INDUCING SUPER-APPROXIMATION.

ALIREZA SALEHI GOLSEFIDY AND XIN ZHANG

Abstract. Let $\Gamma_2\subseteq\Gamma_1$ be finitely generated subgroups of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$. For $i=1$ or 2, let $\mathbb{G}_i$ be the Zariski-closure of Γ_i in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$, $\mathbb{G}_i^\circ$ be the Zariski-connected component of $\mathbb{G}_i$, and let G_i be the closure of Γ_i in $\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$.

In this article we prove that, if $\mathbb{G}_1^\circ$ is the smallest closed normal subgroup of $\mathbb{G}_1^\circ$ which contains $\mathbb{G}_2^\circ$ and $\Gamma_2\curvearrowright G_2$ has spectral gap, then $\Gamma_1\curvearrowright G_1$ has spectral gap.

1. Introduction and the statement of the main results.

Let Γ be a subgroup of a compact, Hausdorff, second countable group G. Let $\overline{\Gamma}$ be the closure of Γ in G. Suppose Ω is a finite symmetric generating set of Γ. Let $\mathcal{P}_\Omega$ be the probability counting measure on Ω, and let

$$T_\Omega:L^2(\overline{\Gamma})\to L^2(\overline{\Gamma}),\ T_\Omega(f):=\mathcal{P}_\Omega*f:=\frac{1}{|\Omega|}\sum_{\omega\in\Omega}L_\omega(f),$$

where $L_\omega(f)(g):=f(\omega^{-1}g)$. Then it is well-known that T_Ω is a self-adjoint operator, $T_\Omega(\mathbb{1}_{\overline{\Gamma}})=\mathbb{1}_{\overline{\Gamma}}$ where $\mathbb{1}_{\overline{\Gamma}}$ is the constant function on $\overline{\Gamma}$, and the operator norm $\|T_\Omega\|$ is 1. So the spectrum of T_Ω is a subset of $[-1,1]$ and T_Ω sends the space $L^2(\overline{\Gamma})^\circ$ orthogonal to the constant functions to itself. Let T_Ω° be the restriction of T_Ω to $L^2(\overline{\Gamma})^\circ$. Let

$$\lambda(\mathcal{P}_\Omega;G):=\sup\{|c||\ c \text{ is in the spectrum of the restriction of } T_\Omega^\circ\}.$$

We say the left action $\Gamma\curvearrowright G$ of Γ on G has *spectral gap* if $\lambda(\mathcal{P}_\Omega;G)<1$.

It is worth mentioning that, if Ω_1 and Ω_2 are two generating sets of Γ and $\lambda(\mathcal{P}_{\Omega_1};G)<1$, then $\lambda(\mathcal{P}_{\Omega_2};G)<1$. So having spectral gap is a property of the action $\Gamma\curvearrowright G$, and it is independent of the choice of a generating set for Γ.

The following is the main theorem of this article.

Theorem 1. *Let $\Gamma_2\subseteq\Gamma_1$ be two finitely generated subgroups of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$. For $i=1,2$, let $\mathbb{G}_i$ be the Zariski-closure of Γ_i in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$ for $i=1,2$, and let $\mathbb{G}_i^\circ$ be the Zariski-connected subgroup of $\mathbb{G}_i$. Suppose the smallest closed normal subgroup of $\mathbb{G}_1^\circ$ which contains $\mathbb{G}_2^\circ$ is $\mathbb{G}_1^\circ$. Then, if $\Gamma_2\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap, then $\Gamma_1\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap.*

Corollary 2. *Let $\Gamma_2\subseteq\Gamma_1$ be two finitely generated subgroups of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$. Let $\mathbb{G}_1$ be the Zariski-closure of Γ_1 in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$, and let $\mathbb{G}_1^\circ$ be the Zariski-connected subgroup of $\mathbb{G}_1$. Suppose $\mathbb{G}_1^\circ$ is an almost $\mathbb{Q}$-simple $\mathbb{Q}$-group, and Γ_2 is an infinite group. Then, if $\Gamma_2\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap, then $\Gamma_1\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap.*

Proof. Since Γ_2 is infinite, the Zariski-connected component $\mathbb{G}_2^\circ$ of the Zariski-closure $\mathbb{G}_2$ of Γ_2 in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$ is a non-trivial (Zariski-connected) $\mathbb{Q}$-subgroup of $\mathbb{G}_1^\circ$. Since $\mathbb{G}_1^\circ$ is an almost $\mathbb{Q}$-simple group and $\mathbb{G}_2^\circ$ is a

Date: 12/26/2016.
1991 *Mathematics Subject Classification.* Primary: 22E40, Secondary: 20G35, 05C25.
A. S-G. was partially supported by the NSF grants DMS-1303121 and DMS-1602137, and A. P. Sloan Research Fellowship.

non-trivial Zariski-connected $\mathbb{Q}$-subgroup of $\mathbb{G}_1^\circ$, the smallest normal subgroup of $\mathbb{G}_1^\circ$ which contains $\mathbb{G}_2^\circ$ is $\mathbb{G}_1^\circ$. And so by Theorem 1 claim follows. □

Notice that the smallest closed normal subgroup of $\mathbb{G}_1^\circ$ which contains $\mathbb{G}_2^\circ$ is $\mathbb{G}_1^\circ$ if and only if the restriction of any non-trivial representation $\rho : \mathbb{G}_1^\circ \to (\mathrm{GL}_m)_{\mathbb{Q}}$ to $\mathbb{G}_2^\circ$ is still non-trivial.

Remark 3. *The first result of this kind goes back to the work of Burger and Sarnak* [BS911]. *Their result implies Theorem 1 when Γ_i's are integral points of (fixed embeddings of) two Zariski-connected semisimple $\mathbb{Q}$-groups $\mathbb{G}_i$'s.*

Theorem 1 has an immediate application in explicit construction of expanders. Let us quickly recall that a family of d-regular graphs X_i is called a family of expanders if the size of vertices $|V(X_i)|$ goes to infinity and there is a positive number δ_0 such that for any subset A of $V(X_i)$ we have

$$\frac{|e(A, V(X_i) \setminus A)|}{\min(|A|, |V(X_i) \setminus A|)} > \delta_0,$$

where $e(A, B)$ is the set of edges that connect a vertex in A to a vertex in B. Expanders have a lot of applications in theoretical computer science (see [HLW06] for a survey on such applications).

It is well-known that Theorem 1 is equivalent to the following theorem (see [SG16, Remark 15] or [Lub94, Section 4.3])

Theorem 1′. *Let Ω_1 and Ω_2 be two finite symmetric subsets of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$. For $i = 1, 2$, let Γ_i be the group generated by Ω_i, and $\mathbb{G}_i^\circ$ be the Zariski-connected component of the Zariski-closure of Γ_i in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$. Suppose $\Gamma_2 \subseteq \Gamma_1$ and the normal closure of $\mathbb{G}_2^\circ$ in $\mathbb{G}_1^\circ$ is $\mathbb{G}_1^\circ$. Then if the family of Cayley graphs $\{\mathrm{Cay}(\pi_q(\Gamma_2), \pi_q(\Omega_2)\}_{\gcd(q,q_0)=1}$ is a family of expanders, then $\{\mathrm{Cay}(\pi_q(\Gamma_1), \pi_q(\Omega_1)\}_{\gcd(q,q_0)=1}$ is a family of expanders.*

Definition 4. *Let Ω be a finite symmetric subset of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$. We say that the group $\Gamma = \langle \Omega \rangle$ generated by Ω has super-approximation with respect to a subset C of positive integers if the family of Cayley graphs $\{\mathrm{Cay}(\pi_m(\Gamma), \pi_m(\Omega)\}_{m \in C}$ is a family of expanders.*

We simply say $\Gamma \subseteq \mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$ has super-approximation if it has super-approximation with respect to $\{q \in \mathbb{Z}^+ |\, \gcd(q, q_0) = 1\}$.

In the past decade there has been a surge in proving that super-approximation is a Zariski-topological property (see [BG08-a]-[BV12] and [SG16]-[SGV12]). By now we know that

(1) A finite generated Zariski-dense subgroup of $\mathrm{SL}_{n_0}(\mathbb{Z})$ has super-approximation with respect to $\mathbb{Z}^+$ (see [BV12, Theorem 1]).
(2) A finitely generated subgroup Γ of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$ has super-approximation with respect to
$$\{q^{m_0} |\, q \text{ is a square-free integer }, \gcd(q, q_0) = 1\}$$
if and only if $\mathbb{G}^\circ = [\mathbb{G}^\circ, \mathbb{G}^\circ]$ where $\mathbb{G}^\circ$ is the Zariski-connected component of the Zariski-closure of Γ. (see [SGV12, Theorem 1] and [SG, Theorem 1]).
(3) A finitely generated subgroup Γ of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$ has super-approximation with respect to
$$\{p^n |\, n \in \mathbb{Z}^+, p \text{ is a prime which does not divide } q_0\}$$
if and only if $\mathbb{G}^\circ = [\mathbb{G}^\circ, \mathbb{G}^\circ]$ where $\mathbb{G}^\circ$ is the Zariski-connected component of the Zariski-closure of Γ. (see [SG, Theorem 1]).

The following is the main conjecture on this subject.

Conjecture 5. *A finitely generated subgroup Γ of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$ has super-approximation if and only if $\mathbb{G}^\circ = [\mathbb{G}^\circ, \mathbb{G}^\circ]$ where $\mathbb{G}^\circ$ is the Zariski-connected component of the Zariski-closure of Γ.*

Relaxing the condition on the set of possible residues is crucial in some of the results where super-approximation is used in combination with *large sieve* or *thermodynamical* techniques (for instance see [BK14, BKM, MOW]).

Theorem 1 is about inducing super-approximation property from a subgroup with *large* Zariski-closure to the group itself. So since we know (infinite) arithmetic groups in semisimple $\mathbb{Q}$-groups, i.e. $\mathbb{Z}[1/q_0]$-points in a semisimple $\mathbb{Q}$-group, have super-approximation, we get the following corollary.

Corollary 6. *Let Γ be a finitely generated subgroup of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$. Suppose the Zariski-closure of Γ in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$ is an almost $\mathbb{Q}$-simple group. Suppose further that Γ contains an infinite arithmetic subgroup of some semisimple group. Then Γ has super-approximation.*

Using the mentioned result of Bourgain and Varjú [BV12, Theorem 1], we get the following corollary of Theorem 1.

Corollary 7. *Let Γ be a finitely generated subgroup of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$. Suppose the Zariski-closure of Γ in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$ is an almost $\mathbb{Q}$-simple group. Suppose further that there is a subgroup $\Lambda \subseteq \Gamma \cap \mathrm{GL}_{n_0}(\mathbb{Z})$ whose Zariski-closure is isomorphic to $(\mathrm{SL}_m)_{\mathbb{Q}}$ for some positive integer m. Then Γ has super-approximation.*

Proof. Let $\mathbb{H}$ be the Zariski-closure of Λ in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$. By the assumption, there is a $\mathbb{Q}$-isomorphism $\rho : \mathbb{H} \to (\mathrm{SL}_m)_{\mathbb{Q}}$. By [SG, Lemma 13], there is $g \in \mathrm{SL}_m(\mathbb{Q})$ such that $\rho(\Lambda) \subseteq g\,\mathrm{SL}_m(\mathbb{Z})g^{-1}$. And so $g^{-1}\rho(\Lambda)g$ is a finitely generated Zariski-dense subgroup of $\mathrm{SL}_m(\mathbb{Z})$. Hence by [BV12, Theorem 1] and [SG16, Remark 15] we have that $g^{-1}\rho(\Lambda)g \curvearrowright \prod_p \mathrm{SL}_m(\mathbb{Z}_p)$ has spectral gap.

Now let $\overline{\Lambda}$ be the closure of Λ in $\prod_p \mathrm{GL}_{n_0}(\mathbb{Z}_p)$, and let $\mathbb{A}$ be the ring of adeles of $\mathbb{Q}$. Since ρ induces a topological isomorphism $\rho : \mathbb{H}(\mathbb{A}) \to \mathrm{SL}_m(\mathbb{A})$, $g^{-1}\rho(\overline{\Lambda})g$ is the closure of $g^{-1}\rho(\Lambda)g$ in $\prod_p \mathrm{SL}_m(\mathbb{Z}_p)$. Since $g^{-1}\rho(\Lambda)g \curvearrowright \prod_p \mathrm{SL}_m(\mathbb{Z}_p)$ has spectral gap, we get that $\rho(\Lambda) \curvearrowright \rho(\overline{\Lambda})$ has spectral gap. And so $\Lambda \curvearrowright \overline{\Lambda}$ has spectral gap. Therefore by Theorem 1 and [SG16, Remark 15] the claim follows. ☐

This kind of result was first obtained by Varjú in the appendix of [BK14] where he proved a special case of Corollary 6 for the group of symmetries of an Apollonian packing. More recently in [FSZ, Theorem 1.3] a special case of Corollary 7 is proved where the Zariski-closure of Γ is assumed to be isomorphic to the restriction of scalars $R_{k/\mathbb{Q}}((\mathrm{SL}_2)_{\mathbb{Q}})$ of $(\mathrm{SL}_2)_{\mathbb{Q}}$ for a finite extension $k/\mathbb{Q}$.

1.1. **Outline of the proof.** Here is an outline of the main ideas of the proof.

Step 0. (Initial preparation) Preliminary reductions: it is showed that one can essentially work under the extra assumptions that the Zariski-closure $\mathbb{G}_i$ of Γ_i in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$ is Zariski-connected for $i = 1, 2$; and $\mathbb{G}_1$ is simply-connected (see Section 8).

