Universidad Autónoma de Madrid

Tesis Doctoral

Representation Growth

Autor:
Javier García Rodríguez

Director:
Andrei Jaikin Zapirain

Octubre 2016

a Laura.

Abstract

The main results in this thesis deal with the representation theory of certain classes of groups. More precisely, if $r_n(\Gamma)$ denotes the number of non-isomorphic n-dimensional complex representations of a group Γ, we study the numbers $r_n(\Gamma)$ and the relation of this arithmetic information with structural properties of Γ.

In chapter 1 we present the required preliminary theory. In chapter 2 we introduce the Congruence Subgroup Problem for an algebraic group G defined over a global field k.

In chapter 3 we consider $\Gamma = G(\mathcal{O}_S)$ an arithmetic subgroup of a semisimple algebraic k-group for some global field k with ring of S-integers $\mathcal{O}_S$. If the Lie algebra of G is perfect, Lubotzky and Martin showed in [56] that if Γ has the weak Congruence Subgroup Property then Γ has Polynomial Representation Growth, that is, $r_n(\Gamma) \le p(n)$ for some polynomial p. By using a different approach, we show that the same holds for any semisimple algebraic group G including those with a non-perfect Lie algebra.

In chapter 4 we apply our results on representation growth of groups of the form $\Gamma = G(\mathcal{O}_S)$ to show that if Γ has the weak Congruence Subgroup Property then $s_n(\Gamma) \le n^{D \log n}$ for some constant D, where $s_n(\Gamma)$ denotes the number of subgroups of Γ of index at most n. As before, this extends similar results of Lubotzky [54], Nikolov, Abert, Szegedy [1] and Golsefidy [24] for almost simple groups with perfect Lie algebra to any simple algebraic k-group G.

In chapter 5 we consider $\Gamma = 1 + J$, where J is a finite nilpotent associative algebra, this is called an algebra group. The Fake Degree Conjecture says that for algebra groups the numbers $r_n(\Gamma)$ may be obtained by looking at the square root of the sizes of the orbits arising from Kirillov's Orbit Method. In [36] Jaikin gave a 2-group that served as a counterexample to this conjecture. We provide counterexamples for any prime p by looking at groups of the form $\Gamma = 1 + I_{\mathbb{F}_q}$, where $I_{\mathbb{F}_q}$ is the augmentation ideal of the group algebra $\mathbb{F}_q[\pi]$ for some p-group π. Moreover, we show that for such groups $r_1(\Gamma) = q^{k(\pi)-1}|\operatorname{B}_0(\pi)|$, where $\operatorname{B}_0(\pi)$ is the Bogomolov multiplier of π.

Finally in chapter 6, we consider $\Gamma = \prod_{i \in I} S_i$, where the S_i are nonabelian finite simple group. We give a characterization of the groups of this form having Polynomial Representation Growth. We also show that within this class one can obtain any rate of representation growth, i.e., for any $\alpha > 0$ there exists $\Gamma = \prod_{i \in I} S_i$ where the S_i are finite simple groups of Lie type such that $r_n(\Gamma) \sim n^\alpha$. Moreover, we may take all S_i with a fixed Lie type. This complements results of Kassabov and Nikolov in [42].

Agradecimientos

enseñarme con paciencia ese lenguaje tan raro que habláis.

Gracias a mis analistas preferidos Jose y Adri por la no numerable cantidad de cosas que he aprendido de vosotros y sobre todo por convencerme de volver a la lucha armada.

Gracias a mi matemática preferida, María Medina. Por empezar todas las mañanas con una gran sonrisa y hacer que un mal café sea el mejor de todos. Por reverdecer acelgas por muy pochas que estén, por todas las historias contadas, escritas y por escribir.

Gracias a mi Jota, por estar desde siempre y para siempre. Por saber que tengo una amiga que no puedo perder por muchas tesis de 1000 páginas que tenga que hacer.

Gracias a mis otros amigos matemáticos, Bruno y Poli, por todos los buenos momentos desde que empezamos a hacer cuentas.

Gracias a Fer, el matemático que más me ha influenciado y acompañado desde que empecé, compañero de recomendaciones, amarguras y eternas discusiones, gracias por confiar siempre en mí, especialmente en los malos momentos.

Gracias a toda mi familia por apoyarme en todas las etapas hasta llegar hasta aquí. En especial gracias a mis padres y a mi hermana por apoyarme siempre en todo lo que he querido hacer y ayudarme en todo lo que han podido. Gracias con cariño a mis abuelos, por estar siempre orgullosos incluso aunque no entendieran lo que hacía.

Y gracias a ti Laura. Por acompañarme y ayudarme en todo desde siempre. Porque sin ti no habría podido, ni esto ni otras muchas cosas. Porque estás 100 páginas también son mérito, esfuerzo y sacrificio tuyo. Por ser la mejor parte de todo desde que tengo memoria.

Contents

Introducción

Sea Γ un grupo. Una representación de Γ es un homomorfismo de grupos $\rho : \Gamma \to \mathrm{GL}(V)$ para algún espacio vectorial complejo finito dimensional V. La Teoría de Representaciones estudia la relación entre propiedades estructurales de Γ y sus representaciones. El Teorema de Burnside fue la primera gran contribución de la Teoría de Representaciones y desde entonces se ha convertido en un área de investigación en sí misma. Este trabajo se centra en la teoría de representaciones de ciertas clases de grupos. El bloque principal está dedicado al estudio de la teoría de representaciones (más concretamente, del crecimiento de representaciones) de grupos aritméticos, aunque también abordamos cuestiones relacionadas con la teoría de representaciones de álgebras de grupo y el crecimiento de representaciones de (productos directos de) grupos finitos simples.

Sea Γ un grupo y denotemos por $r_n(\Gamma)$ el número de clases de isomorfía de representaciones irreducibles n-dimensionales de Γ. Si Γ es finito sabemos que $r_n(\Gamma) = 0$ para $n \geq |\Gamma|^{1/2}$. El estudio de grupos finitos a través de las dimensiones de sus representaciones irreducibles y clases de conjugación es una gran área de investigación, e.g., ver [34] o [32] y referencias allí indicadas. Por otro lado para Γ infinito $r_n(\Gamma)$ puede ser infinito. El comportamiento asintótico de la sucesión $r_n(\Gamma)$ es el crecimiento de representaciones del grupo Γ. Supongamos que $r_n(\Gamma) < \infty$ para todo n. Entonces podemos asociar a la sucesión $\{r_n(\Gamma)\}$ una zeta función de Dirichlet

$$\zeta_\Gamma(s) = \sum_{n=1}^{\infty} r_n(\Gamma) n^{-s} \quad (s \in \mathbb{C}).$$

La abscisa the convergencia $\alpha(\Gamma)$ de $\zeta_\Gamma(s)$ es el ínfimo de todos los $\alpha \in \mathbb{R}_{\geq 0}$ tales que la serie $\zeta_\Gamma(s)$ converge en el semiplano derecho $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \alpha\}$. La abscisa $\alpha(\Gamma)$ es finita si y solo si Γ tiene Crecimiento Polinomial de Representaciones (CPR), es decir, si $r_n(\Gamma) \leq p(n)$ para algún polinomio p.

Crecimiento de Representaciones de Grupos Aritméticos

Sea k un cuerpo global, S un conjunto finito de valuaciones de k que contiene a todas las arquimedianas y $\mathcal{O}_S$ el anillo de S-enteros correspondiente. Sea G un k-grupo conexo simplemente conexo y semisimple y supongamos $G \subseteq \mathrm{GL}_N$. Un grupo Γ es un grupo aritmético si es conmensurable con

$$G(\mathcal{O}_S) := G(k) \cap \mathrm{GL}_N(\mathcal{O}_S).$$

Nótese que en términos del crecimiento de representaciones de un grupo aritmético Γ podemos asumir $\Gamma = G(\mathcal{O}_S)$. En [56], Lubotzky y Martin iniciaron el estudio del crecimiento de representaciones de grupos aritméticos. Establecieron una conexión entre tener CPR y el famoso Problema de los Subgrupos de Congruencia. Decimos que G tiene la Propiedad de los Subgrupos de Congruencia con respecto a S si todo subgrupo de índice finito $H \leq G(\mathcal{O}_S)$ contiene algún subgrupo de congruencia principal $G(\mathfrak{p})$ para algún ideal $\mathfrak{p} \subset \mathcal{O}_S$. En el capítulo 2 presentamos el Problema de los Subgrupos de Congruencia y explicamos la condición (ligeramente más débil) de tener la Propiedad débil de los Subgrupos de Congruencia (PdSC).

Teorema (Lubotzky y Martin). *Supongamos que G tiene la Propiedad débil de los Subgrupos de Congruencia con respecto a S. Si $\operatorname{char} k = 2$, asumimos también que G no contiene factores de tipo A_1 o C_m para cualquier m. Entonces Γ tiene Crecimiento Polinomial de Representaciones. Además, si $\operatorname{char} k = 0$ el recíproco también es cierto.*

Si G tiene la Propiedad débil de los Subgrupos de Congruencia con respecto a S, la compleción profinita $\widehat{G(\mathcal{O}_S)}$ puede estudiarse a través de la compleción de congruencia $\overline{G(\mathcal{O}_S)}$, la cuál, por el Teorema Fuerte de Aproximación, es isomorfa a $G(\widehat{\mathcal{O}}_S)$. Es decir, el crecimiento de representaciones de Γ viene dado por el de

$$G(\widehat{\mathcal{O}}_S) = \prod_{v \notin S} G(\mathcal{O}_v).$$

Cada factor local $G(\mathcal{O}_v)$ es un grupo compacto k_v-analítico. Para obtener un crecimiento polinomial de representaciones la clave es encontrar una cota uniforme de tal manera que $r_n(G(\mathcal{O}_v)) \leq cn^c$ para todo $v \notin S$. Lubotzky y Martin obtuvieron esta cota uniforme cuando L_G, el álgebra de Lie del grupo algebraico G, es perfecta, equivalentemente, si $\operatorname{char} k = 2$ el grupo G no contiene factores de tipo A_1 o C_m. Cuando el álgebra de Lie no es perfecta Jaikin obtuvo en [38] crecimiento polinomial de representaciones para cada factor local, es decir, para cada v existe una constante c_v tal que $r_n(G(\mathcal{O}_v)) \leq c_v n^{c_v}$. Siguiendo las ideas de Jaikin para el caso local abordamos el caso global al obtener una cota polinomial uniforme para todo v, lo que finalmente lleva al siguiente Teorema (cf. Theorem 3.3).

Teorema 0.1. *Sean k, S, Γ y G como anteriormente. Si G tiene la Propiedad débil de los Subgrupos de Congruencia con respecto a S, entonces Γ tiene Crecimiento Polinomial de Representaciones.*

El trabajo de Lubotzky y Martin en [56] inició el estudio del crecimiento de representaciones de grupos aritméticos (con la Propiedad débil de Subgrupos de Congruencia). En [50] Larsen y Lubotzky estudiaron la abscisa de convergencia $\alpha(\Gamma)$ y Avni demostró en [7] que ésta es un número racional para $\operatorname{char} k = 0$. Una gran parte del trabajo reciente en el área ha sido realizado por Avni, Klopsch, Onn y Voll en una seria de artículos (véase [3], [4], [5] y [6]). Recomendamos [48] para una visión general sobre el área.

Crecimiento de Subgrupos de Grupos Aritméticos

Sea Γ un grupo finitamente generado. Escribiremos $a_n(\Gamma)$ para denotar el número de subgrupos de Γ de índice n y definimos $s_n(\Gamma) := \sum_{i=1}^{n} a_n(\Gamma)$. En analogía con el Crecimiento de Representaciones[1] el Crecimiento de Subgrupos de Γ viene dado por el comportamiento asintótico de $a_n(\Gamma)$ (equivalentemente $s_n(\Gamma)$). El estudio de propiedades estructurales de Γ a través de su crecimiento de subgrupos ha dado pie a una teoría profunda con muchos resultados y aplicaciones, véase [55] y referencias allí.

Al igual que antes, nos centraremos en el crecimiento de subgrupos de grupos aritméticos, más concretamente, nos fijaremos en el crecimiento de subgrupos de un grupo $\Gamma = G(\mathcal{O}_S)$, donde G es un grupo algebraico sobre k que es conexo, simplemente conexo y casi simple y $\mathcal{O}_S$ es el anillo de S-enteros del cuerpo global k.

Si el grupo G tiene la Propiedad de los Subgrupos de Congruencia con respecto a S, entonces todo subgrupo de índice finito es un subgrupo de congruencia y por tanto $s_n(\Gamma) = \gamma_n(\Gamma)$, donde $\gamma_n(\Gamma)$ denota el número de subgrupos de congruencia de índice como mucho n. El estudio del crecimiento de subgrupos de congruencia de grupos aritméticos fue iniciado por Lubotzky en [54]. Para char $k = 0$ Lubotzky encuentra cotas inferiores y superiores para $\gamma_n(\Gamma)$.

Teorema ([54, Teorema A y F]). *Sea* $\Gamma = G(\mathcal{O}_S)$ *como anteriormente. Si* char $k = 0$, *entonces existen constantes* c_1, c_2 *tales que*

$$n^{\frac{c_1 \log^2 n}{\log \log n}} \leq \gamma_n(\Gamma) \leq n^{\frac{c_2 \log^2 n}{\log \log n}}.$$

Si char $k > 0$ *y si* char $k = 2$ *asumimos que* G *no es de tipo* A_1 *o* C_m, *entonces existen constantes* c_3, c_4 *tales que*

$$n^{c_3 \log n} \leq \gamma_n(\Gamma) \leq n^{c_4 \log^2 n}.$$

Abért, Nikolov y Szegedy mejoraron la cota superior en [1].

Teorema ([1, Teorema 1]). *Sea* $\Gamma = G(\mathcal{O}_S)$ *como anteriormente y supongamos que* char $k > 0$. *Supongamos que* G *es split sobre* k *y que si* char $k = 2$ *entonces* G *no es de tipo* A_1 *o* C_m. *Entonces existe una constante* C *que solo depende del rango de Lie de* G *tal que*

$$\gamma_n(\Gamma) \leq n^{D \log n}.$$

En [24], entre otros resultados, Golsefidy obtiene una cota similar sin la necesidad de que G sea split sobre k.

Teorema. *Sea* $\Gamma = G(\mathcal{O}_S)$ *como anteriormente y supongamos que* char $k \geq 5$. *Entonces existen constantes* C *y* D *tales que*

$$n^{C \log n} \leq \gamma_n(\Gamma) \leq n^{D \log n}.$$

---

[1]El estudio de propiedades estructurales de un grupo Γ a través de su crecimiento de subgrupos en realidad precede al enfoque desde el punto de vista del crecimiento de representaciones, de hecho, este último está motivado de alguna manera por la rica teoría de Crecimiento de Subgrupos.

En los resultados previos es necesario que el álgebra de Lie (graduada) asociada a cada factor local $G(\mathcal{O}_v)$ sea perfecta. De ahí la necesidad de excluir los casos en los que G es de tipo A_1 o C_m. Abordamos esta dificultad aplicando el Teorema 0.1 y cierta relación entre el crecimiento de subgrupos y el crecimiento de representaciones.

Teorema 0.2 (cf. Theorem 4.1 y 4.2). *Sea $\Gamma = G(\mathcal{O}_S)$ como anteriormente. Entonces existe una constante $D > 0$ tal que*

$$\gamma_n(\Gamma) \leq n^{D \log n}.$$

Supongamos que G tiene la Propiedad débil de los Subgrupos de Congruencia con respecto a S. Entonces

$$s_n(\Gamma) \leq n^{D \log n}.$$

La Conjetura de los Pseudogrados

Sea J un álgebra associativa finito dimensional sobre un cuerpo finito $\mathbb{F}_q$. Asumamos además que J es nilpotente, es decir, $J^n = 0$ para algún n. Podemos entonces dar al conjunto formal $1 + J = \{1 + j \ : \ j \in J\}$ una estructura de grupo definiendo $(1+j)(1+h) := 1 + j + h + jh$ y $(1+j)^{-1} := \sum_{k=0}^{n-1}(-1)^k j^k$. Llamamos a los grupos de la forma $1 + J$ grupos asociados a álgebras; éstos fueron introducidos por Isaacs en [34] como una generalización de los grupos unitriangulares $U_n(\mathbb{F}_q) = 1 + \mathfrak{u}(\mathbb{F}_q)$, donde $\mathfrak{u}_n(\mathbb{F}_q)$ es el álgebra de matrices cuadradas de tamañano n estrictamente triangulares superiores.

El grupo $1 + J$ actúa de manera natural en el álgebra J y esto induce una acción de $1 + J$ en $\mathrm{Irr}(J)$, los caracteres irreducibles del grupo aditivo de J. En este contexto es posible adaptar el método de las órbitas de Kirillov y tratar de construir una biyección

$$(1 + J)\text{-órbitas en } \mathrm{Irr}(J) \quad \to \quad \mathrm{Irr}(1 + J).$$

Existen serias dificultades para llevar a cabo esta construcción y una tal biyección solo se obtiene cuando $J^p = 0$, donde $p = \mathrm{char}\,\mathbb{F}_q$. Sin embargo la adaptación del método de las órbitas de Kirillov sugiere una función

$$\begin{array}{ccc} (1 + J)\text{-órbitas en } \mathrm{Irr}(J) & \to & \{\chi(1) \ : \ \chi \in \mathrm{Irr}(1 + J)\} \\ \Omega & \mapsto & |\Omega|^{1/2}. \end{array}$$

Isaacs conjeturó que esta función está bien definida y que los $|\Omega|^{1/2}$ (los pseudogrados), contando con multiplicidad, son los grados de los caracteres irreducibles de $\mathrm{Irr}(1 + J)$ para cualquier grupo asociado a un álgebra $1 + J$. Esta conjetura es conocida como la Conjetura de los Pseudogrados. En [36] Jaikin refutó la Conjetura de los Pseudogrados construyendo un grupo asociado a una $\mathbb{F}_2$-álgebra que servía de contraejemplo. No obstante, el comportamiento especial del primo $p = 2$ en correspondencias de caracteres y varios cálculos experimentales sugerían que la conjetura podría ser cierta para grupos asociados a $\mathbb{F}_q$-álgebras donde $\mathrm{char}\,\mathbb{F}_q > 2$. Consideremos la siguiente familia de grupos asociados a $\mathbb{F}_q$-álgebras. Si $\mathrm{char}\,\mathbb{F}_q = p$, consideremos un p-grupo π y sea $I_{\mathbb{F}_q}$ el ideal de augmentación

del álgebra de grupo $\mathbb{F}_q[\pi]$. Entonces $1 + I_{\mathbb{F}_q}$ es un grupo asociado a una $\mathbb{F}_q$-algebra. Si la Conjetura de los Pseudogrados fuera cierta es fácil ver (Lemma 5.3.2) que se debe tener

$$|(1 + I_{\mathbb{F}_q})_{\mathrm{ab}}| = q^{\mathrm{k}(\pi)-1},$$

donde $(1 + I_{\mathbb{F}_q})_{\mathrm{ab}}$ es la abelianización del grupo $1 + I_{\mathbb{F}_q}$ y $\mathrm{k}(\pi)$ denota el número de clases de conjugación del grupo π. El siguiente Teorema da una descripción del tamaño de la abelianización de los grupos de la forma $1 + I_{\mathbb{F}_q}$.

Teorema 0.3 (cf. Theorem 5.4)**.** *Sea π un p-grupo y $I_{\mathbb{F}_q}$ el ideal de augmentación de $\mathbb{F}_q[\pi]$. Entonces*
$$|(1 + I_{\mathbb{F}_q})_{\mathrm{ab}}| = q^{\mathrm{k}(\pi)-1}|B_0(\pi)|.$$

El grupo $B_0(\pi)$ que aparece en el Teorema es el multiplicador de Bogomolov del grupo π. Como para cada primo p existen p-grupos con multiplicador de Bogomolov no trivial el Teorema anterior ofrece contrajemplos a la Conjetura de los Pseudogrados para todo primo p.

La inesperada aparición del multiplicador de Bogomolov en el Teorema anterior nos llevó a seguir investigando los grupos $(1 + I_{\mathbb{F}_q})_{\mathrm{ab}}$. Nótese que para toda $\mathbb{F}_q$-álgebra R, $1 + I_{\mathbb{F}_q} \otimes R$ da un grupo asociado a una $\mathbb{F}_q$-álgebra. Esto define un $\mathbb{F}_q$-grupo algebraico afín G tal que $1 + I_{\mathbb{F}_q} = G(\mathbb{F}_q)$.

Teorema 0.4 (cf. Theorem 5.5)**.** *Sea π un p-grupo y $1 + I_{\mathbb{F}_q}$ el grupo asociado a la $\mathbb{F}_q$-álgebra correspondiente. Sea G el $\mathbb{F}_q$-grupo algebraico asociado. Entonces el grupo derivado $[G, G]$ es un grupo algebraico afín definido sobre $\mathbb{F}_q$ y se tiene*

$$[G, G](\mathbb{F}_q)/[G(\mathbb{F}_q), G(\mathbb{F}_q)] \cong B_0(\pi).$$

Los resultados que aparecen en este capítulo fueron obtenidos en colaboración con Andrei Jaikin y Urban Jezernik y pueden encontrarse en [23].

Productos Directos de Grupos Finitos Simples

Consideremos la siguiente clase de grupos

$$\mathcal{C} := \{\mathbf{H} = \prod_{i \in I} S_i \ : \ S_i \text{ es un grupo finito simple no abeliano}\}.$$

Dago un grupo Γ definimos $R_n(\Gamma) := \sum_{i=1}^{n} r_i(\Gamma)$. Hemos obtenido una caracterización de los grupos en $\mathcal{C}$ que tienen Crecimiento Polinomial de Representaciones.

Teorema 0.5 (c.f Theorem 6.1)**.** *Sea $\mathbf{H} = \prod_{i \in I} S_i$ un producto cartesiano de grupos finitos simples no abelianos y sea $l_{\mathbf{H}}(n) := |\{i \in I : R_n(S_i) > 1\}|$. Entonces $\mathbf{H}$ tiene Crecimiento Polinomial de Representaciones si y solo si $l_{\mathbf{H}}(n)$ esta acotado polinomialmente.*

Es natural preguntarse qué tipos de crecimiento de representaciones pueden ocurrir dentro de los grupos de $\mathcal{C}$ que tienen CPR. En [42], Kassabov y Nikolov estudiaron

cuestiones relacionadas con la clase de grupos $\mathcal{C}$, y más concretamente con la subclase $\mathcal{A} \subset \mathcal{C}$ donde

$$\mathcal{A} := \{\mathbf{H} = \prod_{i \in I} S_i \ : \ S_i = \text{Alt}(m) \text{ para algún } m \geq 5\}$$

y $\text{Alt}(m)$ denota el grupo alternado de m letras. Mostraron que dentro de esta clase $\mathcal{A}$ cualquier tipo de crecimiento de representaciones es posible.

Teorema ([42, Theorem 1.8]). *Para cualquier $b > 0$, existe un grupo $\mathbf{H} \in \mathcal{A}$ tal que $\alpha(\mathbf{H}) = b$.*

Los grupos que aparecen en la prueba del Teorema anterior son de la forma

$$\mathbf{H} = \prod_{i \geq 5} \text{Alt}(i+1)^{f(i)},$$

para alguna $f : \mathbb{N} \to \mathbb{N}$. En particular los factores simples de $\mathbf{H}$ tienen rango no acotado [2] como grupos alternados. Queremos obtener un resultado similar para la subclase $\mathcal{L} \subset \mathcal{C}$, donde

$$\mathcal{L} := \{\mathbf{H} = \prod_{i \in I} S_i \ : \ S_i \text{ es un grupo finito simple de tipo Lie}\}.$$

Obtenemos este resultado en el siguiente Teorema, donde probamos que un resultado análogo es cierto para esta subclase. En nuestro caso, todos los factores simples pueden tener el mismo rango de Lie.

Teorema 0.6 (cf. Theorem 6.12). *Para cualquier $c > 0$, existe un grupo $\mathbf{H} = \prod_{i \in \mathbb{N}} S_i \in \mathcal{L}$ tal que $\alpha(\mathbf{H}) = c$. Además $\mathbf{H}$ puede ser elegido de tal manera que solo ocurra un tipo de Lie entre sus factores.*

Los resultados presentados en este capítulo fueron obtenidos en colaboración con Benjamin Klopsch durante mi estancia en la Universidad de Düsseldorf.

---

[2] Dado S un grupo finito simple no abeliano definimos $\text{rk}\, S = m$ si $S = \text{Alt}(m)$ y $\text{rk}\, S = \text{rk}\, L$ si S es un grupo simple de tipo Lie.

Introduction

Let Γ be a group. A representation of Γ is a homomorphism of groups $\rho : \Gamma \to \mathrm{GL}(V)$ for some finite dimensional complex vector space V. Representation Theory studies the interplay between the structural properties of Γ and its representations. Burnside's Theorem was the first important application of Representation Theory and since then it has become a research area on its own. This work focuses on the representation theory of certain classes of groups. The main body is dedicated to the study of the representation theory (more precisely, the representation growth) of arithmetic groups although we also address some questions related to the representation theory of algebra groups and the representation growth of (direct products of) finite simple groups.

Let Γ be a group and write $r_n(\Gamma)$ for the number of isomorphism classes of n-dimensional irreducible complex representations of Γ. If Γ is finite then $r_n(\Gamma) = 0$ for $n \geq |\Gamma|^{1/2}$. The study of finite groups by means of their irreducible character degrees and conjugacy classes is a well established research area, e.g., see [34] or [32] and references therein. On the other hand for Γ infinite $r_n(\Gamma)$ might well be infinite. The asymptotic behaviour of the sequence $r_n(\Gamma)$ gives the Representation Growth of the group Γ. Let us assume that $r_n(\Gamma) < \infty$ for every n. Then we can associate to the sequence $\{r_n(\Gamma)\}$ a Dirichlet zeta function

$$\zeta_\Gamma(s) = \sum_{n=1}^{\infty} r_n(\Gamma) n^{-s} \quad (s \in \mathbb{C}).$$

The abscissa of convergence $\alpha(\Gamma)$ of $\zeta_\Gamma(s)$ is the infimum of all $\alpha \in \mathbb{R}_{\geq 0}$ such that the series $\zeta_\Gamma(s)$ converges on the right half plane $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \alpha\}$. The abscissa $\alpha(\Gamma)$ is finite if and only if Γ has Polynomial Representation Growth (PRG), that is, if $r_n(\Gamma) \leq p(n)$ for some polynomial p.

Representation Growth of Arithmetic Groups

Let k be a global field, S a finite set of valuations of k containing all archimedean ones and $\mathcal{O}_S$ the corresponding ring of S-integers. Consider G a connected simply connected semisimple algebraic k-group and suppose $G \subseteq \mathrm{GL}_N$. A group Γ is an arithmetic group if it is commensurable with

$$G(\mathcal{O}_S) := G(k) \cap \mathrm{GL}_N(\mathcal{O}_S).$$

Note that in terms of the representation growth of an arithmetic group Γ we may assume that $\Gamma = G(\mathcal{O}_S)$. In [56], Lubotzky and Martin initiated the study of the representation

growth of arithmetic groups. They established a strong connection between having PRG and the famous Congruence Subgroup Problem. Recall that G is said to have the Congruence Subgroup Property with respect to S if every finite index subgroup $H \leq G(\mathcal{O}_S)$ contains some principal congruence subgroup $G(\mathfrak{p})$ for some ideal $\mathfrak{p} \subset \mathcal{O}_S$. In Chapter 2 we present the corresponding Congruence Subgroup Problem and explain the (slightly weaker) condition of having the weak Congruence Subgroup Property (wCSP).

Theorem (Lubotzky and Martin). *Suppose G has the weak Congruence Subgroup Property with respect to S. If $\operatorname{char} k = 2$, assume that G does not contain factors of type A_1 or C_m for any m. Then Γ has Polynomial Representation Growth. Moreover, if $\operatorname{char} k = 0$ the converse holds.*

If G has the weak Congruence Subgroup Property with respect to S, the profinite completion $\widehat{G(\mathcal{O}_S)}$ can be studied through the congruence completion $\overline{G(\mathcal{O}_S)}$, which, by the Strong Approximation Theorem, is isomorphic to $G(\widehat{\mathcal{O}}_S)$. that is, the representation growth of Γ is given by that of

$$G(\widehat{\mathcal{O}}_S) = \prod_{v \notin S} G(\mathcal{O}_v).$$

Each local factor $G(\mathcal{O}_v)$ is a compact k_v-analytic group. To obtain polynomial representation growth the key is to find a uniform bound such that $r_n(G(\mathcal{O}_v)) \leq cn^c$ for every $v \notin S$. Lubotzky and Martin obtained this uniform bound when L_G, the Lie algebra of the algebraic group G, is perfect, i.e., if $\operatorname{char} k = 2$ the group G does not contain factors of type A_1 or C_m. When the Lie algebra is not perfect Jaikin obtained in [38] polynomial representation growth for each local factor, that is, for every v there exists a constant c_v such that $r_n(G(\mathcal{O}_v)) \leq c_v n^{c_v}$. Following Jaikin's ideas for the local case we handle the global case by obtaining a uniform polynomial bound for every v, which ultimately gives the following Theorem (cf. Theorem 3.3).

Theorem 0.1. *Let k, S, Γ and G be as above. If G has the weak Congruence Subgroup Property with respect to S, then Γ has Polynomial Representation Growth.*

The work of Lubotzky and Martin in [56] initiated the study of representation growth of arithmetic groups (with weak CSP). In [50] Larsen and Lubotzky studied the abscisa of convergence $\alpha(\Gamma)$ and Avni showed in [7] that this is a rational number for $\operatorname{char} k = 0$. Most of the recent work has been done by Avni, Klopsch, Onn and Voll in a series of papers (see [3], [4], [5] and [6]). We recommend [48] for a survey on representation growth.

Subgroup Growth of Arithmetic Groups

Let Γ be a finitely generated group. Let us write $a_n(\Gamma)$ for the number of subgroups of Γ of index n and put $s_n(\Gamma) := \sum_{i=1}^{n} a_n(\Gamma)$. Analogously as for the Representation Growth[3]

---

[3]The study of structural properties of a group Γ my means of its subgroup growth actually precedes the representation growth approach and the latter is somehow motivated by the fruitful theory of Subgroup Growth.

the Subgroup Growth of Γ is given by the asymptotic behaviour of $a_n(\Gamma)$ (equivalently $s_n(\Gamma)$). The study of structural properties of Γ via its subgroup growth has evolved into a deep theory with many important results and applications, see [55] and references therein.

As above, we focus on the subgroup growth of arithmetic groups, more precisely, we look at the subgroup growth of a group $\Gamma = G(\mathcal{O}_S)$, where G is a connected simply connected simple k-group and $\mathcal{O}_S$ is the ring of S-integers of the global field k.

If the group G has the Congruence Subgroup Property with respect to S, then every finite index subgroup is a congruence subgroup and so $s_n(\Gamma) = \gamma_n(\Gamma)$, where $\gamma_n(\Gamma)$ stands for the number of congruence subgroups of index at most n. The study of the subgroup growth of congruence subgroups of arithmetic groups was initiated by Lubotzky in [54]. For char $k = 0$ Lubotzky finds lower and upper bounds for $\gamma_n(\Gamma)$.

Theorem ([54, Theorem A and F]). *Let $\Gamma = G(\mathcal{O}_S)$ be as above. If char $k = 0$, then there exist constants c_1, c_2 such that*

$$n^{\frac{c_1 \log^2 n}{\log \log n}} \leq \gamma_n(\Gamma) \leq n^{\frac{c_2 \log^2 n}{\log \log n}}.$$

If char $k > 0$ and in case char $k = 2$ G is not of type A_1 or C_m, then there exists constants c_3, c_4 such that

$$n^{c_3 \log n} \leq \gamma_n(\Gamma) \leq n^{c_4 \log^2 n}.$$

Abért, Nikolov and Szegedy improved the upper bound in [1].

Theorem ([1, Theorem 1]). *Let $\Gamma = G(\mathcal{O}_S)$ be as above and suppose char $k > 0$. Suppose that G splits over k and if char $k = 2$ suppose G is not of type A_1 or C_m. Then there exists a constant C which depends only on the Lie rank of G such that*

$$\gamma_n(\Gamma) \leq n^{D \log n}.$$

In [24], among other things, Golsefidy obtained a similar bound without the split assumption.

Theorem. *Let $\Gamma = G(\mathcal{O}_S)$ be as above and suppose char $k \geq 5$. Then there exist constants C and D such that*
$$n^{C \log n} \leq \gamma_n(\Gamma) \leq n^{D \log n}.$$

In the results above it is necessary that the (graded) Lie algebra associated to each local factor $G(\mathcal{O}_v)$ is perfect. This excludes the cases where G is of type A_1 or C_m. We overcome this difficulty by applying Theorem 0.1 and the relation between subgroup and representation growth.

Theorem 0.2 (cf. Theorem 4.1 and 4.2). *Let $\Gamma = G(\mathcal{O}_S)$ be as above. Then there exists a constant $D > 0$ such that*
$$\gamma_n(\Gamma) \leq n^{D \log n}.$$

Suppose that G has the weak Congruence Subgroup Property with respect to S. Then

$$s_n(\Gamma) \leq n^{D \log n}.$$

The Fake Degree Conjecture

Let J be a finite dimensional associative algebra over a finite field $\mathbb{F}_q$. Assume further that J is nilpotent, that is, $J^n = 0$ for some n. Then one can give to the formal set $1 + J = \{1 + j \; : \; j \in J\}$ a group structure by defining $(1 + j)(1 + h) := 1 + j + h + jh$ and $(1 + j)^{-1} := \sum_{k=0}^{n-1} (-1)^k j^k$. Groups of the form $1 + J$ are called Algebra Groups and were introduced by Isaacs in [34] as a generalization of the unitriangular groups $U_n(\mathbb{F}_q) = 1 + \mathfrak{u}(\mathbb{F}_q)$, where $\mathfrak{u}_n(\mathbb{F}_q)$ is the algebra of strictly upper triangular square matrices of size n.

The group $1 + J$ acts naturally on the algebra J and this induces an action of $1 + J$ on $\mathrm{Irr}(J)$, the irreducible characters of the additive group of J. In this setting, it is possible to adapt Kirillov's Orbit Method and try to build a bijection

$$(1 + J)\text{-orbits in } \mathrm{Irr}(J) \quad \rightarrow \quad \mathrm{Irr}(1 + J).$$

This approach has serious difficulties and such a bijection is only obtained when $J^p = 0$, where $p = \mathrm{char}\,\mathbb{F}_q$. Nevertheless, the adaptation of Kirillov's Orbit Method suggests a map

$$
\begin{array}{ccc}
(1 + J)\text{-orbits in } \mathrm{Irr}(J) & \rightarrow & \{\chi(1) \; : \; \chi \in \mathrm{Irr}(1 + J)\} \\
\Omega & \mapsto & |\Omega|^{1/2}.
\end{array}
$$

Isaacs conjectured that this map is well defined and that the $|\Omega|^{1/2}$'s (the fake degrees), counting multiplicities, give the irreducible character degrees of $\mathrm{Irr}(1 + J)$ for every algebra group $1 + J$. This is known as the Fake Degree Conjecture. In [36] Jaikin disproved the Fake Degree Conjecture by providing an $\mathbb{F}_2$-algebra group which served as a counterexample. Nevertheless, the particular behaviour of the prime $p = 2$ in character correspondences and experimental computations suggested that the conjecture might hold for $\mathbb{F}_q$-algebra groups with $\mathrm{char}\,\mathbb{F}_q > 2$. Let us consider the following family of $\mathbb{F}_q$-algebra groups. If $\mathrm{char}\,\mathbb{F}_q = p$, take a p-group π and let $\mathrm{I}_{\mathbb{F}_q}$ the augmentation ideal of the group algebra $\mathbb{F}_q[\pi]$. Then $1 + \mathrm{I}_{\mathbb{F}_q}$ is an $\mathbb{F}_q$-algebra group. If the Fake Degree Conjecture holds it is easy to see (Lemma 5.3.2) that we must have

$$|(1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}}| = q^{\mathrm{k}(\pi)-1},$$

where $(1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}}$ is the abelianization of the group $1 + \mathrm{I}_{\mathbb{F}_q}$ and $\mathrm{k}(\pi)$ stands for the number of conjugacy classes of the group π. The following Theorem gives a description of the size of the abelianization of groups of the form $1 + \mathrm{I}_{\mathbb{F}_q}$.

Theorem 0.3 (cf. Theorem 5.4). *Let π be a p-group and $\mathrm{I}_{\mathbb{F}_q}$ the augmentation ideal of $\mathbb{F}_q[\pi]$. Then*

$$|(1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}}| = q^{\mathrm{k}(\pi)-1}|B_0(\pi)|.$$

The group $B_0(\pi)$ appearing in the Theorem is the Bogomolov multiplier of the group π. Since for every prime p there exist p-groups with nontrivial Bogomolov multiplier, the previous Theorem provides counterexamples for the Fake Degree Conjecture for every prime p.

The somehow unexpected appearance of the Bogomolov multiplier in the previous Theorem led us to further investigation of the groups $(1 + I_{\mathbb{F}_q})_{\mathrm{ab}}$. Note that for every $\mathbb{F}_q$-algebra R, $1 + I_{\mathbb{F}_q} \otimes R$ gives an $\mathbb{F}_q$-algebra group. This defines an affine algebraic $\mathbb{F}_q$-group G such that $1 + I_{\mathbb{F}_q} = G(\mathbb{F}_q)$.

Theorem 0.4 (cf. Theorem 5.5). *Let π be a p-group and $1 + I_{\mathbb{F}_q}$ the associated $\mathbb{F}_q$-algebra group. Let us consider the associated algebraic $\mathbb{F}_q$-group G as above. Then the derived group $[G, G]$ is an affine algebraic group defined over $\mathbb{F}_q$ and we have*

$$[G, G](\mathbb{F}_q)/[G(\mathbb{F}_q), G(\mathbb{F}_q)] \cong B_0(\pi).$$

The results appearing in this chapter were obtained in joint work with Andrei Jaikin and Urban Jezernik and can be found in [23].

Direct Products of Finite Simple Groups

Let us consider the class of groups

$$\mathcal{C} := \{\mathbf{H} = \prod_{i \in I} S_i \ : \ S_i \text{ is a nonabelian finite simple group}\}.$$

Given a group Γ let us put $R_n(\Gamma) := \sum_{i=1}^{n} r_i(\Gamma)$. We obtain a characterization of groups in $\mathcal{C}$ having Polynomial Representation Growth.

Theorem 0.5 (c.f Theorem 6.1). *Let $\mathbf{H} = \prod_{i \in I} S_i$ be a cartesian product of nonabelian finite simple groups and let $l_{\mathbf{H}}(n) := |\{i \in I : R_n(S_i) > 1\}|$. Then $\mathbf{H}$ has Polynomial Representation Growth if and only if $l_{\mathbf{H}}(n)$ is polynomially bounded.*

It is natural to ask what types of representation growth can occur among groups in $\mathcal{C}$ having PRG. In [42], Kassabov and Nikolov studied questions related to the class $\mathcal{C}$, and more in particular about the subclass $\mathcal{A} \subset \mathcal{C}$ where

$$\mathcal{A} := \{\mathbf{H} = \prod_{i \in I} S_i \ : \ S_i = \mathrm{Alt}(m) \text{ for some } m \geq 5\}$$

and $\mathrm{Alt}(m)$ denotes the alternating group on m letters. They showed that within the class $\mathcal{A}$ any type of representation growth is possible.

Theorem ([42, Theorem 1.8]). *For any $b > 0$, there exists a group $\mathbf{H} \in \mathcal{A}$ such that $\alpha(\mathbf{H}) = b$.*

The groups appearing in the proof of the previous Theorem are of the form

$$\mathbf{H} = \prod_{i \geq 5} \mathrm{Alt}(i+1)^{f(i)},$$

for some $f : \mathbb{N} \to \mathbb{N}$. In particular the simple factors of $\mathbf{H}$ have unbounded rank[4] as alternating groups. We want to obtain a similar result for the subclass $\mathcal{L} \subset \mathcal{C}$, where

$$\mathcal{L} := \{\mathbf{H} = \prod_{i \in I} S_i \ : \ S_i \text{ is a finite simple group of Lie type}\}.$$

---

[4]For S a nonabelian finite simple group we define $\mathrm{rk}\, S = m$ if $S = \mathrm{Alt}(m)$ and $\mathrm{rk}\, S = \mathrm{rk}\, L$ if S is a simple group of Lie type L.

We do this in the following Theorem, where it is shown that an analogous result holds for this class. In our case, all of the simple factors may have the same Lie rank.

Theorem 0.6 (cf. Theorem 6.12). *For any $c > 0$, there exists a group $\mathbf{H} = \prod_{i \in \mathbb{N}} S_i \in \mathcal{L}$ such that $\alpha(\mathbf{H}) = c$. Moreover $\mathbf{H}$ can be chosen so that only one Lie type occurs among its factors.*

The results presented in this chapter where obtained in collaboration with Benjamin Klopsch during my research stay at Heinrich Heine Universtät Düsseldorf.

Chapter 1

Preliminaries

1.1   Global and local fields

By a **global field** we mean a finite field extension of $\mathbb{Q}$ or of $\mathbb{F}_q(t)$ for some prime power q. Global fields have interesting arithmetic properties, resembling those of $\mathbb{Q}$.

Let k be a field. A multiplicative **valuation** or an absolute value on k is a function $v : k \to \mathbb{R}_{\geq 0}$ which satisfies:

   i) $v(x) = 0$ if and only if $x = 0$.

   ii) $v(xy) = v(x)v(y)$ for every $x, y \in k$.

   iii) $v(x + y) \leq v(x) + v(y)$ for every $x, y \in k$.

A valuation v is said to be non-archimedean if it satisfies the ultrametric inequality

$$v(x + y) \leq \max\{v(x), v(y)\} \text{ for every } x, y \in k,$$

and is said to be archimedean otherwise.

We will always assume that a valuation is nontrivial, i.e., $v(x) \neq 1$ for some $x \in k \setminus \{0\}$. Any valuation v defines a metric d_v on k, given by $d_v(x, y) = v(x - y)$ for $x, y \in k$. Two valuations are said to be equivalent if the metrics they induce define the same topology on k. This gives an equivalence relation among valuations of a field k. From now on a valuation will be identified with its equivalence class.

The set of (equivalence classes of) valuations of k will be denoted by V_k. Let us write V_∞ for the set of archimedean valuations and V_f for the non-archimedean ones. The set of archimedean valuations V_∞ is non-empty if and only if char $k = 0$. Note that given a valuation k_v, addition in k is continuous with respect to the topology induced by v. We can consider its completion k_v which is again a valued field where multiplication, addition and the valuation naturally extend those of k.

Given $S \subseteq V_k$ we define the ring of S-integers to be

$$\mathcal{O}_S := \{x \in k \ : \ v(x) \leq 1 \text{ for every } v \in V_f \setminus S\}.$$

The ultrametric inequality for non-archimedean valuations guarantees that $\mathcal{O}_S$ is a subring of the field k.

A **local field** is a field isomorphic either to $\mathbb{C}$ or $\mathbb{R}$ or a finite field extension of the p-adic numbers $\mathbb{Q}_p$ or of the field of formal Laurent series over a finite field $\mathbb{F}_q((t))$.

Suppose now that k is a global field. For every $v \in V_k$ the completion k_v is a local field and v extends to a valuation on k_v which we will continue to denote by v. The following cases may occur: If $v \in V_\infty$ then k_v is isomorphic to $\mathbb{C}$ or $\mathbb{R}$. If $v \in V_f$ and char $k = 0$ then k_v is isomorphic to a finite extension of $\mathbb{Q}_p$ for some prime p. If char $k = p > 0$ then k_v is isomorphic to a finite extension of $\mathbb{F}_q((t))$ for some p-power q.

Suppose now v is non-archimedean. Then

$$\mathcal{O}_v := \{x \in k_v \ : \ v(x) \leq 1\}$$

is a ring. It is the unique maximal compact subring of k_v and is called the **ring of integers** of k_v. The ring $\mathcal{O}_v$ is a discrete valuation ring with maximal ideal

$$\mathfrak{m}_v := \{x \in \mathcal{O}_v \ : \ v(x) < 1\}.$$

It follows that $\mathbb{F}_v := \mathcal{O}_v/\mathfrak{m}_v$ is a field, called the residue field of v (or of k_v). For $x \in \mathfrak{m}_v$ we will write

$$\mathrm{ord}_v(x) := \max\{k \ : \ x \in \mathfrak{m}_v^k\}.$$

We define the **adèle ring or ring of adèles** of the global field k as

$$\mathbb{A}_k := \{(x_v)_{v \in V_k} \in \prod_{v \in V_k} k_v \ : \ x_v \in \mathcal{O}_v \text{ for almost every } v \in V_f\}.$$

Note that $\mathbb{A}_k$ is a subring of the ring $\prod_{v \in V_k} k_v$, where ring operations are made componentwise. The ring $\mathbb{A}_k$ is endowed with the restricted direct product topology with respect to the $\mathcal{O}_v$ ($v \in V_f$), that is, the open sets are of the form $\prod_{v \in V_k} X_v$, where X_v is open in k_v for every $v \in V_k$ and $X_v = \mathcal{O}_v$ for almost every $v \in V_f$. With this topology $\mathbb{A}_k$ is a locally compact topological group. Note that if $x \in k$, then $x \in \mathcal{O}_v$ for almost every $v \in V_f$. It follows that we can embed k diagonally into $\mathbb{A}_k$ as the set of **principal adèles**, $x \mapsto (x)_{v \in V_k}$. Moreover k is discrete in $\mathbb{A}_k$. Given a finite subset $S \subset V_f$ we will write $\mathbb{A}_S$ for the image of $\mathbb{A}_k$ under the natural projection onto the direct product $\prod_{v \notin S} k_v$.

The following Lemma gives a bound for the number of distinct valuations in terms of the size of their residue field, see [56, Lemma 4.7.(a)] for a proof.

Lemma 1.1.1. *Let k be a global field. There exists $a \in \mathbb{N}$, depending only on the field k, such that the number of $v \in V_f$ such that $|\mathbb{F}_v| \leq n$ is bounded by an, and hence also by n^b for some $b \in \mathbb{N}$.*

We shall also need an application of Chebotarev Density Theorem, see [62] for more details.

Theorem 1.1 (Chebotarev density Theorem)**.** *Let k be a global field and K a finite Galois extension of k. Let C be a conjugacy class in $\mathrm{Gal}(K/k)$. Let Σ_C be the set of non-archimedean places $v \in V_f$ that are unramified in k and have Frobenius conjugacy class C. The set Σ_C has a positive Dirichlet density and it is equal to $|C|/|\mathrm{Gal}(K/k)|$. In particular, Σ_C is infinite.*

Lemma 1.1.2. *Let k be a global field and K a finite Galois field extension of k. Then for infinitely many $v \in V_f$ we have $K \subset k_v$.*

Proof. By Chebotarev Density Theorem applied to the trivial conjugacy class $C = \{1\}$ we obtain that there are infinitely many $v \in V_f$ such that v completely splits in K, i.e., $K_w = k_v$, where w is the extension of v to K. But this in particular implies that $K \subseteq k_v$. $\qquad\square$

1.2 Topological groups

We begin by recalling some definitions and concepts generally related to topological spaces. Let us recall that a **filter** $\mathfrak{F}$ in a set X is a collection of non-empty subsets of X such that:

   i) If $F \in \mathfrak{F}$ and $F \subseteq E$, then $E \in \mathfrak{F}$.

   ii) If $E, F \in \mathfrak{F}$ then $E \cap F \in \mathfrak{F}$.

The main example for us is the set of neighbourhoods $\mathfrak{N}(x)$ of an element x in a topological space X, which we called the **neighbourhood filter** of x. In this setting we say that a filter $\mathfrak{F}$ on X **converges** to $x \in X$ if $\mathfrak{N}(x) \subseteq \mathfrak{F}$. Recall that a **filter basis** $\mathfrak{B}$ on a set X is a collection of subsets of X such that:

   i) If $F_1, F_2 \in \mathfrak{B}$, then there exists $F \in \mathfrak{B}$ such that $F \subseteq F_1 \cap F_2$.

   ii) $\emptyset \notin \mathfrak{B}$.

The collection of supersets of a filter basis on X gives a filter on X.

To define the completion of a topological group we first need to establish a notion of nearness of a pair of points in a topological space X. This is done via uniform structures. A uniform structure on a set X consists of a family E of subsets of $X \times X$ called entourages satisfying:

  E1) If $V \in E$ and $V \subseteq U$, then $U \in E$.

  E2) If $U, V \in E$, then $U \cap V \in E$.

  E3) If $V \in E$, then $\Delta = \{(x, x) \,:\, x \in X\} \subseteq V$.

  E4) If $V \in E$, then $V^{-1} := \{(x, y) \,:\, (y, x) \in V\} \in E$.

  E5) If $V \in E$, then there exists $W \in E$ such that $W \circ W \subset V$, where $W \circ W := \{(x, z) \,:\, (x, y), (y, z) \in W$ for some $y \in W\}$.

If $(x, y) \in V$ for some $V \in E$ we say that x is **V-close** to y. We say that $A \subseteq X$ is **V-small** if $A \times A \subseteq V$, equivalently, if every pair of points in A are V-close. Hence, entourages provide a way to measure the nearness of a pair of points in X. Given a uniform structure on X one can endow X with a topology as follows. For every $V \in E$

and $x \in X$ put $V(x) := \{y \in X : (x, y) \in V\}$. Then, for every $x \in X$ we define a system of neighbourhoods of x to be

$$\mathcal{N}(x) := \{V(x) : V \in E\}.$$

It follows that X is Hausdorff if and only if $\bigcap_{V \in E} V = \Delta$. The uniform structure allows us to define a notion of uniform continuity. Namely, a function $f : X \to Y$ between uniform spaces (X, E) and (Y, E') is said to be **uniformly continuous** if for every $W \in E'$ there exists $V \in E$ such that $(f(x), f(x')) \in W$ for every $(x, x') \in V$.

