On the model theory of higher rank arithmetic groups

Nir Avni and Chen Meiri

August 24, 2020

Abstract

Let $\Gamma$ be a centerless irreducible higher rank arithmetic lattice in characteristic zero. We prove that if $\Gamma$ is either non-uniform or is uniform of orthogonal type and dimension at least 9, then $\Gamma$ is bi-interpretable with the ring $\mathbb{Z}$ of integers. It follows that the first order theory of $\Gamma$ is undecidable, that all finitely generated subgroups of $\Gamma$ are definable, and that $\Gamma$ is characterized by a single first order sentence among all finitely generated groups.

1 Introduction

In this paper, we continue the study, initiated in [ALM], of the model theory of higher rank arithmetic groups. One of the central themes in the study of arithmetic groups is the contrast between arithmetic groups of $S$-rank 1 and arithmetic groups of $S$-rank bigger than 1. Examples of such dichotomy are Margulis’s Normal Subgroup Theorem, the Congruence Subgroup Property, and, to lesser extent, superrigidity. The results of this paper, together with results of Sela ([Sel1, Sel2]) and Kharlampovich–Myasnikov ([KM1, KM2]) for hyperbolic groups (which include, in particular, free groups and uniform rank one orthogonal groups), show that there is also a sharp contrast between the model theories of rank one arithmetic groups and higher rank arithmetic groups.

This paper focuses on higher rank non-uniform arithmetic groups and uniform arithmetic groups of orthogonal type. We show that the model theories of these groups are closely related to the model theory of the ring of
integers. More precisely, we show that such groups are bi-interpretable with the ring $\mathbb{Z}$. The notion of bi-interpretability is defined in §2; in category-theoretic terminology, two structures are bi-interpretable when their categories of imaginaries are equivalent as categories over the category of sets, see Remark 2.1 for the precise statement.

The setup is the following:

**Setting 1.1.** $K$ is a number field, $S$ is a finite set of places containing all archimedean ones, $A$ is the ring of $S$-integers in $K$, $G$ is a connected group scheme over $A$ such that $G_K$ is connected, simply connected, absolutely simple, rank$_S G \geq 2$ and $G$ satisfies one of the following:

1. $G_K$ is isotropic.

2. $G = \text{Spin}_q$, where $q : A^n \to A$ is a regular quadratic form on $A^n$ and there is a place $w \in S$ such that rank$_w G \geq 2$ (note that this rank is the Witt index, denoted by $i_q(K_w^n)$, of $q$ on $K_w^n$).

Finally, $\Gamma$ is a centerless congruence subgroup of $G(A)$.

For a specific example of a uniform lattice that satisfies the assumptions in Setting 1.1 let $D$ to be a square-free positive integer, let $A$ to be the ring of integers of $\mathbb{Q}(\sqrt{D})$, let $q$ be the quadratic from $q(\bar{x}) = x_1^2 + \ldots + x_n^2 - \sqrt{D}x_S^2 - \sqrt{D}x_9^2$, and let $\Gamma$ be the $p$th congruence subgroup of $\text{SO}_q(A)$, for some non-dyadic $p \triangleleft A$.

The main result of this paper is:

**Theorem 1.2.** Under Setting 1.1 assume further that $n \geq 9$ if $G = \text{Spin}_q$. The group $\Gamma$ is bi-interpretable with the ring $\mathbb{Z}$.

Theorem 1.2 together with the results of Sela and Kharlampovich–Myasnikov on hyperbolic groups lead to following conjecture:

**Conjecture 1.3.** Let $\Delta$ be an irreducible lattice in a semisimple group $\prod_{v \in S} G(K_v)$. Then $\Delta$ is bi-interpretable with the ring of integers if and only if rank$_S G \geq 2$.

Bi-interpretability with the integers has many consequences, we discuss a few of them.

**Corollary 1.4.** Under Setting 1.1 assume that $n \geq 9$ if $G = \text{Spin}_q$. The first order theory of $\Gamma$ is undecidable.
Indeed, $\Gamma$ interprets the ring of integers and the first order theory of every structure that interprets the ring of integers is undecidable. On the other hand, Kharlampovich–Myasnikov [KM1] proved that the first order theory of non-abelian free groups is decidable. In the preprint [KM3], they extended this result to all torsion free hyperbolic groups.

**Corollary 1.5.** Under Setting 1.1, assume that $n \geq 9$ if $G = \text{Spin}_q$. All the finitely generated subgroups of $\Gamma$ are definable.

Corollary 1.5 is an immediate consequence of Theorem 1.2 and a theorem of Gödel which states that any recursively enumerable set in $\mathbb{Z}^n$ is definable. In contrast, Sela [Sel2] and Kharlampovich–Myasnikov [KM2] proved that the only definable non-trivial proper subgroups of a torsion free hyperbolic group are its cyclic subgroups.

