Higher rank arithmetic lattices have bounded representation growth

Avraham Aizenbud, Nir Avni

December 24, 2014

Abstract

If $\Gamma$ is an arithmetic lattice whose $\mathbb{Q}$-rank is greater than one, let $r_n(\Gamma)$ be the number of irreducible $n$-dimensional representations of $\Gamma$ up to isomorphism. We find a constant $C$ such that $r_n(\Gamma) = O(n^C)$ for every such $\Gamma$. We also prove similar results for lattices in positive characteristic.

Contents

1 Introduction 2
   1.1 Main results ......................................................... 2
   1.2 Ideas of the proof of Theorem D ................................. 5
   1.3 Structure of the paper ........................................... 5
   1.4 Acknowledgements ................................................. 6

2 Preliminaries 6
   2.1 Singularities ....................................................... 6
   2.2 Jet schemes and Mustata’s theorem ............................... 7
   2.3 Rational singularities and representation growth ................ 8
   2.4 Definable Integrals ................................................. 9
   2.5 Representation zeta functions as quantifier-free definable integrals .......... 12

3 Uniform bounds on local zeta functions 13
   3.1 The main estimate .................................................. 13
   3.2 $\zeta_{G(F_q[t]/t^m)}(2n)$ tends to 1 .............................. 13
   3.3 $\zeta_{G(\mathbb{Z}_q)}(2n)$ tends to 1 ............................... 14
   3.4 Proof of Theorem 3.1.1 ........................................... 19
1 Introduction

1.1 Main results

For a topological group $\Gamma$, let $r_n(\Gamma)$ be the number of isomorphism classes of irreducible, $n$-dimensional, complex, continuous representations of $\Gamma$. The sequence $r_n(\Gamma)$ is called the representation growth sequence of $\Gamma$. In general, $r_n(\Gamma)$ can be infinite, but we will only consider groups for which $r_n(\Gamma)$ is finite for any $n$.

The study of the representation growth sequence was introduced at [9], and [13]. For more recent results, we refer the reader to [1], [2], [3], [11], [12], and the references therein. In this paper, we study the asymptotics of the representation growth sequences of arithmetic groups.

Throughout this paper, we fix an affine group scheme $G$ over $\mathbb{Z}$ whose generic fiber $G_\mathbb{Q} = G \times_{\text{Spec} \mathbb{Z}} \text{Spec} \mathbb{Q}$ is $\mathbb{Q}$-simple, connected, and simply connected. In addition, fix an embedding $G \hookrightarrow \text{GL}_N$. We will study the representation growth of the groups $\Gamma = G(O)$, where $O$ is the ring of integers of a global field (perhaps localized by finitely many places).

An important example is $\text{SL}_d(\mathbb{Z})$. The main theorem of [13] implies that, if the $\mathbb{Q}$-rank of $G_\mathbb{Q}$ is greater than one, then the sequence $r_n(G(O))$ is bounded by some polynomial in $n$.

In order to catch the rate of polynomial growth of $r_n(G(O))$, we introduce the following definition:

**Definition.** Let $\Gamma$ be a topological group, and assume that the sequence $r_n(\Gamma)$ is bounded by a polynomial. The representation zeta function of $\Gamma$ is the Dirichlet series

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

The maximal domain of absolute convergence of the series (1) is a half plane of the form $\{ \Re(s) > \alpha(\Gamma) \}$. The real number $\alpha(\Gamma)$ is called the abscissa of convergence of $\zeta_\Gamma$ or of $\Gamma$. 2
The relation between $\alpha(\Gamma)$ and the growth rate of $r_n(\Gamma)$ is the following:

$$
\alpha(\Gamma) = \limsup_{n \to \infty} \frac{\log (r_1(\Gamma) + \cdots + r_n(\Gamma))}{\log n}.
$$

If $\Gamma = G(O)$ as above, the lim sup in (2) is actually a limit and is a rational number (see [2]).

Our results are formulated using the following notation:

**Notation.** Let $\mathfrak{g}$ be a simple factor of the Lie algebra of $G_{\mathbb{Q}}$ (note that they are all isomorphic). Denote

$$
B(G) = \begin{cases}
22 & \mathfrak{g} = \mathfrak{sl}_d \text{ or } \mathfrak{so}_d \\
40 & \mathfrak{g} = \mathfrak{sp}_{2d} \\
3\dim(\mathfrak{g}) + 1 & \text{if } \mathfrak{g} \text{ is exceptional}
\end{cases}
$$

Denote also $C(G) = \lceil \frac{B(G) + 2}{2} \rceil$.

Note that $B(G)$ is bounded by 745 for any $G$.

**Notation.** Let $k$ be a global field and $T$ be a finite set of places containing all archimedean ones. We denote by $O_{k,T}$ the ring $T$-integers

$$
O_{k,T} = \{ x \in k \mid \forall v \notin T \text{ we have } \|x\|_v \leq 1 \}.
$$

Our first result is the following:

**Theorem A.** Assume that the $\mathbb{Q}$-rank of $G_{\mathbb{Q}}$ is greater than one. There is a constant $C$ such that, if $k$ is a global field of characteristic greater than $C$ and $T$ is a finite set of places of $k$ containing all archimedean ones, then $\alpha(G(O_{k,T})) \leq B(G)$.

In fact, we prove Theorem A for the larger collection of arithmetic groups satisfying the Congruence Subgroup Property, see Theorem 4.2.2. As a result, we get the following dichotomy for the representation growth of an arithmetic group $\Gamma$ in characteristic zero: either $r_n(\Gamma) = O(n^{745})$, or $r_n(\Gamma)$ grows super-polynomially in $n$ (this happens if $\Gamma$ does not satisfy the Congruence Subgroup Property—see [13]).

We will deduce Theorem A from the following adelic version, which is applicable also for low rank groups. In the following, if $A$ is a ring, we denote its pro-finite completion by $\hat{A}$. 
**Theorem B.** There is a constant $C$ such that, if $k$ is a global field of characteristic at least $C$ and $T$ is a finite set of places of $k$ containing all archimedean ones, then $\alpha \left( \hat{G(\hat{O}_{k,T})} \right) \leq \mathcal{B}(G)$.

From Theorem B and Theorem 2.3.1 below, we deduce the following statement about finite groups like $G(\mathbb{Z}/N\mathbb{Z})$, generalizing [1, Corollary XI]:

**Corollary C.** There is a constant $C$ such that, for any ring of integers $O$ of a global field of characteristic greater than $C$, any non-trivial ideal $I$ of $O$, and any natural number $n \geq C(G) + 1$, the following holds. Let $g_1, h_1, \ldots, g_n, h_n$ be random elements in $G(\hat{O}/I)$ and every $g \in G(\hat{O}/I)$,

$$\text{Prob} \left( [g_1, h_1] \cdots [g_n, h_n] = g \right) < \frac{C}{|G(\hat{O}/I)|}.$$

Theorem B is proved using the algebraic variety parameterizing homomorphisms from a surface group into $G$:

**Definition.** Let $G$ be an algebraic group and let $n \in \mathbb{Z}_{\geq 1}$. Let $\Sigma_n$ be the closed surface of genus $n$. The deformation variety of $\Sigma_n$ in $G$ is the variety

$$\text{Def}_{G,n} = \text{Hom}(\pi_1(\Sigma_n), G) = \{ (g_1, h_1, \ldots, g_n, h_n) \in G \mid [g_1, h_1] \cdots [g_n, h_n] = 1 \}.$$

In order to prove Theorem B, we will relate the representation growth of the group $G(\hat{O})$ and properties of the singularities of the complex deformation varieties $\text{Def}_{G,n}(\mathbb{C})$. The notion of rational singularity is defined in Subsection 2.1.

**Theorem D.** There is a constant $C$ such that, for any global field $k$ of characteristic greater than $C$, any finite set $T$ of places of $k$ containing all archimedean places, and any natural number $n$, if $\text{Def}_{G,n}(\mathbb{C})$ has rational singularities, then $\alpha \left( \hat{G(\hat{O}_{k,T})} \right) \leq 2n - 2$.

Theorem B follows from Theorem D and [1, Theorem VIII], which claims that $\text{Def}_{G,n}(\mathbb{C})$ has rational singularities if $n \geq C(G)$.

**Remark.** Consider the following statements:

1. $\alpha(G(O)) < 2n - 2$.
2. $\alpha(G(O_v)) < 2n - 2$ for any valuation $v$ of $O$.
3. $\text{Def}_{G,n}$ has rational singularities.
4. \( \alpha(G(O)) \leq 2n - 2 \).

Then \((1) \implies (2) \iff (3) \implies (4) \).

The implication \((1) \implies (2) \) follows easily from the observation that, using the map \( G(O) \to G(O_v) \), we get that \( r_n(G(O_v)) \leq r_n(G(O)) \). The equivalence \((2) \iff (3) \) is proved in [1]. In this paper, we prove \((3) \implies (4) \).

**Remark 1.1.1.** The assumption that \( G \) is defined over \( \mathbb{Z} \) can be weakened to assuming that \( G \) is defined over the ring of \( T \)-integers in a number field. Indeed, if \( G \subset \text{GL}_{O_{k,T}} \) is defined over \( O_{k,T} \), let \( G \) be the Zariski closure of \( G \) in \( \text{GL}_{O_k} \). The theorems above applied to the restriction of scalars \( \text{Res}_{O_k/\mathbb{Z}}G \) imply the theorems for \( G \).

### 1.2 Ideas of the proof of Theorem D

Suppose, for simplicity, that \( k = \mathbb{Q} \) and \( T = \emptyset \). In this case, \( G(\widehat{O}_{k,T}) = \prod_p G(\mathbb{Z}_p) \), so we need to estimate the abscissa of convergence of \( \prod_p \zeta_{G(\mathbb{Z}_p)}(s) \). Our main estimate, Theorem 3.1.1, states that, if Def_{G,n} has rational singularities, then

\[
\zeta_{G(\mathbb{Z}_p)}(2n - 2) - 1 < \frac{C}{p}.
\]

There is \( \delta > 0 \) such that the minimal dimension of a non-trivial representation of \( G(\mathbb{Z}_p) \) is at least \( p^\delta \) (see, e.g., [13, Proposition 4.6]). We get that \( \zeta_{G(\mathbb{Z}_p)}(2n - 2 + \epsilon) - 1 < Cp^{-1-\epsilon\delta} \), so the infinite product \( \prod \zeta_{G(\mathbb{Z}_p)}(2n - 2 + \epsilon) \) converges.