Step 1. (Reduction to an Adelic Bounded Generation) Using Varjú's Lemma [BK14, Lemma A.2] and [SG16, Lemma 16], the proof of Theorem 1 is reduced to an adelic bounded generation statement (see Theorem 27). The following is a variant of [BK14, Lemma A.2].

Lemma 8 (Varjú's Lemma)**.** *Suppose G is a finite group, H is a subgroup of G, and*

$$G = g_1 H g_1^{-1} \cdot g_2 H g_2^{-1} \cdots g_n H g_n^{-1}$$

for some $g_i \in G$. Let Ω be a symmetric generating set of H. Then

$$\lambda(\mathcal{P}_{\Omega'}; G) \le f(|\Omega|, \lambda(\mathcal{P}_\Omega; H), n) < 1,$$

where $\Omega' := \bigcup_{i=1}^n g_i \Omega g_i^{-1}$ and $f : \mathbb{Z}^+ \times [0,1] \times \mathbb{Z}^+ \to [0,1)$.

By [SG16, Lemma 16], it is enough to get a spectral gap for a subgroup of finite index. Hence altogether it is enough to prove the following (see Theorem 27):

Adelic Bounded Generation: *there are* $\gamma_1, \ldots, \gamma_m \in \Gamma_1$ *such that* $\gamma_1 \widehat{\Gamma}_2 \gamma_1^{-1} \cdots \gamma_m \widehat{\Gamma}_2 \gamma_m^{-1}$ *is an open subgroup of* $\widehat{\Gamma}_1$ *where* $\widehat{\Gamma}_i$ *is the closure of* Γ_i *in* $\prod_{p \nmid q_0} \mathrm{GL}_{n_0}(\mathbb{Z}_p)$.

To get the above mentioned Adelic Bounded Generation result, we prove many bounded generation results from various angles: Lie algebras; Zariski topology; and p-adic topology (with certain uniformity on p). Here is a bit more detailed description of these steps.

Step 2. (Generating the Lie algebra) We prove that $\mathrm{Lie}(\mathbb{G}_2)(\mathbb{Q})$ generates $\mathrm{Lie}(\mathbb{G}_1)(\mathbb{Q})$ as a Γ_1-module.

Step 3. (Bounded Generation: Zariski topology) The infinitesimal result proved in the previous step shows that $(g_1, \ldots, g_n) \mapsto \gamma_1 g_1 \gamma_1^{-1} \cdots \gamma_n g_n \gamma_n g^{-1}$ is a geometrically dominant morphism from $\mathbb{G}_2 \times \cdots \times \mathbb{G}_2$ to $\mathbb{G}_1$ for suitable γ_i's in Γ_1. Looking at the scheme theoretic closure of Γ_i, we deduce that for almost all the geometric fibers $\mathbb{G}_i^{(p)}$ we still get dominant morphisms (see Proposition 18).

Step 4. (Bounded Generation: p-adic topology) Based on a quantitative open function theorem for p-adic analytic functions proved in [SG, Lemma 45'], we show the following p-adic topological bounded generation with certain uniformity on p (see Proposition 20):

there are a positive integer N *and* $\gamma_1, \ldots, \gamma_n \in \Gamma_1$ *such that* $\Gamma_{1,p}[p^N] \subseteq \gamma_1 \Gamma_{2,p} \gamma_1^{-1} \cdots \gamma_n \Gamma_{2,p} \gamma_n^{-1}$ *where* $\Gamma_{i,p}$ *is the closure of* Γ_i *in* $\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ *and* $\Gamma_{1,p}[p^N] := \Gamma_{1,p} \cap 1 + p^N \mathfrak{gl}_{n_0}(\mathbb{Z}_p)$.

Step 5. (Bounded Generation: modulo p, for large primes) Step 3 gave us certain dominant morphisms. A result of Pink and Rütsche [PR09, Proposition 2.5] helps us to deduce that the image of these morphisms applied to the $\mathfrak{f}_p$-points of the underlying varieties is *large* [1]. And so by a result of Gowers [Gow08] (also see [NP11, Corollary 1]) we get that the three fold multiple of the image of such a morphism is the entire $\mathfrak{f}_p$-points of the considered group. So altogether using Nori's strong approximation [Nor87, Theorem 5.4] we get the following (see Lemma 24)

there are $\gamma_1, \ldots, \gamma_n \in \Gamma_1$ *such that for large enough* p *we have* $\pi_p(\gamma_1 \Gamma_{2,p} \gamma_1^{-1} \ldots \gamma_n \Gamma_{2,p} \gamma_n^{-1}) = \pi_p(\Gamma_{1,p})$, *where* π_p *is the group homomorphism induced by the quotient map* $\mathbb{Z}_p \to \mathfrak{f}_p$.

Step 6. (Proving the Adelic Bounded Generation) Using the truncated logarithmic maps (see Lemma 25), Step 2, taking multiple commutators, and Step 5, we can generate the first N *p-adic layers* of $\Gamma_{1,p}$ for large enough p. This result together with Step 4 give us the Adelic Bounded Generation.

Acknowledgment

The first author would like to thank Amir Mohammadi for many valuable conversations. The second author is grateful to Alex Kontorovich for useful discussion on this topic. Authors would like to thank Alex Kontorovich, Alex Lubotzky, Amir Mohammadi, Peter Sarnak, and Peter Varjú for their comments on the earlier version of this note.

2. Preliminary results.

In this section, we gather some of the needed well-known results and adapt them to our setting.

2.1. Recalling basic analytic properties of $\mathbb{Q}_p$-points of an algebraic group.

For the convenience of the reader, in this section some of the well-known analytic properties of the $\mathbb{Q}_p$-points $\mathbb{G}(\mathbb{Q}_p)$ of a linear algebraic $\mathbb{Q}_p$-group $\mathbb{G} \subseteq (\mathrm{GL}_{n_0})_{\mathbb{Q}_p}$ is recalled. For instance, we will present a detailed argument of why the logarithmic function induces bijection between $G_c := \mathbb{G}(\mathbb{Q}_p) \cap (I + p^c \mathfrak{gl}_{n_0}(\mathbb{Z}_p))$ and $\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap p^c \mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ if c is a positive integer and $c > 1$ when $p = 2$.

[1] In this note $\mathfrak{f}_q$ denotes the finite field with q elements.

We start by summarizing the basic properties of the logarithmic and the exponential functions. In what follows c_0 is 1 if p is odd and it is 2 if $p=2$. For any prime p, the exponential function

$$\exp: p^{c_0}\mathfrak{gl}_{n_0}(\mathbb{Z}_p)\to \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{c_0}],\ \exp(x):=\sum_{i=0}^{\infty} x^i/i!$$

and the logarithmic function

$$\log: \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{c_0}]\to p^{c_0}\mathfrak{gl}_{n_0}(\mathbb{Z}_p),\ \log g:=-\sum_{i=1}^{\infty}(I-g)^i/i$$

are well-defined analytic functions, and inverse of each other, where

$$\mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{c_0}]:=\ker(\mathrm{GL}_{n_0}(\mathbb{Z}_p)\xrightarrow{\pi_{p^{c_0}}}\mathrm{GL}_{n_0}(\mathbb{Z}/p^{c_0}\mathbb{Z}));$$

moreover we have

$$\|\exp(x)-I\|_p=\|x\|_p,\ \text{and}\ \|\log(g)\|_p=\|g-I\|_p,$$

for any $x\in p^{c_0}\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ and $g\in \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{c_0}]$. Therefore for any integer $c\ge c_0$ the exponential and the logarithmic functions induce bijections between $\mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^c]$ and $p^c\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$.

The next lemma is an easy corollary of the chain rule, but a direct detailed argument is presented.

Lemma 9. *Let p be a prime, and $x\in p^{c_0}\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ where $c_0=2$ when $p=2$ is odd and $c_0=1$ otherwise. Suppose $f\in\mathbb{Q}[X_{ij}]$ is a polynomial on the entries of n_0-by-n_0 matrices. Then*

$$\lim_{n\to\infty}\frac{f(\exp(p^n x))-f(I)}{p^n}=(df)_I(x),$$

where

$$(df)_I(Y_{ij}):=\sum_{ij}\frac{\partial f}{\partial X_{ij}}(I)Y_{ij}.$$

Proof. After multiplying f by a suitable non-zero integer, we can and will assume that f has integer coefficients. To make the symbols a bit more clear, we view f as a polynomial of n_0^2 variables T_i. Here J denotes a multi-index, i.e. $J=(j_1,\ldots,j_{n_0^2})$ where j_i are non-negative integers. We denote the symbolic higher-order partial derivatives of a polynomial f by $\partial_J f$. For a multi-index J, let $\mathbf{T}^J$ be the monomial $\prod_i T_i^{j_i}$. By Taylor expansion we have

$$f(I+[T_i])=\sum_J \partial_J f(I)\mathbf{T}^J=f(I)+(df)_I(T_i)+\sum_{J,\|J\|_1>1}\partial_J f(I)\mathbf{T}^J, \tag{1}$$

where $[T_i]$ is the n_0-by-n_0 matrix whose ij-entry is $T_{n_0(i-1)+j}$ and $\|J\|_1:=\sum_i |j_i|$. For $x\in p^{c_0}\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ and a positive integer n, let $t_i:=T_i(\exp(p^n x)-I)$ be the i-th component of $\exp(p^n x)-I$ in the above ordering. So

$$\left\|\frac{f(\exp(p^n x))-f(I)-(df)_I(t_i)}{p^n}\right\|_p=\left\|\frac{\sum_{J,\|J\|_1>1}\partial_J f(I)\mathbf{t}^J}{p^n}\right\|_p\le\frac{\|\exp(p^n x)-I\|_p^2}{\|p^n\|_p}=\frac{\|p^n x\|_p^2}{\|p^n\|_p}\le\|p^n\|_p. \tag{2}$$

On the other hand, $t_i=\sum_{k=1}^{\infty}(p^{kn}/k!)T_i(x^k)$ where $T_i(\cdot)$ is the function which gives the i-th component of a matrix in the above ordering. Thus we get

$$\left\|\frac{(df)_I(t_i)}{p^n}-(df)_I(x)\right\|_p=\|\sum_{k=2}^{\infty}(p^{(k-1)n}/k!)(df)_I(x^k)\|_p\le\|p^n\|_p. \tag{3}$$

Hence by (2) and (3) we get

$$\left\|\frac{f(\exp(p^n x))-f(I)}{p^n}-(df)_I(x)\right\|_p\le\|p^n\|_p,$$

which implies our claim. □

Corollary 10. *Let $\mathbb{G} \subseteq (\mathrm{GL}_{n_0})_{\mathbb{Q}_p}$ be a given embedding of a Zariski-connected $\mathbb{Q}_p$-group $\mathbb{G}$. Then for any positive integer c which is more than 1 for $p = 2$, the logarithmic function*

$$\log : \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^c] \to \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap p^c\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$$

is a well-defined injection.

Proof. We already know that $\log : \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^c] \to p^c\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ is a bijection. So it is enough to show that for any $g \in G_c := \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^c]$ we have $\log g \in \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$.

Next we notice that the natural embedding $g \mapsto \mathrm{diag}(g, (\det g)^{-1})$ of $(\mathrm{GL}_{n_0})_{\mathbb{Z}_p}$ into $(\mathrm{SL}_{n_0+1})_{\mathbb{Z}_p}$ sends $\mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^c]$ to $\mathrm{SL}_{n_0+1}(\mathbb{Z}_p)[p^c]$ and commutes with the logarithmic function. So we can and will consider $\mathbb{G}$ as a subgroup of $(\mathrm{SL}_{n_0+1})_{\mathbb{Q}_p}$. So $\mathbb{G}$ as a closed subset of $(\mathrm{SL}_{n_0+1})_{\mathbb{Q}_p}$ is given by relations f_i, where f_i are polynomials on the entries of $(n_0 + 1)$-by-$(n_0 + 1)$ matrices. Hence

$$\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) = \{x \in \mathfrak{gl}_{n_0+1}(\mathbb{Q}_p) |\ (df_i)_I(x) = 0\}.$$

By Lemma 10, we have

$$(df_i)_I(\log g) = \lim_{n\to\infty} \frac{f_i(\exp(p^n \log g)) - f_i(I)}{p^n} = \lim_{n\to\infty} \frac{f_i(g^{p^n}) - f_i(I)}{p^n} = 0,$$

which implies $\log g \in \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$. □

Proposition 11. *Let $\mathbb{G} \subseteq (\mathrm{GL}_{n_0})_{\mathbb{Q}_p}$ be a given embedding of a Zariski-connected $\mathbb{Q}_p$-group $\mathbb{G}$. Then for a positive integer c, which is at least 2 if $p = 2$, the logarithmic function*

$$\log : \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^c] \to \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap p^c\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$$

is a bijection; and so the restriction of the exponential function is its inverse.

Proof. First we prove the claim when c is large depending on the embedding of $\mathbb{G}$.

By [Mar91, Chapter I, Lemma 2.5.1 (i)], we have that the dimension of $\mathbb{G}(\mathbb{Q}_p)$ as a $\mathbb{Q}_p$-analytic manifold is the same as $\dim \mathbb{G}$. Since, by Lemma 10, the restriction of the logarithmic function is an analytic immersion of $G_2 := \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^2]$ into $\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$ and as p-adic analytic manifolds G_2 has the same dimension as $\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$, we have that for some positive integer c_1

$$p^{c_1}\mathfrak{gl}_{n_0}(\mathbb{Z}_p) \cap \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \subseteq \log(G_2).$$

This implies that $\exp(p^{c_1}\mathfrak{gl}_{n_0}(\mathbb{Z}_p) \cap \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)) \subseteq \mathbb{G}(\mathbb{Q}_p)$. Hence for any $c \geq c_1$ we have

$$\exp(p^c\mathfrak{gl}_{n_0}(\mathbb{Z}_p) \cap \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)) \subseteq G_c, \tag{4}$$

So by (4) and Lemma 10 we get that $\log : G_c \to \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap p^c\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ is a bijection.