In a similar fashion as a fundamental system of neighbourhoods of a given topology we can define the notion of a fundamental system of entourages of a uniform structure. A family $\mathcal{F} \subseteq E$ is called a **fundamental system of entourages** for E if for every $V \in E$ there exists some $W \in \mathcal{F}$ such that $W \subseteq V$. Equivalently given a fundamental system of entourages $\mathcal{F}$ of a uniform structure E, we can recover E as

$$E = \{V \subseteq X \times X : W \subseteq V \text{ for some } W \in \mathcal{F}\}.$$

A family $\mathcal{F}$ of subsets of $X \times X$ serves as a fundamental system of entourages for a uniform structure on X if and only if $\mathcal{F}$ satisfies the following properties:

F1) For every $U, V \in \mathcal{F}$ there exists $W \in \mathcal{F}$ such that $W \subseteq U \cap V$.

F2) If $V \in \mathcal{F}$, then $\Delta \subseteq V$.

F3) If $V \in \mathcal{F}$, then there exists $W \in \mathcal{F}$ such that $W \in V^{-1}$.

F4) If $V \in \mathcal{F}$, then there exists $W \in \mathcal{F}$ such that $W \circ W \subseteq V$.

An entourage V such that $V = V^{-1}$ is called **symmetric**. If V is symmetric, then $V \cap V^{-1}$ and $V \cup V^{-1}$ are entourages and from this one can check that the set of symmetric entourages forms a fundamental system of entourages.

Given a uniform space X with uniform structure E we want to construct the completion $\widehat{X}$ of X. To this end we need to introduce the notion of a **Cauchy filter**. A filter $\mathfrak{F}$ of X is Cauchy if for every entourage $V \in E$ there exists $F \in \mathfrak{F}$ such that F is V-small, i.e., $F \times F \subseteq V$.

Proposition 1.2.1 ([16, II.3.2.5]). *Let X be a uniform space. For each Cauchy filter $\mathfrak{F}$ on X there is a unique minimal Cauchy filter $\mathfrak{F}_0$ coarser than $\mathfrak{F}$. If $\mathfrak{B}$ is a base of $\mathfrak{F}$ and $\mathfrak{S}$ is a fundamental system of symmetric entourages of X, then the sets $V(M) := \{\bigcup_{x \in M} V(x)\}$ for $M \in \mathfrak{B}$ and $V \in \mathfrak{S}$ form a base of $\mathfrak{F}_0$.*

A uniform space X is called **complete** if every Cauchy filter on X converges to some point.

Theorem 1.2 ([16, Theorem II.3.7.3]). *Let X be a uniform space. Then there exists a complete Hausdorff uniform space $\widehat{X}$ and a uniformly continuous mapping $i : X \to \widehat{X}$ having the following property: Given any uniformly continuous mapping $f : X \to Y$ for*

some complete Hausdorff uniform space Y, there is a unique uniformly continuous mapping $\hat{f} : \widehat{X} \to Y$ such that $f = g \circ i$.

Moreover if (i', X') is another pair consisting of a complete Hausdorff uniform space X' and a uniformly continuous mapping $i' : X \to X'$ having the previous property, then there is a unique isomorphism $\phi : \widehat{X} \to X'$ such that $i' = \phi \circ i$.

Sketch of proof. The space $\widehat{X}$ is defined as the set of minimal Cauchy filters on X (these are the minimal elements with respect to inclusion of the set of Cauchy filters on X). We shall define a uniform structure on $\widehat{X}$. For this purpose, if V is any symmetric entourage of X, let $\widehat{V}$ denote the set of all pairs $(\mathfrak{F}, \mathfrak{G})$ of minimal Cauchy filters which have in common a V-small set. One can check that the sets $\widehat{V}$ form a fundamental system of entourages of a uniform structure on $\widehat{X}$ and that $\widehat{X}$ with this uniform structure is a complete space. The map $i : X \to \widehat{X}$ sends every element $x \in X$ to $N(x)$, which is a minimal Cauchy filter. One can check that the pair $(i, \widehat{X})$ satifies all the required properties. □

Before moving to topological group completions we give the following Theorem about extension of uniformly continuous functions.

Theorem 1.3 ([16, Theorem II.3.6.2]). *Let $f : A \to X'$ be a function from a dense subset A of a uniform space X to a complete Hausdorff uniform space X' and suppose that f is uniformly continuous on A. Then f can be extended to the whole of X by continuity, and the extended function $\hat{f}$ is uniformly continuous.*

This has as an immediate consequence:

Corollary 1.2.1. *Let X and X' be two complete Hausdorff uniform spaces, and let A, A' be dense subsets of X and X' respectively. Then every isomorphism $f : A \to A'$ extends to an isomorphism $\hat{f} : X \to X'$.*

1.2.1 Topological groups and group completions

A **topological group** is a topological space G together with a group structure such that multiplication $m : G \times G \to G$ and inversion $i : G \to G$ are continuous. We will write $H \leq_o G$, respectively $H \leq_c G$, whenever H is an open subgroup, respectively closed subgroup, of G. We similarly write $H \unlhd_o G$ in case H is a normal subgroup. Let us denote by $\mathfrak{N}(e) = \mathfrak{N}$ the neighbourhood filter of the identity element e. Since multiplication by an element $g \in G$ is a homeomorphism, $g \cdot \mathfrak{N}$ or $\mathfrak{N} \cdot g$ are the neighbourhood filter of the element g. Hence the topology on a topological group G is determined by $\mathfrak{N}$. Since in a topological group multiplication and inversion (and hence also conjugation) are continuous it follows that $\mathfrak{N}$ satisfies:

(GB1) For every $U \in \mathfrak{N}$ there exists $V \in \mathfrak{N}$ such that $V \cdot V \subseteq U$.

(GB2) For every $U \in \mathfrak{N}$ we have $U^{-1} \in \mathfrak{N}$.

(GB3) For every $g \in G$ and every $U \in \mathfrak{N}$ we have $gUg^{-1} \in \mathfrak{N}$.

Conversely, we have:

Proposition 1.2.2 ([16, III.1.2.1]). *Let $\mathfrak{N}$ be a filter on a group G such that $\mathfrak{N}$ satisfies (GB1), (GB2) and (GB3). Then there is a unique topology on G, compatible with the group structure of G, for which $\mathfrak{N}$ is the neighbourhood filter of the identity element.*

Let G be an abstract group and $\mathfrak{F}$ a family of subgroups of G. Consider $\mathfrak{B}$ the set of finite intersections of groups of the form $g^{-1}Fg$ for $g \in G$, $F \in \mathfrak{F}$. Then $\mathfrak{B}$ is a filter base and by construction its associated filter satisfies (GB1), (GB2) and (GB3). From any family of subgroups $\mathfrak{F}$ of a given group G, one can construct a topology on G such that F is open for every $F \in \mathfrak{F}$ and with this topology G becomes a topological group.

Let us now focus on Hausdorff topological groups. Recall that we denote by $\mathfrak{N}(e)$ the neighbourhood filter of the identity element in G. It is easy to check that the families

$$\mathcal{F}_r := \{V_r = \{(x,y) \,:\, yx^{-1} \in V\} \quad : V \in \mathfrak{N}(e)\}$$
$$\mathcal{F}_l := \{V_l = \{(x,y) \,:\, x^{-1}y \in V\} \quad : V \in \mathfrak{N}(e)\}$$

satisfy the required properties to be a fundamental system of entourages, and hence define a uniform structure E_r (repectively E_l) on G called the right (respectively left) uniform structure of G which is compatible with the original topology of G, i.e., this uniformity induces the original topology on G. If we now consider $G_l = (G, E_l)$, we want to give to $\widehat{G}_l$ (the completion of G_l as a uniform space, see Theorem 1.2) a topological group structure such that G is a dense subgroup of $\widehat{G}_l$. For this we need to define a continuous multiplication and inversion on $\widehat{G}_l$ extending those of G.

Proposition 1.2.3 ([16], Proposition III.3.4.6). *Let $\mathfrak{F}$ and $\mathfrak{G}$ be two Cauchy filters on G_l. Then the image of the filter $\mathfrak{F} \times \mathfrak{G}$ under the map $(x, y) \mapsto (xy)$ is a Cauchy filter base on G_l.*

It follows that we can define a multiplication on $\widehat{G}_l$ that extends the original one in G. To show that we can also extend inversion to $\widehat{G}_l$ we must assume that the function $x \mapsto x^{-1}$ maps Cauchy filters to Cauchy filters[1]. However let us note that if G has a neighbourhood base of the identity consisting of subgroups then this condition is automatically satisfied. Moreover one can show that the group $\widehat{G}_l$ obtained in this way is unique, in particular, $\widehat{G}_l \cong \widehat{G}_r$. In the end we obtain the following Theorem.

Theorem 1.4 ([16], Theorem III.3.4.1). *A Hausdorff topological group G is isomorphic to a dense subgroup of a complete group $\widehat{G}$ if and only if the image under the symmetry $x \mapsto x^{-l}$ of a Cauchy filter with respect to the left uniformity of G is a Cauchy filter with respect to this uniformity. The complete group $\widehat{G}$, which is called the completion of G, is then unique up to isomorphism.*

1.2.2 Profinite groups

A **directed system** $(\Lambda, \leq)$ is a partially ordered set such that for every pair of elements $\lambda_1, \lambda_2 \in \Lambda$ there exists an element λ_0 such that $\lambda_0 \geq \lambda_1, \lambda_2$. The collection of (normal) subgroups of a group is a directed system ordered by reverse inclusion.

---

[1]There are examples of groups where this assumption is not satisfied, see [16, Exercise 16 X.3].

A **projective system** is a collection of sets $(X_\lambda)_{\lambda \in \Lambda}$ for some directed system Λ together with maps $f_{\lambda \mu} : X_\lambda \to X_\mu$ for every $\lambda \geq \mu$. Given such a directed system we define its **projective limit** as

$$\varprojlim_{\lambda \in \Lambda} := \{(x_\lambda)_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} X_\lambda \; : \; f_{\lambda \mu}(x_\lambda) = x_\mu \text{ for every } \lambda \geq \mu\}$$

If we have a family of normal subgroups $\mathfrak{N}$ of a given group G closed under intersection, then we have group homomorphisms $f_{NM} : G/N \to G/M$ whenever $N \leq M$. This way $\varprojlim_{N \in \mathfrak{N}} G/N$ becomes a subgroup of the direct product $\prod_{N \in \mathfrak{N}} G/N$. If all quotients are finite and we give them the discrete topology, then the inverse limit becomes a closed subgroup of the compact group $\prod_{N \in \mathfrak{N}} G/N$ called the pro-$\mathfrak{N}$ completion of G. If we take $\mathfrak{N}$ to be the family of all finite index normal subgroups of G, then

$$\widehat{G} := \varprojlim_{N \in \mathfrak{N}} G/N$$

is called the profinite completion of G[2].

A **profinite group** G is a compact Hausdorff topological group whose open subgroups form a base for the neighbourhoods of the identity. The following Theorem collects equivalent characterizations of profinite groups:

Theorem 1.5 ([22], Chapter 1)**.** *Let G be a topological group. The following are equivalent:*

i) G is profinite.

ii) G is totally disconnected.

iii) $G \cong \varprojlim_{N \trianglelefteq_o G} G/N$

iv) G has a neighbourhood base of the identity consisting of finite index open subgroups and G is complete.

Consider now an abstract group G and $\mathfrak{N}$ a family of finite index normal subgroups closed under intersection and such that $\bigcap_{N \in \mathfrak{N}} N = e$. On the one hand $\mathfrak{N}$ satisfies (GB1), (GB2) and (GB3) so it induces a topology on G, which makes G into a Hausdorff topological group, and this gives G a uniform structure as well. On the other hand $\varprojlim_{N \in \mathfrak{N}} G/N$ is a profinite group.

Proposition 1.2.4. *Let G and $\mathfrak{N}$ be as above. Then $\widehat{G}_l \cong \varprojlim_{N \in \mathfrak{N}} G/N$.*

Proof. Note that G is dense both in $\varprojlim_{N \in \mathfrak{N}} G/N$ and $\widehat{G}_l$. Since the identity map $\mathrm{id} : G \to G$ is continuous with respect to these structures, Corollary 1.2.1 gives the result. $\qquad\square$

A profinite group is called **pro-nilpotent** if it can be realized as an inverse limit of nilpotent groups. Similarly, a profinite group is called a **pro-p group** if it can be realized as an inverse limit of p-groups.

---

[2]Proposition 1.2.4 justifies the overlaping of notation.

1.2.3 Analytic groups

Throughout this section k is a local field complete with respect to a non-archimedean valuation, $\mathcal{O}$ denotes its valuation ring and $\mathfrak{m}$ its maximal ideal. We refer to Part II of [79] for a more detailed exposition.

Let G be a topological group and suppose further that G has the structure of an analytic manifold over k. We say that G is an **analytic group** over k or a k-analytic group if multiplication $m : G \times G \to G$ and inversion $i : G \to G$ are analytic maps. If G is a $\mathbb{Q}_p$-analytic group we say that G is a **p-adic analytic group**. The following Lemma shows that every k_v-analytic group can be seen either as a p-adic analytic group or an $F_p((t))$-analytic group, see [22, Exercise 13.4].

Lemma 1.2.1. *Suppose k' is a finite separable extension of k with ring of integers $\mathcal{O}'$. Let G be a k'-analytic group and $U \leq_o G$ an $\mathcal{O}'$-standard subgroup (see definition below). Then G has the structure of a k-analytic group as well and U becomes an $\mathcal{O}$-standard subgroup with respect to this structure.*

Formal group laws

Let us write $\mathbf{x} = (x_1, \ldots, x_n)$ to denote a tuple of n variables. For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ let us write $\mathbf{x}^\alpha = x_1^{\alpha_1} \ldots, x_n^{\alpha_n}$ and $|\alpha| = \sum_{i=1}^n \alpha_i$. Given a commutative ring R consider the formal power series ring $R[[x_1, \ldots, x_n]] = R[[\mathbf{x}]]$. A **formal group law** over R in n variables is an n-tuple $F = (F_1, \ldots, F_n)$ of formal power series in $2n$ variables, $F_i \in R[[\mathbf{x}, \mathbf{y}]]$ such that:

1. $F(\mathbf{x}, 0) = \mathbf{x}$ and $F(0, \mathbf{y}) = \mathbf{y}$.

2. $F(F(\mathbf{x}, \mathbf{y}), \mathbf{z}) = F(\mathbf{x}, F(\mathbf{y}, \mathbf{z}))$.

If there is no danger of confusion we will write $\mathbf{x}\mathbf{y} = F(\mathbf{x}, \mathbf{y})$.

Proposition 1.2.5. *Let $F = (F_1, \ldots, F_n)$ be a formal group law over R and let $O(3)$ denote some formal power series whose homogeneous components of degree strictly less than 3 are zero. Then:*

i) For every $1 \leq i \leq n$ we have

$$F_i(\mathbf{x}, \mathbf{y}) = x_i + y_i + \sum_{|\alpha|, |\beta| \geq 1} c_{\alpha\beta} \mathbf{x}^\alpha \mathbf{y}^\beta.$$

ii) There exists a unique $\phi = (\phi_1, \ldots, \phi_n)$ where $\phi_i \in R[[\mathbf{x}]]$ called the formal inverse such that $\phi(0) = 0$ and

$$F(\mathbf{x}, \phi(\mathbf{x})) = F(\phi(\mathbf{x}), \mathbf{x}) = 0.$$

We will write $\mathbf{x}^{-1} := \phi(\mathbf{x})$.

iii) $F(\mathbf{x}, \mathbf{y}) = \mathbf{x} + \mathbf{y} + B(\mathbf{x}, \mathbf{y}) + O(3)$, *where B is an R-bilinear form. We define*

$$[\mathbf{x}, \mathbf{y}] := B(\mathbf{x}, \mathbf{y}) - B(\mathbf{y}, \mathbf{x}).$$

.

iv) $\mathbf{x}^{-1} = -\mathbf{x} + B(\mathbf{x}, \mathbf{x}) + O(3)$.

v) $F(F(\mathbf{x}, \mathbf{y}), \mathbf{x}^{-1}) = \mathbf{y} + [\mathbf{x}, \mathbf{y}] + O(3)$ *and more precisely*

$$\mathbf{x}\mathbf{y}\mathbf{x}^{-1} = \mathbf{y} + [\mathbf{x}, \mathbf{y}] + \sum_{|\alpha|, |\beta| \geq 1, |\alpha| + |\beta| \geq 3} d_{\alpha, \beta} \mathbf{x}^{\alpha} \mathbf{y}^{\beta},$$

where $d_{\alpha, \beta} \in R$.

vi) $\mathbf{x}^{-1}\mathbf{y}^{-1}\mathbf{x}\mathbf{y} = [\mathbf{x}, \mathbf{y}] + O(3)$.

vii) $[\mathbf{x}, [\mathbf{y}, \mathbf{z}] + [\mathbf{y}, [\mathbf{z}, \mathbf{x}]] + [\mathbf{z}, [\mathbf{x}, \mathbf{y}]] = 0$.

viii) $\mathbf{x}^m = \sum_{i=1}^{\infty} \binom{m}{i} \psi_i(\mathbf{x})$, *where $\psi_i(\mathbf{x})$ has order at least i.*

Standard groups

Let $F = (F_1, \dots, F_n)$ a group law over $\mathcal{O}$ and put

$$G = \{(g_1, \dots, g_n) \ : \ x_i \in \mathfrak{m}\} = (\mathfrak{m})^n.$$

Given $g = (g_1, \dots, g_n)$, $h = (h_1, \dots, h_n) \in G$, define multiplication on G by $gh := F(g, h)$ and inversion by $g^{-1} := \phi(g)$ where ϕ is the inverse associated to F. Then G is an analytic k-group. Any group isomorphic to one of the form of G is called an $\mathcal{O}$-**standard group**. To every $\mathcal{O}$-standard group G one can associate a corresponding $\mathcal{O}$-Lie algebra, namely we take $\mathcal{L}_G := (\mathcal{O}^n, [\ \ ])$ and define for $\mathbf{x}, \mathbf{y} \in \mathcal{O}^n$

$$[\mathbf{x}, \mathbf{y}] = B(x, y) - B(y, x),$$

where B is the $\mathcal{O}$-bilinear form associated to the formal group law F as in 1.2.5.iii), which by 1.2.5.vii) defines a Lie bracket. Note that by 1.2.5.v) we have

$$\mathbf{x}\mathbf{y}\mathbf{x}^{-1} = \mathbf{y} + [\mathbf{x}, \mathbf{y}] + \sum_{|\alpha|, |\beta| \geq 1, |\alpha| + |\beta| \geq 3} d_{\alpha\beta} \mathbf{x}^{\alpha} \mathbf{y}^{\beta} = \mathbf{y} \operatorname{Ad}_{\mathcal{O}}(\mathbf{x}) + \mathbf{O}_{\mathbf{y}}(2),$$

where $O_y(2)$ denotes some power series whose terms have degree at least 2 in y_i. Hence $\operatorname{Ad}_{\mathcal{O}} : G \to \operatorname{Aut}_{\mathcal{O}}(\mathcal{L}_G)$ gives an $\mathcal{O}$-linear action of G on $\mathcal{L}_G$ called the **adjoint action**. For $g \in G$, $\operatorname{Ad}_{\mathcal{O}}(g)$ is given by

$$\mathbf{x} \mapsto \mathbf{x} + [\mathbf{g}, \mathbf{x}] + \sum_{|\beta|=1} d_{\alpha, \beta} \mathbf{g}^{\alpha} \mathbf{x}^{\beta}. \tag{1.1}$$

Theorem 1.6. *Every k-analytic group G has an open $\mathcal{O}$-standard subgroup.*

The Lie algeba of an analytic group and the adjoint action

Given a k-analytic group G, let $U \leq_o G$ be an open standard subgroup with a homeomorphism: $f : U \to k^n$ such that $f(1) = 0$. Then the group law in U gives a formal group law F on k^n. Now let us denote by $\mathcal{L}(G)$ the tangent space of G at 1. Then the differential of f at 1 gives an isomorphism $df : \mathcal{L}(G) \to k^n$. For every $x, y \in \mathcal{L}(G)$ we define

$$df([x, y]) = [df(x), df(y)]_F,$$

where the Lie bracket on the right is the one associated to the formal group law F. Note that since U is standard, the formal group F can actually be interpreted as a formal group law over $\mathcal{O}$. The associated Lie bracket is thus $\mathcal{O}$-linear and extends to a k-linear bracket.

If U' is another standard subgroup with chart $f' : U' \to k^n$ an associated formal group law F', then $f^{-1} \circ f'_{|f(U \cap U')} \to f'(U \cap U')$ gives a local analytic isomorphism at 0 and induces a formal homomorphism from F to F'. The following lemma shows that $\mathcal{L}(G)$ is well defined.

Lemma 1.2.2. *Let F and F' be two formal group laws and let f be a formal homomorphism from F to F' (that is, $f(F(X, Y)) = F'(f(X), f(Y))$). Let f_1 be the linear part of f. Then:*

$$[f_1(X), f_1(Y)]'_F = f_1([X, Y[_F).$$

Equivalently, if we denote by $k[G]$ the k-algebra of analytic functions on G, there is a natural isomorphism from $\mathcal{L}(G)$ to the space of left invariant derivations of $k[G]$, which is a Lie algebra, see 1.4 below. One can endow $\mathcal{L}(G)$ with a Lie algebra structure via this isomorphism and this gives the same Lie algebra structure on $\mathcal{L}(G)$ as before.

For $g \in G$, let φ_g denote conjugation by g. Then φ_g defines an automorphism of G and by the previous lemma its differential $d\varphi_g$ gives an automorphism of $\mathcal{L}(G)$. The adjoint action of G is $\mathrm{Ad}_{k_v} : G \to \mathrm{Aut}_{k_v}(\mathcal{L}(G))$, given by $g \mapsto d\varphi_g$. Moreover, Ad_{k_v} is an analytic map. Indeed, since Ad_{k_v} is clearly a group homomorphism, it suffices to check that Ad_{k_v} is analytic at e. Now in local coordinates, it follows from (1.1) that Ad_{k_v} is analytic at e.

1.3 Affine algebraic varieties

We refer to [12] for a more detailed presentation. Let K be an algebraically closed field. A K-space $(X, \mathcal{O}_X)$ is a topological space X together with a sheaf $\mathcal{O}_X$ of K-algebras on X whose stalks are local rings. We will often write X for $(X, \mathcal{O}_X)$ and $K[X] = \mathcal{O}_X(X)$. For $x \in X$ we write $\mathcal{O}_x$ for the stalk over x. Its maximal ideal is denoted $\mathfrak{m}_x$ and its residue class field by $K(x)$. A morphism $(Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X)$ is a continuous function $f : Y \to X$ together with K-algebra homomorphisms $f_U^V : \mathcal{O}_X(U) \to \mathcal{O}_Y(V)$ whenever $U \subset X$, $V \subset Y$ are open subsets such that $f(V) \subset U$. These maps are required to be compatible with the respective restriction homomorphisms in $\mathcal{O}_X$ and $\mathcal{O}_Y$. For $y \in Y$ we can pass to the limit over neighborhoods V of y and U of $x = f(y)$ to obtain a homomorphism $f_y : \mathcal{O}_x \to \mathcal{O}_y$. It is further required of a morphism that this always be a local homomorphism, that is, that $f_y(\mathfrak{m}_x) \subseteq \mathfrak{m}_y$.

An **affine K-algebra** A is a finitely generated K-algebra. We write

$$\mathrm{Spec}_m(A) := \{\mathfrak{m} \subset A \;:\; \mathfrak{m} \text{ is a maximal ideal}\}.$$

Recall that the Nullstellensatz gives a canonical bijection

$$
\begin{array}{rccl}
e: & \mathrm{Hom}_K(A, K) & \to & X := \mathrm{Spec}(A) \\
& g & \mapsto & \ker g.
\end{array}
$$

Given $x \in X$ and $f \in A$ we will write $f(x) = e^{-1}(x)(f)$. The resulting function $f : X \to K$ determines f modulo the nilradical of A. Hence if A is reduced (i.e. the nilradical of A is trival), we can identify A with a ring of X-valued functions on X. We give X the structure of a K-space as follows. We endow X with the Zariski topology, that is, the closed sets are of the form

$$V(J) = \{\mathfrak{m} \in X \;:\; J \subseteq \mathfrak{m}\}$$

for some $J \subseteq A$. Moreover, to every open subset $U \subseteq X$ we associate the K-algebra $A_{S(U)}$, the localization of A at $A \setminus S(U)$, where $S(U)$ is the set of $f \in A$ such that $f(x) \neq 0$ for every $x \in U$. This gives a presheaf on the topological space X, which induces a sheaf $\tilde{A}$ on X. It is easy to see that for every $x \in X$ the stalk at x is isomorphic to the local ring A_x.

Any K-space isomorphic to one of the form $(\mathrm{Spec}_m(A), \tilde{A})$ will be called an **affine K-space**. A homomorphism $\alpha^* : A \to B$ of affine K-algebras induces a continuous function $\alpha : Y \to X$, where $Y = \mathrm{Spec}_m(B)$. If $U \subset X$ and $V \subset Y$ are open and $\alpha(V) \subseteq U$ then $\alpha(S(U)) \subseteq S(V)$ so there is a natural homomorphism $A_{S(U)} \to B_{S(V)}$. These induce a morphism on the associated K-spaces $(Y, \tilde{B}) \to (X, \tilde{A})$. Hence the assignment $A \mapsto \mathrm{Spec}_m(A)$ gives a contravariant functor from the category of affine K-algebras to the category of affine K-spaces.

Theorem 1.7. *Let $X = \mathrm{Spec}_m(A)$, $Y = \mathrm{Spec}_m(B)$ be affine K-spaces. The natural map $A \mapsto \tilde{A}(X)$ is an isomorphism, and the map*

$$
\begin{array}{rccl}
\mathrm{Mor}_K(Y, X) & \to & \mathrm{Hom}_K(A, B) \\
\alpha & \mapsto & \alpha^*
\end{array}
$$

is bijective. Thus the assignment $A \to \mathrm{Spec}_m(A)$ is a contravariant equivalence from the category of affine K-algebras to the category of affine K-spaces.

Let X and Y be affine K-spaces. The product $X \times Y$ is characterized by the property that morphisms from an affine K-space Z to $X \times Y$ are pairs of morphisms to the two factors. Applying this to $Z = \mathrm{Spec}_m(K)$ we find that the underlying set of $X \times Y$ is the usual cartesian product. From 1.7 it follows immediately that the product of affine K-spaces $\mathrm{Spec}_m(A)$ and $\mathrm{Spec}_m(B)$ exists and equals $\mathrm{Spec}_m(A \otimes_K B)$.

An affine K-space $X = \mathrm{Spec}_m(A)$ is said to be an **affine K-variety** if A is reduced. By gluing affine K-spaces one can construct the more general concepts of K-schemes and K-varieties. However, throughout this work we will only encounter affine K-spaces

and affine varieties, so whenever we use the terms K-space and K-variety we mean affine K-space and affine K-variety.

From now on let $X = \mathrm{Spec}_m(K[X])$ be a K-variety. A subvariety Y of X is a closed subset $Y \subseteq X$ where $\mathcal{O}_Y = \mathcal{O}_{X|Y}$ Every such Y is given by an ideal $I \subseteq K[X]$ and $Y = \mathrm{Spec}_m(K[X]/I) \hookrightarrow \mathrm{Spec}_m(K[X])$.

We recall that a topological space X is said to be irreducible if it is not empty and is not the union of two proper closed subsets. An algebraic variety is said to be **irreducible**, if it is not empty and can not be represented as a union of two proper algebraic subvarieties. Every algebraic variety X is a union of finitely many maximal algebraic irreducible subvarieties which are called the **irreducible components** of X. We define the **dimension** of X, $\dim X$, as the supremum of the lengths, n, of chains $F_0 \subset F_1 \subset \ldots \subset F_n$ of distinct irreducible closed sets in X.

k-structures, k-varieties and k-morphisms

Let k be a subfield of K. Given a K-algebra A a **k-structure** on A is a k-subalgebra A_k such that we have a natural isomorphism $K \otimes_k A_k \cong A$.

Let Y be an algebraic subvariety of the affine space $K^n = \mathrm{Spec}_m(K[x_1, \ldots, x_n])$. The subvariety Y is called **k-closed** or closed over k if X is the set of common zeros of a finite system of polynomials with coefficients in k. A subvariety Y is k-closed if and only if it is invariant under the natural action on K^n of the Galois group of the field K over k. Let us denote by $I(Y) \subseteq K[x_1, \ldots, x_n]$ the ideal of polynomials vanishing on Y, and put $I_k(Y) = I(Y) \cap k[x_1, \ldots, x_n]$. A subvariety Y is said to be **k-defined**, or defined over k, if $I_k(Y)$ is a k-structure on $I(Y)$, i.e., if $I(Y) = K \otimes_k I_k(Y)$. A subvariety Y is closed over k if and only if it is defined over some purely inseparable field extension of k. If Y is defined over k, then $K[Y] = K \otimes_k k[Y]$, where $k[Y] = k[x_1, \ldots, x_n]/I_k(Y)$. In other words, if Y is defined over k, then the k-algebra $k[Y]$ is a k-structure on the K-algebra $K[Y]$. A function $f \in K[Y]$ is said to be defined over k if $f \in k[Y]$.

To define a k-structure on an affine algebraic variety X is the same thing as to define an isomorphism $\alpha : X \twoheadrightarrow Y$ of the variety X onto an algebraic subvariety Y of an affine space which is defined over k. An affine variety equipped with a k-structure is called an **affine k-variety**. The image of the k-algebra $k[Y]$ under the comorphism α^* is called the algebra of k-regular functions on the k-variety X and is denoted by $k[X]$. Note that $k[X]$ is a k-structure of the k-algebra $K[X]$ of regular functions on X. Two k-structures on an affine variety are called equivalent if the corresponding algebras of k-regular functions coincide. We say that a morphism $\alpha : X \to X'$ between two affine k-varieties is defined over k or that α is a k-morphism if the image of $k[X']$ under the comorphism α^* is contained in $k[X]$. If Y and Y' are subvarieties of affine spaces defined over k, then a morphism $\alpha : Y \twoheadrightarrow Y'$ is defined over k if and only if α is defined by polynomials with coefficients in k.

If X and Y are affine k-varieties then $X \times Y$ becomes a k-variety with k-structure given by $k[X] \otimes_k k[Y]$.

If X is an affine k-variety , we denote by $X(k) = \mathrm{Hom}_k(k[X], k)$ the set of its **k-rational points**.

We shall identify the k-variety X with the set $X(K)$. In particular, a susbset $A \subseteq X$ is

said to be **Zariski-dense** if it is dense in $X(K)$.

Theorem 1.8 ([12, AG.14.4]). *Let V be a k-variety and $X \subseteq V(k)$. Then the Zariski closure of X is defined over k.*

Tangent spaces and differentials

Let X be an affine K-variety. Recall that $\mathcal{O}_x$ denotes the local ring at x and $\mathfrak{m}_x$ is the unique maximal ideal in $\mathcal{O}_x$. Note that K is naturally isomorphic to the quotient ring $K(x) = \mathcal{O}_x/\mathfrak{m}_x$. We denote the image of the element $f \in \mathcal{O}_x$ under the projection $\mathcal{O}_x \to \mathcal{O}_x/\mathfrak{m}_x \cong K$ by $f(x)$. A **derivation** at the point x is a K-linear map $\delta : \mathcal{O}_x \to K$ such that $\delta(fg) = f(x)\delta(g) + \delta(f)g(x)$ for every $f, g \in \mathcal{O}_x$. We define $\mathcal{T}_x(X)$ to be the set of derivations at x, which has a natural structure of K-vector space. The space $\mathcal{T}_x(X)$ is called the **tangent space of X at x**. Note that there is a natural isomorphism between $\mathcal{T}_x(X)$ and $\operatorname{Hom}_K(\mathfrak{m}_x/\mathfrak{m}_x^2)$. Equivalently, one can interpret $\mathcal{T}_x(X)$ via dual numbers as follows. Recall that given a ring R, the ring of dual numbers of R is $R[\epsilon] \cong R[T|T^2 = 0]$ and there is a natural projection $R[\epsilon] \twoheadrightarrow R$. This induces a morphism $\operatorname{Hom}_K(K[X], K[\epsilon]) \to \operatorname{Hom}_K(K[X], K)$ whose fibre above x is K-isomorphic to $\mathcal{T}_x(X)$.

If $\alpha : X \to Y$ is a morphism of algebraic varieties, we can define a map $d\alpha_x : \mathcal{T}_x(X) \to \mathcal{T}_{\alpha(x)}(Y)$, called the **differential of α at x**, as follows: if $v \in \mathcal{T}_x(X)$, $f \in \mathcal{O}_{f(x)}$ and α^* is the comorphism of α, we set $d\alpha_x(v)(f) = v(\alpha^*(f))$. If X is a k-variety for some subfield k one can give a k-structure $\mathcal{O}_{x,k}$ to the local ring $\mathcal{O}_x$ and and this induces a k-structure $\mathcal{T}_{x,k}(X)$ on $\mathcal{T}_x(X)$ given by the k-linear derivations from $\mathcal{O}_{x,k}$ to k and we have $\mathcal{T}_{x,k} \cong \ker(\operatorname{Hom}_k(k[X], k[\epsilon]) \to \operatorname{Hom}_k(k[X], k))$. Moreover, if α is a k-morphism then $d\alpha_x(\mathcal{T}_{x,k}(X)) \subseteq \mathcal{T}_{f(x),k}(Y)$. We call a point $x \in X$ a **simple point** if $\mathcal{O}_x$ is a regular local ring. If X is an irreducible variety this means that $\dim X = \dim \mathcal{T}_x(X)$ (if X is irreducible we always have $\dim \mathcal{T}_x(X) \geq \dim X$). The set of simple points of X is Zariski dense and open in X. If all points are simple, then we say that X is **smooth**.

Local fields and the space of adèles

Let X be an affine k-variety and let $\iota : X \to \mathbb{A}^n$ be an embedding onto a closed subvariety of an affine space. We make an abuse of notation an identify $X = \iota(X)$. For every $v \in V_k$ the subspace $X(k_v) = \operatorname{Hom}(k[X], k_v)$ can be given a topology induced by that of k_v. Indeed, since $X \subseteq \mathbb{A}^n$ we can see $X(k_v) \subseteq k_v^n$ and give $X(k_v)$ the topology as a subspace of the topological space k_v^n. Hence $X(k_v)$ is a closed subspace of a locally compact topological space, which is itself locally compact. It is easily checked that this topology does not depend on the embedding ι of X into $\mathbb{A}^n$.

For $v \in V_f$ let us write $X(\mathcal{O}_v)$ for the points in X all of whose coordinates lie in $\mathcal{O}_v$, so we have $X(\mathcal{O}_v) \subseteq X(k_v)$ is a compact subspace. We define the **adèle space of X** as follows:

$$X(\mathbb{A}) = \{(x_v)_{v \in V_k} \in \prod_{v \in V_k} X(k_v) \ : \ x_v \in X(\mathcal{O}_v) \text{ for almost every } v \in V_f\}.$$

We endow $X(\mathbb{A}_k)$ with a topology by considering it as a subspace of the restricted topological direct product of the $X(k_v)$ with respect to $X(\mathcal{O}_v)$, that is, open sets are of the form

$\prod_{v \in v_k} \mathcal{O}_v$ where $\mathcal{O}_v$ is open in $X(k_v)$ and $\mathcal{O}_v = X(\mathcal{O}_v)$ for almost every $v \in V_k$. One can check that the space $X(\mathbb{A}_k)$ does not depend on the initial embedding ι of X into an affine space. Since the $X(\mathcal{O}_v)$ are compact and $X(k_v)$ is locally compact, $X(\mathbb{A}_k)$ is a locally compact space. In the same way that k embeds diagonally as a discrete subspace in $\mathbb{A}_k$, $X(k)$ embeds diagonally as a discrete subspace in $X(\mathbb{A}_k)$, that is, $X(k)$ is naturally identified with the set of principal adèles of $X(\mathbb{A}_k)$ via the diagonal embedding $x \mapsto (x)_{v \in V_f}$.

1.4   Algebraic groups

Let G be an affine algebraic variety over an algebraically closed field K. Suppose that we have morphisms of algebraic varieties $m : G \times G \to G$, $i : G \to G$ and $e : G \to K$ (i.e. $e \in G(K)$) such that G is a group with multiplication given by m, inversion given by i and e as an identity element. Then we call G an **algebraic group**.

If G is a k-variety and the morphisms m, i and e are defined over k, then G is said to be defined over k or an **algebraic k-group** or simply a k-group.

A subgroup H of an algebraic group G is called algebraic if H is an algebraic subvariety of G. Algebraic subgroups defined over k (as algebraic subvarieties) are called k-subgroups. An algebraic subgroup of an algebraic group is called k-closed or closed over k (respectively k-defined or defined over k) if it is k-closed (respectively k-defined) as an algebraic subvariety.

By the center of a k-group G we mean the center of the group $G(K)$, which is an algebraic subgroup of G that is k-closed and will be denoted $Z(G)$.

An algebraic group morphism $\alpha : G \to G'$ is defined as a group homomorphism which is an algebraic variety morphism. The morphism α is said to be k-defined if it is k-defined as morphism of algebraic varieties. If G and G' are k-groups we say that they are isomorphic over k or k-isomorphic if there exists a k-isomorphism $\alpha : G \to G'$.

The following proposition shows that every affine algebraic k-group is linear.

Proposition 1.4.1 ([12, Proposition I.1.10]). *Let G be an affine k-group, then G is k-isomorphic to a k-subgroup of the group GL_n for some n.*

Algebraic subgroups of GL_n are called **linear algebraic groups**. The algebra $k[\mathrm{GL}_n]$ has the form $k[GL_n] = k[x_{11}, x_{12}, \ldots, x_{nn}, \det^{-1}]$, where we have chosen coordinates such that for a matrix $g = (g_{ij}) \in \mathrm{GL}_n$ we have $x_{ij}(g) = g_{ij} - \delta_{ij}$ and $\det(g) = \det((g_{ij}))$. Note that with respect to this coordinates, the identity matrix has zero coordinates except for $\det \mathrm{Id} = 1$.

An algebraic group is called **connected** if it is connected in the Zariski topology. We will denote by G^0 the connected component of the identity in the group G, that is the maximal connected algebraic subgroup of G.

Proposition 1.4.2 ([12, I.1.2]). *Let G be an affine algebraic k-group. The factor group G/G^0 is finite, G^0 is defined over k and every algebraic subgroup of finite index in G contains G^0.*

Reductive, semisimple and (almost) simple groups

Let K be an algebraically closed field and G a linear algebraic group. Fix an embedding $\iota : G \to \mathrm{GL}_n(K)$ for some n and assume from now on that $G \subseteq \mathrm{GL}_n(K)$. An element $g \in G$ is said to be **semisimple** if it is diagonalizable as an element of $\mathrm{End}_n(K)$. An element $g \in G$ is said to be **unipotent** if $g - \mathrm{Id}$ is a nilpotent element in $\mathrm{End}_n(K)$. These concepts are independent of the chosen embedding ι. We say that G is unipotent if all of its elements are unipotent.

The **unipotent radical** $\mathrm{R}_u(G)$ of an algebraic group G is the maximal connected algebraic unipotent normal subgroup in G. If $\mathrm{R}_u(G)$ is trivial then G is said to be a **reductive** group. We present some results concerning reductive groups.

Theorem 1.9 ([15, 2.14 and 2.15]). *Let G be a connected reductive k-group. Then*

i) If k is infinite then $G(k)$ is Zariski dense in G.

ii) $Z(G)$ is defined over k.

The following Theorem by Mostow (see [65, 7.1] or [14, Proposition 5.1]) shows that in charactersitic 0 any k-group G is a semidirect product of a reductive k-subgroup H and its unipotent radical $\mathrm{R}_u(G)$ ($\mathrm{R}_u(G)$ is a k-defined subgroup of G).

Theorem 1.10. *Suppose* $\mathrm{char}\, k = 0$. *Let G be a k-group and $\mathrm{R}_u(G)$ its unipotent radical. Then there exists a reductive k-subgroup H such that $G = H \ltimes \mathrm{R}_u(G)$ (as k-groups).*

.

Lemma 1.4.1. *Let G a connected reductive k-group. Then $G = [G, G] \cdot Z(G)^0$.*

The **solvable radical** $\mathrm{R}_s(G)$ of an algebraic group G is the maximal connected algebraic solvable normal subgroup in G. If $\mathrm{R}_s(G)$ is trivial then G is said to be **semisimple**.

An algebraic group G is called (absolutely) **simple** (respectively (absolutely) **almost simple**) if the trivial subgroup is the only proper algebraic normal subgroup of G (respectively all such subgroups are finite). If G is an algebraic k-group, then G is called k-simple (respectively almost k-simple) if this condition holds for k-closed normal subgroups.

Tori, rank and root systems

A commutative algebraic group T is said to be a **torus** if it is connected and T is isomorphic to the product of $\dim T$ many copies of the group $\mathbb{G}_m$. A torus T is called **k-split** or split over k if it is defined over k and is k-isomorphic to the direct product of $\dim T$ many copies of $\mathbb{G}_m$. Every torus defined over k is split over some finite separable field extension of k.

Let G be an algebraic k-group. If G is reductive, then (see [15, 4.21 and 8.2]) the maximal k-split tori of G are conjugate by elements of $G(k)$ and, hence, all have the same dimension. If G is reductive we denote by $\mathrm{rank}_k G$ the k-rank of the group G, i.e., the common dimension of maximal k-split tori in G. If $\mathrm{rank}_k G > 0$, then G is said to be **k-isotropic** or isotropic over k. Otherwise G is said to be **k-anisotropic** or anisotropic

over k. An almost k-simple factor of G which is k-isotropic (resp. k-anisotropic) will be called a k-isotropic (resp. k-anisotropic) factor. A reductive k-group G is called k-split or split over k, if G contains a k-split torus which is a maximal torus of the group G, in other words, if $\operatorname{rank}_k G = \operatorname{rank}_K G$ where K is the algebraic closure of k.

Let G be a connected semisimple algebraic k-group and let T be a maximal k-split torus in G. Then one can associate to the pair (T, G) a root system $\Phi(T, G)$. We refer to [12, Chapters 4 and 5] for a detailed exposition on this subject.

Isogenies and simply connected groups

A surjective group homomorphism with finite kernel is called an **isogeny**. A morphism $f : G \to G'$ of algebraic groups is called **quasi-central** if $\ker f \subset Z(G)$. In other words, f is quasi-central if there exists a mapping $\chi : f(G) \times f(G) \to G$ such that $\chi(f(x), f(y)) = xyx^{-1}y^{-1}$ for all $x, y \in G$. We say that f is **central** if it is quasi-central and the mapping χ is a morphism of algebraic varieties. We say that a connected semisimple group G is **simply connected** if every central isogeny $f : G' \to G$ between connected algebraic groups is an algebraic group isomorphism.

Theorem 1.11. *If G is a semisimple k-group there exists a connected simply connected semisimple k-group $\widetilde{G}$ and a central k-isogeny $p : \widetilde{G} \to G$.*

Theorem 1.12 ([15, 2.15])**.** *Let G be an algebraic k-group. Suppose that G is connected and semisimple. Then:*

i) G decomposes uniquely (up to permutation of the factors) into an almost direct product of connected non-commutative almost simple algebraic subgroups $G_1, \ldots, G_m$, i.e., there exists a central isogeny

$$p : G_1 \times \ldots \times G_m \to G.$$

ii) G decomposes uniquely (up to permutation of the factors) into an almost direct product of connected non-commutative almost k-simple k-subgroups $G'_1, \ldots, G'_r$, i.e., there exists a central k-isogeny

$$p' : G'_1 \times \ldots \times G'_r \to G.$$

Moreover, the almost simple factors (almost k-simple factors) are invariant under isogenies (k-isogenies), that is, if $f : G \to H$ is an isogeny (k-isogeny), the image of an almost simple factor (almost k-simple factor) is an almost simple factor (almost k-simple factor).

The Lie algebra of an algebraic group

Recall that given an R-algebra A for some commutative ring R, an R-derivation of A is an R-linear map $D : A \to A$ such that $D(ab) = D(a)b + aD(b)$. We denote by $\mathrm{Der}_R(A)$ the set of R-derivations of A. It is easy to check that for $D, E \in \mathrm{Der}_R(A)$ $[D, E] := DE - ED$ belongs to $\mathrm{Der}_R(A)$ as well. Hence $\mathrm{Der}_R(A)$ has a Lie algebra structure.

Let G be an algebraic k-group. We will write $L_G = \mathcal{T}_e(G)$ and give it the structure of a Lie algebra as follows. For every $x \in G$, left multiplication by g gives an automorphism $\lambda_g : K[G] \to K[G]$. We define

$$\mathrm{Lie}(G) := \{D \in \mathrm{Der}_K(A) \mid \lambda_g D = D\lambda_g, \text{ for every } g \in G\}.$$

One checks that $\mathrm{Lie}(G)$ is a Lie subalgebra of $\mathrm{Der}_K(A)$. Moreover, one can give $\mathrm{Lie}(G)$ a k-structure via

$$\mathrm{Lie}(G)_k := \{D \in \mathrm{Lie}(G) \mid D(k[G]) \subseteq k[G]\}.$$

Now note that evaluation at e gives a map $D \mapsto D_e$ from $\mathrm{Lie}(G) \to \mathcal{T}_e(G)$ such that $D_e(f) = (D(f))(e)$. Moreover, this is a linear isomorphism, so L_G becomes a Lie algebra via this isomorphism.

Restriction of scalars

We refer to [15, 6.17-2.21], [59, 1.7] and [87, 1.3] for a detailed presentation. Let l be a finite separable extension of k. If V is an l-variety we want to find a k-variety W such that in some sense $W(k)$ corresponds to $V(l)$. Suppose V is an affine l-variety given by some ideal $I \leq l[x_1, \ldots, x_n]$, i.e., $l[V] = l[x_1, \ldots, x_n]/I$. Let $\sigma \in \mathrm{Gal}(l/k)$ and define V^σ to be the l-variety defined by $I^\sigma := \sigma(I)$, i.e., $l[V^\sigma] = l[x_1, \ldots, x_n]/I^\sigma$. Analogously if $p : V \to V'$ is an l-morphism of l-varieties we obtain from σ a morphism $p^\sigma : V^\sigma \to V'^\sigma$. Let $\{\sigma_1 = \mathrm{Id}, \sigma_2, \ldots, \sigma_d\}$ be the set of all distinct k-embeddings of the field l into the algebraic closure of k. Then for each l-variety V there exists a k-variety W and an l-morphism $p : W \to V$ such that the map $(p^{\sigma_1}, \ldots, p^{\sigma_d}) : W \to V^{\sigma_1} \times \ldots V^{\sigma_d}$ is an isomorphism of algebraic varieties. Moreover, the pair (W, p) is defined uniquely up to k-isomorphism.

The variety W is denoted by $R_{l/k}(V)$ and is called the **restriction of scalars** from l to k of V. The restriction of scalars from l to k, $R_{l/k}$, gives a functor from the category of l-varieties into the category of k-varieties. The map $p : R_{l/k}(V) \to V$ has the following universal property: for a k-variety X and an l-morphism $f : X \to V$ there exists a unique k-morphism $\phi : X \to R_{l/k}(V)$ such that $f = p \circ \phi$. Notice that if f is an l-group morphism, then ϕ is a k-group morphism. The restriction of the projection projection $p : W \to V$ to $W(k)$ induces a bijection between $W(k)$ and $V(l)$. We denote by $R_{l/k}^0$ the inverse map to $p_{|V(k)}$. If V is an l-group, then $R_{l/k}(V)$ is a k-group, p is an l-group morphism and $R_{l/k}^0 : V(l) \to W(k)$ is a group isomorphism.

Theorem 1.13 ([83, 3.1.2]]). *Let G be a simply connected almost k-simple k-group. Then there exist a finite separable extension k' of k and a connected simply connected absolutely almost simple k'-group H such that $G = R_{k'/k}(H)$.*

1.5 Affine group schemes

We refer to [89, Chapter 1 and 2] for a more detailed presentation. Throughout this section let k be a commutative ring with 1. A functor $F : k - \text{algebras} \to \text{Sets}$ is said to be **representable** if there exists a k-algebra A and a natural correspondence between $F(R)$ and $\text{Hom}_k(A, R)$ for every k-algebra R, in this case we will say that A represents F. If F is representable, $k[F]$ will denote a k-algebra which represents F.

An **affine group scheme over k** or an affine group k-scheme is a representable functor from the category of k-algebras to groups. Suppose G is an affine group scheme over k represented by a k-algebra $k[G]$, then multiplication and inversion induce k-algebra maps $\Delta : k[G] \to k[G] \otimes_k k[G]$ (comultiplication), $\epsilon : k[G] \to k$ (counit) and $S : k[G] \to k[G]$ (antipode) such that $(k[G], \Delta, \epsilon, S)$ becomes a Hopf Algebra. Equivalently, every Hopf k-algebra A, gives an affine group k-schme G given by $G(R) = \text{Hom}_k(A, R)$ for every k-algebra R, where multiplication, unit and inverse are induced from Δ, ϵ and S.