In order to prove (3), we consider the representation zeta functions of the finite groups \( \zeta_{G(\mathbb{Z}/p^m)} \), where \( p \) is a prime and \( m \) is an integer. Let \( F(m,p) = \zeta_{G(\mathbb{Z}/p^m)}(2n - 2) \). Since \( \lim_{m \to \infty} F(m,p) = \zeta_{G(\mathbb{Z}_p)}(2n - 2) \), our earlier results imply that \( F(m,p) \) are bounded in \( m \) for every \( p \). Using a theorem of Mustata and the fact that \( F(m,p) \) are bounded by \( m \) for almost all \( p \), we show that, for any \( m \), the sequence \( F(m,p) \) tends to one as \( p \) goes to infinity. Roughly speaking, we use the orbit method to show that \( F(m,p) \) is described by a motivic integral (with parameters \( m \) and \( p \)), and, therefore, has a formula involving simple expressions in \( m \) and \( p \) as well as the number of \( \mathbb{F}_p \)-points on \( \mathbb{Z} \)-schemes. Using Chebotarev’s theorem and the Lang–Weil estimates, we show that the limits over each parameter suffice to prove the estimate (3).

### 1.3 Structure of the paper

In §2 we give the necessary preliminaries for the paper. In §§2.1–§2.2 we review the relevant algebraic geometry. In §§2.3 we review the results of [1]. In §§2.4 we review relevant parts from the theory of motivic integration.
In §3 we prove the estimate (3), deferring some proofs to Appendix A.
In §4 we prove Theorems A and D. As mentioned above, these imply Theorem B and Corollary C.

In Appendix A we give a version of the Kirillov orbit method. Using it and the results of [3], we prove that the right hand side \( \zeta_{G(\mathbb{Z}_p)}(2n - 2) - 1 \) of the estimate (3) can be approximated by a motivic integral.

1.4 Acknowledgements
We thank Vladimir Hinich for useful discussions. Part of this paper was written during the program ‘Multiplicity Problems in Harmonic Analysis’ held at the Hausdorff Institute (2012-2014). A.A. was partially supported by ISF grant 687/13 and NSF grant DMS-1100943. N.A. was partially supported by NSF grants DMS-0901638 and DMS-1303205. Both of us were partially supported by BSF grant 2012247.

2 Preliminaries
2.1 Singularities
In this section, we review the notions of resolution of singularities, rational singularities, and complete intersections. For more detailed overview, we refer the reader to [1, Appendix B].

Definition 2.1.1. Let \( X \) be an algebraic variety defined over a field \( k \). A resolution of singularities of \( X \) is a proper map \( p : \tilde{X} \to X \) such that

- \( \tilde{X} \) is smooth.
- The restriction of \( p \) to \( p^{-1}(X^{sm}) \) is an isomorphism.

Definition 2.1.2 (cf. [10, I §3, page 50-51]). Let \( X \) be an algebraic variety defined over a field \( k \) of characteristic 0.

1. We say that \( X \) has rational singularities if, for any (equivalently, for some) resolution of singularities \( p : \tilde{X} \to X \), the natural morphism \( Rp_*(\mathcal{O}_{\tilde{X}}) \to \mathcal{O}_X \) is an isomorphism.

2. A (usually singular) point \( x \in X(k) \) is a rational singularity if there is a Zariski neighborhood \( U \subset X \) of \( x \) that has rational singularities.
Definition 2.1.3. Let $X$ be an $n$-dimensional scheme of finite type over a field $k$. We say that $X$ is a local complete intersection if there is an open cover $X = \bigcup U_i$ and, for each $i$, there is an embedding $U_i \hookrightarrow \mathbb{A}^N$, such that $U_i$ is the zero locus of $N-n$ polynomials.

2.2 Jet schemes and Mustata’s theorem

In this section we recall the definition of jet schemes and quote one of our main tools, Mustata’s theorem (see [15]), which relates rational singularities and irreducibility of jet schemes. We will use repeatedly the following simple lemma:

Lemma 2.2.1. Suppose that $Z \to T \to S$ and $X \to S$ are morphisms of schemes. Then $\text{Hom}_T(Z, X \times_T S) \cong \text{Hom}_S(Z, X)$.

We move on to define jet schemes.

Notation 2.2.2. For a scheme $Y$, denote $Y^{[m]} = Y \times_{\text{Spec} \mathbb{Z}} \text{Spec} \mathbb{Z}[t]/t^{m+1}$.

The projection $Y^{[m]} \to Y$ is finite and (locally) free. For every scheme $S$, the assignment $Y \mapsto Y^{[m]}$ gives rise to a functor between $(\text{Sch}_S)$ and $(\text{Sch}_{S^{[m]}})$.

Notation 2.2.3. Let $X \to S$ be an affine morphism of finite type. Let $\mathcal{J}_m(X/S)$ be the restriction of scalars of $X^{[m]}$ along the map $S^{[m]} \to S$, i.e., the functor $\mathcal{J}_m(X/S) : (\text{Sch}_S) \to (\text{Set})$ given by

$$\mathcal{J}_m(X/S)(Z) = \text{Hom}_{S^{[m]}}(Z^{[m]}, X^{[m]}) \cong \text{Hom}_S(Z^{[m]}, X).$$

From [16, §7.6], we get

Theorem-Definition 2.2.4. The functor $\mathcal{J}_m(X/S)$ is representable by a scheme of finite type over $S$. We call the representing scheme the $m$-th relative jet scheme of $X \to S$ and denote it by $\text{Jet}_m(X/S)$.

Let $X \to S$ be a morphism as above. For any morphisms $Z \to T \to S$ of schemes, we have a canonical bijections

$$\text{Hom}_T(Z, \text{Jet}_m(X \times_S T/T)) \cong \text{Hom}_T(Z^{[m]}, X \times_S T) \cong \text{Hom}_S(Z^{[m]}, X) \cong$$

$$\cong \text{Hom}_S(Z, \text{Jet}_m(X/S)) \cong \text{Hom}_T(Z, \text{Jet}_m(X/S) \times_S T),$$

which is functorial in $Z$, and, therefore, defines an isomorphism $\text{Jet}_m(X \times_S T/T) \cong \text{Jet}_m(X/S) \times_S T$.

Theorem 2.2.5 ([15]). Let $X$ be an irreducible local complete intersection variety defined over a field $k$ of characteristic 0. Then the following are equivalent:

1. $X$ has rational singularities.

2. All the jet schemes $\text{Jet}_m(X/k)$ are irreducible.
2.3 Rational singularities and representation growth

In this section we review the results of [1], and state our second main tool, relating rational singularities to representation growth. The starting point for [1] was the following Theorem of Frobenius:

**Theorem 2.3.1** (Frobenius). *Let $\Gamma$ be a finite group, and let $n \geq 1$ be an integer. For every $g \in \Gamma$, the number of solutions to the equation $[x_1, y_1] \cdots [x_n, y_n] = g$ is equal to*

$$|\Gamma|^{2n-1} \sum_{\pi \in \text{Irr}(\Gamma)} \frac{\chi_\pi(g)}{(\dim \pi)^{2n-1}},$$

*where $\text{Irr}(\Gamma)$ denotes the set of isomorphism classes of irreducible representations of $\Gamma$ and $\chi_\pi$ denotes the character of $\pi$.*

We will use the following

**Theorem 2.3.2** ([1, Theorem IV]). *Let $H$ be a semi-simple algebraic group defined over a finitely generated field $k$ of characteristic 0 and let $n \in \mathbb{Z}_{\geq 2}$. The following are equivalent:*

1. *The point $(1, \ldots, 1)$ is a rational singularity of the deformation variety $\text{Def}_{H,n}$. *
2. *For every non-archimedian local field $F$ containing $k$ and every compact open subgroup $\Gamma \subset H(F)$, the series*

$$\zeta(2n - 2) = \sum_{\pi \in \text{Irr}(\Gamma')} (\dim \pi)^{2-2n}$$

*converges.*

3. *For every finite extension $k'/k$, there is a local field $F'$ containing $k'$ and a compact open subgroup $\Gamma \subset H(F)$ such that the series*

$$\zeta(2n - 2) = \sum_{\pi \in \text{Irr}(\Gamma')} (\dim \pi)^{2-2n}$$

*converges.*

Using this theorem we established the following relation between representation growths in different characteristics:
Theorem 2.3.3 ([1, Theorem V]). Let $H$ be an affine group scheme over a localization of $\mathbb{Z}$ by finitely many primes. Assume that the generic fiber of $H$ is semi-simple, and let $n \geq 1$ be an integer.

There is a constant $p_0$ such that, if $F_1, F_2$ are local fields with isomorphic residue fields of characteristic greater than $p_0$, and if $O_1, O_2$ denote the rings of integers of $F_1$ and $F_2$, then the series
\[
\zeta_{H(O_1)}(2n) = \sum_{\pi \in \text{Irr}(H(O_1))} \frac{\text{dim} \pi}{\pi^{-2n}}
\]
converges if and only if the series
\[
\zeta_{H(O_2)}(2n) = \sum_{\pi \in \text{Irr}(H(O_2))} \frac{\text{dim} \pi}{\pi^{-2n}}
\]
converges. Moreover, in this case, $\zeta_{H(O_1)}(2n) = \zeta_{H(O_2)}(2n)$.

2.4 Definable Integrals

In this section, we recall the setting of definable $p$-adic integrals and state two theorems about them. One is a uniformity result about $p$-adic integrals, and is a special case of [8, Theorem 1.3]. The other is the claim that representation zeta functions are approximated by $p$-adic integrals. The proof of the last claim is given in the appendix.

2.4.1 The Denef–Pas language

Let $L_\emptyset$ be the first-order language with:

- Three sorts, denoted by $VF$, $RF$, and $VG$, and called the valued field sort, the residue field sort, and the valuation group sort, respectively.

- Five constants, $0_{VF}, 1_{VF} \in VF$, $0_{RF}, 1_{RF} \in RF$, and $0_{VG}, \infty_{VG} \in VG$.

- Seven functions, $+_VF : VF \times VF \to VF$, $\cdot_VF : VF \times VF \to VF$, $+_RF : RF \times RF \to RF$, $\cdot_RF : RF \times RF \to RF$, $+_VG : VG \times VG \to VG$, $\text{val} : VF \setminus \{0_{VF}\} \to VG$, and $\text{ac} : VF \setminus \{0_{VF}\} \to RF$.

- One binary relation, $<$, on $VG$. 


2.4.2 Structures

Suppose that $F$ is a field with a non-archimedean valuation $v$. Denote $O = \{x \in F \mid v(x) \geq 0\}$ and $m = \{x \in F \mid v(x) > 0\}$. Assume that the short exact sequence

$$1 \to O^\times/(1 + m) \to F^\times/(1 + m) \to F^\times/O^\times \to 1 \quad (4)$$

splits, and let $\sigma : F^\times/(1 + m) \to O^\times/(1 + m)$ be such a splitting. An important example is the case where $F$ is a local field. In this case, if $\pi$ is a uniformizer, then $x \in F^\times \mapsto x/\pi^{v(x)} \in O^\times$ descends to a splitting of $(4)$.

