamma)$ grows polynomially $\iff$ $\widehat{r}_n(\Gamma_0) = r_n(\widehat{\Gamma}_0) = r_n(\overline{\Gamma_0})$ grows polynomially $\iff$ $r_n(G(\widehat{\mathcal{O}}_S))$ grows polynomially, as required. □

With this result we have shown that Theorem 3.1 is equivalent to the following.

Theorem 3.9. *Let $k, \mathcal{O}, S$ and G be as in Theorem 3.1. Then $G(\widehat{\mathcal{O}_S})$ has polynomial representation growth.*

This means that we can focus solely on so called "congruence" representations.

Definition 3.10. A congruence representation is a representation whose kernel contains a congruence subgroup.

It may not be immediately clear why Theorem 3.9 is any easier to prove than Theorem 3.3. One heuristic is that congruence representations can be regarded as representations of $G(\mathcal{O}_S/I)$. We know at least something about the structure of this group as the $\mathcal{O}_S/I$-points of an algebraic group. This is much better than the case of $\widehat{G(\mathcal{O}_S)}$, where all we know is that a representation factors into a representation of some finite quotient of $G(\mathcal{O}_S)$, which we have no control over.

Another reason this reduction is an improvement, is because of Corollary 2.26, which gives a decomposition of $G(\widehat{\mathcal{O}}_S)$ into a product of profinite groups of the form $G(\mathcal{O}_v)$. This product gives us a natural place to start, and these groups also have some useful additional structure, which we will explore in the next section.

3.3 The graded Lie algebra of a local group

We start this section by clarifying the following piece of terminology.

Terminology 3.11. Local groups are groups of the form $G(\mathcal{O}_v)$ for $v \in V_f$.

The nomenclature is completely analogous to the naming of local fields in number theory. In this section we explore the graded Lie algebra that can be attached to these local groups. It is related to but distinct from the Lie algebra of Definition 1.67. Many results in this chapter leverage this specific Lie theory, so while a lot of this is very similar in style to the Lie theory one might have previously seen in this thesis or elsewhere, it is important to write out the definitions and results carefully.

Recall that $\mathfrak{m}_v \lhd \mathcal{O}_v$ is the unique maximal ideal. All nontrivial ideals in $\mathcal{O}_v$ are some power of $\mathfrak{m}_v$, so they form a descending chain

$$(\mathcal{O}_v \supset)\, \mathfrak{m}_v \supset \mathfrak{m}_v^2 \supset \mathfrak{m}_v^3 \supset \cdots .$$

The simple ideal structure generally makes the local rings $\mathcal{O}_v$ easier to study than the global ring $\mathcal{O}_S$. The same is true of the associated groups. Analogously to Definition 2.18 we define the following.

Definition 3.12. We write $N_n^{(v)} = G(\mathcal{O}_v) \cap \ker(\mathrm{GL}_N(\mathcal{O}_v) \to \mathrm{GL}_N(\mathcal{O}_v/\mathfrak{m}_v^n))$ for the n-th (principal) congruence subgroup of $G(\mathcal{O}_v)$. If π is a generator for $\mathfrak{m}_v$ then

$$N_n^{(v)} = \{1 + \pi^n M \in G(\mathcal{O}_v) : M \in M_N(\mathcal{O}_v)\}.$$

The congruence subgroups give a filtration of $G(\mathcal{O}_v)$ by normal subgroups

$$(G(\mathcal{O}_v) \geq)\, N_1^{(v)} \geq N_2^{(v)} \geq N_3^{(v)} \geq \cdots.$$

Remark 3.13. $G(\mathcal{O}_v)$ inherits a topology from the topology on $M_N(\mathcal{O}_v)$, which inherits its topology from $\mathcal{O}_v$ via the bijection $M_N(\mathcal{O}_v) \cong \mathcal{O}_v^{N^2}$. Given this, the family $\{N_n^{(v)}\}_{n=1}^{\infty}$ forms a basis of open normal subgroups for the topology on $G(\mathcal{O}_v)$. This can be thought of as the congruence subgroup property for $G(\mathcal{O}_v)$, as it shows that any open subgroup of $G(\mathcal{O}_v)$ contains a principal congruence subgroup. An exploration of this in the case of $\mathrm{GL}_d(\mathbb{Z}_p)$ can be found in [DDSMS03, Section 5.1].

The principal congruence subgroups are normal, so we can define the following.

Definition 3.14. The graded Lie algebra associated to the local group $G(\mathcal{O}_v)$ is

$$L^{(v)} := \bigoplus_{n=1}^{\infty} L_n^{(v)} := \bigoplus_{n=1}^{\infty} N_n^{(v)}/N_{n+1}^{(v)}.$$

We will simply use the term Lie algebra when there is no ambiguity between $L^{(v)}$ and Definition 1.67.

There is some explanation necessary in order to justify calling this construction a Lie algebra. Each graded component $L_n^{(v)}$ is certainly a group, but it is also abelian since

$$\begin{aligned}
(1+\pi^n X)N_{n+1}^{(v)}(1+\pi^n Y)N_{n+1}^{(v)} &= (1+\pi^n X+\pi^n Y+\pi^{2n}XY)N_{n+1}^{(v)} \\
&= (1+\pi^n X+\pi^n Y)(1+\pi^{2n}XY)N_{n+1}^{(v)} \\
&= (1+\pi^n X+\pi^n Y)(1+\pi^{2n}YX)N_{n+1}^{(v)} \\
&= (1+\pi^n X+\pi^n Y+\pi^{2n}YX)N_{n+1}^{(v)} \\
&= (1+\pi^n Y)N_{n+1}^{(v)}(1+\pi^n X)N_{n+1}^{(v)},
\end{aligned}$$

where $X, Y \in M_n(\mathcal{O}_v)$. Intuitively we can switch the order of the XY term because modulo $N_{n+1}^{(v)}$ we ignore anything that happens beyond π^{n+1}. We therefore define addition on each graded component of $L^{(v)}$ as

$$xN_{n+1}^{(v)} + yN_{n+1}^{(v)} := xyN_{n+1}^{(v)}.$$

Now as an abelian group $L^{(v)}$ is a $\mathbb{Z}$-module. However since $p = p_v \in \mathfrak{m}_v$ we have for any $x = (1 + \pi^n X)N_{n+1}^{(v)} \in L_n^{(v)}$ that

$$p \cdot x = (1 + \pi^n X)^p N_{n+1}^{(v)} = (1 + O(\pi^{n+1}))N_{n+1}^{(v)} = 1N_{n+1}^{(v)} = 0.$$

All cross terms pick up an extra factor of π by the binomial theorem and the fact that $p \in \mathfrak{m}_v = (\pi)$. Therefore the multiplication by p is trivial, so $L^{(v)}$ is an $\mathbb{F}_p$ vector space.

So far the graded components function independently. Linking them together is the Lie bracket, defined as

$$[\cdot, \cdot] : L_n^{(v)} \times L_m^{(v)} \to L_{n+m}^{(v)},\ [xN_{n+1}^{(v)}, yN_{m+1}^{(v)}] = xyx^{-1}y^{-1}N_{n+m+1}^{(v)}$$

on $L_n^{(v)} \times L_m^{(v)}$ and extended to be bilinear. Antisymmetry of the bracket comes from noticing that switching the roles of x and y in the above definition gives the group inverse, which given the way we defined addition is an additive inverse.

If one takes $x = I + \pi^n X \in N_n^{(v)}$ and $y = I + \pi^m Y \in N_m^{(v)}$ we see that

$$[xN_{n+1}^{(v)}, yN_{m+1}^{(v)}] = (I + \pi^{n+m}(XY - YX))N_{n+m+1}^{(v)}.$$

So the Lie bracket we have defined just takes the commutator of the matrices X and Y defining our elements. This tells us that this Lie bracket satisfies the Jacobi identity. The last thing we have to mention before learning more about the Lie algebra is the following lemma.

Lemma 3.15. *For $p \in \mathfrak{m}_v$, $N_1^{(v)}$ is a pro-p group, specifically*

$$N_1^{(v)} \cong \varprojlim_n N_1^{(v)}/N_n^{(v)}.$$

Proof. Since all congruence subgroups are normal in $G(\mathcal{O}_v)$ we can consider the quotient groups $N_1^{(v)}/N_n^{(v)}$. They are finite because congruence subgroups are finite index in $G(\mathcal{O}_v)$. All quotients $N_n^{(v)}/N_{n+1}^{(v)}$ are p groups because they are $\mathbb{F}_p$ vector spaces. Therefore any quotient $N_1^{(v)}/N_n^{(v)}$ is a finite p-group.

There are compatible maps $\pi_n : N_1^{(v)} \to N_1^{(v)}/N_n^{(v)}$. To prove $N_1^{(v)}$ is in fact the limit of this system, suppose G has compatible maps $\phi_n : G \to N_1^{(v)}/N_n^{(v)}$. If a suitable map $\phi : G \to N_1^{(v)}$ exists it must satisfy

$$\phi(g)_{ij} \equiv \phi_n(g)_{ij} \mod \mathfrak{m}_v^n.$$

That is, we know what every entry of $\phi(g)$ is modulo every power of $\mathfrak{m}_v$.

Since $\mathcal{O}_v \cong \varprojlim_n \mathcal{O}_v/\mathfrak{m}_v^n$ this defines an element of $\mathcal{O}_v$, so in fact ϕ is a well defined map. To check it is a group homomorphism can be done. It involves ensuring that the entries of $\phi(g)\phi(h)$ and $\phi(gh)$ are the same modulo every power of $\mathfrak{m}_v$, which boils down to the fact that reducing modulo $\mathfrak{m}_v^n$ is a ring homomorphism. □

The fact that $N_1^{(v)}$ is pro-p makes kernels of its representations particularly easy to study. Representations of pro-p groups are induced from one-dimensional representations of finite index subgroups, and the kernels of one-dimensional representations contain the commutator subgroup of the domain. Restricting a representation to $N_1^{(v)}$ will be one of the first things we do when proving anything about representations of $G(\mathcal{O}_v)$.

The next thing we wish to do is define the set of $v \in V_f$ for which the graded Lie algebra of the local group behaves particularly nicely.

Definition 3.16. Let $\mathcal{P}_1 \subset V_f$ be the set of $v \in V_f$ such that:

(a) $G(\mathbb{F}_v)$ is a perfect finite central extension of a finite simple group of Lie type $H(q_v)$, where H is the Lie type of G;

(b) For every $n \in \mathbb{N}$, $|N_n^{(v)}/N_{n+1}^{(v)}| \leq q_v^{N^2}$;

(c) For every $n, m \in \mathbb{N}$ with $|n - m| \leq 1$, $[N_n^{(v)}, N_m^{(v)}] = N_{n+m}^{(v)}$;

(d) $G(\mathcal{O}_v)$ is perfect;

(e) There exists an $\mathbb{F}_v$-scalar multiplication on $L^{(v)}$ making $(L^{(v)}, [-,-])$ into a graded Lie algebra over $\mathbb{F}_v$.

Terminology 3.17. We refer to $\mathcal{P}_1$ as the set of "good primes" for a fixed G and k. Similarly we refer to $\mathcal{P}_2 := V_f \setminus \mathcal{P}_1$ as the set of "bad primes".

It turns out that conditions (a)-(e) are generically true. Specifically

Proposition 3.18. *The set $\mathcal{P}_1 \subset V_f$ consists of all but finitely many primes $v \in V_f$.*

Proof Sketch. (a): [MT11, Theorem 24.17] tells us that (a) holds if we disregard the finitely many primes with residue field $\mathbb{F}_2$ or $\mathbb{F}_3$.

(b): This holds for all primes since for any element of $N_n^{(v)}/N_{n+1}^{(v)}$ there are at most $|\pi^n\mathcal{O}_v/\pi^{n+1}\mathcal{O}_v| = q_v$ choices for each of the N^2 entries of the matrix.

(c): Suppose that (c) fails, we will prove a contradiction. Take n, m with $|n-m| \leq 1$ and $[N_n^{(v)}, N_m^{(v)}] \subsetneq N_{n+m}^{(v)}$. Suppose $n+m$ is maximal with this property. Since the Lie algebra of G is perfect the diagrams in [LL11, pages 9,10] with $a = n$, $b = n+1$, $c = m$ and $d = m+1$ tell us that

$$[N_n^{(v)}/N_{n+1}^{(v)}, N_m^{(v)}/N_{m+1}^{(v)}] = N_{n+m}^{(v)}/N_{n+m+1}^{(v)}.$$

However, by our choice of n and m there exists an $x \in N_{n+m}^{(v)} \setminus [N_n^{(v)}, N_m^{(v)}]$. Combining this with the above equation tells us that

$$\bar{x} \in N_{n+m}^{(v)}/N_{n+m+1}^{(v)} = [N_n^{(v)}/N_{n+1}^{(v)}, N_m^{(v)}/N_{m+1}^{(v)}].$$

Now suppose without loss of generality that $n \leq m$, then

$$\begin{aligned} x &\in [N_n^{(v)}, N_m^{(v)}]N_{n+m+1}^{(v)} \\ &= [N_n^{(v)}, N_m^{(v)}][N_{n+1}^{(v)}, N_m^{(v)}] \\ &\subset [N_n^{(v)}, N_m^{(v)}], \end{aligned}$$

but this is a contradiction because x was chosen to not be in this set.

(d): By definition of the groups $N_1^{(v)}$ and $G(\mathbb{F}_v)$ we have an exact sequence

$$1 \to N_1^{(v)} \to G(\mathcal{O}_v) \to G(\mathbb{F}_v) \to 1.$$

Given this, the abelianisation of $G(\mathcal{O}_v)$ fits into the exact sequence

$$1 \to N_1^{(v)}/(N_1^{(v)} \cap [G(\mathcal{O}_v), G(\mathcal{O}_v)]) \to G(\mathcal{O}_v)/[G(\mathcal{O}_v), G(\mathcal{O}_v)] \to G(\mathbb{F}_v)/[G(\mathbb{F}_v), G(\mathbb{F}_v)] \to 1.$$

Note that using condition (a) we may assume $G(\mathbb{F}_v)$ is perfect, so has trivial abelianisation. Therefore we have an isomorphism

$$N_1^{(v)}/(N_1^{(v)} \cap [G(\mathcal{O}_v), G(\mathcal{O}_v)]) \xrightarrow{\sim} G(\mathcal{O}_v)/[G(\mathcal{O}_v), G(\mathcal{O}_v)].$$

Furthermore condition (c) tells us that

$$N_1^{(v)} \cap [G(\mathcal{O}_v), G(\mathcal{O}_v)] \supset N_1^{(v)} \cap [N_1^{(v)}, N_1^{(v)}] = N_2^{(v)}.$$

Therefore it suffices to prove that $[G(\mathcal{O}_v)/N_2^{(v)}, N_1^{(v)}/N_2^{(v)}] \supset N_1^{(v)}/N_2^{(v)}$. This comes from the fact that the Lie algebra (As in Definition 1.67) of $G(\mathcal{O}_v)$ is perfect.

(e): Follows from the discussion at the bottom of page 9 in [LL11]. □

Anyone who has studied Lie theory of any form before knows that it is fruitful to consider how subgroups interact with the Lie algebra. The graded Lie algebra is no exception.

Definition 3.19. If $H \leq N_1^{(v)}$ is an open subgroup, then we can define the graded Lie subalgebra corresponding to H by

$$L^{(v)}(H) := \bigoplus_{n=1}^{\infty} L_n^{(v)}(H),$$

where

$$L_n^{(v)}(H) := (H \cap N_n^{(v)})N_{n+1}^{(v)}/N_{n+1}^{(v)}.$$

The previous analysis applies verbatim regarding the definition of the Lie bracket and addition. Naturally the index of the subgroup determines the index of the graded Lie subalgebra.