**Corollary 1.6.** Under Setting 1.1, assume that $n \geq 9$ if $G = \text{Spin}_q$. Then, in the class of finitely generated groups, $\Gamma$ is determined by a single first order sentence, in the following sense: there is a first order sentence $\varphi$ such that, if $\Lambda$ is a finitely generated group, then $\Lambda$ satisfies $\varphi$ if and only if $\Lambda \cong \Gamma$.

Corollary 1.6 follows from a result of Khelif [Khe, Lemma 1]. This corollary should be compared with the following result of Sela (Sel2): for any torsion-free hyperbolic group $\Gamma$, any first order sentence that holds in $\Gamma$, also holds in $\Gamma \ast F_n$ (and vice versa).

The property that a group is determined by a single first order sentence (in the class of all finitely generated groups) was first studied by Nies in a more general setting (see Nie1 and Khe, Las1, Las2, Nie2, Nie3, OS for more recent work). Nies called this property *quasi-finitely axiomatizable*. There are groups which are quasi-finitely axiomatizable but are not bi-interpretable with the integers. For example, Khelif and Nies (see Khe and Nie3) proved that the Heisenberg group $U_3(\mathbb{Z})$ is quasi-finitely axiomatizable but not bi-interpretable with the integers.

We now discuss the assumption about the triviality of the center. It is possible to extend Corollary 1.6 and prove that any central extension of $\Gamma$ by a finite group is quasi-finitely axiomatizable. It turns out that generalizing Theorem 1.2 to central extensions is related to word width in $\Gamma$. Recall that every group $\Gamma$ as in Setting 1.1 is finitely presented (see PR Theroem 5.11 and the reference therein).
Theorem 1.7. Let \( \Gamma \) be a finitely presented group which is bi-interpretable with the ring \( \mathbb{Z} \). Let \( \Delta \) be a central extension of \( \Gamma \) by a group of size \( d \). Then \( \Delta \) is bi-interpretable with \( \mathbb{Z} \) if and only if the word \( x^d[y,z] \) has finite width in \( \Gamma \).

We find the connection between bi-interpretability and width of words exciting because, even though width of words has been extensively studied (see, for example, [Seg] and [Sha] and the reference therein), to the best of our knowledge, there is not even one example of a non-silly word \( w \) and a higher rank uniform lattice \( \Gamma \) for which it is known whether the width of \( w \) in \( \Gamma \) is finite or not. We note that more is known about widths of words in non-uniform lattices, see, for example, [AM] for widths of words in \( \text{SL}_n(\mathbb{Z}) \).

We conjecture that higher rank lattices have finite word widths:

Conjecture 1.8. Let \( \Delta \) be an irreducible lattice in a semisimple group \( \prod_{v \in S} G(O_S) \) and let \( w \in F_n \) be a word. Then the width of \( w \) in \( \Delta \) is finite if and only if \( \text{rank}_S G \geq 2 \).

For the only if direction, see [BBT].

In the proof of Theorem 1.2 we prove an effective version of a theorem of Kneser which might be interesting on its own. In order to state it, we need a couple of definitions.

Definition 1.9. Under Setting 1.1, assume that \( G = \text{Spin}_q \) and let \( S_{\text{def}} \) be the set of real places \( v \in S \), for which \( \text{Spin}_q(K_v) \) is compact.

1. For every \( v \in S_{\text{def}} \), let \( || \cdot ||_v \) be the norm on \( K^n_v \) defined by \( ||a||_v := \sqrt{q(a)} \) for every \( a \in K^n_v \).

2. For every \( v \in S_{\text{def}} \), let \( \text{dist}_v(\cdot, \cdot) \) be the bi-invariant metric on \( \text{SO}_q(K_v) \) defined by for all \( \alpha, \beta \in \text{SO}_q(K_v) \),

\[
\text{dist}_v(\alpha, \beta) := \sup\{||(\alpha - \beta)a||_v \mid a \in K^n_v \text{ and } ||a||_v = 1\}.
\]

3. An element \( \alpha \in \text{SO}_q(K) \) is called \( \epsilon \)-separated if for every \( v \in S_{\text{def}} \),

\[
\text{dist}_v(\alpha, Z(\text{SO}_q(K_v))) \geq \epsilon.
\]

4. An element \( \alpha \in \Gamma \) is called \( \epsilon \)-separated if its image in \( \text{SO}_q(K) \) is \( \epsilon \)-separated.

\( w \in F_n \) is called silly if its image in the abelianization \( \mathbb{Z}^n \) of \( F_n \) is primitive. If \( w \) is silly, then \( w(\Gamma) = \Gamma \), for any group \( \Gamma \).
Definition 1.10. For every element $\alpha$ in a group $\Gamma$ denote
\[ \text{gcl}_\Gamma(\alpha) := \{ \beta \alpha \beta^{-1}, \beta \alpha^{-1} \beta^{-1}, \text{id} | \beta \in \Gamma \}. \]
Note that $\text{gcl}_\Gamma(\alpha)$ is a symmetric and normal set.