Theorem 1.14. *Affine group schemes over k correspond to Hopf algebras over k.*

Dual numbers and the functor Lie

Given a k-algebra R, the algebra of dual numbers of R is the k-algebra $R[\epsilon] := R[x]/\langle x^2 \rangle$. More precisely, $R[\epsilon] = R + R\epsilon$ is a free R-module of rank 2 with multiplication given by $(a + b\epsilon)(c + d\epsilon) = ac + (ad + bc)\epsilon$ for $a, b, c, d \in R$. Note that we have two natural k-algebra morphism $\iota_R : R \to R[\epsilon]$ and $p_R : R[\epsilon] \to R$ such that $p_r \circ \iota_R = \text{id}_R$.

Consider now an affine group k-scheme G. Then we have a map $G(p_R) : G(R[\epsilon]) \to G(R)$. We define $\text{Lie}(G)(R) := \ker G(p_R)$. Let us write $I_G := \ker(\epsilon : k[G] \to k)$.

Theorem 1.15. *For every k-agebra R there are isomorphisms of abelian groups between the following:*

i) $\text{Der}_k(A, R)$.

ii) $\text{Hom}_k(I_G/I_G^2, R)$.

iii) $\text{Lie}(G)(R)$.

These isomorphisms are natural in R and compatible with the action of R.

Affine algebraic groups and affine group schemes

Let now k be a field. Given an affine algebraic k-group G the algebra of regular functions $k[G]$ defines a representable functor, which by abuse of notation we will continue to denote by G,

$$G : \quad k\text{-algebras} \quad \to \quad \text{Sets}$$
$$R \quad \mapsto \quad \text{Hom}_k(k[G], R)$$

Note that the multiplication, inversion and unit maps in G gives comaps $m^* : k[G] \to k[G] \otimes_k k[G]$, $i^* : k[G] \to k[G]$ and $\epsilon^* : k \to k[G]$. Since G is an algebraic group these comaps make $k[G]$ a Hopf algebra over k. It follows that we can see an affine algebraic k-group as an affine group k-scheme which is represented by $k[G]$.

1.6 Representation Theory

Definition. Let Γ be a group. A **complex representation** of Γ is a group homomorphism

$$\rho : \Gamma \to \mathrm{GL}(V),$$

where V is a finite dimensional $\mathbb{C}$-vector space. Equivalently, a representation of Γ is a linear action of Γ on a finite dimensional complex vector space V. We say write $\dim \rho = \dim V$ for the dimension of ρ.

If the group Γ has a topology, we require ρ to be **continuous**, where $\mathrm{GL}(V)$ is given the usual topology[3] as a subset of the $\mathbb{C}$-vector space $\mathrm{End}_{\mathbb{C}}(V)$.

We say that ρ is **finite** if it has finite image, otherwise we say that ρ is infinite.

A **subrepresentation** of ρ is given by a subspace $W \subseteq V$ such that $\rho(\Gamma)(W) \subseteq W$. Note that if W is such a subspace, ρ gives a linear action of Γ on W and hence a representation $\rho_{|W} : \Gamma \to \mathrm{GL}(W)$.

A representation ρ is **irreducible** if it has no nontrivial subrepresentation $0 \subset W \subset V$.

Two representations $\rho : \Gamma \to \mathrm{GL}(V)$ and $\rho' : \Gamma \to \mathrm{GL}(W)$ are **isomorphic**, $\rho \cong \rho'$, if there exists an isomorphism of vector spaces $f : V \to W$ such that $f(\rho(g)(v)) = \rho'(g)(f(v))$ for every $v \in V$ and $g \in \Gamma$. The relation $\cong$ gives an equivalence relation. We write $\mathrm{Rep}_n(\Gamma)$ (respectively $\mathrm{Irr}_n(\Gamma)$) for the set of isomorphism classes of n-dimensional complex representations (respectively irreducible representations) and put $\mathrm{Rep}(\Gamma) := \bigcup_n \mathrm{Rep}_n(\Gamma)$ (repectively $\mathrm{Irr}(\Gamma) = \bigcup_n \mathrm{Irr}_n(\Gamma)$). We will also write $\mathrm{Irr}_{\leq n}(\Gamma) = \bigcup_{i \leq n} \mathrm{Irr}_i(\Gamma)$. We will usually make an abuse of notation by identifying a class $\overline{\rho} \in \mathrm{Irr}(\Gamma)$ with one of its representatives ρ.

We say that $\rho \in \mathrm{Irr}(\Gamma)$ is an **irreducible constituent** of a representation $\theta : \Gamma \to \mathrm{GL}_n(V)$ if there exists a subrepresentation $W \subseteq V$ such that $\rho \cong \theta_{|W}$.

Given two representation $\rho_1 : \Gamma \to \mathrm{GL}(V)$ and $\rho_2 : \Gamma \to \mathrm{GL}(W)$ we can construct a new representation $\rho_1 \oplus \rho_2 : \Gamma \to \mathrm{GL}(V \oplus W)$, called the direct sum of ρ_1 and ρ_2, by diagonally embedding $\mathrm{GL}(V)$ and $\mathrm{GL}(W)$ into $\mathrm{GL}(V \oplus W)$.

A representation $\rho \in \mathrm{Rep}(\Gamma)$ is called **completely reducible** if it is isomorphic to a direct sum of irreducible subrepresentations.

Theorem 1.16 (Maschke's Theorem)**.** *If Γ is a finite group, then every representation of Γ is completely reducible.*

Given $\rho \in \mathrm{Rep}(\Gamma)$ by Maschke's Theorem we have $\rho = m_1 \lambda_1 \oplus \ldots \oplus m_r \lambda_r$ for some $\lambda_i \in \mathrm{Irr}(\Gamma)$. The λ_i are called the irreducible constituents of ρ and $m_i \in \mathbb{N}$ is the multiplicity of λ_i in ρ, where $m\lambda := \oplus_{i=1}^n \lambda$. If $\lambda \in \mathrm{Irr}(\Gamma)$, we write $\langle \rho, \lambda \rangle$ for the multiplicity of λ in ρ (which might be equal to zero). Both the irreducible constituents of a representation and their multiplicities are uniquely determined.

---

[3]Often in the literature $\mathrm{GL}(V)$ is given the discrete topology. This ensures that a continuous homomorphism from a profinite group Γ to $\mathrm{GL}(V)$ has finite image. Nevertheless, one gets the same conclusion if $\mathrm{GL}(V)$ is given the usual topology, see Lemma 3.1.1.

Suppose now $\Gamma' \leq \Gamma$ is a finite index subgroup such that $|\Gamma : \Gamma'| = m$. If $\rho : \Gamma \to \mathrm{GL}(V)$ is a representation of Γ, we can consider the restriction of ρ to Γ', $\rho_{|\Gamma'} : \Gamma' \to \mathrm{GL}(V)$, which gives a representation of Γ'.

Given $\rho : \Gamma \to \mathrm{GL}(V)$ we say that ρ is **imprimitive** if there exist $W_1, \ldots, W_n$ subspaces of V such that $V = \bigoplus W_i$ and the W_i are transitively permuted by the action of Γ, otherwise we say it is **primitive**. Given a representation $\rho \in \mathrm{Rep}_n(\Gamma')$ there exists a representation $\mathrm{Ind}_{\Gamma'}^{\Gamma}(\rho) : \Gamma \to \mathrm{GL}(V)$ having an imprimitive decomposition $V = \bigoplus_{i=1}^{n} W_i$, where Γ' is the stabilizer of W_1 and $\rho \cong \left(\mathrm{Ind}_{\Gamma'}^{\Gamma}(\rho)_{|\Gamma'} \right)_{|W_1}$.

Theorem 1.17 (Frobenius reciprocity). *Let Γ be a group and $\Gamma' \leq \Gamma$ a finite index subgroup. If $\rho \in \mathrm{Irr}(\Gamma)$ and $\rho' \in \mathrm{Irr}(\Gamma')$ then*

$$\langle \rho, \mathrm{Ind}_{\Gamma'}^{\Gamma} \rho' \rangle = \langle \rho_{|\Gamma'}, \rho' \rangle.$$

Consider now $N \trianglelefteq \Gamma$. If $\lambda \in \mathrm{Rep}(N)$, then for $g \in \Gamma$ we can define λ^g given by $\lambda^g(n) = (gng^{-1})$. If λ is irreducible then so is λ^g. This gives an action of Γ on $\mathrm{Irr}(N)$. We have the following Theorem.

Theorem 1.18 (Clifford Theory). *Let $N \trianglelefteq \Gamma$ and consider $\lambda \in \mathrm{Irr}(N)$. Let $H = \mathrm{St}_\Gamma(\lambda) = \{g \in \Gamma \ : \ \lambda^g \cong \lambda\}$. Then the map*

$$\mathrm{Ind} : \quad \begin{array}{ccc} \{\psi \in \mathrm{Irr}(H) \ : \ < \psi_{|N}, \lambda > \neq 0\} & \to & \{\rho \in \mathrm{Irr}(\Gamma) \ : \ < \rho_{|N}, \lambda > \neq 0\} \\ \psi & \mapsto & \mathrm{Ind}_{H}^{\Gamma} \psi \end{array}$$

is a bijection. In other words, every irreducible representation $\rho \in \mathrm{Irr}(\Gamma)$ such that $< \rho_N, \lambda > \neq 0$ is induced from an irreducible representation of the stabilizer of λ.

Given a representation $\rho : \Gamma \to \mathrm{GL}(V)$ we define its **character**

$$\begin{array}{cccc} \chi_\rho : & \Gamma & \to & \mathbb{C} \\ & g & \mapsto & \mathrm{tr}\, \rho(g), \end{array}$$

where $\mathrm{tr}\, \rho(g)$ stands for the trace of the matrix $\rho(g)$. Note that $\dim \rho = \chi_\rho(1)$, so given a character χ its dimension or degree is given by $\chi(1)$. A character of an irreducible representation is said to be an irreducible character. It is easy to check that character are constant on conjugacy classes and that two isomorphic representations have the same character. Conversely we have the following Theorem.

Theorem 1.19. *Let Γ be a finite group. Then two representations $\rho_1, \rho_2 \in \mathrm{Rep}_n(\Gamma)$ are isomorphic if and only if $\chi_{\rho_1} = \chi_{\rho_2}$. Moreover, $\rho \cong m_1 \lambda_1 \oplus \ldots m_k \lambda_k$ if and only if $\chi_\rho = m_1 \chi_{\lambda_1} + \ldots + \chi_{\lambda_k}$.*

It follows that a representation of a finite group is completely determined by its character.

A **projective representation** of Γ is a group homomorphism

$$\rho : \Gamma \to \mathrm{PGL}(V)$$

where V is a finite dimensional complex vector space and $\mathrm{PGL}(V)$ stands for the projective linear group of V. We write $\dim \rho = \dim V$.

1.7 Finite groups of Lie type

We refer to [57, Part III] and references therein for a more detailed presentation. Let p be a prime, let q denote some p-power and let us write $\mathbb{F}$ for an algebraic closure of $\mathbb{F}_p$. Suppose G is a reductive algebraic group defined over $\mathbb{F}_q$. The map $F^0 : \mathbb{F}_q[G] \to \mathbb{F}_q[G]$ given by $x \mapsto x^q$ is an $\mathbb{F}_q$-endomorphism of the algebra $\mathbb{F}_q[G]$. Hence, the map $\mathrm{Frob}_q := F^0 \otimes \mathrm{Id}$ gives a map $\mathbb{F}[G] \to \mathbb{F}[G]$ called the **Frobenius endomorphism** of G. A **Steinberg endomorphism** of a linear algebraic group G is an endomorphism $F : G \to G$ such that $F^m = \mathrm{Frob}_q$ for some $\mathbb{F}_q$-structure of G and some $m \geq 1$. A **finite group of Lie type** is a group of the form G^F where G is a reductive algebraic group and F is a Steinberg endomorphism of G. Finite groups of Lie type give rise to an important part of the finite simple groups.

Theorem 1.20 (Tits, see [57, 24.17]). *Let G be a simply connected absolutely simple linear algebraic $\mathbb{F}_q$-group with Steinberg endomorphism F. Then, except for a finite number of exceptions (in particular whenever $q \neq 2, 3$) G^F is perfect and $G^F/Z(G^F)$ is a finite simple group.*

A finite simple group of the form $G^F/Z(G^F)$ is called a **finite simple group of Lie type**.

Let G be a connected reductive algebraic group with root system Φ and let F be a Frobenius endomorphism of G with respect to some $\mathbb{F}_q$-structure of G. Then F induces an automorphism τ of the Coxeter diagram associated to Φ. Moreover if G is an absolutely almost simple simply connected algebraic group, F is uniquely determined (up to inner automorphism) by the pair (τ, q), see [57, Theorem 22.5]. Given a reductive algebraic group G and a Frobenius automorphism F, we will say that the finite group G^F is of type $L = (\Phi, \tau)$, where Φ is the root system of G and τ is the automorphism induced by F on the corresponding Coxeter diagram. By a **Lie type** L we mean a pair (Φ, τ) obtained as the type of some finite group of Lie type G^F. For a root system Φ, we denote by $\mathrm{rk}\,\Phi$ its rank and by Φ^+ a choice of positive roots. For a Lie type $L = (\Phi, \tau)$ we write $\mathrm{rk}\,L = \mathrm{rk}\,\Phi$. Finally, given an irreducible root system Φ its Coxeter number h is defined by $h = |\Phi|/\mathrm{rk}\,\Phi$.

The following is Lemma 4.11 in [56].

Lemma 1.7.1. *Let Φ be a perfect finite central extension of a finite simple group of Lie type $H(\mathbb{F}_q)/Z(H(\mathbb{F}_q))$. Then there exists $\delta > 0$, depending neither on q nor on the Lie type, such that every nontrivial complex projective representation of Φ has dimension at least q^δ. In particular, any proper subgroup $\Phi' \leq \Phi$ has index at least q^δ.*

1.8 Commutative algebra

Let R be a ring and M an R-module (we will consider all modules to be right modules). If R and M carry topological structures, the action of R on M is assumed to be continous and all submodules are considered to be closed. Given $r \in R$ and $m \in M$, we will write $[m, r] = mr - m$. If $M' \subseteq M$ and $R' \subseteq R$, denote by $[M', R']$ the smallest R-module containing all elements of the form $[m, r]$, where $m \in M'$, $r \in R'$.

If a group H acts by automorphisms on an abelian group M, we call M an H-module. We adopt similar conventions and notation for H-modules as for R-modules.

Lemma 1.8.1. *Let H be a pro-p group, M an abelian pro-p group and suppose that M is an H-module. If $M/[M,H]$ is finite, then M is a finitely generated H-module. Conversely, if M has finite exponent and M is a finitely generated H-module then $M/[M,H]$ is finite.*

Proof. Suppose that $M/[M,H]$ is finite. Let $m_1, \ldots, m_r \in M$ be representatives of $M/[M,H]$ and write N for the H-submodule they generate. Suppose $N \lneq M$, then there exists an H-module $L \leq_o M$ such that $N + L \lneq M$ ([75, Lemma 5.3.3(c)]). Pick M' maximal H-module such that $N + L \leq M'$, then M/M' is a finite simple H-module (i.e., it has no nontrivial proper H-submodules). But H being a pro-p group, this implies that H acts trivially on M/M' (otherwise the set of fixed points would be a nontrivial proper H-submodule as we have a p-group acting on a set of p-power order), that is, $[M,H] \subseteq M'$. It follows that $N + [M,H] \leq M'$, which contradicts the construction of N. Therefore, $N = M$ and $m_1, \ldots, m_r$ generate M.

Conversely, suppose that M is finitely generated and M has finite exponent. Then the action of H on $M/[M,H]$ is trivial, hence it is just a finitely generated abelian group with finite exponent, hence finite. $\qquad\square$

Chapter 2

The Congruence Subgroup Problem

2.1 Introduction

Let k be a global field, S a finite set of valuations and $\mathcal{O}_S$ the ring of S-integers. Prototypical examples of global fields are $\mathbb{Q}$ and $\mathbb{F}_p(t)$ with rings of S-integers $\mathbb{Z}$ ($S = \emptyset$) and $\mathbb{F}_p[t]$ ($S = \{v_\infty\}$[1]). Let us consider an algebraic group G defined over k. The relation between the group $G(k)$ of k-rational points of G and the arithmetic of k represents a source of interesting questions. The arithmetic of k is best reflected on its rings of S-integers $\mathcal{O}_S$. Analogously, if we fix a k-embedding $\iota : G \to \mathrm{GL}_n$, we can see $G(k)$ as a subgroup of $\mathrm{GL}_n(k)$ and set

$$G(\mathcal{O}_S) := G(k) \cap \mathrm{GL}_n(\mathcal{O}_S).$$

Note that, in general, the group $G(\mathcal{O}_S)$ depends on the choice of the k-embedding. For instance, if we take $G = (k, +)$, the additive group of k, and two different embeddings $\iota_j : G \to \mathrm{GL}_2$, given by

$$\iota_1 : \ x \mapsto \begin{pmatrix} 1 & \frac{x}{2} \\ 0 & 1 \end{pmatrix} \quad \iota_2 : \ x \mapsto \begin{pmatrix} 1 & \frac{x}{3} \\ 0 & 1 \end{pmatrix},$$

we obtain different groups $G(\mathcal{O}_S)$ for each embedding. Nevertheless certain properties have an intrinsic nature that are independent of the chosen embedding. The Congruence Subgroup Property is one of these. Let us start by giving an example that lies in the origin of the subject.

Take $k = \mathbb{Q}$, $\mathcal{O}_S = \mathbb{Z}$ and $G = \mathrm{SL}_n$ ($n \geq 2$). For every integer $m \in \mathbb{Z}$ we have a ring homomorphism $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ and this gives a group homomorphism $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$. The kernel of this map is called the principal congruence subgroup of level m. Any subgroup of $\mathrm{SL}_n(\mathbb{Z})$ which contains a principal congruence subgroup of some level is called a congruence subgroup. Note that $\mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$ is a finite subgroup, hence every congruence subgroup has finite index in $\mathrm{SL}_n(\mathbb{Z})$. The Congruence Subgroup Problem asks whether

---

[1]v_∞ stands for the degree valuation on $\mathbb{F}_p(t)$: $v_\infty(0) = 0$ and $v_\infty(\frac{f}{g}) = e^{-(\deg g - \deg f)}$.

every finite index subgroup is a congruence subgroup, or more generally, how far this is from being true.

By the end of the 19 century Fricke and Klein showed that the answer is negative for $\mathrm{SL}_2(\mathbb{Q})$. In the 1960s Bass, Lazard and Serre [8] and independently Mennicke [61] solved the problem in the affirmative for SL_n, $n \geq 3$. The formulation of the problem for G any linear algebraic group and k a global field was introduced in [9]. We refer to the surveys [74], [72] or the book [82] for more references and results on the Congruence Subgroup Problem.

2.2 Arithmetic groups

Throughout this section we follow [59, 1.3]. Let k be a global field. We refer to section 1.1 for notation and definitions concerning global and local fields. Fix a finite subset S of V_k that is supposed to be non-empty[2] in case $\operatorname{char} k > 0$. Recall that

$$\mathcal{O}_S = \{x \in k \mid x \in \mathcal{O}_v \ \forall v \in V_f \setminus S\}$$

is the ring of S-integers of the field k.

Let G be an algebraic k-group. We fix a k-embedding[3] $\iota : G \hookrightarrow \mathrm{GL}_N$ and consider from now on $G \subseteq \mathrm{GL}_N$. We define the group of S-integral points of G as

$$G(\mathcal{O}_S) := G(k) \cap \mathrm{GL}_N(\mathcal{O}_S).$$

Let us note that G is an affine k-variety, that is, we can see G as the vanishing set of a radical ideal $J \leq K[x_{11}, \ldots, x_{NN}]$, where K is an algebraic closure of k. Since G is a k-group, we have $J = J_k \otimes K$ where $J_k := J \cap k[x_{11}, \ldots, x_{NN}]$. Now since GL_N is an affine group $\mathbb{Z}$-scheme it can be seen in particular as an affine group $\mathcal{O}_S$-scheme represented by $\mathcal{O}_S[\mathrm{GL}_N] = \mathbb{Z}[\mathrm{GL}_N] \otimes \mathcal{O}_S$, see section 1.5. If we put $J_{\mathcal{O}_S} := J \cap \mathcal{O}_S[x_{11}, \ldots, x_{NN}]$, we can consider the affine group $\mathcal{O}_S$-subscheme $G_{\mathcal{O}_S}$ defined by the ideal $J_{\mathcal{O}_S}$, i.e., represented by $\mathcal{O}_S[G_{\mathcal{O}_S}] := \mathcal{O}_S[x_{11}, \ldots, x_{NN}]/J_{\mathcal{O}_S}$. Note that by construction we have $k[G] = \mathcal{O}_S[G_{\mathcal{O}_S}] \otimes_{\mathcal{O}_S} k$. We will make an abuse of notation and write G for $G_{\mathcal{O}_S}$ if there is no danger of confusion. Hence, from now on we will assume that G has the structure of an affine group $\mathcal{O}_S$-scheme. In this sense we have

$$G(\mathcal{O}_S) = \operatorname{Hom}_{\mathcal{O}_s}(\mathcal{O}_S[G], \mathcal{O}_S)$$

and the notation is consistent with both descriptions of $G(\mathcal{O}_S)$.

For every ideal $\mathfrak{q}$ of $\mathcal{O}_S$ we define the **principal S-congruence subgroup of level $\mathfrak{q}$** to be

$$G(\mathfrak{q}) := G(\mathcal{O}_S) \cap \mathrm{GL}_N(\mathfrak{q}),$$

where $\mathrm{GL}_N(\mathfrak{q})$ is the subgroup of $\mathrm{GL}_N(\mathcal{O}_S)$ consisting of matrices congruent to the identity matrix modulo $\mathfrak{q}$. Equivalently, we have

$$G(\mathfrak{q}) = G(\mathcal{O}_S) \cap \ker\left(\mathrm{GL}_N(\mathcal{O}_S) \to \mathrm{GL}_N(\mathcal{O}_S/\mathfrak{q})\right).$$

---

[2]Note that otherwise the ring of S-integers is empty.

[3]By Proposition 1.4.1 there exists a k-isomorphism onto a k-subgroup of some GL_n but it is not unique.

If we regard G as an affine group $\mathcal{O}_S$-scheme then $\mathcal{O}_S/\mathfrak{q}$ is an $\mathcal{O}_S$-algebra and we have a map $G(\mathcal{O}_S) \to G(\mathcal{O}_S/\mathfrak{q})$, so equivalently we have

$$G(\mathfrak{q}) = \ker\left(G(\mathcal{O}_S) \to G(\mathcal{O}_S/\mathfrak{q})\right).$$

Subgroups of $G(\mathcal{O}_S)$ containing some $G(\mathfrak{q})$ ($\mathfrak{q} \neq \mathfrak{o}$) are called **S-congruence subgroups**. The following Lemma collects some facts that will be used in the sequel.

Lemma 2.2.1 ([59, 1.3.1.1]). *Let $f : G \to G'$ be a k-morphism (as k-varieties) between linear algebraic k-groups, $G \subseteq GL_n$ and $G' \subseteq \mathrm{GL}_m$. Then*

    i) for every non-zero ideal $\mathfrak{p} \subset \mathcal{O}_S$, there exists a non-zero ideal $\mathfrak{q} \subset \mathcal{O}_S$ such that $f(G(\mathfrak{q})) \subseteq G'(\mathfrak{p})$.

    ii) Suppose that f is a homomorphism of k-groups. Then for every S-congruence subgroup $H \leq G'(\mathcal{O}_S)$, $f^{-1}(H)$ contains an S-congruence subgroup of the group $G(\mathcal{O}_S)$. In particular, the notion of S-congruence subgroup is independent of the chosen embedding.

    iii) Every S-congruence subgroup of the group $G(\mathcal{O}_S)$ is of finite index in $G(\mathcal{O}_S)$.

    iv) Suppose that f is an isomorphism of k-groups. Then the subgroups $f(G(\mathcal{O}_S))$ and $G'(\mathcal{O}_S)$ are commensurable.

    v) For each $g \in G(k)$ the subgroups $gG(\mathcal{O}_S)g^{-1}$ and $G(\mathcal{O}_S)$ are commensurable.

A subgroup of G is called an **S-arithmetic subgroup** if it is commensurable with $G(\mathcal{O}_S)$. From Lemma 2.2.1.iv) it follows that the notion of S-arithmetic subgroup is intrinsic with respect to the k-structure on G, that is, if $f : G \to G'$ is a k-isomorphism of k-groups, then a subgroup Γ of G is S-arithmetic if and only if $f(\Gamma)$ is an S-arithmetic subgroup of G'.

Lemma 2.2.2 ([59, 1.3.1.3]). *Let $f : G \to G'$ be a k-morphism of k-groups and let $\Gamma \subset G$, $\Gamma' \subset G'$ be S-arithmetic subgroups. Then:*

    i) The subgroup $\Gamma \cap f^{-1}(\Gamma')$ is of finite index in Γ, in particular, it is an S-arithmetic subgroup.

    ii) For every $g \in G(k)$ the subgroups $g\Gamma g^{-1}$ and Γ are commensurable.

Theorem 2.1 ([69, Theorem 4.1]). *Suppose $\mathrm{char}\, k = 0$ and let $f : G \to H$ be a surjective morphism of k-groups. Then for every S-arithmetic subgroup Γ of G, $f(\Gamma)$ is an S-arithmetic subgroup.*

A discrete subgroup Γ in a locally compact group H is a **lattice** if $\mu_H(\Gamma \setminus H) < \infty$, where μ_H stands for the Haar measure of H. We present now some results about lattices in semisimple groups and see that S-arithmetic groups are a main source to find them. Recall that k is discrete in $\mathbb{A}_k$, the ring of adèles of k, and so is $G(k)$ in $G(\mathbb{A}_k)$, see sections 1.1 and 1.3. Moreover, if G is connected and reductive we have a characterisation of the groups G for which $G(k)$ is a lattice in $G(\mathbb{A}_k)$. Let $X_k(G)$ be the group of k-rational characters of G, i.e., the group of k-homomorphisms from G to $\mathbb{G}_m$. We have the following Theorem.

Theorem 2.2 ([13] for char $k = 0$ and [11] and [28] for char $k \neq 0$). *Let G be a connected reductive k-group. Then $G(k)$ is a lattice in $G(\mathbb{A}_k)$ if and only if $X_k(G) = 1$.*

It is natural to ask whether $G(\mathcal{O}_S)$ gives a lattice in an appropriate subgroup of $G(\mathbb{A}_k)$. Before proceeding we need to understand when the local factor $G(k_v)$ gives a compact group. Recall that for $v \in V_k$ we say that G is k_v-isotropic if $G(k_v)$ contains a nontrivial k_v-split subtorus. Otherwise we say that G is k_v-anisotropic. We write $\mathrm{rank}_{k_v} G$ for the dimension of a maximal k_v-split subtorus of G, hence G is isotropic (anisotropic) if and only if $\mathrm{rank}_{k_v} G \geq 1$ ($= 0$). Put $\mathcal{A} = \mathcal{A}(G) := \{v \in V_k \ : \ G \text{ is } k_v\text{-anisotropic}\}$. The following Theorem, originally showed by Bruhat and Tits, can be found in [71].

Theorem 2.3. *Let G be a reductive k-group. Then $G(k_v)$ is compact if and only if G is k_v-anisotropic.*

For every $S \subseteq V_k$ let us denote by G_S the subgroup in $G(\mathbb{A}_k)$ consisting of the adeles whose v-component is equal to the identity for every $v \in V_k \setminus S$. Note that if S is finite then $G_S = \prod_{v \in S} G(k_v)$. Let us note that the S-integral points $G(\mathcal{O}_S)$ can be written as

$$G(\mathcal{O}_S) = G(k) \cap (G_{S \cup V_\infty} \cdot \prod_{v \in V_f \setminus S} G(\mathcal{O}_v)). \tag{2.1}$$

Let G be a reductive k-group. Note that for $v \in \mathcal{A} \cap V_f$, $G(k_v)$ is a compact group and hence $G(\mathcal{O}_v)$, being an open subgroup, is of finite index. Since $\mathcal{A}$ is finite ([80, Lemma 4.9]), it follows that $G(\mathcal{O}_S)$ is of finite index in $G(\mathcal{O}_{S \cap \mathcal{A}})$.

On the other hand, since $G(k)$ is discrete in $G(\mathbb{A}_k)$ it follows from (2.1) that $G(\mathcal{O}_S)$ is discrete in

$$\prod_{v \in S \cup V_\infty} G(k_v) = \prod_{v \in (S \cup V_\infty) \setminus \mathcal{A}} G(k_v) \times \prod_{v \in (S \cup V_\infty) \cap \mathcal{A}} G(k_v).$$

The second factor is a compact group, hence $G(\mathcal{O}_S)$ (identified with its image under the diagonal embedding into G_S) is discrete in G_S whenever $V_\infty \setminus \mathcal{A} \subseteq S$.

The above remarks together with Theorem 2.2 give

Theorem 2.4. *Let G be a connected reductive k-group and let $V_\infty \setminus \mathcal{A}(G) \subseteq S$. Then $G(\mathcal{O}_S)$ is a lattice in G_S if and only if $X_k(G) = 1$.*

Let us note that for G semisimple, the condition $X_k(G) = 1$ is automatically satisfied. We begin now to investigate the relation between $G(\mathcal{O}_S)$ being infinite, being Zariski-dense in G and having Strong Approximation.

Proposition 2.2.1. *Let G be a connected semisimple k-group and suppose $V_\infty \setminus \mathcal{A}(G) \subseteq S \subseteq V_k$. Let Γ be an S-arithmetic subgroup of the group $G(k)$. Suppose $\sum_{v \in S} \mathrm{rank}_{k_v} G' > 0$ for every k-simple factor G' of G. Then Γ is infinite and Zariski dense in G.*

Proof. Note that it suffices to consider the case G k-simple. Let H be the Zariski closure of Γ and H^0 be the connected component of the identity in H. By Theorem 1.8, H is defined over k and so is H^0 (1.4.2). Note that $g\Gamma g^{-1}$ is commensurable with Γ for every $g \in G(k)$ (2.2.1).v)) and since H^0 is the intersection of all algebraic subgroups of finite

index in H, it follows that $G(k)$ normalizes H^0. Moreover, since $G(k)$ is Zariski dense in G (1.9.i)), H^0 must be a normal subgroup of G.

Now by assumption $\sum_{v \in S} \mathrm{rank}_{k_v} G > 0$ and this implies (recall Theorem 2.3) that $\prod_{v \in S} G(k_v)$ is not compact. Since $G(\mathcal{O}_S)$ is a lattice in the locally compact group G_S (Theorem 2.4), it follows that $G(\mathcal{O}_S)$, Γ and H are all infinite. But then H^0 is an infinite normal k-subgroup of G, which is a k-simple group. Thus, we must have $H^0 = G$, as desired. $\qquad\square$

An algebraic k-group G is said to have **Strong Approximation** with respect to a finite set of valuations $S \subseteq V_f$ if the group $G(k)G_S$ is dense in $G(\mathbb{A}_k)$. Note that this in particular implies that $G(\mathcal{O}_S)$ is dense in $\prod_{v \in V_f \setminus S} G(\mathcal{O}_v) = G(\widehat{\mathcal{O}}_S)$. We will make use of the Strong Approximation Theorem. This was shown by Kneser ([46]) and Platonov ([68]) for char $k = 0$ and by Margulis ([58] and [59]) and Prasad ([70]) for char $k > 0$.

Theorem 2.5 (Strong Approximation). *Let G be a connected simply connected semisimple k-group. Let $S \subset V$ be a finite set of valuations of k. Suppose that $G_S^i = \prod_{v \in S} G^i(k_v)$ is non-compact for every almost k-simple factor G^i. Then $G(k) \cdot G_S$ is dense in $G(\mathbb{A}_k)$.*

As a direct consequence of the previous results we obtain:

Theorem 2.6. *Let G be a connected semisimple k-group and suppose that $V_\infty \setminus \mathcal{A} \subseteq S \subseteq V$. Then $G(\mathcal{O}_S)$ is infinite if and only if G_S is noncompact. Moreover, if G is simply connected and k-simple, then $G(\mathcal{O}_S)$ is infinite if and only if G has Strong Approximation.*

Proof. By Theorem 2.4, $G(\mathcal{O}_S)$ is a lattice in G_S. Since a compact group does not admit an infinite lattice, the direct implication follows. For the converse note that Theorem 2.3 forces one of the almost k-simple factors of G to be noncompact. But then by Proposition 2.2.1 $G(\mathcal{O}_S)$ must be infinite. For G simply connected and k-simple Theorem 2.5 gives that G has Strong Approximation if and only if G_S is noncompact. $\qquad\square$

Finally the following Lemma describes the relations between arithmetic groups under restriction of scalars, see section 1.4.

Lemma 2.2.3 ([59, 3.1.4]). *Let k' be a finite separable field extension of k, let H be a k' group and let $S \subset V_k$. For each $v \in V_k$, we denote by v' the set of valuations of the field k' extending the valuation v . Put $S' = \bigcup_{v \in S} v'$.*

i) For each $v \in V_k$ there exists a natural k_v-isomorphism

$$f_v : \ R_{k'/k}H \to \prod_{w \in v'} R_{k'_w/k_v}H.$$

The isomorphisms $f_v^{-1} \circ R_{k'_w/k_v}^0$, for $v \in V_k$, $w \in v'$ induce a topological group isomorphism of the adele groups associated with H and $R_{k'/k}H$, whose restriction to $H(k')$ agrees with $R_{k'/k}^0$.

ii) The subgroups $R_{k'/k}^0(H(\mathcal{O}_{S'}))$ and $(R_{k'/k}(H))(\mathcal{O}_S)$ are commensurable.

2.3 The general formulation

Let k be a global field, fix S a non-empty set of valuations containing V_∞ and let $\mathcal{O}_S$ be the ring of S-integers. Let G be an algebraic k-group which is assumed to be embedded in GL_N or to have an affine group $\mathcal{O}_S$-scheme structure as in section 2.2. Let us consider the arithmetic group $G(\mathcal{O}_S)$.

Let $\mathfrak{N}_a$ be the family of all normal subgroups of finite index of $G(\mathcal{O}_S)$. One can consider $\mathfrak{N}_a$ as a fundamental system of neighbourhoods of the identity (see Proposition 1.2.2), this induces a topology τ_a on $G(\mathcal{O}_S)$, which is compatible with the group structure, known as the profinite topology.

A rich source of normal subgroups of finite index of $G(\mathcal{O}_S)$ is provided by the arithmetic of the ring $\mathcal{O}_S$. Namely, for every ideal $\mathfrak{q}$ of $\mathcal{O}_S$ we can consider the principal S-congruence subgroup $G(\mathfrak{q})$. If we take the family $\mathfrak{N}_c$ of all principal S-congruence subgroups of Γ as a fundamental system of neighbourhoods for the identity, this defines a topology τ_c on Γ, which is compatible with the group structure, called the S-congruence topology. Note that every S-congruence subgroup has finite index in $G(\mathcal{O}_S)$ (2.2.1.iii)) , so we have $\mathfrak{N}_c \subseteq \mathfrak{N}_a$.

The **Congruence Subgroup Problem** arises from the following question:

<div style="text-align:center">Is every finite index subgroup in Γ an S-congruence subgroup?</div>

Clearly, an affirmative answer is equivalent to $\tau_c = \tau_a$. This equality can be reinterpreted as follows. Observe that $G(\mathcal{O}_S)$ admits completions $\widehat{G(\mathcal{O}_S)}$ and $\overline{G(\mathcal{O}_S)}$ with respect to the (left) uniform structures induced by τ_a and τ_c, see section 1.2.1. By Proposition 1.2.4 we can describe these completions via projective limits as follows:

$$\widehat{G(\mathcal{O}_S)} = \varprojlim_{N \in \mathfrak{N}_a} G(\mathcal{O}_S)/N \quad \text{and} \quad \overline{G(\mathcal{O}_S)} = \varprojlim_{\mathfrak{o} \neq \mathfrak{q}} G(\mathcal{O}_S)/G(\mathfrak{q}).$$

Since τ_a is finer than τ_c we have a surjective (uniformly) continuous homomorphism $\pi : \widehat{G(\mathcal{O}_S)} \twoheadrightarrow \overline{G(\mathcal{O}_S)}$ (Corollary 1.2.1). It follows that $\tau_a = \tau_c$ if and only if the S-congruence kernel

$$C(G, S) := \ker \pi$$

is the trivial group.

Note that the definitions of $G(\mathcal{O}_S)$ and $G(\mathfrak{q})$ depend on the embedding ι. Nevertheless $C(G, S)$ is independent of the chosen embedding. To see this let us reconstruct $C(G, S)$ in terms of the group $G(k)$. We will analogously use two families of subgroups of $G(k)$.

We say that a subgroup $\Gamma \subset G(k)$ is an S-congruence subgroup if $G(\mathfrak{q}) \subseteq \Gamma$ for some $\mathfrak{q} \neq 0$. The family $\widetilde{\mathfrak{N}}_c$ of all S-congruence subgroups of $G(k)$ serves as a fundamental system of neighbourhoods of the identity and defines a topology $\widetilde{\tau}_c$ on $G(k)$. Indeed, $\widetilde{\mathfrak{N}}_c$ clearly satisfies (GB1) and (GB2) in 1.2.2 and (GB3) follows from Lemma 2.2.1.i) and the fact that conjugation by an element $g \in G(k)$ is a k-automorphism of G. Clearly $\mathfrak{N}_c \subset \widetilde{\mathfrak{N}}_c$, hence $G(\mathcal{O}_S)$ with the topology $\widetilde{\tau}_c$ is a on open subgroup of $G(k)$.

A subgroup $\Gamma \subset G(k)$ is an S-arithmetic[4] subgroup if Γ and $G(\mathcal{O}_S)$ are commensurable. The family $\widetilde{\mathfrak{N}}_a$ of all S-arithmetic subgroups of $G(k)$ serves as a fundamental system of

---

[4]In general a subgroup $H \leq G(\overline{k})$ is called S-arithmetic if H and $G(\mathcal{O}_S)$ are commensurable.

neighbourhoods of the identity and defines a topology $\widetilde{\tau}_a$ on $G(k)$. Indeed, $\widetilde{\mathfrak{N}}_c$ clearly satisfies (GB1) and (GB2), while (GB3) follows from Lemma 2.2.1.v). Clearly $\mathfrak{N}_a \subset \widetilde{\mathfrak{N}}_a$, hence $G(\mathcal{O}_S)$ with the topology $\widetilde{\tau}_a$ is an open subgroup of $G(k)$.

It follows from i) and iv) in Lemma 2.2.1 that the definition of the above topologies on $G(k)$ does not depend on the embedding ι. As above, $\widetilde{\tau}_a$ and $\widetilde{\tau}_c$ induce two uniform structures in $G(k)$ and these give respective completions which will be denoted respectively by $\widehat{G(k)}$ and $\overline{G(k)}$. Since $\widetilde{\tau}_a$ is finer than $\widetilde{\tau}_c$ the identity map in $G(k)$ induces a continuous surjective homomorphism

$$\widetilde{\pi} : \widehat{G(k)} \to \overline{G(k)}.$$

Moreover, note that $\widehat{G(\mathcal{O}_S)}$, respectively $\overline{G(\mathcal{O}_S)}$, is naturally isomorphic to the closure of $G(\mathcal{O}_S)$ with respect to $\widetilde{\tau}_a$, respectively $\widetilde{\tau}_c$, as a subgroup of $\widehat{G(k)}$, respectively $\overline{G(k)}$– since $\bigcap_{N \in \mathfrak{N}_c} = 1$ the group $G(k)$, and in particular $G(\mathcal{O}_S)$, embedds both in $\widehat{G(k)}$ and $\overline{G(k)}$.

Remark. Note that by construction $\overline{G(k)}$ is nothing but the closure of $G(k)$ in the topological group $G(\mathbb{A}_S)$, see section 1.3.

Lemma 2.3.1. *Let $\widetilde{\pi}$ and π be as above. Then $\ker \widetilde{\pi} \cong \ker \pi$. In particular, $C(G, S)$ is independent of the embedding $\iota : G \hookrightarrow \mathrm{GL}_N$.*

Proof. Suppose $x \in \widehat{G(k)}$ is a minimal Cauchy filter on $G(k)$ converging to 1 with respect to $\widetilde{\tau}_c$. This implies that $\widetilde{\mathfrak{N}}_c$ and, in particular, all principal congruence subgroups and $G(\mathcal{O}_S)$ belong to x. Hence, if we look at $x \cap G(\mathcal{O}_S) := \{F \cap G(\mathcal{O}_S) \; : \; F \in x\}$ this gives a filter on $G(\mathcal{O}_S)$ which is Cauchy with respect to (the uniform structure given by) τ_c and converges to 1 in τ_c. It follows that $x \cap G(\mathcal{O}_S)$ gives rise to a point in $\widehat{G(\mathcal{O}_S)}$, which is isomorphic to the closure of $G(\mathcal{O}_S)$ in $\widehat{G(k)}$. This implies that $x \in \widehat{G(\mathcal{O}_S)}$ and so $x \in C(G, S)$. $\square$

Let us note that the proof of the previous Lemma actually shows the following.

Lemma 2.3.2. *Let $\Gamma \le G(k)$ be a subgroup, and denote by $\widehat{\Gamma}$ and $\overline{\Gamma}$ the closure of Γ in $\widehat{G(k)}$ and $\overline{G(k)}$. We have a natural map $\widehat{\Gamma} \to \overline{\Gamma}$. Suppose that Γ is open both in $\widetilde{\tau}_a$ and $\widetilde{\tau}_c$. Then $\ker \widetilde{\pi} \cong C(G, S) \cong \ker(\widehat{\Gamma} \to \overline{\Gamma})$.*

The Congruence Subgroup Problem therefore reduces to the study of the group

$$C(G, S) = \ker \left(\widehat{G(\mathcal{O}_S)} \to \overline{G(\mathcal{O}_S)} \right).$$

Whenever $C(G, S)$ is trivial we say that $G(\mathcal{O}_S)$ has the **Congruence Subgroup Property (CSP)**. If $C(G, S)$ is finite, we say that $G(\mathcal{O}_S)$ has the **weak Congruence Subgroup Property (wCSP)**. Even the finiteness of $C(G, S)$ has some interesting consequences, see Theorem 3.3 and 4.1.

2.4 Reductions and necessary conditions

We begin by describing the behaviour of $C(G, S)$ for different G.

Proposition 2.4.1. *The assignment $G \mapsto C(G, S)$ gives a functor $C(\_, S)$ from the category of affine k-groups to the category of profinite groups.*

Proof. It follows from Lemma 2.3.1 that $C(G, S) = \ker \pi$ is a closed subgroup of $\widehat{G(\mathcal{O}_S)}$, hence a profinite group. Let $f : G \to H$ be a k-morphism of k-groups. Note that $f_{|G(k)} : G(k) \to H(k)$ is continuous with respect to both the congruence and arithmetic topologies (2.2.1.ii) and 2.2.2.i)) and so it extends to a continuous function between the respective completions. Given $x \in \widehat{G(k)}$ a minimal Cauchy filter, since $f_{|G(k)}$ is continuous, $f(x) := \{f(F) \; : \; F \in x\}$ gives a Cauchy filter basis on $H(k)$. Thus we define $C(\_, S) : \widehat{G(k)} \to \widehat{H(k)}$ by assigning to every element $x \in \widehat{G(k)}$ the minimal Cauchy filter containing $f(x)$. Let us check that under this map $C(G, S)$ maps to $C(H, S)$. If $H(\mathfrak{p})$ is a principal S-congruence subgroup in $H(k)$. Then by Lemma 2.2.1.iv) there exists an ideal $\mathfrak{q} \subset \mathcal{O}_S$ such that $f(G(\mathfrak{q})) \subseteq H(\mathcal{O}_S)$. Now if $x \in C(G, S)$ then x converges to 1 in $\tilde{\tau}_c$ and this implies $G(\mathfrak{q}) \in x$. Hence $f(G(\mathfrak{q})) \in f(x)$ and thus any filter contaning $f(x)$ contains $H(\mathfrak{p})$. It follows that $C(\_, S)(f)(C(G, S)) \subseteq C(H, S)$ as desired. $\qquad\square$

Lemma 2.4.1. *If G^0 is the connected component of the identity in G, the inclusion map $i : G^0 \to G$ induces an isomorphism $C(G^0, S) \to C(G, S)$.*

Proof. First let us note that G^0 is a normal k-subgroup of G of finite index (Proposition 1.4.2). Hence we may keep the chosen embedding for G^0 as well and we have $G^0(\mathcal{O}_S) = G(\mathcal{O}_S) \cap G(k)$ and $G^0(\mathfrak{q}) = G(\mathfrak{q}) \cap G^0(k)$ for every ideal $\mathfrak{q} \subseteq \mathcal{O}_S$. Moreover the quotient $G(k)/G^0(k)$ is a finite group, hence $G^0(\mathcal{O}_S)$ has finite index in $G(\mathcal{O}_S)$. This implies that $G^0(\mathcal{O}_S)$ and $G^0(k)$ are open subgroups of $G(k)$ with respect to the arithmetic topology of $G(k)$. By Lemma 2.3.2 it suffices to show that $G^0(k)$ is also open with respect to the congruence topology in $G(k)$, i.e., there exists an ideal $\mathfrak{q} \subseteq \mathcal{O}_S$ such that $G(\mathfrak{q}) \subseteq G^0(k)$.

To prove the claim let us denote by G^0, G^1, ..., G^n the connected components of the algebraic k-group G. The identity component G^0 is defined over k (Proposition 1.4.2) and this implies that $G' := \cup_{i=1}^n G^i$ is defined over k as well[5]. It follows that we have a decomposition $k[G] = k[G^0] \oplus k[G']$ as a direct sum of algebras. Now this implies that $1 = e_0 + e$ for some $e_0 \in k[G^0]$ and $e \in k[G']$.

It follows that $e(g) = 1$, for $g \in G'(k)$, and $e(g) = 0$ for $g \in G^0(k)$. Now we know that $k[G] = k[x_{ij}, \det(x_{ij})^{-1} \, | \, 1 \le i, j \le n]$, where $x_i(1) = 0$ for every $i \in I$. Then $e = f(x_i)$ for some polynomial $f \in k[X_i]$. Pick an ideal $\mathfrak{q} \subseteq \mathcal{O}_S$ such that $c \notin \mathfrak{q}$ for every coefficient $c \in k$ of f. We claim that $G(\mathfrak{q}) \cap G'(k) = \emptyset$ and hence $G(\mathfrak{q}) \subseteq G^0(k)$. Indeed, since $e(1) = 0$, we must have $e(g) = 0 \mod \mathfrak{q}$ for $g \in G(\mathfrak{q})$, but $e(g) = 1$ for every $g \in G'(k)$. Hence we must have $G(\mathfrak{q}) \cap G'(k) = \emptyset$. $\qquad\square$

The following Lemma describes the behaviour of $C(G, S)$ when G is a semidirect product of k-groups.

---

[5]In an algebraic group the connected and irreducible components coincide and are disjoint. The irreducible components are defined over the separable closure k_s and a component is defined over k if and only it is stable under the action of $\mathrm{Gal}(k_s/k)$, which permutes the irreducible components. Now since G^0 is defined over k this implies that $G \setminus G^0$ is stable under $\mathrm{Gal}(k_s/k)$ and hence defined over k, see [12, Proposition I.1.2] and references therein for details.

Lemma 2.4.2 ([73])**.** *Let G be an algebraic k-group, such that G is the semidirect product of a normal k-subgroup N and a k-subgroup H. Then $C(G, S)$ is a semidirect product of $C(H, S)$ and a quotient of $C(N, S)$. In particular, if $C(N, S)$ is trivial then $C(G, S) \cong C(H, S)$.*

2.5 The characteristic 0 case

Throughout this section we assume that char $k = 0$, that is, k is a number field. The aim of this section is to reduce the Congruence Subgroup Problem to the case of semisimple algebraic groups. By Lemma 2.4.1 we may restrict to connected groups. We begin by investigating the additive and multiplicative groups $\mathbb{G}_a$ and $\mathbb{G}_m$.

Lemma 2.5.1. *Let $G = \mathbb{G}_a$, then for any $S \subseteq V_f$ we have $C(G, S) = 1$.*

Proof. Suppose $H \leq \mathcal{O}_S$ has index m. Then $m\mathcal{O}_S \leq H$. $\qquad\square$

To show that the congruence kernel for the multiplicative group is also trivial we will apply the following Theorem by Chevalley ([18, Theorem 1]).

Theorem 2.7. *Suppose $H \leq k^*$ is a finitely generated subgroup. Then, given $m \in \mathbb{N}$ and any non-zero ideal $\mathfrak{p} \subset \mathcal{O}$, there exists a non-zero ideal $\mathfrak{q} \subset \mathcal{O}$ coprime to $\mathfrak{p}$ such that for every $x \in H$ such that $x \equiv 1 \mod \mathfrak{q}$, we have $x \in H^m$. The statement $x \equiv 1 \mod \mathfrak{q}$ is to be interpreted in k, that is, $x - 1 \in \frac{a}{b}\mathfrak{q}$ where $a, b \in \mathcal{O}$ and (b) is coprime to $\mathfrak{q}$.*

Lemma 2.5.2. *Let $G = \mathbb{G}_m$. Then for any finite $S \subseteq V_f$ we have $C(G, S) = 1$.*

Proof. Let $N \leq \mathcal{O}_S^*$ be a subgroup of index m. Then we have $(\mathcal{O}_S^*)^m \leq N$. It is well known that $\mathcal{O}_S^*$ is a finitely generated group. Hence we can apply Theorem 2.7 to $H = \mathcal{O}_S^*$ and $\mathfrak{p} = \prod_{v \in S} \mathfrak{p}_v$ to obtain an ideal $\mathfrak{q}$ coprime to $\mathfrak{p}$ such that for every $x \in \mathcal{O}_S^*$ such that $x \equiv 1 \mod \mathfrak{q}$ we have $x \in (\mathcal{O}_S^*)^m$. Consider $\mathfrak{q}^S := \mathfrak{q}\mathcal{O}_S$. Now observe that $\mathfrak{q}^S$ is an ideal in $\mathcal{O}_S$ ($\mathfrak{q}$ is coprime to $\mathfrak{p}$) and that $G(\mathfrak{q}^S) \subseteq \{x \in \mathcal{O}^* : x \equiv 1 \mod \mathfrak{q}\} \leq (\mathcal{O}_S^*)^m \leq N$, i.e., N is an S-congruence subgroup.