Suppose the closed immersion of $\mathbb{G}$ is given by the ideal $I_{\mathbb{G}} \triangleleft \mathbb{Q}[\mathrm{GL}_{n_0}]$. For any $f \in I_{\mathbb{G}}$ the composite function $f \circ \exp$ defines a p-adic analytic function on $\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap p^{c_0}\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ where $c_0 = 1$ if $p > 2$ and $c_0 = 2$ if $p = 2$. We have proved that this analytic function is identically zero on the open set $\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap p^c\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ if c is large enough. Hence it is zero, which implies

$$\exp(\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap p^{c_0}\mathfrak{gl}_{n_0}(\mathbb{Z}_p)) \subseteq \mathbb{G}(\mathbb{Q}_p).$$

Therefore $\log : \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{c_0}] \to \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap p^{c_0}\mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ is a bijection. □

2.2. **A remark on certain flat models of an algebraic group.** In this work we need to work with certain group schemes over either $\mathbb{Z}[1/q_0]$ or $\mathbb{Z}_p$. In order to treat them at the same time, only in this section, we let A be a PID and F be its quotient field.

Let $\mathbb{G}$ be a linear algebraic group defined over F. For a fixed F-embedding $\rho : \mathbb{G} \to (\mathrm{GL}_{n_0})_F$, $\mathbb{G}_\rho$ denotes the image of ρ. Now we view $(\mathrm{GL}_{n_0})_F$ as the generic fiber of the group scheme $(\mathrm{GL}_{n_0})_A$ and let $\mathcal{G}_\rho$ be the Zariski-closure of $\mathbb{G}_\rho$ in $(\mathrm{GL}_{n_0})_A$.

To clarify the previous paragraph, let $F[\mathrm{GL}_{n_0}]$ be the ring of regular functions of $(\mathrm{GL}_{n_0})_F$ and $I_{\mathbb{G}_\rho}$ be the defining ideal of $\mathbb{G}_\rho$ (which means the scheme structure of $\mathbb{G}_\rho$ is $\mathrm{Spec}(F[\mathrm{GL}_{n_0}]/I_{\mathbb{G}_\rho})$); then the ring of regular functions $A[\mathcal{G}_\rho]$ of $\mathcal{G}_\rho$ is $A[\mathrm{GL}_{n_0}]/(A[\mathrm{GL}_{n_0}] \cap I_{\mathbb{G}_\rho})$ where $A[\mathrm{GL}_{n_0}]$ is the ring of regular functions of $(\mathrm{GL}_{n_0})_A$.

Lemma 12. *In the above setting, the generic fiber of $\mathcal{G}_\rho$ is isomorphic to $\mathbb{G}_\rho$; and, for any A-algebra R with free A-module structure, $\mathcal{G}_\rho(R)$ can be naturally identified with $\mathbb{G}_\rho(R \otimes_A F) \cap \mathrm{GL}_{n_0}(R)$. (Here, since R is a free A-modules, we can and will identify R with a subring of $R \otimes_A F$ through $x \mapsto x \otimes 1$.) In particular, $\mathrm{Lie}(\mathcal{G}_\rho)(R)$ can be naturally identified with $\mathrm{Lie}(\mathbb{G}_\rho)(R \otimes_A F) \cap \mathfrak{gl}_{n_0}(R)$.*

Proof. Let $S := A \setminus \{0\}$ and $\mathfrak{A} := A[\mathrm{GL}_{n_0}]$. Then $F = S^{-1}A$ and $\mathfrak{A} \otimes_A F \simeq S^{-1}\mathfrak{A} = F[\mathrm{GL}_{n_0}]$. Let $I := \mathfrak{A} \cap I_{\mathbb{G}_\rho}$. Then $S^{-1}I = I_{\mathbb{G}_\rho}$. So $(\mathfrak{A}/I) \otimes_A F \simeq S^{-1}(\mathfrak{A}/I) \simeq S^{-1}\mathfrak{A}/S^{-1}I = F[\mathrm{GL}_{n_0}]/I_{\mathbb{G}_\rho} = F[\mathbb{G}_\rho]$.

For any $\phi \in \mathcal{G}_\rho(R) := \mathrm{Hom}_{A-\mathrm{alg.}}(A[\mathcal{G}_\rho], R)$ and $a \in A \setminus \{0\}$, we have $\phi(a) = a\phi(1) \neq 0$ as R is a free A-module. Hence $S^{-1}\phi : S^{-1}A[\mathcal{G}_\rho] \to S^{-1}R$ is well-defined. As we discussed above $S^{-1}A[\mathcal{G}_\rho] = F[\mathbb{G}_\rho]$; and $S^{-1}R \simeq R \otimes_A F$. On the other hand, ϕ can be lifted to an A-algebra homomorphism from $\mathfrak{A}$ to R. So we get the desired point in $\mathbb{G}_\rho(R \otimes_A F) \cap \mathrm{GL}_{n_0}(R)$.

Now suppose $\widehat{\phi} \in \mathbb{G}_\rho(R \otimes_A F) \cap \mathrm{GL}_{n_0}(R)$. This means $\widetilde{\phi} : F[\mathrm{GL}_{n_0}] \to R \otimes_A F$, $\widetilde{\phi}(x) := \widehat{\phi}(x + I_{\mathbb{G}_\rho})$, sends the generators t_{ij}, t of $F[\mathrm{GL}_{n_0}]$ to R.

As A is a PID, $A[\mathcal{G}_\rho]$ is a free A-module; and so we can and will identify $A[\mathcal{G}_\rho]$ by a subring of $S^{-1}A[\mathcal{G}_\rho] = F[\mathbb{G}_\rho]$. Now let ϕ be the A-algebra homomorphism which is the restriction of $\widehat{\phi}$ to $A[\mathcal{G}_\rho]$. Since the standard generators of $F[\mathrm{GL}_{n_0}]$ are sent to R by $\widehat{\phi}$, we can let R to be the codomain of ϕ. Hence we get an A-algebra homomorphism $\phi : A[\mathcal{G}_\rho] \to R$, i.e. $\phi \in \mathcal{G}_\rho(R)$.

To get the last part, we first notice that $R[T]/\langle T^2 \rangle = R \oplus R\overline{T}$ is a free A-module. Hence by the previous part and the definition of Lie algebra we get the following commutative diagram

$$\begin{array}{ccccccccc} 1 \to & \mathrm{Lie}(\mathcal{G}_\rho)(R) & \to & \mathcal{G}_\rho(R[\overline{T}]) & \to & \mathcal{G}_\rho(R) & \to 1 \\ & & & \downarrow\wr & & \downarrow\wr & \\ 1 \to & \mathrm{Lie}(\mathbb{G}_\rho)(R \otimes_A F) \cap \mathfrak{gl}_{n_0}(R) & \to & \mathbb{G}_\rho(R[\overline{T}] \otimes_A F) \cap \mathrm{GL}_{n_0}(R[\overline{T}]) & \to & \mathbb{G}_\rho(R \otimes_A F) \cap \mathrm{GL}_{n_0}(R) & \to 1, \end{array}$$

which implies the last part.

□

3. Generating the Lie algebra as a module under the adjoint action.

In this section, we study perfect algebraic groups and their adjoint representation. The main result of this section is Proposition 13.

Let's recall that the normal closure of an algebraic subgroup $\mathbb{G}_2$ of $\mathbb{G}_1$ is the smallest normal closed subgroup of $\mathbb{G}_2$ in $\mathbb{G}_1$.

Proposition 13. *Let $\mathbb{G}_2 \subseteq \mathbb{G}_1$ be Zariski-connected $\mathbb{Q}$-groups. Suppose $\mathbb{G}_2$ is a perfect $\mathbb{Q}$-subgroup of $\mathbb{G}_1$, and further assume that the normal closure of $\mathbb{G}_2$ in $\mathbb{G}_1$ is $\mathbb{G}_1$. Let $\mathfrak{g}_i := \mathrm{Lie}(\mathbb{G}_i)(\mathbb{Q})$ be the $\mathbb{Q}$-structure of the Lie algebras of $\mathbb{G}_i$. Then $\mathfrak{g}_2$ generates $\mathfrak{g}_1$ as an $\mathbb{G}_1(\mathbb{Q})$-module under the adjoint representation.*

Lemma 14. *Let $\mathbb{G}_2 \subseteq \mathbb{G}_1$ be Zariski-connected $\mathbb{Q}$-groups. Suppose $\mathbb{G}_2$ is a perfect $\mathbb{Q}$-subgroup of $\mathbb{G}_1$, and further assume that the normal closure of $\mathbb{G}_2$ in $\mathbb{G}_1$ is $\mathbb{G}_1$. Then $\mathbb{G}_1$ is perfect.*

Proof. Let $f : \mathbb{G}_1 \to \mathbb{G}_1/[\mathbb{G}_1, \mathbb{G}_1]$ be the natural quotient map. Since $\mathbb{G}_2$ is perfect, $\mathbb{G}_2$ is a subgroup of the kernel of f. Since $\ker(f)$ is a normal subgroup of $\mathbb{G}_1$ and the normal closure of $\mathbb{G}_2$ in $\mathbb{G}_1$ is $\mathbb{G}_1$, we get that $\ker(f) = \mathbb{G}_1$. Hence $\mathbb{G}_1$ is perfect. □

The following lemma has been proved in [SG, Lemma 20] for large finite fields. It is reproved here for the convenience of the reader. Lemma 15 enables us to reduce the proof of Proposition 13 to the case where the unipotent radical of $\mathbb{G}_1$ is abelian.

Lemma 15. *Let $\mathbb{H}$ be a Zariski-connected semisimple $\mathbb{Q}$-group and $\mathbb{U}$ be a unipotent $\mathbb{Q}$-group. Suppose $\mathbb{H}$ acts on $\mathbb{U}$, and let $\mathbb{G} := \mathbb{H} \ltimes \mathbb{U}$. Let $A_{\mathbb{G}}$ be the $\mathbb{Q}$-span of $\mathrm{Ad}(\mathbb{G}(\mathbb{Q})) \subseteq \mathrm{End}_{\mathbb{Q}}(\mathrm{Lie}(\mathbb{G})(\mathbb{Q}))$ and $\mathfrak{a}_{\mathbb{U}}$ be the ideal of $A_{\mathbb{G}}$ generated by $\{\mathrm{Ad}(u) - 1 |\, u \in \mathbb{U}(\mathbb{Q})\}$. Then*

1. *The Jacobson radical $J(A_{\mathbb{G}})$ of $A_{\mathbb{G}}$ is equal to $\mathfrak{a}_{\mathbb{U}}$.*
2. *$[\mathfrak{u}, \mathfrak{u}] \subseteq J(A_{\mathbb{G}})\mathfrak{g}$ where $\mathfrak{u} := \mathrm{Lie}(\mathbb{U})(\mathbb{Q})$ and $\mathbb{G} := \mathrm{Lie}(\mathbb{G})(\mathbb{Q})$.*

Proof. Since $\mathbb{U}$ is unipotent, $\mathfrak{a}_{\mathbb{U}}$ is a nilpotent ideal. Hence $\mathfrak{a}_{\mathbb{U}} \subseteq J(A_{\mathbb{G}})$. Let $A_{\mathbb{H}}$ be the $\mathbb{Q}$-span of $\mathrm{Ad}(\mathbb{H}(\mathbb{Q}))$ as a subset of $\mathrm{End}_{\mathbb{Q}}(\mathfrak{g})$. Since $\mathbb{H}$ is semisimple, $A_{\mathbb{H}}$ is a semisimple algebra. Moreover, as a $\mathbb{Q}$-algebra, we have $A_{\mathbb{G}}/\mathfrak{a}_{\mathbb{U}} \simeq A_{\mathbb{H}}$. Overall we get $J(A_{\mathbb{G}}) = \mathfrak{a}_{\mathbb{U}}$.

Since $\mathbb{U}$ is unipotent, log and exp define $\mathbb{Q}$-morphisms between $\mathbb{U}$ and its Lie algebra. For any $n \in \mathbb{Z}$, $x, y \in \mathfrak{u}$ we have

$$\mathrm{Ad}(\exp(nx))(y) = \exp(n\,\mathrm{ad}(x))(y). \tag{5}$$

Thus for $n \in \mathbb{Z}^+$, $x, y \in \mathfrak{u}$ we have

$$n^{-1}(\mathrm{Ad}(\exp(nx))(y) - y) = [x, y] + \sum_{i=1}^{\dim_{\mathbb{Q}} \mathfrak{u}} \frac{n^i}{i!}\,\mathrm{ad}(x)^i(y) \in J(A_{\mathbb{G}})\mathfrak{g}. \tag{6}$$

Therefore by the Vandermonde determinant we have that $[x, y] \in J(A_{\mathbb{G}})\mathfrak{g}$. □

Lemma 16. *Let $\mathbb{H}$ be a Zariski-connected, semisimple $\mathbb{Q}$-group, and $\mathfrak{h} = \mathrm{Lie}(\mathbb{H})(\mathbb{Q})$. Let M be a subspace of $\mathfrak{h}$ which is $\overline{H} := \mathrm{Ad}(\mathbb{H}(\mathbb{Q}))$-invariant. Then there is a normal subgroup $\mathbb{N}$ of $\mathbb{H}$ such that $\mathrm{Lie}(\mathbb{N})(\mathbb{Q}) = M$; in particular, if M is a proper subspace of $\mathfrak{h}$, then $\mathbb{N}$ is a proper normal subgroup of $\mathbb{H}$.*

Proof. Without loss of generality we can and will assume that $\mathbb{H}$ is simply-connected. So there are Zariski-connected, simply-connected, semisimple, $\mathbb{Q}$-simple groups $\mathbb{H}_i$ such that $\mathbb{H} \simeq \oplus_i \mathbb{H}_i$. Without loss of generality we can and will identify $\mathbb{H}$ with $\oplus_i \mathbb{H}_i$. Therefore $\mathfrak{h}_i := \mathrm{Lie}(\mathbb{H}_i)(\mathbb{Q})$ are simple $\overline{H}$-modules, and M can be identified with a subspace of $\oplus_i \mathfrak{h}_i$.

