Annals of Mathematics **174** (2011), 1009–1056
http://dx.doi.org/10.4007/annals.2011.174.2.6

Arithmetic groups have rational representation growth

By Nir Avni

Abstract

Let Γ be an arithmetic lattice in a semisimple algebraic group over a number field. We show that if Γ has the congruence subgroup property, then the number of n-dimensional irreducible representations of Γ grows like n^{α}, where α is a rational number.

1. Introduction

1.1. *Representation zeta functions.* This article is concerned with counting the number of representations of arithmetic groups. Suppose that Γ is a finitely generated group, and assume that Γ has finitely many irreducible complex representation of any fixed dimension, up to equivalence. Denote the number of irreducible complex representations of Γ of dimension n, up to equivalence by $r_n(\Gamma)$. In [17], the sequence $r_n(\Gamma)$ is called the *representation growth sequence of* Γ. If the sequence $r_n(\Gamma)$ is bounded by a polynomial in n, then it is useful to consider the following generating function.

Definition 1.1. The representation zeta function of Γ is the following function of $s \in \mathbb{C}$:

$$\zeta_\Gamma(s) = \sum_{n=1}^{\infty} r_n(\Gamma) n^{-s} = \sum_{\rho \in \operatorname{Irr}\Gamma} (\dim \rho)^{-s},$$

where $\operatorname{Irr}\Gamma$ denotes the set of finite dimensional, complex, and irreducible representations of Γ.

Note that if the sequence $r_n(\Gamma)$ grows polynomially, then the series above converges in some half plane of the form $\{s \mid \Re(s) > \alpha\}$. The infimum of the set of $\alpha \in \mathbb{R}$ such that the series in Definition 1.1 converges absolutely at $s = \alpha$, is called the *abscissa of convergence of* $\zeta_\Gamma(s)$ (or of Γ); we will denote it by α_Γ. The abscissa of converges is related to the rate of growth of the sequence $r_n(\Gamma)$ by

$$\alpha_\Gamma = \limsup_{N \to \infty} \frac{\log(r_1(\Gamma) + \cdots + r_N(\Gamma))}{\log N}.$$

1.2. *Arithmetic lattices.* The groups which we consider in this paper are arithmetic lattices in semisimple algebraic groups over fields of characteristics 0. We remind the reader of the construction of such groups. Let $\mathbb{K}$ be a finite extension of the field of rational numbers $\mathbb{Q}$. Denote the ring of integers of $\mathbb{K}$ by $\mathbb{O}$. For a valuation v of $\mathbb{K}$, we denote the completion of $\mathbb{K}$ with respect to the valuation v by $\mathbb{K}_v$, and we denote the valuation ring of $\mathbb{K}_v$ by $\mathbb{O}_v$. Suppose that Σ is a finite set of valuations of $\mathbb{K}$, containing all infinite (i.e., archimedian) valuations. The ring of Σ-integers of $\mathbb{K}$ is the set

$$\mathbb{O}_\Sigma = \{x \in \mathbb{K} \mid (\forall v \notin \Sigma) \quad v(x) \geq 0\}.$$

Let $\underline{G} \subset \underline{\mathrm{GL}_N}_{\mathbb{O}_\Sigma}$ be a linear algebraic group scheme over $\operatorname{Spec} \mathbb{O}_\Sigma$[1] whose generic fiber[2] is semisimple, simply connected, and connected. Assume, moreover, that for every non-archimedian valuation $v \in \Sigma$, the group $\underline{G}(\mathbb{K}_v)$ is noncompact. The group $\Gamma = \underline{G}(\mathbb{O}_\Sigma)$ is the arithmetic lattice. It is indeed a lattice, i.e., a discrete subgroup of finite covolume, in the topological group $\prod_{v \in \Sigma} \underline{G}(\mathbb{K}_v)$.

Denote the profinite completion of Γ by $\widehat{\Gamma}$, and, similarly, let $\widehat{\mathbb{O}_\Sigma}$ be the profinite completion of the ring $\mathbb{O}_\Sigma$. By the Chinese remainder theorem, $\widehat{\mathbb{O}_\Sigma} = \prod_{v \notin \Sigma} \mathbb{O}_v$. We say that Γ has the *congruence subgroup property* if the kernel of the natural map

$$\widehat{\Gamma} = \widehat{\underline{G}(\mathbb{O}_\Sigma)} \longrightarrow \underline{G}(\widehat{\mathbb{O}_\Sigma}) = \prod_{v \notin \Sigma} \underline{G}(\mathbb{O}_v)$$

is finite.

It is known that "most" irreducible lattices in Lie groups of rank ≥ 2 have the congruence subgroup property, and a conjecture of Serre asserts that all of them do. See [20] for a survey on the congruence subgroup property.

1.3. *Main Theorem.* In [17] it was proved that an arithmetic lattice in characteristic 0 has the congruence subgroup property if and only if the sequence $r_n(\Gamma)$ grows polynomially. Equivalently, such a lattice, Γ, has the congruence subgroup property if and only if the abscissa of convergence of Γ is finite. The main result in this paper is the following:

[1] Put more simply, we are given a set of polynomials $f_1, \dots, f_k$ in N^2 variables, such that the coefficients of the f_j's are in $\mathbb{O}_\Sigma$, and such that for every ring R and homomorphism $\varphi : \mathbb{O}_\Sigma \to R$, the set of solutions of the system of equations $(\varphi f_1)(x) = \cdots = (\varphi f_k)(x) = 0$ in $R^{N^2} = M_N(R)$ is a subgroup of $\mathrm{GL}_N(R)$. We call this set of solutions the *R points* of $\underline{G}$ and denote it by $\underline{G}(R)$.

[2] The generic fiber of $\underline{G}$ is the algebraic group $\underline{G} \otimes \operatorname{Spec} \overline{\mathbb{K}}$, where $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$.

THEOREM 1.2. *Let Γ be an arithmetic lattice in characteristics* 0 *that satisfies the congruence subgroup property. Then α_Γ — the abscissa of convergence of $\zeta_\Gamma(s)$ — is a rational number.*

Remark 1.3. If Γ does not satisfy the congruence subgroup property, then the sequence $r_n(\Gamma)$ grows super-polynomially by [17], and so the abscissa of convergence of $\zeta_\Gamma(s)$ is ∞.

Unfortunately, the proof of this theorem does not give a hint about the actual value of the abscissa of convergence of Γ, and, in fact, this value is known only in some very special cases; see [14] and [1].

In the rest of this subsection we describe the method of proof of Theorem 1.2. The proof follows a general strategy of Igusa and Denef; see also [22]. If $\Gamma = \underline{G}(\mathbb{O}_\Sigma)$ is an arithmetic lattice that has the congruence subgroup property, then there is a finite index subgroup Δ of Γ such that the representation zeta function of Δ has a Euler-like factorization

$$\zeta_\Delta(s) = \zeta_\infty(s) \times \prod_{\mathfrak{p}} \zeta_{\mathfrak{p}}(s),$$

where the product is over all primes of the ring $\mathbb{O}_\Sigma$, and the local zeta functions $\zeta_\infty(s)$ and $\zeta_{\mathfrak{p}}(s)$ will be described in Section 2. This fact was established in [14] and is a consequence of Margulis' super-rigidity theorem. We shall show that the abscissa of convergence is unchanged when passing to a finite-index subgroup. Hence, it is enough to show that the abscissa of convergence of Δ is rational. The archimedian local zeta function $\zeta_\infty(s)$ was studied in [14], where it was shown that it has a rational abscissa of convergence. In order to show that the infinite product $\prod_{\mathfrak{p}} \zeta_{\mathfrak{p}}(s)$ has rational abscissa of convergence, we will study the dependence of $\zeta_{\mathfrak{p}}(s)$ on the prime ideal $\mathfrak{p}$.

Let $q = |\mathbb{O}_\Sigma/\mathfrak{p}|$. In contrast to the case considered in [22], the local zeta functions are not rational functions in q^{-s}, but rather are of the form

$$\sum_{i=1}^{N(\mathfrak{p})} n_i(\mathfrak{p})^{-s} \cdot f_i(\mathfrak{p}, q^{-s}), \tag{1.1}$$

where $f_i(\mathfrak{p}, x)$ are rational functions in x (this is proved in [12]).

A sequence of numbers, $k(\mathfrak{p})$, indexed by the primes of $\mathbb{O}_\Sigma$, is called geometric if there is a variety $\mathscr{K}$, defined over $\mathbb{O}_\Sigma$, such that for every $\mathfrak{p}$, $k(\mathfrak{p})$ is equal to the number of points of the variety $\mathscr{K}$ over the finite field $\mathbb{O}_\Sigma/\mathfrak{p}$ (this terminology is taken from [13]). A reasonable guess is that the numbers $N(\mathfrak{p}), n_i(\mathfrak{p})$, and the coefficients of the rational functions $f_i(\mathfrak{p}, x)$ that appear in (1.1) are geometric. We make two changes in order to prove this. The first is that we allow $\mathscr{K}$ to be a definable set, rather than a variety; the second is that we replace $\zeta_{\mathfrak{p}}(s)$ by another sequence, $\xi_{\mathfrak{p}}(s)$, such that the abscissae of convergence of $\prod_{\mathfrak{p}} \zeta_{\mathfrak{p}}(s)$ and $\prod_{\mathfrak{p}} \xi_{\mathfrak{p}}(s)$ are equal, and then show that $\xi_{\mathfrak{p}}(s)$ has a geometric formula.

After showing the geometric nature of the "new" local zeta functions, we use standard results in Algebraic Number Theory (the Lang-Weil estimates and Chebotarev Density Theorem) to finish the proof of Theorem 1.2.

1.4. *Organization of the paper.* In Section 2 we set some notation and review the Euler factorization of representation zeta functions of arithmetic lattices. Section 3 is a collection of facts we need from representation theory, algebraic geometry, and the theory of finite groups. In Section 4 we collect necessary facts from the model theory of fields, pseudo-finite fields, and valued fields. In Section 4 we also define the notion of V-function, which is our main technical tool. In Section 5 we show that local zeta functions (or, rather, approximations thereof) are integrals of the same V-function. In Section 6 we show that any Euler product, such that the local factors are integrals of the same V-function, has rational abscissa of convergence.

1.5. *Acknowledgment.* This work is a part of the author's Ph.D. thesis, supervised by Alex Lubotzky. It is a pleasure to thank Alex for introducing the problem to me, for his advices when this work was done, and for his remarks on previous versions of this paper. I have also learned much by talking about this project with Andrei Jaikin, Fritz Grunewald, Michael Larsen, Chris Voll, David Kazhdan, and Udi Hrushovski. I heartily thank them all. I thank Laszlo Pyber for referring me to the the paper [10], and Peter Sarnak for referring me to [21]. Finally, I thank the referee for pointing out many typos and making many suggestions that improved the exposition in this paper.

1.6. *Notation.* For the reader's convenience, here is a list of symbols that are used throughout the article.

- Γ, Δ: lattices.
- $\underline{G}, G_p, G_p^1$: a group scheme, the group $\underline{G}(\mathbb{Z}_p)$, the first congruence subgroup of G_p (i.e., the kernel of the map $\underline{G}(\mathbb{Z}_p) \to \underline{G}(\mathbb{F}_p)$).
- $\mathfrak{g}, \mathfrak{g}_p, \mathfrak{g}_p^1$: the corresponding Lie algebras.
- $\operatorname{Irr} H, \zeta_H(s)$: the set of complex, irreducible, and finite dimensional representations of a group H, the representation zeta function of H (see §1.1).
- $\operatorname{Irr}(H|\rho), \zeta_{H|\rho}(s)$: the irreducible representations of H that lie over ρ, the corresponding zeta function (see §3.1).
- Σ: a finite set of primes.
- Ad^*: coadjoint action.
- $\mathscr{X}, \mathscr{Y}$: the definable sets parametrizing the representations of the first congruence subgroup and of the leaves of the decomposition tree (see §§5.1, 5.3).

- $(\zeta_n(s)) \sim (\xi_n(s))$: equivalence for two sequences of Dirichlet series (see §3.7).
- $\mathcal{L}_{\text{Rings}}, \mathcal{L}_{Vf}, \mathcal{T}_f, \mathcal{T}_{pf}, \mathcal{T}_{Hvf}$: The first order language of rings, the first order language of valued rings, the theory of fields, the theory of pseudo-finite fields, the theory of Henselian valued fields (see §§4.1, 4.4).
- $\mathrm{val}, \mathrm{ac}$: the function symbols for valuation and angular components (see §4.4).
- $\mathbb{A}_V, \mathbb{A}_R, \mathbb{A}_O$: the value field sort, the residue field sort, and the value group sort for $\mathcal{L}_{Vf}$ (see §4.4).
- $\mathbb{M}_p$: the model $(\mathbb{Q}_p, \mathbb{Z}, \mathbb{F}_p)$ for $\mathcal{T}_{Hvf}$ (see §4.4).
- $f^{\mathbb{M}_p}$: the interpretation of the definable function f in the model $\mathbb{M}_p$ (see §4.4).
- Grass,Grass_U: the Grassmanian of subspaces of $\mathfrak{gl}_n$, the subset of unipotent Lie algebras (see §5.3).
- $\Psi_p, \widetilde{\Psi_p}, \Xi_p, \widetilde{\Xi}_p, \Phi_p, \widetilde{\Phi_p}, \Lambda_p, \Omega_p$: various orbit method functions (see §5.1).
- If $\underline{X}$ is a scheme, we denote the definable set associated to it by X, and the base change of X to R by X_R.
- If A is a locally compact abelian group, we denote by $A^\vee$ its Pontrjagin dual.

2. **Euler factorization**

2.1. *Notation.* In order to remove a layer of unnecessary notational complexity, we assume that the arithmetic lattice Γ is defined over $\mathbb{Q}$. That is, we assume that $\Gamma = \underline{G}(\mathbb{Z}_\Sigma)$ where Σ is a finite set of prime numbers and $\underline{G} \subset (\underline{\mathrm{GL}_n})_{\mathbb{Z}_\Sigma}$ is a linear algebraic group scheme over $\operatorname{Spec} \mathbb{Z}_\Sigma$ whose generic fiber is semisimple, simply connected, and connected. The proof for general Γ is completely analogous.

For every prime p not in Σ, we denote the group $\underline{G}(\mathbb{Z}_p)$ by G_p. The first congruence subgroup of G_p — which we denote by G_p^1 — is the kernel of the reduction modulo p homomorphism from G_p to $\underline{G}(\mathbb{F}_p)$.

In the following, the word 'representation' will have several meanings. If the group is discrete, we just mean a complex representation of finite dimension. For profinite groups, a representation should also be continuous (and thus have finite image). If the group is algebraic (or, more generally, pro-algebraic), a representation should be (finite dimensional and) rational. This remark applies also to related notions, such as $\operatorname{Irr} H$ and $\zeta_H(s)$.

2.2. *Euler factorization.* In this subsection, we describe without proofs the Euler factorization of $\zeta_\Gamma(s)$ and refer the reader to [14] for the details. If Δ is a finitely generated group, we denote by $\widehat{\Delta}$ the pro-finite completion of Δ. For a discrete group Δ, the pro-algebraic completion of Δ is defined to be a pro-algebraic group Δ^a, together with a homomorphism $\pi : \Delta \to \Delta^a$, such that every finite dimensional representation of Δ factors uniquely through Δ^a. The pro-algebraic completion is unique up to isomorphism, and, by definition, it has the same representations as the group itself. Therefore $\zeta_\Delta(s) = \zeta_{\Delta^a}(s)$. Note that in this equality, the left-hand side counts all representations of Δ, whereas the right-hand side counts only rational representations of Δ^a.

Suppose $\Gamma = \underline{G}(\mathbb{Z}_\Sigma)$ satisfies the congruence subgroup property. It was shown in [14] that there is a finite index subgroup $\Delta \subset \Gamma$ such that the pro-algebraic completion of Δ is the direct product of $\widehat{\Delta}$ and $\underline{G}(\mathbb{C})$. Because of the congruence subgroup property, and by making Δ smaller if necessary, we may assume that $\widehat{\Delta}$ is a subgroup (of finite index) of $\prod_{p \notin \Sigma} \underline{G}(\mathbb{Z}_p)$. We shall see later (Corollary 3.4) that the abscissa of convergence of Δ is equal to the abscissa of convergence of Γ.

Denote the projection from $\widehat{\Delta}$ to $\underline{G}(\mathbb{Z}_p)$ by π_p. Since $\widehat{\Delta}$ is of finite index in $\prod_{p \notin \Sigma} \underline{G}(\mathbb{Z}_p)$, there is a finite set of primes T, such that if p does not belong to T, then $\pi_p(\widehat{\Delta}) = \underline{G}(\mathbb{Z}_p)$. We then have

$$\zeta_\Delta(s) = \prod_{p \in T} \zeta_{\pi_p(\widehat{\Delta})}(s) \cdot \prod_{p \notin T} \zeta_{G_p}(s) \cdot \zeta_{\underline{G}(\mathbb{C})}(s). \tag{2.1}$$

We shall call the factor $\zeta_{G_p}(s)$ (or $\zeta_{\pi_p(\Delta)}(s)$) the local zeta function at the prime p, and call the factor $\zeta_{\underline{G}(\mathbb{C})}(s)$ the local zeta function at infinity.

The abscissa of convergence for the local zeta function at infinity, $\zeta_{\underline{G}(\mathbb{C})}(s)$, was computed in [14]. If $\underline{G}$ has root system Φ and if we denote the rank of Φ by r, and denote the number of positive roots of Φ (relative to some choice of simple roots) by $|\Phi_+|$, then the abscissa of convergence of $\zeta_{\underline{G}(\mathbb{C})}(s)$ is equal to $\frac{r}{|\Phi_+|}$. In particular, the abscissa of convergence of the local zeta function at infinity is rational.

In [12], the following theorem is proved.

Theorem 2.1. *For every prime p there are*

(1) *a finite set I_p;*
(2) *polynomials $f_i^p(x) \in \mathbb{Z}[x]$ with nonnegative coefficients for $i \in I_p$;*
(3) *nonnegative integers n_i, for $i \in I_p$, and nonnegative integers $A_{i,j}, B_{i,j}$ for $i \in I_p$ and $1 \le j \le n_i$;*

such that

$$\zeta_{G_p}(s) = \sum_{i \in I_p} n_i^{-s} \frac{f_i^p(p^{-s})}{\prod_j \left(1 - p^{-A_{i,j}s + B_{i,j}}\right)}.$$

The same is true for every finite index subgroup of G_p.

In particular, the abscissa of convergence for every local zeta function is rational. In order to prove that the abscissa of convergence of the 'global' zeta function is rational, we shall need to understand the relation between the local zeta functions for different primes. Indeed, this paper is mainly an attempt to give an approximate formula to the local zeta functions, which is uniform in the prime p.

3. Algebraic preliminaries

3.1. *Relative zeta functions.* Let H be a group and let K be a subgroup of H. If ρ is a representation of K, we denote its induction to H by $\operatorname{Ind}_K^H \rho$. If χ is a representation of H, we denote its restriction to K by $\operatorname{Res}_K^H \chi$.

Definition 3.1. Let H be a group, let K be a normal subgroup of H, and let τ be an irreducible representation of K. We denote by $\operatorname{Irr}(H|\tau)$ the set of irreducible representations ρ of H such that τ is a sub-representation of $\operatorname{Res}_K^H \rho$ (or equivalently, such that ρ is a sub-representation of $\operatorname{Ind}_K^H \tau$). Note that if $\rho \in \operatorname{Irr}(H|\tau)$, then $\dim \tau$ divides $\dim \rho$.