$\qquad\square$

Lemma 2.5.3. *Let G be a connected unipotent k-group. Then for any $S \subseteq V_f$ we have $C(S, G) = 1$.*

Proof. We may suppose that G is an algebraic k-subgroup of U_n [89, Theorem 8.3]. One can construct a central normal series of algebraic k-groups

$$\mathrm{U}_n = U_0 \supset U_1 \supset \ldots \supset U_{\frac{n(n-1)}{2}} = 1$$

such that $U_i / U_{i+1} \cong \mathbb{G}_a$ for every $i < \frac{n(n-1)}{2}$. This gives a central normal series

$$G = G_0 \supset G_1 \supset \ldots \supset G_d = 1$$

such that each quotient G_i / G_{i+1} is a isomorphic to $\mathbb{G}_a$ (note that $\mathbb{G}_a$ has no algebraic subgroups) and $d = \dim G$. We apply induction on d. For $d = 1$ this is Lemma 2.5.1.

Suppose the result holds for $d = r - 1$, in particular $C(G_1, S) = 1$. Then G is of the form $\mathbb{G}_a \ltimes G'$ where G' is a unipotent k-group of dimension $d - 1$. By induction and Lemma 2.5.1 we can apply Lemma 2.4.2 to obtain $C(G, S) = 0$. $\qquad\square$

Let us now consider the case of a connected k-group G. By Theorem 1.10, G is the semidirect product of a semisimple k-subgroup and its unipotent radical. Hence, the previous Lemma together with Lemma 2.4.2 shows that for number fields the study of $C(G, S)$ reduces to the case G reductive. The following Lemma shows that we can futher reduce it to the case of a semisimple group.

Lemma 2.5.4 ([72, 2.4]). *Let G be a connected reductive k-group. Then*

$$C(G, S) \cong C([G, G], S).$$

2.6 The semisimple case

Throughout this section we assume that G is a connected semisimple k-group. Note that by Lemma 2.4.1, the assumption G connected is harmless regarding CSP. By Theorem 1.12, G is the almost direct product of its almost k-simple factors $G_1, \ldots, G_m$. We will further assume that $G_i(\mathcal{O}_S)$ is infinite, equivalently $(G_i)_S$ is non-compact (Theorem 2.6), for every $1 \le i \le m$. Let us note that otherwise $C(G_i, S) = 1$. The aim of this section is to reduce, when char $k = 0$, the Congruence Subgroup Problem for semisimple k-groups to the following setting:

(A1) G is simply connected.

(A2) G is almost k-simple.

(A3) G has the Strong Approximation Property.

(A4) G is absolutely almost simple.

(A5) For every $v \in S \cap V_f$ the group $G(k_v)$ is noncompact, equivalently (Theorem 2.3), for every $v \in S \cap V_f$ the group G is k_v-isotropic.

Lemma 2.6.1. *Let G be as above and suppose* char $k = 0$. *Suppose further that $C(S, G)$ is finite. Then G is simply connected.*

Proof. By Theorem 1.12.ii), G is the almost direct product of its almost k-simple factors $G_1, \ldots, G_r$. By Theorem 1.11, there exists a connected simply connected semisimple k-group $\widetilde{G}$ which decomposes as a direct product of its almost k-simple factors $\widetilde{G}_1, \ldots, \widetilde{G}_k$ and a central k-isogeny $p : \widetilde{G} \to G$ with finite kernel μ such that $p(\widetilde{G}_i) = G_i$. Note that $\mathrm{rank}_{k_v} \widetilde{G}_i = \mathrm{rank}_{k_v} G_i$ and so $(\widetilde{G}_i)_S$ is not compact. Hence, by Theorem 2.5 $\widetilde{G}$ has Strong Approximation, that is, $\overline{\widetilde{G}(k)} = \widetilde{G}(\mathbb{A}_S)$. Applying the functor $C(\_, S)$ we obtain the

following commutative diagram.

$$
\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & C(\mu, S) & \longrightarrow & \widehat{\mu(k)} & \xrightarrow{\ \pi_\mu\ } & \mu(\mathbb{A}_S) & & \\
 & & \downarrow{\scriptstyle C(\iota)} & & \downarrow{\scriptstyle \widehat{\iota(k)}} & & \downarrow{\scriptstyle \iota(\mathbb{A}_S)} & & \\
1 & \longrightarrow & C(\widetilde{G}, S) & \longrightarrow & \widehat{\widetilde{G}(k)} & \xrightarrow{\ \pi_{\widetilde{G}}\ } & \widetilde{G}(\mathbb{A}_S) & & \\
 & & \downarrow{\scriptstyle C(p)} & & \downarrow{\scriptstyle \widehat{p(k)}} & & \downarrow{\scriptstyle p(\mathbb{A}_S)} & & \\
1 & \longrightarrow & C(G, S) & \longrightarrow & \widehat{G(k)} & \xrightarrow{\ \pi_G\ } & G(\mathbb{A}_S) & &
\end{array}
$$

Note that by Theorem 2.1 the map $\widehat{p(k)}$ is open and has finite kernel $\widehat{\mu(k)} = \mu(k)$. Hence the horizontal and vertical sequences starting at $1's$ are exact and since $\widetilde{G}$ has Strong Approximation the map $\pi_{\widetilde{G}}$ is surjective. It follows that $C(G, S)$ contains a subgroup isomorphic to $\pi_{\widetilde{G}}^{-1}(\mu(\mathbb{A}_S))/\widehat{\mu(k)}$. Now observe that $\mu(\mathbb{A}_S) \subset \widetilde{G}(\mathbb{A}_S)$ is an infinite group. Indeed by Lemma 1.1.2 if $x \in \mu$ then $x \in \mu(k_v)$ for infinitely many v's. Since μ is nontrivial, this implies that $\mu(\mathbb{A}_S)$ is infinite. Hence $C(G, S)$ contains an infinite subgroup, a contradiction. Therefore G must be simply connected. $\qquad\square$

We can therefore assume from now on that G is a simply connected semisimple group. But then G is the direct product of its almost k-simple factors (see Theorem 1.12). It is then clear that $C(G, S)$ is finite if and only if $C(G_i, S)$ is finite for every k-simple factor G_i. Hence we may assume (A2).

Now G is a connected simply connected almost k-simple group and since we are assuming that $G(\mathcal{O}_S)$ is infinite, Theorem 2.6 gives G_S is non compact, so by the Strong Approximation Theorem G has Strong Approximation, i.e., we may assume (A3). The following Lemma shows that we may assume (A4).

Lemma 2.6.2. *Let G be a connected simply connected almost k-simple k-group. Then there exists a finite separable extension k' of k and a connected simply connected absolutely almost simple k'-group H such that $G = R_{k'/k}(H)$ and $C(G, S) \cong C(H, S')$ where $S' = \cup_{v \in S}\{v' \in V_{k'} \ : \ v'_{|k} = v\}$.*

Proof. By Theorem 1.13 there exist a finite separable extension k' and a connected simply connected absolutely almost simple k'-group H such that $G = R_{k'/k}H$. Now Lemma 2.2.3.ii) shows that $G(\mathcal{O}_S)$ and $R_{k'/k}^0(H(\mathcal{O}_{S'}))$ are commensurable and this implies that the restriction of the respective S-arithemtic topologies to $G(\mathcal{O}_S) \cap R_{k'/k}^0(H(\mathcal{O}_{S'}))$ induce the same topology. Moreover by 2.2.3.i) the respective congruence topologies define the same topology when restricted to the intersection as well. Hence by Lemma 2.3.2 we have $C(G, S) \cong C(H, S')$. $\qquad\square$

Finally we show that (A5) is necessary for G to have CSP.

Lemma 2.6.3. *Let G be a semisimple k-group and assume that $G(\mathcal{O}_S)$ is infinite. Put $\mathcal{A} := \{v \in V_f \ : \ G \text{ is } k_v\text{-anisotropic}\}$. If $\mathcal{A} \cap S$ is non-empty, then $C(G, S)$ is infinite.*

Proof. By Theorem 2.3 $G(k_v)$ is compact for every $v \in \mathcal{A}$. In particular $G(\mathfrak{m}_v^i) \subseteq G(k_v)$ gives a descending sequence of finite index open subgroups with trivial intersection. Note that for $v \in S$ we have $G(\mathcal{O}_S) \subseteq G(k_v)$. Hence, for $v \in \mathcal{A} \cap S$, $G(\mathcal{O}_S) \cap G(\mathfrak{m}_v^i)$ gives a descending sequence of finite index subgroups of $G(\mathcal{O}_S)$ with trivial intersection. Since $v \in S$, none of them are S-congruence subgroups so we can build a surjection

$$C(G, S) \twoheadrightarrow \varprojlim_i G(\mathcal{O}_S)/(G(\mathcal{O}_S) \cap G(\mathfrak{m}_v^i)).$$

Since the latter inverse limit contains $G(\mathcal{O}_S)$ as a subgroup it follows that $C(G, S)$ is infinite. $\qquad\square$

Let us finish this chapter by stating famous Serre's Conjecture.

Conjecture (Serre). Let G be a simply connnected absolutely almost simple k-group. Then $C(G, S)$ is finite if and only if $\text{rank}_S G = \sum_{v \in S} \text{rank}_{k_v} G \geq 2$ and $G(k_v)$ is noncompact for every $v \in S \cap V_f$.

Chapter 3

Representation Growth of Arithmetic Groups

3.1 Representation Growth

In this section we introduce the necessary notation for the study of representation growth and present some well known results on representation theory. We then focus on the representation growth of p-adic analytic and $\mathbb{F}_p[[t]]$-analytic groups. Theorem 3.1 shows that every compact p-adic analytic group with perfect Lie algebra is of representation type c for some c, this was shown by Lubotzky and Martin in [56]. Jaikin showed in [38] that the same result holds for $\mathbb{F}_p[[t]]$-standard groups under the weaker condition (in chase char $k > 0$) of having a finitely generated Lie algebra (see Theorem 3.2). We present both results for completion. Jaikin's avoidance of a perfectness hypothesis in Theorem 3.2 paves the way to extend Theorem 1.2 in [56] to any semisimple group over a global field. We refer to 1.6 for notations and definitions concerning representation theory.

Let Γ be a group. We want to study the representations of the group Γ, in particular, in this work we are interested in representations with finite image. From now on $\mathrm{Rep}(\Gamma)$ (respectively $\mathrm{Irr}(\Gamma)$) denotes the set of isomorphism classes of (irreducible) representations of Γ with finite image. Evidently this is no restriction if Γ is a finite group. The following Lemma shows that for profinite groups this is no restriction either.

Lemma 3.1.1. *Let Γ be a profinite group. Then every representation of Γ factors through a finite index open subgroup. Hence, every representation of Γ has finite image. In particular, if $\widehat{\Gamma}$ is the profinite completion of Γ we have $r_n(\Gamma) = r_n(\widehat{\Gamma})$.*

Proof. Let $\rho \in \mathrm{Rep}_n(\Gamma)$. Recall that ρ is a continuous homomorphism $\rho : \Gamma \to \mathrm{GL}_n(\mathbb{C})$, in particular, $\ker \rho$ is a closed subgroup of Γ and since Γ is compact, so is $\rho(\Gamma)$. This implies that $\rho(\Gamma)$ is a compact Lie group isomorphic to the profinite group $\Gamma/\ker \rho$, which is a totally disconnected group (Theorem 1.5). It follows that the identity component of $\rho(\Gamma)$ must be trivial. Hence $\rho(\Gamma)$ must be finite, since it is compact. This implies that $\{1\}$ is open in $\rho(\Gamma)$ and hence $\ker \rho \leq \Gamma$ is a finite index open subgroup. $\qquad\square$

The previous Lemma shows that most results of the representation theory of finite

groups apply to the representation theory of profinite groups as well. If Γ is finite, then $\mathrm{Irr}(\Gamma)$ is finite as well, however for infinite Γ we may have $\mathrm{Irr}_n(\Gamma) \neq \emptyset$ for infinitely many n. Let us define

$$r_n(\Gamma) = |\mathrm{Irr}_n(\Gamma)|,$$

$$R_n(\Gamma) = \sum_{i=1}^{n} r_n(\Gamma) = |\mathrm{Irr}_{\leq n}(\Gamma)|.$$

We call $r_n(\Gamma)$ the **representation growth function** of Γ. Note that, in general, $r_n(\Gamma)$ may be infinite, e.g., $\Gamma = \mathbb{Z}$.

We say that Γ has **polynomial representation growth** (PRG for short) if the sequence $r_n(\Gamma)$ is polynomially bounded, that is, if there exist constants $c_1, c_2 \in \mathbb{R}$ such that $r_n(\Gamma) \leq c_1 n^{c_2}$ for every n. In particular, this requires $r_n(\Gamma) < \infty$ for every n. Note that $r_n(\Gamma)$ is polynomially bounded if and only if $R_n(\Gamma)$ is.

We say that Γ is of **representation type c** if there exist $c \in \mathbb{R}$ such that $|\Gamma/K_n(\Gamma)| \leq cn^c$ for every n, where

$$K_n(\Gamma) := \bigcap_{\rho \in \mathrm{Rep}_{\leq n}(\Gamma)} \ker \rho = \bigcap_{\rho \in \mathrm{Irr}_{\leq n}(\Gamma)} \ker \rho.$$

Lemma 3.1.2. *Suppose Γ is of representation type c, then Γ has PRG.*

Proof. Note that every $\rho \in \mathrm{Irr}_{\leq n}(\Gamma)$ factors through $K_n(\Gamma)$, hence it can be seen as a representation of $\Gamma/K_n(\Gamma)$. If Γ is of representation type c, we can see $\rho \in \mathrm{Irr}_{\leq n}(\Gamma)$ as a representation of the finite group $\Gamma/K_n(\Gamma)$ which is of order at most cn^c. It follows that $|\mathrm{Irr}_{\leq n}(\Gamma)| \leq cn^c$, hence Γ has PRG. $\qquad\square$

Lemma 3.1.3. *Let Γ be a profinite group and $\Gamma' \leq \Gamma$ a finite index subgroup. Put $m = |\Gamma : \Gamma'|$. Then for every $n \in \mathbb{N}$ we have*

i) $R_n(\Gamma) \leq mR_n(\Gamma')$.

ii) $R_n(\Gamma') \leq mR_{nm}(\Gamma)$.

As a consequence, if Γ and Γ' are commensurable then Γ has PRG if and only if Γ' has PRG.

Proof. Let $\rho \in \mathrm{Irr}_{\leq n}(\Gamma)$ and consider $\rho' \in \mathrm{Irr}_{\leq n}(\Gamma')$ an irreducible constituent of $\rho_{|\Gamma'}$. Note that $N := \ker \rho \cap \Gamma'$ has finite index in Γ, so we may assume that we are working with representations of the finite groups Γ/N and Γ'/N. Hence by Frobenius reciprocity we know that ρ is an irreducible constituent of $\mathrm{Ind}_{\Gamma'}^{\Gamma} \rho'$. Moreover note that the number of irreducible constituents of $\mathrm{Ind}_{\Gamma'}^{\Gamma} \rho'$ is at most m (each of them has ρ' as a constituent when restricted to Γ' by Frobenius reciprocity and $\dim \mathrm{Ind}_{\Gamma'}^{\Gamma} \rho' = m \dim \rho'$). Hence we have a map $f : \mathrm{Irr}_{\leq n}(\Gamma) \to \mathrm{Irr}_{\leq n}(\Gamma')$ whose fibers have size at most m. This proves i).

Now consider $\rho' \in \mathrm{Irr}_{\leq n}(\Gamma')$ and let $\rho \in \mathrm{Irr}(\Gamma)$ be an irreducible constituent of $\mathrm{Ind}_{\Gamma'}^{\Gamma} \rho'$. Clearly ρ has dimension at most nm. Moreover for every such ρ, $\rho_{|\Gamma'}$ can have at most m

irreducible constituents (if k is the number of irreducible constituents of $\rho_{|\Gamma'}$ and λ is one of minimal dimension, say δ, then $k\delta \leq \dim \rho \leq m \dim \lambda$, where the last inequality follows from the fact that ρ is a constituent of $\mathrm{Ind}_{\Gamma'}^{\Gamma} \lambda$ by Frobenius reciprocity). Hence we have a map $f : \mathrm{Irr}_{\leq n}(\Gamma') \to \mathrm{Irr}_{\leq nm}(\Gamma)$ whose fibers have size at most m, which proves ii). $\qquad\square$

Lemma 3.1.4. *Let Γ be a profinite group and $\Gamma' \leq \Gamma$ a finite index open subgroup such that $|\Gamma : \Gamma'| = m$. Then Γ is of representation type c for some $c \in \mathbb{R}_{\geq 0}$ if and only if Γ' is of representation type c' for some $c' \in \mathbb{R}_{\geq 0}$. As a consequence, if Γ and Γ' are commensurable and any of them is of representation type c, there exists d such that Γ, Γ' and $\Gamma \cap \Gamma'$ are of representation type d.*

Proof. First let us suppose that Γ' is representation type c'. Given $\rho \in \mathrm{Irr}_{\leq n}(\Gamma)$, we have $\rho_{|\Gamma'} = \lambda_1 \oplus \ldots \oplus \lambda_r$ for some $\lambda_i \in \mathrm{Irr}_{\leq n}(\Gamma')$. By definition, $K_n(\Gamma') \leq \ker \rho_{|\Gamma'}$ and since $K_n(\Gamma')$ is a characteristic subgroup of Γ' we obtain

$$K_n(\Gamma') \subseteq \bigcap_{g \in \Gamma} (\ker \rho_{|\Gamma'})^g = \ker \mathrm{Ind}_{\Gamma'}^{\Gamma} \left(\rho_{|\Gamma'} \right) \subseteq \ker \rho.$$

It follows that $K_n(\Gamma') \subseteq K_n(\Gamma)$ and so

$$|\Gamma/K_n(\Gamma)| \leq |\Gamma : K_n(\Gamma')| = |\Gamma : \Gamma'||\Gamma' : K_n(\Gamma')| \leq mc'n^{c'} \leq cn^c$$

for some $c \in \mathbb{R}_{\geq 0}$ as required.

Suppose now that Γ is of representation type c. If $\rho' \in \mathrm{Irr}_{\leq n}(\Gamma')$ then $\mathrm{Ind}_{\Gamma'}^{\Gamma} \rho' \in \mathrm{Rep}_{nm}(\Gamma)$. Hence $K_{nm}(\Gamma) \subseteq \ker \mathrm{Ind}_{\Gamma'}^{\Gamma} \rho'$. By Frobenius reciprocity ρ' is a constituent of $\left(\mathrm{Ind}_{\Gamma'}^{\Gamma} \rho' \right)_{|\Gamma'}$, hence $K_{nm}(\Gamma) \cap \Gamma' \subseteq \ker \rho'$. We thus have $K_{nm}(G) \cap \Gamma' \subseteq K_n(\Gamma')$. This gives

$$|\Gamma'/K_n(\Gamma')| \leq |\Gamma'/(K_{nm}(\Gamma) \cap \Gamma')| \leq |\Gamma/K_{nm}(\Gamma)| \leq c(nm)^c \leq c'n^{c'}$$

for some $c' \in \mathbb{R}_{\geq 0}$ as desired.

$\qquad\square$

Lemma 3.1.5. *Let Γ be a pro-nilpotent group. Then for every $\rho \in \mathrm{Irr}(\Gamma)$ there exists $\Gamma' \leq \Gamma$ with $|\Gamma : \Gamma'| = \dim \rho$ and $\rho' \in \mathrm{Irr}(\Gamma')$ such that $\rho = \mathrm{Ind}_{\Gamma'}^{\Gamma} \rho'$.*

Proof. If $\rho \in \mathrm{Irr}(\Gamma)$ then by Lemma 3.1.1, ρ factors through a finite index open subgroup N. Then we can regard ρ as a representation of the finite nilpotent group Γ/N. For a finite nilpotent group every irreducible representation is induced from a linear representation of a subgroup (see [33, Corollary 6.14]. Suppose $\rho \cong \mathrm{Ind}_{\Gamma'N/N}^{\Gamma/N} \lambda$ for some subgroup $\Gamma'N/N$ and representation $\lambda \in \mathrm{Irr}_1(\Gamma'N/N)$. Then the result follows if we regard λ as a representation of $\Gamma'N$. $\qquad\square$

Lemma 3.1.6. *Let Γ be a profinite group and $N \trianglelefteq_o \Gamma$ an open normal subgroup. Then Γ acts on $\mathrm{Irr}(N)$ by conjugation and if $H \leq \Gamma$ is the stabilizer of $\lambda \in \mathrm{Irr}(N)$ the map*

$$\mathrm{Ind} : \begin{array}{ccc} \{\psi \in \mathrm{Irr}(H) \; : \; \langle \psi_{|N}, \lambda \rangle \neq 0\} & \to & \{\rho \in \mathrm{Irr}(\Gamma) \; : \; \langle \rho_{|N}, \lambda \rangle \neq 0\} \\ \psi & \mapsto & \mathrm{Ind}_N^{\Gamma} \psi \end{array}$$

is a bijection.

Proof. This is nothing but to extend Theorem 1.18 to profinite groups. If $\rho \in \mathrm{Irr}(\Gamma)$, by Lemma 3.1.1 ρ factors through some finite index open subgroup M. Moreover we may assume that $M \leq N$, otherwise take $M \cap N$. Suppose λ is an irreducible constituent of $\rho_{|N}$, i.e., $\langle \lambda, \rho_{|N} \rangle \neq 0$. If we regard ρ as a representation of Γ/M and $\lambda \in \mathrm{Irr}(N)$ as a representation of N/M we can apply Theorem 1.18 to obtain a bijection

$$\{\psi \in \mathrm{Irr}(H/M) \,:\, \langle \psi_{|N/M}, \lambda \rangle \neq 0\} \;\to\; \{\rho \in \mathrm{Irr}(\Gamma/M) \,:\, \langle \rho_{|N/M}, \lambda \rangle \neq 0\}$$
$$\psi \qquad\qquad\qquad \mapsto \qquad\qquad \mathrm{Ind}_{H/M}^{\Gamma/M} \psi$$

Hence, regarding $\psi \in \mathrm{Irr}(H/M)$ as a representation of H, we obtain the desired bijection if $\lambda \in \mathrm{Irr}(N)$ factors through M. Since every $\lambda \in \mathrm{Irr}(N)$ factors through some such M the result follows. $\qquad\square$

Lemma 3.1.7. *Suppose Γ_1 and Γ_2 are profinite groups. Then every irreducible representation of $\Gamma_1 \times \Gamma_2$ is of the form $\rho_1 \otimes \rho_2$, where ρ_i is an irreducible representation of Γ_i. In particular, if Γ_1 and Γ_2 have PRG then $\Gamma_1 \times \Gamma_2$ has PRG.*

Proof. The result is true if we assume the groups Γ_1 and Γ_2 are finite. Using again Lemma 3.1.1 we see that every $\rho \in \mathrm{Irr}(\Gamma_1 \times \Gamma_2)$ factors through a finite index open subgroup N. It follows that $(\Gamma_1 \times \Gamma_2)/N$ is isomorphic to $\Gamma_1/(N \cap \Gamma_1) \times \Gamma_2/(N \cap \Gamma_2)$, which is a finite group. If we regard ρ as a representation of this finite group, we have $\rho \cong \lambda_1 \otimes \lambda_2$ for some $\lambda_i \in \mathrm{Irr}(\Gamma_i/N \cap \Gamma_i)$. If we regard λ_1 and λ_2 as representations of Γ_1 and Γ_2 we obtain the desired decomposition.

Now if $\rho_1 \in \mathrm{Irr}_m(\Gamma_1)$ and $\rho_2 \in \mathrm{Irr}_k(\Gamma_2)$ we have by construction $\rho_1 \otimes \rho_2 \in \mathrm{Irr}_{mk}(\Gamma_1 \times \Gamma_2)$. Hence, if $R_n(\Gamma_1) \leq c_1 n^{c_1}$ and $R_n(\Gamma_2) \leq c_2 n^{c_2}$, we have

$$R_n(\Gamma_1 \times \Gamma_2) \leq \sum_{mk=n} R_m(\Gamma_1) R_k(\Gamma_2) \leq c_1 c_2 n^{c_1 + c_2 + 1}$$

and $\Gamma_1 \times \Gamma_2$ has PRG. $\qquad\square$

Theorem 3.1 ([56, 2.7]). *Let G be a compact p-adic analytic group and suppose that the Lie algebra of G is perfect. Then G is of representation type c for some $c \in \mathbb{R}_{\geq 0}$.*

Proof. Every p-adic analytic group has an open standard subgroup U (Theorem 1.6), and since G is compact, every open subgroup has finite index. Thus, by Lemma 3.1.4 it suffices to show that U is of representation type c for some $c \in \mathbb{R}_{\geq 0}$. Moreover, note that, since U is an open subgroup of G, both G and U have the same associated Lie $\mathbb{Q}_p$-algebra. Therefore we may assume that G is a standard group.

This means we have a global chart for G, i.e., a homeomorphism

$$f: \quad G \;\to\; (p\mathbb{Z}_p)^d$$
$$g \;\mapsto\; \mathbf{g},$$

where $d = \dim G$ (as a $\mathbb{Q}_p$-analytic group). Moreover, multiplication in G is given by an analytic function $m : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ with coefficients in $\mathbb{Z}_p$ that can be written as

$$m(\mathbf{x}, \mathbf{y}) = \mathbf{x} + \mathbf{y} + B(\mathbf{x}, \mathbf{y}) + O(3),$$

where B is a $\mathbb{Z}_p$-bilinear form and $O(3)$ is a power series with monomials of total order at least 3, see section 1.2.3. We will make an abuse of notation an identify an element $g \in G$ with its coordinates $\mathbf{g} \in (p\mathbb{Z}_p)^d$. The Lie algebra $\mathcal{L} = \mathcal{L}_G$ associated to the standard group G is $(\mathbb{Z}_p)^d$ with Lie bracket given by $[\mathbf{x}, \mathbf{y}]_L = B(\mathbf{x}, \mathbf{y}) - B(\mathbf{x}, \mathbf{y})$ for $\mathbf{x}, \mathbf{y} \in (\mathbb{Q}_p)^d$. By 1.2.5.vi) the coordinates of the commutator of two elements $x, y \in G$ are given by

$$[\mathbf{x}, \mathbf{y}] := f([x, y]) = [\mathbf{x}, \mathbf{y}]_L + O(3).$$

Let us write $G_i = f^{-1}((p^i \mathbb{Z}_p)^d)$, which gives a natural filtration of G by finite index open normal subgroups. Moreover, by the proof of Theorem 8.31 in [22] we have $G_{i+1} = G^{p^i}$, where the latter subgroup denotes the closed subgroup generated by p^i-powers of elements of G.

Now since $\mathcal{L}(\mathbb{Q}_p) = \mathcal{L} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is perfect, this implies that $p^r \mathcal{L} \subseteq [\mathcal{L}, \mathcal{L}]$ for some $r \in \mathbb{N}$ and so $p^{2n+r} \mathcal{L} \subseteq [p^n \mathcal{L}, p^n \mathcal{L}]$ for every $n \in \mathbb{N}$. This implies that $G_{2n+r} \subseteq [G_n, G_n]G_{3n}$. Indeed, any element $\mathbf{g} \in p^{2n+r} \mathcal{L}$ can be written as a sum of d elements of the form $[\mathbf{x_1}, \mathbf{y_1}]_L + \ldots [\mathbf{x_d}, \mathbf{y_d}]_L$ for some $\mathbf{x_i}, \mathbf{y_i} \in p^n \mathcal{L}$. Thus, applying the above formula for the coordinates of commutators and multiplication, we have that

$$[\mathbf{x_1}, \mathbf{y_1}] \cdots [\mathbf{x_d}, \mathbf{y_d}] = \mathbf{g} + O(3).$$

Therefore $g \in [G_n, G_n]G_{3n}$ and $G_{2n+r} \subseteq [G_n, G_n]G_{3n}$.

If $n \geq r + 2$ then $2(n+1) + r \leq 3n$ and we can apply the above inclusion to obtain $G_{3n} \leq G_{2(n+1)+r} \leq [G_n, G_n]G_{3(n+1)}$. Since this holds for every $n \geq r + 2$, applying induction we obtain that $G_{3n} \subseteq [G_n, G_n]G_{3m}$ for every $m \geq n$, which implies $G_{3n} \leq [G_n, G_n]$.

Consider now $\rho \in \mathrm{Irr}_{p^n}(G)$ where $n \geq r + 2$. Since G is a pro-p group and hence pro-nilpotent, ρ is induced from $\rho' \in \mathrm{Irr}_1(H)$ for some subgroup $H \leq U$ of index p^n (Lemma 3.1.5). Recall that $G_{n+1} = G^{p^n} \leq H$, so we have $G_{3(n+1)} \leq [G_{n+1}, G_{n+1}] \leq [H, H]$. Hence, $G_{3(n+1)} \leq \ker \rho'$ and since $G_{3(n+1)}$ is normal this gives $G_{3(n+1)} \leq \ker \rho$.

It follows that $|G/K_n(G)| \leq G/G_{3(n+1)} = p^{3(n+1)d}$ for $n \geq r + 2$. Therefore, we can find $c \in \mathbb{R}_{\geq 0}$ such that $|G/K_n(G)| \leq cn^c$ for every $n \in \mathbb{N}$. $\qquad \square$

The following Theorem is an unpublished result of A. Jaikin. We present it here for completion.

Theorem 3.2 ([38, Theorem 3.1]). *Let G be an $\mathbb{F}_p[[t]]$-standard group and suppose that $\mathcal{L}_G$ is finitely generated as a G-module. Then G is of representation type c for some $c \in \mathbb{R}_{\geq 0}$.*

Proof. We will use the notation of Theorem 3.1. If $\mathcal{L} = \mathcal{L}_G$ is the $\mathbb{F}_p[[t]]$-Lie algebra of the standard group G, we have now a homeomorphism from G to $t\mathcal{L} = (t F_p[[t]])^d$ given by

$$\begin{array}{rcl} f: & G & \to & (t\mathbb{F}_p[[t]])^d \\ & g & \mapsto & \mathbf{g}, \end{array}$$

where $d = \dim G$. Let us denote the adjoint action of G by $\mathrm{Ad} = \mathrm{Ad}_{\mathbb{F}_p[[t]]} : G \to \mathrm{Aut}_{\mathbb{F}_p[[t]]}(\mathcal{L})$, see section 1.2.3.

If we let G act by conjugation on the abelian group G_k/G_{2k}, from 1.2.5.v) and the description of the adjoint action (see (1.1) in section 1.2.3) we obtain an isomorphism of G-modules

$$\begin{array}{ccc} G_k/G_{2k} & \to & \mathcal{L}/t^k\mathcal{L} \\ g & \mapsto & t^{-k}\mathbf{g} \end{array} \tag{3.1}$$

Let us write A for the $\mathbb{F}_p[[t]]$-subalgebra of $\mathrm{End}_{\mathbb{F}_p[[t]]}(\mathcal{L})$ generated by $\{\mathrm{Ad}(g) : g \in G\}$ and for every subset $H \subseteq G$ let $\mathrm{I}(H)$ denote the left ideal of A generated by $\{\mathrm{Ad}(h) - \mathrm{Id} : h \in H\}$. We will write $\mathrm{I}_k = \mathrm{I}(G_k)$. Note that since G_k is a normal subgroup, I_k is an ideal. Under this notation $[\mathcal{L}, G_k] = \mathcal{L}\mathrm{I}_k$ if we see $\mathcal{L}$ as an $\mathrm{End}_{\mathbb{F}_p[[t]]}(\mathcal{L})$ module. Let us state and prove a series of claims that are required for the proof.

Claim 1. There exists s such that for every $k \geq s$ we have

$$G_{k+s} \leq [G_k, G].$$

By assumption $\mathcal{L}$ is finitely generated as a G-module, equivalently (see 1.8.1) $|\mathcal{L}/[\mathcal{L}, G]|$ is finite. Hence there exists $s \in \mathbb{N}$ such that $t^s\mathcal{L} \subseteq [\mathcal{L}, G]$. From this and isomorphism (3.1) it follows that for every $k \geq s$ we have

$$G_{k+s} \leq [G_k, G]G_{2k}.$$

If we take $n > k$ this gives

$$G_{2n} \leq G_{(n+1)+s} \leq [G_{n+1}, G]G_{2(n+1)} \leq [G_k, G]G_{2(n+1)}.$$

Hence, whenever $k \geq s$ we can apply an inductive argument to obtain

$$G_{k+s} \leq [G_k, G]G_{2n}$$

for every $n > k$ and since G_{k+s} is closed this gives $G_{k+s} \leq [G_k, G]$.

Claim 2. There exists $l \in \mathbb{N}$ such that $\mathrm{I}_1^l \leq tA$.

Note that $\mathbb{F}_q[[t]]$ is a Noetherian local ring and A is an $\mathbb{F}_q[[t]]$-submodule of the finitely generated $\mathbb{F}_q[[t]]$-module $\mathrm{End}_{\mathbb{F}_q[[t]]}(\mathcal{L})$, hence A is finitely generated as well. We can apply Nakayama Lemma to get that A/tA is finite. Now note that from the description of the adjoint action (see (1.1) in section 1.2.3) it follows that $\mathrm{Ad}(G) - \mathrm{Id} \subseteq t\,\mathrm{End}_{\mathbb{F}_p[[t]]}(\mathcal{L})$, which implies $\mathrm{I}_1 \subseteq t\,\mathrm{End}_{\mathbb{F}_p[[t]]}(\mathcal{L})$, i.e., $\mathrm{I}_1^i \subseteq t^i\,\mathrm{End}_{\mathbb{F}_p[[t]]}(\mathcal{L})$. Thus I_1^i gives a strictly decreasing sequence of submodules, so there exists $l \in \mathbb{N}$ such that $\mathrm{I}_1^l \leq tA$.

Claim 3. For every $u > s$ we have $\mathrm{I}_{u+s} \leq \mathrm{I}_1\,\mathrm{I}_u + \mathrm{I}_u\,\mathrm{I}_1$.

By Claim 1 we know that $G_{u+s} \leq [G_u, G]$. Suppose $g = [g_u, g_1]$, where $g_u \in G_u$, $g_1 \in G_1$. Then

$$\begin{aligned} \mathrm{Ad}(g) - \mathrm{Id} &= \mathrm{Ad}([g_u, g_1]) - \mathrm{Id} \\ &= \mathrm{Ad}(g_u^{-1}g_1^{-1})[\mathrm{Ad}(g_u) - \mathrm{Id}, \mathrm{Ad}(g_1) - \mathrm{Id}]_L \in \mathrm{I}_u\,\mathrm{I}_1 + \mathrm{I}_1\,\mathrm{I}_u\,. \end{aligned}$$

If $g = fh$ is a product of commutators in $[G_u, G]$, then

$$\mathrm{Ad}(fh) - \mathrm{Id} = (\mathrm{Ad}(f) - \mathrm{Id})(\mathrm{Ad}(h) - \mathrm{Id}) + \mathrm{Ad}(f) - \mathrm{Id} - (\mathrm{Ad}(h) - \mathrm{Id}) \tag{3.2}$$

and by the previous case $g \in \mathrm{I}_1\,\mathrm{I}_u + \mathrm{I}_u\,\mathrm{I}_1$.

Claim 4. For every $u > s$ we have $\mathrm{I}_{u+(2l-1)s} \leq t\,\mathrm{I}_u$.

Applying the previous claim $(2l - 1)$ times we obtain

$$\mathrm{I}_{u+s(2l-1)} \subseteq \sum_{i+j=2l-1} \mathrm{I}_1^i\,\mathrm{I}_u\,\mathrm{I}_1^j\,.$$

It follows from Claim 2 that $\mathrm{I}_{u+s(2l-1)} \leq t\,\mathrm{I}_u$.

Claim 5. Let H be an open subgroup of G, then $\mathrm{I}_1 / \mathrm{I}(H)$ is finite.

Let $f_1, \ldots, f_{d^2}$ be a set of free generators of $\mathrm{End}_{\mathbb{F}_q[[t]]}(\mathcal{L})$ as an $\mathbb{F}_q[[t]]$-module. Then every element $E \in \mathrm{End}_{\mathbb{F}_q[[t]]}(\mathcal{L})$ can be expressed as linear combination of the f_i with coefficients in $\mathbb{F}_p[[t]]$. If we assign to every such E its coefficients with respect to the f_i, this gives $\mathrm{End}_{\mathbb{F}_q[[t]]}(\mathcal{L})$ the structure of an $\mathbb{F}_q[[t]]$-analytic variety. Note that the map $\mathrm{Ad} - \mathrm{Id} : G \to \mathrm{End}_{\mathbb{F}_p[[t]]}(\mathcal{L})$ is then an analytic map. We can consider any power series in the f_i with coefficients in $\mathbb{F}_p[[t]]$ as an analytic function on $\mathrm{End}_{\mathbb{F}_q[[t]]}(\mathcal{L})$. Since I_1 is finitely generated, to prove the claim it suffices to show that $t^j\,\mathrm{I}_1 \subseteq \mathrm{I}(H)$ for some $j \in \mathbb{N}$. Suppose that there exists no such j, this means that $\mathrm{I}(H)$ is a free $\mathbb{F}_p[[t]]$-module of rank strictly less than that of I_1. So there exist $\alpha_1, \ldots, \alpha_{d^2}$ such that $\psi(\mathbf{f}) = \sum \alpha_i f_i$ satisfies $\psi(\mathrm{Ad}(\mathbf{h}) - \mathrm{Id}) = 0$ for every $h \in H$ but there exists $g \in G$ such that $\psi(\mathrm{Ad}(g) - \mathrm{Id}) \neq 0$. that is, H is contained in the zeroes of some analytic equation but G is not. But this is impossible by [39, Theorem 3.3]

Claim 6. Let $s(G) := \{g \in G \,:\, \mathrm{Ad}(g) \text{ is semisimple}\}$. Then the closed subgroup generated by $s(G)$ is open in G.

Note that $g^{p^d} \in s(G)$ for every $g \in G$. We can apply Zelmanov's positive solution to the Restricted Burnside Problem to obtain that G^{p^d} is a finite index subgroup of G and hence open. It follows that the closed subgroup generated by $s(G)$ is open as well.

Claim 7. Suppose $h \in s(G)$. Then $A(\mathrm{Ad}(h) - \mathrm{Id})^2$, the left ideal of A generated by $(\mathrm{Ad}(h) - \mathrm{Id})^2$, has finite index in $\mathrm{I}(h) = A(\mathrm{Ad}(h) - \mathrm{Id})$.

From the point of view of $\mathbb{F}_p[[t]]$-modules the claim holds if and only if $t^k A(\mathrm{Ad}(h) - \mathrm{Id}) \subseteq A(\mathrm{Ad}(h) - \mathrm{Id})^2$ for some k and this happens if and only if $\mathbb{F}_p((t)) \otimes A(\mathrm{Ad}(h) - \mathrm{Id}) = \mathbb{F}_p((t)) \otimes A(\mathrm{Ad}(h) - \mathrm{Id})^2$. This is an equality of vector spaces and hence reduces to an equality of their respective dimensions, which are stable under extension of scalars, so this holds if and only if $\overline{\mathbb{F}_p((t))} \otimes A(\mathrm{Ad}(h) - \mathrm{Id}) = \overline{\mathbb{F}_p((t))} \otimes A(\mathrm{Ad}(h) - \mathrm{Id})^2$. Now an appropriate change of coordinates allows us to assume that $\mathrm{Ad}(h) - \mathrm{Id}$ is a diagonal matrix, and so for every element $M \in \mathrm{End}_{\overline{\mathbb{F}_p((t))}}(\overline{\mathbb{F}_p((t))}^d)$ we have $M(\mathrm{Ad}(h) - \mathrm{Id}) = 0$ if and only if $M(\mathrm{Ad}(h) - \mathrm{Id})^2 = 0$. Hence $\overline{\mathbb{F}_p((t))} \otimes A(\mathrm{Ad}(h) - \mathrm{Id}) = \overline{\mathbb{F}_p((t))} \otimes A(\mathrm{Ad}(h) - \mathrm{Id})^2$ and we are done.

Claim 8. There exist c_1 and c_2 such that $t^{c_1+kc_2}\,\mathrm{I}_1 \subseteq \mathrm{I}_k$ for every k.

By Claim 5 and 6 we know that $\mathrm{I}(s(G))$ is of finite index in I_1. Pick $g_1, \ldots, g_t \in s(G)$ such that $\mathrm{Ad}(g_i) - \mathrm{Id}$ generate $\mathrm{I}(s(G))$. By Claim 7 we know that $A(\mathrm{Ad}(g_i) - \mathrm{Id})/A(\mathrm{Ad}(g_i) - \mathrm{Id})^2$ is finite. Thus there exists c such that for every i we have $t^c A(\mathrm{Ad}(g_i) - \mathrm{Id}) \subseteq A(\mathrm{Ad}(g_i) - \mathrm{Id})^2$.

53

Hence for every $j \geq 0$ we have

$$t^{c(p^j-1)} \operatorname{I}(s(G)) \leq \sum_i A(\operatorname{Ad}(g_i) - \operatorname{Id})^{p^j} = \sum_i A(\operatorname{Ad}(g_i)^{p^j} - \operatorname{Id}) \leq \operatorname{I}_{p^j}.$$

The last inequality follows from the fact that $G^{p^j} \leq G_{p^j}$, see 1.2.5.viii). Now it is clear that there exist constants c_1 and c_2 satisfying the claim.

Consider now $\rho \in \operatorname{Irr}(G)$ and suppose $G_{2(k-1)} \not\subseteq \ker \rho$ but $G_{2k} \subseteq \ker \rho$. Let $\lambda \in \operatorname{Irr}(G_k)$ be an irreducible constituent of $\rho_{|G_k}$ and let $H \leq G$ be the stabilizer of λ with index $|G/H| = p^m$.

Claim 9. $G_{s(2l-1)(m+1)} \leq H$.

Consider the chain of subgroups

$$H \leq HG_{s(2l-1)(m+1)} \leq HG_{s(2l-1)m} \leq \ldots \leq HG_{s(2l-1)}.$$

Note that $|G : H| = p^m$ implies that there must be an equality in the above chain. If $H = HG_{s(2l-1)(m+1)}$ we are done. If not, suppose $HG_{s(2l-1)i} = HG_{s(2l-1)(i+1)}$ for some $1 \leq i \leq m$. From (3.2) it follows that $\operatorname{I}(JN) = \operatorname{I}(J) + I(N)$ whenever $N \trianglelefteq G$ and $J \leq G$. We can now apply the previous equality of subgroups and Claim 4 to obtain

$$\operatorname{I}(H) + \operatorname{I}_{s(2l-1)i} = \operatorname{I}(H) + \operatorname{I}_{s(2l-1)(i+1)} = \operatorname{I}(H) + t \operatorname{I}_{s(2l-1)i}.$$

If we apply the Nakayama Lemma to the above equality of $\mathbb{F}_q[[t]]$-modules we get $\operatorname{I}_{s(2l-1)i} \leq \operatorname{I}(H)$. In particular, $\mathcal{L} \operatorname{I}_{s(2l-1)i} \leq \mathcal{L} \operatorname{I}(H)$. Therefore, isomorphism (3.1) gives

$$[G_k, G_{s(2l-1)i}]G_{2k} \leq [G, H]G_{2k}.$$

In particular, $G_{s(2l-1)i}$ stabilizes λ and $G_{s(2l-1)(m+1)} \leq G_{s(2l-1)i} \leq H$.

We are now ready to finish the proof. Suppose that $k \geq c_1 + c_2 s(2l-1)(m+1) + 2$. It follows from Claim 8 that

$$t^{c_1+c_2 s(2l-1)(m+1)} \mathcal{L} \operatorname{I}_1 \leq \mathcal{L} \operatorname{I}_{s(2l-1)(m+1)}.$$

Now first applying Claim 1 and then the previous inequality together with isomorphism (3.1) we obtain

$$G_{c_1+c_2 s(2l-1)(m+1)+k+s} \leq [G_{c_1+c_2 s(2l-1)(m+1)+k}, G_1]G_{2k}$$
$$\leq [G_k, G_{s(2l-1)(m+1)}]G_{2k}.$$

However, since by Claim 9 we have $G_{s(2l-1)(m+1)} \leq H$, we must have

$$G_{k+c_1+c_2 s(2l-1)(m+1)} \leq \ker \lambda.$$

But recall that $G_{2(k-1)} \not\subseteq \ker \lambda$ and hence

$$2k - 2 \leq k + c_1 + c_2 s(2l-1)(m+1),$$

equivalently, $k \leq c_1 + c_2 s(2l-1)(m+1) + 2$, which contradicts our assumption. Therefore, we must have

$$k \leq c_1 + c_2 s(2l-1)(m+1) + 2.$$

It follows that $G_{2(c_1+c_2 s(2l-1)(m+1)+2)} \leq \ker \rho$. By Lemma 3.1.6 ρ is induced from an irreducible representation of H and so $\dim \rho \geq p^m$ so we have $G_{2(c_1+c_2 s(2l-1)(\log_p n+1)+2)} \leq \ker \rho$ for some constants d_1, d_2 which only depend on c_1 and c_2. This implies

$$G_{d_1+d_2 \log_p n} \leq K_n(G).$$

Thus, $|G/K_n(G)| \leq |G/G_{d_1+d_2 \log_p n}| = p^{\dim G(d_1+d_2 \log_p n)} \leq cn^c$ for some $c \in \mathbb{R}_{\geq 0}$ as desired. $\qquad \square$

Remark. Note that the above proof works equally well for $\mathbb{Z}_p$-standard groups if we assume that $p^k \mathcal{L}(G) \leq [\mathcal{L}, G]$ for some $k \in \mathbb{N}$, nevertheless for p-adic analytic groups this condition is equivalent to $\mathcal{L}(G) \otimes \mathbb{Q}_p$ being perfect.

3.2 CSP and Representation Growth of Arithmetic Groups

Let k be a global field and G a simply connected semisimple algebraic k-group. Let $S \subset V_k$ be a non-empty finite set of valuations such that $V_\infty \subseteq S$ and Γ and S-arithmetic subgroup of G. In this section we investigate the relation between the weak Congruence Subgroup Property (namely the finiteness of $C(G,S)$) and the representation growth of Γ. The main Theorem is the following.

Theorem 3.3. *Let k, S, Γ and G be as above. If G has the weak Congruence Subgroup Property with respect to S, then Γ has Polynomial Representation Growth.*

As in the previous sections we fix a k-embedding $\iota : G \to \mathrm{GL}_n$. We also give G the structure of an affine group $\mathcal{O}_S$-scheme through this embedding, see section 2.2.

We will make use of the previous sections to reduce Theorem 3.3 to a particular setting. First let us note that, by definition, Γ is commensurable with $G(\mathcal{O}_S)$, so applying Lemma 3.1.3 it follows that Γ has PRG if and only if $G(\mathcal{O}_S)$ does. Hence we may assume that $\Gamma = G(\mathcal{O}_S)$. If $G(\mathcal{O}_S)$ is finite, then so is Γ and Theorem 3.3 becomes trivial, so from now on we will assume that $G(\mathcal{O}_S)$ is infinite.

Let G^0 be the connected component of G. Since G^0 is of finite index in G (Theorem 1.4.2), it follows that $G^0(\mathcal{O}_S)$ has finite index in $G(\mathcal{O}_S)$. Hence applying Lemma 3.1.3 again it suffices to study the representation growth of $G^0(\mathcal{O}_S)$. Moreover by Lemma 2.4.1 G has wCSP if and only if G^0 does, so we may assume that G is connected.

Since G is simply connected, Theorem 1.12 gives that G is a direct product of its almost k-simple factors, say $G_1, \ldots, G_r$. Now Lemma 3.1.7 shows that $G(\mathcal{O}_S)$ has PRG if and only if each $G_i(\mathcal{O}_S)$ has. Hence, we may assume that G is almost k-simple. Moreover Theorem 2.6 now implies that G has Strong Approximation. Recall that this means that $G(k)G_S$ is dense in $G(\mathbb{A}_k)$, which in particular implies that $G(\mathcal{O}_S)$ is dense in $G(\widehat{\mathcal{O}}_S) := \prod_{v \in V_f \setminus S} G(\mathcal{O}_v)$. Hence we have $\overline{G(\mathcal{O}_S)} \cong G(\widehat{\mathcal{O}}_S)$.

Moreover, Lemmata 2.6.2 and 2.2.3 (together with one furhter application of Lemma 3.1.3) allow us to further assume that G is absolutely almost simple.

Now if $G(\mathcal{O}_S)$ has wCSP, then $C(G, S) = \ker\left(\widehat{G(\mathcal{O}_S)} \to G(\widehat{\mathcal{O}}_S)\right)$ is finite. Hence we can find Γ_0 of finite index in $G(\mathcal{O}_S)$ such that its profinite closure $\widehat{\Gamma}_0$ has trivial intersection with $C(G, S)$. Thus, we can see $\widehat{\Gamma}_0$ as a finite index subgroup in $G(\widehat{\mathcal{O}}_S)$. It follows from Lemma 3.1.3 and Lemma 3.1.1 that $G(\mathcal{O}_S)$ has PRG if and only if Γ_0 does, if and only if $\widehat{\Gamma}_0$ does , if and only if $G(\widehat{\mathcal{O}}_S)$ does. Therefore to prove Theorem 3.3 it suffices to show the following Theorem.