Claim. Let $\mathrm{pr}_j : \oplus_i \mathfrak{h}_i \to \mathfrak{h}_j$ be the projection onto the j-th component. Let $J := \{j |\, \mathrm{pr}_j(M) \neq 0\}$. Then $M = \oplus_{j \in J} \mathfrak{h}_j$.

Proof of Claim. For $j \in J$, there is $x = (x_i)_i \in \oplus_i \mathfrak{h}_i$ such that $x_j \neq 0$. So there is $h_j \in \mathbb{H}_j(\mathbb{Q})$ such that $\mathrm{Ad}(h_j)(x_j) \neq x_j$. Hence

$$\mathrm{Ad}(h_j)(x) - x = \mathrm{Ad}(h_j)(x_j) - x_j \in (M \cap \mathfrak{h}_j) \setminus \{0\}.$$

So $M \cap \mathfrak{h}_j \neq 0$. Since $\mathfrak{h}_j$ is a simple $\overline{H}$-module, we get $\mathfrak{h}_j \subseteq M$. Thus $M = \oplus_{j \in J} \mathfrak{h}_j$.

Now it is clear that the subgroup $\mathbb{N} := \oplus_{j \in J} \mathbb{H}_j$ satisfies all the mentioned conditions. □

The next lemma is tightly related to [SGV12, Lemma 13], where normal subgroups of a perfect algebraic group is described. And we closely follow the proof of the mentioned result.

Lemma 17. *Let $\mathbb{H}$ be a Zariski-connected semisimple $\mathbb{Q}$-group. Let $\rho : \mathbb{H} \to \mathbb{GL}(\mathbb{V})$ be a $\mathbb{Q}$-representation of $\mathbb{H}$. Suppose $\mathbb{V}(\overline{\mathbb{Q}})$ has no non-zero $\mathbb{H}(\overline{\mathbb{Q}})$-fixed point. Let $\mathbb{G} := \mathbb{H} \ltimes \mathbb{V}$, and $\mathfrak{g} := \mathrm{Lie}(\mathbb{G})(\mathbb{Q})$. Let M be a subspace of $\mathfrak{g}$ which is $\overline{G} := \mathrm{Ad}(\mathbb{G}(\mathbb{Q}))$-invariant. Then there is a normal subgroup $\mathbb{N}$ of $\mathbb{G}$ such that $M = \mathrm{Lie}(\mathbb{N})(\mathbb{Q})$.*

Proof. Let $M' := M \cap V$, and $\underline{M'}$ be the $\mathbb{Q}$-subgroup of $\mathbb{V}$ which is induced by M'. Since $\mathbb{H}$ is semisimple, $\mathbb{H}(\mathbb{Q})$ is Zariski-dense in $\mathbb{H}$. Hence $\underline{M'}$ is invariant under the action of $\mathbb{H}$.

Passing to $\mathbb{H} \ltimes \mathbb{V}/\underline{M'}$ and $M/M' \subseteq \mathfrak{h} \oplus V/M'$, we can and will assume that $V \cap M = \{0\}$. Thus projection to $\mathfrak{h}$ induces an embedding and we get an $\mathrm{Ad}(\mathbb{H}(\mathbb{Q}))$-module homomorphism $\phi : \mathrm{pr}\, M \to V$, where $\mathrm{pr} : \mathfrak{h} \oplus V \to \mathfrak{h}$ is the projection map, such that

$$M = \{(x, \phi(x)) |\ x \in \mathrm{pr}\, M\}.$$

For any $v \in V$ and $x \in \mathrm{pr}\, M$, we have

$$\mathrm{Ad}(1, v)(x, \phi(x)) - (x, \phi(x)) = (0, [x, v]) \in M. \tag{7}$$

Hence by (7) we have $[\mathrm{pr}\, M, V] = 0$. On the other hand, by Lemma 16, there is a normal subgroup $\mathbb{H}_M$ of $\mathbb{H}$ such that $\mathrm{pr}\, M = \mathrm{Lie}(\mathbb{H}_M)(\mathbb{Q})$. In particular, $\mathbb{H}_M$ is a semisimple $\mathbb{Q}$-group. So we have that $\mathbb{H}_M$ acts trivially on $\mathbb{V}$. Thus $\mathbb{H}_M$ is a normal subgroup of $\mathbb{G}$.

For any h in the centralizer $C_{\mathbb{H}(\mathbb{Q})}(\mathbb{H}_M(\mathbb{Q}))$ of $\mathbb{H}_M(\mathbb{Q})$ in $\mathbb{H}(\mathbb{Q})$ and $x \in \mathrm{pr}\, M$, we have $\mathrm{Ad}(h)(\phi(x)) = \phi(\mathrm{Ad}(h)(x)) = \phi(x)$. On the other hand, since $\mathbb{H}$ is a semisimple $\mathbb{Q}$-group and $\mathbb{H}_M$ is a normal $\mathbb{Q}$-subgroup of $\mathbb{H}$, we have $\mathbb{H}(\mathbb{Q}) = \mathbb{H}_M(\mathbb{Q}) C_{\mathbb{H}(\mathbb{Q})}(\mathbb{H}_M(\mathbb{Q}))$. Overall we get that $\mathbb{H}(\mathbb{Q})$ acts trivially on $\phi(\mathrm{pr}\, M)$. Hence $\phi = 0$, and we get $M = (\mathrm{Lie}\, \mathbb{H}_M)(\mathbb{Q})$. □

Proof of Proposition 13. By Lemma 14, $\mathbb{G}_1$ is perfect. So $\mathbb{G}_1 \simeq \mathbb{H} \ltimes \mathbb{U}$ where $\mathbb{H}$ is a semisimple $\mathbb{Q}$-group $\mathbb{H}$ and $\mathbb{U}$ is a unipotent $\mathbb{Q}$-group. Moreover $\mathbb{V}(\overline{\mathbb{Q}})$ has no non-zero $\mathrm{Ad}(\mathbb{H}(\overline{\mathbb{Q}}))$-fixed element where $\mathbb{V} = \mathbb{U}/[\mathbb{U}, \mathbb{U}]$.

Let M be the $\mathrm{Ad}(\mathbb{G}_1(\mathbb{Q}))$-module generated by $\mathfrak{g}_2$. We want to show that $M = \mathfrak{g}_1$. By Lemma 15 and Nakayama's lemma, it is enough to prove $[\mathfrak{u}, \mathfrak{u}] + M = \mathfrak{g}_1$ where $\mathfrak{u} := \mathrm{Lie}(\mathbb{U})(\mathbb{Q})$.

By applying Lemma 17 for $\mathbb{H} \ltimes \mathbb{V}$ and

$$(M + [\mathfrak{u}, \mathfrak{u}])/[\mathfrak{u}, \mathfrak{u}] \subseteq \mathrm{Lie}(\mathbb{H})(\mathbb{Q}) \oplus \mathrm{Lie}(\mathbb{V})(\mathbb{Q}) = \mathfrak{h} \oplus \mathfrak{u}/[\mathfrak{u}, \mathfrak{u}],$$

we get that there is a normal $\mathbb{Q}$-subgroup $\mathbb{N}$ of $\mathbb{G}_1$ such that $M + [\mathfrak{u}, \mathfrak{u}] = \mathrm{Lie}(\mathbb{N})(\mathbb{Q}) \supseteq \mathrm{Lie}(\mathbb{G}_2)(\mathbb{Q})$. Hence $\mathbb{N} \supseteq \mathbb{G}_2$. Since the normal closure of $\mathbb{G}_2$ in $\mathbb{G}_1$ is $\mathbb{G}_1$, we get that $\mathbb{N} = \mathbb{G}_1$. And so $M + [\mathfrak{u}, \mathfrak{u}] = \mathfrak{g}_1$, which finishes the proof as it was explained above. □

4. Simultaneous bounded generation of almost all the fibers: Zariski-topology.

In this section we prove a *bounded generation* statement at the level of Zariski-topology (see Proposition 18).

To avoid recalling the definition of some well-known terms *within* the statements, they are mentioned here. Along the way, some needed notation is introduced.

Let $\mathrm{Spec}(\mathbb{Z}[1/q_0])$ be the affine scheme of the ring $\mathbb{Z}[1/q_0]$; in particular, the set of its points is

$$\mathrm{Spec}(\mathbb{Z}[1/q_0]) = \{0\} \cup \{p\mathbb{Z}[1/q_0] |\ p \text{ is a prime integer}, p \nmid q_0\}.$$

The point (0) is called the *generic* point (as it is dense). For any $p \in \mathrm{Spec}(\mathbb{Z}[1/q_0])$, the residue field over $p\mathbb{Z}[1/q_0]$ is denoted by $k(p)$; that means $k(p)$ is either the finite field with p elements if $p \neq 0$, or $\mathbb{Q}$ if $p = 0$. For any field F, its algebraic closure is denoted by $\overline{F}$.

Here we have to work with *affine, finite type, reduced, flat* group schemes $\mathcal{G}$ over $\mathbb{Z}[1/q_0]$; that means, as a scheme $\mathcal{G} = \mathrm{Spec}(A)$ where A is a finitely generated $\mathbb{Z}[1/q_0]$-algebra with no non-zero nilpotent element and no additively torsion element, and in addition A has a Hopf algebra structure. For an affine group scheme $\mathcal{G} = \mathrm{Spec}(A)$ over $\mathbb{Z}[1/q_0]$, its fiber over $p \in \mathrm{Spec}(\mathbb{Z}[1/q_0])$ is denoted by $\mathcal{G}^{(p)}$; that means $\mathcal{G}^{(p)} =$

$\mathrm{Spec}(A \otimes_{\mathbb{Z}[1/q_0]} k(p))$. For a group scheme $\mathcal{G}$ over $\mathbb{Z}[1/q_0]$, its geometric fiber over $p \in \mathrm{Spec}(\mathbb{Z}[1/q_0])$ is denoted by $\mathbb{G}^{(p)}$; that means $\mathbb{G}^{(p)} := \mathrm{Spec}(A \otimes_{\mathbb{Z}[1/q_0]} \overline{k(p)})$. The fiber $\mathcal{G}^{(0)}$ over (0) is called the generic fiber, and the geometric fiber $\mathbb{G}^{(0)}$ is sometimes denoted by $\mathbb{G}$. A morphism $f : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ between two schemes is called *dominant* if its image is dense.

For any non-zero integer q, any homomorphism induced by the quotient map $\pi_q : \mathbb{Z}[1/q_0] \to \mathbb{Z}[1/q_0]/q\mathbb{Z}[1/q_0]$ is still denoted by π_q. We let π_0 denote all the homomorphisms induced by the embedding $\pi_0 : \mathbb{Z}[1/q_0] \to \mathbb{Q}$. In particular, for a group scheme $\mathcal{G}$ over $\mathbb{Z}[1/q_0]$ and $p\mathbb{Z}[1/q_0] \in \mathrm{Spec}(\mathbb{Z}[1/q_0])$, we get a group homomorphism $\pi_p : \mathcal{G}(\mathbb{Z}[1/q_0]) \to \mathcal{G}^{(p)}(k(p))$.

The normal closure of an algebraic subgroup $\mathbb{G}_2$ of $\mathbb{G}_1$ is the smallest normal closed subgroup of $\mathbb{G}_2$ in $\mathbb{G}_1$.

Proposition 18. *Let $\Gamma_2 \subseteq \Gamma_1$ be subgroups of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$. For $i = 1, 2$, let $\mathcal{G}_i$ be the Zariski-closure of Γ_i in $(\mathrm{GL}_{n_0})_{\mathbb{Z}[1/q_0]}$, and suppose the geometric generic fiber $\mathbb{G}_i$ of $\mathcal{G}_i$ is irreducible. Suppose the normal closure of $\mathbb{G}_2$ in $\mathbb{G}_1$ is $\mathbb{G}_1$. Then there are $\gamma_1, \ldots, \gamma_c$ in Γ_1 such that the following is a surjective morphism*

$$f^{(p)}_{(\gamma_i)}(h_1, \ldots, h_c) : \mathbb{G}_2^{(p)} \times \cdots \times \mathbb{G}_2^{(p)} \to \mathbb{G}_1^{(p)}, \qquad f^{(p)}_{(\gamma_i)}(h_1, \ldots, h_c) := \pi_p(\gamma_1)h_1\pi_p(\gamma_1)^{-1} \cdots \pi_p(\gamma_c)h_c\pi_p(\gamma_c)^{-1},$$

where $p\mathbb{Z}[1/q_0]$ ranges in a non-empty open subset of $\mathrm{Spec}(\mathbb{Z}[1/q_0])$; that means $p\mathbb{Z}[1/q_0]$ can be any prime ideal except for finitely many non-zero ones. Furthermore $\mathbb{G}_i^{(p)}$ are Zariski-connected.