The following is an effective version of Theorem 6.1 of [Kne]:

**Theorem 1.11.** Under Setting 1.1, assume that $G = \text{Spin}_q$ and $n \geq 7$. For every $\epsilon > 0$ there exists $N = N(n, \epsilon)$ such that for every $\epsilon$-separated element $\alpha \in \Gamma$ and every non-isotropic $a \in A^n$, $\text{gcl}_\Gamma(\alpha)^N a$ contains an $S$-adelic open neighborhood of $\Gamma a$.

**Remark 1.12.** We make the following convention: when we write $N = N(X, Y, Z)$, it means that the constant $N$ depends only on $X$, $Y$ and $Z$. For example, the constant in Theorem 1.11 does not depend on the quadratic from $q$ nor on $\Gamma$.

The paper is organized as follows. In §2 we collect the model-theoretic definitions we use. In §3 we study products of conjugacy classes in locally compact and arithmetic groups. In §4 we show that the collection of congruence subgroups of $\Gamma$ is uniformly definable. In §5 we show that $\Gamma$ interprets the ring $\mathbb{Z}$. In §6 we complete the proof of Theorem 1.2 and show that $\Gamma$ is bi-interpretable with $\mathbb{Z}$. In §7 we prove Theorem 1.1 and, in §8 we prove Theorem 1.11.

**Remark 1.13.** In the final stages of writing this paper, we became aware of the preprint [ST] which proves that a higher rank Chevalley group $G(R)$ is bi-interpretable with $R$, under some conditions on $R$ (which include the case $R = O_S$); see also [MM] for the case $\text{SL}_n(O_S)$. The proofs in these two papers go along the proof of the bi-interpretability of a field $F$ and $\text{SL}_n(F)$, although the analysis in the case of Chevalley groups is harder. In particular, the proof uses in a crucial way information about rational tori and root subgroups, as well as bounded generation. Our goal here is to develop techniques that could be applied to general higher rank lattices. Even in the case of $\text{SL}_n$, the techniques in this paper can be used to prove stronger results: Theorem A.6 implies that, for every $n \geq 3$ and every integral domain $R$ with trivial Jacobson radical and finite Krull dimension, $\text{PSL}_n(R)$ and $R$ are bi-interpretable. In particular, there is no assumption on the stable range of $A$. For example, Theorem A.6 implies that, for every $m \geq 1$, $\text{PSL}_3(\mathbb{Z}[X_1, \ldots, X_m])$ is bi-interpretable with $\mathbb{Z}[X_1, \ldots, X_m]$ (and thus also with $\mathbb{Z}$).
Acknowledgement We thank Alex Lubotzky and Peter Sarnak for helpful discussions. N.A. was partially supported by NSF grant DMS-1902041, BSF grant 2018201, and a Simons Fellowship. C.M. was partially supported by ISF grant 1226/19 and BSF grant 2014099.

2 Model Theory

In this section, we collect the definitions of definable sets, imaginaries, uniformly definable collections, and interpretations.

1. For a first-order language $L$ and an $L$-structure $M$, we let $L_M$ be the language $L$ together with a constant symbol for every element of $M$. We denote the $L_M$-theory of $M$ by $\text{Th}_M$.

2. Let $M$ be an $L$-structure. For every $L_M$-formula $F(x_1, \ldots, x_n)$, denote $F(M) := \{(a_1, \ldots, a_n) \in M^n \mid F(a_1, \ldots, a_n) \text{ holds in } M\}$.

A subset of $M^n$ of the form $F(M)$ is called a definable set (in $M$). Note that we say that $F$ is definable in $M$ although it is a subset of some power of $M$. A function between two definable sets is called definable if its graph is definable.

3. Let $Y$ and $Z$ be two definable subsets in $M$. For every definable subset $X \subseteq Y \times Z$ and every $y \in Y$, denote $X_y := \{z \in Z \mid (y, z) \in X\}$. A collection $Z$ of subsets of a definable set $Z$ is called uniformly definable by a parameter set $Y$ if there exists a definable subset $X \subseteq Y \times Z$ such that $Z = \{X_y \mid y \in Y\}$.

4. Given a definable set $X$ and a definable equivalence relation $E \subseteq X \times X$, the set of $E$-equivalence classes is called an imaginary. Note that any definable set is also an imaginary. The notions of subset, cartesian product, relation, and function are generalized in the obvious way to imaginaries.