Lemma 3.20. *If $H \leq N_1^{(v)}$ is an open subgroup then*

$$[N_1^{(v)} : H] = [L^{(v)} : L^{(v)}(H)].$$

Proof. First we investigate $[N_1^{(v)} : H]$.

$$\begin{aligned}
[N_1^{(v)} : H] &= \frac{[N_1^{(v)} : N_2^{(v)}]}{[H : H \cap N_2^{(v)}]}[N_2^{(v)} : H \cap N_2^{(v)}] \\
&= \frac{[N_1^{(v)} : N_2^{(v)}][N_2^{(v)} : N_3^{(v)}]}{[H \cap N_1^{(v)} : H \cap N_2^{(v)}][H \cap N_2^{(v)} : H \cap N_3^{(v)}]}[N_3^{(v)} : H \cap N_3^{(v)}] \\
&= \prod_{i=1}^{\infty} \frac{[N_i^{(v)} : N_{i+1}^{(v)}]}{[H \cap N_i^{(v)} : H \cap N_{i+1}^{(v)}]}.
\end{aligned}$$

Now investigating $[L^{(v)} : L^{(v)}(H)]$,

$$\begin{aligned}
[L^{(v)} : L^{(v)}(H)] &= \prod_{i=1}^{\infty} [N_i^{(v)}/N_{i+1}^{(v)} : (H \cap N_i^{(v)})N_{i+1}^{(v)}/N_{i+1}^{(v)}] \\
&= \prod_{i=1}^{\infty} [N_i^{(v)} : (H \cap N_i^{(v)})N_{i+1}^{(v)}] \\
&= \prod_{i=1}^{\infty} \frac{[N_i^{(v)} : N_{i+1}^{(v)}]}{[(H \cap N_i^{(v)})N_{i+1}^{(v)} : N_{i+1}^{(v)}]}.
\end{aligned}$$

All but finitely many factors in these products are 1, so there are no issues of convergence. It is now enough to prove that

$$[H \cap N_i^{(v)} : H \cap N_{i+1}^{(v)}] = [(H \cap N_i^{(v)})N_{i+1}^{(v)} : N_{i+1}^{(v)}],$$

which is true because there is a surjective group homomorphism

$$H \cap N_i^{(v)} \to (H \cap N_i^{(v)})N_{i+1}^{(v)}/N_{i+1}^{(v)},$$

whose kernel is exactly $(H \cap N_i^{(v)}) \cap N_{i+1}^{(v)} = H \cap N_{i+1}^{(v)}$. □

The graded Lie algebra detects not only the index of a subgroup. Analysis of the graded Lie algebra gives us information regarding where a subgroup sits with respect to the filtration of principal congruence subgroups.

Proposition 3.21. *If $H \leq G(\mathcal{O}_v)$ is an open subgroup and $L_n^{(v)}(H) = L_n^{(v)}$ for all $n \geq m$, then $H \supset N_m^{(v)}$.*

Proof. We proceed by contrapositive. Suppose that $H \not\supset N_m^{(v)}$. Let n be the smallest n such that $H \supset N_n^{(v)}$. We know this n exists because the congruence subgroups form a basis for the topology. We therefore have simultaneously that $H \supset N_n^{(v)}$ and $H \not\supset N_{n-1}^{(v)}$. We claim that $L_{n-1}^{(v)}(H) \neq L_{n-1}^{(v)}$. Indeed there exists some $x \in N_{n-1}^{(v)} \setminus H$, therefore $xN_n^{(v)} \in L_{n-1}^{(v)}$. However

$$x \notin H = HH \supset (H \cap N_{n-1}^{(v)})H \supset (H \cap N_{n-1}^{(v)})N_n^{(v)}.$$

So $xN_n^{(v)} \in L_{n-1}^{(v)} \setminus L_{n-1}^{(v)}(H)$. Therefore $L_{n-1}^{(v)}(H) \neq L_{n-1}^{(v)}$. □

With the notion of good primes established we are ready to present a proof of Theorem 3.9. We do this in the following section.

3.4 Proof outline

In this section we will give the outline of the proof of Theorem 3.9. It relies on theorems and propositions that will be proven later. This proof outline will serve as motivation for working our way to these results. One can view this section as a further reduction to analysis of the local groups.

Definition 3.22. For a group H, define $K_n(H)$ as

$$K_n(H) = \bigcap_{\rho \in \mathrm{Rep}_n(H)} \ker \rho.$$

Theorem 3.23. *There exists $c > 0$ dependent only on G and k such that for every $v \in V_f$ and every $n \in \mathbb{N}$, $[G(\mathcal{O}_v) : K_n(G(\mathcal{O}_v))] \leq cn^c$.*

Remark 3.24. Given some representation of dimension $< n$ we can add copies of the trivial representation to construct an n-dimensional representation with the same kernel. As such the subgroups $K_n(G(\mathcal{O}_v))$ form a nested sequence of subgroups

$$\cdots \leq K_n(G(\mathcal{O}_v)) \leq \cdots \leq K_2(G(\mathcal{O}_v)) \leq K_1(G(\mathcal{O}_v)).$$

In light of this we see that the dimension $\leq n$ representation theory of $G(\mathcal{O}_v)$ is contained in the representation theory of the finite group $G(\mathcal{O}_v)/K_n(G(\mathcal{O}_v))$, whose size grows polynomially in n. Notice also that this result bounds the number of representations of a given dimension, not just irreducible ones. A few quick corollaries of this are stated below.

Corollary 3.25. *There exists $c > 0$ such that $r_n(G(\mathcal{O}_v)) \leq cn^c$ for every $v \in V_f$ and $n \in \mathbb{N}$.*

Corollary 3.26. *There exists $c > 0$ such that $|\rho(G(\mathcal{O}_v))| \leq cn^c$ for every $v \in V_f$, $n \in \mathbb{N}$ and $\rho \in \mathrm{Rep}_n(G(\mathcal{O}_v))$.*

Remark 3.27. The above corollaries are markedly stronger than saying that $G(\mathcal{O}_v)$ has polynomial representation/image growth for all $v \in V_f$. The representations/images of $G(\mathcal{O}_v)$ are polynomially bounded, **uniformly in** v. This uniformity is critical in making the proof work. We will see how this uniformity is achieved in Section 3.6.

Proposition 3.28. *There exists a $\delta > 0$ such that for every $v \in \mathcal{P}_1$, every nontrivial irreducible representation of $G(\mathcal{O}_v)$ is of dimension at least q_v^δ.*

The above proposition will be used both in the proof of Theorem 3.23 and directly in the proof of Theorem 3.9.

Lemma 3.29. *(a) For $n \in \mathbb{N}$ define $f(n)$ to be the number of tuples $(n_1, ..., n_t)$ of integers such that $n = n_1 \cdots n_t$ and each $n_i > 1$. Then there exists $\mu > 0$ such that $f(n) \leq n^\mu$ for every $n \in \mathbb{N}$.*

(b) There exists $d > 0$, depending only on k, such that the number of $v \in V_f$ with $q_v \leq n$ is bounded by dn. Since $q_v \neq 1$ this quantity is also bounded by n^b for some $b > 0$.

Proof. (a) The first result of Kalmar stated in [Erd41] tells us that

$$\sum_{m=1}^{n} f(m) = \frac{-1}{\beta\zeta'(\beta)} n^\beta (1 + o(1)).$$

Where β is the unique positive solution to $\zeta(\beta) = 2$ (ζ is the Riemann zeta function). Since $f(1) = 0$ we can simply choose μ large enough such that

$$f(n) \leq \sum_{m=1}^{n} f(m) = \frac{-1}{\beta\zeta'(\beta)} n^{\beta}(1 + o(1)) \leq n^{\mu}.$$

(b) If $\operatorname{char} k = 0$ then let $d = [k : \mathbb{Q}]$, we have

$$\begin{aligned} |\{v \in V_f : q_v \leq n\}| &\leq |\{v \in V_f : p_v \leq n\}| \\ &= |\{\mathfrak{p} \lhd \mathcal{O} : \mathfrak{p} \cap \mathbb{Z} = (p),\, p \leq n\}| \\ &\leq [k : \mathbb{Q}]|\{\text{primes } p \leq n\}| \\ &\leq dn. \end{aligned}$$

The finite characteristic case is dealt with by [Ros02, Theorem 5.12].

□

We are now prepared to prove the main theorem.

Proof of Theorem 3.9. Corollary 2.26 tells us that

$$G(\widehat{\mathcal{O}}_S) \cong \prod_{v \in V_f \setminus S} G(\mathcal{O}_v) \cong \prod_{v \in \mathcal{P}_2 \setminus S} G(\mathcal{O}_v) \times \prod_{v \in \mathcal{P}_1 \setminus S} G(\mathcal{O}_v) =: A \times B.$$

A is a finite product of profinite groups, and Corollary 3.25 tells us that each factor has PRG. Therefore A has PRG, and it is enough to prove that B has PRG. The issue now is that B is not a finite product. This is where we will need to leverage some sort of uniformity.

Let $\rho \in \operatorname{Irr}_n(B)$. Since B is a product of profinite groups we apply the Lemma 2.12. This tells us that for some finite t

$$\rho \cong \rho_1 \otimes \cdots \otimes \rho_t,$$

where each $\rho_i \in \operatorname{Irr}_{n_i}(G(\mathcal{O}_{v_i}))$ is nontrivial. Crucially, the $G(\mathcal{O}_{v_i})$ are perfect because $v_i \in \mathcal{P}_1$. In particular they admit no nontrivial one-dimensional representations. Therefore we have that $n_i \geq 2$. This bound on the dimensions of the ρ_i is one of the reasons we needed to treat $\mathcal{P}_2$ separately.

By Lemma 3.29 (a) the number of partitions $(n_1, ..., n_t) \in \mathbb{N}^t$ of n such that $n = n_1 \cdots n_t$ for some t is $\leq n^{\mu}$.

Now we bound for a fixed tuple $(n_1, ..., n_t)$ the number of choices of $G(\mathcal{O}_{v_i})$ such that $\rho_i \in \operatorname{Irr}_{n_i}(G(\mathcal{O}_{v_i}))$ is possible. For $G(\mathcal{O}_{v_i})$ to correspond to ρ_i it must

admit a nontrivial irreducible representation of dimension n_i. Given Proposition 3.28 we have a lower bound on the dimension of any nontrivial representation of $G(\mathcal{O}_{v_i})$. Therefore we must have that $q_{v_i}^{\delta} \leq n_i$. Rearranging this tells us that $q_{v_i} \leq n_i^{1/\delta}$.

Now applying Lemma 3.29 (b) with $n = n_i^{1/\delta}$, the number of valuations v_i for which this is possible is $\leq dn_i^{1/\delta}$. Therefore the total number of choices of $(v_1, ..., v_t)$ for which it is possible that $\rho_i \in \mathrm{Irr}_{n_i}(G(\mathcal{O}_{v_i}))$ is bounded above by

$$dn_1^{1/\delta} dn_2^{1/\delta} \cdots dn_t^{1/\delta} = d^t n^{1/\delta} \leq d^{\log_2(n)} n^{1/\delta}.$$

We know that $t \leq \log_2(n)$ because the $n_i \geq 2$.

Finally, Theorem 3.23 tells us that $r_{n_i}(G(\mathcal{O}_{v_i})) \leq cn_i^c$ for some c **independent of** v_i. Therefore the number of choices of $(\rho_1, ..., \rho_t)$ given a choice of valuations $(v_1, ..., v_t)$ is bounded above by

$$r_{n_1}(G(\mathcal{O}_{v_1})) \cdots r_{n_t}(G(\mathcal{O}_{v_t})) \leq cn_1^c \cdots cn_t^c = c^t n^c \leq c^{\log_2(n)} n^c.$$

To conclude, we have that

$$\begin{aligned} r_n(G(\widehat{\mathcal{O}}_S)) &= \#\{\text{partitions } n_1 n_2 \cdots n_t = n\} \cdot \#\{\text{allowable choices of } (v_1, ..., v_t)\} \\ &\quad \cdot \#\{\text{choices of representations } (\rho_1, ..., \rho_t)\} \\ &\leq n^{\mu} \cdot d^{\log_2(n)} n^{1/\delta} \cdot c^{\log_2(n)} n^c \\ &= n^{\mu} \cdot n^{\log_2(d)} n^{1/\delta} \cdot n^{\log_2(c)} n^c. \end{aligned}$$

So we have shown that $G(\widehat{\mathcal{O}}_S)$ has PRG. □

Theorem 3.23 and Proposition 3.28 are the main sticking points for this proof mathematically, while Lemma 3.29 simply provides necessary bounds for the combinatorics to work out. The two big things we used about the set of good primes $\mathcal{P}_1$ were Proposition 3.28 and the fact that for $v \in \mathcal{P}_1$, $G(\mathcal{O}_v)$ is perfect, hence admits only the trivial one-dimensional representation.

3.5 The bad primes

Before we deal with the good primes $\mathcal{P}_1$, it is important to deal with the bad primes in $\mathcal{P}_2$. We wish to show that for $v \in \mathcal{P}_2$, each $G(\mathcal{O}_v)$ has PRG. Since $\mathcal{P}_2$ is finite it is sufficient to show this in a non-uniform manner.

The following result would give one reason to believe that Theorem 3.23 is possible at all. It tells us that every local group has polynomial representation growth, though it is not necessarily uniform in v.

Lemma 3.30. *For every $v \in V_f$, there exists a $c > 0$ such that for every $n \in \mathbb{N}$, we have*

$$[G(\mathcal{O}_v) : K_n(G(\mathcal{O}_v))] \leq cn^c.$$

Proof idea. The full proof can be found in [LM04, Lemma 4.8] for $\operatorname{char} k = 0$ and [GR16, Theorem 3.1] for $\operatorname{char} k > 0$.

The idea is that $G(\mathcal{O}_v)$ has an open subgroup H which is p-adic analytic in the case of $\operatorname{char} k = 0$.

If $\operatorname{char} k = p$ then there is an analogous notion corresponding to the ring $\mathbb{F}_p[[t]]$ rather than $\mathbb{Z}_p$. These ideas are explored in [JZK07].

From here Assumption 3.2 kicks in to ensure that the Lie algebra associated to this open subgroup is perfect. (There is some work needed to reconcile various notions of the Lie algebra over various rings).

The key is that a natural filtration of the Lie algebra gives a filtration of H. The fact that the Lie algebra is perfect means that this decomposition behaves in a nice way with respect to taking commutator subgroups.

From here the idea is to leverage the pronilpotency of the open subgroup H. Any representation ρ of $G(\mathcal{O}_v)$ can be restricted to H. The restricted representation is then a sum of monomial representations, which are each induced off a subgroup M of index equal to the dimension. The subgroup M must be of some bounded "depth" with respect to the filtration. Then since the representation is one-dimensional $\ker \rho$ contains $[M, M]$, which is also of bounded "depth" because the filtration behaves nicely with respect to commutator subgroups. □

It is good to understand the ideas behind this proof, as they will recur when we deal with $\mathcal{P}_1$ in the next section. The open subgroup we use will be $N_1^{(v)}$, and we will leverage the pronilpotency of this subgroup to find some large subgroup of N_1^v contained in the kernel of the representation.

3.6 The good primes

3.6.1 Nontrivial representations of local groups

So far we have shown that we can deal with every $G(\mathcal{O}_v)$ factor in $G(\widehat{\mathcal{O}}_S)$ individually, that is to say each of them have PRG. The problem we now have is that $G(\widehat{\mathcal{O}}_S)$ is an infinite product, so in order to get PRG for this group we will need a uniformity result over the valuations $v \in V_f \setminus S$. Our aim in this section is to prove a uniform lower bound on the dimension of a nontrivial irrep of $G(\mathcal{O}_v)$.

The uniformity we are after starts as a result that holds for the good primes $v \in \mathcal{P}_1$. In particular it leverages knowledge of the classification of finite groups of Lie type. Recall that for $v \in \mathcal{P}_1$, condition (a) ensures that $G(\mathbb{F}_v)$ is a perfect finite central extension of a finite simple group of Lie type. Therefore any application of the lemma below to $G(\mathbb{F}_v)$ relies on the fact that $v \in \mathcal{P}_1$.

Lemma 3.31. *Let Φ be a perfect finite central extension of a finite simple group of Lie type $H(p^r)$. Then there exists $\delta > 0$ independent of p, r and H, such that any nontrivial complex projective representation has dimension at least $p^{r\delta}$ and any proper subgroup has index at least $p^{r\delta}$.*

To prepare the reader for the technicalities we give a sketch of the proof first. We take a projective representation of Φ and note that it lands in some number field (see Subsection 3.6.2). Reducing modulo a suitable prime gives a representation in some finite field. Finally we leverage classification information about the finite groups of Lie type to get a bound on the dimension of the representation we started with.