Let us recall parts of Proposition 9.6.1, Theorem 9.7.7 and Theorem 12.2.4 from [EGA66] where *constructibility* of being a dominant morphism (see [DG80, Chapter I.3.3] for definition of a constructible set) and *genericness* of dimension, being smooth, and being geometrically irreducible for the fibers of a $\mathbb{Z}[1/q_0]$-scheme are proved (see [DG80, Chapter I.4.4] for definition of a smooth morphism and see [SGV12, Theorem 40, Lemma 42] for an effective version of the former results).

Theorem 19. (1) *Let $\mathcal{V}$ be an affine $\mathbb{Z}[1/q_0]$-scheme of finite type. Suppose the generic fiber $\mathcal{V}^{(0)}$ of $\mathcal{V}$ is smooth and geometrically irreducible; that is to say $\mathbb{V}^{(0)} := \mathcal{V}^{(0)} \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\overline{\mathbb{Q}})$ is irreducible. Then there is $q_1 \in \mathbb{Z} \setminus \{0\}$ such that*
   (a) *For any $p \nmid q_0q_1$, the fiber $\mathcal{V}^{(p)}$ of $\mathcal{V}$ over $p\mathbb{Z}[1/q_0]$ is a smooth $k(p)$-scheme,*
   (b) *For any $p \nmid q_0q_1$, $\mathcal{V}^{(p)}$ is geometrically irreducible; that is to say $\mathbb{V}^{(p)} := \mathcal{V}^{(p)} \times_{\mathrm{Spec}(k(p))} \mathrm{Spec}(\overline{k(p)})$ is irreducible,*
   (c) *For any $p \nmid q_0q_1$, $\dim \mathcal{V}^{(0)} = \dim \mathcal{V}^{(p)} = \dim \mathbb{V}^{(p)}$.*

(2) *Let $\mathcal{V}$ and $\mathcal{W}$ be two affine, of finite type, $\mathbb{Z}[1/q_0]$-schemes. Let $f : \mathcal{V} \to \mathcal{W}$ be a $\mathbb{Z}[1/q_0]$-morphism. Let $\mathbb{V}^{(p)}$ and $\mathbb{W}^{(p)}$ be the geometric fibers over $p\mathbb{Z}[1/q_0] \in \mathrm{Spec}(\mathbb{Z}[1/q_0])$ of $\mathcal{V}$ and $\mathcal{W}$, respectively. Suppose $\mathbb{V}^{(0)}$ and $\mathbb{W}^{(0)}$ are irreducible and $f^{(0)} : \mathbb{V}^{(0)} \to \mathbb{W}^{(0)}$ is dominant. Then there is $q_1 \in \mathbb{Z}\setminus\{0\}$ such that*

$$f^{(p)} : \mathbb{V}^{(p)} \to \mathbb{W}^{(p)}$$

is dominant for any $p \nmid q_0q_1$.

Proof. As it is mentioned earlier, these are special cases of [EGA66, Proposition 9.6.1, Theorem 9.7.7, Theorem 12.2.4]. □

Proof of Proposition 18. We start by getting a dominant map on the geometric fiber of the generic point.
Claim 1. For a given $(\gamma_i)_{i=1}^{c_1} \subseteq \Gamma_1$, if $f^{(0)}_{(\gamma_i)_{i=1}^{c_1}}$ is not dominant, then there are $\gamma_{c_1+1}, \ldots, \gamma_{c_2} \in \Gamma_1$ such that $\dim \left(\overline{\mathrm{Im}(f^{(0)}_{(\gamma_i)_{i=1}^{c_2}})}\right) > \dim \left(\overline{\mathrm{Im}(f^{(0)}_{(\gamma_i)_{i=1}^{c_1}})}\right)$.

Proof of Claim 1. Since $\mathbb{G}_2$ is irreducible, $\mathbb{V} := \overline{\mathrm{Im}(f^{(0)}_{(\gamma_i)})}$ is irreducible. Therefore $\overline{\mathbb{V} \cdot \mathbb{V}^{-1} \cdot \mathbb{V}}$ is irreducible, too. If $\overline{\mathbb{V} \cdot \mathbb{V}^{-1} \cdot \mathbb{V}} \neq \mathbb{V}$, then $\dim \overline{\mathbb{V} \cdot \mathbb{V}^{-1} \cdot \mathbb{V}} > \dim \mathbb{V}$ and we get the desired claim as

$$\overline{\mathbb{V} \cdot \mathbb{V}^{-1} \cdot \mathbb{V}} = \overline{\mathrm{Im}(f^{(0)}_{(\gamma_i)_{i=1}^{c_2}})},$$

where $c_2 := 3c_1$ and $\gamma_{kc_1+i} := \gamma_i$ for $0 \le k \le 2$ and $1 \le i \le c_1$.

So we can and will assume that $\overline{\mathbb{V}\cdot\mathbb{V}^{-1}\cdot\mathbb{V}} = \mathbb{V}$, which implies that $\mathbb{V}$ is a subgroup of $\mathbb{G}_1$. Since the normal closure of $\mathbb{G}_2$ in $\mathbb{G}_1$ is $\mathbb{G}_1$, $\mathbb{V}$ cannot be a normal subgroup of $\mathbb{G}_1$. Since Γ_1 is Zariski-dense in $\mathbb{G}_1$, there is $\gamma \in \Gamma_1$ such that $\gamma\mathbb{V}\gamma^{-1}\cdot\mathbb{V} \ne \mathbb{V}$. Again by irreducibility of $\mathbb{V}$ and $\overline{\gamma\mathbb{V}\gamma^{-1}\cdot\mathbb{V}}$ we get the desired claim.

Claim 2. There are $\gamma_1,\ldots,\gamma_{c_1} \in \Gamma_1$ such that $f^{(0)}_{(\gamma_i)}$ is a dominant map.

Proof of Claim 2. Applying Claim 1 for at most $\dim \mathbb{G}_1$ many times, we get $\gamma_1,\ldots,\gamma_{c_{\dim \mathbb{G}_1}} \in \Gamma_1$ such that $f^{(0)}_{(\gamma_i)}$ is dominant.

Claim 3. There are $q_1 \in \mathbb{Z}\setminus\{0\}$ and $\gamma_1,\ldots,\gamma_{c_1} \in \Gamma_1$ such that for any $p \nmid q_0q_1$ (including $p=0$) we have that $f^{(p)}_{(\gamma_i)}$ is dominant and $\mathbb{G}_i^{(p)}$ is irreducible.

Proof of Claim 3. Let γ_i's be as in Claim 2. Now we can get the rest using Theorem 19 parts 1(b) and (2).

Claim 4. There are $\gamma_1,\ldots,\gamma_c \in \Gamma_1$ and $q_1 \in \mathbb{Z}\setminus\{0\}$ such that for any $p \nmid q_0q_1$ (including $p=0$) we have that $f^{(p)}_{(\gamma_i)}$ is surjective.

Proof of Claim 4. Since $\overline{k(p)}$ is algebraically closed, it is enough to find γ_i such that $f^{(p)}_{(\gamma_i)}$ induces a surjection from $\mathbb{G}_2^{(p)}(\overline{k(p)}) \times\cdots\times \mathbb{G}_2^{(p)}(\overline{k(p)})$ to $\mathbb{G}_1^{(p)}(\overline{k(p)})$ (see [DG80, Corollary 11, Chapter I.3.6]). Let $\gamma_1,\ldots,\gamma_{c_1}$ be as in Claim 3. So by Chevalley's theorem [Hum95, Chapter 4.4], there is an open and dense subset $U_p \subseteq \mathbb{G}_1^{(p)}(\overline{k(p)})$ of $\mathrm{Im}(f^{(p)}_{(\gamma_i)})$. Hence by [Hum95, Chapter 7.4] we have $\mathbb{G}_1^{(p)}(\overline{k(p)}) = U_p\cdot U_p$. Therefore $f^{(p)}_{(\gamma_i)_{i=1}^c}$ is surjective where $c := 2c_1$ and $\gamma_{c_1+i} := \gamma_i$ for any $1 \le i \le c_1$. □

5. Large congruence subgroup: for an arbitrary place.

In this section, we will prove a bounded generation statement in p-adic setting for *arbitrary* p (see Proposition 20).

Besides some well-known terms from algebraic geometry that has been already introduced in Section 4, we need to recall some terms from algebraic group theory. An algebraic group $\mathbb{G}$ is called *perfect* if there is no non-trivial homomorphism to an abelian algebraic group; that is to say the derived subgroup $[\mathbb{G},\mathbb{G}]$ is equal to $\mathbb{G}$. A perfect group $\mathbb{G}$ is isomorphic to $\mathbb{L}\ltimes\mathbb{U}$ where $\mathbb{L}$ is a semisimple group and $\mathbb{U}$ is a unipotent group. We say a perfect group $\mathbb{G}$ is simply connected if its semisimple part is simply connected (see [SGV12, Section 3] for relevant basic properties of perfect algebraic groups).

To avoid repeating a series of assumptions for the statements of this section, we record them here for the future reference.

- (A1) $\Gamma_2 \subseteq \Gamma_1$ are finitely generated subgroups of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$.
- (A2) $\mathcal{G}_i$ is the Zariski-closure of Γ_i in $(\mathrm{GL}_{n_0})_{\mathbb{Z}[1/q_0]}$.
- (A3) For any $p \in \mathrm{Spec}(\mathbb{Z}[1/q_0])$, $\mathcal{G}_i^{(p)}$ is the fiber over p of $\mathcal{G}_i$.
- (A4) For any $p \in \mathrm{Spec}(\mathbb{Z}[1/q_0])$, $\mathbb{G}_i^{(p)}$ is the geometric fiber of $\mathcal{G}_i^{(p)}$.
- (A5) $\mathbb{G}_i := \mathbb{G}_i^{(0)}$ are perfect and $\mathbb{G}_1$ is simply-connected.
- (A6) For $\gamma_i \in \Gamma_1$ and $p \in \mathrm{Spec}(\mathbb{Z}[1/q_0])$, $f_{p,(\gamma_i)} : \mathcal{G}_2^{(p)}\times\cdots\times\mathcal{G}_2^{(p)} \to \mathcal{G}_1^{(p)}$ and $f^{(p)}_{(\gamma_i)} : \mathbb{G}_2^{(p)}\times\cdots\times\mathbb{G}_2^{(p)} \to \mathbb{G}_1^{(p)}$ be the morphisms that are given by
$$(h_i) \mapsto \pi_p(\gamma_1)h_1\pi_p(\gamma_1)^{-1}\cdots\pi_p(\gamma_c)h_1\pi_p(\gamma_c)^{-1}.$$
- (A7) For some $\gamma_1,\ldots,\gamma_{m_0} \in \Gamma_1$, $f^{(p)}_{(\gamma_i)}$ is surjective if p is large enough.

Proposition 20. *In the setting of (A1)-(A7), there are a positive integer N and $\gamma_{m_0+1}, \dots, \gamma_{m_1} \in \Gamma$, such that for any prime $p \nmid q_0$ we have*

$$\Gamma_{1,p}[p^N] \subseteq \gamma_1 \Gamma_{2,p} \gamma_1^{-1} \cdots \gamma_{m_1} \Gamma_{2,p} \gamma_{m_1}^{-1},$$

where $\Gamma_{i,p}$ is the closure of Γ_i in $\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ and $\Gamma_{1,p}[p^N] := \Gamma_{1,p} \cap \ker(\mathcal{G}_1(\mathbb{Z}_p) \xrightarrow{\pi_{p^N}} \mathcal{G}_1(\mathbb{Z}/p^N\mathbb{Z}))$.

Lemma 21. *In the setting of (A1)-(A7), there are $\dim \mathbb{G}_1$-many elements γ'_i in Γ_1 such that*

$$\mathrm{Lie}(\mathbb{G}_1)(\mathbb{Q}) = \sum_{i=1}^{\dim \mathbb{G}_1} \mathrm{Ad}(\gamma'_i)(\mathrm{Lie}(\mathbb{G}_2)(\mathbb{Q})).$$

And so $\sum_{i=1}^{\dim \mathbb{G}_1} \mathrm{Ad}(\gamma'_i)(\mathrm{Lie}(\mathcal{G}_2)(\prod_{q_0 \nmid p} \mathbb{Z}_p))$ is an open subgroup of $\mathrm{Lie}(\mathcal{G}_1)(\prod_{q_0 \nmid p} \mathbb{Z}_p)$.

Proof. The first part is a corollary of Proposition 13 and the assumption that Γ_1 is Zariski-dense in $\mathbb{G}_1$. The second part is consequence of Chinese remainder theorem and the first part. □

Lemma 22. *In the setting of (A1), (A2), and (A5), for any $p \nmid q_0$, let $\Gamma_{1,p}$ be the closure of Γ_1 in $\mathrm{GL}_{n_0}(\mathbb{Z}_p)$, and $\widehat{\Gamma}_1$ be the closure of Γ_1 in $\prod_{p \nmid q_0} \mathrm{GL}_{n_0}(\mathbb{Z}_p)$. Then the following holds:*

1. *(Strong Approximation: simply-connected) $\widehat{\Gamma}_1$ is an open subgroup of $\prod_{p \nmid q_0} \mathcal{G}_1(\mathbb{Z}_p)$; in particular, there is a positive integer c_0 such that for any prime $p \nmid q_0$ and any integer $c \geq c_0$, we have $\Gamma_{1,p}[p^c] = \mathcal{G}_1(\mathbb{Z}_p)[p^c]$ where as before these are principal congruence subgroups.*
2. *(Strong Approximation: general) There is a positive integer c_1 such that for any integer $c \geq c_1$ we have $\mathcal{G}_2(\mathbb{Z}_p)[p^c] = \Gamma_{2,p}[p^c]$. Moreover, if p is large enough, then $\mathcal{G}_2(\mathbb{Z}_p)[p] = \Gamma_{2,p}[p]$*
3. *(Local charts) There is a positive integer c_2 such that for any integer $c \geq c_2$, the exponential and the logarithmic maps induce bijections between $\mathcal{G}_i(\mathbb{Z}_p)[p^c]$ and $\mathrm{Lie}(\mathcal{G}_i)(\mathbb{Z}_p) \cap p^c \mathfrak{gl}_{n_0}(\mathbb{Z}_p)$ for $i = 1$ or 2.*

Proof. The first part is Nori's strong approximation [Nor87, Theorem 5.4]. The third part is a direct consequence of Proposition 11 and Lemma 12.