5. Suppose that $L_1, L_2$ are two (possibly different) first-order languages, and that, for $i = 1, 2$, $M_i$ is a structure of $L_i$. An interpretation of $M_2$ in $M_1$ is a pair $\mathcal{F} = (F, f)$, where $F$ is an imaginary in $M_1$ and $f$ is a bijection between the sets $F$ and $M_2$ such that
(a) For each \( n \)-ary relation symbol \( r \) of \( L_2 \), the imaginary \( f^{-1}(r^{M_2}) \subset F^n \) is definable.

(b) For every function symbol \( g \) of \( L_2 \), say of arity \( (r, s) \), the function \( f^{-1} \circ g^{M_2} \circ f : F^r \to F^s \) is definable.

6. Suppose that \( \mathcal{F} = (F, f) \) is an interpretation of \( M_2 \) in \( M_1 \). By induction on the length of a defining formula, we can define, for each imaginary \( X \) in \( M_2 \), an imaginary \( \mathcal{F}^*X \) of \( M_1 \) and a bijection \( f_X : \mathcal{F}^*X \to X \). Similarly, if \( X \) and \( Y \) are imaginaries in \( M_2 \) and \( g : X \to Y \) is a definable function, then there exists a definable function \( \mathcal{F}^*g : \mathcal{F}^*X \to \mathcal{F}^*Y \) in \( M_2 \).

7. Suppose that, for \( i = 1, 2, 3 \), \( L_i \) is a first order language and \( M_i \) is a structure of \( L_i \). Suppose that \( \mathcal{F} = (F, f) \) is an interpretation of \( M_2 \) in \( M_1 \) and that \( \mathcal{H} = (H, h) \) is an interpretation of \( M_3 \) in \( M_2 \). The composition \( \mathcal{H} \circ \mathcal{F} \) of \( \mathcal{F} \) and \( \mathcal{H} \) is the interpretation of \( M_3 \) in \( M_1 \) given by \( \mathcal{F}^*H, h \circ f_H \).

8. If \( M \) is a structure of a language \( L \) and \( \mathcal{F} = (F, f) \) is a self interpretation of \( M \), we say that \( \mathcal{F} \) is trivial if \( f \) is definable.

9. Let \( L_1, L_2 \) be first order languages, and, for \( i = 1, 2 \), let \( M_i \) be a structure of \( L_i \). Given an interpretation \( \mathcal{F}_{1,2} \) of \( M_2 \) in \( M_1 \) and an interpretation \( \mathcal{F}_{2,1} \) of \( M_1 \) in \( M_2 \), we say that \( (\mathcal{F}_{1,2}, \mathcal{F}_{2,1}) \) is a bi-interpretation if both compositions \( \mathcal{F}_{1,2} \circ \mathcal{F}_{2,3} \) and \( \mathcal{F}_{2,3} \circ \mathcal{F}_{1,2} \) are trivial. If there is a bi-interpretation between \( M_1 \) and \( M_2 \), we say that they are bi-interpretable.

**Remark 2.1.** We can reformulate the notions of interpretations and bi-interpretations in a categorical language. Let \( \text{Cat} \) be the 2-category of categories, and let \( \text{Sets} \) be the category of sets. Given a first order language \( L \) and an \( L \)-structure \( M \), denote by \( \text{Def}_M \) the category whose objects are imaginary sets in \( M \) and whose morphisms are definable maps between them. We have a functor \( M_{pts} : \text{Def}_M \to \text{Sets} \) sending a definable set \( X \) to \( X(M) \). The pair \( (\text{Def}_M, M_{pts}) \) is an object in the slice 2-category \( \text{Cat}_{/\text{Sets}} \). Under these definitions, an interpretation between the structures \( M, N \) is a 1-morphism between the objects \( (M, M_{pts}) \) and \( (N, N_{pts}) \); a bi-interpretation is an equivalence of these objects.
3 Uniform density of conjugacy class products

3.1 Statement of the results

In this section, our setting is more general than Setting 1.1. Instead, we use the following:

Setting 3.1. Assume that

- $K$ is a number field.
- $S$ is a finite set of places of $K$ containing all archimedean places. Denote the ring of $S$-integers of $K$ by $A$.
- $w$ is a place in $S$.
- $D$ is a natural number and $G \subset (GL_D)_A$ is an algebraic group scheme defined over $A$ such that $G_K$ is connected, simply connected, and simple, and such that $G(K_w)$ is non-compact.
- $\Gamma$ is a subgroup of finite index in $G(A)$. If $v$ is a place of $K$, denote the closure of $\Gamma$ in $G(K_v)$ by $\Gamma_v$.