Proof. First we prove that the statement about representations implies the statement about subgroups. If $\Phi' \leq \Phi$ then Φ permutes the coset space Φ/Φ', which gives rise to a nontrivial projective representation of dimension exactly $[\Phi : \Phi']$ by the following composition

$$\Phi \to \mathrm{Perm}(\Phi/\Phi') \xrightarrow{\sim} S_{[\Phi:\Phi']} \hookrightarrow \mathrm{GL}_{[\Phi:\Phi']}(\mathbb{C}) \twoheadrightarrow \mathrm{PGL}_{[\Phi:\Phi']}(\mathbb{C}).$$

Next consider a nontrivial projective representation. The image lands in $\mathrm{PGL}_n(K)$ for K some number field.

We can use the projectivity of the representation to make sure that all matrix entries lie in $\mathcal{O}_K$. We can do this by multiplying by suitable integer scalar matrices. We can then view this representation modulo a suitable prime to get a nontrivial representation $\rho : \Phi \to \mathrm{PGL}_n(F)$ with $\mathrm{char}\,(F) \neq p$ or 0. Consider $\Phi/\ker\rho$, we claim that this is still a perfect central extension of $H(p^r)$. Indeed by definition Φ fits into a SES

$$1 \to Z \to \Phi \xrightarrow{\pi} H(p^r) \to 1,$$

with $Z \subset Z(\Phi)$. Now consider $\ker\rho \subset \Phi$ and note that $Z\ker\rho$ is a normal subgroup, since it is the product of a normal and a central subgroup. Therefore $\pi(Z\ker\rho) \subset H(p^r)$ is a normal subgroup. Since $H(p^r)$ is simple this implies that $\pi(Z\ker\rho) = H(p^r)$ or $\{1\}$.

If $\pi(Z\ker\rho) = H(p^r)$, then since $\pi(Z\ker\rho) = \pi(\ker\rho)$ we can pass to an exact sequence

$$1 \to Z/(\ker\rho \cap Z) \to \Phi/\ker\rho \to 1,$$

so $\Phi/\ker\rho$ is abelian. However Φ is perfect, so this tells us that $\Phi = \ker\rho$, contradicting the fact that ρ is nontrivial.

Therefore $\pi(Z\ker\rho) = \{1\}$, so by the correspondence theorem $Z\ker\rho = Z$ and hence $\ker\rho \subset Z$.

Therefore we may without loss of generality assume that ρ is injective.

Now by [KL$^+$90, Corollary 5.3.3 and Theorem 5.3.9], we see that the argument comes down to taking δ to be a minimum over a finite table of values. □

There are some nonobvious steps in the above proof. In particular the realisability of representations of a finite group in a number field. We cover this in Subsection 3.6.2.

Given that the aim of this section is to conclude a dimension bound on the representations of $G(\mathcal{O}_v)$, it is not clear why we are dealing with projective representations at all. Indeed an analogue of Lemma 3.31 for ordinary representations appears entirely within the realm of possibility. We will see in the proof of Proposition 3.28, that information about the projective representations of $G(\mathbb{F}_v)$ is exactly the information we need to conclude similar results for ordinary representations of $G(\mathcal{O}_v)$.

In order to turn Lemma 3.31 into a result about the dimensions of representations of $G(\mathcal{O}_v)$ we will need two more lemmas.

Lemma 3.32. *Let p be a prime and let $q = p^e$, where $e \in \mathbb{N}$. Let V, W, X be finite-dimensional vector spaces over $\mathbb{F}_q$, and let $T : V \times W \to X$ be an $\mathbb{F}_q$-bilinear map such that $T(V \times W)$ spans X over $\mathbb{F}_q$. Suppose that A, B are $\mathbb{F}_p$-subspaces of V, W such that*

$$[V : A][W : B] < q,$$

then $T(A \times B)$ spans X over $\mathbb{F}_p$.

This result likely seems intuitively plausible. Some care is required in the proof, which we relegate to the appendix (Lemma A.2). The proof does not introduce ideas that are important to the main project. However, Lemma 3.32 is important in the sense that it is used in the proof of both critical results Proposition 3.28 and Theorem 3.23.

We will typically apply the above lemma to the graded Lie algebra of $N_1^{(v)}$ and the graded Lie subalgebra corresponding to a subgroup, in order to say

something about where the subgroup sits with respect to the filtration by principal congruence subgroups. The following is a typical example, in which we use this technique to conclude something about low index subgroups of $N_1^{(v)}$.

Lemma 3.33. *Let $v \in \mathcal{P}_1$ and suppose that $H \leq N_1^{(v)}$ is an open subgroup such that $[N_1^{(v)} : H] < q_v^{1/2}$. Then $H \supset N_2^{(v)}, H \trianglelefteq N_1^{(v)}$ and $[H, H] = N_2^{(v)}$.*

Proof. Lemma 3.20 tells us that $[L^{(v)}, L^{(v)}(H)] = [N_1^{(v)} : H] < q_v^{1/2}$. Therefore the index of each grade must also be bounded. Specifically $[L_m^{(v)} : L_m^{(v)}(H)] < q_v^{1/2}$ for all $m \in \mathbb{N}$. Now note that for any $m \in \mathbb{N}$

$$[L_m^{(v)} : L_m^{(v)}(H)][L_1^{(v)} : L_1^{(v)}(H)] < q_v.$$

Now $L_m^{(v)}(H)$ and $L_1^{(v)}(H)$ are $\mathbb{F}_{p_v}$-subspaces of $L_m^{(v)}$ and $L_1^{(v)}$ respectively. The latter are $\mathbb{F}_{q_v}$-vector spaces by property (e) of $\mathcal{P}_1$ (Definition 3.16). We can now apply Lemma 3.32 to the Lie bracket

$$[\cdot, \cdot] : L_m^{(v)} \times L_1^{(v)} \to L_{m+1}^{(v)},\ (xN_{m+1}^{(v)}, yN_2^{(v)}) \mapsto [x, y]N_{m+2}^{(v)}.$$

This tells us that the $\mathbb{F}_{p_v}$-span of $[L_m^{(v)}(H), L_1^{(v)}(H)]$ is $L_{m+1}^{(v)}$. However addition in the Lie-algebra is just given by group multiplication, and the $\mathbb{F}_{p_v}$-scalar multiplication is just repeated addition. Therefore we have that $[L_m^{(v)}(H), L_1^{(v)}(H)] = L_{m+1}^{(v)}$ for all $m \in \mathbb{N}$. Now we note that

$$L_{m+1}(H) \supset [L_m^{(v)}(H), L_1^{(v)}(H)] = L_{m+1}^{(v)}.$$

Therefore $L_{m+1}^{(v)}(H) = L_{m+1}^{(v)}$ for all $m \geq 1$. Applying Proposition 3.21 we conclude that $H \supset N_2^{(v)}$. Since H contains the commutator subgroup $[N_1^{(v)}, N_1^{(v)}] = N_2^{(v)}$ it must be normal in $N_1^{(v)}$. The last thing to prove is that $[H, H] = N_2^{(v)}$. The first containment easily follows by condition (c) on $\mathcal{P}_1$

$$[H, H] \subset [N_1^{(v)}, N_1^{(v)}] = N_2^{(v)}.$$

The second containment is a little trickier. It relies on the observation that

$$[L_m^{(v)}(H), L_1^{(v)}(H)] \subset L_{m+1}([H, H]).$$

Which, after applying our previous analysis of the graded Lie subalgebra attached to H tells us that $L_{m+1}([H, H]) = L_{m+1}$ for all $m \in \mathbb{N}$. Again applying Proposition 3.21 we conclude that $[H, H] \supset N_2^{(v)}$, so $[H, H] = N_2^{(v)}$, as required. □

We are now ready to assemble these pieces into a proof of Proposition 3.28. The proof will include restricting a representation to $N_1^{(v)}$ and leveraging its monomiality. This is exactly the strategy foreshadowed in Section 3.5.

Proof of Proposition 3.28. Choose δ_1 as in Lemma 3.31. Define $\delta < \min\{1/2, \delta_1\}$. Let $v \in \mathcal{P}_1$ and let $(\rho, V) \in \mathrm{Irr}(G(\mathcal{O}_v))$ be nontrivial. We will prove that $\dim V \geq q_v^{\delta}$.

Consider $\rho|_{N_1^{(v)}}$, this gives a direct sum decomposition of $V = W_1 \oplus \cdots \oplus W_m$ into irreducible representations of $N_1^{(v)}$. After reordering let $W := W_1 \oplus \cdots \oplus W_r$ be the first isotypic component, that is, $W_1 \cong W_i$ if and only if $i \leq r$. We now deal with the case $W \neq V$ and $W = V$ separately.

Suppose $W \neq V$: Let H be the inertial subgroup of $G(\mathcal{O}_v)$ corresponding to the representation $(\rho|_{N_1^{(v)}}, W_1)$. Equivalently

$$H = \{g \in G(\mathcal{O}_v) : (\rho^g|_{N_1^{(v)}}, W_1) \cong (\rho|_{N_1^{(v)}}, W_1)\}.$$

Since $W \neq V$, H is a proper subgroup of $G(\mathcal{O}_v)$. Indeed by Theorem 1.35 we know that $\rho|_{N_1^{(v)}}$ is given by a sum of irreducible representations which differ only by first conjugating with something in $G(\mathcal{O}_v)$. If $G(\mathcal{O}_v) = H$ then all of these irreducible components are isomorphic, which would mean that $W = V$.

By Theorem 1.37 let $\sigma \in \mathrm{Irr}(H)$ be such that $\rho = \mathrm{Ind}_H^{G(\mathcal{O}_v)}(\sigma)$, hence

$$\begin{aligned}\dim(\rho) = \dim(\mathrm{Ind}_H^{G(\mathcal{O}_v)}(\sigma)) &= [G(\mathcal{O}_v) : H] \dim(\sigma) \\ &\geq [G(\mathcal{O}_v) : H] = [G(\mathbb{F}_v) : H/N_1^{(v)}].\end{aligned}$$

Now $H/N_1^{(v)} \subsetneq G(\mathbb{F}_v)$ is a proper subgroup. Since $v \in \mathcal{P}_1$ we can apply Lemma 3.31, which gives us $\dim(\rho) \geq q_v^{\delta}$, as required.

Suppose $V = W$: In this case $V = \bigoplus_{i=1}^m W_i$ is a sum of isomorphic irreducible representations of $N_1^{(v)}$. Let $s = \dim(W_i)$. If $s \geq q_v^{\frac{1}{2}}$ we are done because $\dim V \geq s \geq q_v^{\frac{1}{2}} > q_v^{\delta}$.

So suppose that $s < q_v^{\frac{1}{2}}$. By Lemma 2.15 the representation W_i is induced from a one-dimensional representation of a subgroup M with $[N_1^{(v)} : M] = s < q_v^{\frac{1}{2}}$. So by Lemma 3.33 we have that $N_2^{(v)} \leq M \leq N_1^{(v)}$ and $[M, M] = N_2^{(v)}$. Since they are monomial, the irreps W_i descend to irreps of $N_1^{(v)}/[M, M] = N_1^{(v)}/N_2^{(v)}$, which is a finite abelian group. This tells us that $s = 1$.

Now bringing our focus back to the representation V of $G(\mathcal{O}_v)$ we have a decomposition into one-dimensional subspaces

$$V = \bigoplus_{i=1}^m W_i.$$

The action of $N_1^{(v)}$ respects this decomposition, and the W_i are all isomorphic representations of $N_1^{(v)}$; this tells us that $N_1^{(v)}$ acts as scalar multiplication on V. Therefore we can construct a projective representation $\bar{\rho}$ of $G(\mathbb{F}_v)$ in the following way

$$\begin{array}{ccc} G(\mathcal{O}_v) & \xrightarrow{\quad\rho\quad} & \mathrm{GL}(V) \\ \downarrow & & \downarrow \\ G(\mathbb{F}_v) \cong G(\mathcal{O}_v)/N_1^{(v)} & \xrightarrow{\bar{\rho}} & \mathrm{PGL}(V). \end{array}$$

This is a projective representation of $G(\mathbb{F}_v)$. If $\bar{\rho}$ were trivial then $G(\mathcal{O}_v)$ would acts as scalar multiplication on V. However irreducibility V would mean that V is one-dimensional, but $G(\mathcal{O}_v)$ is perfect by property (d) of $\mathcal{P}_1$, hence admits no nontrivial one-dimensional representations. Therefore $\bar{\rho}$ is nontrivial and by Lemma 3.31 we have $\dim(V) \geq q_v^{\delta_1} > q_v^{\delta}$, as required. □

With the proof concluded, we have successfully placed a lower bound on the dimension of any nontrivial irrep of $G(\mathcal{O}_v)$, for $v \in \mathcal{P}_1$.

Remark 3.34. In the $V = W$ case of the above proof we see why projective representations of $G(\mathbb{F}_v)$ were introduced. Using knowledge of $\rho|_{N_1^{(v)}}$ we were allowed to pass from a representation of $G(\mathcal{O}_v)$ to a representation of $G(\mathbb{F}_v)$, at the cost of moving from an ordinary representation to a projective representation. Many steps in this section are insensitive to whether we have a dimension bound for the ordinary or projective representations of $G(\mathbb{F}_v)$. For this particular step it is critical that we know about the projective representations rather than the ordinary representations of $G(\mathbb{F}_v)$.

3.6.2 A representation theoretic detour

In this subsection we take a representation theoretic detour regarding some of the steps involved in proving Lemma 3.31. Specifically the claim that any complex projective representation of a finite group is in fact realisable in some number field K. The uninterested reader may skip this section and still fully understand the main project that follows.

Definition 3.35. A complex (projective) representation of a finite group is realisable over a ring $A \subset \mathbb{C}$ if there exists some basis with respect to which all matrix entries are elements of A.

There are reasons to believe that all complex projective representations are realisable over a number field K. Indeed since the group is finite, for any representation ρ the matrix elements $\rho(g)$ satisfy a system of polynomial equations with coefficients in $\mathbb{Z}$, because $\rho(g)^n = 1$ for some n, however this is a far cry from the claim that every individual entry of this matrix satisfies a polynomial equation with rational coefficients.

A paper by Reynolds [Rey65] proves this claim. A slightly later paper [AK67] proves the same thing but by analysing covering groups, which can be used to lift projective representations to ordinary representations. To state this precisely:

Theorem 3.36. *Every finite group Φ has a finite covering group $\widetilde{\Phi}$, which comes with map $\varphi : \widetilde{\Phi} \to \Phi$. This has the property that for every projective representation $\rho : \Phi \to \mathrm{PGL}_n(\mathbb{C})$ there exists an ordinary representation $\widetilde{\rho} : \widetilde{\Phi} \to \mathrm{GL}_n(\mathbb{C})$ making the following diagram commute*

$$\begin{array}{ccc} \widetilde{\Phi} & \xrightarrow{\widetilde{\rho}} & \mathrm{GL}_n(\mathbb{C}) \\ \downarrow{\scriptstyle \varphi} & & \downarrow \\ \Phi & \xrightarrow{\rho} & \mathrm{PGL}_n(\mathbb{C}). \end{array}$$

This theorem is due to Schur [Sch04]. In light of it, we will focus on realising ordinary representations of finite groups in a number field.

The definitions and arguments that follow are adapted from pages 90-92 and 94 of [Ser77]. The interested reader is encouraged to browse the surrounding material at their leisure.

Definition 3.37. Define $R(\Phi)$ to be the $\mathbb{Z}$-span of all characters of complex finite-dimensional representations of Φ.

Definition 3.38. Define $R_K(\Phi) \subset R(\Phi)$ to be the $\mathbb{Z}$-span of all characters of finite-dimensional representations of Φ, realisable over K.

These are lattices inside the vector space of class functions on Φ, so we have the G-invariant inner product defined in Theorem 1.24 to make sense of the following.

Lemma 3.39. *The complex irreducible characters realisable over K form an orthonormal basis for $R_K(\Phi)$.*

Proof. The complex irreducible characters realisable over K span $R_K(\Phi)$ by definition. Orthonormality comes from Theorem 1.24 given that a representation defined over K is a complex representation, and orthogonality gives linear independence. □

Proposition 3.40. *A complex representation is realisable over $K \subset \mathbb{C}$ iff its character is in $R_K(\Phi)$.*

Proof. The forwards implication is obvious.

For the reverse implication suppose that χ is a character in $R_K(\Phi)$. By Lemma 3.39 χ as a linear combination of the χ_i that form a basis for $R_K(G)$. This is an integer linear combination because everything in sight is a complex representation, and so $V = \oplus_i n_i V_i$, where $n_i = \langle \chi, \chi_i \rangle$. □

Our problem can now be rephrased as finding a number field K such that $R_K(\Phi) = R(\Phi)$. Nothing we have done so far gives any indication of how one might find this field.