Let $r_n(H|\tau)$ be the number of representations in $\operatorname{Irr}(H|\tau)$ of dimension $n \cdot \dim \tau$. We define the relative zeta function as

$$\zeta_{H|\tau}(s) = \sum_n r_n(H|\tau) \cdot n^{-s} = \sum_{\rho \in \operatorname{Irr}(H|\tau)} \left(\frac{\dim \rho}{\dim \tau} \right)^{-s}.$$

Lemma 3.2. *Let H be a group and let K be a normal subgroup of H of finite index. The group H acts on the set* $\operatorname{Irr}(K)$ *by conjugation. For every $\tau \in \operatorname{Irr}(K)$ we denote the stabilizer of τ under this action by* $\operatorname{Stab}_H \tau$. *Then*

$$\zeta_H(s) = \sum_{\tau \in \operatorname{Irr}(K)} \frac{1}{[H : \operatorname{Stab}_H \tau]} (\dim \tau)^{-s} \zeta_{H|\tau}(s).$$

Proof. Let E be the set of pairs $(\tau, \rho) \in \operatorname{Irr}(K) \times \operatorname{Irr}(H)$ such that τ is a sub-representation of $\operatorname{Res}_K^H \rho$. Then

$$\sum_{(\tau,\rho) \in E} \frac{1}{[H : \operatorname{Stab}_H \tau]} (\dim \rho)^{-s} = \sum_{\tau \in \operatorname{Irr}(K)} \frac{1}{[H : \operatorname{Stab}_H \tau]} (\dim \tau)^{-s} \zeta_{H|\tau}(s).$$

On the other hand, for every $\rho \in \operatorname{Irr}(H)$, the set of $\tau \in \operatorname{Irr}(K)$ such that τ is a sub-representation of $\operatorname{Res}_K^H \rho$ is a single H orbit and so

$$\begin{aligned} \sum_{(\tau,\rho) \in E} \frac{1}{[H : \operatorname{Stab}_H \tau]} (\dim \rho)^{-s} &= \sum_{\rho \in \operatorname{Irr}(H)} (\dim \rho)^{-s} \left(\sum_{\tau | (\tau,\rho) \in E} \frac{1}{[H : \operatorname{Stab}_H \tau]} \right) \\ &= \sum_{\rho \in \operatorname{Irr}(H)} (\dim \rho)^{-s}. \end{aligned}$$

□

Lemma 3.3. *Let $K \subset H \subset L$ be groups. Assume that H is of finite index in L and that K is normal in L. Let $\tau \in \operatorname{Irr}(K)$. Then for each N,*

$$\begin{aligned} \frac{1}{[L : H]} \left(r_1(H|\tau) + \cdots + r_{N/[L:H]}(H|\tau) \right) &\leq r_1(L|\tau) + \cdots + r_N(L|\tau) \\ &\leq \left(r_1(H|\tau) + \cdots + r_N(H|\tau) \right) [L : H], \end{aligned}$$

and for every $s \in \mathbb{R}$, if one of $\zeta_{H|\tau}(s)$ or $\zeta_{L|\tau}(s)$ converges, then so does the other, and

$$[L:H]^{-1-s}\zeta_{H|\tau}(s) \leq \zeta_{L|\tau}(s) \leq [L:H] \cdot \zeta_{H|\tau}(s).$$

Proof. Consider the bipartite graph whose vertices are $\operatorname{Irr}(L|\tau) \sqcup \operatorname{Irr}(H|\tau)$ and there is an edge between $\rho_1 \in \operatorname{Irr}(L|\tau)$ and $\rho_2 \in \operatorname{Irr}(H|\tau)$ if ρ_2 is a subrepresentation of $\operatorname{Res}_H^L \rho_1$. Note that

(1) every vertex has positive degree;
(2) the degree of every vertex is bounded by $[L:H]$;
(3) if $\rho_1 \in \operatorname{Irr}(L|\tau)$ and $\rho_2 \in \operatorname{Irr}(H|\tau)$ are connected, then $\dim \rho_1 \leq \dim \rho_2 \leq [L:H] \cdot \dim \rho_1$.

Let $\operatorname{Irr}(L|\tau)_N \subset \operatorname{Irr}(L|\tau)$ be the set of representations of dimension less than or equal to $N \dim \tau$, and define similarly the set $\operatorname{Irr}(H|\tau)_N$. The set $\operatorname{Irr}(L|\tau)_N$ is contained in the set of neighbors of $\operatorname{Irr}(H|\tau)_N$, so

$$|\operatorname{Irr}(L|\tau)_N| \leq |\operatorname{Irr}(H|\tau)_N| \cdot [L:H].$$

Similarly, the set $\operatorname{Irr}(H|\tau)_{N/[L:H]}$ is contained in the set of neighbors of $\operatorname{Irr}(L|\tau)_N$, so

$$|\operatorname{Irr}(H|\tau)_{N/[L:H]}| \leq |\operatorname{Irr}(L|\tau)_N| \cdot [L:H].$$

This proves the first two inequalities. Similar argument shows the other two. □

Corollary 3.4 (see also [17, Cor. 2.3]). *If $H \subset L$ is a subgroup of finite index, then the abscissae of convergence of $\zeta_H(s)$ and of $\zeta_L(s)$ are equal.*

Proof. Take K to be the trivial group in Lemma 3.3. □

3.2. *Lie algebras.* There are several notions of Lie algebras, exponential functions, and logarithmic functions for pro-p groups and for finite subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$. We shall give them all here in order to fix notations. We assume in this section that $\underline{G} \subset \underline{\mathrm{GL}_n}_{\mathbb{Z}_\Sigma}$ is a group scheme over $\operatorname{Spec} \mathbb{Z}_\Sigma$. Recall that we denote the group $\underline{G}(\mathbb{Z}_p)$ by G_p and denote its first congruence subgroup by G_p^1.

We start with the Lie algebra of G_p^1. There are three definitions for the Lie algebra $\mathfrak{g}_p^1$ of G_p^1. Fortunately, they coincide for almost all primes.

Let $\underline{\mathfrak{g}} \subset \underline{M_n}_{\mathbb{Z}_\Sigma}$ be the tangent space at the identity, relative to $\operatorname{Spec} \mathbb{Z}_\Sigma$. For every $p \notin \Sigma$, the set $\underline{\mathfrak{g}}(\mathbb{Z}_p) \subset M_n(\mathbb{Z}_p)$ is closed under addition and under taking commutators. The algebraic Lie algebra of G_p^1 is the set

$$\{A \in \underline{\mathfrak{g}}(\mathbb{Z}_p) \mid A \equiv 0 \pmod{p}\},$$

together with the addition and Lie brackets induced from $M_n(\mathbb{Z}_p)$. Using the embedding of G_p into $\mathrm{GL}_n(\mathbb{Z}_p)$, the analytic Lie algebra is the set of all matrices of the form

$$\log(I-g) = (I-g) + \frac{(I-g)^2}{2} + \frac{(I-g)^3}{3} + \cdots ,$$

where $g \in G_p^1$. For the analytic Lie algebra, the Lie algebra operations, i.e., addition and Lie brackets, are the usual addition and commutator of matrices. The last definition, due to Lazard (see [6, §4.5]) is that the Lie algebra, as a set, is just G_p^1, but the addition and brackets need to be redefined. As stated before, those three definitions give isomorphic Lie algebras for almost all primes. We denote the algebraic Lie algebra of the group G_p^1 by $\mathfrak{g}_p^1$.

We shall use all three definitions. The algebraic definition implies that there is formula $\phi(x_{i,j})$ in n^2 variables, in the language of valued fields (see §4), such that for every prime p and every $A \in M_n(\mathbb{Q}_p)$, we have $A \in \mathfrak{g}_p^1$ if and only if $\phi(A)$ holds. This will enable us to connect the $\mathfrak{g}_p^1$'s for different primes p. The analytic definition is useful in order to treat other pro-p subgroups of G_p; we shall promptly do this. The Lazard definition is used in [12], to which we shall refer.

We fix n and let

$$\mathscr{U} = \{g \in M_n(\mathbb{Z}_p) \mid \lim_{k\to\infty} (g-I)^k = 0\}$$

and

$$\mathscr{N} = \{A \in M_n(\mathbb{Z}_p) \mid \lim_{k\to\infty} A^k = 0\}$$

be the sets of pro-unipotent and pro-nilpotent elements respectively. For $g \in \mathscr{U}$, define $\log(g)$ as the series

$$\log(g) = (g-I) + \frac{(g-I)^2}{2} + \frac{(g-I)^3}{3} + \cdots .$$

For $A \in \mathscr{N}$, define $\exp(A)$ as the series

$$\exp(A) = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots .$$

Lemma 3.5. *If $p > 2n$, then the series defining* log *and* exp *converge, and the functions* log, exp *are inverses. Moreover, if $A, B \in \mathscr{N}$, and the reductions* mod *p, $\overline{A}, \overline{B}$, are in a nilpotent Lie subalgebra of $M_n(\mathbb{F}_p)$, then the Campbell Hausdorff formula holds*:

$$\begin{aligned}(3.1)\quad & \log(\exp(A)\cdot\exp(B)) \\ &= \sum_{m=1}^{\infty} \frac{(-1)^m}{m} \sum_{r_i+s_i>0} \frac{(\sum_{i=1}^m (r_i+s_i))^{-1}}{r_1!\cdot s_1! \times \cdots \times r_m!\cdot s_m!} R_{r_1,s_1,\ldots,r_m,s_m}(A,B),\end{aligned}$$

where $R_{r_i,s_i}(A,B)$ is defined by

$$R_{r_1,s_1,\ldots,r_m,1}(A,B) = (\mathrm{ad}(A))^{r_1}(\mathrm{ad}(B))^{s_1}\cdots(\mathrm{ad}(A))^{r_m}(B),$$

$$R_{r_1,s_1,\ldots,1,0}(A,B) = (\mathrm{ad}(A))^{r_1}(\mathrm{ad}(B))^{s_1}\cdots(\mathrm{ad}(B))^{r_{m-1}}(A),$$

and $R_{r_i,s_i}(A,B) = 0$ otherwise.

Proof. If $A \in \mathscr{N}$, then A^n is divisible by p. Therefore for every N, A^N is divisible by $p^{\lfloor \frac{N}{n} \rfloor}$. As the maximal power of p that divides $N!$ is $\lfloor \frac{N}{p} \rfloor + \lfloor \frac{N}{p^2} \rfloor + \cdots < \frac{2N}{p}$, we get that if $p > 2n$, then the term $\frac{A^N}{N!}$ is divisible by $p^{\lfloor \frac{N}{n} \rfloor - \frac{2N}{p}}$. We get that $v_p\left(\frac{A^N}{N!}\right)$ tends to infinity as N tends to infinity. Therefore, the series defining exp is convergent. The same argument shows that the series defining log is convergent.

Similarly, if $\overline{A}, \overline{B}$ are contained in a nilpotent Lie subalgebra of $\mathfrak{gl}_n(\mathbb{F}_p)$, then $R_{r_1,s_1,\dots,r_m,s_m}(A,B)$ is divisible by

$$p^{\frac{r_1+s_1+\cdots+r_m+s_m}{n}},$$

whereas the maximal power of p that divides $r_1!s_1!\dots r_m!s_m!$ is less than

$$\frac{2(r_1+s_1+\cdots+r_m+s_m)}{p}.$$

So the right-hand side of (3.1) is convergent, and therefore is equal to the left-hand side. □

Definition 3.6. Let $R \subset G_p$ be a pro-p subgroup of G_p such that $G_p^1 \subset R$. Since $\overline{R}$ (the reduction of R modulo p) is a p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$, we know that every element in $\overline{R}$ is unipotent. Hence $R \subset \mathscr{U}$. We define the Lie algebra of R to be the image of R under the map log and denote it by $\mathrm{Lie}(R)$.

Note that $\overline{\mathrm{Lie}(R)} \subset \mathbb{M}_n(\mathbb{F}_p)$ is a nilpotent Lie algebra.

There is yet another notion of Lie algebras, this time for subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$. It is taken from [18]. Assume $p > 2n$ and let $\Upsilon \subset \mathrm{GL}_n(\mathbb{F}_p)$. If $\gamma \in \Upsilon$ is an element of order p, then $(\gamma - I)^n = 0$. We define

$$\log(\gamma) = (\gamma - I) + \frac{(\gamma - I)^2}{2} + \cdots + \frac{(\gamma - I)^{n-1}}{n-1}.$$

The Lie algebra of Υ is the set

$$\mathrm{Lie}(\Upsilon) = \mathbb{F}_p - \mathrm{span}\{\log(\gamma) \mid \gamma \in \Upsilon,\ \text{the order of } \gamma \text{ is } p\}.$$

The set $\mathrm{Lie}(\Upsilon)$ is shown in [18] to be closed under commutators.

3.3. *Orbit method.* Recall that for a locally compact abelian group A, the Pontjagin dual of A — which we denote by $A^\vee$ — is the set of all continuous homomorphisms from A to the circle group $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$.

Let $R \subset G_p$ be a pro-p subgroup such that $G_p^1 \subset R$. Let $\mathfrak{r} = \mathrm{Lie}(R)$. The group R acts on the (additive) group $\mathfrak{r}$ by conjugation, and therefore acts on the Ponrjagin dual $\mathfrak{r}^\vee$. We call this action the *coadjoint* action and denote it by Ad^*. Concretely, it is given by

$$(\mathrm{Ad}^*(g)\theta)(X) = \theta(X^{g^{-1}}) = \theta(gXg^{-1}).$$

THEOREM 3.7. *Given $\underline{G}$, there is an integer p_0, such that if $p > p_0$ is a prime and if $Q \subset R \subset G_p$ are pro-p subgroups of G_p with Lie algebras $\mathfrak{q} \subset \mathfrak{r}$ respectively, then the following hold.*

(1) *There is a bijection Ξ_R between $\operatorname{Ad}^*(R)$ orbits on $\mathfrak{r}^\vee$ and irreducible representations of R. If $\theta \in \mathfrak{r}^\vee$, we shall write $\Xi_R(\theta)$ instead of $\Xi_R(\operatorname{Ad}^*(R)\theta)$.*

(2) *The character of $\Xi_R(\theta)$ is given by*

$$\chi_{\Xi_R(\theta)}(g) = \frac{1}{|\operatorname{Ad}^*(R)\theta|^{1/2}} \sum_{\phi \in \operatorname{Ad}^*(R)\theta} \phi(\log(g)).$$

(3) *If $\theta \in \mathfrak{r}^\vee$, then the dimension of $\Xi_R(\theta)$ is $|\operatorname{Ad}^*(R)\theta|^{1/2}$.*

(4) *If $\theta \in \mathfrak{r}^\vee$, and $\tau \in \mathfrak{q}^\vee$, then $\Xi_Q(\tau)$ is a sub-representation of $\operatorname{Res}^R_S \Xi_R(\theta)$ if and only if there is $g \in R$ such that $\tau = \operatorname{Ad}^*(g)\theta|_{\mathfrak{q}}$.*

Proof. The proof of (1) and (2) is identical to the proof of Theorem 1.1 in [8], using the fact that $\mathfrak{r}$ is closed under addition and brackets and using the Campbell Hausdorff formula. (3) follows from (2) by evaluating the character at 1. (4): By (2), for every $g \in Q$ the evaluation at g of the characters of $\Xi_Q(\tau)$ and $\operatorname{Res}^R_Q \Xi_R(\theta)$ are

$$\chi_{\Xi_Q(\tau)}(g) = \frac{1}{|\operatorname{Ad}^*(Q)\tau|^{1/2}} \sum_{\phi \in \operatorname{Ad}^*(Q)\tau} \phi(\log(g))$$

and

$$\chi_{\operatorname{Res}^R_Q \Xi_R(\theta)} = \frac{1}{|\operatorname{Ad}^*(R)\theta|^{1/2}} \sum_{\psi \in \operatorname{Ad}^*(R)\theta} \psi(\log(g)).$$

The map $\exp : \mathfrak{q} \to Q$ is a measure preserving bijection and hence

$$\begin{aligned}(\Xi_Q(\tau), \operatorname{Res}^R_Q \Xi_R(\theta)) &= \int_Q \chi_{\Xi_Q(\tau)}(g) \cdot \overline{\chi_{\operatorname{Res}^R_Q \Xi_R(\theta)}(g)} dg \\ &= \frac{1}{|\operatorname{Ad}^*(Q)\tau|^{1/2}} \cdot \frac{1}{|\operatorname{Ad}^*(R)\theta|^{1/2}} \sum_{\phi \in \operatorname{Ad}^*(Q)\tau} \sum_{\psi \in \operatorname{Ad}^*(R)\theta} \int_{\mathfrak{q}} \phi(X) \cdot \overline{\psi|_{\mathfrak{q}}(X)} dX.\end{aligned}$$

Every ϕ and $\psi|_{\mathfrak{q}}$ in the above sum are one dimensional characters of $\mathfrak{q}$, and by orthogonality of characters,

$$\int_{\mathfrak{q}} \phi(X)\overline{\psi|_{\mathfrak{q}}(X)} dX = \begin{cases} 1 & \text{if } \phi = \psi|_{\mathfrak{q}} \\ 0 & \text{if } \phi \neq \psi|_{\mathfrak{q}}. \end{cases}$$

The claim follows immediately from this. □

3.4. *Subgroups of* $\operatorname{GL}_n(\mathbb{F}_p)$. We review some definitions from [18], and advise the reader to have a copy in hand. We fix a prime number p and a natural number $p > n$. Let Υ be a subgroup of $\operatorname{GL}_n(\mathbb{F}_p)$. We shall denote by Υ^+ the subgroup of Υ which is generated by the p-elements of Υ.

If $L \subset \mathrm{M}_n(\mathbb{F}_p)$ is a Lie subalgebra, we denote by $\underline{\exp L}$ the algebraic group generated by the one parameter subgroups

$$t \mapsto \exp(tX)$$

for all nilpotent $X \in L$.

If Υ is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$, we define

$$\widetilde{\Upsilon} = \underline{\exp(\mathrm{Lie}(\Upsilon))},$$

where $\mathrm{Lie}(\Upsilon)$ was defined in Section 3.2.

For a subset $S \subset \Upsilon$, we denote the subgroup generated by S by $\langle S \rangle$. For an algebraic group G we denote $\mathrm{Lie}(G)$ as the Lie algebra of G. If G is defined over $\mathbb{F}_p$, then $\mathrm{Lie}(G)$ can be thought of as a subalgebra of $\mathfrak{gl}_n(\mathbb{F}_p)$. If $L \subset \mathfrak{gl}_n(\mathbb{F}_p)$, we denote by $\exp L$ the set of elements of the form $\exp X$ for $X \in L$ a nilpotent element.

Proposition 3.8. *For every n there is an N such that if $L \subset \mathrm{gl}_n(\mathbb{F}_p)$ is Lie algebra that is generated by nilpotents, then $\langle \exp L \rangle = (\exp L)^N$. Moreover, there are elements $X_1, \dots, X_N \in L \cap N_n(\mathbb{F}_p)$ such that*

$$\langle \exp L \rangle = \langle \exp X_1 \rangle \times \cdots \times \langle \exp X_N \rangle.$$

Proof. The claims in the proposition are trivial if p is bounded. For the proof, we shall assume that p is large enough, and so we can use the results of [18]. Also, the first statement clearly follows from the second, so we prove the second claim.

Let $R \subset L$ be the unipotent radical of L. We define algebraic groups

$$A = \underline{\exp L} \quad \text{and} \quad B = \underline{\exp R}.$$

The algebraic group B is normal in A, and therefore the group $B(\mathbb{F}_p)$ is normal in $A(\mathbb{F}_p)$. We have an exact sequence

$$0 \to B(\mathbb{F}_p) \to A(\mathbb{F}_p) \to (A/B)(\mathbb{F}_p) \to H^1(\mathbb{F}_p, B).$$

Since B is unipotent, the Galois cohomology group, $H^1(\mathbb{F}_p, B)$, vanishes, and hence $A(\mathbb{F}_p)/B(\mathbb{F}_p) = (A/B)(\mathbb{F}_p)$. Since $B(\mathbb{F}_p)$ is a p-group, we get that $B(\mathbb{F}_p) \lhd A(\mathbb{F}_p)^+$ and that $A(\mathbb{F}_p)^+/B(\mathbb{F}_p) = (A/B)(\mathbb{F}_p)^+$.

The first part of Theorem A of [18] implies that $\mathrm{Lie}(A) = L$ and $\mathrm{Lie}(B) = R$. Hence $\mathrm{Lie}(A/B) = L/R$. Since L is nilpotently generated, so is L/R. Hence the Lie algebra L/R is semisimple (and not only reductive). In this case, there are nilpotent elements $\overline{X_1}, \dots, \overline{X_M} \in \mathrm{Lie}(A/B)$ (where M depends only on n) such that

$$(A/B)(\mathbb{F}_p)^+ = \langle \exp \overline{X_1} \rangle \times \cdots \times \langle \exp \overline{X_M} \rangle. \tag{3.2}$$

By induction on the nilpotency class of R, there are nilpotent elements $Y_1, \ldots$ $\ldots, Y_K \in R$ such that

$$B(\mathbb{F}_p) = \langle \exp Y_1 \rangle \times \cdots \times \langle \exp Y_K \rangle. \tag{3.3}$$

Choose $X_i \in L$ such that $X_i + R = \overline{X_i}$. From (3.2) and (3.3) we get that

$$A(\mathbb{F}_p)^+ = \langle \exp X_1 \rangle \times \cdots \times \langle \exp X_M \rangle \cdot \langle \exp Y_1 \rangle \times \cdots \times \langle \exp Y_K \rangle.$$

It remains to show that $A(\mathbb{F}_p)^+ = \langle \exp L \rangle$. Clearly, if $X \in L$, then $\exp X \in A(\mathbb{F}_p)$, and so $\langle \exp L \rangle \subset A(\mathbb{F}_p)^+$. For the converse, suppose that $u \in A(\mathbb{F}_p)$ is an element of order p. Denoting $X = \log u$, we get

$$X = \log u \in \langle \log A(\mathbb{F}_p) \rangle \overset{(1)}{=} \operatorname{Lie}\left(\widetilde{A(\mathbb{F}_p)}\right) \overset{(2)}{=} \operatorname{Lie}(A) = \operatorname{Lie}(\underline{\exp L}) \overset{(3)}{=} L,$$

where (1) follows from first part of Theorem B of [18], (2) follows from the second part of the same theorem, and (3) follows from the first part of Theorem A of [18].

Since $A(\mathbb{F}_p)^+$ is generated by the p-elements in $A(\mathbb{F}_p)$, we get that $A(\mathbb{F}_p)^+ \subset \langle \exp L \rangle$. □

We have the following corollary, which will not be used in the rest of the article; see also [10] for a very similar proof.