Theorem 3.4. *Let k be a global field and $S \subset V_k$ a finite set of valuations. Let G be a connected simply connected absolutely almost simple k-group. Then $G(\widehat{\mathcal{O}}_S)$ has Polynomial Representation Growth.*

Remark. Note that in Theorem 3.4 we do not need to assume that G has wCSP with respect to S.

Let us write $V_f^S := \{v \in V_f \ : \ v \notin S\}$. Recall that

$$G(\widehat{\mathcal{O}}_S) \cong \prod_{v \in V_f^S} G(\mathcal{O}_v),$$

so we want to better understand the groups $G(\mathcal{O}_v)$ for $v \in V_f^S$. The idea is to find a uniform bound for the representation growth of the groups $G(\mathcal{O}_v)$, that is, to find $c \in \mathbb{R}_{\geq 0}$ such that for every "good valuation" v the group $G(\mathcal{O}_v)$ has representation type c, and then apply Lemma 3.1.7 to obtain a polynomial bound for the representation growth of $G(\widehat{\mathcal{O}}_S)$. By Proposition 3.2.1 we can control the effect of $G(\mathcal{O}_v)/G(\mathfrak{m}_v)$. Then we show that for almost every v the group $G(\mathfrak{m}_v)$ is $\mathcal{O}_v$-standard (Lemma 3.2.4) and we can "uniformly" apply Theorem 3.2 to obtain Theorem 3.5.

First, let us briefly recall how $G(k_v)$ has the structure of a k_v-analytic group for every $v \in V_f^S$. If we see $G \subseteq \mathrm{GL}_N \subseteq \mathbb{A}^{N^2+1}$, then G is determined by an ideal given by some polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_{N^2+1}]$. Since G is an algebraic variety the set of regular points is Zariski dense in G, moreover since G acts transitively on itself by automorphism, it follows that all points in G are regular. Hence, by the Jacobian Criterion (see for instance [53, Theorem 2.19], the Jacobian of $f_1, \ldots, f_m$ has rank $N^2 + 1 - \dim G$. Thus, applying the Inverse Function Theorem for local fields ([79, Part II, Chapter III]) it follows that at every point $x \in G(k_v)$ the projection onto the, say first, $\dim G$ coordinates defines a chart on an open neighbourhood of x. This gives the structure of a k_v-analytic variety to $G(k_v)$ and multiplication and inversion, which are given by maps of algebraic k-groups, are analytic with respect to this structure.

Now on the one hand we have $\mathcal{L}(G(k_v))$, the k_v-Lie algebra associated to the analytic group $G(k_v)$ and on the other hand we have $L_G(k_v) = k_v \otimes L(k)$ the k_v-Lie algebra associated to the algebraic k-group G. Since $\mathrm{Der}_{k_v}(k_v[G(k_v)]) = k_v \otimes \mathrm{Der}_k(k[G])$ we have $L(k_v) \cong \mathcal{L}(G(k_v))$.

Equivalently, if we regard G as an affine group $\mathcal{O}_S$-scheme then

$$L_G(R) = \mathrm{Der}_{\mathcal{O}_S}(\mathcal{O}_S[G], R) \cong \mathrm{Hom}_{\mathcal{O}_S}(I_{\mathcal{O}_S[G]}/I^2_{\mathcal{O}_S[G]}), R)$$

for every $\mathcal{O}_S$-algebra R, see section 1.5. In particular,

$$L_G(k_v) = L_G(k) \otimes k_v = L_G(\mathcal{O}_S) \otimes k_v \cong \mathcal{L}(G(k_v)).$$

Let us introduce some useful notation and state a series of results which will allow us to prove Theorem 3.4. Given $v \in V_f^S$, recall that $\mathfrak{m}_v$ stands for the maximal ideal of $\mathcal{O}_v$ and let us write $\mathfrak{p}_v := \{x \in \mathcal{O}_S \ : \ x \in \mathcal{O}_v\}$ for the corresponding maximal ideal of $\mathcal{O}_S$. We will fix a uniformizer $\pi_v \in \mathcal{O}_v$ such that $\mathfrak{m}_v = (\pi_v)$. Recall that $\mathbb{F}_v = \mathcal{O}_v/\mathfrak{m}_v$ stands for the corresponding residue field of size $q_v := |\mathbb{F}_v|$. For every $k \in \mathbb{N}$ let us write

$$N_v^k = G(\mathfrak{m}_v^k) := G(\mathcal{O}_v) \cap \ker\left(\mathrm{GL}_N(\mathcal{O}_v) \to \mathrm{GL}_N(\mathcal{O}_v/\mathfrak{m}_v^k)\right),$$

for the principal congruence subgroup of level k of $G(\mathcal{O}_v)$. If we see G embedded in GL_N this is nothing but the points of G whose coordinates lie in $\mathfrak{m}_v^k$. If one thinks of G as an affine group $\mathcal{O}_S$-scheme then

$$G(\mathfrak{m}_v^k) = \{\varphi \in \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_S[G], \mathcal{O}_v) \ : \ \varphi(I_{\mathcal{O}_S[G]}) \subseteq \mathfrak{m}_v^k\},$$

where $I_{\mathcal{O}_S[G]} = \ker \epsilon$ and $\epsilon : \mathcal{O}_S[G] \to \mathcal{O}_S$ represents the identity of $G_{\mathcal{O}_S}$, see section 1.5.

We want to apply Theorem 3.2 to the groups $G(\mathcal{O}_v)$, so we begin by investigating the adjoint action in semisimple algebraic k-groups.

Lemma 3.2.1. *Let Q be a connected simply connected semisimple algebraic group defined over a field F and $H \leq Q(F)$ a Zariski dense subgroup. If L is the Lie algebra of Q, then*

$$L(F) = [L(F), H].$$

Proof. Since we are dealing with vector spaces, the equality amounts to equality of dimensions. Extension of scalars does not affect dimension and hence if $\bar{F}$ is an algebraic closure of F it suffices to show $\bar{F} \otimes_F L(F) = \bar{F} \otimes_F [L(F), H]$, that is, $L(\bar{F}) = [L(\bar{F}), H]$. Moreover, since the adjoint action is Zariski continuous and $[L(\bar{F}), H]$, being a vector subspace, is Zariski closed we have $[L(\bar{F}), H] = [L(\bar{F}), Q(\bar{F})]$. We may therefore assume without loss of generality that F is algebraically closed and that $H = Q(F)$.

In this setting Q can be obtained as a Chevalley group scheme over F (see the comments before Corollary 5.1 in [81]). Let α be a root of an associated (absolute)root system Φ of Q and let X_α denote the corresponding unipotent subgroup, then G is generated by $\{X_\alpha \ : \ \alpha \in \Phi\}$, see [81, Chapter 3]. Then, since Q is simply connected, the subgroup $\langle X_\alpha, X_{-\alpha} \rangle$ acts on its Lie algebra $\mathfrak{x}_{-\alpha} \oplus \mathfrak{h}_\alpha \oplus \mathfrak{x}_\alpha$ as $\mathrm{SL}_2(K)$ acts on its Lie algebra $\mathfrak{sl}_2$ ([81, Corollary 3.6]). Moreover $L(F) = \langle \sum_{\alpha \in \Phi} \mathfrak{x}_{-\alpha} + \mathfrak{h}_\alpha + \mathfrak{x}_\alpha \rangle$, so it suffices to check the equality in the case $Q = \mathrm{SL}_2$ and this reduces to the following quick calculation.

$$\begin{pmatrix} k^{-1} & 0 \\ 0 & k \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} k & 0 \\ 0 & k^{-1} \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad = \begin{pmatrix} 0 & k^2 - 1 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad = k \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ k^2 & 0 \end{pmatrix}$$

From the first calculation we obtain that all elements of the form $\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}$ belong to

$[\mathfrak{sl}_2, \mathrm{SL}_2]$ and by a symmetric operation the same holds for elements of the form $\begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix}$.

Now from the second calculation we obtain that all elements of the form $\begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix}$ belong

to $[\mathfrak{sl}_2, \mathrm{SL}_2]$ and this finishes the proof. $\qquad\square$

As a direct application, we obtain the following Lemma.

Lemma 3.2.2. *Let k, S and G be as in Theorem 3.4. Then for every $v \in V_f^S$, $L(\mathcal{O}_v)$ is finitely generated as an N_v^1-module. Moreover, for almost every $v \in V_f^S$ we have*

$$L(\mathcal{O}_v) = [L(\mathcal{O}_v), G(\mathcal{O}_v)].$$

Proof. $G(\mathcal{O}_S)$ is Zariski-dense by Proposition 2.2.1. Thus, we can apply Lemma 3.2.1 to obtain $L(k) = [L(k), G(\mathcal{O}_S)]$. Since $L(k) = k \otimes_{\mathcal{O}_S} L(\mathcal{O}_S)$, this implies

$$\mathfrak{p}_{v_1}^{i_1} \cdots \mathfrak{p}_{v_t}^{i_t} L(\mathcal{O}_S) \subseteq [L(\mathcal{O}_S), G(\mathcal{O}_S)]$$

for certain prime ideals $\mathfrak{p}_{v_i} \subseteq \mathcal{O}$ corresponding to distinct valuations $v_1, \ldots, v_t \in V_f^S$. It follows that $L(\mathcal{O}_v) = [L(\mathcal{O}_v), G(\mathcal{O}_v)]$ for every $v \in V_f^S \setminus \{v_1, \ldots, v_t\}$.

In general, note that, for $v \in V_f^S$, $G(\mathcal{O}_v)$ is Zariski-dense since $G(\mathcal{O}_S)$ is. It follows that $N_v^1 = G(\mathfrak{m}_v)$, being a finite index subgroup in $G(\mathcal{O}_v)$, is Zariski-dense. Applying Lemma 3.2.1 we obtain $L(k_v) = [L(k_v), N_v^1]$. Hence, $[L(\mathcal{O}_v), N_v^1]$ has finite index in $L(\mathcal{O}_v)$, which implies that $L(\mathcal{O}_v)$ is a finitely generated N_v^1-module (note that N_v^1 is a pro-p group for $p = \mathrm{char}\,\mathbb{F}_v$ and apply Lemma 1.8.1 to $L(\mathcal{O}_v)$ as an N_v^1-module). $\qquad\square$

Lemma 3.2.3. *Let G be a connected simply connected absolutely almost simple algebraic k-group. Then for almost every $v \in V_f^S$ the group $G(\mathcal{O}_v)/N_v^1$ is perfect and is a central extension of a finite simple group of Lie type $H(\mathbb{F}_v)/Z(H(\mathbb{F}_v))$, where H is of the Lie type of G.*

Sketch of proof. The proof of this result rests on the relative theory of reductive group schemes over rings which lies beyond the general scope of this work. We give here a sketch of the proof and point out to references for the details.

Recall that we gave G the structure of an affine group $\mathcal{O}_S$-scheme. Given $v \in V_f^S$, let us write $G_{\mathfrak{p}_v}$ for the reduction of G modulo $\mathfrak{p}_v$, that is, $G_{\mathfrak{p}_v}$ is an affine group $\mathbb{F}_v$-scheme represented by $\mathcal{O}_S[G] \otimes_{\mathcal{O}_S} \mathcal{O}_S/\mathfrak{p}_\mathfrak{v} = \mathcal{O}_S[G] \otimes_{\mathcal{O}_S} \mathbb{F}_v$, where $\mathcal{O}_S[G]$ represents G. Since G is a connected and irreducible algebraic variety (as an affine algebraic group), it is reduced (as an affine group $\mathcal{O}_S$-scheme, that is $\mathcal{O}_S[G]$ has no nilpotent elements) and this implies that the same holds for $G_{\mathfrak{p}_v}$ for almost every $v \in V_f^S$, see [26, Proposition 9.7.7 and 9.7.8]. If $G_{\mathfrak{p}_v}$ is reduced, then it is an algebraic variety and hence has some regular point, but it is also an algebraic $\mathbb{F}_v$ group, so indeed all points are regular and G_v is smooth. Hence we can apply [26, 18.5.17] and obtain that the reduction map $G(\mathcal{O}_v) \to G_{\mathfrak{p}_v}(\mathbb{F}_v)$ is surjective for almost every $v \in V_f^S$.

Now if we see k as the direct limit of the rings $\mathcal{O}_S[1/r]$ for $r \in \mathcal{O}_S$ and since G is a semisimple k-group, we can apply [19, Corollary 3.1.11] to obtain that there exists $s \in \mathcal{O}_S$ (consisting of those "bad" primes) such that $G_{\mathcal{O}_S[1/s]}$ (which is the affine group $\mathcal{O}_S[1/s]$-scheme represented by $\mathcal{O}_S[G] \otimes_{\mathcal{O}_S} \mathcal{O}_S[1/s]$) is a semisimple affine group $\mathcal{O}_S[1/s]$-scheme, that is, for every $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}[1/s])$ the group represented by $\mathcal{O}_S[1/s][G] \otimes_{\mathcal{O}_S[1/s]} (\mathcal{O}_S[1/s]/\mathfrak{p})$ is a semisimple $(\mathcal{O}_S[1/s]/\mathfrak{p})$-group. But note that $\mathcal{O}_S[1/s][G] \otimes_{\mathcal{O}_S[1/s]} (\mathcal{O}_S[1/s]/\mathfrak{p}) = \mathcal{O}_S[G] \otimes \mathbb{F}_v$ where v is the valuation corresponding to the prime ideal $\mathfrak{p} \cap \mathcal{O}_S$. This means that for almost every $v \in V_f^S$ the group $G_{\mathfrak{p}_v}$ is semisimple.

Now maybe after considering a finite extension k' of k (or the corresponding finite integral extension $\mathcal{O}_{S'}$ of $\mathcal{O}_S$) one can find a split maximal k'-torus T in $G_{k'}$ ($G_{\mathcal{O}_{S'}}$) and applying a similar direct limit argument one shows that $T_{\mathfrak{p}}$ is a split maximal torus in $G_{\mathfrak{p}}$ for almost every $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{S'})$ (see section 3 in [19] and in particular Lemmata 3.2.5 and 3.2.7).

This shows that for almost every $v \in V_f^S$ the root systems associated to G and $G_{\mathfrak{p}_v}$ are the same. Since the root system detects being simply connected and absolutely almost simple, this implies that $G_{\mathfrak{p}_v}$ is simply connected and absolutely almost simple for almost every $v \in V_f^S$.

Therefore, for almost every $v \in V_f^S$ the $\mathbb{F}_v$-group $G_{\mathfrak{p}_v}$ is semisimple, simply connected and absolutely almost simple and we have $G(\mathcal{O}_v)/N_v^1 \cong G_{\mathfrak{p}_v}(\mathbb{F}_v)$. Given a connected simply connected absolutely almost simple algebraic group H defined over a finite field $\mathbb{F}_q$, $H(\mathbb{F}_q)$ is perfect and $H(\mathbb{F}_q)/Z(H(\mathbb{F}_q))$ is a finite simple group of Lie type (except for a finite number of q's), see Theorem 1.20. Hence, noting that for a given prime power q there is a finite number of valuations v such that $q = q_v$ (Lemma 1.1.1), it follows that the statement is true for almost every $v \in V_f^S$. $\qquad\square$

Lemma 3.2.4. *Let G be an algebraic group defined over k. Then for almost every $v \in V_f^S$, $G(\mathfrak{m}_v)$ is an $\mathcal{O}_v$-standard subgroup of $G(\mathcal{O}_v)$.*

Proof. Recall that we have given G a structure of affine group $\mathcal{O}_S$-scheme. Multiplication and inverse operations in G are given by $\mathcal{O}_S$-algebra maps $m^* : \mathcal{O}_S[G] \to \mathcal{O}_S[G] \otimes_{\mathcal{O}_S} \mathcal{O}_S[G]$ and $i^* : \mathcal{O}_S[G] \to \mathcal{O}_S[G]$. Recall that the group $G(k_v)$ inherits the structure of a k_v-analytic group, where $G(\mathcal{O}_v)$ and $G(\mathfrak{m}_v)$ are open subgroups. We can interpret $G(\mathfrak{m}_v)$ as

$$G(\mathfrak{m}_v) = \{\varphi \in \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_S[G], \mathcal{O}_v) \; : \; \varphi(I_{\mathcal{O}_S[G]}) \subseteq \mathfrak{m}_v\},$$

where $I_{\mathcal{O}_S[G]} = \ker \epsilon$ and $\epsilon : \mathcal{O}_S[G] \to \mathcal{O}_S$ represents the identity element. If we regard $G \subseteq \mathrm{GL}_N$, this is nothing but the points of G all of whose coordinates lie in $\mathfrak{m}_v$. Let us write $I = I_{\mathcal{O}_S[G]}$ and define

$$I_v := \langle \mathfrak{p}_v, I \cap \mathcal{O}_S[G] \rangle \subset \mathcal{O}_S[G].$$

Consider $\mathcal{O}_S[G]_{I_v}$, the localization of $\mathcal{O}_S[G]$ at I_v. Let $\mathcal{R}_v$ denote the completion of $\mathcal{O}_S[G]_{I_v}$ with respect to its unique maximal $I_v\mathcal{O}_S[G]_{I_v}$ and write $\mathcal{M}_v$ for the maximal ideal of $\mathcal{R}_v$. We then have

$$G(\mathfrak{m}_v) = \{\varphi \in \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_S[G], \mathcal{O}_v) \; : \; \varphi(I_{\mathcal{O}_S[G]}) \subseteq \mathfrak{m}_v\} \cong \mathrm{Hom}(R_v, \mathcal{O}_v),$$

where the latter are assumed to be continuous homomorphisms with respect to the $\mathcal{M}_v$ and $\mathfrak{m}_v$-adic topologies. The isomorphism follows from the fact that any $\varphi \in \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_S[G], \mathcal{O}_v)$ such that $\varphi(I_{\mathcal{O}_S[G]}) \subseteq \mathfrak{m}_v$ uniquily extends to an elelement in $\mathrm{Hom}(\mathcal{R}_v, \mathcal{O}_v)$. Note that the isomorphisms above are indeed group isomorphisms, where multiplication and inversion naturally extend from $G(\mathfrak{m}_v) - m^*$ and i^* extend to $\mathcal{R}_v$ and this represents affine group schemes over $\mathcal{O}_v$.

If we show that $\mathcal{R}_v \cong \mathcal{O}_v[[y_1, \ldots, y_d]]$, the ring of power series over d indeterminates with coefficients in $\mathcal{O}_v$, this would induce an isomorphism of groups $G(\mathfrak{m}_v) \cong \mathrm{Hom}(\mathcal{O}_v[[y_1, \ldots, y_d]], \mathcal{O}_v)$. Note that there is a natural identification $\mathrm{Hom}(\mathcal{O}_v[[y_1, \ldots, y_d]], \mathcal{O}_v) = \mathfrak{m}_v^d$ and under this identification the induced multiplication and inversion in the latter are given by analytic functions on d variables with coefficients in $\mathcal{O}_v$, that is, $G(\mathfrak{m}_v)$ is a standard subgroup of $G(\mathcal{O}_v)$.

We claim that such isomorphism exists for almost every $v \in V_f^S$. First let us note that if $\mathrm{char}\, k = 0$ then $\mathrm{char}\, \mathbb{F}_v \notin \mathcal{M}_v^2$, otherwise $I_{\mathcal{O}_S[G]}$ would not be a proper ideal. Hence we may assume that $\mathrm{char}\, \mathbb{F}_v \notin \mathcal{M}_v^2$. Now it suffices to show that $\mathcal{R}_v$ is regular, since in this case $\mathcal{R}_v$ is a complete regular local ring such that $\mathrm{char}\, \mathbb{F}_v \notin \mathcal{M}_v^2$ and by Cohen's Structure Theorem of complete regular local rings [60, Theorem 29.7] $\mathcal{R}_v \cong \mathcal{O}_v[[y_1, \ldots, y_d]]$. Now $\mathcal{R}_v$ is the completion of $\mathcal{O}[G]_{I_v}$, so $\mathcal{R}$ is regular if and only if $\mathcal{O}[G]_{I_v}$ is ([2, Proposition 11.24]). If $d = \dim G$ (as an affine k-group) then $\dim \mathcal{O}[G] = \dim k[G] + 1$ ($\dim A$ stands for the Krull dimension of a ring A) and $\dim \mathcal{O}_S[G]_{I_v} = d + 1$ for every $v \in V_f^S$ since $\mathcal{O}[G]$ is equicodimensional, see [26, 10.6.1]. Now note that $\dim_{\mathbb{F}_v} I_v/I_v^2 = 1 + \dim_{\mathbb{F}_v}(I \otimes \mathbb{F}_v/I^2 \otimes \mathbb{F}_v)$ and the latter equals $1 + \dim G$ for almost every $v \in V_f^S$ (I/I^2 is isomorphic as a vector space to the tangent space at 1 of G or equivalently its Lie algebra, which is given by linear equations with coefficients in $\mathcal{O}_S$, these equations will clearly give a $\mathbb{F}_v$-vector space of dimension $\dim G$ for almost every $v \in V_f^S$). Hence $\mathcal{O}[G]_{I_v}$ is regular for almost every $v \in V_f^S$ and the proof is complete. $\qquad \square$

Putting together the previous results we obtain the following Lemma.

Lemma 3.2.5. *Let $\mathcal{P}$ be the subset of all $v \in V_f^S$ such that:*

i) *$G(\mathcal{O}_v)/N_v^1$ is perfect and is a central extension of a finite simple group of Lie type $H(\mathbb{F}_v)$, where H is of the Lie type of G.*

ii) *N_v^1 is a standard subgroup of $G(\mathcal{O}_v)$.*

iii) *for every $n \in \mathbb{N}$, $[N_v^n, G(\mathcal{O}_v)] = N_v^n$.*

iv) *$G(\mathcal{O}_v)$ is a perfect group, that is, $G(\mathcal{O}_v) = [G(\mathcal{O}_v), G(\mathcal{O}_v)]$.*

Then $V_f \setminus \mathcal{P}$ is finite, i.e. , statements i), ii), iii) and iv) are satisfied for almost every $v \in V_f^S$.

Proof. Note that i) and ii) are Lemma 3.2.3 and 3.2.4 respectively.

We prove iii). Given $v \in V_f^S$, suppose that $L(\mathcal{O}_v) = [L(\mathcal{O}_v), G(\mathcal{O}_v)]$ and that N_v^1 is a standard subgroup of $G(\mathcal{O}_v)$. The group $N_v^1 = G(\mathfrak{m}_v)$ is a normal subgroup of $G(\mathcal{O}_v)$, so

$G(\mathcal{O}_v)$ acts on it by conjugation. Recall that for an $\mathcal{O}_v$-standard group we have a natural identification $f : N_v^1 \to \mathfrak{m}_v L(\mathcal{O}_v)$ and under this identification we have for every $k \in \mathbb{N}$ an isomorphism of $G(\mathcal{O}_v)$-modules

$$N_v^k/N_v^{2k} \cong L(\mathcal{O}_v)/\mathfrak{m}_v^k L(\mathcal{O}_v).$$

In particular, $L(\mathcal{O}_v) = [L(\mathcal{O}_v), G(\mathcal{O}_v)]$ implies that for every $k \in \mathbb{N}$, we have

$$[N_v^k, G(\mathcal{O}_v)]N_v^{2k} = N_v^k$$

Now fix $n \in \mathbb{N}$. Note that we have

$$[N_v^n, G(\mathcal{O}_v)]N_v^{2n} = [N_v^n, G(\mathcal{O}_v)][N_v^{2n}, G(\mathcal{O}_v)]N_v^{4n}.$$

Hence an easy induction argument gives that for every $k > n$ we have $[N_v^n, G(\mathcal{O}_v)]N_v^k = N_v^n$ and this implies $[N_v^n, G(\mathcal{O}_v)] = N_v^n$. From ii) and Lemma 3.2.2 it follows that our initial assumptions hold for almost every $v \in V_f^S$ and the proof is complete.

For iv) note that i) implies that $[G(\mathcal{O}_v), G(\mathcal{O}_v)]N_v^1 = G(\mathcal{O}_v)$. But iii) implies that $[G(\mathcal{O}_v), N_v^1] = N_v^1$, hence $N_v^1 \subset [G(\mathcal{O}_v), G(\mathcal{O}_v)]$ and $[G(\mathcal{O}_v), G(\mathcal{O}_v)] = G(\mathcal{O}_v)$ for almost every $v \in V_f^S$.

$\square$

We are now ready to prove the following Proposition, which will be used for the proof of Theorem 3.4.

Proposition 3.2.1. *Let $\mathcal{P}$ be as in Lemma 3.2.5. There exists $\delta > 0$ such that for every $v \in \mathcal{P}$, every nontrivial irreducible representation of $G(\mathcal{O}_v)$ is of dimension at least q_v^δ.*

Proof. Pick δ as in Lemma 1.7.1, that is, every projective representation of a perfect central extension of a finite simple group of Lie type, say $H(\mathbb{F}_q)/Z(H(\mathbb{F}_q))$, has dimension at least q^δ. Suppose $v \in \mathcal{P}$ and take $\rho \in \mathrm{Irr}(G(\mathcal{O}_v))$. Let $\rho_{|N_v^1}$ be the restriction of ρ to N_v^1.

If $\rho_{|N_v^1}$ is trivial, that is, if $N_v^1 \subseteq \ker \rho$, we can see ρ as a representation of $G(\mathcal{O}_v)/N_v^1$. By Lemma 3.2.5.i) we can apply Lemma 1.7.1 to get $\dim \rho \geq q_v^\delta$.

Suppose now that there is a nontrivial $\mu \in \mathrm{Irr}(N_v^1)$ such that μ is a constituent of $\rho_{|N_v^1}$. Let $H \leq G(\mathcal{O}_v)$ be the stabilizer of μ. We claim that H is a proper subgroup of $G(\mathcal{O}_v)$. For suppose not, and let $k \in \mathbb{N}$ be maximal such that $\mu_{|N_v^k}$ is nontrivial. By assumption $[N_v^k, N_v^k] \subseteq N_v^{2k} \subseteq \ker \mu$. Hence any nontrivial constituent $\lambda \in \mathrm{Irr}(N_v^k)$ of $\mu_{|N_v^k}$ is linear. Indeed, there is only one such constituent, since $[N_v^k, N_v^1] \leq N_v^{k+1} \leq \ker \mu$ implies $N_v^k \subseteq Z(\mu)$, the center of μ, see [33, 2.26 and 2.27]. It follows that $G(\mathcal{O}_v)$ stabilizes λ. But since λ is linear this implies $[N_v^k, G(\mathcal{O}_v)] \subseteq \ker \lambda$. By lemma 3.2.5.iii), we have $N_v^k = [N_v^k, G(\mathcal{O}_v)]$, i.e., $N_v^k \subseteq \ker \lambda$. But λ is an arbitrary constituent of $\mu_{|N_v^k}$, thus $\mu_{|N_v^k}$ must be trivial, which contradicts our choice of k. Therefore $N_v^1 \leq H < G(\mathcal{O}_v)$. Now by Clifford's Theory (Lemma 3.1.6) , we know that ρ is induced from an irreducible representation $\tilde{\rho} \in \mathrm{Irr}(H)$, in particular $\dim \rho = \dim \tilde{\rho}|G(\mathcal{O}_v) : H|$. We can see H/N_v^1 as a subgroup of $G(\mathcal{O}_v)/N_v^1$ and by Lemma 3.2.5.i) we can apply Lemma 1.7.1 to obtain $|G(\mathcal{O}_v) : H)| \geq q_v^\delta$. It follows that $\dim \rho \geq q_v^\delta$ and the proof is complete. $\square$

Lemma 3.2.6. *For every $v \in V_f^S$, there exists $c > 0$ such that $G(\mathcal{O}_v)$ is of representation type c, i.e., $|G(\mathcal{O}_v)/K_n(G(\mathcal{O}_v))| \leq cn^c$ for every $n \in \mathbb{N}$. In particular $G(\mathcal{O}_v)$ has PRG.*

Proof. Recall that the group $G(\mathcal{O}_v)$ has a natural structure of k_v-analytic group. Hence there exists $H \leq_o G(\mathcal{O}_v)$ such that H is a $\mathcal{O}_v$-standard group. Since H, being an open subgroup of a profinite group, is a finite index subgroup, it suffices to show the claim for such a group H (Lemma 3.1.3). For char $k > 0$, H can be given the structure of an $\mathbb{F}_p[[t]]$-analytic group (Lemma 1.2.1) whose Lie algebra is finitely generated as an H-module by Lemma 3.2.2, so the result follows from Theorem 3.2. Analogously if char $k = 0$, then H can be given the structure of a compact p-adic analytic group for $p = \operatorname{char} \mathbb{F}_v$ (Lemma 1.2.1) with perfect Lie algebra L_G (G is a simple algebraic k-group and for char $k = 0$ this implies its Lie algebra is perfect). Thus the claim follows from Theorem 3.1. $\qquad \square$

Theorem 3.5. *There exists $c > 0$ such that for every $v \in V_f^S$, $G(\mathcal{O}_v)$ is of representation type c.*

Proof. Note that thanks to Lemma 3.2.6 it suffices to show that there exists $c > 0$ such that $G(\mathcal{O}_v)$ is of type c for almost every $v \in V_f^S$. Hence we want to give a polynomial bound for $|G(\mathcal{O}_v)/K_n(G(\mathcal{O}_v))|$ that holds for almost every $v \in V_f^S$. In particular, we may assume that $v \in \mathcal{P}$ (see Lemma 3.2.5 for the definition of $\mathcal{P}$).

Consider $\rho \in \operatorname{Irr}_{\leq n}(G(\mathcal{O}_v))$ and put $r' = \lceil \log_{q_v} n \rceil$. We claim that there exist $c_1, c_2 \in \mathbb{N}$ such that for almost every $v \in V_f^S$ we have $N_v^{c_1 r' + c_2} \subseteq \ker \rho$, in particular,

$$N_v^{c_1 r' + c_2} \subseteq K_n(G(\mathcal{O}_v)).$$

This will finish the proof, for we would have

$$|G(\mathcal{O}_v)/K_n(G(\mathcal{O}_v))| \leq |G(\mathcal{O}_v)/N_v^{c_1 r' + c_2}| = |G(\mathcal{O}_v)/N_v^1||N_v^1/N_v^{c_1 r' + c_2}|.$$

From our initial embedding $\iota : G \to \operatorname{GL}_N$ it follows that $G(\mathcal{O}_v)/N_v^1$ embedds in $\operatorname{GL}_N(\mathbb{F}_v)$ and this implies $|G(\mathcal{O}_v)/N_v^1| \leq q_v^{N^2}$. On the other hand the group N_v^1 is $\mathcal{O}_v$-standard, hence $|N_v^k/N_v^{k+1}| = q_v^{\dim G}$ for every k and we have $|N_v^1/N_v^{c_1 r' + c_2}| \leq q_v^{(c_1 r' + c_2)\dim G}$. Finally note that for $v \in \mathcal{P}$, Proposition 3.2.1 gives $q_v \leq n^{1/\delta}$. All together this implies

$$|G(\mathcal{O}_v)/K_n(G(\mathcal{O}_v))| \leq q_v^{N^2} q_v^{(c_1 r' + c_2)\dim G} \leq n^{c_1 \dim G + (c_2 \dim G + N^2)/\delta}$$

for every $v \in \mathcal{P}$, as we required.

To prove the claim let us first observe that since N_v^1 is a normal subgroup of $G(\mathcal{O}_v)$, it suffices to show

$$N_v^{c_1 r' + c_2} \subseteq K_n(N_v^1).$$

Indeed, suppose $\rho \in \operatorname{Irr}(G(\mathcal{O}_v))$ and let $\rho' \in \operatorname{Irr}(N_v^1)$ be an irreducible constituent of $\rho_{|N_v^1}$. Then we would have $N_v^{c_1 r' + c_2} \subseteq \ker \rho'$, and being normal, $N_v^{c_1 r' + c_2} \subseteq \ker \operatorname{Ind}_{N_v^1}^{G(\mathcal{O}_v)} \rho'$, which by Frobenious reciprocity has ρ as an irreducible constituent. Hence $N_v^{c_1 r' + c_2} \subset \ker \rho$ as we required. To prove the claim we will follow the proof of Theorem 3.2.

Recall that for every $v \in \mathcal{P}$, N_v^1 is a standard subgroup of the $\mathcal{O}_v$-analytic group $G(\mathcal{O}_v)$ with associated Lie algebra $L(\mathcal{O}_v)$. Hence, we have a homeomorphism from N_v^1 to $\pi_v L(\mathcal{O}_v)$ given by

$$
\begin{array}{ccc}
N_v^1 & \to & \pi_v L(\mathcal{O}_v) \\
g & \mapsto & \mathbf{g},
\end{array}
$$

where π_v stands for a uniformizer of the local ring $\mathcal{O}_v$. Let us denote the adjoint action of N_v^1 by $\mathrm{Ad}_v = \mathrm{Ad}_{\mathcal{O}_v} : N_v^1 \to \mathrm{Aut}_{\mathcal{O}_v}(L(\mathcal{O}_v))$. Recall that for every $k \in \mathbb{N}$, N_v^k/N_v^{2k} is an abelian normal subgroup of N_v^1/N_v^{2k}, where N_v^1 acts by conjugation and we have an isomorphism of N_v^1-modules $N_v^k/N_v^{2k} \cong L(\mathcal{O}_v)/\mathfrak{m}_v^k L(\mathcal{O}_v)$ given by

$$
\begin{array}{ccc}
N_v^k/N_v^{2k} & \to & L(\mathcal{O}_v)/\pi_v^k L(\mathcal{O}_v) \\
g & \mapsto & \pi_v^{-k} \mathbf{g},
\end{array}
\tag{3.3}
$$

see the proof of Theorem 3.1. For every $v \in V_f^S$, let us write A_v for the $\mathcal{O}_v$-subalgebra of $\mathrm{End}_{\mathcal{O}_v} L(\mathcal{O}_v)$ generated by $\{\mathrm{Ad}_v(g) : g \in N_v^1\}$ and for every subset $H \subseteq G(\mathcal{O}_v)$ let $I_v(H)$ denote the left ideal of A_v generated by $\{\mathrm{Ad}_v(h) - \mathrm{Id} \; : \; h \in H\}$. We will write $I_{v,k}$ for the ideal $I_v(N_v^k)$.

We will state and prove a series of claims that are required for the proof.

Claim 1. For every $v \in V_f^S$, $[L(\mathcal{O}_v), N_v^1]$ has finite index in $L(\mathcal{O}_v)$.

This is Lemma 3.2.2.

Claim 2. There exists $s \in \mathbb{N}$ such that for almost every $v \in V_f^S$ and every $k > 0$, we have

$$
\mathfrak{m}_v^{sk} L(\mathcal{O}_v) \subseteq [\mathfrak{m}_v^k L(\mathcal{O}_v), N_v^k] = \mathfrak{m}_v^k L(\mathcal{O}_v) \, I_{v,k} \, .
$$

Since G is an algebraic group, the map $\mathrm{Ad} - \mathrm{id}$ is a morphism of algebraic varieties given by

$$
\begin{array}{ccc}
L \times G & \to & L \\
(l \;,\; g) & \mapsto & [l, g] \\
(l_1, \ldots, l_d) \;,\; (g_1, \ldots, g_{N^2}) & \mapsto & (f_1(l_1, \ldots, l_d, g_1, \ldots, g_{N^2}), \\
& & \ldots, \\
& & f_d((l_1, \ldots, l_d, g_1, \ldots, g_{N^2})),
\end{array}
$$

where $d = \dim G$, we have chosen a basis for L such that $(l_1, \ldots, l_d)$ are the coordinates of l and $(g_1, \ldots, g_{N^2})$ stand for the usual coordinates induced from the embedding $G \hookrightarrow \mathrm{GL}_N$. Moreover, the f_i are polynomials with coefficients in $\mathcal{O}_S$ (note that G is an affine group $\mathcal{O}_S$-scheme), which give the coordinates of $[l, g]$ in L with respect to the chosen basis. Note that Ad_v is given by the same polynomials for every $v \in V_f^S$.

Put $\mathbf{x} = (x^1, \ldots, x^d)$, where $x^j = (x_1^j, \ldots, x_d^j)$, $\mathbf{y} = (y^1, \ldots, y^d)$, where $y^j = (y_1^j, \ldots, y_{N^2}^j)$ and similarly for $\mathbf{l} \in (L(\mathcal{O}_v))^d$, $\mathbf{g} \in (N_v^1)^d$. By abuse of notation we will identify elements of $L(\mathcal{O}_v)$ and $G(\mathcal{O}_v)$ with their corresponding coordinates. Consider the matrix $M(\mathbf{x}, \mathbf{y}) = (m_{ij}(\mathbf{x}, \mathbf{y}))_{1 \leq i,j \leq d}$, where $m_{ij}(\mathbf{x}, \mathbf{y}) = f_i(x^j, y^j)$. Then $M(\mathbf{l}, \mathbf{g})$ represents the coordinates of d elements of the form $[l, g]$, where $l \in L(\mathcal{O}_v)$ and $g \in N_v^1$. Write $V(\mathbf{l}, \mathbf{g})$ for the $\mathcal{O}_v$-module generated by these d elements.

Note that for $\mathbf{l} \in (\mathfrak{m}_v^k L(\mathcal{O}_v))^d$ and $\mathbf{g} \in (N_v^r)^d$ we have $V(\mathbf{l}, \mathbf{g}) \subseteq [\mathfrak{m}_v^k L(\mathcal{O}_v), N_v^r]$. Moreover, we claim that there exists a pair $(\mathbf{l}, \mathbf{g}) \in (\mathfrak{m}_v^k L(\mathcal{O}_v))^d \times (N_v^r)^d$ such that equality holds. Indeed, $[\mathfrak{m}_v^k L(\mathcal{O}_v), N_v^k] \subseteq \mathfrak{m}_v^k L(\mathcal{O}_v)$ and $\mathfrak{m}_v^k L(\mathcal{O}_v)$ is a free $\mathcal{O}_v$-module of rank d generated by elements of the form $[l, g]$ for $l \in \mathfrak{m}_v^k L(\mathcal{O}_v)$ and $g \in N_v^r$. Since $\mathcal{O}_v$ is a local ring, this implies that $[\mathfrak{m}_v^k L(\mathcal{O}_v), N_v^r]$ is generated by at most d elements of the form $[l, g]$ where $l \in \mathfrak{m}_v^k L(\mathcal{O}_v)$, $g \in N_v^r$.

Now from Claim 1 it follows that $[L(\mathcal{O}_v), N_v^1]$ has finite index in $L(\mathcal{O}_v)$. Therefore, $[L(\mathcal{O}_v), N_v^1]$ is a free $\mathcal{O}_v$-module of rank d as well. But observe that $V(\mathbf{l}, \mathbf{g})$ is free of rank d if and only if $\det \mathrm{M}(\mathbf{l}, \mathbf{g}) \neq 0$. Hence, there must exist a pair $(\mathbf{l}, \mathbf{g}) \in (\mathfrak{m}_v L(\mathcal{O}_v))^d \times (N_v^1)^d$ such that $\det \mathrm{M}(\mathbf{l}, \mathbf{g}) \neq 0$. In particular $\det \mathrm{M}(\mathbf{x}, \mathbf{y})$ is a nontrivial polynomial with coefficients in $\mathcal{O}_S$. We can see this determinant as a regular function of the affine variety $L \times G$. Moreover, let us note that if we put $r = \mathrm{ord}_v(\det \mathrm{M}(\mathbf{l}, \mathbf{g}))$, then $\mathfrak{m}_v^r L(\mathcal{O}_v) \subseteq V(\mathbf{l}, \mathbf{g})$.

Therefore it suffices to show that there exists $s \in \mathbb{N}$ such that for almost every $v \in V_f^S$ and every $k \geq 1$, there exists a pair $(\mathbf{l_v^k}, \mathbf{g_v^k}) \in (\mathfrak{m}_v^k L(\mathcal{O}_v))^d \times (N_v^k)^d$ that satisfies $\mathrm{ord}_v(\det \mathrm{M}(\mathbf{l_v^k}, \mathbf{g_v^k})) = ks$. This follows from Lemma 3.2.8 below.

Claim 3. For every $u > s$ and for almost every $v \in V_f^S$, we have

$$N_v^{u+s} \leq [N_v^u, N_v^1].$$

Recall that we may assume $v \in \mathcal{P}$, in particular, we may assume that N_v^1 is a standard subgroup of $G(\mathcal{O}_v)$. From the previous claim it follows that $\pi_v^{u+s} L(\mathcal{O}_v) \leq [\pi_v^{u+1} L(\mathcal{O}_v), N_v^1]$. Hence, for $u > s$ the isomorphism (3.3) gives $N_v^{u+s} \leq [N_v^u, N_v^1] N_v^{2u}$. Applying induction on l as in Claim 1 in Theorem 3.2 we obtain that if $u > s$, then for every $l \geq 2u$, $N_v^{u+s} \leq [N_v^u, N_v^1] N_v^l$. Therefore $N_v^{u+s} \leq [N_v^u, N_v^1]$.

Claim 4. There exists $l \in \mathbb{N}$ such that for every $v \in V_f^S$, we have

$$\mathrm{I}_{v,1}^l \leq \pi_v \mathrm{A}_v.$$

Note that A_v is an $\mathcal{O}_v$-submodule of the finitely generated $\mathcal{O}_v$-module $\mathrm{End}_{\mathcal{O}_v}(L(\mathcal{O}_v))$. Since $\mathcal{O}_v$ is Noetherian, this implies that A_v is a finitely generated $\mathcal{O}_v$-module as well. In particular, by Nakayama Lemma $\mathrm{A}_v / \pi_v \mathrm{A}_v$ must be finite. Now note that from the description of the adjoint action (see (1.1) in 1.2.3) it follows that $\mathrm{Ad}(G) - \mathrm{Id} \subseteq \pi_v \mathrm{End}_{\mathcal{O}_v}(L(\mathcal{O}_v))$, which implies $\mathrm{I}_{v,1} \subseteq \pi_v \mathrm{End}_{\mathcal{O}_v}(L(\mathcal{O}_v))$, i.e., $\mathrm{I}_{v,1}^i \subseteq \pi_v^i \mathrm{End}_{\mathcal{O}_v}(L(\mathcal{O}_v))$. Thus $\mathrm{I}_{v,1}^i$ gives a strictly decreasing sequence of submodules, so there exists $l \in \mathbb{N}$ such that $\mathrm{I}_{v,1}^l \leq \pi_v A_v$. But note that since $\mathrm{End}_{\mathcal{O}_v}(L(\mathcal{O}_v))$ is generated by d^2 ($d = \dim G$) elements it suffices to take $l = d^2$, which is independent of v.

Claim 5. For every $u > s$ and for almost every $v \in V_f^S$, we have

$$\mathrm{I}_{v,u+s} \subseteq \mathrm{I}_{v,1} \mathrm{I}_{v,u} + \mathrm{I}_{v,u} \mathrm{I}_{v,1}.$$

If $g \in N_v^{u+s}$, then $g \in [N_v^u, N_v^1]$ for almost every $v \in V_f^S$ by Claim 3. Now apply the same argument as in Claim 3 of Theorem 3.2.

Claim 6. For every $u > s$ and for almost every $v \in V_f^S$ we have

$$\mathrm{I}_{v,u+s(2l-1)} \subseteq \pi_v \mathrm{I}_{v,u}.$$

Applying the previous claim $(2l-1)$ times we obtain

$$\mathrm{I}_{v,u+s(2l-1)} \subseteq \sum_{i+j=2l-1} \mathrm{I}^i_{v,1}\,\mathrm{I}_{v,u}\,\mathrm{I}^j_{v,1}\,.$$

It follows from Claim 4 that $\mathrm{I}_{v,u+s(2l-1)} \leq \pi_v\,\mathrm{I}_{v,u}$.

So far we have shown that the set of all $v \in V^S_f$ that satisfy all of the above claims is cofinite in V^S_f. Hence we may assume that all of the above claims hold for v. Consider now $\rho \in \mathrm{Irr}(N^1_v)$ and suppose that $N^{2(k-1)}_v \not\subseteq \ker\rho$ but $N^{2k}_v \subseteq \ker\rho$. We may assume that $k \geq s$, otherwise $N^{2s}_v \subseteq \ker\rho$ and we may add $2s$ to the constant c_2. Let $\lambda \in \mathrm{Irr}(N^k_v)$ be an irreducible constituent of $\rho_{|N^k_v}$ and let $H \leq N^1_v$ be the stabiliser of λ. Pick δ as in Lemma 1.7.1 and put $r := \lceil \log_{q_v} |N^1_v : H| \rceil$. Note that if $n = \dim\rho$ then $|N^1_v : H| \leq n$ by Lemma 3.1.6 and so $r \leq r'$.

Claim 7. Let $M \leq H$ and suppose $M \trianglelefteq G(\mathcal{O}_v)$. Put $m := \lceil \log_{q_v} |N^1_v : M| \rceil$. Then for almost every $v \in V^S_f$ we have $N^{s(2l-1)(\lceil \frac{m}{\delta}\rceil+1)} \leq H$.

For convenience we will put $c := s(2l-1)$. Consider the chain of subgroups

$$M \leq MN^{c(\lceil \frac{m}{\delta}\rceil+1)}_v \leq MN^{c\lceil \frac{m}{\delta}\rceil}_v \leq MN^{c(\lceil \frac{m}{\delta}\rceil-1)}_v \leq \ldots \leq MN^c_v.$$

Suppose that there is some equality in the above chain, say $MN^{c(i+1)}_v = MN^{ci}_v$ for some $1 \leq i \leq \lceil \frac{m}{\delta}\rceil$. From the previous equality and Claim 6 (see Claim 9 in Theorem 3.1 as well) it follows that

$$\mathrm{I}(M) + \mathrm{I}^{ci}_v = \mathrm{I}(M) + \mathrm{I}^{c(i+1)}_v = \mathrm{I}(M) + \pi_v\,\mathrm{I}^{ci}_v\,.$$

We can apply Nakayama Lemma to the above equality of $\mathcal{O}_v$-modules to obtain $\mathrm{I}^{ci}_v \leq \mathrm{I}(M)$. In particular, $L(\mathcal{O}_v)\,\mathrm{I}^{ci}_v \leq L(\mathcal{O}_v)\,\mathrm{I}(M)$. Therefore, the isomorphism (3.3) gives

$$[N^k_v, N^{ci}_v]N^{2k}_v \leq [N^k_v, M]N^{2k}_v.$$

In particular, N^{ci}_v stabilizes λ and $N^{c(\lceil \frac{m}{\delta}\rceil+1)}_v \leq N^{ci}_v \leq H$. We will show that there must be an equality in the chain. Suppose that all inequalities in the chain are strict. We claim that if $MN^{c(i+1)}_v < MN^{ci}_v$ then $|MN^{c(i+1)}_v : MN^{ci}_v| \geq q^\delta_v$. If this holds, then $|N^1_v : M| \geq \left(q^\delta_v\right)^{\lceil \frac{m}{\delta}\rceil+1} > q^m_v \geq |N^1_v : M|$, which contradicts the choice of m. Suppose then that $MN^{c(i+1)}_v < MN^{ci}_v$ and consider the following refinement.

$$MN^{c(i+1)}_v \leq MN^{c(i+1)-1}_v \leq MN^{c(i+1)-2}_v \leq \ldots \leq N^{ci}_v.$$

Then for some $c(i+1) \leq j \leq ci+1$ we have $MN^{j+1}_v < MN^j_v$. Note that since M is normal in $G(\mathcal{O}_v)$, $G(\mathcal{O}_v)$ acts by conjugation on the abelian group MN^j_v/MN^{j+1}_v. The action is non trivial, for $[G(\mathcal{O}_v), N^j_v] = N^j_v$ by 3.2.5.iii), but N^1_v does act trivially. Hence, MN^j_v/MN^{j+1}_v is a nontrivial $G(\mathcal{O}_v)/N^1_v$ module. By 3.2.5.i) we can apply Lemma 1.7.1 to obtain $|MN^j_v/MN^{j+1}_v| \geq q^\delta_v$, which finishes the proof.

Claim 8. For almost every $v \in V^S_f$ we have $N^{s(2l-1)\lceil \frac{dr}{\delta}\rceil+1}_v \leq H$.