For one-dimensional representations this question is easy. A one-dimensional representation is simply a homomorphism $\Phi \to \mathbb{C}^\times$. Any element of Φ must be sent to a complex number with finite multiplicative order, so the image lies in $\mathbb{Q}(\zeta_n)$, where n is the lcm of the orders of elements in Φ.

One is left to wonder if there is a way to bootstrap from the one-dimensional case to the general case. These prayers are answered by a result known as Brauer's Theorem. To state it we need a definition.

Definition 3.41. A p-elementary subgroup of a group Φ is a subgroup isomorphic to a product of a p-group and a cyclic group of order coprime to p

Theorem 3.42 (Brauer's Theorem)**.** *$R(\Phi)$ is spanned as an abelian group by characters induced from p-elementary subgroups.*

Proof Sketch. For full proof see [Ser77, Section 10.5, Theorems 19 and 20], we will give a very brief sketch.

If V_p is the span of characters induced from p-elementary subgroups of Φ then one can prove that $[R(\Phi) : V_p]$ is finite and coprime with p.

Then one is forced to conclude that $\oplus_p V_p = R(\Phi)$ by noting that the index of the left hand side must be finite and coprime to any prime number p. □

Our desired result becomes a corollary.

Corollary 3.43. *All complex representations of a finite group Φ are realisable over $\mathbb{Q}(\zeta_n)$, where n is the lcm of the orders of elements in Φ. n is also known as the Schur index of Φ.*

Proof. One starts by noting that p-elementary groups are nilpotent and so all characters of p-elementary groups are themselves monomial.

Take χ to be the character of any given representation. Then by Brauer's theorem it is an integer linear combination of characters induced from p-elementary subgroups, which are themselves induced from one-dimensional characters. One-dimensional characters on all subgroups of Φ are realisable over $\mathbb{Q}(\zeta_n)$, since they are simply homomorphisms into $\mathbb{C}^\times$.

Now note that Ind_H^Φ maps $R_{\mathbb{Q}(\zeta_n)}(H) \to R_{\mathbb{Q}(\zeta_n)}(\Phi)$ for *any* subgroup H. This is because if (ρ, V) is a representation of H then the induced representation acts on the vector space $\bigoplus_{g_i \in \Phi/H} g_i V$ by first permuting the factors, then acting according to ρ. Therefore the matrices for $\mathrm{Ind}_H^\Phi(\rho)(g)$ are "monomial in $\rho(h)$", meaning they can be written in block form like a permutation matrix, where the nonzero entries correspond to matrices of the form $\rho(h)$ for some $h \in H$.

So we conclude that $\chi \in R_{\mathbb{Q}(\zeta_n)}(\Phi)$. Therefore the representation associated to χ is realisable over $\mathbb{Q}(\zeta_n)$ by Proposition 3.40. □

Remark 3.44. Notice that the above actually proves that representations of a finite group Φ are realisable over $\mathbb{Z}[\zeta_n]$ for suitable n. Therefore the step in the proof of Lemma 3.31 where we scaled our matrices to ensure all entries lay in the ring of integers $\mathcal{O}_K$ was actually unnecessary if we took $K = \mathbb{Q}(\zeta_n)$ via this proof.

There is a slightly more general question one could ask. If a complex representation is realisable over some number field K, is it necessarily realisable over the ring of integers $\mathcal{O}_K$?

The answer in general is no, as proven in a paper by Cliff, Ritter and Weiss [RCW92]. However if $\mathcal{O}_K$ is a principal ideal domain the then the answer is yes. This can be proved using the classification of modules over a principal ideal domain.

3.6.3 Local polynomial representation growth

Turning our attention back toward the main project, we are almost ready to prove the critical Theorem 3.23. The proof will rely on a new proposition that leverages the graded Lie algebra, as well as Proposition 3.28 and Lemma 3.32, which we proved in Subsection 3.6.1.

Proposition 3.45. *Let $v \in \mathcal{P}_1$ and let $H \leq N_1^{(v)}$ have index at most n. Then $H \supset N_{2r+3}^{(v)}$, where*

$$r = \left\lfloor \frac{\log_{p_v} n}{e_v} \right\rfloor$$

and $[H, H] \supset N_{4r+6}^{(v)}$.

Proof. We have $[L^{(v)} : L^{(v)}(H)] = [N_1^{(v)} : H] \leq n$. Note that

$$\left\lfloor \frac{\log_{p_v} n}{e_v} \right\rfloor = r \implies \frac{\log_{p_v} n}{e_v} < r+1 \implies n < q_v^{r+1}.$$

Guided by this we consider for any $s \geq 2r+2$ the following pairing of factors

$$\underbrace{\left[L_1^{(v)} : L_1^{(v)}(H)\right] \ldots \left[L_{r+1}^{(v)} : L_{r+1}^{(v)}(H)\right] \ldots \left[L_{s-r}^{(v)} : L_{s-r}^{(v)}(H)\right] \ldots \left[L_s^{(v)} : L_s^{(v)}(H)\right]}_{\vdots}.$$

This product gives the index of the grades up to s, so $[L^{(v)} : L^{(v)}(H)] < q_v^{r+1}$. Since we have marked out exactly $r+1$ pairs, there must be some $1 \leq i \leq r+1$ such that

$$[L_i^{(v)} : L_i^{(v)}(H)][L_{s-i+1}^{(v)} : L_{s-i+1}^{(v)}(H)] < q_v.$$

Now applying Lemma 3.32 to $L_i(H)$ and $L_{s-i+1}(H)$ we have

$$L_{s+1}^{(v)}(H) \supset [L_i^{(v)}(H), L_{s-i+1}^{(v)}(H)] = L_{s+1}^{(v)}.$$

Therefore $L_m^{(v)}(H) = L_m^{(v)}$ for all $m = s+1 \geq 2r+3$, so by Proposition 3.21 $H \supset N_{2r+3}^{(v)}$. By condition (c) on $\mathcal{P}_1$

$$[H, H] \supset [N_{2r+3}^{(v)}, N_{2r+3}^{(v)}] = N_{4r+6}^{(v)}.$$

□

The lemma above is another example of how the graded Lie algebra allows us to conclude things about $G(\mathcal{O}_v)$. We are now ready to prove Theorem 3.23, which is of independent interest, as it is far stronger than simply a polynomial representation growth result for $G(\mathcal{O}_v)$.

Proof of Theorem 3.23. We know from Section 3.5 that $[G(\mathcal{O}_v) : K_n(G(\mathcal{O}_v))]$ is polynomially bounded for all $v \in V_f$, so it suffices to bound $[G(\mathcal{O}_v) : K_n(G(\mathcal{O}_v))]$ uniformly polynomially for $v \in \mathcal{P}_1$.

To this end let $\rho \in \mathrm{Rep}(G(\mathcal{O}_v))$ be of dimension at most n for some $v \in \mathcal{P}_1$. If ρ is trivial there is nothing to prove, so assume ρ is nontrivial. Consider $\rho|_{N_1^{(v)}}$. This

decomposes into irreducibles of dimension at most n. Fix some irreducible and call it σ. Since $N_1^{(v)}$ is pro-p, σ is induced from a one-dimensional representation of some subgroup $H \leq N_1^{(v)}$ of index at most n. Therefore $[H, H] \subset \ker \sigma$.

Now $v \in \mathcal{P}_1$, ρ and σ were chosen arbitrarily, but Proposition 3.45 applies to any subgroup $H \leq N_1^{(v)}$ of index at most n. Therefore we have

$$K_n(G(\mathcal{O}_v)) \supset \bigcap_{[N_1^{(v)}:H] \leq n} [H, H] \supset N_{4r+6}^{(v)},$$

with r is as in Proposition 3.45. Now it suffices to prove that $[G(\mathcal{O}_v) : N_{4r+6}^{(v)}]$ is polynomially bounded in n, uniformly in $v \in \mathcal{P}_1$. Recall the notation we defined in Section 3.1. Certainly $|G(\mathbb{F}_v)| \leq q_v^{N^2}$ since there are at most q_v choices for each of the N^2 entries of any matrix in $G(\mathbb{F}_v)$. Hence

$$\begin{aligned}
[G(\mathcal{O}_v) : N_{4r+6}^{(v)}] &= |G(\mathbb{F}_v)|[N_1^{(v)} : N_{4r+6}^{(v)}] \\
&\leq q_v^{N^2} q_v^{(4r+5)N^2} && \text{Condition (b) of } \mathcal{P}_1 \\
&\leq q_v^{N^2} p_v^{e_v(4\frac{\log_{p_v} n}{e_v})N^2} q_v^{5N^2} \\
&= q_v^{6N^2} p_v^{4\log_{p_v}(n)N^2} \\
&= q_v^{6N^2} n^{4N^2}.
\end{aligned}$$

Since ρ is nontrivial and $v \in \mathcal{P}_1$, we have from Proposition 3.28 that $q_v \leq n^{\frac{1}{\delta}}$. Hence

$$[G(\mathcal{O}_v) : K_n(G(\mathcal{O}_v))] \leq [G(\mathcal{O}_v) : N_{4r+6}^{(v)}] \leq n^{\frac{6N^2}{\delta} + 4N^2}.$$

Since every step was independent of $v \in \mathcal{P}_1$, we are done. □

In this proof we again see the theme of restricting our representation to $N_1^{(v)}$ and leveraging monomiality. In this case we used the extra constraints of $\mathcal{P}_1$ in various places to get a uniform polynomial bound. As such we can regard this argument as a more refined version of Lemma 3.30.

With this result proven we have filled in all the pieces we used to prove Theorem 3.9. Therefore we have proven Theorem 3.1, the main goal of the chapter.

3.7 Image growth

3.7.1 Image growth results

In the process of proving Theorem 3.3 we proved that the local groups $G(\mathcal{O}_v)$ have a sequence of normal subgroups $K_n(G(\mathcal{O}_v))$ of polynomially bounded index such

that they are contained in the kernel of any representation of dimension at most n. This easily provides a polynomial bound on the image growth of representations of $G(\mathcal{O}_v)$. In this section we use earlier results to prove various bounds on the images of representations of $G(\widehat{\mathcal{O}}_S)$. Some of these will interestingly be of use when proving the partial converse to our main theorem in Chapter 4.

A natural place to start is with irreducible representations. Due to the transparent structure of irreps of $G(\mathcal{O}_v)$, we can recover a polynomial image growth result for the irreducible representations of $G(\widehat{\mathcal{O}}_S)$. The following proposition does not appear in the original work of Lubotzky and Martin [LM04], we add it here as a small contribution to the literature. It will underscore the added difficulty of moving from irreducible representations to all representations.

Proposition 3.46. *There exists $D > 0$ such that if $\rho \in \mathrm{Irr}_m(G(\widehat{\mathcal{O}}_S))$ with $m \leq n$, then $|\rho(G(\widehat{\mathcal{O}}_S))| \leq Dn^D$.*

Proof. Let $\rho \in \mathrm{Irr}_m(G(\widehat{\mathcal{O}}_S))$ be nontrivial with $m \leq n$. By Corollary 2.26 and Lemma 2.12 we have that

$$\rho \cong \rho_1 \otimes \cdots \otimes \rho_t,$$

where $\rho_i \in \mathrm{Irr}_{n_i}(G(\mathcal{O}_{v_i}))$ and $m = n_1 \cdots n_t$. Let c be as in Theorem 3.23, then

$$\begin{aligned}
|\rho(G(\widehat{\mathcal{O}_S}))| &= [G(\widehat{\mathcal{O}_S}) : \ker \rho] \\
&\leq [G(\mathcal{O}_{v_1}) : \ker \rho_1] \cdots [G(\mathcal{O}_{v_t}) : \ker \rho_t] \\
&\leq [G(\mathcal{O}_{v_1}) : K_{n_1}(G(\mathcal{O}_{v_1}))] \cdots [G(\mathcal{O}_{v_t}) : K_{n_t}(G(\mathcal{O}_{v_t}))] \\
&\leq cn_1^c \cdots cn_t^c \\
&\leq c^t n^c.
\end{aligned}$$

Now for $v \in \mathcal{P}_1$, there are no nontrivial one-dimensional representations of $G(\mathcal{O}_v)$ because the group is perfect. Therefore $t \leq |\mathcal{P}_2| + \log_2(n)$, from which

$$|\rho(G(\widehat{\mathcal{O}_S}))| \leq c^t n^c \leq c^{|\mathcal{P}_2|} c^{\log_2(n)} n^c = c^{|\mathcal{P}_2|} n^{\log_2(c)+c}.$$

Since ρ was chosen arbitrarily we have proven that the irreducible representations of $G(\widehat{\mathcal{O}_S})$ have polynomial image growth. □

For our purposes in the Chapter 4 we will need a bound on the image growth not just of irreducible representations, but of all representations of $G(\widehat{\mathcal{O}_S})$. The structure of a representation of $G(\widehat{\mathcal{O}_S})$ is less transparent than the structure of an irrep. To deal with this we are forced to slightly worsen our bound on the image and settle for a result that holds only in the limit.

We begin with two lemmas that will help us in this more complicated situation.

Lemma 3.47. *Let $d, a \in \mathbb{N}$. Then $\frac{1}{a+1}d^{a+1} \leq \sum_{i=1}^{d} i^a \leq d^{a+1}$.*

The proof of this lemma is a straightforward induction. We relegate the proof to the appendix (Lemma A.3)

Lemma 3.48. *Let $t \in \mathbb{N}$ and let $H = H_1 \times \cdots \times H_t$ be a product of profinite groups. If $\rho \in \mathrm{Rep}_n(H)$ and $n_i(\rho)$ is the maximum dimension among the irreducible components of $\rho|_{H_i}$, then*

$$\sum_{n_i(\rho)>1} n_i(\rho) \leq n.$$

Proof. First suppose that ρ is irreducible. Then

$$\rho \cong \rho_1 \otimes \cdots \otimes \rho_t,$$

where each $\rho_i \in \mathrm{Irr}_{n_i}(H_i)$ and $n = n_1 n_2 \cdots n_t$.

Clearly $\rho|_{H_i} \cong \underbrace{\rho_i \oplus \cdots \oplus \rho_i}_{n/n_i}$ and so $n_i(\rho) = n_i$. Therefore

$$\sum_{n_i(\rho)>1} n_i(\rho) = \sum_{n_i>1} n_i \leq n_1 \cdots n_t = n.$$

Now suppose $\rho = \rho_1 \oplus \rho_2$ is reducible. Certainly $n_i(\rho) = \max\{n_i(\rho_1), n_i(\rho_2)\}$, so we can induct on the number of irreducible components to get

$$\sum_{n_i(\rho)>1} n_i(\rho) \leq \sum_{n_i(\rho_1)>1} n_i(\rho_1) + \sum_{n_i(\rho_2)>1} n_i(\rho_2) \leq \dim(\rho_1) + \dim(\rho_2) = n.$$

□

With these lemmas behind us we are ready to prove our bound on the image growth of all representations of $G(\widehat{\mathcal{O}}_S)$.

Proposition 3.49. *There exists $\gamma \in (0,1)$ such that if n is large enough then for every $\rho \in \mathrm{Rep}_n(G(\widehat{\mathcal{O}}_S))$, we have $|\rho(G(\widehat{\mathcal{O}}_S))| \leq e^{n^\gamma}$.*

In contrast to previous results, this holds only for sufficiently large n. When disproving polynomial representation growth in Chapter 4 we will only need information about infinitely many n, so this will be sufficient for our purposes.

Proof. We begin by regarding $G(\widehat{\mathcal{O}}_S)$ as the product $\prod_{v \in V_f \setminus S} G(\mathcal{O}_v)$. From this we see that any representation descends to a representation of a finite product $G(\mathcal{O}_{v_1}) \times \cdots \times G(\mathcal{O}_{v_t})$.