Corollary 3.9. *For every n there is N such that for every prime p and a group $G \subset \mathrm{GL}_n(\mathbb{F}_p)$, there are elements $x_1, \ldots, x_N \in G$ such that*

$$G = \langle x_1 \rangle \times \cdots \times \langle x_N \rangle.$$

Proof. By Theorem B of [18], $G^+ = \widetilde{G}(\mathbb{F}_p)^+$. Every nilpotent element in $\operatorname{Lie}(\widetilde{G})$ is of the form $\log g$, where $g \in \widetilde{G}(\mathbb{F}_p)^+ = G^+$. Hence, by Proposition 3.8, there are elements $g_1, \ldots, x_M \in G^+$ such that

$$G^+ = \langle g_1 \rangle \times \cdots \times \langle g_M \rangle.$$

By Theorem C of [18], there is an abelian group $H \subset G$ such that HG^+ is normal and of bounded index in G. Moreover, by the proof of the theorem, there is a lifting of $H \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p)$ to $H \hookrightarrow \mathrm{GL}_n(\mathbb{Z}_p)$. Hence H is a finite abelian subgroup of $\mathrm{GL}_n(\mathbb{Q}_p)$ and hence is a product of at most n cyclic groups. It follows that one can find $h_1, \ldots, h_n \in H$ such that

$$H = \langle h_1 \rangle \times \cdots \times \langle h_n \rangle.$$

Finally, there are elements $z_1, \ldots, z_{\log_2 [G:HG^+]} \in G$ such that

$$G/HG^+ = \langle z_1 HG^+ \rangle \times \cdots \times \langle z_{\log_2 [G:HG^+]} HG^+ \rangle.$$

Putting it together,

$$G = \langle g_1 \rangle \times \cdots \times \langle g_M \rangle \cdot \langle h_1 \rangle \times \cdots \times \langle h_n \rangle \cdot \langle z_1 \rangle \times \cdots \times \langle z_{\log_2 [G:HG^+]} \rangle. \qquad \square$$

3.5. *Extensions of representations.* In general, if S is a group, $V \triangleleft S$ is a normal subgroup, and ρ is a representation of V, then the relative zeta function $\zeta_{S|\rho}(s)$ is different from the representation zeta function of the quotient, $\zeta_{S/V}(s)$. There is, however, one important case in which they are equal.

Definition 3.10. Let S be a group and $V \triangleleft S$ be a normal subgroup. Let ρ be a representation of H. We say that ρ is extendible to S if there is a representation χ of S such that $\operatorname{Res}_V^S \chi = \rho$. The representation χ is called an extension of ρ to S.

Suppose $\rho \in \operatorname{Irr} V$ is extendible to S, and let χ be an extension of ρ to S. Every representation τ of S/V can be thought of as a representation of S by composition with the quotient map $S \to S/V$. We have a map

$$\begin{aligned} \operatorname{Irr}(S/V) &\longrightarrow \operatorname{Irr}(S|\rho), \\ \tau &\mapsto \tau \otimes \chi. \end{aligned} \tag{3.4}$$

Proposition 3.11 ([11, Th. 6.16]). *If $V \triangleleft S$, $\rho \in \operatorname{Irr} V$, and $\chi \in \operatorname{Irr} S$ is an extension of ρ to V, then the map* (3.4) *is a bijection. Therefore $\zeta_{V|\rho}(s) = \zeta_{S/V}(s)$.*

Extensions of representations are tightly connected to the second cohomology group of the quotient. The setting is as follows: We have a group S, a normal subgroup $V \triangleleft S$, and an irreducible representation ρ of V. By Clifford's theory, a necessary condition for the extendability of ρ is that S fixes the representation ρ[3]. Assuming this, we construct an element in the second cohomology group $H^2(S/V, \mathbb{C}^\times)$.

Let M be a V-module that gives rise to the representation ρ. Choose a transversal T to V inside S such that $1 \in T$. For every $t \in T$, the V-modules M and tM are isomorphic. We choose an isomorphism $P_t : M \to tM$, and for $t = 1$ we put $P_1 = \mathrm{Id}$. Every element of S can be written as tv, where $t \in T$ and $v \in V$. We define $P_{tv} : M \to tM$ as $P_{tv}(m) = P_t(v \cdot m)$. It can be easily checked that for any $g_1, g_2 \in S$, the operator

$$P^{-1}_{(g_1 g_2)} \circ P_{g_1} \circ P_{g_2} : M \to M$$

is a morphism of V modules, and hence it is a multiplication by a scalar, which we denote by $\alpha(g_1, g_2)$. Note that the value of $\alpha(g_1, g_2)$ depends only on the cosets g_1V, g_2V. The function α is a 2-cocycle, and we denote its image in the second cohomology of S/V by β. Although the cocycle α depends on the choices of T and P_t, the cohomology class β does not. By [11, Th. 11.7], the representation ρ is extendible to S if and only if β is trivial.

[3] That is, that for every $g \in S$, the representation ρ^g, defined by $v \mapsto \rho(g^{-1}vg)$, is equivalent to ρ.

We will be interested in the case that V is a pro-p group. In this case, we have:

PROPOSITION 3.12. *Let S be a profinite group, let $V \lhd S$ be a normal pro-p subgroup of finite index, and let ρ be an irreducible representation of V. If $\beta \in H^2(S/V, \mathbb{C}^\times)$ is the cohomology class attached to S, V, ρ, then β is a p-element in $H^2(S/V, \mathbb{C}^\times)$.*

Proof. Fix volume forms on the tM's. Let $t_1, t_2 \in T$ and suppose $v \in V$ is such that $t_1 t_2 v \in T$. By taking determinants we get

$$\alpha(t_1, t_2)^{\dim(M)} = \det(P_{t_1}) \det(P_{t_2}) \det(P_{t_1 t_2 v})^{-1} \det \rho(v)^{-1}.$$

We can choose the P_t's for $t \in T$ to have determinant 1. Since ρ is an irreducible representation of a pro-p group, $\dim(M)$ is a power of p and $\det \rho(v)$ is a p^n-root of unity for some n. Therefore $\alpha(t_1, t_2)$ is a p^m-root of unity. It follows that the order of β is a power of p. □

The cohomology groups of finite quasi-simple groups are well known; see, for example, [4, Table 5]. In particular, we have:

PROPOSITION 3.13. *For every $r \in \mathbb{N}$ there is $c(r) \in \mathbb{N}$ such that if Θ is a quasi-simple group of Lie rank r, then the order of the group $H^2(\Theta, \mathbb{C}^\times)$ is less than $c(r)$. The same is true for the first cohomology groups $H^1(\Theta, \mathbb{C}^\times)$.*

We shall use Propositions 3.12 and 3.13 for extensions of p groups by finite quasi-simple groups, where the rank of the finite quasi-simple group is bounded, and p is large. In this case there are no p-elements in the second cohomology group, and therefore the relative zeta function is equal to the representation zeta function of the finite quasi-simple group.

3.6. *Zeta functions of finite reductive groups.* The representation zeta functions of the finite simple groups of Lie type were studied in [16] using the Deligne-Lusztig theory.

Let G be a connected, simply connected, and simple algebraic group defined over $\mathbb{F}_p$. Let $T \subset G$ be a maximal torus defined over $\mathbb{F}_p$. Choose a Borel subgroup $B \subset G$, not necessarily defined over $\mathbb{F}_p$, and let U be the unipotent radical of B.

Let $F : G \to G$ be the Frobenius map. Recall that the Lang map $L : G \to G$ is the map

$$g \mapsto g^{-1} \cdot F(G).$$

The group $G(\mathbb{F}_p) \times T(\mathbb{F}_p)$ acts on the variety $L^{-1}(U)$ by $(g,t)(x) = gxt^{-1}$. Therefore, for each i, the i-th étale cohomology with compact support, $H^i_c(L^{-1}; \mathbb{C})$[4], is a $G(\mathbb{F}_p) \times T(\mathbb{F}_p)$-bimodule.

[4] To be more precise, for every prime $\ell \neq p$, we have the cohomology groups $H^i_c(L^{-1}; \overline{\mathbb{Q}_\ell})$. But $\overline{\mathbb{Q}_\ell}$ is isomorphic to $\mathbb{C}$.

Definition 3.14. The Deligne-Lusztig induction of a character θ of $T(\mathbb{F}_p)$ is the θ-isotypic component in the virtual[5] module

$$\sum(-1)^i H^i_c(L^{-1}(U);\mathbb{C}).$$

This is a virtual representation of $G(\mathbb{F}_p)$; it is independent of the choice of B, and we denote it by $R^G_T\theta$.

Lemma 3.15. *For fixed T and θ, all irreducible components of $R^G_T\theta$ have the same central character.*

Proof. For a variety V and $f \in \operatorname{Aut}(V)$, let

$$\mathcal{L}(g,V)=\sum(-1)^i \operatorname{trace}(f|H^i_c(V;\mathbb{C})).$$

By the definition, the character of $R^G_T\theta$ is

$$\operatorname{trace}(R^G_T\theta(g))=\frac{1}{|T(\mathbb{F}_p)|}\sum_{t\in T(\mathbb{F}_p)}\mathcal{L}((g,t),L^{-1}(U))\cdot\theta(t)^{-1}.$$

If $z\in Z(G(\mathbb{F}_p))$ and $t\in T(\mathbb{F}_p)$, then the order of (z,t) as an automorphism of $L^{-1}(U)$ is prime to p. Therefore, by [5, Prop. 10.14], $\mathcal{L}((z,t),L^{-1}(U)) = \mathcal{L}((1,1),(L^{-1}(U))^{(z,t)})$. If $z\neq t$, then $L^{-1}(U)^{(z,t)}=\emptyset$ and $\mathcal{L}((z,t),L^{-1}(U))=0$. If $z=t$, then $L^{-1}(U)^{(z,t)}=L^{-1}(U)$. Therefore, we get

$$\operatorname{trace}(R^G_T\theta(z))=\frac{1}{|T(\mathbb{F}_p)|}\mathcal{L}((1,1),L^{-1}(U))\cdot\theta(z)^{-1}.$$

Since

$$\operatorname{trace}(R^G_T\theta(1))=\frac{1}{|T(\mathbb{F}_p)|}\mathcal{L}((1,1),L^{-1}(U)),$$

the lemma follows. □

The following is a slight generalization of [16, Th. 1.7], which we will need in the following:

Lemma 3.16. *Let G be a simple group scheme. There is a natural number N such that for every $0\le a<N$, we have:*

1. *The isomorphism type of the center of $G(\mathbb{F}_p)$ is the same, for almost all primes congruent to a modulo N. Denote this group by A_a.*
2. *For every $\omega\in A_a^\vee$, there are polynomials $P_1,\dots,P_N,Q_1,\dots,Q_N$ such that for almost all primes p that are congruent to a modulo N, we have*

$$\zeta_{G(\mathbb{F}_p)|\omega}(s)=\sum P_i(p)\cdot(Q_i(p))^{-s}.$$

[5] Virtual means that we are taking formal linear combinations of representations. The result lives in the K group of the category of representations.

Proof. (1) is well known. Let G^* be the dual algebraic group to G, as defined in [5, Def. 13.10]. The representations of $G(\mathbb{F}_p)$ are partitioned into Lusztig cells, $\mathcal{E}(G(\mathbb{F}_p),(s))$, indexed by semi-simple conjugacy classes $(s) \subset G^*(\mathbb{F}_p)$. Each cell consists of the irreducible components of the representation $R_T^G\theta$, where the pair (T,θ), consisting of a maximal torus $T \subset G$ defined over $\mathbb{F}_p$ and a character θ of T, is attached to the conjugacy class (s) by [5, Prop. 13.13]. By [5, Th. 13.23 and Rem. 13.24], for every s, there is a bijection ψ_s between $\mathcal{E}(G(\mathbb{F}_p),(s))$ and $\mathcal{E}(C_{G*(\mathbb{F}_p)}(s),1)$ such that

$$\dim\rho = \frac{|G(\mathbb{F}_p)|_{p'}}{|C_{G*}(s)(\mathbb{F}_p)|_{p'}}\dim\psi_s(\rho),$$

where $|X|_{p'}$ denotes the largest integer prime to p that divides $|X|$.

If $s \in G^*(\mathbb{F}_p)$ is semi-simple, then $C_{G^*}(s)$ is a reductive subgroup of G^* of maximal rank and $C_{G^*(\mathbb{F}_p)}(s) = C_{G^*}(s)(\mathbb{F}_p)$. There are finitely many subgroup schemes $C_1,\dots,C_K \subset G^*$ such that for any prime p and every semi-simple $s \in G^*(\mathbb{F}_p)$, $C_{G^*}(s)$ is conjugate to one of the C_i's. Moreover, for every i there is a polynomial $F_i^1(x) \in \mathbb{Q}[x]$ such that for every p, we have

$$F_i^1(p) = \frac{|G(\mathbb{F}_p)|_{p'}}{|C_i(\mathbb{F}_p)|_{p'}}.$$

By looking at the table of unipotent characters, we see that there are polynomials $F_{i,j}^2(x) \in \mathbb{Q}[x]$, such that for every p, the degrees of the unipotent representations of $C_i(\mathbb{F}_p)$ are $F_{i,1}^2(p),\dots,F_{i,M}^2(p)$.

Finally, by a similar argument to [16, Lemma 4.3], the number of conjugacy classes $(s) \subset G^*(\mathbb{F}_p)$ such that

(1) $C_{G^*}(s)$ is conjugate to $C_i(\mathbb{F}_p)$;

(2) $\theta|_A = \omega$, where (T,θ) is the pair associated to (s);

is of the form $F_{i,\omega,p}^3(p)$, where $F_{i,\omega,p}^3(x) \in \mathbb{Q}[x]$ depends only on i,ω, and the residue class of p modulo some fixed integer N. We get that

$$\zeta_{G(\mathbb{F}_p)|\omega}(s) = \sum_{i=1}^{K} F_{i,\omega,p}^3(p)\cdot F_i^1(p)\cdot\sum_{j=1}^{M} F_{i,j}^2(p)^{-s}. \qquad \square$$

Proposition 3.17. *Let G be a semisimple algebraic group scheme over $\mathbb{Z}_S$. There is a natural number N, and for each $0 \le a < N$, there are two sequences of polynomials*

$$P_1(x),\dots,P_{k_a},Q_1(x),\dots,Q_{k_a}(x) \in \mathbb{Q}[x]$$

such that for every prime p, which is congruent to a modulo N and not in S, we have

$$\zeta_{G(\mathbb{F}_p)}(s) = \sum_{i=1}^{k_a} P_i(p)\cdot Q_i(p)^{-s}.$$

Proof. Let G be a semisimple algebraic group scheme over S. There are simple algebraic group schemes $G_1, \ldots, G_n$ such that for every p, we have a central extension

$$1 \to Z_p \to \prod G_i(\mathbb{F}_p) \to G(\mathbb{F}_p) \to 1.$$

Moreover, the isomorphism classes of Z_p and of the centers of $G_i(\mathbb{F}_p)$ are constant if we fix the residue class of p modulo some N. Fix such a residue class and let Ω be the collection of tuples $(\omega_1, \ldots, \omega_n)$ such that

(1) ω_i is a character of the center of $G_i(\mathbb{F}_p)$;
(2) $\omega_1 \times \cdots \times \omega_n$ is trivial on Z_p.

We have that

$$\zeta_{G(\mathbb{F}_p)}(s) = \sum_{(\omega_1,\ldots,\omega_n)\in\Omega} \zeta_{G_1(\mathbb{F}_p)|\omega_1}(s) \cdot \cdots \cdot \zeta_{G_n(\mathbb{F}_p)|\omega_n}(s).$$

By Lemma 3.16, the proposition is proved. □

3.7. *Equivalence of Euler products.*

Definition 3.18. Let $(\zeta_n(s))_n$ and $(\xi_n(s))_n$ be two sequences of Dirichlet series with nonnegative coefficients. We say that the sequences $(\zeta_n(s))_n$ and $(\xi_n(s))_n$ are *equivalent*, and we write $(\zeta_n(s))_n \sim (\xi_n(s))_n$, if there is a constant $C > 0$ such that for every n and every s, which is greater than the abscissae of convergence of all $\xi_n(s), \zeta_n(s)$,

$$C^{-1-s}\xi_n(s) \leq \zeta_n(s) \leq C^{1+s}\xi_n(s).$$

Lemma 3.19. *Suppose $(\zeta_n(s))_n$ and $(\xi_n(s))_n$ are two sequences of Dirichlet series with nonnegative coefficients and constant terms equal to zero, and suppose that $(\zeta_n(s))_n \sim (\xi_n(s))_n$. Then the abscissae of convergence of the products*

$$\prod_n (1 + \zeta_n(s)) \quad \textit{and} \quad \prod_n (1 + \xi_n(s))$$

are equal.

Proof. Suppose s is greater than the abscissa of convergence of $\prod_n(1 + \zeta_n(s))$. Then for every n, s is greater than the abscissa of convergence of ζ_n, and the sum $\sum_n \zeta_n(s)$ converges. By the assumption, s is greater than the abscissa of convergence of ξ_n for every n, and the sum $\sum \xi_n(s)$ converges. Therefore, s is greater than the abscissa of convergence of $\prod(1 + \xi_n(s))$. By symmetry, the abscissae of convergence of $\prod(1 + \zeta_n(s))$ and $\prod(1 + \xi_n(s))$ are equal. □

3.8. *Resolution of singularities.* In this section we remind the the reader of the notions of resolution of singularities and reduction modulo p of a scheme defined over the rationals.

We start with the notion of (embedded) resolution of singularities. We shall work over the field $\mathbb{Q}$ of rational numbers. Given a polynomial $P(x) \in \mathbb{Q}[x_1, \dots, x_n]$, an embedded resolution of $P(x)$ is a pair $(Y_{\mathbb{Q}}, h)$, where $Y_{\mathbb{Q}}$ is a smooth subvariety of $\mathbb{P}^k_{\mathbb{A}^n_{\mathbb{Q}}}$ and h is the restriction of the natural projection $\mathbb{P}^k_{\mathbb{A}^n_{\mathbb{Q}}} \to \mathbb{A}^n_{\mathbb{Q}}$ to $Y_{\mathbb{Q}}$, such that if we denote by D the subscheme defined by $P(x)$, then

(1) the restriction of h to $Y_{\mathbb{Q}} \setminus h^{-1}(D)$ is an isomorphism onto $\mathbb{A}^n_{\mathbb{Q}} \setminus D$;
(2) $h^{-1}(D)$ is a divisor with normal crossings.

By a well-known theorem of Hironaka, every polynomial (over a field of characteristics 0) has a resolution of singularities.

The second notion we wish to remind the reader of is that of reduction mod p of a variety. Let $Y_{\mathbb{Q}} \subset \mathbb{P}^k_{\mathbb{A}^n_{\mathbb{Q}}}$ be a variety. Consider $\mathbb{P}^k_{\mathbb{A}^n_{\mathbb{Q}}}$ as an open subset of $\mathbb{P}^k_{\mathbb{A}^n_{\mathbb{Z}}}$. Define $Y_{\mathbb{Z}}$ to be the scheme theoretic closure of $Y_{\mathbb{Q}}$ inside $\mathbb{P}^k_{\mathbb{A}^n_{\mathbb{Z}}}$. The reduction mod p of $Y_{\mathbb{Q}}$ is the fiber product $Y_{\mathbb{Z}} \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(\mathbb{F}_p)$.[6]

Definition 3.20. Let $P(x) \in \mathbb{Q}[x_1, \dots, x_n]$ be a polynomial. Let $(Y_{\mathbb{Q}}, h)$ be a resolution of singularities of $P(x)$. We denote the irreducible components of $(h^{-1}(D))_{\mathrm{red}}$ as $E_1, \dots, E_m$. We say that (Y, h) has good reduction modulo p if the following conditions hold.

(1) $Y_{\mathbb{F}_q}$ is smooth;
(2) $\overline{E_i}$ are smooth, and $\cup \overline{E_i}$ has normal crossings;
(3) $\overline{E_i}$ and $\overline{E_j}$ do not have a common irreducible component if $i \neq j$.

It is easy to see that if $(Y_{\mathbb{Q}}, h)$ is a resolution of singularities, then this resolution has a good reduction modulo almost all primes.

4. **Definable families**

4.1. *Definable sets in $\mathcal{T}_f$.* We shall work with several different logical theories (and languages). Recall that the language of rings, $\mathcal{L}_{\mathrm{Rings}}$, is the first order language which has constant symbols 0,1, has only equality as a relation, and has two function symbols: addition and multiplication. We let the theory

[6] A more elementary description, which is true for almost all primes is the following: Suppose $Y_{\mathbb{Q}}$ is defined by the polynomial equations $Q_1(x) = \cdots = Q_m(x) = 0$, where $Q_i(x)$ are polynomials with rational coefficients. For almost all primes p, the denominators of the coefficients of $Q_i(x)$ are not divisible by p and so we can consider the reduction $\overline{Q_i}(x)$ of $Q_i(x)$ mod p. Then $Y_{\mathbb{F}_p}$ is the variety defined by the equations $\overline{Q_1}(x) = \cdots = \overline{Q_m}(x) = 0$.

$\mathcal{T}_f$ (the theory of fields) be the collection of all sentences in $\mathcal{L}_{\text{Rings}}$ that hold for all fields.

It will also be useful to work over different bases. If R is an integral domain, we denote by $\mathcal{L}_{\text{Rings}}(R)$ the language $\mathcal{L}_{\text{Rings}}$ together with constant symbols for the elements of R. The theory $\mathcal{T}_f(R)$ consists of all sentences of $\mathcal{L}_{\text{Rings}}(R)$ that hold for all fields containing R. In particular, it contains all relations that hold between the elements of R.