Definition 3.2. Let $F$ be a local field with ring of integers $R$ and maximal ideal $m$. Let $D$ be a natural number and let $H \subset GL_D$ be a semisimple algebraic group scheme over $R$. Denote the Lie ring of $H$ by $\mathfrak{h}$. We say that $H$ is good if the following conditions hold:

1. $H$ is smooth over $\text{Spec} \, R$.
2. The reduction map $Z(H(R)) \to Z(H(R/m))$ is onto.
3. $H(R/m)$ acts irreducibly on $\mathfrak{h}(R/m)$.
4. The kernel of $\text{Ad} : H(R/m) \to \text{Aut}(\mathfrak{h}(R/m))$ is $Z(H(R/m))$.
5. The characteristic of $R/m$ is greater than $|Z(G)| + (4D \dim H)^4$.

Note that, by the classification of simple algebraic groups over finite fields, we get that $H(\mathbb{F}_q)$ acts irreducibly on its Lie algebra.
Definition 3.3. In Setting 3.1, define $T_{\Gamma}$ to be the set of all places $v \not\in S$ such that $G_{A_v}$ is good and $\Gamma$ is dense in $G(A_v)$.

Remark 3.4. In Setting 3.1, $T_{\Gamma}$ is always finite. Indeed, Condition 1 follows from generic smoothness, Condition 2 follows from generic smoothness of the group scheme $Z(G)$ and Hensel’s lemma, Condition 3 follows because $G(K)$ acts irreducibly on $g(K)$ and this is a Zariski open condition, and Condition 4 follows because it holds over $\overline{K}$.

Definition 3.5. In Setting 3.1, for every real place $v$ of $K$ such that $G(K_v)$ is compact, we define the standard metric on $G(K_v)$ as follows:

1. If $G_{K_v} = \text{Spin}_f$, for some (positive-definite) quadratic form $f$ on $K_v^n$, let $d_v$ be the metric induced by the norm $f$:

$$d_v(g_1, g_2) = \max \left\{ \sqrt{f(g_1 x - g_2 x)} \mid x \in K_v^n, f(x) = 1 \right\}.$$

2. In all other cases, let $d_v$ be the translation-invariant Riemannian metric on $G(K_v)$ whose restriction to the Lie algebra of $G(K_v)$ is the Killing form, and normalized such that the diameter of $d_v$ is one.

Remark 3.6. The reason for the different definition for spin groups is that it simplifies the notations in the proof of Theorem 1.11 in §8. Since the norm metric and the Killing metric are bi-Lipschitz, one can use the Killing metric in both cases after changing some constants in §8.

Definition 3.7. In Setting 3.1, given $g \in \Gamma$ and $\epsilon > 0$, we say that $g$ is $\epsilon$-separated if, for any real valuation $v$ of $K$ such that $G(K_v)$ is compact, we have $d_v(g, Z(G(K_v))) > \epsilon$, where $d_v$ is the standard metric on $G(K_v)$ from Definition 3.5.

The main results of this section are the following three claims:

Proposition 3.8. In Setting 3.1, for every $\epsilon > 0$, there is a natural number $N = N(K, S, D, \epsilon)$ such that the following holds:

If $G(K_w)$ is non-compact, and $g \in \Gamma$ is $\epsilon$-separated, then there is a neighborhood $W$ of the identity in $\prod_{v \in T_{\Gamma}} G(K_v)$ such that the set $gcl_{\Gamma}(g)^N$ contains a dense subset of $W \times \prod_{v \not\in T_{\Gamma} \cup \{w\}} (gcl_{T_{\Gamma}}(g))$. 9
Remark 3.9. Under the more restrictive Setting 1.1, for every non-archimedean \( v \in S \), the group \( G(K_v) \) is non-compact. In that case, we can prove Proposition 3.8 without using Lemma 3.20 below and conclude that (under Setting 1.1) the constant \( N \) depends only on \( D \) and \( \epsilon \).

Proposition 3.10. In Setting 3.1, for every \( \epsilon > 0 \) there exists a constant \( N = N(\Gamma, \epsilon) \) such that, for every \( \epsilon \)-separated element \( g \in \Gamma \), \( \mathrm{gcl}_\Gamma(g)^N \) is dense in \( \langle \mathrm{gcl}_\Gamma(\alpha) \rangle \) with respect to the topology induced by \( G(A(K)_{\{w\}}) \), where \( A_{\{w\}} = \prod_{v \neq w} K_v \) is the ring of \( w \)-adeles. In particular, it is dense in the congruence topology.

Note that the constant \( N \) in Proposition 3.8 depends only on \( K, S, D, \epsilon \) and not on \( G \) or \( \Gamma \). In contrast, the constant \( N \) in Proposition 3.10 does depend on \( \Gamma \).

Proposition 3.11. In Setting 3.1, there exists a constant \( N = N(\Gamma) \) such that, for every principal congruence subgroup \( \Delta \) contained in \( \Gamma \), there are \( \alpha_1, \ldots, \alpha_N \in \Delta \) such that \( \prod_{1 \leq i \leq N} \mathrm{gcl}_\Gamma(\alpha_i) \) is a dense subset of \( \Delta \), with respect to the congruence topology.