Put $H' := \bigcap_{g \in G(\mathcal{O}_v)} H^g$, where $H^g := g^{-1}Hg$. Suppose $|G(\mathcal{O}_v) : H'| \leq |G(\mathcal{O}_v) : H|^d$, where $d = \dim G$. Then, since $H' \trianglelefteq G(\mathcal{O}_v)$ we can apply the previous claim to obtain $N_v^{s(2l-1)(\lceil \frac{dm}{\delta} \rceil + 1)} \leq H$. We claim that $H' = \bigcap_{g_1,\ldots,g_d} H^g$ for some $g_1,\ldots,g_d \in G(\mathcal{O}_v)$, which implies $|G(\mathcal{O}_v) : H'| \leq |G(\mathcal{O}_v) : H|^d$. Let us write $\mathrm{Irr}(N_v^k|N_v^{2k}) := \{\psi \in \mathrm{Irr}(N_v^k) \mid N_v^{2k} \subseteq \ker \psi\}$. Note that $\mathrm{Irr}(N_v^k|N_v^{2k}) \cong \mathrm{Irr}(N_v^k/N_v^{2k})$. Recall that $\lambda \in \mathrm{Irr}(N_v^k|N_v^{2k})$ and since $N_v^k \trianglelefteq G(\mathcal{O}_v)$ we have an action of $G(\mathcal{O}_v)$ in $\mathrm{Irr}(N_v^k)$. Indeed, $G(\mathcal{O}_v)$ acts on $\mathrm{Irr}(N_v^k|N_v^{2k})$ as well. It is clear that H^g is the stabiliser of λ^g under this action. Now by the isomorphism (of $G(\mathcal{O}_v)$-modules) (3.3) we obtain an isomorphism of $G(\mathcal{O}_v)$-modules

$$\mathrm{Irr}(N_v^k|N_v^{2k}) \cong \mathrm{Irr}(N_v^k/N_v^{2k}) \cong \mathrm{Irr}(L(\mathcal{O}_v)/\pi_v^k L(\mathcal{O}_v)).$$

We can give $\mathrm{Irr}(L(\mathcal{O}_v)/\pi_v^k L(\mathcal{O}_v))$ an $\mathcal{O}_v$-module structure given by $r\lambda(l) := \lambda(rl)$ for every $r \in \mathcal{O}_v, \lambda \in \mathrm{Irr}(L(\mathcal{O}_v)/\pi_v^k L(\mathcal{O}_v))$ and $l \in L(\mathcal{O}_v)$. Since the action of $G(\mathcal{O}_v)$ on $L(\mathcal{O}_v)$ is the adjoint action, this action is $\mathcal{O}_v$-linear and it follows that the $\mathcal{O}_v$-structure on $\mathrm{Irr}(L(\mathcal{O}_v)/\pi_v^k L(\mathcal{O}_v))$ is compatible with the $G(\mathcal{O}_v)$-action. It is then clear that for $g \in G(\mathcal{O}_v)$ and $\lambda \in \mathrm{Irr}(L(\mathcal{O}_v)/\pi_v^k L(\mathcal{O}_v))$, g stabilizes λ if and only if g stabilizes $\langle \lambda \rangle_{\mathcal{O}_v}$. Now $L(\mathcal{O}_v)/\pi_v^k L(\mathcal{O}_v)$ is an $\mathcal{O}_v$-module of rank d and so is $\mathrm{Irr}(L(\mathcal{O}_v)/\pi_v^k L(\mathcal{O}_v))$. It follows that for $\lambda \in \mathrm{Irr}(L(\mathcal{O}_v)/\pi_v^k L(\mathcal{O}_v))$, $\langle \lambda^g : g \in G(\mathcal{O}_v) \rangle_{\mathcal{O}_v}$ is an $\mathcal{O}_v$-submodule generated by $\lambda^{g_1}, \ldots, \lambda^{g_d}$ for some $g_1, \ldots, g_d \in G(\mathcal{O}_v)$, which finishes the proof.

We are finally ready to prove our very first claim. Recall that $r := \lceil \log_{q_v} |N_v^1 : H| \rceil$ and let us set $c' := \lceil \frac{d}{\delta} \rceil$. Suppose that $k \geq s^2(2l-1)(c'r+1) + 3$. Then it follows from Claim 2 that

$$\pi_v^{s^2(2l-1)(c'r+1)} L(\mathcal{O}_v) \, \mathrm{I}_{v,1} \leq L(\mathcal{O}_v) \, \mathrm{I}_{v,s(2l-1)(c'r+1)} \, .$$

Now from Claim 3 and isomorphism (3.3), we obtain

$$N_v^{k+s^2(2l-1)(c'r+1)+s} \leq [N_v^{k+s^2(2l-1)(c'r+1)}, N_v^1]N_v^{2k} \leq [N_v^k, N_v^{s(2l-1)(c'r+1)}]N_v^{2k}.$$

However, since $N_v^{s(2l-1)(c'r+1)} \leq H$ (Claim 8), we must have

$$N_v^{k+s^2(2l-1)(c'r+1)} \leq \ker \lambda.$$

But recall that $N_v^{2(k-1)} \not\leq \ker \lambda$, hence $2k - 2 \leq k + s^2(2l-1)(c'r+1)$, or equivalently, $k \leq s^2(2l-1)(c'r+1) + 2$, which contradicts our assumption. Therefore we must have $k \leq s^2(2l-1)(c'r+1)$, so there exist c_1, c_2 such that

$$N_v^{c_1 r' + c_2} \leq N_v^{c_1 r + c_2} \leq K_n(N_v^1),$$

which finishes the proof. $\square$

We are finally ready to Prove Theorem 3.4.

Proof of Theorem 3.4. We want to show that $G(\widehat{\mathcal{O}}_S) \cong \prod_{v \in V_f^S} G(\mathcal{O}_v)$ has polynomial representation growth. Let us consider the set of valuations $\mathcal{P}$, see Lemma 3.2.5. We can write

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

Recall that by Lemma 3.2.6 $G(\mathcal{O}_v)$ has PRG for every $v \in V_f^S$. As $\mathcal{P}$ is confinite in V_f^S, the first term is a finite product of groups each of which having PRG and hence it has itself PRG (Lemma 3.1.7). Therefore it suffices to show that the second term in the above isomorphism has PRG.

Let ρ be an irreducible n-dimensional representation of $\prod_{v \in \mathcal{P}} G(\mathcal{O}_v)$. Then $\rho \cong \rho_1 \otimes \ldots \otimes \rho_t$, where ρ_i is an n_i-dimensional irreducible representation of $G(\mathcal{O}_{v_i})$ for some $v_i \in \mathcal{P}$ and $n_1 \ldots n_t = n$. By 3.2.5.iv) $n_i > 1$ and by Lemma 3.2.9 below there are at most n^d possible configurations of the form $(n_1, \ldots, n_t)$ such that $n_1 \ldots n_t = n$. Given such a configuration $(n_1, \ldots, n_t)$, the number of valuations v_i such that $G(\mathcal{O}_{v_i})$ has a nontrivial representation of dimension n_i is bounded by $n_i^{b/\delta}$ (Proposition 3.2.1 and Lemma 1.1.1). Hence the number of choices for $(v_1, \ldots, v_t)$ is bounded by $\prod n_i^{b/\delta} = n^{b/\delta}$. Now given $(n_1, \ldots, n_t)$ and $(v_1, \ldots, v_t)$, we know that $G(\mathcal{O}_{v_i})$ has at most cn_i^c irreducible representations of dimension n_i (Theorem 3.5). Therefore $\prod_{v \in \mathcal{P}} G(\mathcal{O}_v)$ has at most $n^d n^{b/\delta} c^{\log n} n^c$ irreducible n-dimensional representations. In particular, it has polynomial representation growth, which finishes the proof.

$\square$

Auxiliary results

We present here some auxiliary results that we use in the proofs of the results of the previous section. Lemma 3.2.7 is needed for Lemma 3.2.8, which is the final step of Claim 2 in Theorem 3.5.

Lemma 3.2.7. *Let $f = f(x_1, \ldots, x_n)$ be a nontrivial polynomial with coefficients in a finite field $\mathbb{F}$. Put $d = \max\{\deg_{x_i} f : 1 \le i \le n\}$. If $|\mathbb{F}| > d$, then there exists $\mathbf{y_0} \in \mathbb{F}^n$ such that $f(\mathbf{y_0}) \ne 0$.*

Proof. We will apply induction on the number of variables n.

For $n = 1$ it is clear that the polynomial f can have at most d solutions, which implies the claim.

Now suppose the lemma holds for $n - 1$ variables. We may see $f(x_1, \ldots, x_n) = f(x_n)(x_1, \ldots, x_n)$ as a polynomial in 1 variable with coefficients in $\mathbb{F}(x_1, \ldots, x_{n-1})$ and of degree at most d. This polynomial can have at most d solutions in $\mathbb{F}$. Hence, there exists $y_n \in \mathbb{F}$ such that $f(y_n)(x_1, \ldots, x_{n-1})$ is a nontrivial polynomial with coefficients in $\mathbb{F}$ and of degree at most d. By induction, there exist $y_1, \ldots, y_{n-1} \in \mathbb{F}$ such that $f(y_n)(y_1, \ldots, y_{n-1})$ is nonzero. Then, setting $\mathbf{y_0} = (y_1, \ldots, y_n)$, we have $f(\mathbf{y_0}) \ne 0$ and we are done. $\square$

Lemma 3.2.8. *Given $\mathcal{O}_S[\mathbb{A}^n] := \mathcal{O}_S[x_1, \ldots, x_n]$, put $\tilde{I} := \langle x_1, \ldots, x_n \rangle \lhd \mathcal{O}_S[\mathbb{A}^n]$ and consider a radical prime ideal $J \lhd \tilde{I}$ such that $\mathcal{O}_S[X] := \mathcal{O}_S[\mathbb{A}^n]/J$ is a finitely generated reduced $\mathcal{O}_S$-algebra. Suppose $\mathcal{O}_S[X] \otimes k$ gives an affine k-variety and we further assume that this variety is smooth. For every $\mathcal{O}_S$-algebra R let us write $X(R) = \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_S[X], R)$ for the "R-points" of $\mathcal{O}_S[X]$.*

Suppose that $f \in I = \tilde{I}/J \lhd \mathcal{O}_S[X]$ is non trivial. Then there exists $s \in \mathbb{N}$ such that for almost every $v \in V_f^S$ and every $k \ge 1$ there exists $x_v^k \in X(\mathfrak{m}_v^k)$ with $\mathrm{ord}_v(f(x_v^k)) = ks$.

Proof. The affine k-algebra $k[X] := \mathcal{O}_S(X) \otimes_{\mathcal{O}_S} k$ determines an affine algebraic variety defined over k, which, by construction, is embedded in the affine space $\mathbb{A}^n$. By abuse of notation we will denote this algebraic variety by X. Suppose that $J = \langle g_1, \ldots, g_r \rangle$, let l_i be the linear component (in terms of the x_i's) of g_i and write $L = \langle l_1, \ldots, l_r \rangle \lhd \mathcal{O}_S[\mathbb{A}^n]$ for the ideal generated by the l_i in $\mathcal{O}_S[\mathbb{A}^n]$. Then $k[\mathcal{T}_0(X)] := (\mathcal{O}_S[\mathbb{A}^n]/L) \otimes_{\mathcal{O}_S} k$ is an affine k-algebra which determines the tangent space of X at 0.

The ring $\mathcal{O}_S[X]$ is a Noetherian domain, so we have $\bigcap I^n = 0$ ([2, Corollary 10.18]). Hence, there exists s such that $f \in I^s \setminus I^{s+1}$. Pick $\tilde{f} \in \tilde{I}^s \setminus \tilde{I}^{s+1}$ such that $\pi(\tilde{f}) = f$, where π is the natural projection $\pi : \mathcal{O}_S[\mathbb{A}^n] \to \mathcal{O}_S[X]$, and let $\tilde{h}$ be the homogeneous component of degree s of $\tilde{f}$. We claim that $\tilde{h} \notin L$. Indeed, suppose that $\tilde{h} = \sum l_i m_i$. Then $\tilde{h}' := \sum (g_i - l_i) m_i \in \tilde{I}^{s+1}$ and $\tilde{f}' := \tilde{f} - \tilde{h} + \tilde{h}' \in \tilde{I}^{s+1}$. But note that $\pi(\tilde{h}) = \tilde{h}'$, hence $\pi(\tilde{f}) = \pi(\tilde{f}') = f$, which implies $f \in I^{s+1}$, a contradiction.

Now for every prime ideal $p_v \subseteq \mathcal{O}_S$ we have a reduction map $\tilde{r}_v : \mathcal{O}_S[\mathbb{A}^n] \to \mathbb{F}_v[\mathbb{A}^n] := \mathcal{O}_S[\mathbb{A}^n] \otimes_{\mathcal{O}_S} \mathcal{O}_S/p_v$ and analogously for $\mathcal{O}_S[X] \to \mathbb{F}_v[X_v] := \mathcal{O}_S[X] \otimes_{\mathcal{O}_S} \mathcal{O}_S/p_v$. We say that $\mathbb{F}_v[X_v]$ is the reduction modulo p_v of $\mathcal{O}_S[X]$. Since $\mathcal{O}_S[X]$ is a reduced domain, it follows that for almost every $v \in V_f^S$, $\mathbb{F}_v[X_v]$ is a reduced $\mathbb{F}_v$-algebra with no zero divisors. For those v, $\mathbb{F}_v[X]$ determines an affine algebraic variety defined over $\mathbb{F}_v$, which will be denoted by X_v, with tangent space at 0 given by the affine algebra

$$\mathbb{F}_v[\mathcal{T}_0(X_v)] =: (\mathcal{O}_S[\mathbb{A}^n]/L) \otimes_{\mathcal{O}_S} \mathcal{O}_S/p_v \cong \mathbb{F}_v[\mathbb{A}^n]/ \left(L \otimes_{\mathcal{O}_S} \mathcal{O}_S/p_v \right).$$

If we set $\tilde{h}_v = \tilde{r}_v(\tilde{h})$ and $L_v = \tilde{r}_v(L)$, since $\tilde{h} \notin L$ it follows that $\tilde{h}_v \notin L_v$ for almost every $v \in V_f^S$. It follows that $l(\tilde{h}_v)$, the image of $\tilde{h}_v$ in $\mathbb{F}_v[\mathcal{T}_0(X_v)]$, is non trivial.

Suppose that $\dim k[X] = d$, then since X is a smooth variety we have $\dim \mathcal{T}_0(X) = d$, hence $\dim \mathbb{F}_v[\mathcal{T}_0(X_v)] = d$ for almost every $v \in V_f^S$. Thus, for almost every $v \in V_f^S$ there is an $\mathbb{F}_v$-isomorphism $\rho_v : \mathbb{F}_v[\mathcal{T}_0(X_v)] \to \mathbb{F}_v[x_1, \ldots, x_d]$. By construction $\rho_v(l(\tilde{h}_v))$ is a polynomial of degree s. It follows now from Lemma 3.2.7, that for every v such that $|\mathbb{F}_v| > s$, there exists $\mathbf{y}_\mathbf{v}' \in \mathbb{F}_v^s$ such that $\rho_v(l(\tilde{h}_v))(y_v') \neq 0$, equivalently there exists $\mathbf{y}_\mathbf{v} \in \mathcal{T}_0(X_v)(\mathbb{F}_v)$ such that $\mathbf{y}_\mathbf{v}(l(\tilde{h}_v) \neq 0$, i.e., there exists $\mathbf{x}_\mathbf{v}^\mathbf{0} \in \mathbb{F}_v^n$ such that $\tilde{h}_v(\mathbf{x}_\mathbf{v}^\mathbf{0}) \neq 0$.

If we now reinterpret $\mathcal{T}_0(X_v)(\mathbb{F}_v)$ via dual numbers (for a ring R, $R[\epsilon] \cong R[x]/(x^2)$) and recall that $\mathbb{F}_v[X_v] = \mathcal{O}_S[X] \otimes \mathcal{O}_S/p_v$ we have natural bijections

$$
\begin{aligned}
\mathcal{T}_0(X_v)(\mathbb{F}_v) &= \mathrm{Hom}(\mathbb{F}_v[\mathcal{T}_0(X_v)], \mathbb{F}_v) \\
&\leftrightarrow \{\varphi \in \mathrm{Hom}_{\mathcal{O}_S}(\mathbb{F}_v[X_v], \mathbb{F}_v[\epsilon]) \ : \ \varphi(\tilde{r}_v(\tilde{I})) \subseteq \epsilon \mathbb{F}_v[\epsilon]\} \\
&\leftrightarrow \mathrm{Hom}_{\mathcal{O}_S}(\mathbb{F}_v[X_v], \mathfrak{m}_v^k/\mathfrak{m}_v^{k+1}) \\
&\leftrightarrow \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_S[X], \mathfrak{m}_v^k/\mathfrak{m}_v^{k+1}),
\end{aligned}
$$

where the bijections ($\leftrightarrow$) are induced by the evaluation maps at the x_i's. Recall now (the proof of) Lemma 3.2.4 and set $I_v = \langle p_v, I \rangle$ so that we have

$$\mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_S[X], \mathfrak{m}_v^k/\mathfrak{m}_v^{k+1}) \leftrightarrow \mathrm{Hom}_{\mathcal{O}_S}(\widehat{\mathcal{O}_S[X]}_{I_v}, \mathfrak{m}_v^k/\mathfrak{m}_v^{k+1}),$$

where $\widehat{\mathcal{O}_S[X]}_{I_v}$ denotes the completion of the ring $\mathcal{O}_S[X]_{I_v}$ with respect to its unique maximal ideal and the latter are assumed to be continous homomorphisms with respect to the I_v-adic topology. It follows from the proof of Lemma 3.2.4 that for almost

every $v \in V_f^S$ there is an isomorphism $\widehat{\mathcal{O}_S[X]}_{I_v} \cong \mathcal{O}_v[[y_1, \ldots, y_d]]$, which implies that $\text{Hom}_{\mathcal{O}_S}(\widehat{\mathcal{O}_S[X]}_{I_v}, \mathfrak{m}_v^k) \leftrightarrow (\mathfrak{m}_v^k)^d$ and so for those v's we have a projection

$$\text{Hom}_{\mathcal{O}_S}(\widehat{\mathcal{O}_S[X]}_{I_v}, \mathfrak{m}_v^k) \twoheadrightarrow \text{Hom}_{\mathcal{O}_S}(\widehat{\mathcal{O}_S[X]}_{I_v}, \mathfrak{m}_v^k/\mathfrak{m}_v^{k+1})$$

again induced by the evaluation maps at the x_i's under the corresponding homomorphisms.

Now, following the constructions, this gives for almost every $v \in V_f^S$ a point $x_v^k \in X(\mathfrak{m}_v^k)$ such that $f(x_v^k) \neq 0 \mod \mathfrak{m}_v^{k+1}$. But recall that $\tilde{h}$ has degree s, so $\text{ord}_v(f(x_v^k)) = ks$ as desired. $\square$

The following Lemma is used in the proof of Theorem 3.4.

Lemma 3.2.9 ([56, Lemma 4.7]). *Given $n \in \mathbb{N}$, define $f(n)$ to be the number of tuples $(n_1, \ldots, n_t)$ of integers such that $n_i > 0$ and $n = n_1 \ldots n_t$. Then there exists $d \in \mathbb{N}$ such that $f(n) \leq n^d$ for every $n \in \mathbb{N}$.*

Chapter 4

Subgroup Growth of Arithmetic Groups

4.1 Subgroup Growth

Given a group Γ let us write $a_n(\Gamma)$ for the number of subgroups of Γ of index n and $s_n(\Gamma)$ for the number of subgroups of Γ of index at most n, i.e., $s_n(G) = \sum_{i=1}^{n} a_i(G)$. If Γ is a topological group, we will only consider closed subgroups. Note that if Γ is a profinite group and $H \leq \Gamma$ is a subgroup of finite index, then H is open if and only if it is closed. Hence, $s_n(\Gamma)$ equals the number of closed (equivalently open) subgroups of index at most n.

We recall some standard properties concerning subgroup growth in the following Lemma.

Lemma 4.1.1. *i) If $N \trianglelefteq \Gamma$,then $a_n(\Gamma/N) \leq a_n(\Gamma)$ and $s_n(\Gamma/N) \leq s_n(\Gamma)$.*

ii) If $H \leq \Gamma$ and $|\Gamma : H| = m$, then $a_n(H) \leq a_{mn}(\Gamma)$ and $s_n(H) \leq s_{mn}(\Gamma)$.

iii) Suppose $a_n(\Gamma)$ is finite, then $a_n(\Gamma) = a_n(\Gamma/N)$ for some finite index normal subgroup $N \trianglelefteq \Gamma$. In particular, $a_n(\Gamma) = a_n(\widehat{\Gamma})$, where $\widehat{\Gamma}$ denotes the profinite completion of Γ.

The following Lemma gives an upper bound for the subgroup growth of a finite group.

Lemma 4.1.2. *Let Γ be a finite group. Then $s_n(\Gamma) \leq |\Gamma|^{\log |\Gamma|}$.*

Proof. If $d(H)$ denotes the minimum number of generators of a group H, let us define the rank of G as

$$\mathrm{rk}(\Gamma) := \max\{d(H) \ : \ H \leq \Gamma\}.$$

Thus, every subgroup of Γ is generated by at most $\mathrm{rk}(\Gamma)$ element, so we have

$$s_n(\Gamma) \leq |\Gamma|^{\mathrm{rk}(\Gamma)}.$$

Moreover $\mathrm{rk}(\Gamma) \leq \log |\Gamma|$. Indeed, suppose $d(H) = r$ for some $H \leq \Gamma$, say $H = \langle h_1, \ldots, h_r \rangle$ and put $H_i := < h_1, \ldots, h_i >$. Then

$$|\Gamma| \geq |H| = |H_r : H_{r-1}| \ldots |H_2 : H_1||H_1| \geq 2^r.$$

Therefore $s_n(\Gamma) \leq |\Gamma|^{\mathrm{rk}(\Gamma)} \leq |\Gamma|^{\log |\Gamma|}$ as desired. $\qquad \square$

Lemma 4.1.3. *Let U be a finite index subgroup of Γ with $|\Gamma : U| = m$. Then for each k the number of subgroups H of Γ such that $U \leq H$ and $|H : U| \leq k$ is bounded by $m^{\log k}$.*

Proof. The maximal length of a chain of subgroups between U and H is at most $\log k$, so H can be generated by U and at most $\log k$ further elements. Moreover, note that for $u_1, \ldots, u_{\log k} \in U$ we have $\langle U, h_1, \ldots, h_{\log k} \rangle = \langle U, u_1 h_1, \ldots, u_{\log k} h_{\log k} \rangle$ so the number of distinct subgroups of this form is at most $|\Gamma : U|^{\log k} = m^{\log k}$. $\qquad\square$

Lemma 4.1.4. *Let H be a finite index subgroup of Γ such that $|\Gamma : H| = m$. Then for each $n \in \mathbb{N}$ we have*

$$s_n(\Gamma) \leq (mn)^{\log m} s_n(H).$$

Proof. To each subgroup $S \leq \Gamma$ we associate the subgroup $S \cap H$. If $|\Gamma : S| \leq n$, then $|H : (H \cap S)| \leq n$ as well. Suppose that $U \cap H = S \cap H$, then $|U : (H \cap S)| \leq m$. By the previous lemma the number of such possible U is bounded by $(mn)^{\log m}$, so we have

$$s_n(\Gamma) \leq (mn)^{\log m} s_{nm}(H).$$

$\qquad\square$

Lemma 4.1.5. *Suppose Γ_1 and Γ_2 are commensurable subgroups of a group Γ. Then $s_n(\Gamma_1) \leq n^{D_1 \log n}$ for some $D_1 \in \mathbb{R}_{\geq 0}$ if and only if $s_n(\Gamma_2) \leq n^{D_2 \log n}$ for some $D_2 \in \mathbb{R}_{\geq 0}$.*

Proof. This follows by repeated applications of the inequalities in 4.1.2 and 4.1.4 to the groups Γ_1, Γ_2 and $\Gamma_1 \cap \Gamma_2$. $\qquad\square$

The following lemmata explain how one can obtain information on the subgroup growth of a group from its representation growth.

Lemma 4.1.6. *Let Γ be a group. If Γ is of representation type c, i.e., $|\Gamma : K_n(\Gamma)| \leq n^c$, then $s_n(\Gamma) \leq n^{c^2 \log n}$.*

Proof. i) Let $H \leq \Gamma$ be a subgroup of index at most n. Then Γ permutes the right cosets of H by right multiplication. The associated permutation representation $\rho : \Gamma \to \mathrm{GL}_{|\Gamma:H|}(\mathbb{C})$ is of degree $|\Gamma : H| \leq n$. It follows that $K_n(\Gamma) \subseteq \ker \rho \subseteq H$. This is true for any such H, so we obtain

$$|\Gamma : \bigcap_{|\Gamma:H| \leq n} H| \leq |\Gamma : K_n(\Gamma)| \leq n^c.$$

If we set $S_n := \bigcap_{|\Gamma:H| \leq n} H$, it follows that $S_n \subseteq H$ for any subgroup $H \leq \Gamma$ of index at most n and we have $s_n(\Gamma) = s_n(\Gamma/S_n)$. Now Γ/S_n is a finite group of order at most n^c and we can apply Lemma 4.1.2 to obtain

$$s_n(\Gamma) = s_n(\Gamma/S_n) \leq (n^c)^{\log n^c} = n^{c^2 \log n}.$$

$\qquad\square$

Lemma 4.1.7. *Let Γ be a profinite group with Polynomial Representation Growth, say, $r_n(\Gamma) \leq n^c$. Then for every subgroup $P \leq \Gamma$ of index at most n we have $|P : \overline{[P,P]}| \leq n^{c+1}$.*

Proof. Note that $|P : \overline{[P,P]}| = r_1(P)$. On the other hand, since $|\Gamma : P| \leq n$, by Lemma 3.1.3 we have $r_1(P) \leq n r_n(\Gamma) \leq n^{c+1}$. $\qquad\square$

4.2 CSP and Subgroup Growth of Arithmetic Groups

In this section we show how Theorem 3.4 can be used to obtain results on subgroup growth of arithmetic groups. Let k be a global field and fix $S \subset V_k$ a finite set of valuations which is assumed to be non-empty if char $k > 0$. We aim at proving the following Theorem.

Theorem 4.1. *Let G be a simply connected almost simple k-group. Let $\Gamma \leq G$ be an S-arithmetic subgroup and suppose that G has the weak Congruence Subgroup Property with respect to S. Then there exists a constant $D > 0$ such that $s_n(\Gamma) \leq n^{D \log n}$.*

If Γ is an S-arithmetic group of G, then it is commensurable with $G(\mathcal{O}_S)$. By Lemma 4.1.5 we may assume $\Gamma = G(\mathcal{O}_S)$. We can apply the same scheme of reductions as in section 3.2 by using Lemma 4.1.5 instead of Lemma 3.1.3 to show that we may assume that G is a connected simply connected absolutely almost simple k-group with Strong Approximation.

Recall that since G has wCSP with respect to S, the map

$$\pi : \widehat{G(\mathcal{O}_S)} \twoheadrightarrow G(\widehat{\mathcal{O}}_S).$$

has finite kernel. Thus, there exists a finite index subgroup $\Gamma' \leq \widehat{G(\mathcal{O}_S)}$ that embedds in $G(\widehat{\mathcal{O}}_S)$ as a finite index subgroup. Therefore repeated applications of Lemma 4.1.5 allow us to obtain Theorem 4.1 as a consequence of the following Theorem.

Theorem 4.2. *Let G be a connected simply connected absolutely almost simple k-group. Then there exists a constant D such that*

$$s_n(G(\widehat{\mathcal{O}}_S)) \leq n^{D \log n}.$$

Hence, we are reduced to the study of the subgroup growth of the group $G(\widehat{\mathcal{O}}_S) = \prod_{v \in V_f^S} G(\mathcal{O}_v)$.

We obtain the following Corollary as direct application of Theorem 3.5 and Lemma 4.1.6.

Corollary 4.2.1. *There exists $d > 0$ such that for every $v \in V_f^S$ we have*

$$s_n(G(\mathcal{O}_v)) \leq n^{d \log n}.$$

To prove Theorem 4.2 we basically follow [1] and apply Lemma 4.1.7 in the final step. The following Proposition is [54, Proposition 4.3]. Let us note that in [54] G is assumed to be split, however the same argument works without this assumption.

Theorem 4.3. *Let G be as in Theorem 4.2. If H is a subgroup of index n in $G(\widehat{\mathcal{O}}_S)$, then H contains a sub-normal subgroup of $G(\widehat{\mathcal{O}}_S)$ of index at most n^{d_1} for some constant d_1.*

The following Proposition describes the subnormal subgroups of the local factors $G(\mathcal{O}_v)$ for $v \in \mathcal{P}$ (see Lemma 3.2.5 for the definition of $\mathcal{P}$).

Proposition 4.2.1. *Let $\mathcal{P}$ be as in Lemma 3.2.5. Then for every $v \in \mathcal{P}$ the following hold:*

i) If H is a subnormal subgroup of $G(\mathcal{O}_v)$ such that $HN_v^1 = G(\mathcal{O}_v)$ then $H = G(\mathcal{O}_v)$.

ii) Let Z_v denote the inverse image in $G(\mathcal{O}_v)$ of the center of $G(\mathcal{O}_v/\mathfrak{m}_v)$. If H is a proper subnormal subgroup of $G(\mathcal{O}_v)$ then $H \leq Z_v$.

Proof. i) A proper sub-normal subgroup is contained in a proper normal subgroup, so we may assume that H is normal in $G(\mathcal{O}_v)$. By Lemma 3.2.5.iii), we know that $[N_v^k, G(\mathcal{O}_v)] = N_v^k$ for every k. We claim that $N_v^1 \subseteq HN_v^k$ for every $k \geq 1$. The claim implies that $N_v^1 \subseteq H$ (recall that we assume H to be closed) and hence $H = HN_v^1 = G(\mathcal{O}_v)$ as required.

To prove the claim it suffices to show that $N_v^k \subseteq HN_v^{k+1}$ for every $k \geq 1$. We know that $[N_v^k, G(\mathcal{O}_v)] = [N_v^k, HN_v^1] = N_v^k$. But note that $[N_v^k, HN_v^1] \subseteq [N_v^k, H][N_v^k, N_v^1] \subseteq HN_v^{k+1}$, which proves the claim.

ii) We may assume as above that H is a normal subgroup. By Lemma 3.2.5.i) the group $G(\mathbb{F}_v)/Z(G(\mathbb{F}_v)) \cong G(\mathcal{O}_v)/Z_v$ is a finite simple group. Hence, a proper normal subgroup H either satisfies $HZ_v = G(\mathcal{O}_v)$, whence $H = G(\mathcal{O}_v)$ by i), or $H \leq Z_v$. $\qquad\square$

We can now derive some properties of subnormal subgroups in the global case.

Proposition 4.2.2. *Let H be an open subnormal subgroup of $G(\widehat{\mathcal{O}}_S)$ of index n. Let $\mathcal{P}$ as in Lemma 3.2.5 and define $V(H) := \{v \in \mathcal{P} \mid H \cap G(\mathcal{O}_v) \neq G(\mathcal{O}_v)\}$. Then for every $v \in V(H)$ we have*

$$H \cap G(\mathcal{O}_v) \leq Z_v$$

and there exists a constant d_2 such that

$$\sum_{v \in V(H)} \log q_v \leq \frac{1}{d_2} \log n.$$

Proof. Let $v \in V_f^S$. By definition and Proposition 4.2.1.ii), if $v \in \mathcal{P} \setminus V(H)$, then $G(\mathcal{O}_v) \subseteq H$. On the other hand if $v \in V(H)$, then by Proposition 4.2.1.ii) we have $H \cap G(\mathcal{O}_v) \leq Z_v$. Moreover we claim that $\pi_v(H) \leq Z_v$, where π_v denotes the projection from $G(\widehat{\mathcal{O}}_S)$ to $G(\mathcal{O}_v)$. Note that to prove the claim we may assume that H is a normal subgroup. But for H normal, if $\pi_v(H) = G(\mathcal{O}_v)$ then $H \cap G(\mathcal{O}_v) = G(\mathcal{O}_v)$, since $G(\mathcal{O}_v)$ is a perfect group (Lemma 3.2.5.iv)). We have shown that

$$\prod_{v \in \mathcal{P} \setminus V(H)} G(\mathcal{O}_v) \subseteq H \subseteq \prod_{v \in V_f^S \setminus V(H)} G(\mathcal{O}_v) \times \prod_{v \in V(H)} Z_v.$$

Therefore, if we write $Z(H) := \prod_{v \in V(H)} Z_v$ and $E := \prod_{v \in V_f^S \setminus \mathcal{P}} G(\mathcal{O}_v)$, we may see H as a subgroup of $Z(H) \times E$.

Let us put $\widetilde{G} := \prod_{v \in V(H)} G(\mathcal{O}_v) \times E$. On the one hand $M := |E : \prod_{v \in V_f^S \setminus \mathcal{P}} G(\mathfrak{m}_v)|$ is independent of H. On the other hand $|Z(H) : \prod_{v \in V(H)} G(\mathfrak{m}_v)|$ is negligible compared to $|\prod_{v \in V(H)} G(\mathcal{O}_v) : \prod_{v \in V(H)} G(\mathfrak{m}_v)|$. Let us write

$$\widetilde{G}(1) := \prod_{v \in V(H) \cup (V_f^S \setminus \mathcal{P})} G(\mathfrak{m}_v).$$

Since $|\widetilde{G} : Z(H) \times E| \leq |\widetilde{G} : H|$ we can find a constant d_1' (independent of H) such that $|\widetilde{G} : \widetilde{G}(1)| \leq n^{d_1'}$.

Now note that $|\widetilde{G} : \widetilde{G}(1)|$ is approximately $M \prod_{v \in V(H)} q_v^{d_2'}$, where $d_2' = \dim G$. Moreover we also have

$$\prod_{v \in V(H)} q_v^{d_2} \leq |\widetilde{G} : H| \leq n^{d_1},$$

where d_2 is a constant slightly less than d_2'. In particular, we have

$$\sum_{v \in V(H)} \log q_v \leq \frac{1}{d_2} \log n \tag{4.1}$$

$\square$

We can finally give a proof of Theorem 4.2.

Proof of Theorem 4.2. Let H be an open subgroup of $G(\widehat{\mathcal{O}}_S)$ of index at most n. By Theorem 4.3 and (the proof of) Proposition 4.2.2 there exist constants d_1, d_2 (independent of H), a subnormal subgroup H' and a finite set of valuations $V(H')$ such that

$$|G(\widehat{\mathcal{O}}_S) : H'| \leq n^{d_1},$$

$$|\widetilde{G} : \widetilde{G}(1)| \leq n^{d_1},$$

$$\prod_{v \in \mathcal{P} \setminus V(H')} G(\mathcal{O}_v) \subseteq H' \subseteq \prod_{v \in V_f^S \setminus V(H')} G(\mathcal{O}_v) \times \prod_{v \in V(H')} Z_v,$$

$$\sum_{v \in V(H')} \log q_v \leq \frac{1}{d_2} \log n^{d_1},$$

where $\widetilde{G} = \prod_{v \in V(H')} G(\mathcal{O}_v) \times E$ and $\widetilde{G}(1) = \prod_{v \in V(H') \cup (V_f^S \setminus \mathcal{P})} G(\mathfrak{m}_v)$ are as in Proposition 4.2.2. Then, for fixed $V(H')$, by Lemma 4.1.3 we can reduce the problem to counting subgroups H of index at most n in the group $\widetilde{G}$. By [55, Proposition 1.3.2] we know that

$$s_n(\widetilde{G}) \leq s_n(\widetilde{G}/\widetilde{G}(1)) s_n(\widetilde{G}(1)) n^{\mathrm{rk}(\widetilde{G}/\widetilde{G}(1))} \tag{4.2}$$

where $\mathrm{rk}(\widetilde{G}/\widetilde{G}(1))$ is the maximal cardinality of a minimal generating set of a subgroup of $\widetilde{G}/\widetilde{G}(1)$. Clearly

$$\mathrm{rk}(\widetilde{G}/\widetilde{G}(1)) \leq \log |\widetilde{G}/\widetilde{G}(1)| \leq \log n^{d_1} = d_1 \log n.$$

Applying Lemma 4.1.2 to the finite group $\widetilde{G}/\widetilde{G}(1)$ we obtain

$$s_n(\widetilde{G}/\widetilde{G}(1)) \leq n^{d_1 \log n^{d_1}} = n^{d_1^2 \log n}.$$

To prove the appropriate bound for $s_n(\widetilde{G}(1))$ we apply Lemma 4.1.7. By Theorem 3.4 $G(\widehat{\mathcal{O}}_S)$ has PRG, say $r_n(G(\widehat{\mathcal{O}}_S) \leq n^C$. By construction, it follows that $r_n(\widetilde{G}) \leq n^C$ as well.

Now given a subgroup $K \leq \widetilde{G}(1)$ such that $|\widetilde{G}(1) : K| \leq n$, we have $|\widetilde{G} : K| \leq n^{d_1+1}$. By Lemma 4.1.7 applied to K and $\widetilde{G}$ we get

$$|K : \Phi(K)| \leq (n^{d_1+1})^{C+1} \leq n^E \tag{4.3}$$

for some constant E, where $\Phi(K)$ denotes the Frattini subgroup of K. Now if P is a subgroup of the pro-p group $\widetilde{G}(1)$ of index at most n, find a sequence

$$\widetilde{G}(1) = K_0 \geq K_1 \geq \ldots \geq K_{\lfloor \log_p n \rfloor} = P$$

such that $|K_s : K_{s+1}| = 1$ or p. For every s, $K_s/\Phi(K_s)$ is an elementary abelian p-group which can be interpreted as an $\mathbb{F}_p$-vector space of dimension $d(K_s)$. By construction $\Phi(K_s) \leq K_{s+1}$, hence K_{s+1} can be interpreted as a subspace of codimension at most 1 in $K_s/\Phi(K_s)$. Hence given K_s the number of choices for K_{s+1} is

$$1 + \frac{p^{d(K_s)} - 1}{p - 1} \leq p^{d(K_s)} = |K_s : \Phi(K_s)| \leq n^E,$$

where the last inequality follows from (4.3). Hence the number of possibilities for P is at most $n^{E \log_p n} \leq n^{E_2 \log n}$ for some constant E_2.

If we substitute the above bounds in (4.2) we obtain

$$s_n(\widetilde{G}) \leq n^{d_1^2 \log n} n^{E_2 \log n} n^{d_1 \log n} \leq n^{d_3 \log n} \tag{4.4}$$

for some constant d_3.

We have found the appropriate bound for a fixed $V(H')$, so it remains to estimate the number of possible $V(H')$. Recall that $\sum_{v \in V(H')} \log q_v \leq \frac{1}{d_2} \log n^{d_1}$, in particular, $|V(H')| \leq \frac{d_1}{d_2} \log n$. On the other hand by Lemma 1.1.1 the number of valuations v with $q_v \leq n^{d_1/d_2}$ is bounded by n^{bd_1/d_2}. Therefore the number of possible subsets $V(H')$ is bounded by $n^{B \log n}$ for some constant B. This together with (4.4) gives

$$s_n(G(\widehat{\mathcal{O}}_S)) \leq n^{d_3 \log n} n^B \leq n^{D \log n}$$

for some constant D, which finishes the proof.

$\square$

Chapter 5

Algebra groups and the Fake Degree Conjecture

5.1 Introduction

The theory and results presented in this chapter are motivated by the so-called Fake Degree Conjecture. The Fake Degree Conjecture appears in the context of algebra groups, a class of groups introduced by Isaacs which can be seen as a generalization of unitriangular groups. It is natural to try to adapt Kirillov's Orbit Method for this class of groups and this was first made, under certain hypothesis, by Kazhdan. Kirillov's method suggests a correspondence between the so-called coadjoint orbits and the irreducible characters of the group under study. The Fake Degree Conjecture claims that in the class of algebra groups one can use this correspondence to read the irreducible character degrees from the square root of the sizes of the coadjoint orbits (the fake degrees).

To introduce the class of algebra groups let us first consider the group $U_n(\mathbb{F}_q)$, this is the group of unitriangular matrices of size $n \times n$ with coefficients in the finite field $\mathbb{F}_q$. The unitriangular groups and their representation theory have been object of study for several reasons. Let us note that for $p = \operatorname{char} \mathbb{F}_q$ the group $U_n(\mathbb{F}_q)$ is a Sylow p-subgroup of $\operatorname{GL}_n(\mathbb{F}_q)$. This implies that any p-group can be embedded in some $U_n(\mathbb{F}_q)$, for every finite group can be represented as a permutation matrix group in some $\operatorname{GL}_n(\mathbb{Z})$. The understanding of this class of groups may therefore give information about the family of p-groups. For instance, a lower bound for the number of conjugacy classes of $U_n(\mathbb{F}_p)$ produces an estimate for the number of isomorphism classes of p-groups of order p^n, see [29] and [84]. On the other hand, unitriangular groups have a rich representation theory. Indeed, classifying their irreducible representations is known to be a wild problem. Recent work on the representation theory of unitriangular groups can be found in [20].

The first trivial observation about the representation theory of $U_n(\mathbb{F}_q)$ is that, being a p-group, every irreducible representation has p-power degree. However it was soon observed that all known irreducible representations of $U_n(\mathbb{F}_q)$ have indeed q-power degree. The corresponding conjecture was publicize, among others, by Thompson and read as follows.

Conjecture 1. All irreducible representations of $U_n(\mathbb{F}_q)$ have q-power degree.

In 1977 D. Kazhdan gave in [43] a description of all irreducible characters of the groups $U_n(\mathbb{F}_q)$ in the case where $n \leq p$. Kazhdan adapted Kirillov's Orbit Method thanks to the fact that for $n \leq p$ the logarithm and exponential functions are well defined bijections between the unitriangular group $U_n(\mathbb{F}_q)$ and the strictly uppertriangular matrices $\mathfrak{u}_n(\mathbb{F}_q)$. In this setting we have a natural action of $U_n(\mathbb{F}_q)$ on $\mathfrak{u}_n(\mathbb{F}_q)$ and on its dual $\widehat{\mathfrak{u}_n(\mathbb{F}_q)} := \mathrm{Irr}((\mathfrak{u}_n(\mathbb{F}_q), +))$ (see section 5.2 for more details). For $\lambda \in \mathrm{Irr}(\mathfrak{u}_n(\mathbb{F}_q))$ let Ω_λ denote its corresponding $U_n(\mathbb{F}_q)$-orbit.

Theorem 5.1 ([43, Proposition 1]). *Suppose $n \leq p = \mathrm{char}\,\mathbb{F}_q$. For every $\chi \in \mathrm{Irr}(U_n(\mathbb{F}_q))$ there exists an $\mathbb{F}_q$-subalgebra $\mathfrak{h} \subset \mathfrak{u}_n(\mathbb{F}_q)$ and a linear character $\lambda \in \mathrm{Irr}(\exp(\mathfrak{h}))$ such that*

$$\chi = \lambda^{U_n(\mathbb{F}_q)} = \frac{1}{|\Omega_\lambda|^2} \sum_{\mu \in \Omega_\lambda} \mu \circ \log.$$

In particular, it follows that, for $n \leq p$, every irreducible representation of $U_n(\mathbb{F}_q)$ has degree $|U_n(\mathbb{F}_q)|/|\mathfrak{h}|$ (for some $\mathbb{F}_q$-subalgebra $\mathfrak{h} \subseteq \mathfrak{u}_n(\mathbb{F}_q)$), which is a q-power.

However, for arbitrary n the problem was open until 1995, when I.M. Isaacs presented a proof of a more general statement. In [34] Isaacs generalized the class of groups under study by introducing the concept of "algebra groups", which contains, in particular, the class of unitriangular groups.

Let R be a commutative ring with unit and let us consider a finite associative R-algebra J which is assumed to be nilpotent, i.e., $J^n = 0$ for some $n \in \mathbb{N}$. Let us consider the set of formal objects

$$1 + J := \{\, 1 + x \; : \; x \in J \,\}.$$

Then $1 + J$ is easily seen to be a group with respect to the natural multiplication $(1 + x)(1 + y) = 1 + x + y + xy$. In fact, $1 + J$ is a subgroup of the group of units of the algebra $A = R \cdot 1 + J$, in which J is the Jacobson radical. The group $1 + J$ constructed in this way is the R-algebra group based on J. It is clear that $U_n(\mathbb{F}_q) \cong 1 + \mathfrak{u}_n(\mathbb{F}_q)$, so unitriangular groups are algebra groups. This more general definition allowed Isaacs to apply inductive arguments to a broader class of groups. This way he obtained an affirmative answer to Conjecture 1.

Theorem 5.2 ([34, Theorem A]). *For every $\mathbb{F}_q$-algebra group P (and in particular for any untriangular group $U_n(\mathbb{F}_q)$) every irreducible representation of P has q-power degree.*

Isaacs's result and his new approach motivated further investigation of algebra groups. Theorem 5.2 can be interpreted as a partial generalization of Kazhdan's aforementioned result for certain unitriangular groups to the class of algebra groups. It was natural to study to what extend were Kazhdan's results in [43] extendible to the class of $\mathbb{F}_q$-algebra groups. In the algebra group setting there is a natural bijection given by $1 + x \mapsto x$ between the group $1 + J$ and the algebra J, which may be used to apply Kirillov's Orbit Method (see section 5.2 for more details). In this sense Halasi showed the following partial generalization of Theorem 5.1 to algebra groups.

Theorem 5.3 ([27, Theorem 1.2]). *Let $1 + J$ be an $\mathbb{F}_q$-algebra group and $\chi \in \mathrm{Irr}(1 + J)$. Then there exist an $\mathbb{F}_q$-algebra $H \leq J$ and a linear character $\lambda \in \mathrm{Irr}(1 + H)$ such that $\chi = \lambda^{1+J}$.*

Nevertheless, obtaining a explicit description of all irreducible characters of a given algebra group in terms of coadjoint orbits as in Theorem 5.1 is not possible (see section 5.2). However it was suggested that obtaining the irreducible character degrees might be possible in the following way. Note that in Theorem 5.1, for every $\chi \in \mathrm{Irr}(U_n(\mathbb{F}_q))$, $\chi(1) = |\Omega_\lambda|^{1/2}$ for some $\lambda \in \mathrm{Irr}(\mathfrak{u}_n(\mathbb{F}_q))$ and corresponding $U_n(\mathbb{F}_q)$-orbit Ω_λ. In the case of an algebra group $1 + J$ we similarly have a $(1+J)$-action on both J and $\widehat{J} := \mathrm{Irr}((J, +))$. Consider the list of integers obtained by taking the square roots of the sizes of the conjugation orbits of $1 + J$ on $\mathrm{Irr}(J)$. The sum of these numbers is $|J| = |1 + J|$ and the length of the list is the number of conjugacy classes of $1 + J$. In other words, this list of square roots of orbit sizes resembles the list of degrees of the irreducible characters of $1 + J$. In an unpublished set of notes circulated by Isaacs in 1997, these numbers were called the "fake character degrees" of the algebra group $1 + J$. It was suggested that perhaps they are always the actual irreducible character degrees. This has been later known as the Fake Degree Conjecture.

Conjecture 2 (Fake Degree Conjecture)*.* For every prime power q and every $\mathbb{F}_q$-algebra group $1 + J$ the irreducible character degrees of $1 + J$ coincide, counting multiplicities, with the square root of the cardinalities of the $(1 + J)$-orbits in $\mathrm{Irr}(J)$.

Note that an immediate corollary of this conjecture (see Lemma 5.3.1) is that the orders of $[J, J]_L$ and $[1 + J, 1 + J]$ have to be equal (we write $[a, b]_L = ab - ba$ for Lie brackets when necessary to avoid confusion with group commutators). Thus in order to understand Conjecture 2 one should first answer the following question.

Question 1. *Is it true that the size of $(1 + J)_{\mathrm{ab}}$, the abelianization of $1 + J$, coincides with the index of $[J, J]_L$ in J?*

In [36] Jaikin gave an explicit counterexample to the Fake Degree Conjecture by constructing an $\mathbb{F}_2$-algebra group that gives a negative answer to the above question. However, this approach was not sufficient to disprove the conjecture for odd characteristics. The particular behaviour of the prime $p = 2$ regarding character correspondences and computations for odd p suggested that the Fake Degree Conjecture might hold for algebra groups defined over fields of odd characteristic.

This was our motivation for looking at the following family of examples. Let π be a finite p-group. Given a ring R we will set I_R to be the augmentation ideal of the group ring $R[\pi]$. If we take $R = \mathbb{F}_q$, then $\mathrm{I}_{\mathbb{F}_q}$ is a nilpotent algebra and $1 + \mathrm{I}_{\mathbb{F}_q}$ is the group of normalized units of the modular group ring $\mathbb{F}_q[\pi]$. It is not difficult to see that the index of $[\mathrm{I}_{\mathbb{F}_q}, \mathrm{I}_{\mathbb{F}_q}]_L$ in $\mathrm{I}_{\mathbb{F}_q}$ is equal to $q^{\mathrm{k}(\pi)-1}$, where $\mathrm{k}(\pi)$ is the number of conjugacy classes of π (see Lemma 5.3.2). In section 5.3 we give a disproof for the Fake Degree Conjecture by showing that the aforementioned question cannot have a positive answer for every $\mathbb{F}_q$-algebra group. The disproof points out to a possible relation between $\mathrm{k}(\pi)$ and $(1 + \mathrm{I}_{\mathbb{F}_q})_{ab}$. Our next result describes this relation by determining the size of $(1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}}$, the abelianization of $1 + \mathrm{I}_{\mathbb{F}_q}$.

Theorem 5.4. *Let π be a finite p-group. Then*

$$|(1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}}| = q^{\mathrm{k}(\pi)-1}|\mathrm{B}_0(\pi)|.$$

The group $\mathrm{B}_0(\pi)$ that appears in the Theorem is the *Bogomolov multiplier* of π. It is defined as the subgroup of the Schur multiplier $\mathrm{H}^2(\pi, \mathbb{Q}/\mathbb{Z})$ of π consisting of the cohomology

classes vanishing after restriction to all abelian subgroups of π. The Bogomolov multiplier plays an important role in birational geometry of quotient spaces V/π as it was shown by Bogomolov in [17]. In a dual manner, one may view the group $B_0(\pi)$ as an appropriate quotient of the homological Schur multiplier $H_2(\pi, \mathbb{Z})$, see [64]. We were surprised to discover that, in this form, the Bogomolov multiplier had appeared in the literature much earlier in a paper of W. D. Neumann [66], as well as in the paper of B. Oliver [67] that plays an essential role in our proofs. The latter paper contains various results about Bogomolov multipliers that were only subsequently proved in the cohomological framework.

There are plenty of finite p-groups with nontrivial Bogomolov multipliers (see for example [41]). Thus we obtain explicit counterexamples to the Fake Degree Conjecture for all primes.