By a *$\mathcal{T}_f$-definable set* we shall mean a formula $\phi(x)$ in the language $\mathcal{L}_{\text{Rings}}$ (here and in the following we shall use x to denote a tuple of variables of unspecified length). Let X be a definable set that corresponds to the formula $\phi(x)$. Given a model L of $\mathcal{T}_f$ (i.e., a field) we define the set of L-solutions of X as

$$X(L) = \phi(L) := \{a \in L^n \mid \phi(a)\}.$$

Examples of definable sets are the affine space $\mathbb{A}^n$ defined by the formula $\phi(x_1, \ldots, x_n) :=$ '$0 = 0$' and the general linear group GL_n defined by the formula $\phi(x_{i,j}) :=$ '$\det(x_{i,j}) \neq 0$'. More generally, suppose that $\underline{X} \subset \mathbb{A}^n_{\mathbb{Z}_S}$ is a scheme over $\operatorname{Spec} \mathbb{Z}_S$ given by the equations $f_1(x) = \cdots = f_m(x) = 0$, where $f_i(x) \in \mathbb{Z}_S[x]$. The same equations give us an $\mathcal{L}_{\text{Rings}}(\mathbb{Z}_S)$-definable set, which we shall denote by X.

Suppose that U and V are $\mathcal{T}_f$-definable sets given by formulas $\phi(x)$ and $\psi(x)$ respectively, in the same variables. We say that U and V are equal if $\mathcal{T}_f$ contains the sentence $(\forall x)(\phi(x) \leftrightarrow \psi(x))$. It is possible for two nonequal $\mathcal{T}_f$-definable sets to have the same set of points in some model. However, if two definable sets have the same set of points in every model, then they are equal by the compactness theorem. Similarly, we say that U is contained in V if $\mathcal{T}_f$ contains the sentence $(\forall x)(\phi(x) \to \psi(x))$. The definable sets $V \cap U, V \cup U, V \times U$ are associated with the formulas $\phi(x) \wedge \psi(x), \phi(x) \vee \psi(x)$ and $\phi(x) \wedge \psi(y)$ respectively, where y is a tuple of variables disjoint from x. For the cartesian product, we can omit the requirement that ϕ and ψ have the same number of variables.

A $\mathcal{T}_f$-definable function between the $\mathcal{T}_f$-definable sets U and V is a $\mathcal{T}_f$-definable set W that is contained in $U \times V$, such that $\mathcal{T}_f$ implies that W is a graph of a function (note that this can be expressed in $\mathcal{L}_{\text{Rings}}$). A $\mathcal{T}_f$-definable (linear) group is a $\mathcal{T}_f$-definable subset G of GL_n such that $\mathcal{T}_f$ implies the axioms of a group for G.

Given a $\mathcal{T}_f$-definable set X, the Zariski closure of X is defined in the following way. We look at the ideal of all polynomials $p(x)$ such that $\mathcal{T}_f$ contains the sentence $(\forall x)(\phi(x) \to (p(x) = 0))$. This ideal is generated by a finite number of polynomials, say by $p_i(x)$. The Zariski closure of X is the $\mathcal{T}_f$-definable set given by the formula $p_1(x) = 0 \wedge \cdots \wedge p_N(x) = 0$.

Given a domain R, the notions of $\mathcal{T}_f(R)$-definable sets, functions, and groups are defined similarly. Every $\mathcal{T}_f$-definable set is a $\mathcal{T}_f(R)$-definable set, but note that two nonequal $\mathcal{T}_f$-definable sets can become equal as $\mathcal{T}_f(R)$-definable sets. For example, the formula $\phi(x) :=$ '$1+1=0$' defines a nonempty $\mathcal{T}_f$-definable set (since it has points over $\mathbb{F}_2$) but it becomes empty in $\mathcal{T}_f(\mathbb{F}_3)$.

We stress again that definable sets are not sets, but rather formulas. The expression "$x \in V$" is a synonym for the formula $\phi(x)$ whereas "$a \in V(L)$" means that L is a model for our theory, that a is a tuple of elements of L, and that $\phi(a)$ holds.

Of course, relative notions are very useful. We will only work over a base which is an affine space, but the definitions can be given for general base variety.

Definition 4.1. (1) A $\mathcal{T}_f$-definable family over $\mathbb{A}^n$ is a $\mathcal{T}_f$-definable subset of $\mathbb{A}^n \times \mathbb{A}^m$ for some m.

(2) A morphism between two definable families A, B over $\mathbb{A}^n$ is a definable map $\phi : A \to B$ such that the diagram

$$\begin{tikzcd} A \arrow[rr, "\phi"] \arrow[dr] & & B \arrow[dl] \\ & \mathbb{A}^n & \end{tikzcd}$$

is commutative.

(3) Suppose $A \subset \mathbb{A}^n \times \mathbb{A}^m$ is a $\mathcal{T}_f$-definable family defined by the formula $\phi(x, y)$. Given a model L and $a \in \mathbb{A}^n(L)$, let $K(a) \subset L$ be the subring generated by the coordinates of a. We define the fiber A_a as the $\mathcal{T}_f(K(a))$-definable set defined by the formula $\phi(a, y)$.

The fiber product of two definable families over $\mathbb{A}^n$ is again a definable family over $\mathbb{A}^n$. We denote it by $\times_{\mathbb{A}^n}$.

Definition 4.2. (1) A $\mathcal{T}_f$-definable family of groups over $\mathbb{A}^n$ is a $\mathcal{T}_f$-definable subset G of $\mathbb{A}^n \times \mathrm{GL}_m$ such that $\mathcal{T}_f$ implies that every fiber is a group.

(2) Given a $\mathcal{T}_f$-definable family of groups G and a $\mathcal{T}_f$-definable family Ω over the same base, a definable family of actions is a morphism $G \times_{\mathbb{A}^n} \Omega \to \Omega$ such that for every model L and $a \in \mathbb{A}^n(L)$, the definable map of the fibers is an action.

4.2. *Pseudo-finite fields.* Another theory we shall work with is the asymptotic theory of finite fields, which is also known as the theory of pseudofinite fields of characteristics zero. The language for this theory is again $\mathcal{L}_{\text{Rings}}$. The theory of pseudofinite fields, $\mathcal{T}_{pf}$, consists of all sentences of $\mathcal{L}_{\text{Rings}}$ that hold for all finite fields, except for the fields of characteristics smaller than N for some N. For example, the sentence "There exists a unique field extension of degree 2, up to isomorphism" can be expressed in the language of fields. Since it is true for all finite fields, it belongs to $\mathcal{T}_{pf}$.

Remark 4.3. The use of pseudo-finite fields is for notational simplicity only. If the reader wishes, she can replace all absolute statements of the form "(the first order sentence) X holds in the theory of pseudo-finite fields" by the statement "If p is large enough, then X holds".

Every finite subset of sentences in $\mathcal{T}_{pf}$ has a model, so by the compactness theorem $\mathcal{T}_{pf}$ has a model. Note that if L is a model of $\mathcal{T}_{pf}$, then the characteristics of L is zero (since for every N, the theory $\mathcal{T}_{pf}$ contains the sentences "The characteristics is different from N").

The notions of $\mathcal{T}_{pf}$-definable sets, functions etc. are defined similarly. Every $\mathcal{T}_f$-definable set is a $\mathcal{T}_{pf}$-definable set. Note, however, that there might be more functions between two definable sets (since the requirement that a set is a graph of a function is stronger in $\mathcal{T}_f$ than in $\mathcal{T}_{pf}$).

We denote by $\mathbb{N}$ the set of nonnegative integers. The following theorem is a strengthening of the Lang-Weil estimates (see, for example, [2, Th. 7.1] and the references therein).

THEOREM 4.4. *Let $\phi(x,y)$ be a formula in $\mathcal{L}_{\text{Rings}}$. Then there exists a finite set $D \subset \mathbb{N} \times \mathbb{Q}_{>0} \cup \{(0,0)\}$, formulas $\phi_{(d,\mu)}(y)$ for $(d,\mu) \in D$, and a constant c, such that the following hold.*

(1) *The sentence $(\forall y) \bigvee_D \phi_{(d,\mu)}(y)$ holds in the theory of pseudofinite fields.*
(2) *If p is a prime number, $a \in \mathbb{F}_p^n$, and $\phi_{(d,\mu)}(a)$ holds, then*

$$\Big| |\{x \in \mathbb{F}_p^m | \phi(x,a)\}| - \mu p^d \Big| < cp^{d-\frac{1}{2}}.$$

If the Zariski closure of $\phi(x,a)$ is an irreducible variety and has dimension e, then $\phi_{(e,\mu)}(a)$ holds for some μ.

Note that since $(\forall y) \bigvee_D \phi_{(d,\mu)}(y)$ holds in $\mathcal{T}_{pf}$, then if p is large enough, then for every $a \in \mathbb{F}_p^n$ there is a $(d,\mu) \in D$ such that $\phi_{(d,\mu)}(a)$ holds.

Definition 4.5. A theory $\mathcal{T}$ is called complete if for any sentence ϕ, either $\phi \in \mathcal{T}$ or $\sim \phi \in \mathcal{T}$. A completion of a theory is a complete theory that contains it.

By [2, Th. 6.14], the completions of $\mathcal{T}_{pf}$ are given by specifying which integer polynomials are irreducible over the field (and taking all logical implications). This shows that the set of primes for which a single sentence holds is regular in some way.

Definition 4.6. Let $\mathcal{P}$ be the set of prime numbers. Given an integer polynomial $f(x) \in \mathbb{Z}[x]$, let $\mathcal{P}^f$ be the set of primes p such that $f(x)$ is irreducible modulo p. A set in the Boolean algebra generated by $\mathcal{P}^f$ and the Boolean algebra of finite and co-finite sets in $\mathcal{P}$ is called an Artin set. By the density theorem of Chebotarev, every Artin set is either finite or has a positive analytic density.

We claim that if ϕ is a sentence in the language of fields, then the set of primes p for which ϕ holds in $\mathbb{F}_p$ is an Artin set. For suppose it is not. Enumerate the set of integer polynomials $f_1, f_2, \dots$ and for each i let I_i be the sentence "f_i is irreducible". By our assumption, for every n, there are $J_1^n, \dots, J_n^n$ such that every J_i^n is either equal to I_i or to $\sim I_i$ and such that both

$$\mathcal{T}_{pf} \cup \{J_1^n \wedge \dots \wedge J_n^n \wedge \phi\} \quad \text{and} \quad \mathcal{T}_{pf} \cup \{J_1^n \wedge \dots \wedge J_n^n \wedge \sim \phi\}$$

are satisfiable. A diagonalization argument shows that there is a choice J_1, $J_2, \dots$, where each J_n is equal to either I_n or $\sim I_n$, such that both $\mathcal{T}_{pf} \cup \{J_n\}_n \cup \{\phi\}$ and $\mathcal{T}_{pf} \cup \{J_n\}_n \cup \{\sim \phi\}$ are both satisfiable. But this is a contradiction, since $\mathcal{T}_{pf} \cup \{J_n\}_n$ is complete.

Corollary 4.7. *Let $\phi(x, y)$ be a formula in $\mathcal{L}_{\mathrm{Rings}}$. Then there are*:

(1) *a constant c*;

(2) *a partition of the set of primes into finitely many Artin sets $\mathcal{P}_1, \dots, \mathcal{P}_l$*;

(3) *for each $1 \le i \le l$, a finite set $D_i \subset \mathbb{N} \times \mathbb{Q}_{>0} \cup \{(0,0)\}$*;

(4) *for each $1 \le i \le l$, two functions, $e_i : D_i \to \mathbb{N}$ and $\nu_i : D_i \to \mathbb{Q}_{>0}$*;

such that for every $p \in \mathcal{P}_i$ and every $a \in \mathbb{F}_p^n$, there is a $(d, \mu) \in D_i$ such that

$$\Big| |\{x \in \mathbb{F}_q^m | \phi(x, a)\}| - \mu p^d \Big| < c p^{d - \frac{1}{2}}.$$

If we denote by $N_{(d,\mu)}$ the number of the tuples $a \in \mathbb{F}_p^n$ for which the inequality above holds, then

$$\Big| N_{(d,\mu)} - \nu_i(d, \mu) p^{e_i(d,\mu)} \Big| < c p^{e(d,\mu) - \frac{1}{2}}.$$

Proof. Let c, D, and $\phi_{(d,\mu)}$ be as in Theorem 4.4. For each $(d, \mu) \in D$ apply Theorem 4.4 to the formula $\phi_{(d,\mu)}(y)$. In this degenerate case, the theorem says that there are sentences $\phi_{(d,\mu,e,\nu)}$ such that if $\phi_{(d,\mu,e,\nu)}$ holds, then the number of points in $\phi_{(d,\mu)}(\mathbb{F}_p)$ is $\nu p^e \pm C \cdot p^{e - \frac{1}{2}}$. Let Σ be the set of primes p for which one of the sentences

$$\bigvee \phi_{d,\mu,e,\nu} \qquad (\forall y) \bigvee \phi_{(d,\mu)}(y)$$

does not hold. Since these sentences hold in $\mathcal{T}_{pf}$, we get that Σ is finite. By the above, there is a partition of the primes into Artin sets $\mathcal{P}_i$ such that for each i and (d, μ, e, ν), the sentence $\phi_{(d,\mu,e,\nu)}$ holds for all $\{\mathbb{F}_p \mid p \in \mathcal{P}_i\}$ or for none. By further partitioning of the $\mathcal{P}_i$, we can assume that for each i

either $\mathcal{P}_i$ is infinite and $\mathcal{P}_i \cap \Sigma = \emptyset$, or $\mathcal{P}_i$ is a singleton. For each i such that $\mathcal{P}_i \cap \Sigma = \emptyset$, set $D_i = \{(\mu, d) \mid (\exists y)\phi_{(d,\mu)}(y)$ and let $(e(d,\mu), \nu(d,\mu))$ be the unique (e,ν) such that $\phi_{(d,\mu,e,\nu)}$ holds for all the primes in $\mathcal{P}_i$. For $\mathcal{P}_i$ a singleton, set $D_i = \{(0,1)\}, e(0,1) = \nu(0,1) = 1$. It is clear that if c is large, then the proposition holds. □

4.3. *Definable families of groups.*

Proposition 4.8. *Let $L \subset \mathbb{A}^n \times \mathrm{M}_n$ be a $\mathcal{T}_f$-definable family of Lie algebras. Then there is a definable family $R \subset L$ such that for every model F of $\mathcal{T}_f$ of high enough characteristics, and for every $x \in \mathbb{A}^n(F)$, the fiber R_x is the nilpotent radical of the Lie algebra L_x.*

Proof. By the Jacobson-Morozov theorem, if F has characteristic 0 and $\mathscr{L} \subset \mathrm{M}_n(F)$ is a Lie algebra, then an element $x \in \mathscr{L}$ is in the unipotent radical of $\mathscr{L}$ if and only if for every $y \in \mathscr{L}$, the element $[x,y]$ is nilpotent. By compactness, the same follows for if F is a field of high enough characteristics (n is fixed here). □

For a root datum Φ, denote H_Φ as the adjoint algebraic group attached to Φ.

Lemma 4.9. *Let $G \subset \mathbb{A}^m \times \mathrm{GL}_n$ be a $\mathcal{T}_{pf}$-definable family of semisimple adjoint groups. Then there is a definable partition $\mathbb{A}^m = X_1 \sqcup \cdots \sqcup X_k$, and for every i there are root data $\Phi_{i,1}, \ldots, \Phi_{i,j}$, such that for p large enough, and for $x \in X_i(\mathbb{F}_p)$, the group $G_x(\mathbb{F}_p)$ is isomorphic to $H_{\Phi_{i,1}}(\mathbb{F}_p) \times \cdots \times H_{\Phi_{i,j}}(\mathbb{F}_p)$.*

Proof. We first assume that G is a family of simple adjoint groups. In this case we need to show that for every root datum Φ, the set of $x \in \mathbb{A}^m$ such that G_x is isomorphic to H_Φ, is a definable set. *A priori*, this condition is not definable, as the isomorphism can be a polynomial map of very high degree.

Let $\mathscr{L}_\Phi$ be the Lie algebra attached to Φ. Define a family of Lie algebras $L \subset \mathbb{A}^m \times \mathrm{gl}_n$ as follows: For $x \in \mathbb{A}^m$, let $U_x \subset G_x$ be the set of unipotent elements. Define L_x to be the span of $\log U_x$.

It is known that $G_x(\mathbb{F}_p)$ is isomorphic to $\underline{H}_\Phi(\mathbb{F}_p)$ if and only if $L_x(\mathbb{F}_p)$ is isomorphic to $\mathscr{L}_\Phi$. This, however, is a definable condition, since every morphism between Lie algebras is linear.

The argument for products of simple groups is similar. □

Remark 4.10. This proof actually shows that every map between connected semisimple algebraic groups $G \subset \mathrm{GL}_n$ and $H \subset \mathrm{GL_m}$ can be represented by a polynomial whose degree is bounded as a function of m and n.

Proposition 4.11. *Let X be a definable set in $\mathcal{T}_{pf}$, and let $S \subset X \times \mathrm{GL}_n$ be a family of definable groups in $\mathcal{T}_{pf}$. Then there are:*

(1) *a definable partition* $X = X_1 \sqcup \cdots \sqcup X_m$;
(2) *for each* i, *a finite sequence of root data* $\Phi^i_1, \ldots, \Phi^i_{n_i}$;
(3) *definable families* $U \subset C \subset S$ *of normal subgroups*;
(4) *a constant* c;

such that for every p *large enough*, *for any* i, *and for any* $a \in X_i(\mathbb{F}_p)$, *the following hold.*

(1) $U_a(\mathbb{F}_p)$ *is a unipotent group. Moreover*, $U_a(\mathbb{F}_p)$ *is the maximal normal* p*-subgroup of* $S_a(\mathbb{F}_p)$.
(2) $C_a(\mathbb{F}_p)/U_a(\mathbb{F}_p)$ *is isomorphic to* $H_{\Phi^i_1}(\mathbb{F}_p) \times \cdots \times H_{\Phi^i_{n_i}}(\mathbb{F}_p)$.
(3) *The group* $S_a(\mathbb{F}_p)/C_x(\mathbb{F}_p)$ *is an extension of an abelian group*, *whose order is prime to* p, *by a group of size less than* c.

Proof. Let $P \subset X \times \mathrm{GL}_n$ be the definable family

$$P = \{(x, g) \in S \mid (g-1)^n = 0\}.$$

Since on unipotent elements, the function log is a polynomial, the family

$$L = \{(x, A) \in X \times \mathfrak{gl}_n \mid A \text{ is in the span of } \log P_x\}$$

is a definable family. It is easy to see (see [18, Lemma 1.6]) that if p is large enough, then for every $x \in X(\mathbb{F}_p)$, the set $L_x(\mathbb{F}_p)$ is a Lie algebra. By Proposition 3.8, there is a family $C \subset X \times \mathrm{GL}_n$ such that for every p large enough, and every $x \in X(\mathbb{F}_p)$, the set $C_x(\mathbb{F}_p)$ is equal to the group generated by the set $\exp L_x(\mathbb{F}_p)$. By [18, Th. B], we have that $C_x(\mathbb{F}_p) \subset S_x(\mathbb{F}_p)$ for all p large enough, and hence $C \subset S$. Clearly, C is a family of normal subgroups of S. By [18, Th. C], for every p large enough and every $x \in X(\mathbb{F}_p)$, there is a commutative subgroup $H \subset S_x(\mathbb{F}_p)$ such that $HC_x(\mathbb{F}_p)$ is normal in $S_x(\mathbb{F}_p)$ and its index is less than a constant, which we denote by c. Moreover, by the same theorem, the order of H is prime to p. Claim (3) follows from this.

By Proposition 4.8, there is a definable family of Lie subalgebras $L^u \subset L$ such that for every $x \in X$, the Lie subalgebra L^u_x is the unipotent radical of L_x. By Proposition 3.8, there is a definable family $U \subset C$ such that for every p large enough and every $x \in X(K)$, the set $U_x(\mathbb{F}_p)$ is the subgroup generated by the set $\exp L^u_x(\mathbb{F}_p)$. Clearly, $U_x(\mathbb{F}_p)$ is a unipotent normal p-subgroup of $C_x(\mathbb{F}_p)$. Since $U_x(\mathbb{F}_p)$ is characteristic in $C_x(\mathbb{F}_p)$ and since, if p is large enough, the order of $S_x(\mathbb{F}_p)/C_x(\mathbb{F}_p)$ is not divisible by p, we get that $U_x(\mathbb{F}_p)$ is a normal p-subgroup of $S_x(\mathbb{F}_p)$. This finishes the proof of claim (1), except for the maximality.