Let $\widetilde{\mathbb{G}}_2$ be the simply-connected cover of $\mathbb{G}_2$, and $\iota : \widetilde{\mathbb{G}}_2 \to \mathbb{G}_2$ be the $\mathbb{Q}$-central isogeny. Let $\Lambda := \iota^{-1}(\Gamma_2) \cap \widetilde{\mathbb{G}}_2(\mathbb{Q})$. Then, as in [SGS13, Lemma 24], we have that Λ is a finitely generated, Zariski-dense subgroup of $\widetilde{\mathbb{G}}_2$. Hence, by Nori's strong approximation, we have that the closure Λ_p of Λ in $\iota^{-1}(\mathcal{G}_2(\mathbb{Z}_p))$ is open; and moreover, for large enough p, $\Lambda_p = \iota^{-1}(\mathcal{G}_2(\mathbb{Z}_p))$. Since $|\mathbb{G}_2(\mathbb{Q}_p)/\iota(\widetilde{\mathbb{G}}_2(\mathbb{Q}_p))| \leq p^{c_3}$ where c_3 just depends on the dimension of $\mathbb{G}_2$, we have that $\iota(\Lambda_p) \supseteq \mathcal{G}_2(\mathbb{Z}_p)[p^{c_1}]$ where c_1 just depends on $\Gamma_2 \subseteq \mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$. Therefore $\Gamma_{2,p} \supseteq \mathcal{G}_2(\mathbb{Z}_p)[p^{c_1}]$.

To show the last claim of part (2), we notice that $\mu := \ker(\iota)$ is a central subgroup of $\widetilde{\mathbb{G}}_2$ which is a $\mathbb{Q}_p$-group. Using Galois cohomology, we get the following exact sequence:

$$1 \to \mu(\mathbb{Q}_p) \to \widetilde{\mathbb{G}}_2(\mathbb{Q}_p) \to \mathbb{G}(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p, \mu).$$

Hence $\mathbb{G}(\mathbb{Q}_p)/\iota(\widetilde{\mathbb{G}}_2(\mathbb{Q}_p))$ can be embedded into $H^1(\mathbb{Q}_p, \mu)$, which is an abelian m-torsion group for some m that can be bounded by the dimension of $\mathbb{G}_2$. In particular, for large enough p, $\mathbb{G}(\mathbb{Q}_p)/\iota(\widetilde{\mathbb{G}}_2(\mathbb{Q}_p))$ does not have any p-element. As $\mathcal{G}_2(\mathbb{Z}_p)[p]/\iota(\iota^{-1}(\mathcal{G}_2(\mathbb{Z}_p)))[p]$ can be embedded into $\mathbb{G}(\mathbb{Q}_p)/\iota(\widetilde{\mathbb{G}}_2(\mathbb{Q}_p))$, we get that $\mathcal{G}_2(\mathbb{Z}_p)[p]/\iota(\iota^{-1}(\mathcal{G}_2(\mathbb{Z}_p)))[p]$ has no p-element. On the other hand, $\mathcal{G}_2(\mathbb{Z}_p)[p]$ is a pro-p group, and so all of its finite quotients are p-groups. Therefore we get

$$\mathcal{G}_2(\mathbb{Z}_p)[p] = \iota(\iota^{-1}(\mathcal{G}_2(\mathbb{Z}_p)))[p]. \tag{8}$$

As we said earlier, $\Lambda_p = \iota^{-1}(\mathbb{G}_2(\mathbb{Z}_p))$, for large enough p. Thus by (8) we have

$$\mathcal{G}_2(\mathbb{Z}_p)[p] = \Gamma_{2,p}[p].$$

□

Proof of Proposition 20. Let $m_1 := m_0 + \dim \mathbb{G}_1$ and $\gamma_{m_0+i} := \gamma'_i$ where γ'_i are the elements given by Lemma 21. Let c be an integer larger than $\max\{c_0, c_1, c_2\}$ where c_i's are given in Lemma 22. Let $\mathfrak{g}_{i,p} := \mathrm{Lie}(\mathcal{G}_i)(\mathbb{Z}_p)$. Let $F : p^c\mathfrak{g}_{2,p} \times \cdots \times p^c\mathfrak{g}_{2,p} \to p^c\mathfrak{g}_{1,p}$ be the composite of the following p-adic analytic functions:

$$\begin{aligned} p^c\mathfrak{g}_{2,p} \times \cdots \times p^c\mathfrak{g}_{2,p} &\xrightarrow{\exp} \mathcal{G}_2(\mathbb{Z}_p)[p^c] \times \cdots \times \mathcal{G}_2(\mathbb{Z}_p)[p^c], && \exp(x_1, \ldots, x_{m_1}) := (\exp x_1, \ldots, \exp x_{m_1}),\\ &\xrightarrow{\mathrm{Conj}} \mathcal{G}_1(\mathbb{Z}_p)[p^c] \times \cdots \times \mathcal{G}_1(\mathbb{Z}_p)[p^c], && \mathrm{Conj}(h_1, \ldots, h_{m_1}) := (\gamma_1 h_1 \gamma_1^{-1}, \ldots, \gamma_{m_1} h_{m_1} \gamma_{m_1}^{-1}),\\ &\xrightarrow{\mathrm{Prod}} \mathcal{G}_1(\mathbb{Z}_p)[p^c], && \mathrm{Prod}(g_1, \ldots, g_{m_1}) := g_1 \cdot \cdots \cdot g_{m_1},\\ &\xrightarrow{\log} \mathfrak{g}_{1,p} \cap p^c\mathfrak{gl}_{n_0}(\mathbb{Z}_p), && g \mapsto \log(g). \end{aligned}$$

So by the chain rule we have $dF(\mathbf{0}) : \mathfrak{g}_{2,p} \times \cdots \times \mathfrak{g}_{2,p} \to \mathfrak{g}_{1,p}$ is the composite of the following maps:

$$\begin{aligned} \mathfrak{g}_{2,p} \times \cdots \times \mathfrak{g}_{2,p} &\xrightarrow{d(\exp)(\mathbf{0})} \mathfrak{g}_{2,p} \times \cdots \times \mathfrak{g}_{2,p}, && d(\exp)(\mathbf{0})(x_1, \ldots, x_{m_1}) := (x_1, \ldots, x_{m_1}),\\ &\xrightarrow{d(\mathrm{Conj})(I)} \mathfrak{g}_{1,p} \times \cdots \times \mathfrak{g}_{1,p}, && d(\mathrm{Conj})(I)(x_1, \ldots, x_{m_1}) = (\mathrm{Ad}(\gamma_1)(x_1), \ldots, \mathrm{Ad}(\gamma_{m_1})(x_{m_1})),\\ &\xrightarrow{d(\mathrm{Prod})(I)} \mathfrak{g}_1, && d(\mathrm{Prod})(I)(y_1, \ldots, y_{m_1}) = y_1 + \cdots + y_{m_1},\\ &\xrightarrow{d(\log)(I)} \mathfrak{g}_{1,p}, && d(\log)(I)(y) = y. \end{aligned}$$

Hence by Lemma 21 and Lemma 22, we have that, for large enough p, $dF(\mathbf{0})$ is onto, and for any $p \nmid q_0$ the image of $dF(\mathbf{0})$ is open in $\mathfrak{g}_{1,p}$. Hence for some non-zero integer a_0 we have $N(dF(\mathbf{0})) \geq |a_0|_p$ where, for a d-by-m matrix $X = [\mathbf{v}_1 \cdots \mathbf{v}_m]$, $N(X) := \max_{1 \leq i_1 \leq \cdots \leq i_d \leq m} |\det[\mathbf{v}_{i_1} \cdots \mathbf{v}_{i_d}]|$.

By defintion of F, we have $F(x_1, \ldots, x_{m_1}) = \log(\exp(\mathrm{Ad}(\gamma_1)(x_1)) \cdots \exp(\mathrm{Ad}(\gamma_{m_1})(x_{m_1}))$. Hence by Baker-Campbell-Hausdorff formula [Jac79, Chapter V.5] we have

$$F(x_1, \ldots, x_{m_1}) = \sum_i \mathrm{Ad}(\gamma_i)(x_i) + \sum_{\mathbf{i}} c_{\mathbf{i}} L_{\mathbf{i}}(\mathrm{Ad}(\gamma_1)(x_1), \ldots, \mathrm{Ad}(\gamma_{m_1})(x_{m_1})),$$

where $L_{\mathbf{i}}(y_1, \ldots, y_{m_1})$ is a Lie monomial with multi-index $\mathbf{i}$ and $c_{\mathbf{i}} \in \mathbb{Q}$; moreover using the explicit Baker-Campbell-Hausdorff formula we see that

$$|c_{\mathbf{i}}|_p \leq p^{m_2 \|\mathbf{i}\|_1}, \tag{9}$$

where $\|(i_1, \ldots, i_{m_1})\|_1 = \sum_j i_j$ and m_2 is a constant which depends on m_1 (independent of p). Let $F_1 : \mathfrak{g}_2 \times \cdots \times \mathfrak{g}_2 \to \mathfrak{g}_1$ be $F_1(\mathbf{x}) := F(p^{cm_2}\mathbf{x})$. Choosing $\mathbb{Z}_p$-basis for $\mathfrak{g}_1$ and $\mathfrak{g}_2$, we identify them by $\mathbb{Z}_p^{d_1}$ and $\mathbb{Z}_p^{d_2}$, where $d_i = \dim \mathbb{G}_i$. Now using the mentioned Baker-Campbell-Hausdorff formula, writing the Taylor expansion of F' at $\mathbf{0}$ with respect to the chosen coordinates we get $F_1(\mathbf{x}) = \sum_{\mathbf{i}} (c_{\mathbf{i},1}\mathbf{x}^{\mathbf{i}}, \ldots, c_{\mathbf{i},d_1}\mathbf{x}^{\mathbf{i}})$ and $|c_{\mathbf{i},j}|_p \leq 1$ for any $\mathbf{i}$ and j. We also have $N(dF_1(\mathbf{0})) \geq |a_0 p^{m_2 d_1}|$. Therefore by [SG, Lemma 45'] there is l_0 which is independent of p such that

$$F_1(\mathbf{0}) + p^l \mathbb{Z}_p^{d_1} \subseteq F_1(\mathbb{Z}_p^{d_2 m_1}),$$

which implies that

$$p^l \mathfrak{g}_{1,p} \subseteq \log(\gamma_1 \mathcal{G}_2(\mathbb{Z}_p)[p^c]\gamma_1^{-1} \cdots \gamma_{m_1} \mathcal{G}_2(\mathbb{Z}_p)[p^c]\gamma_{m_1}^{-1}). \tag{10}$$

By Lemma 22 and Equation (10) we have

$$\Gamma_{1,p}[p^l] \subseteq \gamma_1 \mathcal{G}_2(\mathbb{Z}_p)[p^c]\gamma_1^{-1} \cdots \gamma_{m_1} \mathcal{G}_2(\mathbb{Z}_p)[p^c]\gamma_{m_1}^{-1} \subseteq \gamma_1 \Gamma_{2,p} \gamma_1^{-1} \cdots \gamma_{m_1} \Gamma_{2,p} \gamma_{m_1}^{-1}.$$

□

6. Bounded generation: Large primes.

In this section, we will prove a bounded generation statement in p-adic setting for large p (see Proposition 23).

We will be using all the mentioned terms from algebraic geometry and algebraic group theory; in particular, we will operate under the assumptions (A1)-(A7) which are mentioned in Section 5. In addition, we assume γ_i's satisfy Proposition 20 and Lemma 21, which means

(A8) We have $\mathrm{Lie}(\mathbb{G}_1)(\mathbb{Q}) = \sum_{i=1}^{c} \mathrm{Ad}(\gamma_i)(\mathrm{Lie}(\mathbb{G}_2)(\mathbb{Q}))$.
(A9) For a positive integer N and any prime $p \nmid q_0$, we have $\Gamma_{1,p}[p^N] \subseteq \gamma_1\Gamma_{2,p}\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}\gamma_c^{-1}$.

It is worth mentioning that, as we have seen in the proof of Proposition 20, (A1)-(A8) implies (A9).

Proposition 23. *In the setting of (A1)-(A9), there is a positive integer C such that for any large enough p we have*

$$\prod_C(\gamma_1\Gamma_{2,p}\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}\gamma_c^{-1}) = \Gamma_{1,p}, \tag{11}$$

where $\Gamma_{i,p}$ is the closure of Γ_i in $\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ and $\prod_C X = \{x_1\cdots x_C |\ x_i \in X\}$.

It is enough to prove that the equality holds modulo all the powers of p. We start with proving that (11) holds modulo p for $C = 3\dim\mathbb{G}_1$.