3.2 Finite

Lemma 3.12. Let \( H \subseteq \text{GL}_D \) be a connected and simple algebraic group defined over a finite field \( \mathbb{F}_q \) of characteristic \( p > (4D \dim H)^4 \). Denote the Lie algebra of \( H \) by \( \mathfrak{h} \). Denoting the simply connected cover of \( H \) by \( H^{sc} \), assume that \( H^{sc}(\mathbb{F}_q) \) acts irreducibly on \( \mathfrak{h}(\mathbb{F}_q) \). Then, for every non-zero \( X \in \mathfrak{h}(\mathbb{F}_q) \), we have
\[
\underbrace{\text{Ad}(H(\mathbb{F}_q))X + \cdots + \text{Ad}(H(\mathbb{F}_q))X}_{4 \dim H \text{ times}} = \mathfrak{h}(\mathbb{F}_q).
\]

Proof. Denote \( d = \dim H \). It is well-known that \( H^{sc}(\mathbb{F}_q) \) acts irreducibly on \( \mathfrak{h}(\mathbb{F}_q) \) and the action factors through \( H(\mathbb{F}_q) \), it follows that there is no subspace of \( \mathfrak{h}(\mathbb{F}_q) \) which is invariant under all \( p \)-elements of \( H(\mathbb{F}_q) \).

Since \( D < p \), the logarithm map is defined on the set of \( p \) elements of \( H(\mathbb{F}_q) \), and \( \log(u) \in \mathfrak{h}(\mathbb{F}_q) \), for every such \( u \). Since \( \text{Ad}(u) = \exp(ad(\log(u))) \), there is no non-trivial subspace invariant under all elements of the set
\[
\{ad(\log(u)) \mid u \in H(\mathbb{F}_q) \text{ is a } p\text{-element}\}.
\]
It follows that there are $u_1, \ldots, u_d \in H(\mathbb{F}_q)$ such that \{ad$(\log(u_i))X$\} is a basis for $h(\mathbb{F}_q)$.

Denote $u^t = \exp(t \log(u))$ and define a map $F : \mathbb{A}^d \to h$ by

$$F(t_1, \ldots, t_d) = (\text{Ad}(u_1^{t_1}) \circ \text{Ad}(u_2^{t_2}) \circ \cdots \circ \text{Ad}(u_d^{t_d}))(X).$$

$F$ is a polynomial map of degree $2dD$ and its derivative at $(0, \ldots, 0)$ is the map

$$dF(0, \ldots, 0)(t_1, \ldots, t_d) = \sum t_i \text{ad}(\log(u_i))X.$$

Since \{ad$(\log(u_i))X$\} is a basis, $dF(0, \ldots, 0)$ is onto. In particular, $F$ is a dominant map. Let $\mu$ be the measure on $h(\mathbb{F}_q)$ given by $\mu = \sum_{a \in \mathbb{F}_q} \delta_a$, where $\delta_a$ is the delta measure at $a$. For every $t \in \mathbb{F}_q$, $u^t \in H(\mathbb{F}_q)$, so $\text{supp}(\mu) \subseteq \text{Ad}(H(\mathbb{F}_q))X$.

Fix a non-trivial additive character $\psi$ of $\mathbb{F}_q$. Let $\chi : h(\mathbb{F}_q) \to \mathbb{C}^\times$ be an additive character. Then $\chi = \psi \circ \varphi$, where $\varphi : h(\mathbb{F}_q) \to \mathbb{F}_q$ is a $\mathbb{F}_q$-linear map.

Denoting the Fourier transform of $\mu$ by $\hat{\mu}$, we have

$$\hat{\mu}(\chi) = \sum_{a \in \mathbb{F}_q} \psi(-\varphi \circ F)(a).$$

The polynomial $\varphi \circ F$ has degree $2dD < p$. The Weil bounds (see \text{SGA4}$^2$ Proposition 3.8]) give

$$|\hat{\mu}(\chi)| < (2dD)q^{d - \frac{1}{2}},$$

for all non-trivial characters $\chi$. We have

$$\left|\sum_{\chi \text{ non-trivial}} \hat{\mu}^*d(\chi)\right| \leq \sum_{\chi \text{ non-trivial}} |\hat{\mu}(\chi)|^{4d} < q^d(2dD)^{4d}q^{4d^2 - 2d} < q^{4d^2} = \hat{\mu}^*d(1).$$

By Placherel inversion theorem,

$$|\mu^*d(g)| = \left|\sum_{\chi} \hat{\mu}^*d(\chi)\chi(g)\right| \geq \hat{\mu}^*d(1) - \sum_{\chi \text{ non-trivial}} \hat{\mu}^*d(\chi) > 0,$$

so

$$h(\mathbb{F}_q) = \text{supp}(\mu^*d) \subseteq \text{Ad}(H)X + \cdots + \text{Ad}(H)X.$$
3.3 Local

In this section, we prove several local versions of Propositions 3.8, 3.10, and 3.11. The versions we prove are for compact Lie groups (Lemma 3.17), non-compact groups (Lemma 3.18), compact p-adic groups (Lemma 3.20), and another version for compact p-adic groups (Lemma 3.22) which works only for good compact p-adic groups, but gives a uniform bound on the exponent $N$.