For every p large enough and for every $x \in X(\mathbb{F}_p)$, the Lie algebra $L_x(\mathbb{F}_p)/L^u_x(\mathbb{F}_p)$ is reductive. Since it is generated by nilpotents, it is, in fact, semisimple. Theorem B of [18] shows that $C_x(\mathbb{F}_p)/U_x(\mathbb{F}_p)$ is equal to $H(\mathbb{F}_p)^+ = [H(\mathbb{F}_p), H(\mathbb{F}_p)]$, where H is a semisimple algebraic group with Lie algebra $L_x(\mathbb{F}_p)/L^u_x(\mathbb{F}_p)$. By Lemma 4.9 we get a definable partition $X = X_i \sqcup \cdots \sqcup X_m$

and root data Φ^i_j such that for every p large enough and every $x \in X_i(\mathbb{F}_p)$, the group $C_x(\mathbb{F}_p)/U_x(\mathbb{F}_p)$ is isomorphic to

$$H_{\Phi^i_1}(\mathbb{F}_p) \times \cdots \times H_{\Phi^i_{n_i}}(\mathbb{F}_p).$$

Claim (2) follows. Also, it follows that $C_x(\mathbb{F}_p)/U_x(\mathbb{F}_p)$ does not have any normal p groups, and hence the maximality claim in (1) follows. □

4.4. *Henselian valued fields.* We will also work in the theory of valued Henselian fields. The language for this theory is the language $\mathcal{L}_{Vf}$ of valued fields, which we proceed to define. In $\mathcal{L}_{Vf}$ one can quantify over three kinds of variables (which are called sorts): one is the valued fields sort, one is the residue field sort, and one is the value group sort. The language has constants $0, 1$ (which are valued field sort), $\bar{0}, \bar{1}$ (which are residue field sort), and $\tilde{0}$ (which is value group sort). The relations are equality and $\tilde{<}$, but we can only equate expressions of the same sort (so $0 = \bar{0}$ is not a legitimate expression), and only $\tilde{<}$-compare expressions which are in the value group sort. The functions symbols are two sets of addition and multiplication (for the value field and residue field sorts), addition (for the value group sort), and two additional function symbols: a function val (called valuation) from the valued field sort to the value group and a function ac (called angular component) from the value field sort to the residue field sort. Here again, there are definable sets, functions etc. An example of a definable set is $\mathcal{O}$, which is defined by the formula $\phi(x) :=$ '$\operatorname{val}(x) \geq 0$', where x is a variable of valued field sort. Since in $\mathcal{L}_{Vf}$ there is more than one sort, there might be confusion regarding the variables of the definable sets. We resolve this confusion by adding the subscripts V, R, O for valued field, residue field, and value group respectively. So, for example, $\mathbb{A}^n_V$ is the affine space whose coordinates are valued field sort and $(\mathrm{GL}_n)_R$ is the set of invertible $n \times n$ matrices whose entries are from the residue field.

The theory $\mathcal{T}_{Hvf}$ of Henselian valued fields, whose valuation group is elementary equivalent to $\mathbb{Z}$, consists of the following axioms:

- the axioms of fields for the valued field sort and for the residue field sort;
- the axioms of non-archimedian valuation;
- all sentences that hold for $\mathbb{Z}$ for the value group sort;
- the sentences $(\forall x, y \neq 0)\,\operatorname{ac}(xy) = \operatorname{ac}(x) \cdot \operatorname{ac}(y)$, $(\forall x, y \neq 0)(\operatorname{val}(x) < \operatorname{val}(y) \to \operatorname{ac}(x + y) = \operatorname{ac}(x)$, and $(\forall x, y \neq 0)(\operatorname{val}(x) = \operatorname{val}(y) \wedge \operatorname{ac}(x) \neq -\operatorname{ac}(y)) \to \operatorname{ac}(x + y) = \operatorname{ac}(x) + \operatorname{ac}(y)$;
- sentences stating that the field is Henselian.

We shall be mainly interested in the models $\mathbb{M}_p$ of $\mathcal{T}_{Hvf}$, which interpret $\mathbb{A}_V$ as $\mathbb{Q}_p$, interpret $\mathbb{A}_R$ as $\mathbb{F}_p$, interpret $\mathbb{A}_O$ as $\mathbb{Z}$, interpret $\operatorname{val}(x)$ as the p-adic valuation of x, and interpret $\mathrm{ac}(x)$ as the first nonzero coefficient in the p-adic expansion of x.

Let $\mathcal{T}_{Hvf,0}$ be the theory $\mathcal{T}_{Hvf}$ together with the axioms that claim that the characteristic of the residue field is equal to zero. While no $\mathbb{M}_p$ is a model for $\mathcal{T}_{Hvf,0}$, it follows from the compactness theorem that every sentence that holds in $\mathcal{T}_{Hvf,0}$ is also true in all but finitely many of the $\mathbb{M}_p$'s.

Theorem 4.12 (Elimination of quantifiers in Henselian fields; see [19, Th. 4.1]). *Let $\phi(x,y,z)$ be a formula in the language $\mathcal{L}_{Vf}$ where the variable x is of the valued field sort, the variable y is of residue field sort, and the variable z is of value group sort. Then there is a partition of $\mathbb{A}^n_F$ into finitely many constructible sets C_j; and for each j there are polynomials $P^j_1(x),\dots,P^j_n(x)$ that do not vanish on C_j, formulas $\psi^j_1(x,y)$ in the language of rings, and formulas $\psi^j_2(x,y)$ in the language of ordered groups, such that $\mathcal{T}_{Hvf,0}$ implies that $\phi(x,y,z)$ is equivalent to the formula*

$$\bigvee_j \Big(x\in C_j \wedge \psi^j_1(\mathrm{ac}(P^j_1(x)\cdots P^j_n(x)),y)\wedge \psi^j_2(\mathrm{val}(P^j_1(x)\cdots P^j_n(x)),z)\Big)\,.$$

Theorem 4.13 (Elimination of quantifiers in the theory of $\mathbb{Z}$; see [19, Lemma 5.5]). *Let A be a definable set in the language of ordered groups. Then the theory of $\mathbb{Z}$ implies that A is equal to a Boolean combination of definable sets defined by formulas of the form*

$$\phi(x)\geq 0\wedge(\exists y\in\Gamma)\psi(x)=n\cdot y,$$

where $\phi(x),\psi(x)$ are linear functionals with integer coefficients and $n\in\mathbb{N}$.

The following is an easy corollary of Theorem 4.13.

Lemma 4.14. *Every definable function $f:\mathbb{A}^n_O\to\mathbb{A}_O$ is piecewise linear. In other words, there is a partition of $\mathbb{A}^n_O$ to definable sets $\mathbb{A}^n_O=X_1\sqcup\cdots\sqcup X_m$, there are linear functionals $\varphi_1,\dots,\varphi_m$ with rational coefficients, and there are definable elements $\gamma_1,\dots,\gamma_m\in\mathbb{A}_O$ such that $\mathcal{T}_{Hvf}$ implies the sentence*

$$(\forall x\in\mathbb{A}^n_O)\,(x\in X_i\to f(x)=\varphi_i(x)+\gamma_i)\,.$$

Proposition 4.15. *A definable function $q:\mathbb{A}^n_V\to\mathbb{A}^1_O$ is (in $\mathcal{T}_{Hvf,0}$, and, a posteriori, in $\mathbb{M}_p$ for p large enough) piecewise of the form $\frac{1}{n}\mathrm{val}\left(\frac{f(x)}{g(x)}\right)$, where f and g are polynomials.*

Proof. Let $q:\mathbb{A}^n_V\to\mathbb{A}^1_O$ be a definable function. By Theorem 4.12, the graph of q, which is a subset of $\mathbb{A}^n_V\times\mathbb{A}^1_O$, is defined by a formula of the type

$$\bigvee\phi_i(\mathrm{val}(P_1(x)),\dots,\mathrm{val}(P_r(x)),\gamma)\wedge\psi_i(\mathrm{ac}(P_1(x)),\dots,\mathrm{ac}(P_r(x)))$$
$$\wedge\,(Q^i_1(x)\cdots=Q^i_t(x)=0)\wedge(Q^i_{t+1}(x)\neq 0),$$

where $P_i(x)$ and $Q^i_j(x)$ are polynomials, $\phi(y_1, \dots, y_r, z)$ is a formula in the language of ordered groups, and $\psi(x_1, \dots, x_r)$ is a formula in the language of fields. Decompose the domain of q according to the conditions $Q^i_j(x) = 0$ and $\psi_i(\mathrm{ac}(P_j(x)))$. Let A be one of the pieces. On A, the graph of q is given by a formula $\phi(\mathrm{val}(P_j(x)), \gamma)$. Again, by Theorem 4.12, $\mathrm{val}(A)$ is a subset B in $\mathbb{A}^n_O$ which is definable in the language of ordered groups. Therefore the formula $\phi(y_1, \dots, y_r, z)$ defines a graph of a function from B to $\mathbb{A}^1_O$. Since by Lemma 4.14 every such function is piecewise linear, we get that after a further division of the domain, q is of the form required. □

Proposition 4.16. *Let $A \subset \mathbb{A}^n_V \times \mathbb{A}^m_R$ be a definable family. Then there is a definable set $B \subset \mathbb{A}^{l+m}_R$ and a definable function $f : \mathbb{A}^n_V \to \mathbb{A}^l_R$ such that*

$$A = \{(x, y) \in \mathbb{A}^n_V \times \mathbb{A}^m_R \mid (f(x), y) \in B\}$$

in $\mathcal{T}_{Hvf,0}$, and, a posteriori, in all but finitely many of the models $\mathbb{M}_p$. We say that A is the pullback of B via f.

Proof. By elimination of quantifiers we can assume that A is defined by a formula $\phi(x, y)$ (x is a valued field sort and y is a residue field sort) that is the conjunction of conditions of the form

(1) $\psi(\mathrm{val}(P_1(x)), \dots, \mathrm{val}(P_n(x)))$, where P_i are polynomials and ψ is a formula in the language of ordered group;
(2) $\xi(\mathrm{ac}(Q_1(x)), \dots, \mathrm{ac}(Q_m(x)), y)$, where Q_i are polynomials and ξ is a formula in the language of fields.

Decompose $\mathbb{A}^n_V$ according to condition (1). Denote the resulting pieces by X_i, where $i \in I$. For every i there is a formula ξ_i such that the restriction of A over X_i is the pullback of the definable set ξ_i via the map $(\mathrm{ac}(q_1), \dots, \mathrm{ac}(q_m))$. Define a map $\Psi : \mathbb{A}^n_V \to \mathbb{A}^{m+|I|}_R$ by $\Psi(x)_i = \mathrm{ac}(q_i(x))$ for $i \le m$, $\Psi(x)_j = 1$ if $j > m$ and $x \in X_{j-m}$, and $\Psi(x)_j = 0$ if $j > m$ and $x \notin X_{j-m}$. Let $\Omega \subset \mathbb{A}^{m+|I|}_R$ be the definable set that is the conjugation of the conditions

$$z_{j+m} = 1 \to \xi_j(z_1, \dots, z_m)$$

for $j = 1, \dots, |I|$. It is now clear that A is the pullback of Ω via the map Ψ. □

Proposition 4.17. (1) *Given a polynomial $P(x) \in \mathbb{Q}_{\ge 0}[x]$ such that $\lim_{x\to\infty} P(x) = \infty$, there is a definable set Y in the language of rings and a constant c such that for all primes p,*

$$1 - c \cdot p^{-\frac{1}{2}} < \frac{|Y(\mathbb{F}_p)|}{P(p)} < 1 + c \cdot p^{-\frac{1}{2}}.$$

(2) *Let $X \subset \mathbb{A}^n_V$ be a definable set, and let A be a definable family over X. Then there is a definable function $\psi : X \to \mathbb{A}_O$, a definable family B*

over X, and a constant c, such that for all primes p and $x \in X(\mathbb{M}_p)$, either $A_x(\mathbb{M}_p)$ is empty, or

$$1 - c \cdot p^{-\frac{1}{2}} < p^{\psi(x)} \cdot |B_x(\mathbb{M}_p)| \cdot |A_x(\mathbb{M}_p)| < 1 + c \cdot p^{-\frac{1}{2}}.$$

Proof. (1) Suppose that the leading coefficient of $P(x)$ is $\frac{a}{b}x^k$ where a, b, k are positive integers. Let $\phi : C_1 \to C_2$ be a Galois cover defined over $\mathbb{Q}$ of irreducible curves with Galois group $\mathbb{Z}/b$. For almost all primes p, the reduction modulo p of ϕ is also a Galois cover with the same Galois group. Let D be the definable set defined by the formula

$$x \in C_2 \wedge (\exists y \in C_1)(x = \phi(y)).$$

Then by Weil's theorem there is a constant K such that

$$1 - K \cdot p^{-\frac{1}{2}} < \left| \frac{|D(\mathbb{F}_p)|}{\frac{1}{b}p} \right| < 1 + K \cdot p^{-\frac{1}{2}}.$$

To get the claim of the lemma, take $\mathcal{P}$ be the definable set

$$(\underbrace{D \sqcup \cdots \sqcup D}_{a}) \times \mathbb{A}^{k-1}.$$

(2) By Proposition 4.16 and Theorem 4.4 there is a constant K and a partition of X into definable sets X_i, and for each X_i there is $d_i \in \mathbb{N}$ and $c_i \in \mathbb{Q}_{>0}$, such that if $x \in X_i(\mathbb{M}_p)$, then

$$\left| |\mathcal{A}_x(\mathbb{M}_p)| - c_i p^{d_i} \right| < K \cdot p^{d_i - \frac{1}{2}}.$$

Using the construction from (1), one can find definable sets B_i such that for all p,

$$1 - K \cdot p^{-\frac{1}{2}} < \left| \frac{|B_i(\mathbb{F}_p)|}{c_i \cdot p} \right| < 1 + K \cdot p^{-\frac{1}{2}}.$$

Denote by $\mathcal{B}$ the definable family that is equal to B_i over X_i, and denote by $\psi_i : X \to \mathbb{A}^1_O$ the definable function that equals $d_i - 1$ on X_i. Then $\mathcal{B}, \psi$ satisfy the requirements of the lemma. □

4.5. *V-functions.* Definable elements in $\mathbb{A}^1_O$ give us a collection of (rational) numbers, indexed by the prime numbers. Given a definable element $\gamma \in \mathbb{A}^1_O$ and a prime p, we consider the number $\gamma_p = p^{\gamma^{\mathbb{M}_p}}$, where $\gamma^{\mathbb{M}_p} \in \mathbb{Z}$ is the interpretation of γ in the model $\mathbb{M}_p$. More generally, definable functions from $\mathbb{A}^n_V$ to $\mathbb{A}^1_O$ give us a collection of rational-valued functions. Namely, if $f : \mathbb{A}^n_V \to \mathbb{A}^1_O$ is a definable function and p is a prime number, we consider the function $f_p : \mathbb{Q}_p^n \to \mathbb{Q}$ given by $x \mapsto p^{f^{\mathbb{M}_p}(x)}$, where $f^{\mathbb{M}_p}$ is the interpretation of f in the model $\mathbb{M}_p$.

Another source of numbers in $\mathcal{T}_{Hvf}$ is definable sets in $\mathbb{A}^m_R$. Given a definable set $X \subset \mathbb{A}^m_R$ and a prime p, we consider the number $X_p = |X(\mathbb{M}_p)|$ (since $X(\mathbb{M}_p) \subset \mathbb{A}^m_R(\mathbb{M}_p) = \mathbb{F}_p^m$, the set $X(\mathbb{M}_p)$ is indeed finite). As above, from a definable set $Y \subset \mathbb{A}_V^n \times \mathbb{A}_R^m$ we get a collection of integer-valued functions, indexed by the prime numbers. The next definition is a generalization of these two constructions.

Definition 4.18. Let $X \subset \mathbb{A}_V^n$ be a definable set.

(1) A V-function with domain X is a tuple of the form $\mathcal{F} = (X_i, \phi_i, \mathcal{V}_i)_{i \in I}$, where I is a finite set and
  (a) $X_i \subset \mathbb{A}_V^n$ are definable sets that form a partition of X,
  (b) $\phi_i : \mathbb{A}_V^n \to \mathbb{A}_O^1$ are definable maps, and
  (c) $\mathcal{V}_i \subset \mathbb{A}_V^n \times \mathbb{A}_R^{n_i}$ are definable sets.

(2) Given a V-function $\mathcal{F}$ with domain X and a prime number p, we define a function $\mathcal{F}_p : X(\mathbb{M}_p) \times \mathbb{C} \to \mathbb{C}$ by

$$\mathcal{F}_p(x,s) = \sum_{i \in I} 1_{X_i(\mathbb{M}_p)}(x) p^{-s\phi_i(x)} \cdot |\mathcal{V}_i(\mathbb{M}_p)_x|^{-s}.$$

(3) A V-function with domain X is called bounded if there exists a definable element $\gamma \in \mathbb{A}_O$ such that for all i, the following sentences hold.
  (a) $\forall x \in X_i \quad (\phi_i(x) > \gamma)$;
  (b) $\forall (x_1, \ldots, x_n) \in X_i \, ((\mathrm{val}(x_1) < \gamma \vee \cdots \vee \mathrm{val}(x_n) < \gamma) \longrightarrow (\mathcal{V}_i)_x = \emptyset)$.

Remark 4.19. (1) By changing X_i, every sequence of functions of the more general form

$$(x,s) \mapsto \sum_{i \in I} 1_{X_i(\mathbb{M}_p)}(x) p^{-s\phi_i(x) + \psi_i(x)} \cdot |\mathcal{V}_i(\mathbb{M}_p)_x|^{-s} \cdot |\mathcal{W}_i(\mathbb{M}_p)_x|,$$

where $X_i \subset \mathbb{A}_V^n$ are definable sets, $\phi_i, \psi_i : X_i \to \mathbb{A}_O^1$ are definable maps, and $\mathcal{V}_i, \mathcal{W}_i \subset \mathbb{A}_V^n \times \mathbb{A}_R^m$ are definable families, actually comes from a V-function.

(2) If $\mathcal{F}_1$ and $\mathcal{F}_2$ are V-functions, then there are V-functions $\mathcal{G}_+$ and $\mathcal{G}_\times$ such that for every p,

$$(\mathcal{G}_+)_p = (\mathcal{F}_1)_p + (\mathcal{F}_2)_p \quad \text{and} \quad (\mathcal{G}_\times)_p = (\mathcal{F}_1)_p \cdot (\mathcal{F}_2)_p.$$

We shall write $\mathcal{F}_1 + \mathcal{F}_2$, respectively $\mathcal{F}_1 \cdot \mathcal{F}_2$, instead of $\mathcal{G}_+$, respectively $\mathcal{G}_\times$.

Example 4.20. Fix integers A and B. Let $\mathcal{O}^\times \subset \mathbb{A}_V^1$ be the definable set given by the formula '$x \neq 0 \wedge \mathrm{val}(x) \geq 0$', let $\phi : \mathcal{O}^\times \to \mathbb{A}_O^1$ be the function $\phi(x) = A\,\mathrm{val}(x)$, and $\psi : \mathcal{O}^\times \to \mathbb{A}_O^1$ be the function $\psi(x) = (B+1)\,\mathrm{val}(x)$. By the previous remark we get a V-function $\mathcal{F}$ such that

$$\mathcal{F}_p(x,s) = \begin{cases} p^{n(As+B+1)} & \mathrm{val}(x) = n \geq 0 \\ 0 & \text{else} \end{cases}$$

and so

$$\int \mathcal{F}_p(x,s)dx = \frac{p-1}{p}\sum_{n=0}^{\infty} p^{As+B} = \frac{p-1}{p}\frac{1}{1-p^{As+B}}.$$

5. **Uniformity of the local factors I**

Our goal in this section is to prove:

Theorem 5.1. *Let Σ be a finite set of primes, and let $\underline{G}$ be a linear algebraic group scheme over* $\operatorname{Spec}\mathbb{Z}_\Sigma$ *such that the generic fiber of $\underline{G}$ is semisimple, simply connected, and connected. There is a definable set $X \subset \mathbb{A}^n_F$ and a V-function $\mathcal{F}$ with domain X, such that the sequence of functions $\zeta_{\underline{G}(\mathbb{Z}_p)}(s)-1$ is equivalent to the sequence of functions*

$$\xi_p(s) = \int_{X(\mathbb{M}_p)} \mathcal{F}_p(x,s)d\lambda(x),$$

where $d\lambda$ is the restriction of the Haar measure of $\mathbb{Q}_p^n$ to $X(\mathbb{M}_p)$.

By Theorem 2.1, Proposition 4.17, and Example 4.20, it is enough to show that there is a prime p_0 and a V-function $\mathcal{F}$ such that the sequence $(\zeta_{\underline{G}(\mathbb{Z}_p)}(s)-1)_{p>p_0}$ is equivalent to the sequence $(\xi_p(s))_{p>p_0}$ considered in the theorem. Therefore, in this section we will assume that p is large enough.

5.1. *Representations of the first congruence subgroup.* Let $\underline{G}$ be as in Theorem 5.1. The corresponding $\mathcal{T}_{Hvf}$-definable group will be denoted by G. The definable subset $G_{\mathcal{O}}$ is defined by

$$g=(g_{i,j}) \in G_{\mathcal{O}} \iff g \in G \wedge \operatorname{val}(g_{i,j}) \geq 0.$$

For all $p \notin \Sigma$ we have that $G_{\mathcal{O}}(\mathbb{M}_p) = \underline{G}(\mathbb{Z}_p)$, a group which was denoted by G_p.