From this data, we construct a structure for $L_\emptyset$ as follows: the sort $VF$ is interpreted as $F$, the sort $RF$ is interpreted as the residue field of $F$, and the sort $VG$ is interpreted as $\mathbb{Z} \cup \{\infty\}$. The function $\text{val}$ is interpreted as the valuation $v$ and the function $\text{ac}$ is interpreted as the composition

$$F^\times \to F^\times/(1 + m) \xrightarrow{\sigma} O^\times/(1 + m) = RF(F) \setminus \{0\}.$$

The interpretation of the constants, relation, and the rest of the functions is clear. From this point on, when we write a valued field, we mean a valued field together with a section as above, and we consider it as a structure of the Denef–Pas language.

2.4.3 Quantifier-free definable functions

Suppose that $\mathcal{S}$ is a structure for $L$. If $\varphi = \varphi(x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_k)$ is a formula in $L$, where the variables $x_i$ are of $VF$ sort, the variables $y_i$ are of $RF$ sort, and the variables $z_i$ are of $VG$ sort, we denote

$$\varphi(\mathcal{S}) = \{(a_i, b_i, c_i) \in VF(\mathcal{S})^n \times RF(\mathcal{S})^m \times VG(\mathcal{S})^k \mid \varphi(a_i, b_i, c_i) \text{ holds in } \mathcal{S}\}.$$

Definition 2.4.1.

1. We say that two formulas $\phi(x)$ and $\psi(x)$ are equivalent if, for every Henselian valued field $F$, we have $\phi(F) = \psi(F)$. An equivalence class of formulas is called a definable set. If $X$ is a definable set and $F$ is a Henselian valued field, we write $X(F) = \phi(F)$, for any $\phi \in X$.

2. We say that a formula in $L$ is quantifier-free if there are no quantifiers in it. A definable set is called quantifier-free, if there is a quantifier-free formula representing it.
3. Suppose that \(X, Y\) are definable sets on variables \(x, y\) respectively (\(x\) and \(y\) are tuples of variables of the three sorts of \(L\)). A quantifier-free definable set \(\Gamma\) on the tuple of variables \((x, y)\) is called a quantifier-free definable function if, for any Henselian valued field \(F\), the set \(\Gamma(F)\) is the graph of a function between \(X(F)\) and \(Y(F)\), which we also denote by \(\Gamma(F)\).

Example 2.4.2.

1. Let \(X \subset \mathbb{A}_Z^N\) be an affine scheme over \(\text{Spec} \mathbb{Z}\). Choose a generating set \(\{p_1, \ldots, p_M\} \subset \mathbb{Z}[x_1, \ldots, x_N]\) for the ideal of polynomials vanishing on \(X\), and let \(X_{VF}\) be the equivalence class of the formula
\[
(p_1(x_1, \ldots, x_N) = 0) \land \cdots (p_M(x_1, \ldots, x_N) = 0),
\]
where \(x_1, \ldots, x_N\) are of the VF sort. For any valued field \(F\), we have \(X_{VF}(F) = X(F)\). Similarly, there is also a quantifier-free definable set, denoted by \(X_{RF}\), such that \(X_{RF}(F) = X(k)\), for all Henselian valued fields \(F\) with residue field \(k\).

2. Let \(f : X \to Y \to \text{Spec} \mathbb{Z}\) be morphisms of schemes. Then there is a quantifier-free definable function \(f_{VF} : X_{VF} \to Y_{VF}\) such that, for every Henselian valued field \(F\), the function \(f_{VF}(F) : X_{VF}(F) \to Y_{VF}(F)\) coincides with the restriction of \(f\) to \(F\) points.

3. If \(X\) is an algebraic variety and \(p\) is a regular function on \(X\), the formula \(y = \text{val}(p(x))\) gives rise to a quantifier-free definable function from \(X_{VF}\) to \(\mathbb{V}G\).

The following theorem follows from [8, Theorem 1.3]:

Theorem 2.4.3. Let \(X \to \text{Spec} \mathbb{Z}\) be an affine and smooth morphism of relative dimension \(d\), let \(\omega \in \Gamma(X, \Omega^d_{X/\text{Spec} \mathbb{Z}})\), and let \(f_1, f_2 : X_{VF} \to \mathbb{V}G\) be quantifier-free definable functions. Then there are

1. Constant \(C\).
2. A finite set \(S\) of prime numbers.
3. (Finite or infinite) arithmetic progressions \(I_1, \ldots, I_M \subset \mathbb{Z}\).
4. Polynomials \(g_1, \ldots, g_M \in \mathbb{Q}[x, y]\).
5. Reduced affine schemes \(X_1, \ldots, X_M\) of finite type over \(\mathbb{Z}\) which are smooth over \(\text{Spec} \mathbb{Z}[S^{-1}]\) such that \(X_i \times_{\text{Spec} \mathbb{Z}} \text{Spec} \mathbb{Q}\) are non-empty and irreducible.
6. Rational numbers $\alpha_1, \ldots, \alpha_M, \beta_1, \ldots, \beta_M$.

7. Integers $a_{j,k}$ for $j = 1, \ldots, M$ and $k = 1, \ldots, M$.

such that, if $F$ is a local field with residue field $\mathbb{F}_q$ of characteristic not in $S$ and $m \in \mathbb{Z}_{\geq C}$, then

$$
\int_{\{x \in X(F) \mid f_1(x) = m\}} q^{-f_2(x)} |\omega|_F = \sum_{j=1}^{M} 1_{f_j}(m) |X_j(F_q)| \left( \prod (1 - q^{-a_{j,k}}) \right),
$$

where $|\omega|_F$ is the measure on $X(F)$ corresponding to $\omega$. Moreover, we can assume that, for all $j$, $g_j(x,y)$ is positive on $\mathbb{Z}_{\geq C} \times \mathbb{R}_{>1}$.

### 2.5 Representation zeta functions as quantifier-free definable integrals

We will use the following notation

**Notation 2.5.1.**

1. If $p$ is a prime number and $q = p^n$ is a power of $p$, we denote the unique degree-$n$ unramified extension of $\mathbb{Q}_p$ by $\mathbb{Q}_q$, and its ring of integers by $\mathbb{Z}_q$.

2. For a set $S$ of prime numbers, let

$$
\mathcal{P}_S = \{p^n \mid p \text{ is a prime number not in } S \text{ and } n \in \mathbb{N}_{\geq 1}\}.
$$

**Notation 2.5.2.** Let $A$ be a set, and let $(x_a)_{a \in A}$ and $(y_a)_{a \in A}$ be sequences of real numbers indexed by a set $A$. We write `$x_a \sim y_a$ over $a \in A$' if there is a constant $C$ such that $\frac{1}{C} x_a \leq y_a \leq C x_a$ for all $a \in A$.

In Appendix A we prove the following:

**Theorem 2.5.3.** Let $G$ be an algebraic group over $\mathbb{Z}$ whose generic fiber is semi-simple, and let $n \in \mathbb{Z}$ be such that the series defining $\zeta_G(\mathbb{Z}_q)(n)$ converges for every prime power $q$. There is a quantifier-free definable function $f : \text{VF}^{\dim G + 1} \to VG$ and a finite set $S$ of prime numbers such that,

$$
\zeta_G(\mathbb{Z}_q)(n) - \zeta_G(\mathbb{F}_q)(n) \sim \int_{\mathbb{Z}_q^n} q^f(x) dx \quad \text{over } q \in \mathcal{P}_S.
$$
3 Uniform bounds on local zeta functions

3.1 The main estimate

Recall that $G$ is a group scheme over $\mathbb{Z}$ whose generic fiber is simple, connected, and simply connected. The main result of this section is the following:

**Theorem 3.1.1.** For every $n \geq 1$ such that $\text{Def}_{G,n+1}$ has rational singularities, there is a finite set $S$ of prime numbers and an integer $C$ such that, for any $q \in \mathcal{P}_S$,

$$\zeta_{G(\mathbb{Z}_q)}(2n) - 1 = \zeta_{G(\mathbb{F}_q[[t]])}(2n) - 1 \leq Cq^{-1}. $$

We sketch the proof of the theorem. In Section 3.2 we use Mustata’s theorem and the Lang–Weil estimates to show that, for every $m$, the sequence $\zeta_{G(\mathbb{F}_q[[t]])/t^m}(2n)$ tends to 1 as $q$ tends to infinity (Theorem 3.2.1). In Section 3.3, we use the fact that the numbers $\zeta_{G(\mathbb{F}_q[[t]])/t^k}(2n)$ are all uniformly described by a single definable integral (with parameters) and Theorem 2.3.2 in order to show that $\zeta_{G(\mathbb{F}_q[[t]])}(2n)$ tends to 1 as $q$ tends to infinity (Theorem 3.3.1). This implies that $\zeta_{G(\mathbb{Z}_q)}(2n)$ tends to 1 as $q$ tends to infinity. Finally, in Section 3.4, we use the fact that $\zeta_{G(\mathbb{Z}_q)}(2n)$ are all approximated by a single definable integral in order to prove Theorem 3.1.1.

In the rest of the section, fix $n$ such that $\text{Def}_{G,n+1}$ has rational singularities.

3.2 $\zeta_{G(\mathbb{F}_q[[t]])/t^m}(2n)$ tends to 1

In this subsection, we prove

**Theorem 3.2.1.** For every $m \geq 1$, there is a finite set $S$ of prime numbers such that,

$$\lim_{\mathcal{P}_S \ni q \to \infty} \zeta_{G(\mathbb{F}_q[[t]])/t^m}(2n) = 1.$$ 

For the proof, we will use the Lang–Weil estimates (see [14]). We start with the following notation

**Notation 3.2.2.** Suppose that $X$ is a scheme of finite type over $\text{Spec} \mathbb{Z}$ and that $k$ is a field. We denote the number of irreducible components of $X \times_{\text{Spec} \mathbb{Z}} \text{Spec} \bar{k}$ that are defined over $k$ by $c_X(k)$. If $q$ is a prime power, we also write $c_X(q)$ instead of $c_X(\mathbb{F}_q)$.

**Theorem 3.2.3 (Lang–Weil).** Let $X$ be a scheme of finite type over $\text{Spec} \mathbb{Z}$. Let $d = \dim(X \times_{\text{Spec} \mathbb{Z}} \text{Spec} \mathbb{Q})$. There is a finite set $S$ of prime numbers such that

$$\lim_{\mathcal{P}_S \ni q \to \infty} \left| \frac{|X(\mathbb{F}_q)|}{q^d} - c_X(q) \right| = 0.$$
If, in addition, \( X \times_{\text{Spec } \mathbb{Z}} \text{Spec } \mathbb{Q} \) is irreducible and smooth and \( q \in \mathcal{P}_S \), then \( c_X(q) = 0 \implies X(\mathbb{F}_q) = \emptyset \).