We will use the following quantitative version of the open mapping theorem:

Lemma 3.13. Let $R$ be the ring of integers of a non-archimedean local field, let $m \subseteq R$ be the maximal ideal, and let $X, Y \subset R^d$ be $p$-adic manifolds. There is a constant $C$ such that, for every function $f : X \rightarrow Y$ which is given by a convergent power series with coefficients in $R$, every $x_0 \in X$, and every natural number $n$ such that $df_{x_0}(T_{x_0}X \cap R^d) \supseteq m^n(T_{f(x_0)}Y \cap R^d)$, we have $f(X) \supseteq Y \cap (f(x_0) + m^n + C R^d)$. Moreover, for every $k \geq 0$, we have $f(X \cap (x_0 + m^k R^d)) \supseteq Y \cap (f(x_0) + m^{n+k} + C R^d)$.

The following is an immediate consequence of Lemma 3.13:

Lemma 3.14. Suppose that either $X, Y, Z$ are real manifolds or that they are $p$-adic manifolds. Let $f : X \times Y \rightarrow Z$ be a continuously differentiable function. For each $y \in Y$, let $f_y : X \rightarrow Z$ be the function $f_y(x) = f(x, y)$. Assume that there is a point $(x_0, y_0)$ for which $df_{y_0}(x_0) : T_{x_0}X \rightarrow T_{f(x_0,y_0)}Z$ is onto. Then there are open sets $U \subseteq Y$ and $V \subseteq Z$ such that $y_0 \in U$, $f(x_0, y_0) \in V$, and $f_y(X) \supseteq V$, for every $y \in U$.

A compactness argument together with Lemma 3.14 yields:

Corollary 3.15. Suppose that either $X, Y, Z$ are real manifolds or that they are $p$-adic manifolds, let $z_0 \in Z$, and let $C \subseteq Y$ be a compact set. Let $f : X \times Y \rightarrow Z$ be a continuously differentiable function. Assume that, for each $y \in C$ there is $x \in X$ such that $f(x, y) = z_0$ and $df_y(x)$ is onto. Then there is an open set $z_0 \in V \subseteq Z$ such that, for each $y \in C$, $V \subseteq f_y(X)$.

Lemma 3.16. Let $F$ be a local field, let $H$ be a connected and almost simple algebraic group defined over $F$ and let $H = H(F)$. Let $U \subseteq H$ be a neighborhood of 1 and let $C \subseteq H$ be a compact set disjoint from $Z(H)$. Then there is an identity neighborhood $V \subseteq H$ such that, for every $g \in C$, $V \subseteq \text{gcl}_{U}(g)^{\dim_{F}U}$.
Proof. Let \( d = \dim_F H \) and define \( \Phi : U^{2d} \times H \to H \) as the map

\[
\Phi(h_1, \ldots, h_d, x_1, \ldots, x_d, g) = \prod_{i=1}^{d} \left(h_i^{-1}g^{-1}x_ig^{-1}h_i\right).
\]

We claim that the conditions of Corollary 3.15 hold for \( X = U^{2d}, Y = Z = H, \) \( z_0 = 1, C = C, \) and \( f = \Phi. \) It then follows that there is an identity neighborhood \( V \subseteq H \) such that, for all \( g \in C, V \subseteq \Phi_g(U^{2d}) \subseteq \text{gcl}_V(g)^{d}. \)

Denote the Lie algebra of \( H \) by \( \mathfrak{g} \) and let \( g \in C. \) Since \( g \) is not central, the subspace \( W := (\text{Ad}(g) - \text{Id})(\mathfrak{g}) \) is non-trivial. By assumption, the adjoint action of any open subgroup of \( H \) on \( \mathfrak{g} \) is irreducible, so there are \( h_1, \ldots, h_d \in U \) such that \( \text{Ad}(h_1)W + \cdots + \text{Ad}(h_d)W = \mathfrak{g}. \) The linear map \( d\Phi_g(h_1, \ldots, h_d, 1, \ldots, 1) : \mathfrak{g}^{2d} \to \mathfrak{g} \) takes the vector \((0, \ldots, 0, X_1, \ldots, X_d)\) to \( \sum \text{Ad}(h_i)(\text{Ad}(g)X_i - X_i). \) Therefore, the conditions of Corollary 3.15 hold.