Let $\mathfrak{g} \subset (\mathrm{M}_n)_F$ be the definable set such that, for almost all p's, $\mathfrak{g}(\mathbb{M}_p)$ is the Lie algebra $\mathfrak{g}_p$ of G_p; see Section 3.2 for the construction. The definable set

$$\mathfrak{g}^1 = \{A \in \mathfrak{g} \mid \operatorname{val}(A_{i,j}) > 0\}$$

satisfies that $\mathfrak{g}^1(\mathbb{M}_p)$ is the Lie algebra $\mathfrak{g}^1_p$ of G^1_p — the first congruence subgroup of G_p — for almost all p's.

Assume that p is large. The orbit method (Theorem 3.7) gives us a map Ξ_p from $(\mathfrak{g}^1_p)^\vee$ onto $\operatorname{Irr}(G^1_p)$ such that $\Xi_p(\theta)=\Xi_p(\theta')$ if and only if there is a $g \in G^1_p$ such that $\operatorname{Ad}^*(g)\theta=\theta'$.

Recall that $\mathcal{O} \subset \mathbb{A}^1_V$ is the definable set attached to the formula '$\operatorname{val}(x) \geq 0$'. Let $\mathscr{X}$ be the following definable set:

$$\mathscr{X} = \{A \in \mathfrak{g}_F \mid \max\{\operatorname{val}(A_{i,j})\}=0\} \times \mathcal{O} \setminus \{0\}.$$

Consider the function $x \mapsto \exp(2\pi i x)$ defined on $\mathbb{Z}[\frac{1}{p}]$. It has a unique extension to a continuous character of $\mathbb{Q}_p$, which we also denote by $\exp(2\pi i x)$. Let $\langle\, , \rangle$ be the bilinear form

$$\langle A, B\rangle = \operatorname{trace}(A \cdot B)$$

on the space of matrices.

For every prime p, the map $\Phi_p : \mathscr{X}(\mathbb{M}_p) \to (\mathfrak{g}_p^1)^\vee$ given by

$$\Phi_p((A,z))(B) = \exp\left(\frac{2\pi i}{z}\langle A, B\rangle\right)$$

is a surjection. Let Ψ_p be the composition of Ξ_p and Φ_p. We have the following:

Theorem 5.2 ([12, Th. 4.6]). *There are definable functions $\phi_1, \phi_2 : \mathscr{X} \to \mathbb{A}^1_O$ such that for all primes p and for all $(A, z) \in \mathscr{X}(\mathbb{M}_p)$,*

$$\dim \Psi_p(A,z) = p^{\phi_1(A,z)} \qquad \textit{and} \qquad \lambda(\Psi_p^{-1}(\Psi_p(A,z))) = p^{\phi_2(A,z)}.$$

5.2. *Decomposition trees.* We describe our method for extending representations from the first congruence subgroup, G_p^1, to the whole group, G_p. Let ρ be an irreducible representation of G_p^1. Recall that $\operatorname{Irr}(G_p|\rho)$ is the set of irreducible representations of G_p, whose restrictions to G_p^1 contain ρ as a component. We wish to compute the relative zeta function

$$\zeta_{G_p|\rho}(s) = \sum_{\tau \in \operatorname{Irr}(G_p|\rho)} \left(\frac{\dim \tau}{\dim \rho}\right)^{-s}.$$

Consider the stabilizer $G_p^1 \subset S \subset G_p$ of the representation ρ. Let V be the maximal normal pro-p subgroup of S.

Lemma 5.3. *Let $K \subset V \subset S \subset H$ be an increasing chain of groups, and let ρ be an irreducible representation of K. Assume that K is normal in H, that V is normal in S, that S is the stabilizer of ρ in H, and that K is of finite index in H. For a representation τ of V, denote the orbit of τ under the action of S by τ^S. Then*

$$\zeta_{H|\rho}(s) = \sum_{\tau \in \operatorname{Irr}(V|\rho)} \frac{[H:S]^{-s}}{|\tau^S|} \left(\frac{\dim \tau}{\dim \rho}\right)^{-s} \zeta_{S|\tau}(s).$$

Proof. Let $\chi \in \operatorname{Irr}(S|\rho)$. The irreducible components of the restriction $\operatorname{Res}^S_K \chi$ form one S-orbit, since χ is irreducible and K is normal in S. Since this restriction contains ρ as an irreducible component, we deduce that $\operatorname{Res}^S_K \chi = \operatorname{Res}^V_K \circ \operatorname{Res}^S_V \chi$ is a multiple of ρ. Therefore, every irreducible component of $\operatorname{Res}^S_V \chi$ is in $\operatorname{Irr}(V|\rho)$.

Let $\tau \in \operatorname{Irr}(V|\rho)$. The irreducible components of $\operatorname{Res}^S_V \operatorname{Ind}^S_V \tau$ are just τ^S. Therefore, if τ_1, τ_2 are two representations in $\operatorname{Irr}(V|\rho)$, which are in the same

S-orbit, then $\mathrm{Irr}(S|\tau_1) = \mathrm{Irr}(S|\tau_2)$, whereas if τ_1 and τ_2 are not in the same orbit, then $\mathrm{Irr}(S|\tau_1)$ and $\mathrm{Irr}(V|\tau_2)$ are disjoint.

Let $\tau_1, \dots, \tau_m$ be representatives for the S-orbits in $\mathrm{Irr}(V|\rho)$. Using the remark in the previous paragraph, we compute

$$\begin{aligned}\zeta_{S|\rho}(s) &= \sum_{\chi \in \mathrm{Irr}(S|\rho)} \left(\frac{\dim \chi}{\dim \rho}\right)^{-s} = \sum_{i=1}^{m} \sum_{\chi \in \mathrm{Irr}(S|\tau_i)} \left(\frac{\dim \chi}{\dim \rho}\right)^{-s} \\ &= \sum_{\tau \in \mathrm{Irr}(V|\rho)} \frac{1}{|\tau^S|} \left(\frac{\dim \tau}{\dim \rho}\right)^{-s} \sum_{\chi \in \mathrm{Irr}(S|\tau)} \left(\frac{\dim \chi}{\dim \tau}\right)^{-s} \\ &= \sum_{\tau \in \mathrm{Irr}(V|\rho)} \frac{1}{|\tau^S|} \left(\frac{\dim \tau}{\dim \rho}\right)^{-s} \zeta_{S|\tau}(s).\end{aligned}$$

Since for every representation $\chi \in \mathrm{Irr}(S|\rho)$, the induction $\mathrm{Ind}_S^H \chi$ is irreducible, and since all the irreducible representations of H, lying over ρ, are obtained in this way, we get that

$$\zeta_{H|\rho}(s) = \zeta_{S|\rho}(s) \cdot [H : S]^{-s}. \qquad \square$$

Lemma 5.3 reduces the computation of $\zeta_{G_p|\rho}(s)$ to the computation of $\mathrm{Irr}(V|\rho)$, and, for each $\tau \in \mathrm{Irr}(V|\rho)$, a computation of $\zeta_{S|\tau}(s)$.

Let $\mathrm{Irr}(V|\rho) = \{\rho_1, \dots, \rho_n\}$. For each ρ_i, let S_i be the stabilizer of ρ_i in S, let V_i be the maximal normal pro-p subgroup of S_i, and let $\rho_{i,1}, \dots, \rho_{i,n_i}$ be the irreducible characters of V_i lying over ρ_i. The following diagram is a summary of the notation so far:

$$\begin{tikzcd}
 & & (G_p, G_p^1, \rho) \arrow[dl] \arrow[dr] & \\
 & (S, V, \rho_1) \arrow[dl] \arrow[dr] & \cdots & (S, V, \rho_n) \\
(S_1, V_1, \rho_{1,1}) & \cdots & (S_1, V_1, \rho_{1,n_i}) & \cdots .
\end{tikzcd}$$

We may continue in the same fashion, constructing a deeper and deeper trees. We reach a leaf of the tree whenever $S_{i_1\cdots_k}$ is the stabilizer of $\rho_{i_1\cdots i_{k+1}}$ and $S_{i_1\cdots i_k}/V_{i_1\cdots i_k}$ has no nontrivial normal p-subgroups.

We call the resulting tree, whose vertices are labeled by triples $(S_{i_1\cdots i_k}, V_{i_1\cdots i_k}, \rho_{i_1\cdots i_{k+1}})$, the *decomposition tree* of ρ. The relative representation zeta function $\zeta_{G_p|\rho}(s)$ can be easily computed from the decomposition tree, and the relative representation zeta functions of the leaves. The following lemma shows that the zeta functions of the leaves are simple.

Lemma 5.4. *For every n, there is a constant c, that depends only on n, such that if p is a prime number, which is large enough with respect to n, then the following is true: Let $S \subset \mathrm{GL}_n(\mathbb{Z}_p)$ be a group, let V be a normal pro-p subgroup of S that contains the first congruence subgroup G_p^1, and let ρ be a representation of V. Assume that S stabilizes ρ, and assume that S/V has no nontrivial normal p-subgroups. Then*

(1) *the group $(S/V)^+$ is a perfect extension of a direct product of finite simple groups of Lie type*;
(2) $c^{-1-s} \cdot \zeta_{S|\rho}(s) \leq [S : S^+] \cdot \zeta_{(S/V)^+}(s) \leq c^{1+s} \cdot \zeta_{S|\rho}(s)$.

In the middle term, $\zeta_{(S/V)^+}(s)$ is the (nonrelative) representation zeta function of the group $(S/V)^+$ and S^+ is the closed subgroup of S that is generated by the pro-p elements of S.

Proof. Denote the quotient S/G_p^1 by Γ. By a theorem of Larsen and Pink (Theorem 0.2 of [15]), there are normal subgroups $\Gamma_3 \subset \Gamma_2 \subset \Gamma_1 \subset \Gamma$ such that

(1) Γ_3 is a p-group;
(2) Γ_2/Γ_3 is central in Γ_1/Γ_3[7], and its order is prime to p;
(3) Γ_1/Γ_2 is a product of simple finite groups of Lie type;
(4) the index of Γ_1 in Γ is bounded by a function of n only.

Let $\widetilde{\Gamma_i}$ be the subgroups of S such that $\widetilde{\Gamma_i}/G_p^1 = \Gamma_i$.

By our assumptions, S/V has no nontrivial normal p-subgroups. Therefore, $\widetilde{\Gamma_3} = V$.

If p is large enough, then every p-element in Γ has to be contained in Γ_1. Therefore $\Gamma^+ \subset \Gamma_1$. We clearly have that $\Gamma^+/(\Gamma_2 \cap \Gamma^+) \subset \Gamma_1/\Gamma_2$. Since Γ_1/Γ_2 is generated by its elements of order p, and since every such element can be lifted to an element of Γ_1, we get that, in fact, $\Gamma^+/(\Gamma_2 \cap \Gamma^+) = \Gamma_1/\Gamma_2$. We get a central extension

$$0 \to \Gamma_2/\Gamma_3 \to \Gamma^+ \cdot \Gamma_2/\Gamma_3 \to \Gamma^+ \cdot \Gamma_2/\Gamma_2 = \Gamma^+/(\Gamma^+ \cap \Gamma_2) = \Gamma_1/\Gamma_2 \to 0.$$

This extension splits as a direct product $\Gamma^+ \cdot \Gamma_2/\Gamma_3 = P \times A$, where P is a perfect extension and A is abelian. Since the group P is a perfect central extension of a product of finite simple groups of Lie type, and since each finite simple group is generated by its elements of order p, we get that P is generated by its elements of order p. Therefore we get that $\Gamma^+/\Gamma_3 \subset P$. Since the group A is contained in Γ_2/Γ_3 and the order of Γ_2/Γ_3 is prime to p, we get that $\Gamma^+/\Gamma_3 = P$.

[7] This claim is not a part of the statement of Theorem 0.2 of [15]. However, Γ_1, Γ_2, and Γ_3 are constructed as the intersection of Γ with a connected algebraic group, its radical, and its unipotent radical respectively.

We consider first the extensions of ρ to $S^+ \cdot \widetilde{\Gamma_2}$. These extensions are governed by a certain element β in the second cohomology $H^2(S^+ \cdot \widetilde{\Gamma_2}/V, \mathbb{C}^\times)$, as described in Section 3.5. By Proposition 3.12 this element has order p. By Proposition 3.13 the sizes of the first and second cohomology groups of finite simple groups are bounded independently of p. By Künneth formula for the cohomology of products, the sizes of $H^1(\Gamma_1/\Gamma_2, \mathbb{C}^\times)$ and $H^2(\Gamma_1/\Gamma_2, \mathbb{C}^\times)$, and hence of $H^1(P, \mathbb{C}^\times)$ and $H^2(P, \mathbb{C}^\times)$, are bounded independently of p. Since A is an abelian group and its size is prime to p, the sizes of the first and second cohomology groups of A are also prime to p. By Künneth formula again, we get that the size of the second cohomology group $H^2(\Gamma^+ \cdot \Gamma_2/\Gamma_3, \mathbb{C}^\times)$ is prime to p and hence contains no elements of order p. Therefore, the representation ρ extends to a representation of $S^+ \cdot \widetilde{\Gamma_2}$. By Proposition 3.11, every representation in $\mathrm{Irr}(S^+|\rho)$ is of the form $\chi_0 \otimes \theta$, where χ_0 is a fixed extension and θ is a character of $S^+ \cdot \widetilde{\Gamma_2}/V = P \times A$. We conclude that

$$\zeta_{S^+ \cdot \widetilde{\Gamma_2}|\rho}(s) = \zeta_{P \times A}(s) = \zeta_{(S/V)^+}(s) \cdot |A|.$$

Since $S^+ \cdot \widetilde{\Gamma_2} = \widetilde{\Gamma_1}$ has a bounded index in S, we conclude from Lemma 3.3 that there is a constant c_1 such that

$$c_1^{-1-s} \cdot \zeta_{S|\rho}(s) \leq \zeta_{S^+ \cdot \widetilde{\Gamma_2}|\rho}(s) \leq c_1^{1+s} \cdot \zeta_{S|\rho}(s).$$

Finally, since

$$\frac{|A|}{[S : S^+]} = \frac{[\Gamma^+ \cdot \Gamma_2/\Gamma_3 : P]}{[S : S^+]} = \frac{[\Gamma_1 : \Gamma^+]}{[\Gamma : \Gamma^+]} = [\Gamma : \Gamma_1]^{-1}$$

is bounded as a function of n, we get the conclusion of the theorem. □

The computation of $\zeta_{G_p|\rho}$ is thus reduced to the computation of the decomposition tree of ρ. In the next section we shall show how to construct the decomposition trees for families — both for varying the representation ρ and for varying the prime p as well.

5.3. *The family of decomposition trees.* Let Grass be the Grassmanian of subspaces of $\mathfrak{g}_R$, considered as a $\mathcal{T}_{Hvf}$-definable set (see §4.1). We have the tautological bundle $\widetilde{\mathrm{Grass}} \subset \mathrm{Grass} \times \mathfrak{g}_R$ consisting of pairs (v, A) such that A belongs to the subspace v of $\mathfrak{g}$. We consider $\widetilde{\mathrm{Grass}}$ also as a definable set. The condition that $v \in \mathrm{Grass}$ is closed under Lie brackets, is a definable condition; so is the condition that $v \in \mathrm{Grass}$ is a nilpotent Lie subalgebra of $\mathfrak{g}_R$. We denote the definable subset of Grass that consists of the nilpotent Lie subalgebras of $\mathfrak{g}$ by Grass_U. For every prime p, if $v \in \mathrm{Grass}_U(\mathbb{M}_p)$, then the set

$$L(v) = \{A \in \mathfrak{g}_p \mid \mathrm{ac}(A) \in v\}$$

is a pro-nilpotent Lie subalgebra of $\mathfrak{g}_p$. If p is large enough, then $\exp(L(v))$ is a pro-p subgroup of G_p and the Orbit Method (Theorem 3.7) holds for it.

Let $\mathscr{X}$ be the definable set defined in 5.1. Recall that for every p large enough we have constructed a map

$$\Phi_p : \mathscr{X}(\mathbb{M}_p) \to (\mathfrak{g}_p^1)^\vee.$$

We wish to extend this map to larger subalgebras of $\mathfrak{g}_p$. If $v \in \mathrm{Grass}_U$, we denote by v^T the set of elements in $\mathfrak{g}_R$ whose transpose is contained in v. Given a prime p, an element $x = (A, z) \in \mathscr{X}(\mathbb{M}_p)$, a nilpotent Lie subalgebra $v \in \mathrm{Grass}_U(\mathbb{M}_p)$, and an element $\theta \in v^T$, we define a linear character $\widetilde{\Phi_p}(x, v, \theta) \in L(v)^\vee$ by

$$\widetilde{\Phi_p}(x, v, \theta)(B) = \exp\left(\frac{2\pi i}{z}\langle A, B\rangle\right) \cdot \exp\left(\frac{2\pi i}{p}\langle \theta, \mathrm{ac}(B)\rangle\right)$$

for every $B \in L(v)$.

Let $\mathscr{Y} \subset \mathscr{X} \times \mathrm{Grass}_U \times \mathfrak{g}$ be the definable set consisting of triples (x, v, θ) such that $\theta \in v^T$. We denote by $\widetilde{\Xi_p}$ the Orbit Method map from $L(v)^\vee$ to $\mathrm{Irr}(\exp(L(v)))$, and denote by $\widetilde{\Psi_p}$ the composition of $\widetilde{\Phi_p}$ and $\widetilde{\Xi_p}$. We get a diagram

(5.1)

$$\begin{tikzcd}
\mathscr{Y}(\mathbb{M}_p) \arrow[r, "\widetilde{\Phi_p}"] \arrow[d] & \bigsqcup_{v \in \mathrm{Grass}_U(\mathbb{M}_p)} L(v)^\vee \arrow[r, "\widetilde{\Xi_p}"] \arrow[d] & \bigsqcup_{v \in \mathrm{Grass}_U(\mathbb{M}_p)} \mathrm{Irr}(\exp(L(v))) \arrow[d] \\
\mathscr{X}(\mathbb{M}_p) \arrow[r, "\Phi_p"] & (\mathfrak{g}_p^1)^\vee \arrow[r, "\Xi_p"] & \mathrm{Irr}(G_p^1),
\end{tikzcd}$$

where the leftmost vertical arrow is the projection to the first coordinate and the other two vertical arrows are the restriction maps. It is easy to see that this diagram commutes.

Definition 5.5. Let $G_{\mathcal{O}}$ be the definable set

$$g = (g_{i,j}) \in G_{\mathcal{O}} \quad \Longleftrightarrow \quad g \in G \wedge \mathrm{val}(g_{i,j}) \geq 0.$$

We have that $G_{\mathcal{O}}(\mathbb{M}_p) = G_p$.

Definition 5.6. We define actions of $G_{\mathcal{O}}$ on $\mathscr{X}$ and $\mathscr{Y}$ in the following way.

(1) If $g \in G_{\mathcal{O}}$ and $x = (A, z) \in \mathscr{X}$, we define

$$g \cdot (A, z) = (g^{-1} A g, z).$$

(2) Let $g \in G_{\mathcal{O}}$ and $y = (x, v, \theta) \in \mathscr{Y}$. Let $w \in \mathrm{Grass}_U$ be the subspace $\mathrm{Ad}(\mathrm{ac}(g))v$. There is a unique $\tau \in (\mathrm{Ad}(\mathrm{ac}(g))v)^T$ such that for every $A \in v$,

$$\langle A, \theta\rangle = \langle \mathrm{ac}(g)^{-1} A \,\mathrm{ac}(g), \tau\rangle.$$

We define $g \cdot (x, v, \theta) = (g \cdot x, w, \tau)$.

For every prime p, the group G_p acts on each vertex of Diagram (5.1): on the vertices of the left column $G_p = G_{\mathcal{O}}(\mathbb{M}_p)$ acts via Definition 5.6, on the vertices of the middle column G_p acts by the coadjoint action, and on the vertices of the right column G_p acts by conjugation.

LEMMA 5.7. *All arrows in Diagram* (5.1) *intertwine the different actions of* G_p.

Proof. For Φ_p, $\widetilde{\Phi}_p$, and the leftmost and middle vertical arrows, this is a simple computation. For Ξ_p, $\widetilde{\Xi_p}$, and the rightmost vertical arrow, this follows from Theorem 3.7. □

LEMMA 5.8. *There is a definable family* $\mathcal{N} \subset \mathrm{Grass}_U \times G$ *such that for every* $v \in \mathrm{Grass}_U$, *the fiber* $\mathcal{N}_v$ *is the normalizer of the subgroup* $\exp(L(v))$ *in* G.

LEMMA 5.9. (1) *There is a definable set* $S^{\mathrm{char}} \subset \mathscr{Y} \times G_{\mathcal{O}}$ *such that for every* p *and every* $y \in \mathscr{Y}(\mathbb{M}_p)$, *we have that* $S^{\mathrm{char}}_y(\mathbb{M}_p)$ *is the stabilizer in* $N_{G_p}(L(v))$ *of the linear character* $\widetilde{\Phi_p}(y)$ *of* $L(v)$.

(2) *There is a definable set* $S^{\mathrm{rep}} \subset \mathscr{Y} \times G_{\mathcal{O}}$ *such that for every* p *and every* $y \in \mathscr{Y}(\mathbb{M}_p)$, *we have that* $S^{\mathrm{rep}}_y(\mathbb{M}_p)$ *is the stabilizer in* $N_{G_p}(\exp(L(v)))$ *of the representation* $\widetilde{\Psi_p}(y)$ *of* $\exp(L(v))$.