**Proof of Theorem 3.2.1.** Let

\[
X = \text{Def}_{G,n+1} = \{(g_1, h_1, \ldots, g_{n+1}, h_{n+1}) \in G^{2n+2} \mid [g_1, h_1] \cdots [g_{n+1}, h_{n+1}] = 1\},
\]

and let \( X_m = \text{Jet}_m(X/\text{Spec } \mathbb{Z}) \). Mustata’s Theorem implies that \( X_m \times \text{Spec } \mathbb{Q} = \text{Jet}_m(X \times \text{Spec } \mathbb{Q}/\text{Spec } \mathbb{Q}) \) is an absolutely irreducible variety of dimension \( m \cdot \dim(X \times \text{Spec } \mathbb{Q}) = m \cdot (2n - 1) \cdot \dim G \). By the Lang–Weil estimates, there is a finite set \( S \) of prime numbers such that, for all \( q \in \mathcal{P}_S \), we have \( |X_m(\mathbb{F}_q)| = q^{m(2n-1)\dim G}(1 + o_q(1)) \).

Since \( X_m \times \text{Spec } \mathbb{F}_q = \text{Jet}_m(X \times \text{Spec } \mathbb{F}_q/\text{Spec } \mathbb{F}_q) \), we have

\[
X_m(\mathbb{F}_q) = \{(g_1, \ldots, h_{n+1}) \in G(\mathbb{F}_q[t]/t^m)^{2n+2} \mid [g_1, h_1] \cdots [g_{n+1}, h_{n+1}] = 1\}.
\]

By Theorem 2.3.1 applied with \( \Gamma = G(\mathbb{F}_q[t]/t^m) \) and \( g = 1 \), we have

\[
\zeta_{G(\mathbb{F}_q[t]/t^m)}(2n) = \frac{|X_m(\mathbb{F}_q)|}{|G(\mathbb{F}_q[t]/t^m)|^{2n-1}}.
\]

For \( q \in \mathcal{P}_S \), we have

\[
\zeta_{G(\mathbb{F}_q[t]/t^m)}(2n) = \frac{|X_m(\mathbb{F}_q)|}{|G(\mathbb{F}_q[t]/t^m)|^{2n-1}} = \frac{q^{m(2n-1)\dim G}(1 + O(q^{-1/2}))}{(q^{m\dim G}(1 + O(q^{-1/2})))^{2n-1}} \to 1.
\]

\[\square\]

### 3.3 \( \zeta_{G(\mathbb{Z}_q)}(2n) \) tends to 1

Next, we prove a weak version of Theorem 3.1.1

**Theorem 3.3.1.** There is a finite set \( S \) of prime numbers such that, for every \( n \) for which \( \text{Def}_{G,n+1} \) has rational singularities, we have

\[
\lim_{\mathcal{P}_S \ni q \to \infty} \zeta_{G(\mathbb{Z}_q)}(2n) = \lim_{\mathcal{P}_S \ni q \to \infty} \zeta_{G(\mathbb{F}_q[t])}(2n) = 1. \quad (5)
\]

#### 3.3.1 Irreducible components modulo \( p \)

**Proposition 3.3.2.** Suppose that \( X \) is a scheme of finite type over \( \text{Spec } \mathbb{Z} \). Assume that \( X_{\mathbb{Q}} := X \times \text{Spec } \mathbb{Q} \) is irreducible. Then
1. For almost all prime numbers \( p \), we have \( c_X(\mathbb{F}_p) = c_X(\overline{\mathbb{Q}}) \).

2. If \( c_X(\overline{\mathbb{Q}}) > 1 \), then there are infinitely many prime numbers \( p \) such that \( c_X(p) < c_X(\overline{\mathbb{Q}}) \).

**Definition 3.3.3.** Let \( S \) be an irreducible scheme with generic point \( \eta \), let \( s \) be a closed point of \( S \), and let \( \varphi : X \to S \) be a morphism of finite type. Define a relation \( R_{S,s} \) between the set of irreducible components of \( X_\eta := \varphi^{-1}(\eta) \) and the set of irreducible components of \( X_s := \varphi^{-1}(s) \) by \((Y_1, Y_2) \in R_{S,s}\) if \( Y_2 \subset Y_1 \).

**Theorem 3.3.4.** (cf. [6, Proposition 9.7.8]) Let \( S \) be an irreducible scheme with generic point \( \eta \) and let \( \varphi : X \to S \) be a morphism of finite type. Assume that all irreducible components of \( X_\eta \) are absolutely irreducible. There is an open set \( U \subset S \) such that, for any closed point \( s \in U \),

1. All irreducible components of \( X_s \) are absolutely irreducible.
2. The relation \( R_{\eta,s} \) is the graph of a bijection.

Let \( X \to \text{Spec} \mathbb{Z} \) be a scheme of finite type. Let \( L/\mathbb{Q} \) be a Galois extension such that all irreducible components of \( X \times \text{Spec} L \) are absolutely irreducible, and let \( O \) be the ring of integers of \( L \). The group \( \text{Gal}(L/\mathbb{Q}) \) acts on the set of irreducible components of \( X \times \text{Spec} L \). For any prime ideal \( \mathfrak{p} \) of \( O \) with residue field \( k_\mathfrak{p} \), consider the decomposition group \( D_\mathfrak{p} = \{ \sigma \in \text{Gal}(L/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p} \} \), and the homomorphism \( \Phi_\mathfrak{p} : D_\mathfrak{p} \to \text{Gal}(k_\mathfrak{p}/\mathbb{F}_p) \). The group \( \text{Gal}(k_\mathfrak{p}/\mathbb{F}_p) \) acts on the set of irreducible components of \( X_{k_\mathfrak{p}} \). The following is obvious

**Proposition 3.3.5.** Under the assumptions above, for any \((Y_1, Y_2) \in R_{\text{Spec} O, \mathfrak{p}} \) and \( \sigma \in D_\mathfrak{p} \), we have \((\sigma \cdot Y_1, \Phi_\mathfrak{p}(\sigma) \cdot Y_2) \in R_{\text{Spec} O, \mathfrak{p}} \).

Proposition 3.3.5, Theorem 3.3.4, and Chebotarev’s density theorem imply Proposition 3.3.2

**3.3.2 Proof of Theorem 3.3.1**

**Lemma 3.3.6.** Let \( X \) be a scheme of finite type over \( \text{Spec} \mathbb{Z} \) whose generic fiber is non-empty, let \( g(x, y) \) be a real polynomial, let \( \alpha, \beta \in \mathbb{R} \), let \( a_1, \ldots, a_n \) be negative integers, and let \( S \) be a finite set of prime numbers. Set

\[
P(m, q) = |X(\mathbb{F}_q)| \cdot q^{am+\beta} \prod_{k=1}^{n} \frac{1}{1 - q^{a_k}}.
\]

Then the following claims hold:
1. Assume that either
   
   (a) \( \alpha > 0 \) or
   (b) \( \alpha = 0 \) and \( g \) depends on \( m \) non-trivially (i.e. \( \frac{\partial g}{\partial m} \neq 0 \)).

   Then \( \lim_{m \to \infty} P(m, q) = \pm \infty \) for infinitely many \( q \in \mathcal{P}_S \).

2. If \( \alpha < 0 \) then there is \( D \) such that \( \lim_{q \to \infty} P(m, q) = 0 \) uniformly for \( m > D \).

Proof.

1. The limit \( \lim_{m \to \infty} P(m, q) \) will be infinity if \( X(\mathbb{F}_q) \neq \emptyset \), and, by Lang–Weil, this happens for infinitely many \( q \in \mathcal{P}_S \).

2. Suppose that the degree of \( g \) is \( d \). Then there is a constant \( M \) such that \( |g(m, q)| \leq Mm^d q^d \). In addition, There is a constant \( e \) such that \( |X(\mathbb{F}_q)| < eq^{\dim X} \) for all \( q \in \mathcal{P}_S \). Hence, there is a constant \( C \) such that

\[
|P(m, q)| \leq Cm^d q^{\alpha m + \beta + d + \dim X}.
\]

This implies the assertion.

\[ \square \]

**Notation 3.3.7.** For a polynomial \( g(x) \), let \( g^{\text{top}} \) be the coefficient of the monomial of highest degree in \( g \).

**Lemma 3.3.8.** Let \( X \) be a scheme of finite type over \( \text{Spec} \mathbb{Z} \), whose generic fiber is non-empty and irreducible, let \( g(x) \) be a real polynomial, let \( \beta \in \mathbb{R} \), let \( a_1, \ldots, a_m \) be negative integers, and let \( S \) be a finite set of prime numbers. Set

\[
P(q) = \frac{|X(\mathbb{F}_q)| g(q) q^\beta}{\prod (1-q^{a_k})}.
\]

Let \( d = \dim X + \deg g + \beta \). Then

1. If \( d > 0 \) then \( \lim \sup_{\mathcal{P}_S \ni q \to \infty} P(q) = \infty \).
2. If \( d < 0 \) then \( P(q)q^d \) is bounded for \( q \in \mathcal{P}_S \). In particular, \( \lim_{q \to \infty} P(q) = 0 \).
3. If \( d = 0 \), then \( \lim_{\mathcal{P}_S \ni q \to \infty} (P(q) - g^{\text{top}} c_X(q)) = 0 \).

Proof. These are immediate consequences of the Lang–Weil estimates. \[ \square \]

16
We now prove Theorem 3.3.1.

**Proof of Theorem 3.3.1.** By Theorem 2.3.1, we have

\[
\zeta_{G(F_q[[t]]/t^m)}(2n) = \frac{|\{(g_1, h_1, \ldots, g_n, h_n) \in G(F_q[[t]]/t^m)^{2n} \mid [g_1, h_1] \cdots [g_n, h_n] = 1\}|}{|G(F_q[[t]]/t^m)|^{2n-1}} =
\]

\[
= \frac{q^{m(2n-1)\dim G}}{|G(F_q[[t]]/t^m)|^{2n-1}} \cdot q^{-m(2n-1)\dim G} \int_{G(F_q[[t]])^{2n}} F(g_1, h_1, \ldots, g_n, h_n, m) dg_1 \cdots dh_n,
\]

where \( F \) is the function

\[
F(g_1, \ldots, h_n, m) = \begin{cases} 1 & [g_1, h_1] \cdots [g_n, h_n] \equiv 1 \pmod{t^m} \\ 0 & \text{else} \end{cases}
\]

Let \( S_0 \) be the (finite) set of primes \( p \) for which the map \( G \to \text{Spec} \mathbb{Z} \) is not smooth over \( p \). For \( q \in \mathcal{P}_{S_0} \), the numbers \( q^{m(2n-1)\dim G}/|G(F_q[[t]]/t^m)|^{2n-1} \) do not depend on \( m \) and tend to 1 as \( q \) tends to infinity.