For any $\rho \in \mathrm{Rep}_n(G(\mathcal{O}_v)$, let $n_i := n_i(\rho)$ as in Lemma 3.48. We use the full strength of Theorem 3.23 to say that $\rho|_{G(\mathcal{O}_{v_i})}$, while being a direct sum of possibly many nonisomorphic representations of dimension at most n_i, must descend to a representation of $G(\mathcal{O}_{v_i})/K_{n_i}(G(\mathcal{O}_{v_i}))$. Therefore we may regard any ρ as a representation of the finite group $G(\mathcal{O}_{v_1})/K_{n_1}(G(\mathcal{O}_{v_1})) \times \cdots \times G(\mathcal{O}_{v_t})/K_{n_t}(G(\mathcal{O}_{v_t})$. Note that t is dependent on ρ. Therefore

$$\begin{aligned}\sup_{\dim(\rho)=n} |\rho(G(\widehat{\mathcal{O}}_S))| &\leq \sup_{\dim(\rho)=n} \prod_{i=1}^{t} |G(\mathcal{O}_{v_i})/K_{n_i}(G(\mathcal{O}_{v_i}))| && \text{Theorem 3.23} \\ &\leq \sup_{\sum_i n_i(\rho)\leq n} c^t(n_1(\rho)\cdots n_t(\rho))^c && \text{Lemma 3.48.}\end{aligned}$$

Both the $n_i(\rho)$ and t are dependent on ρ in a complicated way. The first thing we wish to do is remove the complexity introduced by the choice of $n_i(\rho)$. We do this by optimising a function over a domain that includes all possible choices of $n_i(\rho)$ and more. We consider the function

$$f : \Delta := \left\{ (x_1, ..., x_t) \in \mathbb{R}^t : x_i \geq 0, \sum_i x_i \leq n \right\} \to \mathbb{R},\ f(x_1, ..., x_t) = x_1 \cdots x_t.$$

Elementary calculus tells us that the maximum of this function occurs at the point $f(n/t, ..., n/t) = (n/t)^t$. The domain is certainly much larger than the valid possibilities of $n_i(\rho)$, so we have

$$\sup_{\sum_i n_i(\rho)\leq n} c^t(n_1(\rho)\cdots n_t(\rho))^c \leq \sup_t \max_{(x_1,...,x_t)\in\Delta} c^t f(x_1, ..., x_t)^c \leq \sup_t c^t(n/t)^{tc}. \tag{3.2}$$

We still have a complicated dependence of t on ρ. To remove this we take the same approach as before. We attempt to find an upper bound for t in terms of n; this will give us a closed bounded interval over which to optimise this function of t. Lemma 3.30 allows us to assume that $v_1, ..., v_t \in \mathcal{P}_1$. (Specifically, any factors corresponding to some $v \in \mathcal{P}_2$ will contribute to the image some polynomially bounded amount, which we can ignore in the limit by increasing γ slightly).

For $m \in \mathbb{N}$, Proposition 3.28 tells us that any $G(\mathcal{O}_v)$ admitting a nontrivial representation of dimension m must satisfy $q_v^\delta \leq m$, while Lemma 3.29 (b) tells us that the number of $v \in \mathcal{P}_1$ with $q_v \leq m^{\frac{1}{\delta}}$ is less than $m^{\frac{b}{\delta}}$. Therefore the number of $v \in \mathcal{P}_1$ admitting a nontrivial representation of dimension m is bounded above by m^a where $a = \frac{b}{\delta}$. With this in mind we now have

$$2^a \cdot 2 + 3^a \cdot 3 + \cdots d^a \cdot d \leq n_1(\rho) + \cdots + n_t(\rho),$$

for any d such that $2^a + 3^a + \cdots + d^a \leq t$. This comes from supposing that the $n_i(\rho)$ are as small as possible. Now applying Lemma 3.47 to the LHS and Lemma 3.48 to the RHS we get that

$$\frac{1}{a+2}d^{a+2} \leq n. \tag{3.3}$$

Applying the second inequality in Lemma 3.47 we get that

$$2^a + 3^a + \cdots + d^a \leq d^{a+1},$$

so any d such that $d^{a+1} \leq t$ is a valid choice of d. In particular choosing $d = \left\lfloor t^{\frac{1}{a+1}} \right\rfloor$ and substituting into Equation 3.3 we get

$$\frac{1}{a+2}\left\lfloor t^{\frac{1}{a+1}} \right\rfloor^{a+2} \leq n \implies t^{\frac{1}{a+1}} \leq (a+2)^{\frac{1}{a+2}} n^{\frac{1}{a+2}} + 1.$$

Rearranging for t and applying the binomial theorem we have for n sufficiently large that

$$\begin{aligned} t &\leq ((a+2)^{\frac{1}{a+2}} n^{\frac{1}{a+2}} + 1)^{a+1} \\ &= (a+2)^{\frac{a+1}{a+2}} n^{\frac{a+1}{a+2}} + O(n^{\frac{a}{a+2}}) \\ &\leq \beta n^{\frac{a+1}{a+2}} =: \beta n^{\gamma_0}. \end{aligned}$$

Define $\gamma_0 := \frac{a+1}{a+2}$ and $\beta > (a+2)^{\frac{a+1}{a+2}}$. We have achieved an upper bound on t, so we can now optimise this function to find an upper bound dependent only on n.

Consider the function $g : [1, \alpha] \to \mathbb{R}$, $g(y) = (n/y)^y$. After another elementary optimisation calculation we have that if $\ln n - \ln \alpha \geq 1$ then the maximum of this function is achieved at α. In the following application we will have $\alpha = \beta n^{\gamma_0}$ so since $\gamma_0 < 1$ we can ensure that $\ln n - \ln \alpha \geq 1$ by taking n sufficiently large.

Finally, let $\gamma \in (\gamma_0, 1)$. Following on from Equation 3.2 we have

$$\begin{aligned} \sup_t c^t (n/t)^{tc} &\leq \sup_{t \in [1, \beta n^{\gamma_0}]} c^t (n/t)^{tc} && \text{upper bound on } t \\ &\leq c^{\beta n^{\gamma_0}} (n/\beta n^{\gamma_0})^{c\beta n^{\gamma_0}} && \text{maximum of } g \\ &= (\beta^{-\beta c} c^{\beta})^{n^{\gamma_0}} n^{(1-\gamma_0)cbn^{\gamma_0}} \\ &\leq e^{n^{\gamma}} && n >> 0. \end{aligned}$$

To check the last inequality take ln of both sides and analyse which grows faster in the limit.

Stringing together all of the inequalities we worked through in the proof we get the desired bound on the image of any n-dimensional representation of $G(\widehat{\mathcal{O}}_S)$. $\square$

This result can be aptly described as an "exponential image growth" type result. Having dealt with both the irreducible and reducible representations of $G(\widehat{\mathcal{O}}_S)$, there is one more result we have to record before moving on to Chapter 4. It involves the local groups $G(\mathcal{O}_v)$ and their representations over fields of finite characteristic.

Proposition 3.50. *Let F be a finite field of characteristic $l \neq 0$; let $v \in V_f$ and let $\rho : G(\mathcal{O}_v) \to \mathrm{GL}_n(F)$ be a representation. Suppose that $l \neq p_v =: p$, then $|\rho(G(\mathcal{O}_v))| \leq Dn^D$ for some $D > 0$ depending only on G, k and v.*

Proof. Let ρ be as in the statement of the proposition and define $\sigma = \rho|_{N_1^{(v)}}$. $\sigma(N_1^{(v)})$ is a finite p-group and $l \neq p$, so we can lift σ to a complex representation $\widetilde{\sigma} : N_1^{(v)} \to \mathrm{GL}_n(\mathbb{C})$ (See Subsection 3.7.2). We have that

$$\ker \rho \supset \ker \sigma \supset \ker \widetilde{\sigma} \supset N_1^{(v)} \cap \ker \left(\mathrm{Ind}_{N_1^{(v)}}^{G(\mathcal{O}_v)}(\widetilde{\sigma}) \right).$$

Let $b = [G(\mathcal{O}_v) : N_1^{(v)}]$, then leveraging Theorem 3.23 we have

$$\begin{aligned} |\rho(G(\mathcal{O}_v))| &= [G(\mathcal{O}_v) : \ker \rho] \\ &\leq \left[G(\mathcal{O}_v) : N_1^{(v)} \cap \ker \left(\mathrm{Ind}_{N_1^{(v)}}^{G(\mathcal{O}_v)}(\widetilde{\sigma}) \right) \right] \\ &\leq [G(\mathcal{O}_v) : N_1^{(v)}][G(\mathcal{O}_v) : K_{bn}(G(\mathcal{O}_v))] \\ &\leq b \cdot c(bn)^c \qquad \text{Theorem 3.23.} \end{aligned}$$

So taking $D := cb^{c+1}$ gives the desired result. □

Remark 3.51. Interestingly this proof works independent of *which* finite field of characteristic l we take our representations in.

3.7.2 A second representation theoretic detour

In the proof of Proposition 3.50 we glibly remarked that any representation of a finite p-group in some finite field of characteristic not dividing p can be lifted to a complex representation, whose kernel is contained in the original representation. In this detour we justify this claim and study more broadly what it takes to change the field of a representation.

A naive approach to this problem is to take some representation over $\mathbb{F}_p$ and try to lift it to a representation over $\mathbb{Z}$ such that the reduction modulo p gives our

original representation back. One runs into trouble when the original representation is not realised over $\mathbb{F}_p$, and the fact that not all complex representations are realised over $\mathbb{Z}$ means we will have to do something more sophisticated.

If we bracket for now the issue of there existing a lift, we can focus on generalising the idea of "reducing a representation modulo p" to something that works for any complex representation. The natural generalisation of this idea is to assume that the representation is realisable over a ring of integers. Thankfully our earlier detour into representation theory (Subsection 3.6.2) gives us a ring of integers from which to salvage this approach.

This approach is inspired by [Lan02, Exercise 27, Chapter XVIII] another approach can be found in [Ser77, Chapter 18]. We begin by constructing a map Λ, which takes irreducible representations over $\mathbb{C}$ and returns representations over $\overline{\mathbb{F}_p}$.

Let (ρ, V) be an irreducible complex representation of a finite group G, by Corollary 3.43 and Remark 3.44 from the previous representation theoretic detour this representation is realisable over $\mathbb{Z}[\zeta_n]$ where n is the Schur index of G. This is simply a choice of basis for V. Now take some prime ideal $\mathfrak{p} \lhd \mathbb{Z}[\zeta_n]$ lying over p. Then $\mathbb{Z}[\zeta_n]/\mathfrak{p} \cong \mathbb{F}_{p^r}$ for some r. Viewing the matrix entries of $\rho(g)$ modulo p gives us a representation over $\mathbb{F}_{p^r}$ and hence over $\overline{\mathbb{F}_p}$. We call this representation $\Lambda(V)$; we also use Λ to denote the induced map on characters.

In general what is going on is the following. If E is a finitely generated free $\mathbb{Z}[\zeta_n]$-module with a G-action, we can take the tensor product with either $\mathbb{C}$ or $\mathbb{Z}[\zeta_n]/\mathfrak{p}$ to get a representation over $\mathbb{C}$ or $\mathbb{F}_{p^r}$ respectively. Given a representation over $\mathbb{F}_{p^r}$ we can tensor with $\overline{\mathbb{F}_p}$ to get a representation over $\overline{\mathbb{F}_p}$. Diagrammatically:

$$\mathbb{C} \otimes_{\mathbb{Z}[\zeta_n]} E \longleftarrow E \longrightarrow \mathbb{Z}[\zeta_n]/\mathfrak{p} \otimes_{\mathbb{Z}[\zeta_n]} E \longrightarrow \overline{\mathbb{F}_p} \otimes_{\mathbb{F}_{p^k}} \mathbb{Z}[\zeta_n]/\mathfrak{p} \otimes_{\mathbb{Z}[\zeta_n]} E.$$

From this point of view Λ uses results from Subsection 3.7.2 to reverse the left hand arrow. The map Λ is perfectly well defined for any choice of p, but in the case of $p \nmid |G|$ things are particularly nice.

Theorem 3.52. *If $p \nmid |G|$ then the map Λ constructed above is a bijection*

$$\{\textit{Irreps of } G \textit{ over } \mathbb{C}\} \overset{1:1}{\underset{\Lambda}{\rightarrow}} \{\textit{Irreps of } G \textit{ over } \overline{\mathbb{F}_p}\}.$$

Proof. The first thing to note is that since $\overline{\mathbb{F}_p}$ is algebraically closed and $p \nmid |G|$ the proof of Theorem 1.24 holds. We need algebraic closure for the existence of an eigenvalue in the proof of Schur's lemma [Ser77, Chapter 2 Proposition 4], and we

need the condition on the characteristic in order to define the inner product with respect to which the irreducible characters form an orthonormal basis. Therefore the set of irreducible characters over $\mathbb{C}$ and $\overline{\mathbb{F}_p}$ are the same cardinality (that of the number of conjugacy classes of G).

At this point we don't even know that Λ takes irreducible representations to irreducible representations. The key to this proof will be to consider what Λ does to the characters of representations. If $\chi : G \to \mathbb{C}$ is an irreducible complex character then $\Lambda(\chi)$ is the composition

$$\Lambda(\chi) : G \xrightarrow{\chi} \mathbb{Z}[\zeta_n] \to \mathbb{Z}[\zeta_n]/\mathfrak{p}.$$

The image of χ is contained in $\mathbb{Z}[\zeta_n]$ by our previous representation theoretic detour. The first step in defining Λ was a choice of basis for V, which does not change the character. The second step was reducing the matrix elements of the representation modulo $\mathfrak{p}$, which corresponds to projection onto $\mathbb{Z}[\zeta_n]/\mathfrak{p}$.

Now we note that if χ_i and χ_j are complex irreducible characters of G then

$$\langle \Lambda(\chi_i), \Lambda(\chi_j) \rangle = \delta_{ij} \in \mathbb{Z}[\zeta_n]/\mathfrak{p}.$$

From this we see that Λ maps irreducible representations to irreducible representations, furthermore it tells us that Λ is injective, since $\Lambda(\chi_i)$ and $\Lambda(\chi_j)$ are linearly independent if $i \neq j$. Since there are as many irreducible characters of G over $\mathbb{C}$ as there are over $\overline{\mathbb{F}_p}$, Λ is a bijection. □

This result completely classifies the representation theory of G over $\overline{\mathbb{F}_p}$ in terms of its complex representation theory (when $p \nmid |G|$). We use it to prove a more general statement than that which was used in the proof of Proposition 3.50.

Corollary 3.53. *Let $\rho : G \to \mathrm{GL}_N(F)$ be a representation of a finite group G in a finite field F with $\mathrm{char}\,(F) = p$. Suppose $p \nmid |G|$, then we can lift ρ to a representation $\tilde{\rho} : G \to \mathrm{GL}_N(\mathbb{C})$ over the complex numbers such that $\ker \rho \supset \ker \tilde{\rho}$.*

Proof. Let $\rho : G \to \mathrm{GL}_N(F)$ be as in the statement of the theorem. Decompose ρ into irreducible representations over $\overline{F} = \overline{\mathbb{F}_p}$. Since Λ is a bijection, each of these arise as the reduction of a complex representation modulo $\mathfrak{p} \lhd \mathbb{Z}[\zeta_n]$. Let $\widetilde{\rho} : G \to \mathrm{GL}_N(\mathbb{C})$ be the sum of these complex representations. Then certainly $\ker \rho \supset \ker \widetilde{\rho}$, since reducing the entries of a matrix modulo $\mathfrak{p}$ can only make more matrices the identity. □

Remark 3.54. The proof of this statement is independent of *which* finite field F of characteristic p one chooses, mirroring Remark 3.51. This can be viewed as a virtue of working over the algebraic closure $\overline{\mathbb{F}_p}$.

Chapter 4

Groups without the CSP

4.1 Proving a partial converse

In this section we prove a partial converse to the main Theorem 3.1. Fix notation as in Section 3.1, with the added assumption that G is simple and that $\operatorname{char} k = 0$.

Theorem 4.1. *Assume Conjecture A holds for $G(k)$. If $\widehat{r}_n(\Gamma)$ is polynomially bounded, then Γ has the CSP.*

Conjecture A (Margulis-Platonov Conjecture)**.** *For any non-central, finite index, normal subgroup $N \trianglelefteq G(k)$ there exists a finite index normal subgroup $W \trianglelefteq \prod_{v\in T} G(k_v)$ such that $N = \delta^{-1}(W)$, where*

$$\delta : G(k) \to \prod_{v\in T} G(k_v)$$

is the diagonal map and $T = \{v \in V \setminus S : G(k_v) \text{ is compact}\}$.

Though this conjecture may seem opaque, it is known to be true in almost all cases. For specifics see the interlude between Theorems 1.2 and 1.3 in [LM04], or more recently [PR10, Section 3.5].

The idea of the proof is to show that groups without the CSP fail to have PRG. Groups without the CSP all have some minimal complexity to their structure. We use this complexity to disprove polynomial representation growth.