THEOREM 5.10. *Let* $\mathfrak{N}$ *be the set of nilpotent matrices in* $\mathfrak{g}$. *There is a natural number* N *and a sequence of definable families* $\mathcal{T}_i \subset \mathscr{X} \times (\mathrm{Grass}_U \times \mathfrak{N})^i$, *for* $i = 1, \dots, N$, *such that if we denote the natural projection from* $\mathcal{T}_{i+1}$ *to* $\mathcal{T}_i$ *by* π_i, *then*:

(1) $\mathcal{T}_1 = \mathscr{X} \times \{0\} \times \{0\}$;

(2) *for every prime* p, *every* $(x, v_1, \theta_1, \dots, v_i, \theta_i) \in \mathcal{T}_i(\mathbb{M}_p)$, *and every* $j \leq i$, *we have* $\theta_j \in v_j^T$;

(3) *for every prime* p *and every* $(x, v_1, \theta_1, \dots, v_i, \theta_i) \in \mathcal{T}_i(\mathbb{M}_p)$, *the fiber* $\pi_i^{-1}(x, v_1, \theta_1, \dots, v_i, \theta_i)$ *consists of the tuples* $(x, v_1, \theta_1, \dots, v_i, \theta_i, v, \theta)$ *such that* $\exp(L(v))$ *is the maximal normal* p *subgroup of the group* $\mathrm{Stab}_{N(v_1)\cap\cdots\cap N(v_i)} \widetilde{\Psi_p}(v_i, \theta_i)$, *and* $\widetilde{\Phi_p}(v, \theta)$ *is an extension of* $\widetilde{\Phi_p}(v_i, \theta_i)$;

(4) *for every prime* p *and every* $(x, v_1, \theta_1, \dots, v_N, \theta_N) \in \mathcal{T}_N(\mathbb{M}_p)$, *the maximal normal pro-*p *subgroup of the group* $\mathrm{Stab}_{N(v_1)\cap\cdots\cap N(v_N)} \widetilde{\Psi_p}(v_N, \theta_N)$ *is* $\exp(L(v_N))$;

(5) *there is a definable partition of* $\mathcal{T}_N$ *into finitely many pieces such that the semisimple hull of the stabilizer is constant along each piece.*

Proof. We construct $\mathcal{T}_i$ by induction. The set $\mathcal{T}_1$ is defined by the first requirement. Suppose we have constructed $\mathcal{T}_i$. By Lemma 5.9, there is a definable family $S \subset \mathcal{T}_i \times G_{\mathcal{O}}$ such that for every prime p and every $t =$

$(x, v_1, \theta_1, \ldots, v_i, \theta_i) \in \mathcal{T}_i(\mathbb{M}_p)$, the set $S_t(\mathbb{M}_p) \subset G_p$ is the stabilizer of $\widetilde{\Psi_p}(x, v_i, \theta_i)$ in the intersection $N_{G_p}(\exp(L(v_1))) \cap \ldots N_{G_p}(\exp(L(v_i)))$. By Proposition 4.11, there is a definable sub-family $U \subset S$ such that for every p and $t \in \mathcal{T}_i(\mathbb{M}_p)$, the fiber $U_t(\mathbb{M}_p)$ is the maximal normal pro-p subgroup of $S_t(\mathbb{M}_p)$. Hence we have a definable family $\mathcal{T}_i' \subset \mathcal{T}_i \times \text{Grass}$ such that for every p and t as above, $(\mathcal{T}_i')_t(\mathbb{M}_p)$ is the required unipotent radical. It is easy to see that defining $\mathcal{T}_{i+1}$ as consisting of the tuples $(x, v_1, \theta_1, \ldots, v_i, \theta_i, v, \theta)$ such that $(x, v_1, \theta_1, \ldots, v_i, \theta_i, v) \in \mathcal{T}_i'$ and $\theta \in v^T$, results in a definable family satisfying the second and third requirements.

Finally, for every i, either $\dim(v_i) < \dim(v_{i+1})$, or the unipotent radical of the stabilizer is equal to $\exp(L(v_i))$. Therefore the map $\mathcal{T}_{i+1} \to \mathcal{T}_i$ is an isomorphism for $i > N := \dim(G)$.

The last claim follows from Proposition 4.11. □

Lemma 5.11. *There is a definable partition of $\mathscr{Y}$ into sets $\mathscr{Y}_0, \ldots, \mathscr{Y}_N$ such that if $(x, v, \theta) \in \mathscr{Y}_i$; then*

$$\frac{|\operatorname{Ad}(L(v))(\widetilde{\Phi_p}(x, v, \theta))|}{|\operatorname{Ad}(G_p^1)\Phi_p(x)|} = p^{2i}$$

and therefore

$$\frac{\dim \widetilde{\Psi_p}(x, v, \theta)}{\dim \Psi_p(x)} = p^i.$$

Proof. The family of stabilizers of $\widetilde{\Phi_p}(x, v, \theta)$ is definable, and therefore its reduction modulo p is also definable. By Theorem 4.4, the dimension of the fibers are definable. This gives the first identity.

The second identity follows from the first. □

5.4. *Proof of Theorem* 5.1. We assume first that p is large enough. By Lemma 5.9 there is a definable family $S^{\text{rep}} \subset \mathscr{Y} \times G_{\mathcal{O}}$ such that for every $y = (x, v, \theta) \in \mathscr{Y}(\mathbb{M}_p)$, the fiber S_y^{rep} is the stabilizer in $N_{G_p}(L(v))$ of the representation $\widetilde{\Psi_p}(x, v, \theta) \in \operatorname{Irr}(\exp(L(v)))$. By the same lemma, there is a definable family $S^{\text{char}} \subset \mathscr{Y} \times G_V$ such that for every prime p and $y = (x, v, \theta) \in \mathscr{Y}(\mathbb{M}_p)$, the set $S_y^{\text{char}}(\mathbb{M}_p)$ is the stabilizer in $N_{G_p}(\exp(L(v)))$ of the character $\widetilde{\Phi_p}(x, v, \theta) \in L(v)^\vee$.

Definition 5.12. Let $\mathcal{T}_i$ be the decomposition tree constructed in Theorem 5.10. For every k, if p is a prime, $\ell = (x, v_1, \theta_1, \ldots, v_k, \theta_k) \in \mathcal{T}_k(\mathbb{M}_p)$, and $0 < j \le k$, we denote

$$S_0^{\text{rep}}(\ell) = G_p; \quad S_0^{\text{char}}(\ell) = G_p; \quad \Psi_0(\ell) = \Psi_p(x);$$

$$S_j^{\text{rep}}(\ell) = S_{(x,v_j,\theta_j)}^{\text{rep}}(\mathbb{M}_p); \quad S_j^{\text{char}}(\ell) = S_{(x,v_j,\theta_j)}^{\text{char}}(\mathbb{M}_p); \quad \Psi_j(\ell) = \widetilde{\Psi_p}(x, v_j, \theta_j),$$

and define

$$W_j(\ell) = \left| \left(\exp(L(v_j)) \cap S_{j-1}^{\mathrm{char}}(\ell) \right) (x, v_1, \theta_1, \ldots, v_j, \theta_j) \right|$$

and

$$R_k(\ell) = \frac{[G_p : S_{k-1}^{\mathrm{rep}}(\ell)]^{-s}}{\prod_{i \leq k-1} [S_i^{\mathrm{rep}}(\ell) : S_i^{\mathrm{char}}(\ell) \cdot \exp(L(v_i))] \cdot W_i(\ell)} \cdot \left(\frac{\dim \Psi_{k-1}(\ell)}{\dim \Psi_0(\ell)} \right)^{-s}.$$

Lemma 5.13. *Let $\mathcal{T}_i$ be the decomposition tree constructed in Theorem* 5.10. *For every prime p, every $x \in \mathscr{X}(\mathbb{M}_p)$, and every $k \leq N$,*

$$\zeta_{G_p | \Psi_p(x)}(s) = \sum_{\ell \in (\mathcal{T}_{k+1})_x(\mathbb{M}_p)} R_k(\ell) \cdot \zeta_{S_k^{\mathrm{rep}}(\ell) | \Psi_k(\ell)}(s).$$

Proof. Fix p and $x \in \mathscr{X}$. We prove the lemma by induction on k. The case $k = 0$ is trivial.

Suppose we know the claim for $k-1$. Let $\ell \in (\mathcal{T}_k)_x(\mathbb{M}_p)$. The representation $\Psi_{k-1}(\ell)$ is a representation of $\exp(L(v_{k-1}))$, and its stabilizer in $S_{k-1}^{\mathrm{rep}}(\ell)$ is just $S_k^{\mathrm{rep}}(\ell)$. The maximal normal pro-p subgroup of $S_k^{\mathrm{rep}}(\ell)$ is, by the construction, $\exp(L(v_k))$. From Lemma 5.3, we have that

$$\begin{aligned} &\sum_{\ell \in (\mathcal{T}_k)_x(\mathbb{M}_p)} R_{k-1}(\ell) \zeta_{S_{k-1}^{\mathrm{rep}}(\ell) | \Psi_{k-1}(\ell)}(s) \\ &\qquad = \sum_{\ell \in (\mathcal{T}_k)_x(\mathbb{M}_p)} R_{k-1}(\ell) \sum_{\tau \in \mathrm{Irr}(\exp(v_k) | \Psi_{k-1}(\ell))} \frac{[S_{k-1}^{\mathrm{rep}}(\ell) : S_k^{\mathrm{rep}}(\ell)]^{-s}}{|\tau^{S_k^{\mathrm{rep}}(\ell)}|} \\ &\qquad\quad \cdot \left(\frac{\dim \tau}{\dim \Psi_{k-1}(\ell)} \right)^{-s} \cdot \zeta_{S_k^{\mathrm{rep}}(\ell) | \tau}(s). \end{aligned}$$

For every $\ell \in \mathcal{T}_k(\mathbb{M}_p)$, the map $\Psi_k : (\mathcal{T}_{k+1})_\ell(\mathbb{M}_p) \to \mathrm{Irr}(\exp(L(v_k)) | \Psi_{k-1}(\ell))$ is onto. Hence, by Lemma 5.14,

$$\begin{aligned} &= \sum_{\ell \in (\mathcal{T}_k)_x(\mathbb{M}_p)} \sum_{\mathfrak{f} \in (\mathcal{T}_{k+1})_\ell(\mathbb{M}_p)} R_{k-1}(\ell) \\ &\cdot \frac{[S_{k-1}^{\mathrm{rep}}(\ell) : S_k^{\mathrm{rep}}(\ell)]^{-s}}{|\Psi_k(\mathfrak{f})^{S_k^{\mathrm{rep}}(\ell)}| \cdot |\Psi_k^{-1}(\Psi_k(\mathfrak{f})) \cap (\mathcal{T}_{k+1})_\ell(\mathbb{M}_p)|} \left(\frac{\dim \Psi_k(\mathfrak{f})}{\dim \Psi_{k-1}(\ell)} \right)^{-s} \cdot \zeta_{S_k^{\mathrm{rep}}(\ell) | \Psi_k(\mathfrak{f})}(s). \end{aligned}$$

By definition, $S_k^{\mathrm{rep}}(\ell) = S_k^{\mathrm{rep}}(\mathfrak{f})$. By Theorem 3.7, $|\Psi_k^{-1}(\Psi_k(\mathfrak{f})) \cap (\mathcal{T}_{k+1})_\ell(\mathbb{M}_p)|$ is equal to the size of the orbit of $\mathfrak{f}$ under $\exp(L(v_k)) \cap S_{k-1}^{\mathrm{char}}(\ell)$, which is just $W_k(\mathfrak{f})$. Finally, the stabilizer of $\Psi_k(\mathfrak{f})$ in $S_k^{\mathrm{rep}}(\ell)$ is equal to $S_k^{\mathrm{char}}(\ell) \cdot \exp(L(v_k))$, and therefore $|\Psi_k(\mathfrak{f})^{S_k^{\mathrm{rep}}(\ell)}| = [S_k^{\mathrm{rep}}(\ell) : S_k^{\mathrm{char}} \cdot \exp(L(v_k))]$. Finally, since

$$R_k(\mathfrak{f}) = \frac{[S_{k-1}^{\mathrm{rep}}(\mathfrak{f}) : S_k^{\mathrm{rep}}(\mathfrak{f})]^{-s}}{[S_{k-1}^{\mathrm{rep}}(\ell) : S_{k-1}^{\mathrm{char}}(\ell) \cdot \exp(L(v_k))] \cdot W_k(\mathfrak{f})} \cdot \left(\frac{\dim \Psi_k(\mathfrak{f})}{\dim \Psi_{k-1}(\mathfrak{f})} \right)^{-s},$$

the inductive claim follows. □

By Proposition 4.16 and Lemma 4.9 there is a definable partition of $\mathcal{T}_N$ into sets $\mathcal{T}_N^1,\dots,\mathcal{T}_N^M$, and for each part there is a root datum $\mathcal{D}^i$ such that for each prime p and for each $\ell\in\mathcal{T}_N^i(\mathbb{M}_p)$, the group $(S^{\mathrm{rep}}_{(x,v_N,\theta_N)}(\ell))^+/\exp(L(v_N))$ is isomorphic to $H_{\mathcal{D}^i}(\mathbb{F}_p)$. By Lemma 5.4 we get that there is a constant c such that

$$c^{-1}\cdot\zeta_{S_N^{\mathrm{rep}}(\ell)|\Psi_N(\ell)}(s)<\zeta_{H_{\mathcal{D}}(\mathbb{F}_p)}(s)[S_N^{\mathrm{rep}}(\ell):(S_N^{\mathrm{rep}}(\ell))^+]<c\cdot\zeta_{S_N^{\mathrm{rep}}(\ell)|\Psi_N(\ell)}(s).$$

By Proposition 4.17 there is a V-function $\mathcal{G}$ with domain $\mathcal{T}_N$ and a constant c such that for every p and every $\ell\in\mathcal{T}_N(\mathbb{M}_p)$,

$$c^{-1}\mathcal{G}^{\mathbb{M}_p}(\ell)<[S_N^{\mathrm{rep}}(\ell):(S_N^{\mathrm{rep}}(\ell))^+]<c\mathcal{G}^{\mathbb{M}_p}(\ell).$$

Together with Proposition 3.17 and Proposition 4.17, we get that there is a V-function $\mathcal{F}_{\mathcal{D}}$ on $\mathcal{T}_N$ such that for all p's large enough,

$$\zeta_{S_N^{\mathrm{rep}}(\ell)|\Psi_N(\ell)}(s)\sim\mathcal{F}_{\mathcal{D}}^{\mathbb{M}_p}(s).\tag{5.2}$$

By Lemmas 3.2 and 5.14 we get that

$$\begin{aligned}\zeta_{G_p}(s)&=\sum_{\rho\in\mathrm{Irr}(G_p^1)}\frac{1}{[G_p:\mathrm{Stab}_{G_p}\rho]}(\dim\rho)^{-s}\cdot\zeta_{G_p|\rho}(s)\\&=\int_{x\in\mathscr{X}}\frac{1}{\lambda(\Psi_p^{-1}(\Psi_p(x)))}\cdot\frac{1}{[G_p:\mathrm{Stab}_{G_p}\Psi_p(x)]}(\dim\Psi_p(x))^{-s}\cdot\zeta_{G_p|\Psi_p(x)}(s)dx,\end{aligned}$$

and by Lemma 5.13 and Theorem 5.2,

$$\begin{aligned}&=\int_{x\in\mathscr{X}}p^{\phi_1(x)+s\phi_2(x)}\cdot\frac{1}{[G_p:\mathrm{Stab}_{G_p}\Psi_p(x)]}\cdot\sum_{\ell\in(\mathcal{T}_{N+1})_x(\mathbb{M}_p)}R(\ell)\cdot\zeta_{S_N^{\mathrm{rep}}(\ell)|\Psi_N(\ell)}(s)\\&=\int_{\ell\in\mathcal{T}_{N+1}(\mathbb{M}_p)}p^{\phi_1(\pi(\ell))+s\phi_2(\pi(\ell))}\cdot\frac{1}{[G_p:\mathrm{Stab}_{G_p}\Psi_p(x)]}\cdot R(\ell)\cdot\zeta_{S_N^{\mathrm{rep}}(\ell)|\Psi_N(\ell)}(s).\end{aligned}$$

There is a V-function $\mathcal{F}_{stab}$ with domain $\mathcal{T}_N$ and a constant c such that for all primes p and all $\ell=(x,v,\theta)\in\mathcal{T}_{N+1}(\mathbb{M}_p)$,

$$c^{-1}\mathcal{F}_{stab}^{\mathbb{M}_p}(\ell)<\frac{1}{[G_p:\mathrm{Stab}_{G_p}\Psi_p(x)]}=\frac{[\mathrm{Stab}_{G_p}\Psi_p(x):G_p^1]}{[G_p:G_p^1]}<c\mathcal{F}_{stab}^{\mathbb{M}_p}(\ell).\tag{5.3}$$

Similarly, using Proposition 4.17, there is a V-function $\mathcal{F}_R$ with domain $\mathcal{T}_{N+1}$ such that for all p and $\ell\in\mathcal{T}_{N+1}(\mathbb{M}_p)$,

$$c^{-1}\mathcal{F}_R^{\mathbb{M}_p}(\ell)<R(\ell)<c\mathcal{F}_R^{\mathbb{M}_p}(\ell).\tag{5.4}$$

By (5.2), (5.3), and (5.4), we get that

$$\zeta_{G_p}(s)\sim\int_{\ell\in\mathcal{T}_{N+1}(\mathbb{M}_p)}p^{\phi_1(\pi(\ell))+s\phi_2(\pi(\ell))}\cdot\mathcal{F}_{\mathrm{Stab}}^{\mathbb{M}_p}(\ell)\cdot\mathcal{F}_R^{\mathbb{M}_p}(\ell)\cdot\mathcal{F}_D^{\mathbb{M}_p}(\ell),$$

which proves Theorem 5.1.

Lemma 5.14. (1) *Let A, B be finite sets, let $\phi : A \to B$ be an onto function, and let $f : B \to \mathbb{C}$ be any function. Denote the composition of f and ϕ by g. Then*

$$\sum_{b\in B} f(b) = \sum_{a\in A} \frac{1}{|\phi^{-1}(\phi(a))|} g(a).$$

(2) *Let (A, μ) be a probability space, let B be a countable set, let $\phi : A \to B$ be a measurable function, and let $f : B \to \mathbb{C}$ be any bounded function. Denote the composition of f and ϕ by g. Then*

$$\sum_{b\in B} f(b) = \int_{a\in A} \frac{1}{\mu(\phi^{-1}(\phi(a)))} g(a)da.$$

6. Uniformity of the local factors II

6.1. *Motivic integration.*

Definition 6.1. An R-function is a pair (V, W) of definable sets in the language of rings such that $W \subset V \times \mathbb{A}^n$. If $f = (V, W)$ is a function of type (B) and p is a prime, we set

$$f_p(s) = \sum_{a\in V(\mathbb{F}_p)} |W_a(\mathbb{F}_p)|^{-s}.$$

Theorem 6.2. *Let $\mathcal{F}$ be a bounded V-function with domain X. Then there are integer constants A_i, B_i, and R-functions f_i, such that for all but finitely many primes p,*

$$\int_{X(\mathbb{M}_p)} \mathcal{F}_p(x, s)dx = \sum_i (f_i)_p(s) \cdot \prod_j \frac{p^{A_j s + B_j}}{1 - p^{A_j s + B_j}}.$$

Proof. It is enough to prove the theorem for V-functions that consist of only one triple $(X, f, \mathcal{V})$, where $X \subset \{(x_1, \dots, x_n) \in \mathbb{A}_V^n \mid \mathrm{val}(x_i) \geq 0\}$ is a definable set, $f : X \to \mathbb{A}_O$ is a definable function such that $f(x) \geq 0$, and $\mathcal{V} \subset \mathbb{A}_V^n \times \mathbb{A}_R^m$ is a definable set. By 4.12, 4.15, and 4.16 we can assume that there are integral polynomials $P_1(x), \dots, P_r(x), Q_1(x), Q_2(x)$, a formula $\varphi(\omega_1, \dots, \omega_r)$ in the language of fields, a formula $\psi(\gamma_1, \dots \gamma_r)$ in the language of ordered groups, a formula $\xi(x_1, \dots, x_r, \omega_1, \dots, \omega_m)$ in the language of fields, and an integer e such that

(1) X is the set defined by the formula

$$\varphi(\mathrm{ac}(P_1(x)), \dots, \mathrm{ac}(P_r(x))) \wedge \psi(\mathrm{val}(P_1(x)), \dots, \mathrm{val}(P_r(x)));$$

(2) $f(x) = \frac{1}{e}(\mathrm{val}(Q_1(x)) - \mathrm{val}(Q_2(x)))$;

(3) $\mathcal{V}$ is the set defined by the formula

$$\xi(\mathrm{ac}(P_1(x)), \dots, \mathrm{ac}(P_r(x)), \omega_1, \dots, \omega_m).$$

Let $(Y_{\mathbb{Q}}, h_{\mathbb{Q}})$ be a resolution of singularities (see §3.8) for the polynomial $\prod_i P_i(x) \cdot Q_1(x) \cdot Q_2(x)$. Note that $Y_{\mathbb{Q}}$ has dimension n. We denote the irreducible components of $h^{-1}(D)$ by E_i, and denote the closure of $Y_{\mathbb{Q}}$ inside $\mathbb{P}^m_{\mathbb{A}^n_{\mathbb{Z}}}$ by $Y_{\mathbb{Z}}$. For any i, denote the multiplicity of $(E_i)_{\mathrm{red}}$ inside $h^{-1}(D)$ by N_i, and denote the multiplicity of $(E_i)_{\mathrm{red}}$ inside the divisor $h^*(dx_1 \wedge \cdots \wedge dx_n)$ by $\nu_i - 1$.