Our next result provides a conceptual explanation for the equality in Theorem 5.4. Note that multiplication and inversion in $1 + I_{\mathbb{F}_q}$ extend to $1 + I_{\mathbb{F}_q} \otimes R$ for every $\mathbb{F}_q$-algebra R. Hence we can associate to $(1 + I_{\mathbb{F}_q})$ an algebraic group G defined over $\mathbb{F}_q$. It is clear that G is a unipotent group. A direct calculation shows that the $\mathbb{F}_q$-Lie algebra L_G of G is isomorphic to $I_{\mathbb{F}_q}$. The derived subgroup G' of G is also a unipotent algebraic group defined over $\mathbb{F}_q$ ([12, Corollary I.2.3]), and so by [40, Remark A.3], $|G'(\mathbb{F}_q)| = q^{\dim G'}$. Note that in general we have only an inclusion

$$(1 + I_{\mathbb{F}_q})' = G(\mathbb{F}_q)' \subseteq G'(\mathbb{F}_q),$$

but not the equality.

Theorem 5.5. *Let π be a finite p-group and G the associated algebraic $\mathbb{F}_q$-group as above.*

1. *We have*
$$\dim G' = \dim_{\mathbb{F}_q}[L_G, L_G]_L = |\pi| - k(\pi).$$

   In particular,
$$|G(\mathbb{F}_q) : G'(\mathbb{F}_q)| = q^{k(\pi)-1}.$$

2. *For every $q = p^n$, we have*
$$G'(\mathbb{F}_q)/G(\mathbb{F}_q)' \cong B_0(\pi).$$

Our hope is that the second statement of the theorem would help better understand the structure of the Bogomolov multiplier. As an example of this reasoning, recall that a classical problem about the Schur multiplier asks what is the relation between the exponent of a finite group and of its Schur multiplier ([78]). Standard arguments reduce this question to the case of p-groups . It is known that the exponent of the Schur multiplier is bounded by some function that depends only on the exponent of the group ([63]), but this bound is obtained from the bounds that appear in the solution of the Restricted Burnside Problem and so it is probably very far from being optimal. Applying the homological description of the Bogomolov multiplier, it is not difficult to see that the exponent of the Schur multiplier is at most the product of the exponent of the group by the exponent of the Bogomolov multiplier. Thus, we hope that the following theorem would help obtain a better bound on the exponent of the Schur multiplier.

Theorem 5.6. *Let π be a finite p-group and G the associated algebraic $\mathbb{F}_p$-group associated to $1 + \mathrm{I}_{\mathbb{F}_p}$ as above. For every $q = p^n$, we have*

$$\exp \mathrm{B}_0(\pi) = \min\{m \mid G'(\mathbb{F}_q) \subseteq G(\mathbb{F}_{q^m})'\}.$$

5.2 Algebra groups and Kirillov's Orbit Method

Throughout this section we mainly follow [77]. Fix a prime p and let R be a commutative ring with unit and char $R = p$. Let us consider a finite associative R-algebra J and assume further that J is nilpotent, i.e. $J^n = 0$ for some $n \in \mathbb{N}$. We define the R-algebra group based on J as

$$1 + J = \{1 + j \ : \ j \in J\},$$

where group multiplication and inverse are given by

$$(1 + j)(1 + h) = 1 + j + h + jh,$$

$$(1 + j)^{-1} = \sum_{k=0}^{n-1}(-1)^k j^k.$$

Associativity of the algebra multiplication guarantees that the group operation is associative and thanks to the nilpotency of J the inverse operation is well defined. Note that $|J| = |1+J|$ and hence $1 + J$ is a finite p-group. Groups constructed in this manner are called R-algebra groups.

Let us note that given any finite associative R-algebra A, $1 + \mathrm{Rad}(A)$ is an R-algebra group. From now on we will take $R = \mathbb{F}_q$ (q being some p-power) and in this case J becomes an $\mathbb{F}_q$-vector space. Nevertheless, some of the results presented below hold for more general R. Let us present some examples of algebra groups that will be useful later on.

Example. Take $J = \mathfrak{u}_n(\mathbb{F}_q)$ be the strictly upper triangular matrices of size $n \times n$ with entries in $\mathbb{F}_q$. Then $1 + J = 1 + U_n(\mathbb{F}_q)$ is the unitriangular group of dimension n over $\mathbb{F}_q$.

Example. Let π be a finite p-group and consider the group algebra $\mathbb{F}_q[\pi]$. Let us write $\mathrm{I}_{\mathbb{F}_q[\pi]} := \ker(\mathbb{F}_q[\pi] \to \mathbb{F}_q)$ for the augmentation ideal. Then $\mathrm{Rad}\,\mathbb{F}_q[\pi] = \mathrm{I}_{\mathbb{F}_q[\pi]}$ and $1 + \mathrm{I}_{\mathbb{F}_q[\pi]}$ is an algebra group. Note that we can describe the units of $\mathbb{F}_q[\pi]$ as $(\mathbb{F}_q[\pi])^* \cong \mathbb{F}_q^* \times \left(1 + \mathrm{I}_{\mathbb{F}_q[\pi]}\right)$. For this reason $1 + \mathrm{I}_{\mathbb{F}_q[\pi]}$ is called the group of normalized units of $\mathbb{F}_q[\pi]$.

As explained in the introduction Isaacs introduced this class of groups motivated by Conjecture 1 on unitriangular groups. Isaac's Theorem 5.2 can be seen as a generalization of Kazhdan's results on unitriangular groups (Theorem 5.1). Kazhdan's work followed the spirit of Kirillov's Orbit Method. Kirillov presented in [44] a method to describe the irreducible unitary representations of a connected simply connected nilpotent Lie group N. If we denote by $\mathfrak{n}$ the Lie algebra of the Lie group N, the adjoint action on $\mathfrak{n}$ induces an N-action on $\hat{\mathfrak{n}}$, the unitary dual of $(\mathfrak{n}, +)$. Kirillov established a correspondence between N-orbits in $\hat{\mathfrak{n}}$ and irreducible unitary representations of N (up to isomorphism). Kirillov's Orbit Method has been applied to several class of groups, among others p-groups and pro-p

groups ([25], [30] and [37]), finitely generated nilpotent groups ([85]) and arithmetic groups ([5]), see [45] for a general discussion. We explain how to adapt Kirillov's Orbit Method to the class of $\mathbb{F}_q$-algebra groups and show that it works best for groups of nilpotency class strictly less than p.

Let J be as above and $1 + J$ the associated $\mathbb{F}_q$-algebra group. There is a natural action of $1 + J$ on J given by

$$a^{(1+b)} = (1 + b)^{-1}a(1 + b) \quad \text{for every } a, b \in J.$$

Note that this action is equivalent to the conjugation action of $1+J$ on itself, the equivalence being given by $a \mapsto 1+a$. The $(1+J)$-action on J, induces a $(1+J)$-action on $\widehat{J} := \text{Irr}(J, +)$, called the coadjoint action, given by

$$\lambda^{1+b}(a) = \lambda(a^{(1+b)^{-1}}) \text{ for every } \lambda \in \text{Irr}(J) \quad \text{and every } a, b \in J.$$

Let us write $\text{Fun}(1 + J)^{1+J}$ for the set of complex functions on $1 + J$ that are constant on conjugacy classes. From the above setting one can immediately construct an assignment

$$\begin{aligned} (1 + J)\text{-orbits in } \text{Irr}(J) &\rightarrow &\text{Fun}(1 + J)^{1+J} \\ \Omega &\mapsto &\chi_\Omega(1 + j) := |\Omega|^{-1/2} \textstyle\sum_{\lambda \in \Omega} \lambda(j), \end{aligned}$$

which associates to each coadjoint orbit Ω a class function of $1 + J$. The following Lemma states some remarkable properties of the functions χ_Ω.

Lemma 5.2.1. *Let J be as above and $1 + J$ the associated algebra group.*

i) The number of $(1 + J)$-orbits in J and in $\text{Irr}(J)$ equals $\text{k}(1 + J)$, the number of conjugacy classes of $1 + J$.

ii) Let Ω_1 and Ω_2 be two $(1 + J)$-orbits in $\text{Irr}(J)$. Then

$$\langle \chi_{\Omega_1}, \chi_{\Omega_2} \rangle = \begin{cases} 1 & \text{if } \Omega_1 = \Omega_2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. i) It was pointed out above that the $(1 + J)$-action on J is equivalent to the conjugation action of $1 + J$ on itself. Hence the number of $(1 + J)$-orbits in J equals $\text{k}(1+J)$. Now by the well known orbit-counting formula often known as Burnside's Lemma, the number of orbits of a $(1 + J)$-action equals the average number of fixed points of the elements of $1 + J$ in this action. Hence it suffices to show that an element $g \in 1 + J$ has the same number of fixed points in J and in $\text{Irr}(J)$.

Given $g \in 1+J$, note that the action of g on J is $\mathbb{F}_q$-linear, hence $f_g : J \to J, j \mapsto j^g - j$, is an $\mathbb{F}_q$-linear homomorphism. Now g fixes $\lambda \in \hat{J}$ if and only if $\lambda(j^g - j) = 0$ for every $j \in J$, i.e., if and only if $\text{im}\, f_g \subseteq \ker \lambda$. Since $\text{im}\, f_g$ is clearly a subgroup of $(J, +)$, the number of characters $\lambda \in \text{Irr}(J)$ vanishing in $\text{im}\, f_g$ equals $|J/\text{im}\, f_g|$. On the other hand, note that $j \in J$ is fixed by g if and only if $j \in \ker f_g$. Clearly $|\ker f_g| = |J/\text{im}\, f_g|$ and so the number of fixed points of g in J and $\text{Irr}(J)$ coincide.

ii) We claim that for every $\lambda, \phi \in \mathrm{Irr}(J)$, $\langle \lambda, \phi \rangle = 1$ if $\lambda = \phi$ and $\langle \lambda, \phi \rangle = 0$ otherwise. Indeed, note that every χ_Ω is the sum of the distinct $\lambda \in \Omega$ and the summands are disjoint for distinct orbits Ω, so orthogonality of irreducible characters proves the claim. The result is now clear. $\qquad \square$

It follows from Lemma 5.2.1 that $\{\chi_\Omega : \Omega \text{ is a } (1+J)\text{-orbit}\}$ is a set of $\mathrm{k}(1+J)$ orthonormal functions in $\mathrm{Fun}(1+J)^{1+J}$. It is tempting to think that this could be the set of irreducible characters of $1 + J$. However, note that $\chi_\Omega(1) = |\Omega|^{1/2}$. Thus for χ_Ω to be a character, the number of elements in every orbit must be a square. Computing the length of an orbit amounts to knowing the order of the stabilizer of any of its elements. The interplay between the algebra and group structures will allow us to obtain a nice description of the stabilizer of a given character $\lambda \in \mathrm{Irr}(J)$. At this point let us remark that together with the associative multiplication, the algebra J inherits a Lie algebra structure given by the bracket $[a, b] = ab - ba$.

Let us now introduce for every $\lambda \in \mathrm{Irr}(J)$ the form $B_\lambda : J \times J \to \mathbb{C}^*$ given by $(a, b) \mapsto \lambda([a, b])$. Put $\mathrm{Rad}\, B_\lambda := \{j \in J : B_\lambda(j, u) = 1 \ \forall u \in J\}$. We will say that B_λ is non-degenerate if $\mathrm{Rad}\, B_\lambda = 0$. For every $\mathbb{F}_q$-subspace $H \subseteq J$ we will write $H^\perp = \{j \in J : B_\lambda(j, h) = 1 \ \forall h \in H\}$ and we will call an $\mathbb{F}_q$-subspace $H \subseteq J$ isotropic if $H \subseteq H^\perp$.

The following Lemma states some important properties of the forms B_λ and explains how to use them to obtain the stabilizer of a character $\lambda \in \mathrm{Irr}(J)$.

Lemma 5.2.2. *Given $\lambda \in \mathrm{Irr}(J)$, let $B_\lambda : J \times J \to \mathbb{C}^*$ be as above. Then:*

i) $B_\lambda(u + v, w) = B_\lambda(u, w)B_\lambda(v, w)$, $B_\lambda(u, v + w) = B_\lambda(u, v)B_\lambda(u, w)$, $B_\lambda(ru, u) = 1$, $B_\lambda(ru, v) = B_\lambda(u, rv)$ *and* $B_\lambda(uv, w) = B_\lambda(u, vw)B_\lambda(v, wu)$ *for every* $u, v, w \in J$, $r \in \mathbb{F}_q$.

ii) *For every $\mathbb{F}_q$-linear subspace $H \subseteq J$, $H^\perp$ is an $\mathbb{F}_q$-linear subspace. In particular, $\mathrm{Rad}\, B_\lambda = J^\perp$ is an $\mathbb{F}_q$-linear subspace.*

iii) $\mathrm{St}_{1+J}(\lambda) = 1 + \mathrm{Rad}\, B_\lambda$.

iv) *If H is maximal isotropic $\mathbb{F}_q$-linear subspace, then $|J/H| = |H/\mathrm{Rad}\, B_\lambda|$. In particular $|J/\mathrm{Rad}\, B_\lambda| = |\Omega_\lambda|$ is a square.*

Proof. i) Since both λ and the Lie bracket are bilinear with respect to addition the first two equalities hold. For the third, note that the Lie bracket is $\mathbb{F}_q$-linear and hence $[ru, u] = r[u, u] = 0$ for every $u \in J$, $r \in \mathbb{F}_q$. From the previous equalities it follows that $B_\lambda(r(u + v), u + v) = B_\lambda(ru, v)B_\lambda(rv, u) = 1$ (in particular $B_\lambda(u, v)^{-1} = B_\lambda(v, u)$) for every $u, v \in J$, $r \in \mathbb{F}_q$. It follows that $B_\lambda(ru, v) = B_\lambda(rv, u)^{-1} = B_\lambda(u, rv)$. The last equality follows from the Jacobi identity of Lie algebras.

ii) For every $u, v \in H^\perp$ and $w \in H$, applying i) we have

$$B_\lambda(ru + v, w) = B_\lambda(ru, w)B_\lambda(v, w) = B_\lambda(u, rw)B_\lambda(v, w) = 1.$$

Hence $H^\perp$ is an $\mathbb{F}_q$-linear subspace.

iii) Let $g = 1 + u$ be an element of $1 + J$. Then g fixes λ if and only if for every $v \in J$, $\lambda(gvg^{-1}) = \lambda(v)$ or equivalently $\lambda(gvg^{-1} - v) = 0$. Since multiplication by g acts bijectively on J we may change v for vg in the above equality so this amounts to $\lambda(gv - vg) = \lambda(uv - vu) = \lambda([u,v]) = 0$ for every $v \in J$, i.e., $u \in \mathrm{Rad}_{B_\lambda}$.

iv) Let us first assume that $\mathrm{Rad}\, B_\lambda = 0$. Then B_λ induces an isomorphism:

$$\begin{array}{rccc} \phi: & (J, +) & \to & (\mathrm{Irr}(J), \cdot) \\ & j & \mapsto & B_\lambda^j: \quad \begin{array}{ccc} J & \to & \mathbb{C}* \\ u & \mapsto & B_\lambda(j, u) \end{array} \end{array}$$

Note that for an $\mathbb{F}_q$-subspace $H \subseteq J$, we have an isomorphism $\phi(H^\perp) \cong \mathrm{Irr}(J/H)$, in particular, $|H^\perp| = |J/H|$. If we assume H isotropic, then $H \subseteq H^\perp$. Moreover, equality holds precisely when H is a maximal isotropic subspace. Indeed, if $h \in H^\perp$ then $H + \mathbb{F}_q h$ is isotropic, hence $h \in H$. It follows that for H maximal isotropic we have $|H| = |J/H^\perp| = |J/H|$.

If $\mathrm{Rad}\, B_\lambda \neq 0$ then $\tilde{\lambda} : J/\mathrm{Rad}\, B_\lambda \times J/\mathrm{Rad}\, B_\lambda \to \mathbb{C}^*$ given by $(u + \mathrm{Rad}\, B_\lambda, v + \mathrm{Rad}\, B_\lambda) \mapsto \lambda([u,v])$ is a nondegenerate form and the claim easily follows from the previous claim. $\qquad\square$

The previous Lemma gives further evidence that the χ_Ω could be the irreducible characters of $1 + J$. Now since $1 + J$ is a finite p-group, by [34, Corollary 6.14] every irreducible character of $1 + J$ is induced from a linear character of a subgroup $N \leq 1 + J$. Hence it will be reasonable to try to obtain χ_Ω as the induced character of a linear character ψ of a subgroup $1 + H_\Omega$, where $H_\Omega \subseteq J$ is a subalgebra of index $|\Omega|^{1/2}$. Note that for $\lambda \in \Omega$, we have

$$\chi_\Omega(1 + u) = \sum_{g \in (1+J)/St_{1+J}(\lambda)} \lambda^g(u),$$

thus it will be natural to pick $\psi_\lambda \in \mathrm{Irr}(H_\Omega)$ such that $\psi_\lambda(1 + j) := \lambda(j)$.

However this approach has serious obstructions. One can easily observe that this will not work even for an abelian R-algebra J. Indeed, in this case, for any coadjoint orbit Ω, $|\Omega| = 1$, which would imply $H_\Omega = J$ for every Ω. But note that for ψ_λ to be a character we must have $\lambda(u+j) = \lambda(u)\lambda(j) = \psi_\lambda(1+u)\psi_\lambda(1+j) = \psi_\lambda(1+u+j+uj) = \lambda(u+j+uj) = \lambda(u+j)\lambda(uj)$ for every $u, j \in J$, that is $J^2 \subseteq \ker \lambda$. If this were to hold for every $\lambda \in \hat{J}$, then $J^2 = 0$ and this is certainly a very strong restriction which does not hold for every commutative $\mathbb{F}_q$-algebra J.

Nevertheless another approach is possible. Let us observe that the abovementioned strategy will make sense equally well if we set a correspondence of the form

$$\begin{array}{rcc} (1+J) - \text{orbits in } \mathrm{Irr}(J) & \to & \mathrm{Fun}(1+J)^{1+J} \\ \Omega & \mapsto & \chi_\Omega(e(j)) := \frac{1}{|\Omega|^{\frac{1}{2}}} \sum_{\lambda \in \Omega} \lambda(j), \end{array}$$

where $e : J \to 1 + J$ is any bijection preservig the $(1+J)$-actions. Observe that the assigment $j \mapsto 1 + j$ clearly satisfies this property. It is not clear how to find an alternative

map different from the obvious one, however if we assume that $J^p = 0$ (i.e. if $n \leq p$) we can consider the exponential map given by

$$
\begin{aligned}
\exp: \quad J &\to \quad 1 + J \\
j &\mapsto \quad \exp(j) = \sum_{k=0}^{n} \frac{j^k}{k!}
\end{aligned}
$$

Note that $(J, +)$ is a p-group and hence the map $j \mapsto \frac{j}{k}$ is to be considered as the inverse of the map $j \mapsto kj$, which is well defined. As usual, its inverse is given by the logaritm

$$
\begin{aligned}
\log: \quad 1 + J &\to \quad J \\
1 + j &\mapsto \quad \log(1 + j) = \sum_{k=1}^{n} (-1)^{k+1} \frac{j^k}{k}
\end{aligned}
$$

It is clear that both maps respect the $(1 + J)$-action on both J and $1 + J$. For the rest of the section we will assume that $J^p = 0$. We will show that, in this case, the outlined strategy works and we have a bijection

$$
\begin{aligned}
(1 + J)\text{-orbits in } \mathrm{Irr}(J) &\to \quad \mathrm{Irr}(1 + J) \\
\Omega &\mapsto \quad \exp(j) \mapsto \sum_{\lambda \in \Omega} \lambda(j) \\
& \qquad \quad 1 + j \mapsto \sum_{\lambda \in \Omega} \lambda(\log(1 + j))
\end{aligned}
$$

First let us recall that thanks to the universal Baker-Campbell-Hausdorff Formula (see [47, Lemma 9.15]), for every $u, j \in J$ we have $\exp(u) \exp(j) = \exp(u + j + \gamma(u, j))$, where $\gamma(u, j)$ is a sum of Lie words on the elements u and j. It follows that given $H_\lambda \subseteq J$ a subalgebra of index $|\Omega|^{1/2}$, $\exp(H_\lambda) = 1 + H_\lambda$ is a subgroup of $1 + J$ with the same index. Let us now define $\psi_\lambda(\exp(j)) = \lambda(j)$. Then for ψ_λ to be a linear character of $\exp(H_\lambda)$ we must have

$$
\begin{aligned}
\lambda(u + j) = \lambda(u)\lambda(j) &= \psi_\lambda(\exp(j))\psi_\lambda(\exp(u)) \\
&= \psi_\lambda(\exp(u + j + \gamma(u, j)) = \lambda(u + j + \gamma(u, j)).
\end{aligned} \tag{5.1}
$$

Thus, if $[H_\lambda, H_\lambda] \subseteq \ker \lambda$, then ψ_λ is a linear character of $\exp(H_\lambda)$. Therefore, to construct ψ_λ with the desires properties it suffices to find a maximal isotropic subalgebra with respect to B_λ. This is the content of the following Proposition.

Proposition 5.2.1. *Let $\lambda \in \mathrm{Irr}(J)$ and consider the form B_λ as above. Then there exists an $\mathbb{F}_q$-subalgebra H_λ such that H_λ is a maximal isotropic subspace of J.*

Proof. We will apply induction on $\dim_{\mathbb{F}_q} J$. The result is clear if B_λ is trivial. By refining the chain of ideals $\{0\} = J^p \subseteq J^{p-1} \subseteq \ldots J^2 \subseteq J$ we can obtain a chain of ideals

$$
\{0\} = J_{k+1} \subseteq J_k \subseteq \ldots \subseteq J_2 \subseteq J_1 = J
$$

such that J_i/J_{i+1} has dimension 1 for every $i \leq k$. Since B_λ is nontrivial, J is not isotropic, so there exists $i \leq k + 1$ such that J_i is isotropic but J_{i-1} is not. Note that $J_i \nsubseteq \mathrm{Rad}\, B_\lambda$, for J_i has codimension 1 in J_{i-1} and so the latter would be isotropic as well. Hence $J_i^\perp \subsetneq J$. Note that $J_i^\perp$ is a subalgebra (recall that $B_\lambda(uv, w) = B_\lambda(u, vw)B_\lambda(v, wu)$ by 5.2.2.i)). If we consider the restriction of B_λ to $J_i^\perp$ as a form on $J_i^\perp$, by induction there

exists a subalgebra $H_\lambda \subseteq J_i^\perp$ that is a maximal isotropic subspace of $J_i^\perp$. We claim that H_λ is a maximal isotropic subspace of J as well. Indeed, suppose $H_\lambda \subseteq U$ for some maximal isotropic subspace U. First note that $J_i \subseteq H_\lambda$ for H_λ is maximal within $J_i^\perp$ and $J_i + H_\lambda \subseteq J_i^\perp$ is isotropic. This implies $J_i \subseteq U$ and since U is isotropic, we have $U \subseteq J_i^\perp$. Since H_λ was maximal, this forces $H_\lambda = U$ and the claim follows. $\square$

It only remains to show that $\psi_\lambda^{1+J}(1+j) = \chi_\Omega(\exp(j))$, which will show that the latter is a character of $1 + J$. We will first need the following Proposition.

Proposition 5.2.2. *Let $\lambda, \phi \in \mathrm{Irr}(J)$ an consider a maximal isotropic subspace $H_\lambda \subseteq J$ for B_λ as in Proposition 5.2.1. Then $\phi_{|H_\lambda} = \lambda_{|H_\lambda}$ if and only if λ and ϕ are $1 + H_\lambda$ conjugate.*

Proof. Note first that by construction $(B_\lambda)_{|H_\lambda}$ is trivial and so by Lemma 5.2.2.iii) if $\lambda = \phi^g$ for some $g \in 1 + H_\lambda$, then for any $h \in H_\lambda$ we have

$$\lambda(h) = \phi^g(h) = \phi(h^{g^{-1}}) = \phi(h).$$

Now let Σ be the set of elements $\phi \in \mathrm{Irr}(J)$ such that $\lambda_{|H_\lambda} = \phi_{|H_\lambda}$, then $|\Sigma| = |J/H_\lambda|$. On the other hand, $1 + H_\lambda$ acts on Σ and the $(1 + H_\lambda)$-orbit of λ has size $|H_\lambda|/|\mathrm{St}_{1+J}(\lambda)| = |H_\lambda|/|\mathrm{Rad}\, B_\lambda| = |J/H_\lambda| = |\Sigma|$ by Lemma 5.2.2.iv). Therefore Σ is the $(1 + H_\lambda)$-orbit of λ and we are done. $\square$

Theorem 5.7. *Let $1 + J$ be an algebra group with $J^p = 0$. Consider $\lambda \in \mathrm{Irr}(J)$ and let Ω be its corresponding $(1 + J)$-orbit. Then*

$$\chi_{\Omega,\exp}(j) := \chi_\Omega(\exp(j)) = |\Omega|^{-1/2} \sum_{\lambda \in \Omega} \lambda(j)$$

is an irreducible character of $1 + J$. Moreover, all irreducible characters of $1 + J$ are of this form.

Proof. For a $(1 + J)$-orbit Ω take $\lambda \in \Omega$ and let H_λ be as in Proposition 5.2.1. By (5.1) the function ψ_λ given by $\psi_\lambda(\exp(j)) = \lambda(j)$ is an irreducible character of $1 + H_\lambda$. We claim that $\psi_\lambda^{1+J} = \chi_\Omega(\exp(j))$. This would show that $\chi_{\Omega,\exp}$ is a character of $1 + J$. Let us define $\widetilde{\psi}_\lambda : 1 + J \to \mathbb{C}$ that maps $1 + h \mapsto \psi_\lambda(1 + h)$ for $1 + h \in 1 + H_\lambda$ and vanishes elsewhere. By definition we have

$$\psi_\lambda^{1+J}(\exp(j)) = \frac{1}{|H_\lambda|} \sum_{g \in 1+J} \widetilde{\psi}_\lambda(\exp(j)^{g^{-1}}) = \frac{1}{|H_\lambda|} \sum_{g \in 1+J} \widetilde{\psi}_\lambda(\exp(j^{g^{-1}}))$$

$$= \frac{1}{|H_\lambda|} \sum_{\substack{g \in 1+J \\ j^{g^{-1}} \in H_\lambda}} \lambda(j^{g^{-1}})$$

Let us consider $\mathrm{Irr}(J/H_\lambda)$ and regard its elements as members of $\mathrm{Irr}(J)$. By orthogonality relations of irreducible characters we obtain $\sum_{\nu \in \mathrm{Irr}(J/H_\lambda)} \nu(j) = |J/H_\lambda|$ if $j \in H_\lambda$ and 0

otherwise. Hence, we can rewrite

$$\psi_\lambda^{1+J}(\exp(j)) = \frac{1}{|J|} \sum_{\substack{g\in 1+J \\ \nu\in\mathrm{Irr}(J/H_\lambda)}} \lambda(j^{g^{-1}})\nu(j^{g^{-1}}) = \frac{1}{|J|} \sum_{\substack{g\in 1+J \\ \nu\in\mathrm{Irr}(J/H_\lambda)}} (\lambda\nu)^g(j)$$

$$= \frac{1}{|J|} \sum_{\substack{g\in 1+J \\ \nu\in\Sigma}} \nu^g(j) = \frac{|\Sigma|}{|J|} \sum_{g\in 1+J} \lambda^g(j),$$

where Σ is the set of $\nu \in \mathrm{Irr}(J)$ such that $\nu_{|H_\lambda} = \lambda_{|H_\lambda}$ and we have $|\Sigma| = |H_\lambda|/|\mathrm{Rad}\, B_\lambda|$, see (the proof of) Proposition 5.2.2. Now recall that $\mathrm{St}_{1+J}(\lambda) = 1 + \mathrm{Rad}\, B_\lambda$ by Lemma 5.2.2.iii), so we obtain

$$\psi_\lambda^{1+J}(\exp(j)) = \frac{|\Sigma|}{|J|} \sum_{g\in 1+J} \lambda^g(j) = \frac{|\mathrm{St}_{1+J}(\lambda)|}{|H_\lambda|} \sum_{\mu\in\Omega_\lambda} \mu(j) = |\Omega_\lambda|^{-1/2} \sum_{\mu\in\Omega_\lambda} \mu(j).$$

Therefore $\chi_{\Omega,\exp}$ is indeed a character. So we obtain $\mathrm{k}(1 + J)$ characters of the form $\chi_{\Omega,\exp}$ which, applying the same idea as in Lemma 5.2.1.ii), are irreducible, whence the Theorem. $\qquad\square$

By using the Lazard Correspondence one can extend Theorem 5.7 to the class of p-groups of nilpotency class less than p, see [77]. Nevertheless the approach presented above is more convenient for our results. In general it is not possible to extend Theorem 5.7 to algebra groups where J^p is not necessarily equal to 0. Indeed, suppose that J is an $\mathbb{F}_p$-algebra, then by construction of χ_Ω all character values of χ_Ω lie in $\mathbb{Q}(\xi)$ where ξ is a nontrivial p^{th} root of unity. This would force all character values to be real if $p = 2$. A well known result from Character Theory says that if χ takes real values for every $\chi \in \mathrm{Irr}(1+J)$ then every element $g \in 1 + J$ is conjugate to its inverse. However, one can find $\mathbb{F}_2$-algebra groups where the last condition does not hold, see [35].

Note that in Theorem 5.7, the character degrees are given by $|\Omega_\lambda|^{1/2}$. So even though Kirillov's Orbit Method cannot provide all of the irreducible characters, it might be possible that one can obtain the irreducible character degrees by looking at the size of the coadjoint orbits $|\Omega_\lambda|$. This is the content of the Fake Degree Conjecture, which we present in the following section.

5.3 The Fake Degree Conjecture: a disproof

Kirillov's corespondence between $(1 + J)$-orbits in $\mathrm{Irr}(J)$ and $\mathrm{Irr}(1 + J)$ suggests a correspondence

$$\begin{array}{ccc} (1 + J) - \text{orbits in } \mathrm{Irr}(J) & \to & \{\chi(1) : \chi \in \mathrm{Irr}(1 + J)\} \\ \Omega & \mapsto & |\Omega|^{\frac{1}{2}} \end{array}$$

The Fake Degree Conjecture suggests that this correspondence is well defined and gives a bijection counting multiplicities for every algebra group $1 + J$. To show that the Fake

Degree Conjecture is false, we will focus on linear characters. The correspondence then restricts to a bijection between linear characters of $1 + J$ and fixed points of $\mathrm{Irr}(J)$ under the coadjoint action of $1 + J$. The idea of the proof is to show that this leads to a contradiction.

Lemma 5.3.1. *Let J be a finite dimensional nilpotent algebra over a finite field $\mathbb{F}$. Then the number of fixed points in $\mathrm{Irr}(J)$ under the coadjoint action of $1 + J$ equals the index of $[J, J]_L$ in J. In particular if the Fake Degree Conjecture holds,*

$$|J/[J,J]_L| = |(1 + J)_{\mathrm{ab}}|. \tag{5.2}$$

Proof. By Lemma 5.2.2.iii), $\lambda \in \mathrm{Irr}(J)$ is fixed under the coadjoint action of $1 + J$ if and only if $\mathrm{Rad}\, B_\lambda = J$, which amounts to $\lambda([J,J]_L) = 0$. It is now clear that the number of fixed points in $\mathrm{Irr}(J)$ equals the number of linear forms vanishing on $[J, J]_L$ and hence if the Fake Degree Conjecture holds

$$|J/[J,J]_L| = |\{\text{fixed points of } \mathrm{Irr}(J)\}| = |\mathrm{Lin}(1 + J)| = |(1 + J)_{\mathrm{ab}}|.$$

$\square$

The following family of examples will prove to be key for the study of the equality (5.2). Let π be a finite p-group and $\mathbb{F}_q[\pi]$ the group algebra over the finite field $\mathbb{F}_q$. The augmentation ideal

$$\mathrm{I}_{\mathbb{F}_q} := \{\sum_{h \in \pi} c_h h \ : \sum_{h \in \pi} c_h = 0\}$$

coincides with the Jacobson radical $\mathrm{Rad}\,\mathbb{F}_q[\pi]$ of $\mathbb{F}_q[\pi]$ and hence it is a nilpotent ideal. We can then consider the algebra group $1 + \mathrm{I}_{\mathbb{F}_q}$, these are the normalized units of $\mathbb{F}_q[\pi]$. If the Fake Degree Conjecture holds, we know

$$|[1 + \mathrm{I}_{\mathbb{F}_p}, 1 + \mathrm{I}_{\mathbb{F}_q}]| = |[\mathrm{I}_{\mathbb{F}_q}, \mathrm{I}_{\mathbb{F}_q}]_L|.$$

The following Lemma gives a relation between the size of $[\mathrm{I}_{\mathbb{F}_q}, \mathrm{I}_{\mathbb{F}_q}]_L$ and the number of conjugacy classes of the group π.

Lemma 5.3.2. *Let π be a finite group and F a field. Then*

$$\dim_{\mathrm{F}} \mathrm{I}_{\mathrm{F}} / [\mathrm{I}_{\mathrm{F}}, \mathrm{I}_{\mathrm{F}}]_L = \mathrm{k}(\pi) - 1.$$

Proof. It is clear that the set π is an F-basis for $\mathrm{F}[\pi]$. We first claim that

$$\dim_{\mathrm{F}} \mathrm{F}[\pi]/[\mathrm{F}[\pi], \mathrm{F}[\pi]]_L = \mathrm{k}(\pi).$$

Let $x_1, \ldots, x_{\mathrm{k}(\pi)}$ be representatives of conjugacy classes of π. Observe that for any $x, y, g \in \pi$ with $y = g^{-1}xg$, we have $x - y = [g, g^{-1}x]_L$. The elements $\bar{x}_1, \ldots, \bar{x}_{\mathrm{k}(\pi)}$ therefore span $\mathrm{F}[\pi]/[\mathrm{F}[\pi], \mathrm{F}[\pi]]_L$.

Set λ_i to be the linear functional on $\mathrm{F}[\pi]$ that takes the value 1 on the elements corresponding to the conjugacy class of x_i and vanishes elsewhere. Observe that for any $g, h \in \pi$, we have $[g, h]_L = g(hg)g^{-1} - hg$ and hence each λ_i induces a linear functional

on $F[\pi]/[F[\pi], F[\pi]]_L$. Now if $\sum_j \alpha_j \bar{x}_j = 0$ for some $\alpha_j \in F$, then $\alpha_i = \lambda_i(\sum_j \alpha_j \bar{x}_j) = 0$ for each i. It follows that $\bar{x}_1, \ldots, \bar{x}_{k(\pi)}$ are also linearly independent and hence a basis. This proves the claim.

Now, it is clear that $\{g - 1 : g \in \pi \setminus \{1\}\}$ is an F-basis for I_F. Since for any $g, h \in \pi$, we have $[g, h]_L = [g - 1, h - 1]_L$, it follows that $[F[\pi], F[\pi]]_L = [I_F, I_F]_L$, whence the lemma. $\square$

As an immediate consequence of the above results we obtain

Proposition 5.3.1. *Let π be a finite p-group and $I_{\mathbb{F}_q}$ the augmentation ideal of $\mathbb{F}_q[\pi]$. If the Fake Degree Conjecture holds, then for any finite p-group π,*

$$|1 + I_{\mathbb{F}_q}/[1 + I_{\mathbb{F}_q}, 1 + I_{\mathbb{F}_q}]| = |I_{\mathbb{F}_q}/[I_{\mathbb{F}_q}, I_{\mathbb{F}_q}]_L| = q^{k(\pi)-1}.$$

Theorem 5.8. *The Fake Degree Conjecture is false for any prime p.*

Proof. Let us assume that the Fake Degree Conjecture holds for $\mathbb{F}_p$-algebra groups for some prime p. Take the p-group

$$\pi := \langle x_1, x_2, x_3, x_4 : x_i^p = [x_j, x_k, x_l] = 1 \text{ for all } i, j, k, l \in \{1, 2, 3, 4\}\rangle.$$

Consider the element $z := [x_1, x_2][x_3, x_4] \in Z(\pi)$ and write $\widetilde{\pi} := \pi/\langle z \rangle$. We denote by $I_{\mathbb{F}_p}$ the augmentation ideal of $\mathbb{F}_p[\pi]$ and by $\widetilde{I}_{\mathbb{F}_p}$ the augmentation ideal of $\mathbb{F}_p[\widetilde{\pi}]$. We will try to estimate $|1 + I_{\mathbb{F}_p}/[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}]|$. For this consider the series of subgroups

$$A_i := 1 + (z - 1)^i \mathbb{F}_p[\pi] \trianglelefteq 1 + I_{\mathbb{F}_p} , \ i \in \{1, \ldots, p - 1\}.$$

We then have:

$$|1 + I_{\mathbb{F}_p}/[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}]| = |1 + I_{\mathbb{F}_p}/A_1[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}]| \cdot$$
$$\prod_{i=1}^{p-1} |A_i[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}]/A_{i+1}[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}]|.$$

The first term is just $|1 + \widetilde{I}_{\mathbb{F}_p}/[1 + \widetilde{I}_{\mathbb{F}_p}, 1 + \widetilde{I}_{\mathbb{F}_p}]| = p^{k(\widetilde{\pi})-1}$, by the preceding Proposition. For the rest of the terms observe that we have isomorphisms:

$$A_i[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}]/A_{i+1}[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}] \cong A_i/(A_{i+1}[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}] \cap A_i).$$

Moreover we have an isomorphism of $1 + I_{\mathbb{F}_p}$-modules between A_i/A_{i+1} and $\mathbb{F}_p[\widetilde{\pi}]$, where $1 + I_{\mathbb{F}_p}$ acts naturally by conjugation and the isomorphism is given by $1 + (z - 1)x \mapsto \bar{x}$ for every $x \in \pi$. We observe that $1 + I_{\mathbb{F}_p}$ acts trivially on the quotient $A_i/(A_{i+1}[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}] \cap A_i)$ and hence $|A_i/(A_{i+1}[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}] \cap A_i)| \leq |\mathbb{F}_p[\widetilde{\pi}]/[\mathbb{F}_p[\widetilde{\pi}], 1 + I_{\mathbb{F}_p}]|$. However

$$[\mathbb{F}_p\widetilde{\pi}, 1 + I_{\mathbb{F}_p}] = [\mathbb{F}_p[\widetilde{\pi}], 1 + \widetilde{I}_{\mathbb{F}_p}] = [\mathbb{F}_p[\widetilde{\pi}], \widetilde{I}_{\mathbb{F}_p}]_L = [\widetilde{I}_{\mathbb{F}_p}, \widetilde{I}_{\mathbb{F}_p}],$$

since for every $h \in \widetilde{\pi}$ and $g \in 1 + \widetilde{I}_{\mathbb{F}_p}$ we have $h - h^g = [g^{-1}, gh]_L$. This in turn implies that for every $i \in \{1, \ldots, p - 1\}$ we have

$$|A_i/(A_{i+1}[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}] \cap A_i)| \leq |\mathbb{F}_p[\widetilde{\pi}]/[\mathbb{F}_p[\widetilde{\pi}], 1 + I_{\mathbb{F}_p}]|$$
$$= |\mathbb{F}_p[\widetilde{\pi}]/[\mathbb{F}_p[\widetilde{\pi}], \mathbb{F}_p[\widetilde{\pi}]]_L| = p^{k(\widetilde{\pi})}.$$

We can in fact sharpen this inequality for $i = 1$. Observe that $z = 1 + (z-1)1$ is a commutator and hence belongs to $A_2[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}] \cap A_1$, however $1 \notin [\mathbb{F}_p[\widetilde{\pi}], \mathbb{F}_p[\widetilde{\pi}]]_L$. Hence

$$|A_1/(A_2[1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}] \cap A_1)| \leq p^{\mathrm{k}(\widetilde{\pi})-1}.$$

Therefore we have shown the following inequality

$$|1 + I_{\mathbb{F}_p} / [1 + I_{\mathbb{F}_p}, 1 + I_{\mathbb{F}_p}]| \leq p^{p \, \mathrm{k}(\widetilde{\pi})-2}.$$

The following lemma establishes the relation between $\mathrm{k}(\pi)$ and $\mathrm{k}(\widetilde{\pi})$:

Lemma 5.3.3. *Let π and $\widetilde{\pi}$ be as above, then $\mathrm{k}(\pi) = p \, \mathrm{k}(\widetilde{\pi})$.*

Proof. Let $\{\overline{x^{h_0=1}}, \overline{x^{h_1}}, \ldots, \overline{x^{h_n}}\}$ be a conjugacy class in $\widetilde{\pi}$, where $\overline{x}$ stands for $x\langle z \rangle \in \widetilde{\pi}$. Let us show that $\{x, x_{h_1}, \ldots, x^{h_n}\}$ is a conjugacy class in π. If there exists $h \in \pi$ such that $x^h \notin \{x, x^{h_1}, \ldots, x^{h_n}\}$, then $x^h = x^{h_i} z^k$ for some $i \in \{0, \ldots, n\}$, $k \in \{1, \ldots, p-1\}$. Hence $x = x^{h_i h^{-1}} z^k$, which implies $z = [h_i h^{-1}, x^{1/k}]$, but z is not a simple commutator. Since x was an arbitrary representative of $\overline{x}$, it follows that $\overline{x}^{\widetilde{\pi}}$ splits into p distinct conjugacy classes of π. $\qquad\square$

Substituting this in the previous inequality we obtain

$$|1 + I_{\mathbb{F}_p} / [1 + I_{F_p}, 1 + I_{\mathbb{F}_p}]| \leq p^{\mathrm{k}(\pi)-2},$$

which contradicts the previous Proposition. $\qquad\square$

5.4 Abelianization of groups of units and the Bogomolov multiplier

Motivated by the results in the previous section, we want to better understand the groups $(1 + I_{\mathbb{F}_q})_{\mathrm{ab}}$. To this end we will apply Oliver's results in [67]. This will allow us to prove Theorem 5.10 which gives enough information about the group $(1 + I_{\mathbb{F}_q})$ to prove Theorem 5.4.

5.4.1 The group $(1 + I_{\mathbb{F}_q})_{\mathrm{ab}}$

Given a ring R, recall that I_R denotes the augmention ideal of the group ring $R[\pi]$, that is,

$$I_R := \ker(R[\pi] \to R) = \{\sum_{g \in \pi} r_g g \ : \ \sum_{g \in \pi} r_g = 0\}.$$

We will approach the group $(1 + I_{\mathbb{F}_q})_{\mathrm{ab}}$ via K-theory. Given a ring R, the first K-theoretical group of R is defined as

$$\mathrm{K}_1(\mathrm{R}) := \mathrm{GL}(\mathrm{R})_{\mathrm{ab}}.$$

When R is a local ring, we have $\mathrm{K}_1(\mathrm{R}) \cong (\mathrm{R}^*)_{\mathrm{ab}}$ (see [76, Corollary 2.2.6]), the abelianization of the group of units of the ring R. Hence we have $\mathrm{K}_1(\mathbb{F}_q[\pi]) \cong \mathbb{F}_q^* \times (1 + I_{\mathbb{F}_q})_{\mathrm{ab}}$. We will apply the results in [67], to obtain information about the group $\mathrm{K}_1(\mathbb{F}_q[\pi])$.

Let us first introduce the appropriate setting. Let $\mathcal{O}$ be the ring of integers of a p-adic field k. We define

$$\mathrm{SK}_1(\mathcal{O}[\pi]) := \ker\left(\mathrm{K}_1(\mathcal{O}[\pi]) \to \mathrm{K}_1(k[\pi])\right)$$
$$\mathrm{Wh}(\mathcal{O}[\pi]) := \mathrm{K}_1(\mathcal{O}[\pi])/\left(\mathcal{O}^* \times \pi_{\mathrm{ab}}\right)$$
$$\mathrm{Wh}'(\mathcal{O}[\pi]) := \mathrm{Wh}(\mathcal{O}[\pi])/\mathrm{SK}_1(\mathcal{O}[\pi])$$

The main Theorem in [67] is the following.

Theorem 5.9. *Let π be a p-group and $\mathcal{O}$ the ring of integers of a p-adic local field. Then*

$$\mathrm{SK}_1(\mathcal{O}[\pi]) \cong B_0(\pi).$$

Recall that the Bogomolov multiplier of the group π is defined as

$$B_0(\pi) = H_2(\pi,\mathbb{Z})/H_2^{\mathrm{ab}}(\pi,\mathbb{Z}),$$

where $H_2^{\mathrm{ab}}(\pi,\mathbb{Z})$ denotes the subgroup of $H_2(\pi,\mathbb{Z})$ generated by $H_2(\tau,\mathbb{Z})$ for every abelian subgroup $\tau \leq \pi$.

Let us introduce the appropriate setting to apply Theorem 5.9. Let ζ_{q-1} be a primitive $q-1$-root of unity. If p is a prime and q is a power of p, let $\mathrm{R}_q = \mathbb{Z}_p[\zeta_{q-1}]$ be a finite extension of the p-adic integers $\mathbb{Z}_p$. Note that $\mathrm{R}_q/p\,\mathrm{R}_q \cong \mathbb{F}_q$. Fix a $\mathbb{Z}_p$-basis $B_q = \{\lambda_j \mid 1 \leq j \leq n\}$ of R_q and let φ be a generator of $\mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{R}_q) \cong \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ such that $\varphi(\lambda) \equiv \lambda^p \pmod{p}$. Let us define

$$\bar{\mathrm{I}}_{\mathrm{R}_q} = \mathrm{I}_{\mathrm{R}_q}/\langle x - x^g \mid x \in \mathrm{I}_{\mathrm{R}_q}, g \in \pi\rangle.$$

Set $\mathcal{C}$ to be a set of nontrivial conjugacy class representatives of π. Then $\bar{\mathrm{I}}_{\mathrm{R}_q}$ can be regarded as a free $\mathbb{Z}_p$-module with basis $\{\lambda\overline{(1-r)} \mid \lambda \in B_q, r \in \mathcal{C}\}$. Finally define the abelian group M_q to be

$$\mathrm{M}_q = \bar{\mathrm{I}}_{\mathrm{R}_q}/\langle p\lambda\overline{(1-r)} - \varphi(\lambda)\overline{(1-r^p)} \mid \lambda \in B_q, \ r \in \mathcal{C}\rangle.$$

The proof of Theorem 5.4 rests on the following structural description of the group $(1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}}$.

Theorem 5.10. *Let π be a finite p-group. There is an exact sequence*

$$1 \longrightarrow B_0(\pi) \times \pi_{\mathrm{ab}} \longrightarrow (1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}} \longrightarrow \mathrm{M}_q \longrightarrow \pi_{\mathrm{ab}} \longrightarrow 1.$$

Proof. Our proof relies on inspecting the connection between $\mathrm{K}_1(\mathbb{F}_q[\pi])$ and $\mathrm{K}_1(\mathrm{R}_q[\pi])$ by utilizing the results of [67]. By Theorem 5.9, we know that $\mathrm{SK}_1(\mathrm{R}_q[\pi]) \cong B_0(\pi)$. The crux of understanding the structure of the group $\mathrm{K}_1(\mathrm{R}_q[\pi])$ is in the short exact sequence (see [67, Theorem 2])

$$1 \longrightarrow \mathrm{Wh}'(\mathrm{R}_q[\pi]) \xrightarrow{\ \Gamma\ } \bar{\mathrm{I}}_{\mathrm{R}_q} \longrightarrow \pi_{\mathrm{ab}} \longrightarrow 1,$$

where the map Γ is defined by composing the p-adic logarithm with a linear automorphism of $\bar{I}_{R_q} \otimes \mathbb{Q}_p$. More precisely, there is a map $\mathrm{Log}\colon 1 + I_{R_q} \to I_{R_q} \otimes \mathbb{Q}_p$, which induces an injection $\log\colon \mathrm{Wh}'(R_q[\pi]) \to \bar{I}_{R_q} \otimes \mathbb{Q}_p$. Setting $\Phi\colon I_{R_q} \to I_{R_q}$ to be the map $\sum_{g \in \pi} \alpha_g g \mapsto \sum_{g \in \pi} \varphi(\alpha_g) g^p$, we define $\Gamma\colon \mathrm{Wh}'(R_q[\pi]) \to \bar{I}_{R_q} \otimes \mathbb{Q}_p$ as the composite of log followed by the linear map $1 - \frac{1}{p}\Phi$. It is shown in [67, Proposition 10] that $\mathrm{im}\,\Gamma \subseteq \bar{I}_{R_q}$, i.e., Γ is integer-valued. We thus have a diagram

$$
\begin{array}{c}
1 + I_{R_q} \\
\downarrow \qquad \searrow^{(1 - \frac{1}{p}\Phi) \circ \log} \\
1 \longrightarrow \mathrm{Wh}'(R_q[\pi]) \xrightarrow{\ \Gamma\ } \bar{I}_{R_q}.
\end{array}
\tag{5.3}
$$

The group $\mathrm{Wh}'(R_q[\pi])$ is torsion-free (cf. [86]), so we have an explicit description

$$
K_1(R_q[\pi]) \cong R_q^* \times SK_1(R_q[\pi]) \times \pi_{\mathrm{ab}} \times \mathrm{Wh}'(R_q[\pi]).
\tag{5.4}
$$

To relate the results above to $K_1(\mathbb{F}_q[\pi])$, we use the functoriallity of K_1. Given a ring R and and ideal $I \subset R$, the projection map $R \to R/I$ induces a map $\mu\colon K_1(R) \to K_1(R/I)$ whose kernel is denoted by $K_1(R, I)$. Let $\mathfrak{p}$ be the ideal in $R_q[\pi]$ generated by p. Since $\mathbb{F}_q[\pi] = R_q[\pi]/\mathfrak{p}$ we obtain an exact sequence

$$
K_1(R_q[\pi], \mathfrak{p}) \xrightarrow{\ \partial\ } K_1(R_q[\pi]) \xrightarrow{\ \mu\ } K_1(\mathbb{F}_q[\pi]) \longrightarrow 1.
\tag{5.5}
$$

Since $R_q[\pi]$ is a local ring ([10, Corollary XI.1.4]), we have $K_1(R_q[\pi]) \cong R_q^* \times (1 + I_{R_q})$ and so the map μ indeed surjects onto $K_1(\mathbb{F}_q[\pi]) = \mathbb{F}_q^* \times (1 + I_{\mathbb{F}_q})$. Moreover $K_1(R_q[\pi], \mathfrak{p}) = (1 + p R_q) \times K_1(R_q[\pi], p I_{R_q})$ and $R_q^*/(1 + p R_q) \cong \mathbb{F}_q^*$. Hence (5.4) and (5.5) give a reduced exact sequence

$$
K_1(R_q[\pi], p I_{R_q}) \xrightarrow{\ \partial\ } \mathrm{Wh}'(R_q[\pi]) \xrightarrow{\ \mu\ } \frac{(1 + I_{\mathbb{F}_q})_{\mathrm{ab}}}{\mu(SK_1(R_q[\pi]) \times \pi_{\mathrm{ab}})} \longrightarrow 1.
\tag{5.6}
$$

To determine the structure of the relative group $K_1(R_q[\pi], p I_{R_q})$ and its connection to the map ∂, we make use of [67, Proposition 2]. The restriction of the logarithm map Log to $1 + p I_{R_q}$ induces an isomorphism $\log\colon K_1(R_q[\pi], p I_{R_q}) \to p\bar{I}_{R_q}$ such that the following diagram commutes:

$$
\begin{array}{c}
1 + p I_{R_q} \\
\downarrow \qquad \searrow^{\log} \\
1 \longrightarrow K_1(R_q[\pi], p I_{R_q}) \xrightarrow{\ \log\ } p\bar{I}_{R_q}.
\end{array}
\tag{5.7}
$$

In particular, the group $K_1(R_q[\pi], p I_{R_q})$ is torsion-free, and so $\mu(SK_1(R_q[\pi]) \times \pi_{\mathrm{ab}}) \cong SK_1(R_q[\pi]) \times \pi_{\mathrm{ab}}$. Note that by [10, Theorem V.9.1], the vertical map $1 + p I_{R_q} \to K_1(R_q[\pi], p I_{R_q})$ of the above diagram is surjective.