The first step of this approach is the reason for the added assumptions in Theorem 4.1. In particular we need $\operatorname{char} k = 0$ and Conjecture A to use the following result.

Lemma 4.2 (Rapinchuk's Lemma)**.** *Suppose* $\operatorname{char} k = 0$*, Conjecture A holds and that* Γ *fails to have the congruence subgroup property. Then there is some finite index subgroup* $\Gamma_0 \leq \Gamma$*, such that* $\widehat{\Gamma}_0$ *surjects onto a group* E *of the of the form*

$$1 \to W \to E \to H \to 1,$$

where $W = \prod_{i=1}^{\infty} F$ *for some finite simple group* F*. There are three cases:*

(a) F *is non-abelian and* H *is an open subgroup of* $G(\widehat{\mathcal{O}}_S)$*;*

(b) $F = C_l$ *is abelian and* H *is an open pro-*p_v *subgroup of* $G(\mathcal{O}_v)$*, for some* $v \in V_f \setminus S$*;*

(b1) $l \neq p_v$*;*

(b2) $l = p_v$*.*

Proof. See [Lub95, Sections 2.1-2.6]. □

Rapinchuk's Lemma is only proven in characteristic 0 with Conjecture A. The extent to which these facts can be salvaged in positive characteristic will determine how far the proof we present will go in the positive characteristic case. We now give a very short proof of Theorem 4.1, shifting all of the work into the Propositions and Lemmas to come.

Proof of Theorem 4.1. Suppose that Γ does not have CSP, then by Rapinchuk's Lemma there is a finite index subgroup $\Gamma_0 \leq \Gamma$, whose profinite completion $\widehat{\Gamma}_0$ surjects onto a group E of the form in case (a), (b1) or (b2) of Rapinchuk's Lemma.

Applying Corollary 2.6 and Lemma 2.3 we have that $\widehat{r}_n(\Gamma)$ is polynomially bounded if and only if $\widehat{r}_n(\Gamma_0) = r_n(\widehat{\Gamma}_0) \geq r_n(E)$ is. Propositions 4.3, 4.5 and 4.6 show that $r_n(E)$ is not polynomially bounded in cases (a), (b1) and (b2) respectively. Therefore $\widehat{r}_n(\Gamma)$ is not polynomially bounded, as required. □

We have thus reduced the problem to disproving PRG for groups of the form E in Rapinchuk's Lemma. The proofs for cases (a) and (b1) work in positive characteristic, while the proof of (b2) only works in characteristic 0.

Proposition 4.3 (Case a)**.** *Let E be a profinite group admitting a SES of the form*

$$1 \to W \to E \xrightarrow{\pi} H \to 1,$$

where $H \leq G(\widehat{\mathcal{O}_S})$ is finite index and $W = \prod_{i=1}^{\infty} F$, where F is non-abelian finite and simple. That is to say let E be as in case (a) of Rapinchuk's Lemma. Then for some $\varepsilon > 0$ and $c > 1$ we have

$$\log_c R_n(E) > \varepsilon \log_c n \log_c \log_c n,$$

for infinitely many n. In particular, E does not have PRG.

Heuristic 4.4. The idea of the proof is to use the structure of W to build many representations of a finite index subgroup of E. We use a different subgroup for different n. From there we apply results from Section 3.7 to bound the index of these subgroups. This ties the representation growth of E to the finite index subgroups, allowing us to disprove PRG for E.

The proof of this result given in [LM04] is (understandably) light on some details. We give an expanded proof, including extra lemmas that have been relegated to Appendix A. Despite the straightforward idea, this is a by far the longest single proof in the thesis.

Proof. Choose $\gamma, \gamma_1, \gamma_2, \gamma_3$ such that $0 < \gamma' < \gamma < \gamma_3 < 1$, $0 < \gamma_1 < \gamma_2 < 1 - \gamma_3$, with γ' as in Proposition 3.49.

Let $U \triangleleft E$ be an open normal subgroup of E. Passing to the relevant quotients we get a SES of finite groups

$$1 \to W/(W \cap U) \to E/U \xrightarrow{\pi} H/\pi(U) \to 1.$$

Name these groups W', E' and H'. Due to simplicity and finiteness of F we have that $W' \cong F^m$. By a judicious choice of U we can make m any number we like.

Since W' is normal in E' we know that E' acts by conjugation on W'. We wish for this action to be faithful. To achieve this note that

$$C_{E'}(W') \cap W' = Z(W') = 1,$$

because F was assumed to be non-abelian and simple. Therefore we can enlarge U to be the preimage of $C_{E'}(W')$ in E without changing m. Our situation now is an exact sequence of finite groups

$$1 \to F^m \to E' \xrightarrow{\pi} H' \to 1,$$

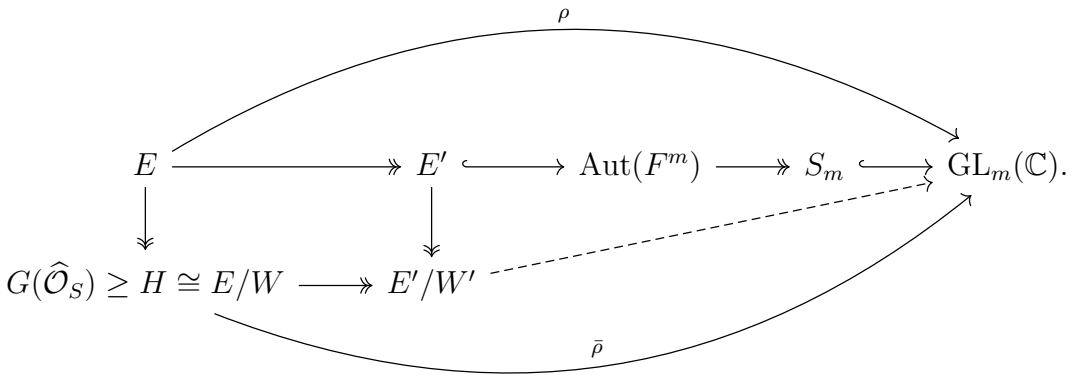
with $C_{E'}(W) = 1$. In particular the action of conjugation of E' on F^m is faithful and so E' can be identified as a subgroup of $\mathrm{Aut}(F^m)$. This yields a homomorphism $E' \hookrightarrow \mathrm{Aut}(F^m) \cong (\mathrm{Aut}(F))^m \rtimes S_m \twoheadrightarrow S_m$. (See Lemma A.4). This homomorphism keeps track of how conjugation by an element $e \in E'$ permutes the factors of F^m. Finally $S_m \hookrightarrow \mathrm{GL}_m(\mathbb{C})$, so we have constructed a representation of E' via the composition

$$E' \hookrightarrow \mathrm{Aut}(F^m) \twoheadrightarrow S_m \hookrightarrow \mathrm{GL}_m(\mathbb{C}).$$

Let $K \leq E'$ be the kernel of this representation. Since K by definition does not permute the factors of F^m we can view it as a subgroup of $(\mathrm{Aut}(F))^m$. In particular note that $F^m \leq K \leq (\mathrm{Aut}(F))^m$ (See Lemma A.5).

It is not obvious at this point, but the group K, wedged between F^m and $(\mathrm{Aut}(F))^m$ is the key subgroup of which we will construct many representations. However, to make this group relevant we need an upper bound on $[E' : K]$. To do this we leverage results from Section 3.7 regarding the image growth of representations of $G(\widehat{\mathcal{O}_S})$. It is surprising that this relies on work done in Chapter 3, which runs exactly converse to this chapter.

To apply the results of Chapter 4 we will need to have a representation of $G(\widehat{\mathcal{O}_S})$. We construct it in the following way. Consider the representation ρ of E given by:



Since $W' = F^m \leq K$ in E' we have that $W \leq \ker(\rho)$ in E. Therefore ρ descends to a representation $\bar{\rho}$ of the quotient $E/W \cong H$ (See diagram above). Now $H \leq G(\widehat{\mathcal{O}_S})$ so we can induce $\bar{\rho}$ to get a representation of $G(\widehat{\mathcal{O}_S})$.

Let $a = [G(\widehat{\mathcal{O}_S}) : H]$, we have

$$\begin{aligned}
[E' : K] &= [E : \ker(\rho)] \\
&= [H : \ker(\bar{\rho})] \\
&\leq \frac{[G(\widehat{\mathcal{O}_S}) : \ker(\mathrm{Ind}_H^{G(\widehat{\mathcal{O}_S})}(\bar{\rho}))]}{[G(\widehat{\mathcal{O}_S}) : H]} && \text{Lemma 1.31} \\
&\leq |\mathrm{Ind}_H^{G(\widehat{\mathcal{O}_S})}(\bar{\rho})(G(\widehat{\mathcal{O}}_S))| \\
&\leq e^{(am)^{\gamma'}} && \text{Proposition 3.49} \\
&\leq e^{m^{\gamma}} && m >> 0 \text{ Lemma A.6.} \qquad (4.1)
\end{aligned}$$

Keep in mind that $\dim(\mathrm{Ind}_H^{G(\widehat{\mathcal{O}_S})}(\bar{\rho})) = am$. This bound on the index is strong enough to tie the representations of K (for various m) to the representation growth of E. We will see this later on, but for now we proceed with constructing representations of K.

Regard F as a normal subgroup of $\mathrm{Aut}(F)$ (Lemma A.5). Fix an irrep (σ, V) of $\mathrm{Aut}(F)$ such that $\sigma|_F$ is nontrivial (for example by inducing a nontrivial irrep of F and taking an irreducible component).

We can write $\sigma|_F$ as a sum of irreducibles $\tau_1 \oplus \cdots \oplus \tau_s$ for some s. No τ_i is trivial, because $\{v \in V : \sigma(x)v = v, \forall\, x \in F\}$ would form a nontrivial $\mathrm{Aut}(F)$-invariant subspace of (σ, V). Normality of $F \trianglelefteq \mathrm{Aut}(F)$ is critical here.

Let $c = \dim \sigma$. Note that $c > 1$ because F is non-abelian and simple (hence perfect), therefore admits only the trivial one-dimensional representation. Now we will use σ to construct many irreducible representations of K.

For all $S \subset \{1, ..., m\}$ define an irreducible representation of $(\mathrm{Aut}(F))^m$ by taking σ in the i-th component when $i \in S$ and the trivial representation otherwise. Now take σ_S to be an irreducible component of the restriction to K. The dimension of σ_S is at most $c^{|S|} = (\dim \sigma)^{|S|}$.

We now show that if $S_1 \neq S_2$ then $\sigma_{S_1} \neq \sigma_{S_2}$. In other words we have a unique irrep of K for each subset of $\{1, ..., m\}$. We see this by considering the restrictions to F^m. The irreducible components of $\sigma_S|_{F^m}$ are of the form $\phi_1 \otimes \cdots \otimes \phi_m$ with $\phi_i \in \{\tau_1, ..., \tau_s\}$ if $i \in S$ and trivial otherwise. Therefore, since the restrictions to F^m are different we must have $\sigma_{S_1} \neq \sigma_{S_2}$.

We have now constructed more than enough representations to prove what we want, we just need to be precise in how we conclude. Let $f : \mathbb{N} \to \mathbb{N}$ be a function such that

$$\lim_{m\to\infty} \frac{f(m)}{m^{\gamma}} = \infty \qquad \text{and} \qquad \lim_{m\to\infty} \frac{f(m)}{m^{\gamma_3}} = 0.$$

Practically speaking the way in which we will use this is to say that for m sufficiently large that

$$m^{\gamma} < f(m) < m^{\gamma_3}.$$

An example of such a function f would be $f(m) = \lfloor m^{\beta} \rfloor$ for $\beta \in (\gamma, \gamma_3)$.

For the rest of the proof we will assume that m is sufficiently large, and denote our use of this fact by $m >> 0$. Let us start by bounding below the number of representations of the form σ_S when $|S| = f(m)$.

$$\begin{aligned}
\binom{m}{f(m)} &= \frac{m!}{(m-f(m))!f(m)!} \\
&\geq \frac{(m-f(m))^{f(m)}}{f(m)^{f(m)}} \\
&\geq \left(\frac{m-m^{\gamma}}{f(m)}\right)^{f(m)} && m >> 0 \\
&= \left((1-m^{\gamma-1}) \cdot \frac{m}{f(m)}\right)^{f(m)} \\
&\geq \left(c^{-1} \cdot \frac{m}{f(m)}\right)^{f(m)} && m >> 0 \\
&= c^{f(m)(\log_c(m)-\log_c(f(m))-1)} \\
&\geq c^{f(m)(\log_c(m)-\log_c(m^{\gamma_3})-1)} && m >> 0 \\
&= c^{f(m)((1-\gamma_3)\log_c(m)-1)} \\
&\geq c^{\gamma_2 f(m)\log_c(m)} && m >> 0 \\
&= m^{\gamma_2 f(m)}.
\end{aligned}$$

Thus we have constructed at least $m^{\gamma_2 f(m)}$ nonisomorphic representations of K of the form σ_S with $|S| = f(m)$. In particular we have that

$$R_{c^{f(m)}}(K) \geq m^{\gamma_2 f(m)}, \tag{4.2}$$

for all m sufficiently large. In reality we have only used a fraction of the representations we constructed. Indeed we could construct more irreducible representations by considering σ_S when $|S| \leq f(m)$, but the improvement is not necessary for the proof and would make the lower bound slightly harder to compute.

Keep in mind that at this point it does not make any sense to say something like "K does not have PRG" because our finite group K is dependent on our choice of m.

Now we are ready to put together the pieces we have created to conclude the proof. Let $n = [E' : K]c^{f(m)}$. We have

$$\begin{aligned} R_n(E) &\geq R_n(E') && \text{Lemma 2.3} \\ &\geq \frac{1}{[E' : K]} R_{c^{f(m)}}(K) && \text{Lemma 2.5} \\ &\geq e^{-m^\gamma} m^{\gamma_2 f(m)} && \text{Equation 4.1 and 4.2} \\ &\geq m^{\gamma_1 f(m)}. && \text{Lemma A.7} \end{aligned}$$

Taking logarithms of the above we get that

$$\log_c(R_n(E)) \geq \gamma_1 f(m) \log_c(m) \geq \gamma_1 f(m) \log_c f(m). \tag{4.3}$$

We need to bound $f(m)$ and $\log_c f(m)$ below to get the result we are looking for. Define $\kappa > \frac{1}{\ln c} + 1$. Combining Equation 4.1 and Lemma A.8 we have that $n \leq e^{m^\gamma} c^{f(m)} \leq c^{\kappa f(m)}$. Taking logarithms of this inequality we get

$$\log_c(n) \leq \kappa f(m). \tag{4.4}$$

Taking logarithms once more we have

$$\log_c \log_c n \leq \log_c(\kappa) + \log_c(f(m)) \leq \kappa \log_c f(m). \tag{4.5}$$

The last inequality is true for m sufficiently large because $\kappa > 1$ and $\log_c \kappa$ is a constant. Equations 4.4 and 4.5 bound $f(m)$ and $\log_c f(m)$ respectively. Combining both of these with Equation 4.3 gives us

$$\log_c(R_n(E)) \geq \frac{\gamma_1}{\kappa^2} \log_c n \log_c \log_c n. \tag{4.6}$$

Therefore by setting $\varepsilon = \frac{\gamma_1}{\kappa^2}$ we have proven what we set out to show. □

The above takes care of case (a) in Rapinchuk's lemma. Everything in the proof works if $\operatorname{char} k \neq 0$. We now deal with case (b1). The proof we give also works if $\operatorname{char} k \neq 0$. The proof idea is similar to the previous proposition, but instead of constructing representations by hand we count monomial representations.

Proposition 4.5 (Case b1)**.** *Let E be a profinite group admitting a SES of the form*

$$1 \to W \to E \xrightarrow{\pi} H \to 1,$$

where H is an open pro-p subgroup of $G(\mathcal{O}_v)$ for some $v \in V_f \backslash S$ and $W = \prod_{i=1}^{\infty} F$, where $F = C_l$ for $l \neq p_v = p$ is finite and simple. That is to say let E be as in case (b1) of Rapinchuk's Lemma. Then there exists $\gamma > 0$ such that $R_n(E) > e^{n^\gamma}$ for infinitely many n. In particular E does not have PRG.

Proof. Let $m \in \mathbb{N}$. Choose an open subgroup $U \leq E$ such that $W/(W \cap U) \cong C_l^m$. Define $W' := W/(W \cap U) \cong C_l^m$, $E' := E/U$ and $H' := H/\pi(U)$. We have an exact sequence of finite groups

$$1 \to W' \to E' \to H' \to 1.$$

H' is a p-group and l is coprime to p, so by the Schur-Zassenhaus Theorem [Zas13, Chapter IV, Section 7, Theorem 25] the exact sequence splits.