Let Σ be the finite set of primes p such that $(Y_{\mathbb{Q}}, h_{\mathbb{Q}})$ does not have a good reduction modulo p. For every $p \notin \Sigma$ and for every closed point $\overline{a}$ of $Y_{\mathbb{F}_p}$ (which we identify with the subscheme of $Y_{\mathbb{Z}}$ lying above $\mathrm{Spec}(\mathbb{F}_p)$) there is a natural number d, an open neighborhood U, regular functions $u, y_1, \ldots, y_n$, and natural numbers $N_1, \ldots, N_d$, such that

(1) y_i form a system of parameters for $Y_{\mathbb{Z}}$ in U;
(2) y_i is a local equation for one of the divisors E_{n_i} in U for $i \leq d$;
(3) u is invertible in U;
(4) $(\prod P_i \cdot Q_1 \cdot Q_2) \circ h = u y_1^{N_1} \cdots y_d^{N_d}$;
(5) U is irreducible and smooth.

By (1), (4), and (5), there are natural numbers $N_{i,j}, M_{k,j}$, $i = 1, \ldots, r$, $j = 1, \ldots, d$ and $k = 1, 2$ and regular functions u_i, v_k that are invertible on U such that

$$P_i \circ h = u_i \prod y_j^{N_{i,j}}$$

and

$$Q_k \circ h = v_k \prod y_j^{M_{k,j}}.$$

By compactness, there are finite number of such neighborhoods that cover $Y_{\mathbb{Z}_\Sigma} = Y_{\mathbb{Z}} \times \mathrm{Spec}\, \mathbb{Z}_\Sigma$[8]. Denote them by $U_1, \ldots, U_l$. Let $U_i' = U_i \setminus \cup_{j<i} U_j$. We consider U_j' as definable sets.

Let p be a prime that is not contained in Σ, and fix $i \in \{1, \ldots, l\}$. For every $\overline{a} \in U_i'(\mathbb{F}_p)$ and for every $z \in Y(\mathbb{Q}_p)$ such that $\mathrm{ac}(z) = \overline{a}$, we have

$$P_i \circ h(z) = u_i(z) \prod y_j^{N_{i,j}}(z)$$

and similarly

$$Q_k \circ h(z) = v_k(z) \prod y_j^{M_{k,j}}(z).$$

The functions u_i are regular and nonvanishing. For almost all primes p we have that $\mathrm{val}\left(\frac{du_i}{dz_j}\right) \geq 0$. Therefore the angular component of $u_i(z)$ depends only on the reduction of z: $\mathrm{ac}(u_i(z)) = \overline{u_i}(\mathrm{ac}(z))$. It follows that $h^{-1}(X)$ can be decomposed into definable sets defined by formulas of the form

$$\varphi'(\mathrm{ac}(z), \mathrm{ac}(y_i(z))) \wedge \psi(\mathrm{val}(y_i(z))),$$

[8] $Y_{\mathbb{Z}_\Sigma}$ is the part of $Y_{\mathbb{Z}}$ that lies over the primes not in Σ.

where φ' is a formula in the language of fields and ψ is a formula in the language of ordered groups. Also, we have that in each piece,

$$f \circ h(z) = \frac{1}{e} \sum (M_{1,i} - M_{2,i}) \operatorname{val}(y_i(z))$$

and

$$|h^*(dx_1 \wedge \cdots \wedge dx_n)| = \prod |y_i|^{\nu_i - 1} |dy_1 \wedge \cdots \wedge dy_n|.$$

For a set X, let 1_X be the characteristic function of X. Similarly, for a formula $\eta(t)$, let 1_η be the characteristic function of the set $\{t \mid \eta(t)\}$. By the chain rule, we have

$$\begin{aligned}\int_{\mathbb{Q}_p^n} & 1_X(x) p^{-sf(x)} |\mathcal{V}(\mathbb{F}_p)_x|^{-s} \\ &= \int_{z \in Y(\mathbb{Q}_p)} 1_{h^{-1}(X)}(z) p^{-sf \circ h(z)} |\mathcal{V}(\mathbb{F}_p)_{h(z)}|^{-s} |h^*(dx_1 \wedge \cdots \wedge dx_n)|.\end{aligned}$$

Decomposing the domain of integration according to the angular component of z, the integral is equal to

$$\begin{aligned}\sum_i \sum_{\overline{a} \in U_i'(\mathbb{F}_p)} & \int_{z \in Y(\mathbb{Q}_p) \wedge \operatorname{ac}(z) = \overline{a}} 1_{\phi(\overline{a}, \operatorname{ac}(y_i(-)))}(z) \\ & \cdot 1_{\psi(\operatorname{val}(y_i(-)))}(z) p^{\sum(-\frac{s}{e}(M_{1,i} - M_{2,i}) + \nu_i - 1) \operatorname{val}(y_i(z))} |\mathcal{V}(\mathbb{F}_p)_{h(z)}|^{-s}.\end{aligned}$$

For every $\overline{a}$, The map $(y_i) : \{z \in Y(\mathbb{Q}_p) \mid \operatorname{ac}(z) = \overline{a}\} \to (p\mathbb{Z}_p)^n$ is a measure preserving bijection. Therefore the above sum equals

$$\sum_i \frac{1}{p^{2n}} \left(\sum_{(\overline{a}, \overline{b}) \in V_i(\mathbb{F}_p)} |W_i(\mathbb{F}_p)_{(\overline{a}, \overline{b})}|^{-s} \right) \left(\sum_{\gamma \in C} p^{-s(\overline{n} \cdot \gamma) + (\overline{m} \cdot \gamma)} \right). \tag{6.1}$$

Where $V \subset U_i' \times \mathbb{A}_R^n$ is defined by the formula

$$(x, y) \in V \iff x \in U_i' \wedge \phi(x, y),$$

$W \subset V \times \mathbb{A}_R^m$ is defined by the formula

$$(x, y, z) \in W \iff (x, y) \in U_i' \wedge \xi(\overline{u}(x) \cdot \prod y_j^{N_{i,j}}, z),$$

$C \subset \mathbb{A}_O^n$ is defined by the formula

$$\gamma \in C \iff \psi(\gamma) \wedge \bigwedge \gamma_i > 0,$$

and the functionals $\overline{n}, \overline{m}$ are defined by

$$\overline{n}_i = (M_{1,i} - M_{2,i})/e, \quad \overline{m}_i = \nu_i - 1.$$

For every i, the first sum in (6.1) is an R-function, which we shall denote by g_i. By elimination of quantifiers for the value group (Theorem 4.13), C can be decomposed into sets defined by conditions of the form

$$\phi(x) \geq 0 \wedge \psi(x) \text{ is divisible by } N,$$

where $\phi(x), \psi(x)$ are affine functionals. After a further decomposition, we can assume each of these sets to be intersection of a cone and a coset of $N\mathbb{Z}^n$ for some fixed N. It is well known that it is possible to further divide these sets and get that each set is of the form

$$\{n_1 v_1 + \cdots + n_k v_k \mid n_1, \ldots, n_k \in \mathbb{N}\}$$

for some vectors $v_1, \ldots, v_k$ (this fact is used in the desingularization theorem for Toric varieties; see [7, §2.6]). On each cone we have to sum a geometric series, so the sum is of the form

$$\prod_j \frac{p^{A_j s + B_j}}{1 - p^{A_j s + B_j}},$$

and so for every $p \notin \Sigma$,

$$\int_{X(\mathbb{M}_p)} \mathcal{F}_p(x, s) dx = \sum_i (g_i)_p(s) \prod_j \frac{p^{A_{i,j} s + B_{i,j}}}{1 - p^{A_{i,j} s + B_{i,j}}}.$$

If $p \in \Sigma$, we can resolve the singularities of $\prod_i P_i(x) \cdot Q_1(x) \cdot Q_2(x)$ in $\mathbb{Q}_p[x]$. By similar arguments to the above, we get that there are integers $n_i, m_i, C_{i,j}, D_{i,j}$ such that

$$\int_{X(\mathbb{M}_p)} \mathcal{F}_p(x, s) dx = \sum_i n_i (m_i)^{-s} \prod_j \frac{p^{C_{i,j} s + D_{i,j}}}{1 - p^{C_{i,j} s + D_{i,j}}}.$$

Arguing as in the proof of Theorem 5.1, we can find R-functions f_i and integers $A_{i,j}, B_{i,j}$ such that for all p,

$$\int_{X(\mathbb{M}_p)} \mathcal{F}_p(x, s) dx = \sum_i (f_i)_p(s) \prod_j \frac{p^{A_{i,j} s + B_{i,j}}}{1 - p^{A_{i,j} s + B_{i,j}}}. \qquad \square$$

Remark 6.3. Instead of using resolution of singularities, it is possible to prove Theorem 6.2 using the methods of [3] or [9].

6.2. *Proof of Theorem* 1.2.

THEOREM 6.4. *There is a partition of the set of primes into finitely many Artin sets, and for each Artin set the following is true: There is a finite set I, and for each $i \in I$ there are nonnegative integers, d_i and e_i, and two finite sequences of nonnegative integers, $A_{i,j}$ and $B_{i,j}$, such that the sequence of the functions $\zeta_{G_p}(s) - 1$ is equivalent to the sequence of the functions*

$$s \mapsto \sum_{i \in I} p^{d_i - e_i s} \cdot \prod_j \frac{p^{-A_{i,j} s + B_{i,j}}}{1 - p^{-A_{i,j} s + B_{i,j}}}.$$

Moreover, $e_i + \sum_j A_{i,j} > 0$ for every i.

Proof. By Theorems 5.1 and 6.2, there is a V-function $\mathcal{F}$ and R-functions f_j such that

$$\zeta_{G_p}(s) - 1 \sim \int_{X(\mathbb{M}_p)} \mathcal{F}_p(x,s)dx = \sum_j (f_j)_p(s) \cdot \prod_k \frac{p^{A_{j,k}s+B_{j,k}}}{1-p^{A_{j,k}s+B_{j,k}}}. \tag{6.2}$$

Let $f = (V, W)$ be an R-function. By Corollary 4.7, there is a constant c, a partition of the primes into Artin sets $\mathcal{P}_i$, and for each i a finite set $D_i \subset \mathbb{N} \times \mathbb{Q}_{>0}$, such that for all $p \in \mathcal{P}_i$ and $a \in V(\mathbb{F}_p)$,

$$\Big| |W_a(\mathbb{F}_p)| - \mu p^d \Big| < cp^{d-\frac{1}{2}} \tag{6.3}$$

for some $(d, \mu) \in D_i$. Moreover, if we denote by $L_{d,\mu,p}$ the set of elements a in $V(\mathbb{F}_p)$ such that (6.3) holds, then

$$||L_{d,\mu,p}| - \nu p^e| < cp^{e-\frac{1}{2}}$$

for some $e = e(d, \mu) \in \mathbb{N}$ and $\nu = \nu(e, \mu) \in \mathbb{Q}_{>0}$.

For every $p \in \mathcal{P}_i$,

$$\begin{aligned} f_p(s) &= \sum_{a \in V(\mathbb{F}_p)} |W_a(\mathbb{F}_p)|^{-s} = \sum_{(d,\mu)\in D_i} \sum_{a \in L_{(d,\mu,p)}} |W_a(\mathbb{F}_p)|^{-s} \\ &\sim \sum_{(d,\mu)\in D_i} \nu(d,\mu) \cdot p^{e(d,\mu)} \cdot \left(\mu \cdot p^d\right)^{-s} \sim \sum_{(d,\mu)\in D_i} p^{e(d,\mu)-ds} \end{aligned}$$

which together with (6.2) implies the theorem. □

We can finally prove Theorem 1.2.

Proof of Theorem 1.2. Recall from Section 2 that there is a finite index subgroup $\Delta \subset \Gamma$, such that the pro-algebraic completion of Δ has finite index in the group

$$\prod_{p \notin \Sigma} \underline{G}(\mathbb{Z}_p) \times \underline{G}(\mathbb{C}).$$

By Corollary 3.4, it suffices to prove that the abscissa of convergence of the Dirichlet series

$$\prod_{p \notin \Sigma} \zeta_{G_p}(s) \cdot \zeta_{\underline{G}(\mathbb{C})}(s)$$

is rational.

By Theorem 6.4, there is a partition of the set of primes into finitely many Artin sets $\mathcal{A}_1, \ldots, \mathcal{A}_n$, and for each $\mathcal{A}_i$ there are constants $d_i, e_i, A_{i,j}, B_{i,j}$, such that for $p \in \mathcal{A}_i$,

$$\zeta_{G_p}(s) - 1 \sim \sum_{i \in I} p^{d_i - e_i s} \cdot \prod_j \frac{p^{-A_{i,j}s+B_{i,j}}}{1-p^{-A_{i,j}s+B_{i,j}}}.$$

Since the abscissa of convergence of a product of two Dirichlet series is the maximum of the abscissae of convergence of the two series, it is enough to show that the abscissae of convergence of

(1) $\zeta_{\underline{G}(\mathbb{C})}(s)$, and
(2) $\prod_{p\in\mathcal{A}_i}\zeta_{G_p}(s)$ for $i=1,\ldots,n$

are rational. As noted in Section 2, the abscissa of convergence of $\zeta_{\underline{G}(\mathbb{C})}(s)$ is rational. By Theorem 2.1, the abscissa of convergence of each $\zeta_{G_p}(s)$ is rational. Thus, if $\mathcal{A}_i$ is finite, then the abscissa of convergence of $\prod_{p\in\mathcal{A}_i}\zeta_{G_p}(s)$ is rational. We can assume that $\mathcal{A}_i$ is infinite and hence has positive analytic density. By Lemma 3.19, it is enough to show that the abscissa of convergence of the product

$$\prod_{p\in\mathcal{A}}\left(1+p^{d-es}\cdot\prod_j\frac{p^{-A_js+B_j}}{1-p^{-A_js+B_j}}\right) \tag{6.4}$$

is rational for all subsets $\mathcal{A}$ of primes with positive density and nonnegative integers d,e,A_j,B_j. We shall show that the abscissa of convergence of this product is

$$\max\left\{\frac{\sum_j B_j+d_i+1}{e_i+\sum_j A_j},\frac{B_j}{A_j}\right\}.$$

Every factor in the product has a pole at $s=\frac{B_j}{A_j}$, so the abscissa of convergence is greater than the maximum of those expressions. If

$$s>\max\left\{\frac{B_j}{A_j}\right\},$$

then there is a constant $D>0$ such that for all $p\in\mathcal{A}$, $1-p^{-A_js+B_j}>D$. Therefore

$$\begin{aligned}p^{\left(\sum_j -A_j-e_i\right)s+\sum_j B_j+d_j}&<p^{d_i}p^{-se_i}\cdot\prod_j\frac{p^{-A_js+B_j}}{1-p^{-A_js+B_j}}\\&<\frac{1}{D^m}p^{\left(\sum_j -A_j-e_i\right)s+\sum_j B_j+d_j},\end{aligned}$$

and we see that if

$$\left(\sum_j -A_j-e_i\right)s+\sum_j B_j+d_j<-1,$$

then the product (6.4) is greater than the product $\prod_{p\in\mathcal{A}}(1+\frac{1}{p})$ which diverges, since $\mathcal{A}$ has positive analytic density.

Similarly, by comparing the product to the (convergent) product $\prod_{p\in\mathcal{A}} \cdot(1+\frac{1}{p^{1+\epsilon}})$, we see that if

$$s > \frac{\sum_j B_j + d_i + 1}{e_i + \sum_j A_j},$$

then the product (6.4) converges. □

References

[1] N. Avni, B. Klopsch, U. Onn, and C. Voll, Representation zeta functions of compact p-adic analytic groups and arithmetic groups, preprint. Available at http://arxiv.org/abs/1007.2900.

[2] Z. Chatzidakis, Notes on the model theory of finite and pseudo-finite fields. Available at http://www.logique.jussieu.fr/~zoe/index.html.

[3] R. Cluckers and F. Loeser, Constructible motivic functions and motivic integration, *Invent. Math.* **173** (2008), 23–121. MR 2403394. Zbl 1179.14011. http://dx.doi.org/10.1007/s00222-008-0114-1.

[4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Oxford University Press, Eynsham, 1985. MR 0827219. Zbl 0568.20001.

[5] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type*, *London Math. Soc. Student Texts*, Cambridge Univ. Press, Cambridge, 1991. MR 1118841. Zbl 0815.20014.

[6] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic Pro-p Groups*, second ed., *Cambridge Stud. Adv. Math.* **61**, Cambridge Univ. Press, Cambridge, 1999. MR 1720368. Zbl 0934.20001. http://dx.doi.org/10.1017/CBO9780511470882.

[7] W. Fulton, *Introduction to Toric Varieties. The William H. Roever Lectures in Geometry*, *Ann. of Math. Stud.* **131**, Princeton Univ. Press, Princeton, NJ, 1993. MR 1234037. Zbl 0813.14039.

[8] R. E. Howe, Kirillov theory for compact p-adic groups, *Pacific J. Math.* **73** (1977), 365–381. MR 0579176. Zbl 0385.22007. Available at http://projecteuclid.org/getRecord?id=euclid.pjm/1102810616.

[9] E. Hrushovski and D. Kazhdan, Integration in valued fields, in *Algebraic Geometry and Number Theory*, *Progr. Math.* **253**, Birkhäuser, Boston, MA, 2006, pp. 261–405. MR 2263194. Zbl 1136.03025. http://dx.doi.org/10.1007/978-0-8176-4532-8_4.

[10] E. Hrushovski and A. Pillay, Definable subgroups of algebraic groups over finite fields, *J. Reine Angew. Math.* **462** (1995), 69–91. MR 1329903. Zbl 0823.12005.

[11] I. M. Isaacs, *Character Theory of Finite Groups*, **69**, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976, Pure Appl. Math. MR 0460423. Zbl 0337.20005.

[12] A. Jaikin-Zapirain, Zeta function of representations of compact p-adic analytic groups, *J. Amer. Math. Soc.* **19** (2006), 91–118. MR 2169043. Zbl 1092.20023. http://dx.doi.org/10.1090/S0894-0347-05-00501-1.

[13] D. Kazhdan, An algebraic integration, in *Mathematics: Frontiers and Perspectives*, Amer. Math. Soc., Providence, RI, 2000, pp. 93–115. MR 1754770. Zbl 0976.20030.

[14] M. Larsen and A. Lubotzky, Representation growth of linear groups, *J. Eur. Math. Soc.* (*JEMS*) **10** (2008), 351–390. MR 2390327. Zbl 1142.22006. http://dx.doi.org/10.4171/JEMS/113.

[15] M. Larsen and R. Pink, Finite subgroups of algebraic groups, preprint. Available at http://www.math.ethz.ch/~pink/ftp/LP5.pdf.

[16] M. W. Liebeck and A. Shalev, Character degrees and random walks in finite groups of Lie type, *Proc. London Math. Soc.* **90** (2005), 61–86. MR 2107038. Zbl 1077.20020. http://dx.doi.org/10.1112/S0024611504014935.

[17] A. Lubotzky and B. Martin, Polynomial representation growth and the congruence subgroup problem, *Israel J. Math.* **144** (2004), 293–316. MR 2121543. Zbl 1134.20056. http://dx.doi.org/10.1007/BF02916715.

[18] M. V. Nori, On subgroups of $\mathrm{GL}_n(\mathbf{F}_p)$, *Invent. Math.* **88** (1987), 257–275. MR 0880952. Zbl 0632.20030. http://dx.doi.org/10.1007/BF01388909.

[19] J. Pas, Uniform p-adic cell decomposition and local zeta functions, *J. Reine Angew. Math.* **399** (1989), 137–172. MR 1004136. Zbl 0666.12014. http://dx.doi.org/10.1515/crll.1989.399.137.

[20] M. S. Raghunathan, The congruence subgroup problem, *Proc. Indian Acad. Sci. Math. Sci.* **114** (2004), 299–308. MR 2067695. Zbl 1086.20024. http://dx.doi.org/10.1007/BF02829437.

[21] P. Sarnak and S. Adams, Betti numbers of congruence groups, *Israel J. Math.* **88** (1994), 31–72, with an appendix by Ze'ev Rudnick. MR 1303490. Zbl 0843.11027. http://dx.doi.org/10.1007/BF02937506.

[22] M. du Sautoy and F. Grunewald, Analytic properties of zeta functions and subgroup growth, *Ann. of Math.* **152** (2000), 793–833. MR 1815702. Zbl 1006.11051. http://dx.doi.org/10.2307/2661355.

(Received: March 9, 2008)

The Hebrew University of Jerusalem, Jerusalem, Israel
E-mail: avni.nir@gmail.com