Let

\[
\mathcal{I}_{m,q} = q^{-m(2n-1)\dim G} \int_{G(F_q[[t]])^{2n}} F(g_1, h_1, \ldots, g_n, h_n, m) dg_1 \cdots dh_n.
\]

Since \( F \) is quantifier-free, Theorem 2.4.3 implies that there are:

1. A constant \( M \).
2. A finite set \( S \) of prime numbers.
3. (Finite or infinite) arithmetic progressions \( I_1, \ldots, I_M \subset \mathbb{Z}_{\geq 0} \).
4. Polynomials \( g_1, \ldots, g_M \in \mathbb{Q}[x,y] \) such that each \( g_i(x,y) \) is positive on \( I_i \times \mathbb{R}_{>1} \).
5. Reduced affine schemes \( X_1, \ldots, X_M \) of finite type over \( \mathbb{Z} \) which are smooth over \( \text{Spec} \mathbb{Z}[S^{-1}] \) such that \( X_i \times_{\text{Spec} \mathbb{Z}} \text{Spec} \mathbb{Q} \) are non-empty and irreducible.
6. Rational numbers \( \alpha_1, \ldots, \alpha_M, \beta_1, \ldots, \beta_M \).
7. Integers \( a_{j,k} \) for \( j = 1, \ldots, M \) and \( k = 1, \ldots, M_j \).
such that, for any \( q \in \mathcal{P}_S \) and any \( m \geq 0 \),

\[
\mathcal{I}_{m,q} = \sum_{j=1}^{M} 1_{I_j}(m)|X_j(\mathbb{F}_q)| \frac{g_j(m,q)q^{\alpha_j m + \beta_j}}{\prod (1 - q^{-a_{jk}})}.
\]  

(6)

We will apply (6) only for \( m \) large enough. Hence, we can also assume that all \( I_j \) are infinite. In addition, we can (and will) assume that \( S \) contains \( S_0 \) and that \( \zeta_{G(\mathbb{F}_q[\ell])}(2n) = \zeta_{G(\mathbb{Z}_q)}(2n) \) for all \( q \in \mathcal{P}_S \) (by Theorem 2.3.3).

By Theorem 2.3.2 we have

\[
\lim_{m \to \infty} \zeta_{G(\mathbb{F}_q[\ell]/\ell^m)}(2n) = \zeta_{G(\mathbb{F}_q[\ell])}(2n) < \infty,
\]

and, therefore, \( \lim_{m \to \infty} \mathcal{I}_{m,q} < \infty \) for \( q \in \mathcal{P}_S \). Since each summand in the right hand side of (6) is non-negative, we get that, for each \( j \) and \( q \in \mathcal{P}_S \),

\[
\limsup_{m \to \infty} 1_{I_j}(m)|X_j(\mathbb{F}_q)| \frac{g_j(m,q)q^{\alpha_j m + \beta_j}}{\prod (1 - q^{-a_{jk}})} < \infty.
\]  

(7)

For each \( j \), Lemma 3.3.6 implies that either \( \alpha_j < 0 \) or \( \alpha_j = 0 \) and \( g_j \) is independent of \( m \). Let \( J_1 = \{ j \mid \alpha_j < 0 \} \). If \( j \notin J_1 \), we will write \( g_j(q) \) instead of \( g_j(m,q) \).

Theorem 3.2.1 implies that, for each \( m \), there is a finite set \( T_m \) of prime numbers (which we can assume to include \( S \)) such that

\[
\lim_{\mathcal{P}_{T_m} \ni q \to \infty} \mathcal{I}_{m,q} = \lim_{\mathcal{P}_{T_m} \ni q \to \infty} \zeta_{G(\mathbb{F}_q[\ell]/\ell^m)}(2n) = 1.
\]

Since each summand in the right hand side of (6) is non-negative, we get that, for each \( j \notin J_1 \) and \( m \),

\[
\limsup_{\mathcal{P}_{S \cup T_m} \ni q \to \infty} 1_{I_j}(m)|X_j(\mathbb{F}_q)| \frac{g_j(q)q^{\beta_j}}{\prod (1 - q^{-a_{jk}})} < \infty.
\]  

(8)

By Lemma 3.3.8, we get that \( \dim X_j + \deg g_j + \beta_j \leq 0 \). Let \( J_2 = \{ j \mid \dim X_j + \deg g_j + \beta_j < 0 \} \).

By Lemma 3.3.6, there is a number \( D \) such that, for \( m > D \), we have

\[
1 = \lim_{\mathcal{P}_{T_m} \ni q \to \infty} \mathcal{I}_{m,q} = \lim_{\mathcal{P}_{T_m} \ni q \to \infty} \sum_{j \notin J_1 \cup J_2} 1_{I_j}(m)|X_j(\mathbb{F}_q)| \frac{g_j(q)q^{\beta_j}}{\prod (1 - q^{-a_{jk}})} = \lim_{\mathcal{P}_{S \cup T_m} \ni q \to \infty} \sum_{j \notin J_1 \cup J_2} 1_{I_j}(m)g_j^{\text{top}}c_{X_j}(q)
\]  

(9)
By Proposition 3.3.2, for almost all prime numbers $p$, we have $\lim_{r \to \infty} c_{X_j}(p^r) = c_{X_j}(\mathbb{Q})$, for every $j$. Fix such a prime $p$ such that $p \notin T_m$. Taking the limit in (9) over $q = p^r$ ($r \to \infty$), we get that

$$\sum_{j \notin J_1 \cup J_2} 1_{I_j}(m) g_j^{top} c_{X_j}(\mathbb{Q}) = 1,$$

for every $m > D$. We claim that $c_{X_j}(\mathbb{Q}) = 1$ for every $j$. Assuming the contrary, let $j$ be such that $c_{X_j}(\mathbb{Q}) > 1$. Let $m$ be such that $m > D$ and $m \in I_j$. By Proposition 3.3.2, there are infinitely many prime numbers $q \in \mathcal{P}_{T_m}$ such that $c_{X_j}(q) < c_{X_j}(\mathbb{Q})$. Taking the limit in (9) over such $q$, we get a contradiction. This shows that $c_{X_j}(\mathbb{Q}) = 1$. It follows that, after enlarging $S$, we can assume that $(X_j)_{\mathbb{F}_q}$ are absolutely irreducible, for every $j$.

This implies that the limit

$$\lim_{m \to \infty} \frac{|X_j(\mathbb{F}_q)| g_j(q) q^\beta_j}{\prod (1 - q^{-a_{jk}})}$$

exists and is equal to $g_j^{top}$. Therefore, by Lemmas 3.3.6 and 3.3.8,

$$\lim_{m \to \infty} \zeta_{G(\mathbb{F}_q[[t]]/t^m)}(2n) = \lim_{m \to \infty} \sum_{j \notin J_1 \cup J_2} 1_{I_j}(m) \frac{|X_j(\mathbb{F}_q)| g_j(q) q^\beta_j}{\prod (1 - q^{-a_{jk}})} = \lim_{m \to \infty} \sum_{j \notin J_1 \cup J_2} 1_{I_j}(m) g_j^{top} = 1.$$

Finally, by Theorem 2.3.3, we can enlarge $S$ further so that $\zeta_{G(\mathbb{Z}_q)}(2n) = \zeta_{G(\mathbb{F}_q[[t]])}(2n)$ for all $q \in \mathcal{P}_S$. We get

$$\lim_{m \to \infty} \zeta_{G(\mathbb{Z}_q)}(2n) = \lim_{m \to \infty} \zeta_{G(\mathbb{F}_q[[t]])}(2n) = \lim_{m \to \infty} \lim_{m \to \infty} \zeta_{G(\mathbb{F}_q[[t]]/t^m)}(2n) = 1.$$

\[\square\]

### 3.4 Proof of Theorem 3.1.1

We are now ready to prove Theorem 3.1.1

**Proof of Theorem 3.1.1.** We first discuss $\zeta_{G(\mathbb{F}_q)}(2n) - 1$. Since we assume that the generic fiber of $G$ is simply connected, there is a finite set $S_1$ of prime numbers such that $G(\mathbb{F}_q)$ is perfect for every $q \in \mathcal{P}_S$ (see, e.g. [3, Remark 3.2]). Let $\Phi$ be the absolute root system of $G$. [3, Theorem 3.1] states, in particular, that there is a constant $C_1$ and, for each $q \in \mathcal{P}_{S_1}$, a negative integer $a_1(q)$ such that

$$\zeta_{G(\mathbb{F}_q)}(2n) - 1 < C_1 q^{-1}.$$
Together with Theorem 3.3.1, we get that there is a finite set $S'_1 \supset S_1$ of primes such that

$$
\lim_{P_{S'_1} \ni q \to \infty} \left( \zeta_{G(\mathbb{Z}_q)}(2n) - \zeta_{G(\mathbb{F}_q)}(2n) \right) = 0.
$$

(10)

By Theorems 2.5.3 and 2.4.3, there are

1. Constant $M$.
2. A finite set $S_2$ of prime numbers.
3. Polynomials $g_1, \ldots, g_M \in \mathbb{Q}[x]$ such that each $g_i(y)$ is positive on $\mathbb{R}_{>1}$.
4. Reduced affine schemes $X_1, \ldots, X_M$ of finite type over $\mathbb{Z}$ which are smooth over $\text{Spec} \mathbb{Z}[S^{-1}]$ such that $X_i \times_{\text{Spec} \mathbb{Z}} \text{Spec} \mathbb{Q}$ are non-empty and irreducible.
5. Rational numbers $\beta_1, \ldots, \beta_M$.
6. Integers $a_{j,k}$ for $j = 1, \ldots, M$ and $k = 1, \ldots, M_j$.

such that

$$
\zeta_{G(\mathbb{Z}_q)}(2n) - \zeta_{G(\mathbb{F}_q)}(2n) \sim \sum_{j=1}^{M} |X_j(\mathbb{F}_q)| \frac{g_j(q)q^{\beta_j}}{\prod (1 - q^{a_{j,k}})} \text{ over } q \in P_{S_2}.
$$

Setting $S = S'_1 \cup S_2$, we have that, for each $j$,

$$
\limsup_{P_S \ni q \to \infty} |X_j(\mathbb{F}_q)| \frac{g_j(q)q^{\beta_j}}{\prod (1 - q^{a_{j,k}})} = 0.
$$

By Lemma 3.3.8, we get that there is a constant $C_3$ such that

$$
|X_j(\mathbb{F}_q)| \frac{g_j(q)q^{\beta_j}}{\prod (1 - q^{a_{j,k}})} < \frac{C_3}{q}. \tag{11}
$$

It follows that there is a constant $C$ such that

$$
\zeta_{G(\mathbb{Z}_q)}(2n) - 1 = \zeta_{G(\mathbb{Z}_p)}(2n) - \zeta_{G(\mathbb{F}_q)}(2n) + \zeta_{G(\mathbb{F}_q)}(2n) - 1 \leq \frac{C}{q}.
$$

$\square$
4 Global abscissae

The goal of this section is to prove Theorem D and a generalization of Theorem A. We first introduce the setting.