Lemma 24. *In the setting of (A1)-(A8), for large enough p, we have*

$$\prod_{3\dim\mathbb{G}_1}\pi_p(\gamma_1\Gamma_{2,p}\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}\gamma_c^{-1}) = \pi_p(\Gamma_{1,p}),$$

where $\Gamma_{i,p}$ is the closure of Γ_i in $\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ and $\prod_C X = \{x_1\cdots x_C |\ x_i \in X\}$.

Proof. By (A7), for large enough p, $f_{p,(\gamma_i)_{i=1}^c}$ is dominant. By (A5) and Proposition 18, for large enough p, $\mathbb{G}_2^{(p)}$ is irreducible. So by [PR09, Proposition 2.4] fibers of $f_{p,(\gamma_i)_{i=1}^{cd_1}}$ have dimension at most $d_1(cd_2-1)$, where $d_1 = \dim\mathbb{G}_1$, $d_2 = \dim\mathbb{G}_2$, $\gamma_{rc+i} = \gamma_i$ for $0 \le r < d_1$ and $1 \le i \le c$.

Clearly $f_p := f_{p,(\gamma_i)_{i=1}^{cd_1}}$ is dominant. Hence, by [PR09, Proposition 2.5], there is a positive constant C_1 such that for any prime p and any $y \in \mathcal{G}_1^{(p)}(k(p))$ we have

$$|f_p^{-1}(y)(k(p))| \le C_1 p^{\dim(f_p^{-1}(y))}. \tag{12}$$

Since any fiber of f has dimension at most $d_1(cd_2-1)$, by (12) we get

$$|\pi_p(\Gamma_{2,p})|^{cd_1} \le \sum_{y\in f_p(\underbrace{\pi_p(\Gamma_{2,p})\times\cdots\times\pi_p(\Gamma_{2,p})}_{cd_1\ \text{times}})} |f_p^{-1}(y)(k(p))| \le C_1 p^{d_1(cd_2-1)}|f_p(\Gamma_{2,p})|. \tag{13}$$

Since $\mathbb{G}_2$ is perfect, by Nori's strong approximation (see [SGV12, Section 3]) and the well-known order of finite quasi-simple groups of Lie type we have that there is a positive constant C_2 such that $|\pi_p(\Gamma_{2,p})| \ge C_2^{-1}p^{d_2}$ for any large enough prime p. So together with (13) we get

$$C_2^{-cd_1}C_1^{-1}p^{d_1} \le |f_p(\underbrace{\pi_p(\Gamma_{2,p})\times\cdots\times\pi_p(\Gamma_{2,p})}_{cd_1\ \text{times}})| = |\prod_{d_1}\pi_p(\gamma_1\Gamma_{2,p}\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}\gamma_c^{-1})|. \tag{14}$$

Since $\mathbb{G}_1$ is perfect and $\mathbb{G}_1$ is simply-connected, again by Nori's strong approximation (see [SGV12, Section 3]) and the well-known order of finite quasi-simple groups of Lie type we have that there is a constant C_3 such that $|\pi_p(\Gamma_{1,p})| \ge C_3^{-1}p^{d_2}$ for any large enough prime p. Hence by (14) we get

$$C_4^{-1}|\pi_p(\Gamma_{1,p})| \le |\prod_{d_1}\pi_p(\gamma_1\Gamma_{2,p}\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}\gamma_c^{-1})|, \tag{15}$$

for some positive constant C_4. By Nori's Strong Approximation (see [Nor87, Theorem 5.4] or [SGV12, Theorem A]) we have that $\pi_p(\Gamma_{1,p}) = \mathcal{L}_p(k(p)) \ltimes \mathcal{U}_p(k(p))$ for large enough p, where $\mathcal{L}_p$ is a semisimple, simply connected, Zariski connected $k(p)$-group with dimension at most d_1 and $\mathcal{U}_p$ is a unipotent Zariski connected $k(p)$-group with dimension at most d_1. Let ρ be an irreducible (complex) representation of $\pi_p(\Gamma_{1,p})$. By [SGV12, Corollary 4], the restriction of ρ to $\mathcal{L}_p(k(p))$ is not trivial. Hence by [LS74]

$$\dim\rho \ge |\mathcal{L}_p(k(p))|^{1/C_5} \ge |\pi_p(\Gamma_{1,p})|^{1/C_6} \tag{16}$$

for some positive constants C_5 and C_6 (depending only on d_1). By (15), (16), and a theorem of Gowers [Gow08] (see [NP11, Corollary 1]), it follows that

$$\prod_{3d_1} \pi_p(\gamma_1\Gamma_{2,p}\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}\gamma_c^{-1}) = \pi_p(\Gamma_{1,p})$$

for large enough p. □

Next we generate the k-th grade $\Gamma_{1,p}[p^k]/\Gamma_{1,p}[p^{k+1}]$ using γ_i's. Let us recall the connection between the k-th grade and the Lie algebra of the group scheme $\mathcal{G}_i$.

Lemma 25. *In the setting of (A1)-(A5), for large enough prime p and any positive integer k,*

$$\Psi_k : \mathcal{G}_i(\mathbb{Z}_p)[p^k]/\mathcal{G}_i(\mathbb{Z}_p)[p^{k+1}] \to \mathfrak{g}_{i,p}/p\mathfrak{g}_{i,p}, \qquad \Psi_k((I+p^kx)\mathcal{G}_i(\mathbb{Z}_p)[p^{k+1}]) := \pi_p(x),$$

where $\mathfrak{g}_{i,p} := \mathrm{Lie}(\mathcal{G}_i)(\mathbb{Z}_p)$, is an isomorphism; moreover for any $g \in \mathcal{G}_i(\mathbb{Z}_p)$ and $g' \in \mathcal{G}_i(\mathbb{Z}_p)[p^k]$ we have

$$\Psi_k(gg'g^{-1}\mathcal{G}_i(\mathbb{Z}_p)[p^{k+1}]) = \mathrm{Ad}(\pi_p(g))(\Psi_k(g'\mathcal{G}_i(\mathbb{Z}_p)[p^{k+1}])).$$

Proof. By the discussion in [SG16, Section 2.9], we get that

$$\widetilde{\Psi}_k : \mathcal{G}_i(\mathbb{Z}_p)[p^k]/\mathcal{G}_i(\mathbb{Z}_p)[p^{k+1}] \to \mathrm{Lie}(\mathcal{G}_i)(\mathbb{Z}_p/p\mathbb{Z}_p), \quad \widetilde{\Psi}_k((I+p^kx)\mathcal{G}_i(\mathbb{Z}_p)[p^{k+1}]) := \pi_p(x),$$

is a well-defined injective group homomorphism.

For large p, $\mathcal{G}_i \times_{\mathbb{Z}[1/q_0]} \mathbb{Z}_p$ is a smooth $\mathbb{Z}_p$-group scheme, and so $\mathrm{Lie}(\mathcal{G}_i)(\mathbb{Z}_p/p\mathbb{Z}_p)$ is naturally isomorphic to $\mathfrak{g}_i/p\mathfrak{g}_i$. So we get that Ψ_k is a well-defined injective group homomorphism.

For any $x \in \mathfrak{g}_{i,p}$ and $p > 2$, by Proposition 11, $\exp(p^kx) \in \mathcal{G}_i(\mathbb{Z}_p)[p^k]$. By the definition of the exponential function we can see that

$$\Psi_k(\exp(p^kx)\mathcal{G}_i(\mathbb{Z}_p)[p^{k+1}]) = \pi_p(x),$$

which implies that Ψ_k is a group isomorphism. The other part of Lemma is easy to check. □

Lemma 26. *In the setting of (A1)-(A8), for large enough p and any positive integer k, we have*

$$(\gamma_1\Gamma_{2,p}[p^k]\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}[p^k]\gamma_c^{-1})\Gamma_{1,p}[p^{k+1}] = \Gamma_{1,p}[p^k].$$

Proof. By (A8), for large enough p, we have $\mathfrak{g}_{1,p} = \sum_{i=1}^c \mathrm{Ad}(\gamma_i)(\mathfrak{g}_{2,p})$ where $\mathfrak{g}_{i,p} := \mathrm{Lie}(\mathcal{G}_i)(\mathbb{Z}_p)$. Hence, by Lemma 25, we have

$$(\gamma_1\mathcal{G}_2(\mathbb{Z}_p)[p^k]\gamma_1^{-1}\cdots\gamma_c\mathcal{G}_2(\mathbb{Z}_p)[p^k]\gamma_c^{-1})\mathcal{G}_1(\mathbb{Z}_p)[p^{k+1}] = \mathcal{G}_1(\mathbb{Z}_p)[p^k]. \tag{17}$$

On the other hand, by the second part of Lemma 22, we have that, for large enough p, $\Gamma_{i,p}[p^k] = \mathcal{G}_i(\mathbb{Z}_p)[p^k]$, which together with (17) implies the claim. □

Proof of Proposition 23. Using Lemma 25, for $k = 1, \ldots, N-1$, we get that

$$\prod_{N-1}(\gamma_1\Gamma_{2,p}[p]\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}[p]\gamma_c^{-1})\Gamma_{1,p}[p^N] = \Gamma_{1,p}[p]. \tag{18}$$

Lemma 24 and Equation (18), we get

$$\prod_{3\dim\mathbb{G}_1+N-1}(\gamma_1\Gamma_{2,p}\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}\gamma_c^{-1})\Gamma_{1,p}[p^N] = \Gamma_{1,p}. \tag{19}$$

Condition (A9) together with Equation (19) imply that

$$\prod_{3\dim\mathbb{G}_1+N}(\gamma_1\Gamma_{2,p}\gamma_1^{-1}\cdots\gamma_c\Gamma_{2,p}\gamma_c^{-1}) = \Gamma_{1,p}.$$

□

7. Bounded generation: Adelic version.

In this section, we will prove an adelic bounded generation statement (see Theorem 27).

We will be working under the assumptions (A1)-(A5) mentioned at the beginning of Section 5.

Theorem 27. *In the setting of (A1)-(A5), let $\widehat{\Gamma}_i$ be the closure of Γ_i in $\prod_{p\nmid q_0} \mathrm{GL}_{n_0}(\mathbb{Z}_p)$. Then there are $\gamma_1, \ldots, \gamma_m \in \Gamma_1$ such that*

$$\gamma_1 \widehat{\Gamma}_2 \gamma_1^{-1} \cdots \gamma_m \widehat{\Gamma}_2 \gamma_m^{-1} \subseteq \widehat{\Gamma}_1$$

is an open subgroup of $\widehat{\Gamma}_1$.

Proof. As in the proof of Lemma 22 and [SGS13, Lemma 24], let $\widetilde{\mathbb{G}}_2$ be the simply-connected cover of $\mathbb{G}_2$, and $\iota : \widetilde{\mathbb{G}}_2 \to \mathbb{G}_2$ be the $\mathbb{Q}$-central isogeny. Let $\Lambda := \iota^{-1}(\Gamma_2) \cap \widetilde{\mathbb{G}}_2(\mathbb{Q})$ and $\Gamma'_2 := \iota(\Lambda)$. Then, as in [SGS13, Lemma 24], Λ is a finitely generated Zariski-dense subgroup of $\widetilde{\mathbb{G}}_2$; and so Γ'_2 is a finitely generated Zariski-dense subgroup of $\mathbb{G}_2$. We also notice that $\Gamma'_2 \subseteq \Gamma_2 \subseteq \Gamma_1$.

By Nori's strong approximation, the closure $\widehat{\Lambda}$ of Λ in $\prod_{p\nmid q_0} \iota^{-1}(\mathcal{G}_2(\mathbb{Z}_p))$ is open. So passing to a finite-index subgroup of Λ, if needed, we can and will assume that $\widehat{\Lambda} = \prod_{p\nmid q_0} \Lambda_p$ where Λ_p is the closure of Λ in $\iota^{-1}(\mathcal{G}_2(\mathbb{Z}_p))$. Therefore the closure of Γ'_2 in $\prod_{p\nmid q_0} \mathcal{G}_2(\mathbb{Z}_p)$ is $\iota(\widehat{\Lambda}) = \prod_{p\nmid q_0} \Gamma'_{2,p}$, where $\Gamma'_{2,p}$ is the closure of Γ'_2 in $\mathcal{G}_2(\mathbb{Z}_p)$. We notice that Γ'_2 is a finitely generated subgroup of Γ_2, and it is Zariski-dense in $\mathbb{G}_2$ since $\mathbb{G}_2$ is Zariski-connected.