It therefore makes sense to consider the centraliser $C_{H'}(W')$, that is, elements of H' that fix W' pointwise under conjugation. Now certainly since W' and H' have trivial intersection we may enlarge U to be the preimage of $C_{H'}(W')$ in E without changing m. Therefore we may assume that H' acts faithfully on W' by conjugation.

Note that $\ker(E \twoheadrightarrow E' \twoheadrightarrow H') = UW$ has index $|H'|$ with an abelian quotient

$$UW/(U \cap W)U \cong W/(U \cap W) \cong C_l^m,$$

of size l^m. Therefore we conclude for all m that

$$A_{|H'|}(E) \geq l^m. \tag{4.7}$$

We now wish to bound $|H'|$, since $A_n(E)$ is related to $R_n(E)$. Note that $W' \cong C_l^m \cong \mathbb{F}_l^m$, so the action of H' on W' by conjugation gives us an injective homomorphism $\rho' : H' \hookrightarrow \mathrm{Aut}(C_l^m) \cong \mathrm{GL}_m(\mathbb{F}_l)$ (additivity implies linearity because the $\mathbb{F}_p$-scalar multiplication is just repeated addition). Now define ρ to be the composition

$$H \twoheadrightarrow H' \hookrightarrow \mathrm{GL}_m(\mathbb{F}_l).$$

Similarly to the proof of Proposition 4.3 we induce ρ to get a representation of

$G(\mathcal{O}_v)$, to which we apply a result from Section 3.7. Let $a = [G(\mathcal{O}_v) : H]$.

$$\begin{aligned}
|H'| &= |\rho'(H')| && \rho' \text{ is injective} \\
&= |\rho(H)| \\
&\leq |\mathrm{Ind}_H^{G(\mathcal{O}_v)}(\rho)(G(\mathcal{O}_v))| \\
&\leq c'(am)^{c'} && \text{Proposition 3.50} \\
&\leq cm^c && \text{let } c := c'a^{c'}.
\end{aligned}$$

Applying this bound on $|H'|$ to Equation 4.7 and letting $n = cm^c$ we see for infinitely many n that

$$\begin{aligned}
R_n(E) &\geq \frac{A_n(E)}{n} && \text{Lemma 2.17} \\
&\geq \frac{l^m}{cm^c} \\
&> e^{(cm^c)^\gamma} && m >> 0, \text{ Lemma A.9} \\
&= e^{n^\gamma},
\end{aligned}$$

provided $\gamma \in (0, 1/c)$. Therefore E does not have PRG, as required. □

For this case the monomial representations of E were sufficient to disprove polynomial representation growth. The same will be true in the following case, but the proof will only work in characteristic 0. We use a similar strategy as the previous proposition, this time utilising results from the theory of p-adic analytic groups. Use of this theory is specific to characteristic 0.

Proposition 4.6 (Case b2)**.** *Let E be a profinite group admitting a SES of the form*

$$1 \to W \to E \xrightarrow{\pi} H \to 1,$$

where H is an open pro-p subgroup of $G(\mathcal{O}_v)$ for some $v \in V_f \backslash S$ and $W = \prod_{i=1}^{\infty} F$, where $F = C_l$ for $p_v = p = l$ is finite and simple. That is to say let E be as in case (b2) of Rapinchuk's lemma. Then there exists $\gamma > 0$ such that $R_n(E) > e^{n^\gamma}$ for infinitely many n. In particular E does not have PRG.

Proof. E is a topological extension of pro-p groups and thus pro-p. Consider the closed subgroup E^{p^m} generated by the p^m powers in E. We have an exact sequence

$$1 \to W' \to E' \to H' \to 1,$$

where $E' := E/E^{p^m}$, $W' := W/(W \cap E^{p^m})$ and $H' = H/\pi(E^{p^m}) = H/H^{p^m}$.

E is not p-adic analytic because the closed subgroup $W = \prod_{i=1}^{\infty} C_p$ is not topologically finitely generated. However E is topologically finitely generated by Lemma 4.7, so by [DDSMS03, Corollary 11.6] we have $[E : E^{p^m}] \geq p^{p^m}$ for all m.

On the other hand H is p-adic analytic (see Lemma 4.8) and so by [DDSMS03, Theorem 3.16] we have $[H : H^{p^m}] \leq (p^m)^d$ for some fixed d.

Therefore we have $|E'| \geq p^{p^m}$ and $|H'| \leq (p^m)^d$. So

$$|W'| = \frac{|E'|}{|H'|} \geq p^{p^m - dm}.$$

Consider $\ker(E \to H \to H') = E^{p^m}W$. Analogously to the proof of case (b1) this is an index $|H'|$ subgroup of E with an abelian quotient of size $|W'|$. Therefore

$$A_{p^{dm}}(E) \geq p^{p^m - dm},$$

so if we let $n = p^{dm}$, we have for infinitely many n that

$$\begin{aligned} R_n(E) &\geq \frac{A_n(E)}{n} && \text{Lemma 2.17} \\ &= \frac{A_{p^{dm}}(E)}{n} \\ &\geq \frac{p^{p^m - dm}}{n} \\ &= \frac{p^{n^{\frac{1}{d}}}}{n^2} \\ &> e^{n^\gamma} && n >> 0, \text{ Lemma A.10,} \end{aligned}$$

provided $\gamma \in (0, 1/d)$. Therefore E does not have polynomial representation growth, as required. □

Now we take a moment to tie up the finite generation of E, and the fact that H is p-adic analytic.

Lemma 4.7. *The group E, as in the proof of case (b2) is topologically finitely generated.*

Proof. $\Gamma = G(\mathcal{O}_S)$ is finitely generated due to [Abe06, Theorem 0.2.5]. Any finite index subgroup $\Gamma_0 \leq \Gamma$ is finitely generated by Lemma A.11.

Since Γ_0 is dense in its profinite completion, $\widehat{\Gamma}_0$ is topologically finitely generated. $\widehat{\Gamma}_0$ surjects onto E, so E must also be topologically finitely generated. □

Lemma 4.8. *The group H, as in the proof of case (b2) is p-adic analytic.*

Proof. We will prove that H is a closed subgroup of $\mathrm{GL}_{N'}(\mathbb{Z}_p)$ for some N'. Certainly $H \leq G(\mathcal{O}_v)$ is a closed subgroup.

Now $G(\mathcal{O}_v) \leq \mathrm{GL}_N(\mathcal{O}_v)$ is a Zariski closed subset cut out by the defining equations of G. However $\mathcal{O}_v \cong (\mathbb{Z}_p)^t$ as $\mathbb{Z}_p$-modules (since $\operatorname{char} k = 0$), therefore $\mathrm{GL}_N(\mathcal{O}_v) \cong \mathrm{GL}_{tN}(\mathbb{Z}_p)$. Since the defining equations of G had coefficients in $\mathcal{O}$, under this isomorphism $G(\mathcal{O}_v)$ becomes a Zariski closed subset of $\mathrm{GL}_{tN}(\mathbb{Z}_p)$ with defining equations that have coefficients in $\mathbb{Z}$. It remains to show that this realises $G(\mathcal{O}_v)$ as a closed subgroup in the profinite topology. Suppose that $g_1, ..., g_m \in \mathbb{Z}[x_1, ..., x_{(tN)^2}]$ are a set of defining equations for $G(\mathcal{O}_v) \leq \mathrm{GL}_{tN}(\mathbb{Z}_p)$. Since $\mathrm{GL}_{tN}(\mathbb{Z}_p)$ inherits its topology from $\mathrm{M}_{tN}(\mathbb{Z}_p) \cong (\mathbb{Z}_p)^{(tN)^2}$, it suffices to prove that $G(\mathcal{O}_v)$ is closed in $(\mathbb{Z}_p)^{tN}$.

$$\begin{aligned} G(\mathcal{O}_v) &= \{(x_1, ..., x_{(tN)^2}) \in \mathrm{GL}_{tN}(\mathbb{Z}_p) : g_i(x_1, ..., x_{(tN)^2}) = 0,\ 1 \leq i \leq m\} \\ &= \mathrm{GL}_{tN}(\mathbb{Z}_p) \cap \bigcap_{i=1}^{m} \{(x_1, ..., x_{(tN)^2}) \in (\mathbb{Z}_p)^{tN} : g_i(x_1, ..., x_{(tN)^2}) = 0\} \\ &= \mathrm{GL}_{tN}(\mathbb{Z}_p) \cap \bigcap_{i=1}^{m} \bigcap_{j=1}^{\infty} \{(x_1, ..., x_{(tN)^2}) \in (\mathbb{Z}_p)^{tN} : g_i(x_1, ..., x_{(tN)^2}) \equiv 0 \mod p^j\}. \end{aligned}$$

$\mathrm{GL}_{tN}(\mathbb{Z}_p)$ is a closed subset of $\mathrm{M}_{tN}(\mathbb{Z}_p)$ by [DDSMS03, Section 5.1]. The rest is an intersection of closed sets since the fact that the g_i are polynomials means that the condition $g_i(x_1, ..., x_{(tN)^2}) \equiv 0 \mod p^j$ only depends on $x_1, ..., x_{(tN)^2}$ up to their congruence modulo p^j.

Therefore H is a closed subgroup of $\mathrm{GL}_{tN}(\mathbb{Z}_p)$, hence is p-adic analytic. □

We have now proven Theorem 4.1, which completes the characterisation of groups with the CSP as exactly those with PRG when $\operatorname{char} k = 0$ (modulo the mild additional hypotheses). The PhD thesis of García-Rodríguez [GR16] shows that Assumption 3.2 can be dropped from Theorem 3.1. If the Margulis-Platonov Conjecture A can be completely established then we will have a full characterisation without caveats in the case of $\operatorname{char} k = 0$.

Generalising Rapinchuk's Lemma appears to be the greatest impediment to adapting the approach of this chapter to the case of $\operatorname{char} k > 0$. Supposing this is possible the proofs given for case (a) and (b1) work, but case (b2) will require a different proof. Perhaps the theory of $\mathbb{F}_p[[t]]$-standard groups can serve as a stand-in for the theory of p-adic analytic groups.

Appendix A

Unenlightening lemmas

Here we compile the proofs of lemmas used in Chapters 3 and 4. The author recommends the reader to use this appendix as a reference, only to be read when a step in the main text is unclear, or if the reader's curiosity is up to the task.

The lemmas are each straightforward to prove, but are numerous and uninteresting enough that their presence in the main text would have been distracting. The proofs themselves are generally unenlightening, but we include them here for completeness.

We start with a fact about profinite completions and subgroups, used in Section 3.2.

Lemma A.1. *Let $H \leq G$ be a finite index subgroup. Then the closure of the image of H in $\widehat{G}$ is isomorphic to $\widehat{H}$.*

Proof. Recall that $H \leq G$ is a finite index subgroup. By properties of the profinite completion we have the commuting square

$$\begin{array}{ccc} H & \hookrightarrow & G \\ \downarrow & & \downarrow \\ \widehat{H} & \xrightarrow{\phi} & \widehat{G}. \end{array}$$

The bottom arrow of the diagram gives a map $\widehat{H} \to \overline{H}$. The image of H in $\widehat{H}$ is dense, so by properties of continuous maps we have

$$\phi(\widehat{H}) = \phi(\overline{H}) \subset \overline{\phi(H)} = \overline{H}.$$

Here we see Notation 3.6 at its most ambiguous. The first overline denotes a closure in $\widehat{H}$, the second overline a closure in $\widehat{G}$, and the last equality is true

because we are taking $\overline{H}$ to mean the closure of the image of H in $\widehat{G}$. In other words we use commutativity of the square.

Now $H \subset \phi(\widehat{H}) \subset \overline{H}$, but since $\widehat{H}$ is compact, ϕ is continuous and $\widehat{G}$ is Hausdorff $\phi(\widehat{H})$ is closed. Therefore $\phi(\widehat{H}) = \overline{H}$, so ϕ is surjective.

To check ϕ is injective take $(h_I I)_{I \triangleleft H} \in \ker(\phi)$. $h_I I$ is the identity if $I = N \cap H$, with $N \triangleleft G$ finite index. Now if $I \triangleleft H$ is finite index the fact that $[G : H] < \infty$ means that $\cap_{g \in G} g I g^{-1} \cap H \subset I$ is finite index, normal and of the form mentioned previously. Therefore $h_I I$ is the identity for all finite index normal subgroups I. Therefore ϕ has trivial kernel and is injective. □

Here we include a proof of Lemma 3.32.

Lemma A.2. *Let p be a prime and let $q = p^e$, where $e \in \mathbb{N}$. Let V, W, X be finite-dimensional vector spaces over $\mathbb{F}_q$, and let $T : V \times W \to X$ be an $\mathbb{F}_q$-bilinear map such that $T(V \times W)$ spans X over $\mathbb{F}_q$. Suppose that A, B are $\mathbb{F}_p$-subspaces of V, W such that*

$$[V : A][W : B] < q,$$

then $T(A \times B)$ spans X over $\mathbb{F}_p$.

Proof. We begin with the case of $V = W = X = \mathbb{F}_q$, and T given by multiplication in $\mathbb{F}_q$. The strategy is to show that any nonzero $\mathbb{F}_p$-linear functional $f : \mathbb{F}_q \to \mathbb{F}_p$ does not vanish on $T(A \times B)$. Given f, we can define an $\mathbb{F}_p$-bilinear form

$$Q_f : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q,\ Q_f(x, y) := f(xy).$$

We claim that Q_f is nondegenerate. Indeed there exists some $z \in \mathbb{F}_q$ such that $f(z) \neq 0$ and so for any $0 \neq x \in \mathbb{F}_q$ we have $Q_f(x, x^{-1}z) = f(xx^{-1}z) = f(z) \neq 0$. Therefore $Q(x, \cdot) \neq 0$. This then implies that the $\mathbb{F}_p$-dimension of $A^\perp$ is equal to the $\mathbb{F}_p$-codimension of A. Next we use the index condition on A and B to make conclusions about their dimensions.

$$\begin{aligned} [V : A][W : B] &< q \\ p^{e - \dim A} p^{e - \dim B} &< p^e \\ (e - \dim A) + (e - \dim B) &< e \qquad \text{Taking } \log_p \\ \dim A + \dim B &> e. \end{aligned}$$

This condition tells us that $B \not\subset A^\perp$, which tells us that $Q_f(a, b) \neq 0$ for some $a \in A$ and $b \in B$. Of course this says that $f(T(a, b)) = f(ab) \neq 0$, so f does not

vanish on $T(A \times B)$. Since f was an arbitrary $\mathbb{F}_p$-linear functional this tells us that $T(A \times B)$ spans $\mathbb{F}_q = X$ over $\mathbb{F}_p$.

Now take the general case. Let Y be the $\mathbb{F}_p$-span of $T(A \times B)$. Our index condition on A and B implies that A and B contain $\mathbb{F}_q$-bases for V and W respectively. Therefore Y spans X over $\mathbb{F}_q$. To show that Y spans X over $\mathbb{F}_p$ consider a transversal for $\mathbb{F}_q$ over $\mathbb{F}_p$; it is sufficient to prove that Y is invariant under multiplication by $\mathbb{F}_q$.

Let $a \in A$, $b \in B$ and $w \in \mathbb{F}_q$. We want to show that $wT(a,b) \in Y$. Define the following $\mathbb{F}_p$-subspaces of $\mathbb{F}_q$:

$$A' = \{x \in \mathbb{F}_q : xa \in A\},$$
$$B' = \{x \in \mathbb{F}_q : xb \in B\}.$$

The plan is to apply the special case to these subspaces. Note that

$$\mathbb{F}_q/A' \cong \mathbb{F}_q a/(\mathbb{F}_q a \cap A) \cong (A + \mathbb{F}_q a)/A \subset V/A.$$

The first isomorphism is given by mapping $x \mapsto xa$, the rest are easy to see. Similarly $\mathbb{F}_q/B' \subset W/B$. This tells us that $[\mathbb{F}_q : A'][\mathbb{F}_q : B'] \leq [V : A][W : B] < q$, so applying the special case tells us that $A'B'$ spans $\mathbb{F}_q$ over $\mathbb{F}_p$. Importantly for any $w \in \mathbb{F}_q$ we have $w = \sum_i x_i y_i$ where $x_i \in A'$ and $y_i \in B'$. Then by the the $\mathbb{F}_q$-bilinearity of T we have that

$$wT(a,b) = \left(\sum_i x_i y_i\right) T(a,b) = \sum_i T(x_i a, y_i b) \in Y,$$

so we have proven that Y is invariant under multiplication by $\mathbb{F}_q$. □

Now we deliver the promised induction argument for Lemma 3.47.