4.1 Representation zeta functions of adelic groups and the proof of Theorem D

Proof of Theorem D. Theorem 3.1.1 implies that there is a finite set $S$ of prime numbers and a constant $D$ such that, for every $q \in P_S$,

$$\zeta_{G}(\mathbb{Z}_q)(2n-2) - 1 = \zeta_{G(\mathbb{F}_q[[t]])}(2n-2) - 1 \leq Dq^{-1}. \quad (12)$$

Let $C > \max S$, let $k$ be a global field of characteristic greater than $C$, let $T$ be a finite set of places of $k$ containing all archimedean ones, and let $n$ be such that $\text{Def}_{G_{\mathbb{Q},n}}$ has rational singularities. We will show that $\zeta_{G}(\mathcal{O}_{k,T})(2n-2+\epsilon)$ converges, for every positive $\epsilon$.

For any non-archimedean place $v$, let $O_v$ be the ring of integers of the completion $k_v$, and let $|v|$ be the size of the residue field of $O_v$. We have that $\zeta_{G(\mathcal{O}_{k,T})}(s) = \prod_{v \in T} \zeta_{G(O_v)}(s)$, by which we mean, in particular, that the left hand side converges absolutely if and only if each of the terms on the right hand side converges absolutely, and their product converges absolutely. By [1, Theorem IV] and the assumptions, the series $\zeta_{G(O_v)}(2n-2)$ converges for every $v$. Thus, it is enough to prove that $\prod_{v \notin T'} \zeta_{G(O_v)}(2n-2+\epsilon)$ converges, for some finite set of places $T' \supset T$.

For almost all places $v$ we have

$$O_v \cong \mathbb{Z}|v| \text{ or } O_v \cong \mathbb{F}|v|[[t]]. \quad (13)$$

By [13, Proposition 4.6], there is a constant $\delta > 0$ such that, for almost all places $v$, the minimal dimension of a non-trivial representation of $G(O_v)$ is at least $|v|^\delta$. It follows that

$$\zeta_{G(O_v)}(2n-2+\epsilon) - 1 \leq |v|^{-\epsilon \delta} \left( \zeta_{G(O_v)}(2n-2) - 1 \right). \quad (14)$$

Let $T' \supset T$ be a finite set of places such that (12), (13), and (14) hold for any $v \notin T'$. We have

$$\prod_{v \notin T'} \zeta_{G(O_v)}(2n-2+\epsilon) \leq \prod_{v \notin T'} (1 + D|v|^{-1-\epsilon \delta}) \leq \prod_{v \notin T'} (1 + |v|^{-1-\epsilon \delta})^D \leq \prod_{v \notin T'} (1 - |v|^{-1-\epsilon \delta})^{-D} \leq$$
\[
\leq \prod_{v \text{ non-archimedean}} (1 - |v|^{-1 - \epsilon \delta})^{-D} = \zeta_k(1 + \epsilon \delta)^D,
\]
where \( \zeta_k \) is the Dedekind zeta function of \( k \).

### 4.2 Representation zeta functions of arithmetic groups and the proof of Theorem A

In order to formulate a generalization of Theorem A, we use the following definition.

**Definition 4.2.1.** Let \( k \) be a global field, and let \( T \) be a finite set of places of \( k \) containing all archimedean ones. We say that \( G(O_{k,T}) \) has the weak Congruence Subgroup Property (wCSP for short) if the canonical map

\[
\eta : \widehat{G(O_{k,T})} \to G(\widehat{O_{k,T}})
\]

has a finite kernel. Here, the domain of \( \eta \) is the pro-finite completion of \( G(O_{k,T}) \), and its range is the pro-congruence completion of the same group.

Under our assumptions on \( G \), the map \( \eta \) is always surjective by the Strong Approximation Theorem ([18, Chapter 7]). It is known that, if \( \text{rk}_k G_k \geq 2 \), then \( G(O_{k,T}) \) satisfies wCSP. More generally, a conjecture of Serre asserts that the group \( G(O_{k,T}) \) has wCSP whenever \( \sum_{v \in T} \text{rk}_{k_v} G \geq 2 \) and \( \text{rk}_{k_v} G \geq 1 \) for any finite place \( v \in T \). This conjecture is known in many cases; see, for example, [19]. In particular, it is known to hold for groups whose \( \mathbb{Q} \) rank is greater than one.

In view of the above, the following theorem implies Theorem A.

**Theorem 4.2.2.** There is a constant \( C \) such that the following holds. For every global field \( k \) of characteristic larger than \( C \), finite set \( T \) of places of \( k \) containing all the archimedean ones, and any natural number \( n \) such that \( \text{Def}_{G_{\mathbb{Q},n}} \) has rational singularities, if \( G(O_{k,T}) \) has wCSP, then \( \alpha(G(O_{k,T})) \leq 2n - 2 \).

Theorem 4.2.2 follows from Theorem B and the following theorem.

**Theorem 4.2.3.** Let \( k \) be a global field and let \( T \) be a finite set of places of \( k \) containing all the archimedean ones. Assume that \( G(O_{k,T}) \) satisfies wCSP, then \( \alpha(G(O_{k,T})) = \alpha(G(\widehat{O_{k,T}})) \).

**Proof.** For any non-archimedean place \( v \) of \( k \), let \( O_v \) be the ring of integers of \( k_v \). By [11, Theorem 5.1 and Proposition 6.6], \( \alpha(G(\mathbb{C})) \leq \alpha(G(O_v)) \), for any non-archimedean place \( v \). By [11, Theorem 3.3] and [13, Lemma 2.2], we get \( \alpha(G(O_{k,T})) = \alpha(G(\widehat{O_{k,T}})) \). \( \square \)
A Kirillov’s Orbit Method for unramified extensions of big pro-$p$ groups

Recall that $G$ is an algebraic group scheme over $\mathbb{Z}$ whose generic fiber is semi-simple together with a fixed embedding $G \hookrightarrow \text{GL}_N$. The following weak version of Theorem 2.5.3 was proved in [3]:

**Theorem A.0.4.** Let $n$ be such that the series defining $\zeta_{G(\mathbb{Z}_q)}(n)$ converges for every prime power $q$. There is a quantifier-free definable function $f : \text{VF}^{\dim G+1} \to \text{VG}$ such that, for every finite extension $L \supset \mathbb{Q}$, there is finite set $S(L)$ of primes of $O_L$ for which

$$\zeta_{G(O_L, q)}(n) - \zeta_{G(O_L / q)}(n) \sim \int_{O_L^{\dim G+1}} q^{f(x)} dx \quad \text{over } q \notin S(L).$$

Theorem 2.5.3 is equivalent to the claim that there is a finite set $S$ of primes in $\mathbb{Z}$ such that, for every $L$, one can take $S(L)$ to be the set

$$\{ q \mid q \cap \mathbb{Z} \in S \text{ or } q \cap \mathbb{Z} \text{ ramifies in } L \}.$$

The argument in [3] gives explicit conditions on the primes $q \notin S(L)$ in Theorem A.0.4. Some of these conditions depend only on $q \cap \mathbb{Z}$ and not on $L$. Another condition is that $q \cap \mathbb{Z}$ is unramified in $L$. The rest of the conditions roughly say that Kirillov’s orbit method holds for some pro-$p$ subgroups of $G(O_L, q)$. In order to formulate these conditions, we will use the following definitions:

**Definition A.0.5.** Let $p$ be a prime, let $q$ be a power of $p$, and let $n$ be a positive integer. Denote the reduction maps $G(\mathbb{Z}_q) \to G(\mathbb{Z}_q / p^n)$ and $\mathfrak{g}(\mathbb{Z}_q) \to \mathfrak{g}(\mathbb{Z}_q / p^n)$ by $\pi_n$ and $\delta_n$ respectively.

1. We denote the kernel of $\pi_n$ by $G(\mathbb{Z}_q)^{(n)}$.
2. We denote the kernel of $\delta_n$ by $\mathfrak{g}(\mathbb{Z}_q)^{(n)}$.
3. Fix a $p$-Sylow subgroup $U \subset G(\mathbb{F}_q)$. We denote the subgroup $\pi_1^{-1}(U)$ by $\text{Syl}(G(\mathbb{Z}_q))$. For almost any $p$, this an Iwahori subgroup of $G(\mathbb{Q}_q)$.

**Definition A.0.6.** Let $q$ be a prime power. We say that $(G, q)$ is a Kirillov pair if the following conditions hold:
1. For every \( g \in \text{Syl}(G(\mathbb{Z}_q)) \), the series
\[
\log(g) := (g - 1) - \frac{1}{2}(g - 1)^2 + \frac{1}{3}(g - 1)^3 - \cdots \tag{15}
\]
converges in \( \mathfrak{gl}_N(\mathbb{Q}_q) \).

2. For every group \( \Lambda \) satisfying \( G(\mathbb{Z}_q)^{(1)} \subset \Lambda \subset \text{Syl}(G(\mathbb{Z}_q)) \), the subset \( \log(\Lambda) \) is a Lie subring of \( \mathfrak{gl}_N(\mathbb{Z}_q) \). Moreover, \( \log \) induces a bijection between the collection of groups \( \Lambda \) satisfying \( G(\mathbb{Z}_q)^{(1)} \subset \Lambda \subset \text{Syl}(G(\mathbb{Z}_q)) \) and the collection of Lie rings \( \lambda \) satisfying \( \log (G(\mathbb{Z}_q)^{(1)} \subset \lambda \subset \log (\text{Syl}(G(\mathbb{Z}_q))) \).

3. For every group \( \Lambda \) satisfying \( G(\mathbb{Z}_q)^{(1)} \subset \Lambda \subset \text{Syl}(G(\mathbb{Z}_q)) \), there is a bijection between irreducible representations of \( \Lambda \) up to conjugation and \( \Lambda \)-orbits in the Pontrjagin dual of the additive group \( \log(\Lambda) \) such that, if a representation \( \rho \) corresponds to an orbit \( \mathcal{O} \), then \( \dim \rho = |\mathcal{O}|^{1/2} \).

We denote the collection of primes powers \( q \) such that \( (G, q) \) is Kirillov by \( \mathcal{K} \).

The proof of Theorem A.0.4 in [3] gives the following

**Theorem A.0.7.** Let \( n \) be such that the series defining \( \zeta_{G(\mathbb{Z}_q)}(n) \) converges for every prime power \( q \). There is a finite set \( S \) of primes and a quantifier-free definable function \( f \) such that
\[
\zeta_{G(\mathbb{Z}_q)}(n) - \zeta_{G(\mathbb{F}_q)}(n) \sim \int_{\mathbb{Z}_q^{\text{dim}G+1}} q^{f(x)} \, dx \quad \text{over } q \in \mathcal{K} \cap \mathcal{P}_S.
\]

Hence, in order to prove Theorem 2.5.3, it is enough to prove the following:

**Theorem A.0.8.** There is a finite set \( S \) of prime numbers such that \( \mathcal{P}_S \subset \mathcal{K} \).

We prove Theorem A.0.8 in the next two subsections.