We now collect the stated results to prove the theorem. First combine the diagrams (5.3) and (5.7) into the following diagram:

$$\begin{array}{ccc}
1 + p\,\mathrm{I}_{\mathrm{R}_q} & \xrightarrow{\hspace{4cm}} & 1 + \mathrm{I}_{\mathrm{R}_q} \\
\downarrow & & \downarrow \\
\mathrm{K}_1(\mathrm{R}_q[\pi], p\,\mathrm{I}_{\mathrm{R}_q}) & \xrightarrow[\partial]{\log} \mathrm{Wh}'(\mathrm{R}_q[\pi]) & \\
\downarrow{\scriptstyle\log} & & \downarrow{\scriptstyle\Gamma} \\
p\bar{\mathrm{I}}_{\mathrm{R}_q} & \xrightarrow{1-\frac{1}{p}\Phi} & \bar{\mathrm{I}}_{\mathrm{R}_q}.
\end{array}$$

(5.8)

Since the back and top rectangles commute and the left-most vertical map is surjective, it follows that the bottom rectangle also commutes. Whence $\operatorname{coker}\partial \cong \operatorname{coker}(1 - \frac{1}{p}\Phi)$. Observing that the latter group is isomorphic to M_q, the exact sequence (5.6) gives an exact sequence

$$1 \longrightarrow \mathrm{B}_0(\pi) \times \pi_{\mathrm{ab}} \longrightarrow (1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}} \longrightarrow \mathrm{M}_q \longrightarrow \pi_{\mathrm{ab}} \longrightarrow 1. \qquad (5.9)$$

The proof is complete. $\hspace{10cm}\square$

We now derive Theorem 5.4 from Theorem 5.10.

Proof of Theorem 5.4. The exact sequence of Theorem 5.10 implies that $|(1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}}| = |\mathrm{B}_0(\pi)| \cdot |\mathrm{M}_q|$. Hence it suffices to compute $|\mathrm{M}_q|$. To this end, we filter M_q by the series of its subgroups

$$\mathrm{M}_q \supseteq p\,\mathrm{M}_q \supseteq p^2\,\mathrm{M}_q \supseteq \cdots.$$

Note that the relations $p\lambda\overline{(1 - r)} - \varphi(\lambda)\overline{(1 - r^p)} = 0$ imply $(\exp\pi)\,\mathrm{M}_q = 0$, so the above series reaches 0.

For each $i \geq 0$, put

$$\pi_i = \{x^{p^i} \mid x \in \pi\} \text{ and } \mathcal{C}_i = \mathcal{C} \cap (\pi_i \setminus \pi_{i+1}).$$

Note that $\mathcal{C}_i$ is empty for $p^i \geq \exp\pi$. Now,

$$p^i\,\mathrm{M}_q\,/p^{i+1}\,\mathrm{M}_q = \langle \lambda\overline{(1 - r)} \mid \lambda \in B_q,\ r \in \mathcal{C}_i \rangle \cong \bigoplus_{\mathcal{C}_i} C_p^n.$$

It follows that $|\mathrm{M}_q| = q^{|\mathcal{C}|} = q^{\mathrm{k}(\pi)-1}$ and the proof is complete. $\hspace{3cm}\square$

5.4.2 B_0 and rationality questions in unipotent groups

As explained in the introduction, for a linear algebraic $\mathbb{F}_q$-group we have $G(\mathbb{F}_q)' = [G(\mathbb{F}_q), G(\mathbb{F}_q)] \subseteq G'(\mathbb{F}_q)$, where G' is the derived group of G. Suppose now G is the group defined by the algebra group $1 + \mathrm{I}_{\mathbb{F}_p}$ where $\mathrm{I}_{\mathbb{F}_p}$ is the augmentation ideal of $\mathbb{F}_p[\pi]$ for some p-group π. Theorem 5.5 and 5.6 give a precise description of the behaviour of the difference between $G'(\mathbb{F}_q)$ and $G(\mathbb{F}_q)'$ for this class of groups.

Proofs of Theorem 5.5 and 5.6. We will consider an extension $\mathbb{F}_l$ of $\mathbb{F}_q$ of degree m. The inclusion $G(\mathbb{F}_q) \subseteq G(\mathbb{F}_l)$ induces a map $f \colon G(\mathbb{F}_q)_{\mathrm{ab}} \to G(\mathbb{F}_l)_{\mathrm{ab}}$ with

$$\ker f = (G(\mathbb{F}_q) \cap G(\mathbb{F}_l)')/G(\mathbb{F}_q)'.$$

Note that there exists a large enough m such that $G'(\mathbb{F}_q) = G(\mathbb{F}_q) \cap G(\mathbb{F}_l)'$, and hence $\ker f = G'(\mathbb{F}_q)/G(\mathbb{F}_q)'$. For this reason we want to understand $\ker f$ for a given m.

The inclusion $\mathbb{F}_q \subseteq \mathbb{F}_l$ induces a map

$$\mathrm{incl} \colon \mathrm{K}_1(\mathbb{F}_q[\pi]) \to \mathrm{K}_1(\mathbb{F}_l[\pi]).$$

Note that f is just the restriction of incl to $(1 + \mathrm{I}_{\mathbb{F}_q})_{\mathrm{ab}}$. Recalling sequence (5.6) from the proof of Theorem 5.10, we set

$$\mathrm{SK}_1(\mathbb{F}_l[\pi]) = \mu(\mathrm{SK}_1(\mathrm{R}_l[\pi]) \subseteq (1 + \mathrm{I}_{\mathbb{F}_l})_{\mathrm{ab}} = G(\mathbb{F}_l)/G(\mathbb{F}_l)'.$$

Commutativity of the diagram

$$\begin{array}{ccc}
\mathrm{K}_1(\mathrm{R}_q[\pi]) & \xrightarrow{\ \mu\ } & \mathrm{K}_1(\mathbb{F}_q[\pi]) \\
\downarrow{\scriptstyle \mathrm{incl}} & & \downarrow{\scriptstyle \mathrm{incl}} \\
\mathrm{K}_1(\mathrm{R}_l[\pi]) & \xrightarrow{\ \mu\ } & \mathrm{K}_1(\mathbb{F}_l[\pi])
\end{array} \qquad (5.10)$$

shows that incl restricts to a map $\mathrm{incl} \colon \mathrm{SK}_1(\mathbb{F}_q[\pi]) \to \mathrm{SK}_1(\mathbb{F}_l[\pi])$. Recall that $\mathrm{SK}_1(\mathrm{R}_l[\pi]) \cong \mathrm{B}_0(\pi)$, so we obtain from sequence (5.9) the commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{SK}_1(\mathbb{F}_q[\pi]) \times \pi_{\mathrm{ab}} & \longrightarrow & G(\mathbb{F}_q)_{\mathrm{ab}} & \longrightarrow & \mathrm{M}_q & \longrightarrow & \pi_{\mathrm{ab}} & \longrightarrow & 1 \\
& & \downarrow{\scriptstyle \mathrm{incl} \times \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \iota} & & & & \\
1 & \longrightarrow & \mathrm{SK}_1(\mathbb{F}_l[\pi]) \times \pi_{\mathrm{ab}} & \longrightarrow & G(\mathbb{F}_l)_{\mathrm{ab}} & \longrightarrow & \mathrm{M}_l & \longrightarrow & \pi_{\mathrm{ab}} & \longrightarrow & 1,
\end{array}$$

where ι is the map induced by the inclusion $\mathrm{I}_{\mathrm{R}_q} \subseteq \mathrm{I}_{\mathrm{R}_l}$.

We will now show that $\ker \iota = 0$. This will imply $\ker f \subseteq \mathrm{SK}_1(\mathbb{F}_q[\pi])$. Without loss of generality, we may assume that there is an inclusion of bases $B_q \subseteq B_l$. As in the proof of Theorem 5.4, let us consider the series

$$\mathrm{M}_l \supseteq p\,\mathrm{M}_l \supseteq p^2\,\mathrm{M}_l \supseteq \cdots.$$

Observe again that for each $i \geq 0$ we have

$$p^i\,\mathrm{M}_q\,/p^{i+1}\,\mathrm{M}_q = \langle \lambda \overline{(1-r)} \mid \lambda \in B_q,\ r \in \mathcal{C}_i \rangle,$$
$$p^i\,\mathrm{M}_l\,/p^{i+1}\,\mathrm{M}_l = \langle \lambda \overline{(1-r)} \mid \lambda \in B_l,\ r \in \mathcal{C}_i \rangle.$$

If we consider the graded groups associated to the series above, we get an induced map

$$\mathrm{gr}(\iota) \colon \bigoplus_{i \geq 0} p^i\,\mathrm{M}_q\,/p^{i+1}\,\mathrm{M}_q \to \bigoplus_{i \geq 0} p^i\,\mathrm{M}_l\,/p^{i+1}\,\mathrm{M}_l.$$

By construction ι is induced by the assignments $\lambda\overline{(1-r)} \mapsto \lambda\overline{(1-r)}$, for every $\lambda \in B_q$, $r \in \mathcal{C}$. Hence $\mathrm{gr}(\iota)$ is injective in every component and therefore injective. This implies $\ker \iota = 0$, as desired. In particular, we obtain that

$$|G(\mathbb{F}_q)/G'(\mathbb{F}_q)| \geq |\, M_q\,| = q^{\mathrm{k}(\pi)-1}. \tag{5.11}$$

We are now ready to show the first statement of Theorem 5.5. Observe that G is a unipotent connected algebraic group defined over $\mathbb{F}_p$ and so is G' ([12, Corollary I.2.3]). Hence $G' \cong_{\mathbb{F}_p} \mathbb{A}^{\dim G'}$ (cf. [40, Remark A.3]) and so $|G'(\mathbb{F}_p)| = p^{\dim G'}$. By (5.11), we have $|G(\mathbb{F}_p)/G'(\mathbb{F}_p)| \geq p^{\mathrm{k}(\pi)-1}$, whence $\dim G' \leq |\pi| - \mathrm{k}(\pi)$. On the other hand we have $[L_G, L_G]_L = [\mathrm{I}_\mathbb{F}, \mathrm{I}_\mathbb{F}]_L$, which, by Lemma 5.3.2, has dimension $|\pi| - \mathrm{k}(\pi)$. It is known that for an algebraic group, $\dim G' \geq \dim[L_G, L_G]_L$ (see [31, Corollary 10.5]). Thus $\dim G' = |\pi| - \mathrm{k}(\pi)$.

Let us set $e = \exp \mathrm{B}_0(\pi)$, the exponent of the group $\mathrm{B}_0(\pi)$. We now claim that $\ker f = \mathrm{SK}_1(\mathbb{F}_q[\pi])$ if and only if e divides $m = |\mathbb{F}_l : \mathbb{F}_q|$. This will imply the second statement of Theorem 5.5 and also Theorem 5.6.

Let us consider $\mathbb{F}_l[\pi] \cong \bigoplus_{i=1}^{m} \mathbb{F}_q[\pi]$ as a free $\mathbb{F}_q[\pi]$-module. This gives a natural inclusion $\mathrm{GL}_1(\mathbb{F}_l[\pi]) \to \mathrm{GL}_m(\mathbb{F}_q[\pi])$, which induces the transfer map

$$\mathrm{trf}\colon \mathrm{K}_1(\mathbb{F}_l[\pi]) \to \mathrm{K}_1(\mathbb{F}_q[\pi]).$$

Note that if $x \in \mathrm{K}_1(\mathbb{F}_q[\pi])$, then $(\mathrm{trf} \circ \mathrm{incl})(x) = x^m$. By commutativity of (5.10) the transfer map restricts to a map

$$\mathrm{trf}\colon \mathrm{SK}_1(\mathbb{F}_l[\pi]) \to \mathrm{SK}_1(\mathbb{F}_q[\pi]).$$

Moreover, by [67, Proposition 21] the transfer map is an isomorphism. It thus follows that $\mathrm{incl}(\mathrm{SK}_1(\mathbb{F}_q[\pi])) = 1$ if and only if e divides m. Hence $\ker f = \mathrm{SK}_1(\mathbb{F}_q[\pi])$ if and only if e divides m and we are done. $\qquad\square$

Chapter 6

Finite groups of Lie type

6.1 Introduction

In this chapter we investigate the representation growth of a certain class of groups arising from finite simple groups. We refer to Section 3.1 for notation and concepts relating to representation growth. As above, we only consider continuous representations. Let H be a group and suppose that $r_n(H) < \infty$ for every n. Then one can formally define the representation zeta function of H as the Dirichlet series

$$\zeta_H(s) = \sum_{n \in \mathbb{N}} r_n(G) n^{-s}.$$

We write $\alpha(H)$ for the abscissa of convergence of ζ_H. Recall that given a group Γ we define $R_n(\Gamma) = \sum_{i=1}^n r_n(\Gamma)$. The invariant $\alpha(H)$ is related to the asymptotic behaviour of the sequence $R_n(H)$ by the equation

$$\alpha(H) = \limsup \frac{\log R_n(H)}{\log n}.$$

Let us consider the class of groups

$$\mathcal{C} := \{\mathbf{H} = \prod_{i \in I} S_i \;:\; S_i \text{ is a nonabelian finite simple group}\}.$$

We want to study the representation growth of groups in this class. In particular, we want to understand under which conditions a group of this class has polynomial representation growth. Given a cartesian product of finite groups $\mathbf{H} = \prod_{i \in I} S_i$, let us define $L_{\mathbf{H}}(n) := \{i \in I : R_n(S_i) > 1\}$ and put $l_{\mathbf{H}}(n) := |L_n|$. Hence, $l_{\mathbf{H}}$ counts the number of factors in $\mathbf{H}$ with a nontrivial irreducible representation of dimension at most n. We will usually write $l(n) = l_{\mathbf{H}}(n)$ when there is no danger of confusion. We immediately obtain the following necessary condition.

Lemma 6.1.1. *Let $\mathbf{H} = \prod_{i \in I} S_i$. If $l_{\mathbf{H}}(n)$ is not polynomially bounded then $\mathbf{H}$ does not have PRG.*

We aim at proving that for $\mathbf{H} \in \mathcal{C}$, then the converse is also true.

Theorem 6.1. *Let* $\mathbf{H} = \prod_{i \in I} S_i$ *be a cartesian product of nonabelian finite simple groups and let* $l_{\mathbf{H}}(n) := |\{i \in I : R_n(S_i) > 1\}|$. *Then* $\mathbf{H}$ *has PRG if and only if* $l_{\mathbf{H}}(n)$ *is polynomially bounded.*

Theorem 6.1 provides us with a way to construct numerous examples of groups within $\mathcal{C}$ having PRG. We will denote this subclass of groups by $\mathcal{C}_{PRG}$. It is natural to ask what types of representation growth can occur among groups in $\mathcal{C}_{PRG}$. In [42], Kassabov and Nikolov studied questions related to the class $\mathcal{C}$, and more in particular about the subclass $\mathcal{A} \subset \mathcal{C}$ where

$$\mathcal{A} := \{\mathbf{H} = \prod_{i \in I} S_i \ : \ S_i = \mathrm{Alt}(m) \text{ for some } m \geq 5\},$$

where $\mathrm{Alt}(m)$ denotes the alternating group on m letters. They showed that within the class $\mathcal{A}$ any type of representation growth is possible.

Theorem 6.2. *For any* $b > 0$, *there exists a group* $\mathbf{H} \in \mathcal{A}_{PRG}$ *such that* $\alpha(\mathbf{H}) = b$.

The groups appearing in the proof of Theorem 6.2 are of the form

$$\mathbf{H} = \prod_{i \geq 5} \mathrm{Alt}(i+1)^{f(i)},$$

for some $f : \mathbb{N} \to \mathbb{N}$. In particular the simple factors of $\mathbf{H}$ have unbounded rank [1] as alternating groups. We want to obtain a similar result for the subclass $\mathcal{L} \subset \mathcal{C}$, where

$$\mathcal{L} := \{\mathbf{H} = \prod_{i \in I} S_i \ : \ S_i \text{ is a finite simple group of Lie type}\}.$$

We do this in the following theorem, where it is shown that an analogous result holds for this class. In our case, all of the simple factors may have the same Lie rank.

Theorem 6.3. *For any* $c > 0$, *there exists a group* $\mathbf{H} = \prod_{i \in \mathbb{N}} S_i \in \mathcal{L}_{PRG}$ *such that* $\alpha(\mathbf{H}) = c$. *Moreover* $\mathbf{H}$ *can be chosen so that only one Lie type occur among its factors.*

It is natural to ask whether the cumbersome groups appearing in the proof of Theorem 6.3 are finitely generated as profinite groups. We give a positive answer in the following theorem.

Theorem 6.4. *Let* $\mathbf{H} \in \mathcal{C}$. *If* $\mathbf{H}$ *has PRG then* $\mathbf{H}$ *is finitely generated as a profinite group.*

The next natural question is whether such a group is the profinite completion of finitely generated residually finite group. If this is true, we say that the group in question is a profinite completion. This question was answered by Kassabov and Nikolov for cartesian products with factors of unbounded rank (see [42, Theorem 1.4]).

---

[1]For S a nonabelian finite simple groups we define $\mathrm{rk}\, S = m$ if $S = \mathrm{Alt}(m)$ and $\mathrm{rk}\, S = \mathrm{rk}\, L$ if S is a simple group of Lie type L.

Theorem 6.5. *Let $\mathbf{H} = \prod_{i \in \mathbb{N}} S_i^{c(i)}$ where the $\{S_i\}$ are an infinite family of finite simple groups such that $\operatorname{rk} S_i \to \infty$. If $\mathbf{H}$ is topologically finitely generated then it is a profinite completion.*

Moreover they also explain why the condition $\operatorname{rk} S_i \to \infty$ is necessary. In particular, the groups appearing in the proof of Theorem 6.3 are not profinite completions. It is not clear however whether Theorem 6.3 remains true if we require $\mathbf{H}$ to be a profinite completion.

6.2 Representation Growth of Finite Groups of Lie Type

We refer to section 1.7 for definitons and concepts regarding finite groups of Lie type. Let G be a connected simply connected absolutely almost simple affine algebraic group with Steinberg endomorphism $F : G \to G$, then (except for a finite number of exceptions) the group G^F is quasisimple and in particular $G^F/Z(G^F)$ is a simple group (see Theorem 1.20). Finite simple groups of this form are called finite simple groups of Lie type. According to the classification of finite simple groups, all but a finite number of the nonabelian finite simple groups are either an alternating group or a finite simple group of Lie type. Therefore the asymptotic behaviour of the representation growth of groups of the form G^F may be used to derive asympotic properties for the representation growth of finite simple groups of Lie type. The representation growth of the quasisimple groups G^F has been studied in [52] by Liebeck and Shalev using Deligne-Lusztig theory. For a prime power q and Lie type L, let $L(q)$ denote (if there exists one) a finite quasisimple group of type L defined over $\mathbb{F}_q$.

Theorem 6.6 ([52, Theorem 1.1])**.** *Fix a Lie type L and let h be the corresponding Coxeter number. Then for any fixed real number $t > 2/h$, we have*

$$\zeta_{L(q)}(t) \to 1 \ as \ q \to \infty.$$

Theorem 6.7 ([52, Theorem 1.2])**.** *Fix a real number $t > 0$. Then there is an integer $r(t)$ such that for any $L(q)$ with $\operatorname{rk} L \geq r(t)$, we have*

$$\zeta_{L(q)}(t) \to 1 \ as \ |L(q)| \to \infty.$$

The corresponding result for alternating groups reads as follows.

Theorem 6.8 ([51, Corollary 2.7])**.** *Fix a real number $t > 0$. Let A_n denote the alternating group on n elements, then*
$$\zeta_{A_n}(t) \to 1 \ as \ n \to \infty.$$

Note that for a finite simple group of Lie type $S = L(q)/Z(L(q))$ for some Lie type L and primer power q, we have $\zeta_S(t) \leq \zeta_{L(q)}(t)$ for every $t > 0$. Therefore the above theorems provide information about the asymptotic behaviour of the representation zeta functions for all the infinite series of nonabelian finite simple groups. As a corollary, one obtains a general result for the representation growth of any nonabelian finite simple group.

Corollary 6.2.1. *Let S denote a nonabelian finite simple group.*

i) For $t > 1$, we have

$$\zeta_S(t) \to 1 \ as \ |S| \to \infty.$$

ii) There exists an absolute constant c such that $r_n(S) < cn$ for every nonabelian finite simple group S.

For the proof of Theorem 6.3 we will need a more precise study of the representation zeta functions $\zeta_{L(q)}(s)$. Let us first introduce some concepts which will be useful for comparing different zeta functions, cf. [6, Definition 2.4]. Let $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ and $g(s) = \sum_{n=1}^{\infty} b_n n^{-s}$ be Dirichtlet generating series, i.e., Dirichlet series with integer coefficients $a_n, b_n \geq 0$. Let $C \in \mathbb{R}$. We write $f \lesssim_C g$ if f and g have the same abscissa of convergence α and $f(s) \leq C^{1+s}g(s)$ for every $s > \alpha$. We write $f \sim_C g$ if $f \lesssim_C g$ and $g \lesssim_C f$.

In [6] Avni, Klopsch, Onn and Voll obtained a precise description of the asymptotic behaviour of the representation zeta functions of finite groups of Lie type.

Theorem 6.9 ([6, Theorem 3.1 (3.1)]). *For every connected semi-simple algebraic group G defined over a finite field $\mathbb{F}_q$ with absolute root system Φ*

$$\zeta_{G(\mathbb{F}_q)}(s) \sim_C 1 + q^{\operatorname{rk}\Phi - |\Phi^+|s} = 1 + q^{k(1-\frac{h}{2}s)}.$$

The following lemma provides a way to study inifinite products of representation zeta functions.

Lemma 6.2.1. *Let f, g be Dirichlet generating series and denote by α_f and α_g their corresponding abscissae of convergence. Suppose that $f = \prod_{m=1}^{\infty}(1 + f_m)$ and $g = \prod_{m=1}^{\infty}(1 + g_m)$, where f_m, g_m are Dirichlet generating series with vanishing constant terms. Suppose further that there exists $C \in \mathbb{R}_{>0}$ such that, for all m, $f_m \lesssim_C g_m$. Then $\alpha_f \leq \alpha_g$.*

Finally the following Theorem will be used several times to obtain the necessary bounds to apply Theorem 6.1, see [49].

Theorem 6.10. *There are absolute constants $d, e > 1$ such that for any finite simple group of Lie type S and any irreducible projective representation χ of S we have*

$$\chi(1) > dq^{er}$$

where $r = \operatorname{rk} L$, and S is of type L and defined over $\mathbb{F}_q$.

6.3 Polynomial Representation Growth in $\mathcal{C}$

We begin by giving a proof to Lemma 6.1.1.

Proof of Lemma 6.1.1. Suppose that $l(n)$ is not polynomially bounded. Observe that for some (distinct) $i_1, \ldots, i_t \in I$ and ρ_{i_j}, an n_{i_j}-dimensional irreducible representation of the group S_{i_j}, the tensor product $\rho_{i_1} \otimes \ldots \otimes \rho_{i_t}$ naturally defines an irreducible n-dimensional

representation of the group $\prod_{j=1}^{t} S_{i_j}$ (and in particular of $\mathbf{H}$), where $n = n_{i_1} \ldots n_{i_t}$. Indeed, every irreducible representation of $\mathbf{H}$ has this form. In particular, it follows that

$$R_{n^2}(\mathbf{H}) \geq \frac{l(n)(l(n)-1)}{2}.$$

Hence $R_n(\mathbf{H})$ cannot be polynomially bounded, as we assumed that $l(n)$ is not. This implies that $r_n(\mathbf{H})$ is not polynomially bounded. □

Proof of Theorem 6.1. The direct implication follows from Lemma 6.1.1.

For the converse take a as in Lemma 3.2.9. Since $i(n)$ is polynomially bounded and $l_H(1) = 1$ (the S_i being nonabelian and simple), we can take $b \in \mathbb{N}$ such that $l_H(n) \leq n^b$. Similarly, by Corollary 6.2.1 we can take $c \in \mathbb{N}$ such that $r_n(S) \leq n^c$ for every nonabelian finite simple group S.

Now let ρ be an irreducible n-dimensional representation of $\mathbf{H} = \prod_{i \in I} S_i$. Recall that $\rho \cong \rho_{i_1} \otimes \ldots \otimes \rho_{i_t}$ for some (distinct) $i_1, \ldots, i_t \in I$, where ρ_{i_j} is a nontrivial n_{i_j}-dimensional irreducible representation of S_{i_j} and $n_{i_1} \ldots n_{i_t} = n$. Moreover, $n_{i_j} > 1$ since the groups S_{i_j} are simple. By the previous lemma there are at most n^a possible configurations of the form $(n_1, \ldots, n_t)$ such that $n_1 \ldots n_t = n$. Given such a configuration $(n_{i_1}, \ldots, n_{i_t})$, the number of factors S of $\mathbf{H}$ such that S has a representation of dimension n_{i_j} is at most $l_H(n_{i_j}) \leq n_{i_j}^b$. Hence the number of choices of factors $(i_1, \ldots, i_t) \in I^t$ for such a configuration is bounded by $\prod n_{i_j}^b = n^b$. Now each group S_{i_j} has at most $n_{i_j}^c$ irreducible representations of dimension n_{i_j}. Therefore $r_n(\mathbf{H}) \leq n^a n^b n^c = n^{a+b+c}$ and $\mathbf{H}$ has polynomial representation growth. □

Given a finite group G let us denote by $d(G)$ the minimal number of generators of G. It is known that $d(S) = 2$ for every nonabelian finite simple group. The following result in [88] will be used for the proof Theorem 6.4.

Theorem 6.11. *Let S be a nonabelian finite simple group. For every $e \in \mathbb{N}$, $d\left(S^{|S|^e}\right) = e + 2$.*

Proof of Theorem 6.4. Suppose $\mathbf{H}$ has PRG. For S a nonabelian finite simple group, let $c(S)$ denote the number of copies of S appearing as a composition factor of $\mathbf{H}$. By Theorem 6.1 we know that $l(n) \leq n^e$ for some $e \in \mathbb{N}$. Since for every finite group S, S has a nontrivial irreducible representation of dimension less than $|S|$, it follows that $c(S) \leq l(|S|) \leq |S|^e$ for every S. Note that we can write $\mathbf{H} = \prod_S S^{c(S)}$, where S runs along the nonabelian finite simple groups.

Applying Theorem 6.11, we obtain that, for every S, $S^{c(S)}$ is generated by e elements. Let us pick for every S a tuple $(g_1^S, \ldots, g_e^S) \in S^{c(S)}$ such that $< g_1^S, \ldots, g_e^S >= S^{c(S)}$. We claim that the e-tuple $(\mathbf{g_1} = \prod_S g_1^S, \ldots, \mathbf{g_e} = \prod_S g_e^S)$ generates $\mathbf{H}$ as a profinite group. Put $\mathbf{G} = < \mathbf{g_1}, \ldots, \mathbf{g_e} >$. It follows by construction that $\mathbf{G} \times \prod_{Q \neq S} Q^{c(Q)} = \mathbf{H}$. Thefore

$$\mathbf{H}/\prod_{Q \not\cong S} Q^{c(Q)} \cong S^{c(S)}$$

is in the top of $\mathbf{G}$ for every S. But this clearly implies $\mathbf{G} = \mathbf{H}$.

□

6.4 Types of representation growth

Example. Let us first look at an example to ilustrate the idea of the construction. Let us consider the groups $\mathrm{SL}_2(\mathbb{F}_q)$. The representation theory of these groups is well understood (see [21, Chapter 15]) and we know that for $q = p^n$ (p odd prime) their representation zeta functions are given by

$$
\begin{aligned}
\zeta_{\mathrm{SL}_2(\mathbb{F}_q)} =&\, 1 + q^{-s} + \frac{q-3}{2}(q+1)^{-s+2} + 2\left(\frac{q+1}{2}\right)^{-s} + \\
& \frac{q-1}{2}(q-1)^{-s} + 2\left(\frac{q-1}{2}\right)^{-s}.
\end{aligned}
$$

For convinience, we will encode the nontrivial part as

$$
f(q, s) = \zeta_{\mathrm{SL}_2(\mathbb{F}_q)}(s) - 1
$$

Fix an odd prime p and consider now the group $\mathbf{H} = \prod_{i \in \mathbb{N}} \mathrm{SL}_2(\mathbb{F}_{p^i})$. Note that all factors of the cartesian product have rank 1. Hence, applying Theorem 6.10 we readily obtain that if $\mathrm{SL}_2(\mathbb{F}_q)$ has a representation of dimension n, then $n > dq^e$. It follows that $l_H(n) < \log_p(n/d)$, in particular, $l_H(n)$ is polynomially bounded and $\mathbf{H}$ has PRG. Recalling once again that irreducible representations of $\mathbf{H}$ are given by finite tensor products of irreducible representations of the factors $\mathrm{SL}_2(\mathbb{F}_q)$, we obtain that the representation zeta function of $\mathbf{H}$ is given by

$$
\zeta_{\mathbf{H}}(s) = \prod_{i \in \mathbb{N}} \zeta_{\mathrm{SL}_2(\mathbb{F}_{p^i})}(s) = \prod_{i \in \mathbb{N}} (1 + f(p^i, s)).
$$

It follows that $\zeta_{\mathbf{H}}(s)$ converges if and only if $\sum_{i \in \mathbb{N}} f(p^i, s)$ does. An analysis of the summands ocurrying in each $f(p^i, s)$ gives that the latter series converges if and only if the series $\sum_{q=p^i} q^{-s+1} = \sum_{i \in \mathbb{N}} (p^{-s+1})^i$ does. The latter expression, being a geometric series, converges if and only if $p^{-s+1} < 1$, that is, if and only if $s > 1$. Therefore $\alpha(\mathbf{H}) = 1$. $\quad\square$

Theorem 6.12. *Given $c \in \mathbb{R}_{>0}$, there exists a Lie type L, a prime number p and $\mathbf{H} = \prod_{i \in \mathbb{N}} S_i$, where for every $i \in \mathbb{N}$, $S_i = L(q)$ for some p-power q, such that $\mathbf{H}$ has PRG and $\alpha(\mathbf{H}) = c$.*

Proof. Given $c \in \mathbb{R}_{>0}$, pick a Lie type L with Coxeter number h and $k = \mathrm{rk}\,\Phi$ such that $khc > 2$. Let us assume that h is an even integer (this holds for all root systems except for those of type A_{2k}, moreover and easy adaptation of the proof also works for h odd). Construct a sequence of natural numbers $\{a_n\} \subseteq \mathbb{N}$ such that $c - \frac{a_n}{n} < \frac{1}{n}$ for every $n \in \mathbb{N}$. Clearly $a_n \to c$ and there exists $N \in \mathbb{N}$ such that $hka_n > 2$ for every $n > N$. Pick a prime number p. Consider the function $f : \mathbb{N} \to \mathbb{N}$ given by $i \mapsto p^{\frac{k(ha_i - 2i)}{2}}$ if $i > N$, $i \mapsto 0$ otherwise. Recall that $L(q)$ denotes a quasisimple group of type L defined over $\mathbb{F}_q$. Finally consider the group

$$
\mathbf{H} = \prod_{i \in \mathbb{N}} L(p^i)^{f(i)}.
$$

We claim that $\alpha(\mathbf{H}) = c$. First observe that, by Theorem 6.10, if $L(p^i)$ has an irreducible representation of dimension n, then $n > dp^{ier}$, that is, $i < \frac{\log(n/d)}{re \log p} \leq C \log n$ for some constant C. On the other hand note that $f(i) = p^{\frac{ik(ha_i - 2i)}{2i}} \leq p^{\frac{ikhc-2i}{2}} = p^{Di}$ for some constant D. Thus

$$l_H(n) < C \log n f(C \log n) \leq C \log n p^{D \log n} \leq C \log n n^{D \log p},$$

that is, $l_H(n)$ is polynomially bounded. By Theorem 6.1 $\mathbf{H}$ has PRG and we have

$$\zeta_{\mathbf{H}} = \prod_{i \in \mathbb{N}} \zeta_{L(p^i)}^{f(i)}.$$

Now by Theorem 6.9 we know that

$$\zeta_{L(p^i)} \lesssim_C 1 + p^{i(\operatorname{rk} \Phi - |\Phi^+|s)} = 1 + p^{ik\left(1 - \frac{h}{2}s\right)}.$$

Therefore an application of Lemma 6.2.1 gives

$$\alpha(\mathbf{H}) = \alpha \left(\prod_{i \in \mathbb{N}} \left(1 + p^{ik\left(1 - \frac{h}{2}s\right)} \right)^{f(i)} \right).$$

The latter product convergences if and only if the series

$$\sum_{i \in \mathbb{N}} f(i) p^{ik\left(1 - \frac{h}{2}s\right)} = \sum_{i > N} p^{\frac{k(ha_i - 2i)}{2}} p^{ik\left(1 - \frac{h}{2}s\right)} = \sum_{i > N} p^{\frac{ikh}{2}\left(\frac{a_i}{i} - s\right)}$$

converges. We claim that the latter series converges if and only if $s > c$. Suppose first that $s > c$, then $\frac{a_i}{i} - s < -\epsilon$ for some $\epsilon > 0$. Thefore

$$\sum_{i > N} p^{\frac{ikh}{2}\left(\frac{a_i}{i} - s\right)} \leq \sum_{i > N} p^{\frac{ikh}{2}(c-s)}.$$

Since the latter is a subseries of a geometric series of ratio $p^{\frac{kh}{2}(c-s)} < 1$, it converges. Suppose now that $s < c$. Then there exists $N < M \in \mathbb{N}$ and $\epsilon > 0$ such that $\frac{a_i}{i} - s > \epsilon$ for every $i > M$. Hence

$$\sum_{i > N} p^{\frac{ikh}{2}\left(\frac{a_i}{i} - s\right)} \geq \sum_{i > M} p^{\frac{ikh}{2}\left(\frac{a_i}{i} - s\right)} \geq \sum_{i > M} p^{\frac{ikh}{2}(\epsilon)}.$$

Since the latter series is a tale of a geometric series of ratio $p^{\frac{kh}{2}(\epsilon)} > 1$, it does not converge. $\square$

Theorem 6.3 is now a corollary of Theorem 6.12.

Proof of theorem 6.3. Let us pick $L = (A_p, \mathrm{id})$ such that $\operatorname{rk} \Phi = p$ is a prime number and $pc > 2$. Now by (the proof of) Theorem 6.12 there exists $H = \prod_{i \in \mathbb{N}} S_i$ such that for every $i \in \mathbb{N}$, $S_i = L(p^e)$ for some $e \in \mathbb{N}$ and $\alpha(\mathbf{H}) = c$. Note that in this case we have $L(p^e) = \mathrm{SL}_p(\mathbb{F}_{p^e})$ and $Z(\mathrm{SL}_p(\mathbb{F}_{p^e})) = 1$, since there are no nontrivial p^{th}-roots of unity in a field of characteristic p. Hence the groups $L(p^e)$ are indeed simple and the theorem follows. Note that one can similarly find an appropriate Lie type within the other infinite families $(B_i, C_i, D_i, i \in \mathbb{N})$ and mimic the above construction for that type. $\square$

Bibliography

[1] M. Abért, N. Nikolov, B. Szegedy, *Congruence subgroup growth of arithmetic groups in positive characteristic*, Duke Math. J. **177** (2003).

[2] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company (1969).

[3] N. Avni, B. Klopsch, U. Onn, C. Voll, *On representation zeta functions of groups and a conjecture of Larsen-Lubotzky*, C. R. Math. Acad. Sci. Paris **348** (2010), no. 7-8.

[4] N. Avni, B. Klopsch, U. Onn, C. Voll, *Representation zeta functions of compact p-adic analytic groups and arithmetic groups*, Duke Math. J. **162** (2013), no. 1.

[5] N. Avni, B. Klopsch, U. Onn, C. Voll, *Similarity classes of integral p-adic matrices and representation zeta functions of groups of type A_2*, Proc. Lond. Math. Soc. (3) **112** (2016), no. 2.

[6] N. Avni, B. Klopsch, U. Onn, C. Voll, *Arithmetic Groups, Base Change, and Representation Growth*, Geometric and Functional Analysis, Vol. **26**, Issue 1 (2016).

[7] N. Avni, Arithmetic groups have rational representation growth, Ann. of Math. (2) **174** (2011), no. 2.

[8] H. Bass, M. Lazard, J-P. Serre, *Sous-groupes d'indices finis dans* $SL(n, Z)$, Bull. Amer. Math. Soc. **70** (1964).

[9] H. Bass, J. Milnor, J-P. Serre, *Solution of the congruence subgroup problem for* $SL_n(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Publ. Math. IHES **33** (1967).

[10] H. Bass, *Algebraic K-theory*, W. A. Benjamin, New York, Amsterdam (1968).

[11] H. Behr, *Endliche Erzeugbarkeit arithmetischer Gruppen über globalen Körpern*, J. Reine Angew. Math. **229** (1968).

[12] A. Borel, *Linear algebraic groups*, Graduate Texts in Mathematics **126**, Springer-Verlag (1991).

[13] A. Borel, *Some finiteness properties of adele groups over number fields*, Publ. Math. IHES **16** (1963).

[14] A. Borel, J. P. Serre, *Theoremes de finitude en cohomologie galoisienne*, Commentarii Mathematici Helvetici, Vol. **39** (1964).

[15] A. Borel, J. Tits, *Groupes réductifs*, Publications mathématiques de l'I.H.E.S., tomé **27** (1965).

[16] N. Bourbaki, *General Topology*, Springer-Verlag (1995).

[17] F. A. Bogomolov, *The Brauer group of quotient spaces by linear group actions*, Izv. Akad. Nauk SSSR Ser. Mat. 51 (1987), 485–516; English transl. in Math. USSR Izv. 30 (1988).

[18] C. Chevalley, *Deux Theoremes d'Arithmetique*, Journal of the Mathematical Society of Japan Vol. **3**, No. 1 (1951).

[19] B. Conrad, *Reductive group schemes*, Société Mathématique de France (2014).

[20] P. Diaconis, I. M. Isaacs, *Super Characters and Superclasses for Algebra Groups*, Trans. of Amer. Math. Soc. Vol. **360**, Number 5, (2008).

[21] F. Digne, J. Michel, *Representations of Finite Groups of Lie Type*, London Mathematical Society Student Texts **21**, Cambridge University Press (1991).

[22] J. D. Dixon, M. P. F. du Sautoy, A. Mann, D. Segal, *Analytic Pro-p Groups*, second edition, Cambridge Studies in Advanced Mathematics, Vol. **61**, Cambridge University Press, Cambridge (1999).

[23] J. García Rodríguez, A. Jaikin-Zapirain, U. Jezernik, *Units of group rings, the Bogomolov multiplier and the fake degree conjecture*, Mathematical Proceedings of the Cambridge Philosophical Society, (2016),published online doi: 10.1017/S0305004116000748.

[24] A. S. Golsefidy, *Counting lattices in simple Lie groups: the positive characteristic case*, Duke Math. J. **161**, no. 3 (2012).

[25] J. González-Sánchez, *Kirillov's Orbit Method for p-Groups and Pro-p Groups*, Communications in Algebra, **37** (2009).

[26] A. Grothendieck, *Éléments de géométrie algébrique (rédigés avec la collaboration de Jean Dieudonné) : IV. Étude locale des schémas et des morphismes de schémas, Troisième partie*, Publication mathématiques de l'I.H.É.S., tome **28** (1966).

[27] Z. Halasi, *On the characters and commutators of finite algebra groups*, Journal of Algebra **275** (2004).

[28] G. Harder, *Minkowskische Reduktionstheorie über Funtionenkörpern*, Invent. math. **7** (1969).

[29] G. Higman, *Enumerating p-groups. I: Inequalities*, Proc. London Math. Soc. **10** (1960).

[30] R. E. Howe, *Kirillov Theory for Compact p-adic Groups*, Pacific Journal of Mathematics, Vol. **73** (1977).

[31] J. E. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics **21**, Springer-Verlag, New York (1975).

[32] B. Huppert, *Character theory of finite groups*, Walter de Gruyter & Co., Berlin, (1998).

[33] I. M. Isaacs, *Character Theory of Finite Groups*, Pure and Applied Mathematics **69**, Academic Press (1976).

[34] I. M. Isaacs, *Characters of Groups Associated with Finite Algebras*, Journal of Algebra **177** (1995).

[35] I. M. Isaacs, D. Karagueuzian, *Conjugacy in Groups of Upper Triangular Matrices*, Journal of Algebra **202** (1998).

[36] A. Jaikin-Zapirain, *A counterexample to the fake degree conjecture*, Chebyshevskii Sb. **5** (2004), no. 1(9), 188–192.

[37] A. Jaikin-Zapirain, *Zeta function of representations of compact p-adic analytic groups*, J. Amer. Math. Soc. **19** (2006), no. 1, 91–118.

[38] A. Jaikin, *On the representation growth of pro-p groups*, preprint (2004).

[39] A. Jaikin, B. Klopsch, *Analytic groups over general pro-p domains*, Journal London Math. Soc. **76** (2007).

[40] T. Kambayashi, M. Miyanishi, M. Takeuchi, *Unipotent algebraic groups*, Lecture notes in Mathematics **414**, Springer-Verlag, Berlin-Heidelberg (1974).

[41] M. C. Kang, *Bogomolov multipliers and retract rationality for semidirect products*, J. Algebra **397** (2014), 407–425.

[42] M. Kassabov, N. Nikolov, *Cartesian Products as Profinite Completions*, IMRN, Volume **2006** Article ID 72947.

[43] D. Kazhdan, *Proof of Springer's Hypothesis*, Israel Journal of Mathematics, Vol. **28**, No. 4 (1977).

[44] A. A. Kirillov, *Unitary representations of nilpotent Lie groups*, Russian Math. Surveys **17** (1962).

[45] A. A. Kirillov, *Merits and demerits of the Orbit Method*, Bull. Amer. Math. Soc. Vol **36** (1999).

[46] M. Kneser, *Starke Approximation in algebraischen Gruppen, I*, J. Reine Angew.Math. **218** (1965).

[47] E. I. Khukhro, *p-Automorphism of Finite p-Groups*, London Mathematical Society Lecture Notes Series **246**, Cambridge University Press (1998).

[48] B. Klopsch, *Representation growth and representation zeta functions of groups*, Note Mat. **33** (2013), no. 1.

[49] V. Landazuri, *On the minimal degrees of projective representations of the finite Chevalley groups*, Journal of Algebra **32** (1974).

[50] M. Larsen, A. Lubotzky, *Representation growth of linear groups*, J. Eur. Math. Soc. **10** (2008).

[51] M. W. Liebeck, A. Shalev, *Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks*, Journal of Algebra **276** (2004).

[52] M. W. Liebeck, A. Shalev, *Character Degrees and Random Walks in Finite Groups of Lie type*, Proc. London Math. Soc. (3) **90** (2005).

[53] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics **6**, Oxford University Press (2002).

[54] A. Lubotzky, *Subgroup growth and congruence subgroups*, Inventiones mathematicae **199** (1995) 267-295.

[55] A. Lubotzky, D. Segal, *Subgroup Growth*, Progress in Mathematics, Volume **212**, Birkhäuser (2003).

[56] A. Lubotzky and B. Martin, *Polynomial representation growth and the Congruence Subgroup Problem*, Israel Journal of Mathematics **144** (2004), 293-316.

[57] G. Malle, D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*, Cambridge studies in advanced mathematics **133**, Cambridge University Press (2011).

[58] G. A. Margulis, *Cobounded subgroups in algebraic groups over local fields*, Funkcional. Anal. i Priložen. 11:2 (1977). In Russian; translated in Funct. Anal. Appl. 11:2 (1977).

[59] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Vol. **17**, Springer-Verlag, Berlin (1991).

[60] H. Matsumura, *Commutative ring theory*, Cambridge studies in advanced mathematics **8**, Cambridge University Press (1989).

[61] J. Mennicke *Finite factor groups of the unimodular group*, Ann. Math. **81** (1965).

[62] J. Milne, *Class Field Theory*, Retrieved from http://www.jmilne.org/math/CourseNotes/CFT.pdf, Version 4.02, March 23, 2013.

[63] P. Moravec, *Schur multipliers and power endomorphisms of groups*, J. Algebra **308** (2007), no. 1, 12–25.

[64] P. Moravec, *Unramified groups of finite and infinite groups*, Amer. J. Math. **134** (2012), no. 6, 1679–1704.

[65] G. D. Mostow, *Fully reducible subgroups*, American Journal of Mathematics, Vol. **78**, No. 1 (1956).

[66] W. D. *Neumann, Manifold cutting and pasting groups*, Topology **14** (1975), no. 3, 237-244.

[67] R. Oliver, SK$_1$ *for finite group rings: II*, Math. Scand. **47** (1980), 195–231.

[68] V. P. Platonov, *The problem of strong approximation and the Kneser–Tits hypothesis for algebraic groups*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969). In Russian; translated in Math. USSR Izv. 3:3 (1969).

[69] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Pure and Applied Mathematics, Vol. **139**, Academic Press, Boston, MA (1994).

[70] G. Prasad, *Strong approximation for semi-simple groups over function fields*, Annals of Mathematics **105** (1977), 553-572.

[71] G. Prasad, *Elementary proof of a theorem of Bruhat-Tits-Rousseau and of a theorem of Tits*, Bulletin de la S. M. F., tome **110** (1982), p. 197-202.

[72] G. Prasad, A. Rapinchuk, *Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre*, Collected papers of John Milnor. V: Algebra (ed. H. Bass and TY Lam), Amer. Math. Soc., Providence, RI (2010).

[73] M. S. Raghunathan, *On the Congruence Subgroup Problem*, Publ. Math. I.H.E.S., tome **46** (1976).

[74] M. S. Raghunathan, *The congruence subgroup problem*, Proc. Indian Acad. Sci. (Math. Sci.) Vol. **114**, No. 4 (2004).

[75] L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge, A series of Modern Surveys in Mathematics, Volume **40**, Second edition, Springer, Berlin (2000).

[76] J. Rosenberg, *Algebraic K-theory and its applications*, Graduate Texts in Mathematics 147, Springer-Verlag (1994).

[77] J. Sangroniz, *Characters of algebra groups and unitriangular groups*, Finite groups 2003, Walter de Gruyter, Berlin (2004).

[78] I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **127** (1904), 20-50.

[79] J-P. Serre, *Lie Algebras and Lie Groups*, Lecture Notes in Mathematics **1500**, Springer-Verlag (1992).

[80] T. A. Springer, *Reductive groups*, Automorphic forms, representations and *L*-functions, Proc. Symp. Pure Math., vol. **33**, Part 2 (1977).

[81] R. Steinberg, *Lectures on Chevalley Groups*, Yale University (1967).

[82] B. Sury, *The Congruence Subgroup Problem*, Texts and Readings in Mathematics **24**, Hindustan Book Agency (2003).

[83] J. Tits, *Classification of algebraic semisimple groups, algebraic groups, and discontinuous groups*, Symposium Colorado, Boulder (1965) , AMS Proc. Symp. Pure Math. IX.

[84] A. Vera López, J. M. Arregi, *Conjugacy classes in Sylow p-subgroups of* $GL(n, q)$. *IV*, Glasgow Math. J. **36** (1994).

[85] C. Voll, *Functional equations for zeta functions of groups and rings*, Ann. Math. **172** (2010).

[86] C. T. C. Wall, *Norms of units in group rings*, Proc. London Math. Soc. (3) **29** (1974), 593-632.

[87] A. Weil, *Adeles and algebraic groups*, Int. for Advanced Study, Princeton, N.J. (1961).

[88] J. Wiegold, *Growth Sequences of Finite Groups IV*, Austral. Math. Soc. (Series A) **29** (1980).

[89] William C. Waterhouse *Introduction to Affine Group Schemes* Graduate Texts in Mathematics **66**, Springer-Verlag (1979).