Lemma A.3. *Let $d, a \in \mathbb{N}$. Then $\frac{1}{a+1} d^{a+1} \leq \sum_{i=1}^{d} i^a \leq d^{a+1}$.*

Proof. The second inequality is obvious. The first inequality we will prove by induction on d. If $d = 1$ then the inequality is clearly true. Now suppose it holds for d, then

$$\begin{aligned}
\frac{1}{a+1}(d+1)^{a+1} &= \frac{1}{a+1} d^{a+1} + \sum_{i=0}^{a} \frac{1}{a+1} \binom{a+1}{i} d^i \\
&\leq \sum_{i=0}^{d} i^a + \sum_{i=0}^{a} \binom{a}{i} d^i \\
&= \sum_{i=0}^{d} i^a + (d+1)^a = \sum_{i=0}^{d+1} i^a.
\end{aligned}$$

□

We now begin with lemmas regarding the structure of $\mathrm{Aut}(F)$ and $\mathrm{Aut}(F^m)$, where F is a finite simple non-abelian group.

Lemma A.4. $\mathrm{Aut}(F^m) \cong S_m \ltimes (\mathrm{Aut}(F))^m$ *if* F *is a finite simple non-abelian group.*

Proof. The key insight is that since F is simple and non-abelian, all simple normal subgroups of F^m are $\{1\}^{i-1} \times F \times \{1\}^{m-i}$ for some i.

Suppose that $N \trianglelefteq F^m$ is simple. Let $1 \neq (x_1, ..., x_m) \in N$, therefore there exists an i with $x_i \neq 1$. Since F is non-abelian there exists a y that does not commute with x_i. Due to the normality of N we have $(x_1, ..., yx_iy^{-1}, ..., x_n) \in N$. Multiplying our original element by the inverse of this one we see that $(1, ..., 1, x_iyx_i^{-1}y^{-1}, 1, ..., 1) \in N$, hence $\{1\}^{i-1} \times F \times \{1\}^{m-i} = N$ due to the simplicity of both groups.

Let $\phi \in \mathrm{Aut}(F^m)$. Since simplicity and normality of subgroups are preserved under isomorphism we have the following commutative diagram

$$\begin{array}{ccc} F \times \cdots \times F & \xrightarrow{\quad\phi\quad} & F^m \\ \uparrow & & \uparrow \\ \{1\}^{i-1} \times F \times \{1\}^{m-i} & \xrightarrow{\sim} & \{1\}^{j-1} \times F \times \{1\}^{m-j}. \end{array}$$

Therefore define $\tau : \mathrm{Aut}(F^m) \to S_m$ by $\tau(\phi)(i) := j$. Concretely $\tau(\phi)$ keeps track of the way in which ϕ permutes the factors of F^m. This is certainly a group homomorphism, the kernel of which are the automorphisms that fix each of the factors of F^m. Therefore we have the short exact sequence

$$1 \to \mathrm{Aut}(F)^m \to \mathrm{Aut}(F^m) \xrightarrow{\tau} S_m \to 1.$$

All that is left is to show that this exact sequence splits. We can describe a section $s : S_m \to \mathrm{Aut}(F^m)$ in the following way. For $\sigma \in S_m$ define $s(\sigma) : F^m \to F^m$ by

$$s(\sigma)(x_1, ..., x_m) := (x_{\sigma(1)}, ..., x_{\sigma(m)}).$$

Therefore $\mathrm{Aut}(F^m) \cong S_m \ltimes (\mathrm{Aut}(F))^m$, as required. □

Lemma A.5. *If* F *is finite, simple and non-abelian then* $F \trianglelefteq \mathrm{Aut}(F)$ *via the map*

$$\varphi : F \to \mathrm{Aut}(F),\ x \mapsto \varphi_x(y) = xyx^{-1}.$$

Proof. Since F is simple $\ker(\varphi) = F$ or $\{1\}$.

If $\ker(\varphi) = F$ then for every $x \in F$ we have $\varphi_x = \mathrm{id}_F$. Therefore for every $y \in F$ we have $\varphi_x(y) = y$. Unwinding the definitions this tells us that for all $x, y \in F$, $xy = yx$. This is a contradiction because F is non-abelian. We conclude that φ is in fact injective.

To prove normality let $\psi \in \mathrm{Aut}(F)$ and let $x, y \in F$, then

$$\begin{aligned}\psi(\varphi_x(\psi^{-1}(y))) &= \psi(x\psi^{-1}(y)x^{-1}) \\ &= \psi(x)y\psi(x^{-1}) \\ &= \varphi_{\psi(x)}(y).\end{aligned}$$

Therefore $\psi\varphi_x\psi^{-1} = \varphi_{\psi(x)}$, which proves that $F \trianglelefteq \mathrm{Aut}(F)$ via φ. i.e F embeds as a normal subgroup of its automorphisms via the action on itself by conjugation. □

We now prove the lemmas regarding limit inequalities. All of these use essentially same technique of proving that the natural log of the ratio of the two terms goes to infinity.

Lemma A.6. *With γ', γ and a chosen as in Proposition 4.3 we have for m sufficiently large that*

$$e^{(am)^{\gamma'}} \leq e^{m^{\gamma}}.$$

Proof. Recall that $0 < \gamma' < \gamma$ and $a \geq 1$.

It suffices to prove that

$$\lim_{m\to\infty} e^{-(am)^{\gamma'}} e^{m^{\gamma}} = \infty.$$

To do this we will prove that the natural log of the limit goes to infinity.

$$\begin{aligned}\lim_{m\to\infty} \ln(e^{-(am)^{\gamma'}} e^{m^{\gamma}}) &= \lim_{m\to\infty} -(am)^{\gamma'} + m^{\gamma} \\ &= \infty,\end{aligned}$$

since $0 < \gamma' < \gamma$, so the m^{γ} term dominates. □

Lemma A.7. *With $\gamma, \gamma_1, \gamma_2$ and $f(m)$ chosen as in Proposition 4.3 we have for m sufficiently large that*

$$e^{-m^{\gamma}} m^{\gamma_2 f(m)} \geq m^{\gamma_1 f(m)}.$$

Proof. Recall that γ, γ_1 and γ_2 were chosen such that $\gamma > 0$, $0 < \gamma_1 < \gamma_2$ and $m^\gamma < f(m) < m^{\gamma_3}$ for m sufficiently large.

It suffices to prove that

$$\lim_{m\to\infty} e^{-m^\gamma} m^{\gamma_2 f(m)} m^{-\gamma_1 f(m)} = \infty.$$

To do this we will prove that the natural log of the limit goes to infinity.

$$\begin{aligned}\lim_{m\to\infty} \ln\left(e^{-m^\gamma} m^{\gamma_2 f(m)} m^{-\gamma_1 f(m)}\right) &= \lim_{m\to\infty} -m^\gamma + (\gamma_2 - \gamma_1) f(m) \ln(m) \\ &\geq \lim_{m\to\infty} m^\gamma(-1 + (\gamma_2 - \gamma_1)\ln(m)) \\ &= \infty,\end{aligned}$$

since m^γ goes to infinity and $-1 + (\gamma_2 - \gamma_1)\ln(m)$ is eventually positive (for $m > e^{\frac{1}{\gamma_2 - \gamma_1}}$). □

Lemma A.8. *For $c, \gamma, f(m)$ chosen as in Proposition 4.3 and $\kappa > \frac{1}{\ln c} + 1$, we have for m sufficiently large that*

$$e^{m^\gamma} c^{f(m)} \leq c^{\kappa f(m)}.$$

Proof. Recall that $\gamma > 0$ and f were chosen such that $\lim_{m\to\infty} \frac{f(m)}{m^\gamma} = \infty$ and that $c > 1$. We wish to prove that

$$\lim_{m\to\infty} c^{\kappa f(m)} e^{-m^\gamma} c^{-f(m)} = \infty.$$

To do this it suffices to prove that the natural log of the limit goes to infinity, and indeed

$$\begin{aligned}\lim_{m\to\infty} \ln(c^{\kappa f(m)} e^{-m^\gamma} c^{-f(m)}) &= \lim_{m\to\infty} (\kappa - 1) f(m) \ln(c) - m^\gamma \\ &\geq \lim_{m\to\infty} f(m) - m^\gamma \qquad \text{Since } \kappa > \frac{1}{\ln c} + 1 \\ &= \lim_{m\to\infty} \left(\frac{f(m)}{m^\gamma} - 1\right) m^\gamma \\ &= \infty,\end{aligned}$$

since f was chosen such that $\lim_{m\to\infty} \frac{f(m)}{m^\gamma} = \infty$. □

Lemma A.9. *With constants chosen as in Proposition 4.5 and $\gamma \in (0, 1/c)$ then for m sufficiently large*

$$\frac{l^m}{cm^c} > e^{(cm^c)^\gamma}.$$

Proof. Recall that l is a prime number and so $l > 1$. It suffices to prove that

$$\lim_{m\to\infty} \frac{l^m}{cm^c e^{(cm^c)^\gamma}} = \infty.$$

To do this we will prove that the natural log of the limit goes to infinity.

$$\lim_{m\to\infty} \ln\left(\frac{l^m}{cm^c e^{(cm^c)^\gamma}}\right) = \lim_{m\to\infty} m\ln(l) - \ln(c) - c\ln(m) - (cm^c)^\gamma.$$

Provided $\gamma \in (0, 1/c)$ we have $c\gamma < 1$, and so the fastest growing term is $m\ln(l)$. Therefore the limit goes to infinity. □

Lemma A.10. *With constants chosen as in Proposition 4.6 and $\gamma \in (0, 1/d)$ then for n sufficiently large*

$$\frac{p^{n^{\frac{1}{d}}}}{n^2} > e^{n^\gamma}.$$

Proof. It suffices to prove that

$$\lim_{n\to\infty} \frac{p^{n^{\frac{1}{d}}}}{e^{n^\gamma} n^2} = \infty.$$

To do this it suffices to prove that the natural log of the limit goes to infinity.

$$\lim_{n\to\infty} \ln\left(\frac{p^{n^{\frac{1}{d}}}}{e^{n^\gamma} n^2}\right) = \lim_{n\to\infty} n^{\frac{1}{d}} \ln p - n^\gamma - 2\ln n.$$

Since $\gamma < 1/d$ we have that $n^{\frac{1}{d}}$ is the fastest growing term, and so the limit tends to infinity. □

The following lemma is an elementary fact about finitely generated groups. We have included a proof that uses algebraic topology for fun, but a purely group theoretic proof can be found in [Ros94, page 55].

Lemma A.11. *A finite index subgroup of a finitely generated group is finitely generated.*

Proof. Let $G_0 \leq G$ be a finite index subgroup and suppose that G is finitely generated. Then we can construct a 2-dimensional CW complex X with finite 1-skeleton such that $\pi_1(X) = G$ [Hat05, Corollary 1.28]. There is a finite-sheeted covering space $\widetilde{X}$ such that $\pi_1(\widetilde{X}) = G_0$ [Hat05, Proposition 1.36]. Since $\widetilde{X}$ also has finite 1-skeleton we conclude that G_0 is finitely generated. □

Bibliography

[Abe06] Herbert Abels. *Finite presentability of S-arithmetic groups. Compact presentability of solvable groups*, volume 1261. Springer, 2006.

[AK67] JL Alperin and Tzee-Nan Kuo. The exponent and the projective representations of a finite group. *Illinois Journal of Mathematics*, 11(3):410–413, 1967.

[AM18] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to commutative algebra*. CRC Press, 2018.

[BLS64] Hyman Bass, Michel Lazard, and Jean-Pierre Serre. Sous-groupes dindice fini dans (,). *Bulletin of the American mathematical society*, 70(3):385–392, 1964.

[DDSMS03] John D Dixon, Marcus PF Du Sautoy, Avinoam Mann, and Dan Segal. *Analytic pro-p groups*. Number 61 in Cambridge studies in advanced mathematics. Cambridge University Press, 2003.

[Erd41] P Erdos. On some asymptotic formulas in the theory of the" factorisatio numerorum". *Annals of Mathematics*, pages 989–993, 1941.

[GR16] Javier García-Rodríguez. Representation growth. *arXiv preprint arXiv:1612.06178*, 2016.

[Hat05] Allen Hatcher. *Algebraic topology*. , 2005.

[Hum12] James E Humphreys. *Linear algebraic groups*, volume 21. Springer Science & Business Media, 2012.

[Isa94] I Martin Isaacs. *Character theory of finite groups*, volume 69. Courier Corporation, 1994.

[JZK07] Andrei Jaikin-Zapirain and Benjamin Klopsch. Analytic groups over general pro-p domains. *Journal of the London Mathematical Society*, 76(2):365–383, 2007.

[KL+90] Peter B Kleidman, Martin W Liebeck, et al. *The subgroup structure of the finite classical groups*, volume 129. Cambridge University Press, 1990.

[Klo12] Benjamin Klopsch. Representation growth and representation zeta functions of groups. *arXiv preprint arXiv:1209.2896*, 2012.

[KNV11] Benjamin Klopsch, Nikolay Nikolov, and Christopher Voll. *Lectures on profinite topics in group theory*, volume 77, chapter II Strong approximation methods. Cambridge University Press, 2011.

[Lan02] Serge Lang. Representations of finite groups. In *Algebra*, pages 663–729. Springer, 2002.

[LL11] Michael Larsen and Alexander Lubotzky. Normal subgroup growth of linear groups: the (g2; f4; e8)-theorem. *arXiv preprint arXiv:1108.1044*, 2011.

[LM04] Alexander Lubotzky and Benjamin Martin. Polynomial representation growth and the congruence subgroup problem. *Israel Journal of Mathematics*, 144(2):293–316, 2004.

[Lub95] Alexander Lubotzky. Subgroup growth and congruence subgroups. *Inventiones mathematicae*, 119(1):267–295, 1995.

[Mil06] JS Milne. Algebraic groups and arithmetic groups. *JS Milne*, pages 1–219, 2006.

[MT11] Gunter Malle and Donna Testerman. *Linear algebraic groups and finite groups of Lie type*, volume 133. Cambridge University Press, 2011.

[Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[PR93] Vladimir P Platonov and Andrei S Rapinchuk. Abstract properties of-arithmetic groups and the congruence problem. *Izvestiya: Mathematics*, 40(3):455, 1993.

[PR10] Gopal Prasad and Andrei S Rapinchuk. Developments on the congruence subgroup problem after the work of bass, milnor and serre. *American Mathematical Society, Providence, RI*, 2010.

[Pra77] Gopal Prasad. Strong approximation for semi-simple groups over function fields. *Annals of Mathematics*, 105(3):553–572, 1977.

[PRR93] Vladimir Platonov, Andrei Rapinchuk, and Rachel Rowen. *Algebraic groups and number theory*, volume 139. Academic press, 1993.

[Rag76] Madabusi S Raghunathan. On the congruence subgroup problem. *Publications Mathématiques de l'IHÉS*, 46:107–161, 1976.

[RCW92] J. Ritter, G. Cliff, and A. Weiss. Group representations and integrality. *Journal fur die reine und angewandte Mathematik*, 1992(426):193–202, 1992.

[Rey65] WF Reynolds. Projective representations of finite groups in cyclotomic fields. *Illinois Journal of Mathematics*, 9(2):191–198, 1965.

[Ros94] John S Rose. *A course on group theory*. Courier Corporation, 1994.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2002.

[RV13] Dinakar Ramakrishnan and Robert J Valenza. *Fourier analysis on number fields*, volume 186. Springer Science & Business Media, 2013.

[Sch04] J Schur. Über die darstellung der endlichen gruppen durch gebrochen lineare substitutionen. *Reine Angew. Math.*, 127:20–50, 1904.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*, volume 42. Springer, 1977.

[Ste12] Peter Stevenhagen. Number rings. *Mastermath course, Leiden University*, 2012.

[Wat12] William C Waterhouse. *Introduction to affine group schemes*, volume 66. Springer Science & Business Media, 2012.

[Zas13] Hans J Zassenhaus. *The theory of groups*. Courier Corporation, 2013.