### A.1 Kirillov’s Orbit Method

We first note that, if \( g \in \text{Syl}(G(\mathbb{Z}_q)) \), then the reduction of \( g - 1 \) to \( \mathfrak{gl}_N(\mathbb{F}_q) \) is nilpotent. In particular, \( \text{val}_{\mathbb{Q}_q}((g - 1)^n) \geq \left\lceil \frac{n}{N} \right\rceil \). Hence, Condition 1. in Definition A.0.6 holds for every prime power \( q \). A standard argument shows that \( \log(g) \in \mathfrak{g}(\mathbb{Q}_q) \).

The following Lemma is standard

**Lemma A.1.1.** There is a finite set \( S \) of primes such that, for all \( q \in \mathcal{P}_S \),

24
1. For every $g \in \text{Syl}(G(\mathbb{Z}_q))$ and every $n$, we have $\frac{1}{n}(g - 1)^n \in \mathfrak{gl}_N(\mathbb{Z}_q)$, and, therefore, $\log(\text{Syl}(G(\mathbb{Z}_q))) \subseteq \mathfrak{gl}_N(\mathbb{Z}_q)$. Since the reductions of $\frac{1}{n}(g - 1)^n$ are commuting nilpotents, we get that the reductions of each element of $\log(\text{Syl}(G(\mathbb{Z}_q)))$ to $\mathfrak{gl}_N(\mathbb{F}_q)$ is nilpotent.

2. The series defining $\exp$ converges on $\log(\text{Syl}(G(\mathbb{Z}_q)))$ and is an inverse function to $\log$.

3. For every $g \in \text{Syl}(G(\mathbb{Z}_q))$ and $n \in \mathbb{N}$, the functions $\exp$ and $\log$ are inverse bijections between the cosets $gG(\mathbb{Z}_q)^{(n)}$ and $\log(g) + g(\mathbb{Z}_q)^{(n)}$.

Recall that the Campbell–Hausdorff formula is the formal Lie series equality

$$\log (\exp(X) \cdot \exp(Y)) = CH_1(X, Y) + CH_2(X, Y) + \cdots$$  \hspace{1cm} (16)

where $CH_i$ is some homogeneous Lie polynomial of degree $i$ with coefficients in $\mathbb{Q}$. For example, $CH_1(X,Y) = X + Y$, $CH_2(X,Y) = \frac{1}{2}[X,Y]$, and $CH_3(X,Y) = \frac{1}{12}([X,[X,Y]] - [Y,[X,Y]])$.

**Definition A.1.2.** Fix a prime $p$ and a natural number $i$.

1. Let $A_i$ be the $\mathbb{Q}$-vector space of non-associative polynomials of degree $i$ in two variables $X,Y$. For an element $P \in A_i$, let $\text{val}_p(P)$ be the minimum of the $p$-adic valuations of the coefficients of $P$.

2. Let $L_i$ be the $\mathbb{Q}$-vector space of Lie polynomials of degree $i$ in $X,Y$. We have a natural surjection $\sigma : A_i \rightarrow L_i$. Given $\Phi \in L_i$, let $\text{val}_p(\Phi) = \max \{ \text{val}_p(P) \mid \sigma(P) = \Phi \}$.

**Lemma A.1.3** ([5, Page 123]). For any prime $p > 2$, $\text{val}_p(CH_i) \geq \frac{i-1}{p-1}$.

Lemma A.1.3 implies that, after possibly enlarging $S$, the series in (16) converge.

**Lemma A.1.4.** Suppose that $p > N$, $p \notin S$, and $q$ is a power of $p$. Then

1. If $g,h \in \text{Syl}(G(\mathbb{Z}_q))$, then there is $x \in \langle g,h \rangle G(\mathbb{Z}_q)^{(1)}$ such that $g^p h^p = x^p$ modulo $G(\mathbb{Z}_q)^{(2)}$.

2. If $g,h \in \text{Syl}(G(\mathbb{Z}_q))$ satisfy $g^p h^p = x^p$ modulo $G(\mathbb{Z}_q)^{(2)}$, then $\log(g) + \log(h) = \log(x)$ modulo $p$.

3. If $G(\mathbb{Z}_q)^{(1)} \subset \Lambda \subset \text{Syl}(G(\mathbb{Z}_q))$ is a group, then $\log(\Lambda)$ is an additive subgroup of $g(\mathbb{Z}_q)$. 

25
Proof.

1. The group $\langle g, h \rangle G^{(1)}(\mathbb{Z}_q)/G^{(2)}(\mathbb{Z}_q)$ is a $p$-group of exponent $N < p$. Hence, it is regular (see [7]), so the result holds.

2. Let $g^ph^p = x^py$ with $y \in G^{(2)}(\mathbb{Z}_q)$. Let $A = \log(g), B = \log(h), C = \log(x)$. By Lemma A.1.1, there is $D \in \mathfrak{g}(\mathbb{Z}_q)^{(1)}$ such that $y = \exp(pD)$. We have

$$e^{pA}e^{pB} = e^{pC}e^{pD},$$

so, by Campbell–Hausdorff,

$$pA + pB \equiv pC + pD \pmod{p^2},$$

which implies the claim, as $p|D$.

3. Given $g, h \in \Lambda$, the previous claims imply that there is $x \in \Lambda$ such that $\log(g) + \log(h) \in \log(x) + \mathfrak{g}(\mathbb{Z}_q)^{(1)}$. By Lemma A.1.1, there is $y \in xG(\mathbb{Z}_q)^{(1)} \subset \Lambda$ such that $\log(y) = \log(g) + \log(h)$.

\[\]

We now show that Condition 2. in Definition A.0.6 holds. By [17, Lemma 1.6] and Lemma A.1.4, we get that $\log \Lambda$ is a Lie subring of $\mathfrak{g}(\mathbb{Z}_q)$. Conversely, if $\lambda \subseteq \log(Syl(G(\mathbb{Z}_q)))$ is a Lie subring, then the Campbell–Hausdorff formula implies that $\exp(\lambda)$ is a group.

Definition A.1.5.

1. Let $\Lambda$ be a pro-finite group. We denote the collection of locally constant complex valued functions on $\Lambda$ by $S(\Lambda)$. The vector space $S(\Lambda)$ is a ring under convolution (with respect to the normalized Haar measure).

2. Let $\Lambda$ be a pro-finite group, and let $\Delta$ be a group acting on $\Lambda$ by automorphisms. We denote the collection of $\Delta$-invariant complex-valued locally constant functions on $\Lambda$ by $S(\Lambda)^\Delta$. It is also a ring under convolution.

The core of the Kirillov orbit method is the following theorem which we prove in the next subsection.
Theorem A.1.6. There is a finite set $S$ of primes such that, for every $q \in \mathcal{P}_S$ and every subgroup $G(Z_q)^{(1)} \subset \Lambda \subset \text{Syl}(G(Z_q))$, the map

$$\log^* : \mathcal{S}(\log(\Lambda))^\Lambda \to \mathcal{S}(\Lambda)^\Lambda$$

is an isomorphism of convolution algebras. Here, $\Lambda$ acts on itself and on $\log(\Lambda)$ by the adjoint actions.

The following Corollary of Theorem A.1.6 implies Theorem A.0.8:

Corollary A.1.7. There is a finite set $S$ of primes such that, for every $q \in \mathcal{P}_S$ and every subgroup $G(Z_q)^{(1)} \subset \Lambda \subset \text{Syl}(G(Z_q))$, there is a bijection between irreducible representations of $\Lambda$ and $\Lambda$-orbits in the Pontrjagin dual of the additive group $\log(\Lambda)$ such that, if a representation $\rho$ corresponds to an orbit $O$, then, for every $g \in \Lambda$,

$$\chi_\rho(g) = \frac{1}{|O|^{1/2}} \sum_{\psi \in O} \psi(\log g).$$

Proof. It is easily seen that the functions $\frac{1}{|O|^{1/2}} \sum_{\psi \in O} \psi$ are the indecomposable idempotents of $\mathcal{S}(\log(\Lambda))^\Lambda$. Hence, their compositions with log are the minimal idempotents of $\mathcal{S}(\Lambda)^\Lambda$, i.e. the functions $\frac{1}{(\dim \pi)^{1/2}} \chi_\pi$ for $\pi \in \text{Irr} \Lambda$. \qed

A.2 Proof of Theorem A.1.6

Our argument follows [4]. We start by establishing a formal identity between Lie series. Let $\mathcal{L} = \oplus \mathcal{L}_i$ be the free Lie algebra over $\mathbb{Q}$ on two generators, $X$ and $Y$ graded by degree. We denote the completion of $\mathcal{L}$ with respect to this grading by $\hat{\mathcal{L}}$. If $\Phi(X,Y) \in \hat{\mathcal{L}}$, we write $\Phi(X,Y) = \Phi_1(X,Y) + \Phi_2(X,Y) + \cdots$, where $\Phi_n(X,Y) \in \mathcal{L}$ is homogeneous of degree $n$. The composition map $\mathcal{L} \times \mathcal{L} \times \mathcal{L} \to \mathcal{L}$ sending $(\Phi(X,Y), \Psi_1(X,Y), \Psi_2(X,Y))$ to $\Phi(\Psi_1(X,Y), \Psi_2(X,Y))$ extends to $\hat{\mathcal{L}}$ by continuity.

Define the element $X^Y \in \hat{\mathcal{L}}$ by

$$X^Y := \exp(\text{ad}(Y)) \cdot X = X + [Y,X] + \frac{1}{2!}[Y,[Y,X]] + \frac{1}{3!}[Y,[Y,[Y,X]]] + \cdots \in \hat{\mathcal{L}}.$$

Proposition A.2.1. There are $\Phi(X,Y), \Psi(X,Y) \in \hat{\mathcal{L}}$ such that,

1. $\text{val}_p(\Phi_n), \text{val}_p(\Psi_n) \geq -\frac{2n-2}{p-1}$.

2. $\text{CH}_1(X,Y) + \text{CH}_2(X,Y) + \cdots = X^{\Phi(X,Y)} + Y^{\Psi(X,Y)}$. 