By Proposition 18 applied to $\Gamma'_2 \subseteq \Gamma_1$, we get that $\Gamma'_2 \subseteq \Gamma_1$ satisfy (A1)-(A7) for some $\gamma_i \in \Gamma_1$. Hence by Proposition 20 for some $\gamma_i \in \Gamma_1$ and positive integer N we have

$$\Gamma_{1,p}[p^N] \subseteq \gamma_1 \Gamma'_{2,p} \gamma_1^{-1} \cdots \gamma_{m_1} \Gamma'_{2,p} \gamma_{m_1}^{-1}. \tag{20}$$

By Lemma 21 applied to $\Gamma'_2 \subseteq \Gamma_1$, there are γ_i in Γ_1 such that (A1)-(A9) hold for $\Gamma'_2 \subseteq \Gamma_1$. Therefore there are γ_i in Γ_1 such that, for any large prime p, we have

$$\gamma_1 \Gamma'_{2,p} \gamma_1^{-1} \cdots \gamma_{m_2} \Gamma'_{2,p} \gamma_{m_2}^{-1} = \Gamma_{1,p}. \tag{21}$$

By Equations (20) and (21), we have there are γ_i in Γ_1 such that

$$\gamma_1 \widehat{\Gamma}'_2 \gamma_1^{-1} \cdots \gamma_{m_3} \widehat{\Gamma}'_2 \gamma_{m_3}^{-1} = \prod_{p\nmid q_0} (\gamma_1 \Gamma'_{2,p} \gamma_1^{-1} \cdots \gamma_{m_3} \Gamma'_{2,p} \gamma_{m_3}^{-1}) \supseteq \prod_{p\nmid q_0, p<p_0} \Gamma_{1,p}[p^N] \cdot \prod_{p\geq p_0} \Gamma_{1,p}. \tag{22}$$

Therefore $\gamma_1 \widehat{\Gamma}_2 \gamma_1^{-1} \cdots \gamma_{m_3} \widehat{\Gamma}_2 \gamma_{m_3}^{-1}$ contains an open normal subgroup (of finite index) of $\widehat{\Gamma}_1$. So by multiplying this set by itself finitely many times we get an open subgroup of $\widehat{\Gamma}_1$. This means there are γ_i in Γ_1 such that $\gamma_1 \widehat{\Gamma}_2 \gamma_1^{-1} \cdots \gamma_m \widehat{\Gamma}_2 \gamma_m^{-1}$ is an open subgroup of $\widehat{\Gamma}_1$. □

8. Proof of Theorem 1: inducing super-approximation.

Let us recall that $\mathbb{G}_i$ is the Zariski-closure of Γ_i in $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$ and $\mathbb{G}_i^{\circ}$ is the Zariski-connected component of $\mathbb{G}_i$. Let $\widetilde{\mathbb{G}}_1$ be the simply-connected cover of $\mathbb{G}_1^{\circ}$ and $\iota : \widetilde{\mathbb{G}}_1 \to \mathbb{G}_1^{\circ}$ be its covering map. Let $\widetilde{\Lambda}_1 := \iota^{-1}(\Gamma_i) \cap \widetilde{\mathbb{G}}_1(\mathbb{Q})$, $\widetilde{\Lambda}_2 := \iota^{-1}(\Gamma_2) \cap \widetilde{\Lambda}_1 \cap \widetilde{\mathbb{G}}_2(\mathbb{Q})$, where $\widetilde{\mathbb{G}}_2$ is the Zariski-connected component of the Zariski-closure of $\iota^{-1}(\Gamma_2) \cap \widetilde{\Lambda}_1$ in $\widetilde{\mathbb{G}}_1$. Finally let $\Lambda_i := \iota(\widetilde{\Lambda}_i)$.

Now we will check that $\widetilde{\Lambda}_2 \subseteq \widetilde{\Lambda}_1$ satisfy conditions (A1) and (A5).

(A1) First we notice that $\mathbb{G}_1^{\circ}(\mathbb{Q}) \cap \Gamma_1$ is a subgroup of finite-index of Γ_1, and so it is finitely generated. Since $\mathbb{G}_1^{\circ}(\mathbb{Q})/\iota(\widetilde{\mathbb{G}}_1(\mathbb{Q}))$ is an abelian bounded torsion group and $\mathbb{G}_1^{\circ}(\mathbb{Q}) \cap \Gamma_1$ is finitely generated, we have that Λ_1 is a subgroup of finite-index in Γ_1. Thus Λ_1 is finitely generated. Since $\ker(\iota)(\mathbb{Q})$ is finite, we get that $\widetilde{\Lambda}_1$ is finitely-generated.

By a similar argument we get $\iota(\iota^{-1}(\Gamma_2)\cap\widetilde{\Lambda}_1)$ is a finite-index subgroup of $\Gamma_2\cap\mathbb{G}_1^\circ(\mathbb{Q})$. Therefore Λ_2 is a subgroup of finite-index in Γ_2. Hence it is finitely-generated, and so is $\widetilde{\Lambda}_2$.

By [SG16, Lemma 11], there is a $\mathbb{Q}$-embedding $\widetilde{\mathbb{G}}_1\subseteq(\mathrm{GL}_{n_1})_{\mathbb{Q}}$ such that $\widetilde{\Lambda}_1\subseteq\mathrm{GL}_{n_1}(\mathbb{Z}[1/q_0])$. So we have $\widetilde{\Lambda}_2\subseteq\widetilde{\Lambda}_1$ are two finitely generated subgroups of $\mathrm{GL}_{n_1}(\mathbb{Z}[1/q_0])$.

(A5) Since Γ_1 is Zariski-dense in $\mathbb{G}_1$, $\Gamma_1\cap\mathbb{G}_1^\circ(\mathbb{Q})$ is Zariski-dense in $\mathbb{G}_1^\circ$. Since Λ_1 is a finite-index subgroup of $\Gamma_1\cap\mathbb{G}_1^\circ(\mathbb{Q})$, it is Zariski-dense in $\mathbb{G}_1^\circ$. So the restriction of ι to the Zariski-closure of $\widetilde{\Lambda}_1$ is still surjective. And so $\widetilde{\Lambda}_1$ is Zariski-dense in $\widetilde{\mathbb{G}}_1$.

Since Λ_2 is a subgroup of finite-index in Γ_2, its Zariski-closure is a subgroup of finite index of $\mathbb{G}_2$. On the other hand, $\widetilde{\Lambda}_2$ is Zariski-dense in a Zariski-connected group $\widetilde{\mathbb{G}}_2$. Hence the Zariski-closure of $\Lambda_2=\iota(\widetilde{\Lambda}_2)$ is a Zariski-connected group. Therefore the Zariski-closure of Λ_2 is $\mathbb{G}_2^\circ$.

Since $\Gamma_2\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap, by [SG16, Proposition 8], $\mathbb{G}_2^\circ$ is perfect. By Lemma 14, we get that $\mathbb{G}_1^\circ$ is perfect. Therefore $\widetilde{\mathbb{G}}_i$'s are perfect.

Hence by Theorem 27 we have that there are $\widetilde{\lambda}_i\in\widetilde{\Lambda}_1$ such that $\widetilde{\lambda}_1\widehat{\widetilde{\Lambda}}_2\widetilde{\lambda}_1^{-1}\cdots\widetilde{\lambda}_m\widehat{\widetilde{\Lambda}}_2\widetilde{\lambda}_m^{-1}$ is an open subgroup of $\widehat{\widetilde{\Lambda}}_1$ where $\widehat{\widetilde{\Lambda}}_i$ is the closure of $\widetilde{\Lambda}_i$ in $\prod_{p\nmid q_0}\mathrm{GL}_{n_1}(\mathbb{Z}_p)$. Hence, applying ι and letting $\lambda_i:=\iota(\widetilde{\lambda}_i)$, we get that $\lambda_1\widehat{\Lambda}_2\lambda_1^{-1}\cdots\lambda_m\widehat{\Lambda}_2\lambda_m^{-1}$ is an open subgroup of $\widehat{\Lambda}_1$ where $\widehat{\Lambda}_i$ is the closure of Λ_i in $\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$.

Claim 1. Let $\overline{\Omega}_2$ be a finite symmetric generating set of Λ_2. Let $\Omega:=\bigcup_{i=1}^m\lambda_i\overline{\Omega}_2\lambda_i^{-1}$ and $\Lambda:=\langle\Omega\rangle$. Then $\Lambda\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap.

Proof of Claim 1. The closure of Λ in $\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ is

$$\widehat{\Lambda}:=\lambda_1\widehat{\Lambda}_2\lambda_1^{-1}\cdots\lambda_m\widehat{\Lambda}_2\lambda_m^{-1}. \tag{23}$$

By [SG16, Remark 15, (5)], $\lambda(\mathcal{P}_\Omega;\widehat{\Lambda})=\sup_{\gcd(q,q_0)=1}\lambda(\mathcal{P}_{\pi_q(\Omega)};\pi_q(\Lambda))$.

On the other hand, by [SG16, Section 2.3] we have that $\Gamma_2\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap if and only if $\Lambda_2\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap. Hence

$$1>\lambda(\mathcal{P}_{\overline{\Omega}_2};\widehat{\Lambda}_2)=\sup_{\gcd(q,q_0)=1}\lambda(\mathcal{P}_{\pi_q(\overline{\Omega}_2)};\pi_q(\Lambda_2)). \tag{24}$$

Therefore, by Varjú's lemma [BK14, Lemma A.4], Equations (23) and (24), we get that $\lambda(\mathcal{P}_\Omega;\widehat{\Lambda})<1$. □

Claim 2. $\Lambda_1\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap.

Proof of Claim 2. Let $\overline{\Lambda}:=\Lambda_1\cap\widehat{\Lambda}$ where $\widehat{\Lambda}$ is given in the proof of Claim 1. Since $\widehat{\Lambda}$ is a subgroup of finite index of $\widehat{\Lambda}_1$, $\overline{\Lambda}$ is a subgroup of finite index of Λ_1. Therefore by [SG16, Section 2.3] we have that $\Lambda_1\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap if and only if $\overline{\Lambda}\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap. Since $\Lambda\subseteq\overline{\Lambda}$, both of them are dense in $\widehat{\Lambda}$, and $\Lambda\curvearrowright\widehat{\Lambda}$ has spectral gap, we get that $\overline{\Lambda}\curvearrowright\widehat{\Lambda}$ has spectral gap. Thus $\Lambda_1\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap. □

Since Λ_1 is a subgroup of finite index of Γ_1 and $\Lambda_1\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap, another application of [SG16, Section 2.3] implies that $\Gamma_1\curvearrowright\prod_{p\nmid q_0}\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ has spectral gap.

References

[BG08-a] J. Bourgain, A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathfrak{f}_p)$, Annals of Mathematics **167** (2008) 625–642.

[BG08-b] J. Bourgain, A. Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$*:I,* Journal of European Mathematical Society **10** (2008) 987–1011.

[BG09] J. Bourgain, A. Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$*:II.* With an appendix by J. Bourgain, Journal of European Mathematical Society **11**, no. 5., (2009) 1057–1103.

[BGS10] J. Bourgain, A. Gamburd, P. Sarnak, *Affine linear sieve, expanders, and sum-product,* Inventiones Mathematicae **179**, no. 3., (2010) 559–644.

[BK14] J. Bourgain, A. Kontorovich, *On the local-global conjecture for integral Apollonian gaskets.* With an appendix by P. Varjú, Inventiones Mathematicae **196** (2014), no. 3, 589–650.

[BKM] J. Bourgain, A. Kontorovich, M. Magee, *Thermodynamic expansion to arbitrary moduli*, to appear as an appendix in Journal für die reine und angewandte Mathematik.

[BV12] J. Bourgain, P. Varjú, *Expansion in* $\mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$*, q arbitrary,* Inventiones Mathematicae **188**, no 1, (2012) 151–173.

[BS911] M. Burger, P. Sarnak, *Ramanujan duals II,* Inventions Mathematicae **106** (1991) 1–11.

[DG80] M. Demazure and P. Gabriel, Introduction to Algebraic Geometry and Algebraic Groups, New York, NY, North-Holland publishing company, 1980.

[FSZ] E. Fuchs, K. Stange, X. Zhang, *Local-global principles in circle packings,* preprint.

[Gow08] W.T. Gowers, *Quasirandom Groups,* Combinatorics, Probability and Computing **17** (2008) 363–387.

[EGA66] A. Grothendieck, *EGA IV, triosiéme partie,* Publications Mathematiques de IHES **28** (1966).

[HLW06] S. Hoory, N. Linial, A. Widgerson, *Expander graphs and their application,* Bull. AMS **43**, no. 4, (2006) 439–561.

[Hum95] J. Humphreys, Linear algebraic groups, Graduate texts in mathematics **21**, Springer-Verlag, New York.

[Jac79] N. Jacobson, Lie algebras, Dover publications, Inc., New York, 1979.

[LS74] V. Landazuri and G.M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups,* Journal of Algebra **32** (1974) 418–443.

[Lub94] A. Lubotzky, Discrete Groups, Expanding Graphs and Invariant Measures, Birkhäuser, Boston, 1994.

[Mar91] G.A. Margulis, Discrete subgroups of semisimple Lie groups, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **17** Springer-Verlag, 1991.

[MOW] M. Magee, H. Oh, D. Winter, *Uniform congruence counting for Schottky semigroups in* $\mathrm{SL}_2(\mathbb{Z})$*.* With an appendix by J. Bourgain, A. Kontorovich, M. Magee. To appear in Journal für die reine und angewandte Mathematik.

[NP11] N. Nikolov and L. Pyber, *Product decompositions of quasirandom groups and a Jordan type theorem,* Journal of the European Mathematical Society **13**, no 4, (2011) 1063–1077.

[Nor87] M. V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathfrak{f}_p)$*,* Inventiones Mathematicae **88** (1987) 257–275.

[PR09] R. Pink, E. Rütsche, *Adelic openness for Drinfeld modules in generic characteristic,* Journal of Number Theory **129** (2009) 882–907.

[SG16] A. Salehi Golsefidy, *Super-Approximation, I:* $\mathfrak{p}$*-adic semisimple case,* Accepted for publication in International Mathematics Research Notices (2016). `dx.doi.org/10.1093/imrn/rnw208`

[SG] A. Salehi Golsefidy, *Super-Approximation, II: The p-adic and bounded power of square-free integers cases,* preprint.

[SGS13] A. Salehi Golsefidy, P. Sarnak, *Affine sieve*, Journal of American Mathematical Society, **26**, no. 4, (2013) 1085–1105.

[SGV12] A. Salehi Golsefidy and P. Varjú, *Expansions in perfect groups,* Geometric And Functional Analysis **22**, no. 6, (2012) 1832–1891.

Mathematics Dept, University of California, San Diego, CA 92093-0112.

E-mail address: `golsefidy@ucsd.edu`

Mathematics Dept, University of Illinois, Urbana, IL 61801.

E-mail address: `xz87@illinois.edu`