27
Proof. We construct \( \Phi_n \) and \( \Psi_n \) recursively in \( n \), starting from \( \Phi_1(X,Y) = -\frac{1}{4}Y \) and \( \Psi_1(X,Y) = \frac{1}{4}X \). For \( n \geq 2 \), the degree \( n + 1 \) terms in Condition 2 are

\[
\text{CH}_{n+1}(X,Y) = [\Phi_n(X,Y), X] + \sum_{k=2}^{n} \frac{1}{k!} [\Phi_{j_1}, \cdots [\Phi_{j_k}, X] \cdots ] + [\Psi_n(X,Y), Y] + \sum_{k=2}^{n} \frac{1}{k!} [\Psi_{j_1}, \cdots [\Psi_{j_k}, Y] \cdots ],
\]

where the inner summations are over \( j_1, \ldots, j_k \) satisfying \( j_1 + \cdots + j_k = n \). By induction,

\[
\text{val}_p \left( \frac{1}{k!} [\Phi_{j_1}, \cdots [\Phi_{j_k}, X] \cdots ] \right) \geq -\frac{k}{p-1} - \frac{2(j_1 + \cdots + j_k) - 2k}{p-1} = -\frac{2n - k}{p-1} \geq -\frac{2n}{p-1},
\]

and

\[
\text{val}_p(\text{CH}_{n+1}) \geq -\frac{n}{p-1} \geq -\frac{2n}{p-1}.
\]

This implies that we can write (17) as

\[
[\Phi_n(X,Y), X] + [\Psi_n(X,Y), Y] = \Xi,
\]

where \( \Xi \in \mathcal{L} \) is an homogeneous element of degree \( n + 1 \) with valuation at least \(-\frac{2n}{p-1}\).

The proposition follows from the following Lemma. \( \square \)

**Lemma A.2.2.** Let \( \mathcal{L}_{n,\mathbb{Z}} \) be the collection of homogeneous Lie polynomials of degree \( n \) with integral coefficients. For any \( n \geq 2 \) and \( \Xi \in \mathcal{L}_{n,\mathbb{Z}} \), there are \( \Phi, \Psi \in \mathcal{L}_{n-1,\mathbb{Z}} \) such that \( \Xi = [\Phi, X] + [\Psi, Y] \).

**Proof.** We can assume that \( \Xi \) is a represented by a monomial, \( \Xi = [\Theta, \Theta'] \), where \( \Theta, \Theta' \) are lower-degree monomials. The proof is by induction on \( n \) and \( \deg(\Theta') \). The cases \( n = 2 \) or \( \deg(\Theta_2) = 1 \) are clear. For the induction step, the induction hypothesis implies that we can write \( \Theta' = [\Upsilon_1, X] + [\Upsilon_2, Y] \), so it is enough to prove the claim assuming \( \Xi = [\Theta, [\Upsilon, X]] \). By Jacobi identity, \( [\Theta, [\Upsilon, X]] = [[\Theta, \Upsilon], X] - [[\Theta, X], \Upsilon] \). The first term has the desired form, and we can use induction on the second term, since \( \deg(\Upsilon) = \deg(\Theta') - 1 \). \( \square \)

**Definition A.2.3.** An element \( \Phi \in \hat{\mathcal{L}} \) has slope \( \geq k \) if \( \text{val}_p(\Phi_n) \geq -\lfloor \frac{p}{k} \rfloor \).

**Lemma A.2.4.** Let \( \Phi \in \hat{\mathcal{L}} \). If \( \Phi \) has slope \( \geq k \), then \( X^\Phi \) has slope \( \geq \frac{k}{2} \min \{k, p-1\} \).
Proof. It is enough to show that, for any \( k \), the element \( \frac{1}{k!}[\Phi, [\Phi, \cdots [\Phi, X] \cdots ]] \) has slope \( \geq \max\{k, p-1\} \). The degree \( n \) homogenous part of \( \frac{1}{k!}[\Phi, [\Phi, \cdots [\Phi, X] \cdots ]] \) is a sum of elements of the form \( \frac{1}{k!}[\Phi_{j_1}, [\Phi_{j_2}, \cdots [\Phi_{j_k}, X] \cdots ]] \), where \( j_1 + \cdots + j_k = n - 1 \). By the assumptions, 
\[
\text{val}_p \left( \frac{1}{k!}[\Phi_{j_1}, [\Phi_{j_2}, \cdots [\Phi_{j_k}, X] \cdots ]] \right) \geq -\frac{k}{p-1} - \sum \left\lfloor \frac{j_i}{k} \right\rfloor \geq -\frac{n-1}{p-1} - \frac{n-1}{k} \geq \frac{2n}{\max\{k, p-1\}}.
\]

\( \Box \)

Example A.2.5. The series \( \Phi(X, Y), \Psi(X, Y) \) from Proposition A.2.1 have slopes \( \geq \frac{p-1}{2} \) and the series \( X^\Phi \) and \( Y^\Psi \) have slopes \( \geq \frac{p-1}{4} \).

Definition A.2.6. Let \( \lambda \) be a torsion-free \( \mathbb{Z}_p \)-module together with a Lie bracket. We say that \( \lambda \) is \( k \)-powerful if \( [\lambda, k\lambda] := [\lambda, [\lambda, \cdots ]] \subset p\lambda \).

Lemma A.2.7. There is a finite set \( S \) of primes such that, for any \( q \in \mathcal{P}_S \) and any \( G^{(1)}(\mathbb{Z}_q) \subset \Lambda \subset \text{Syl}(G(\mathbb{Z}_q)) \), the Lie ring \( \log(\Lambda) \) is \( 3N \)-powerful.

Proof. Choose \( S \) such that Lemmas A.1.1 and A.1.4 hold for any \( q \in \mathcal{P}_S \). Let \( \lambda = \log(\Lambda) \) and \( \Lambda = \lambda/\mathfrak{gl}^{(1)}(\mathbb{Z}_q) \subset \mathfrak{gl}_N(\mathbb{F}_q) \). Since \( \Lambda \) is nilpotent, we get that \( [\Lambda, \lambda] = 0 \) and \( [\Lambda, 2\mathfrak{gl}_N(\mathbb{F}_q)] = 0 \). Hence, 
\[
[\lambda, 3N\lambda] \subset [\lambda, 2N\mathfrak{gl}(\mathbb{Z}_q)] \cap \lambda \subset p\mathfrak{gl}_N(\mathbb{Z}_q) \cap \lambda \subset p\lambda.
\]

\( \Box \)

Suppose that \( \lambda \) is \( k \)-powerful. Consider the filtration
\[
\lambda \supset \lambda, \lambda + p\lambda \supset \cdots \supset \lambda, p\lambda \supset p\lambda \supset p(\lambda, \lambda + p\lambda) \supset \cdots
\]
i.e. define \( \mathcal{F}^{nk+b} \lambda = p^b ([\lambda, \lambda] + p\lambda) \) for \( b \in \{0, \ldots, k-1\} \). The following are easy to verify:
\[
[\mathcal{F}^i\lambda, \mathcal{F}^j\lambda] \subset \mathcal{F}^{i+j}\lambda \quad [\lambda, \mathcal{F}^i\lambda] \subset \mathcal{F}^{i+1}\lambda \quad (18)
\]

Proposition A.2.8. Let \( \lambda \) be \( k \)-powerful.

1. Assume that \( \Phi \in \widehat{\mathcal{L}} \) has slope \( \geq 2k \). Then, for any \( x, y \in \lambda \),
   \( (a) \) \( \Phi_n(x, y) \in \lambda \).
   \( (b) \) The series \( \Phi(x, y) \) converges and its limit is in \( \lambda \).
   \( (c) \) If \( z, w \in \mathcal{F}^i\lambda \) then \( \Phi(x + z, y + w) - \Phi(x, y) \equiv \Phi_1(x + z, y + w) - \Phi_1(x, y) \mod \mathcal{F}^{i+1}\lambda \).
2. Assume that $\Phi, \Psi \in \hat{L}$ have slopes $\geq k$ and that $\Phi_1(X, Y) = X, \Psi_1(X, Y) = Y$. Then the map $(\Phi, \Psi) : \lambda \times \lambda \rightarrow \lambda \times \lambda$ is measure preserving homeomorphism.

Proof.

1. Suppose that $P(X, Y) \in L$ is homogeneous of degree $n$ and has integral coefficients. If $x, y \in \lambda$, Equation (18) implies that $P(x, y) \in F^{n-1} \lambda$. Since $\Phi$ has slope $\geq 2k$, we get that $\Phi(x, y) \in F^{n-1-k[n/2k]} \lambda$, proving (1a) and (1b).

For $P(X, Y)$ as above, if $x, y \in \lambda$ and $z, w \in F^i \lambda$, then $P(x + z, y + w) - P(x, y) \in F^{i+1} \lambda$. Since $\Phi$ has slope $\geq 2k$, we get that, for $n > 1$,

$$\Phi_n(x + z, y + w) - \Phi_n(x, y) \in F^{i+n-1-k[n/2k]} \lambda \subset F^{i+1} \lambda,$$

proving (1b).

2. By the previous claims, for any $i$, the map $(\Phi, \Psi)$ descends to a map from $(\lambda/F^i \lambda) \times (\lambda/F^i \lambda)$ to itself. We show by induction on $i$ that this map is injective. This will prove claim (2). The case $i = 1$ is clear. For $i > 1$, if $(\Phi(x, y), \Psi(x, y)) = (\Phi(x', y'), \Psi(x', y'))$, the induction hypothesis implies that $x - x', y - y' \in F^{i-1} \lambda$, but then

$$0 = (\Phi(x, y), \Psi(x, y)) - (\Phi(x', y'), \Psi(x', y')) \equiv (x - x', y - y') \mod F^i \lambda.$$

We can now prove Theorem A.1.6

Proof. Let $S$ be a set of primes containing all primes up to $24N + 1$ and such that such that Lemmas A.1.1, A.1.4, and A.2.7 hold for $q \in P_S$. Denote $\lambda = \log(\Lambda)$. For $x, y \in \lambda$, let $x \circ y = \log(\exp(x) \cdot \exp(y))$. The pair $(\lambda, \circ)$ is a group isomorphic to $(\Lambda, \cdot)$. The two operations, $+, \circ$ give two convolutions $\ast, \circledast$ on $S(\lambda)$. In order to prove Theorem A.1.6, it is enough to show that the identity map $(S(\lambda)^{\lambda}, \ast) \rightarrow (S(\lambda)^{\lambda}, \circledast)$ is an isomorphism.

Let $\Phi(X, Y), \Psi(X, Y)$ be the Lie series from Proposition A.2.1. By our assumptions and Example A.2.5, $X^\Phi$ and $Y^\Psi$ have slopes $\geq 6N$. By Lemma A.2.7 and Proposition A.2.8, the map $T : \lambda \times \lambda \rightarrow \lambda \times \lambda$ given by $T(x, y) = (x^{\Phi(x, y)}, y^{\Psi(x, y)})$ is a well-defined measure-preserving homeomorphism. For every $z \in \lambda$, the restriction of $T$ to $\{(x, y) \in \lambda^2 \mid x \circ y = z\}$ is a bijection with $\{(x, y) \in \lambda^2 \mid x + y = z\}$. Hence, for every $f, g \in S(\lambda)^{\lambda}$ and $z \in \lambda,$
\[ f \ast g(z) = \int_{\{(x,y) | x \cdot y = z\}} f(x)g(y) = \int_{\{(x,y) | x + y = z\}} f(x)g(y^{\Psi(x,y)}) = \]
\[ = \int_{\{(x,y) | x + y = z\}} f(x)g(y) = f \ast g(z). \]

References


31