Lemma 3.17. Let \( H \) be a compact connected almost simple real Lie group, and let \( C \subseteq H \) be a compact set disjoint from \( Z(H). \) There is an \( N = N(H, C) \) such that, for every \( g \in C, \) \( \text{gcl}_H(g)^N = H. \)

Proof. Let \( \rho \) be a bi-invariant Riemannian metric on \( H \) with diameter 1. By Lemma 3.16 (applied with \( U = H \)), there is an \( \epsilon > 0 \) such that \( \text{gcl}(g)^{\dim H} \) contains the ball of radius \( \epsilon \) around the identity, for all \( g \in C. \) Since the metric is bi-invariant and geodesic, the product of a ball of radius \( a_1 \) and a ball of radius \( a_2 \) is a ball of radius \( \min\{a_1 + a_2, 1\}. \) It follows that \( \text{gcl}_H(g)^{\lfloor 1/\epsilon \rfloor \dim H} = H. \)

Lemma 3.18. Let \( F \) be a local field, let \( H \) be connected semisimple algebraic group over \( F \) such that \( H(F) \) is non compact, and let \( H \subseteq H(F) \) be an open subgroup. Then there is \( N = N(F, H, H) \) such that, for every \( g \in H, \) we have \( \text{gcl}_H(g)^N = \langle \text{gcl}_H(g) \rangle \)

Proof. The claim is clear for \( g \in Z(H) \) (taking \( N = |Z(H)| \)), so we may assume \( g \notin Z(H). \) Fix a maximal split torus \( A \subseteq H(F), \) a maximal compact subgroup \( K \subseteq H(F), \) and a non-trivial unipotent \( u_0. \)

First assume that \( F \) is non-archimedean. By Lemma 3.16 applied with \( C = \{u_0\} \) and \( U = H, \) there is an open neighborhood of 1 that is contained in \( \text{gcl}_H(u_0)^{\dim_F H}. \) In particular, there is a natural number \( M \) such that the set \( \text{gcl}_H(u_0)^{\dim_F H} \cap K \) contains a subgroup of index at most \( M \) in \( K. \)
We will show that the claim of the lemma holds with $N = 2(\dim_F H)^2 + 5(\dim_F H)(\dim_F A) + M^2$.

By Lemma 3.16 applied with $C = \{g\}$ and $U = H$, $gcl_H(g)^{\dim_F H}$ contains an open neighborhood of $1$. Since it is conjugation invariant, $gcl_H(g)^{\dim_F H}$ contains all unipotents. In particular, it contains $u_0$. It follows that $gcl_H(g)^{\dim_F H}^2$ contains a subgroup of index at most $M$ in $K$.

For any root $\alpha$ of $A$, there is a homomorphism $\phi_\alpha : SL_2(F) \to H(F)$ whose image contains the root group. We claim that $\phi_\alpha^{-1}(H) = SL_2(F)$. Indeed, let $H_+ = \left\{ x \in F \mid \phi_\alpha \left( \begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right) \in H \right\}$, $H_0 = \left\{ x \in F^\times \mid \phi_\alpha \left( \begin{array}{cc} x & 0 \\ x^{-1} & 1 \end{array} \right) \in H \right\}$, and $H_- = \left\{ x \in F \mid \phi_\alpha \left( \begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right) \in H \right\}$. Then $H_+, H_-$ are finite index subgroups of $F$ that are invariant under $H_0$, which is a finite index subgroup of $F^\times$. Hence, $H_+ = H_- = F$ and $\phi_\alpha^{-1}(H) = SL_2(F)$.

For every unipotent element $u \in SL_2(F)$, we have $gcl_{SL_2(F)}(u)^5 = SL_2(F)$ (see, for example, [VW, Theorem 2.5]). Hence, $gcl_H(g)^{\dim_F H}$ contains the entire root subgroup of $\alpha$. Since the root subgroups of $A$ generate $A$, we get that $A \subseteq gcl_H(g)^{\dim_F H}$. By Cartan decomposition, we get that $gcl_H(g)^{\dim_F H}^2$ contains a subset of index at most $M^2$ in $H(F)$, and the claim follows.

In the case $F$ is archimedean, the proof is similar, replacing the condition that $gcl_H(u_0)^{\dim_F H} \cap K$ contains a subgroup of index at most $M$ in $K$ by the condition that $(gcl_H(u_0)^{\dim_F H} \cap K)^M = K$.

For the rest of this subsection, we will use the following setting:

**Setting 3.19.** $F$ is a non-archimedean local field with ring of integers $R$ and maximal ideal $m$. $D$ is a natural number, $H \subseteq GL_D$ is a simple algebraic group over $R$, and $H \subseteq H(R)$ is a compact open subgroup. We denote the Lie ring of $H$ by $h$, the $m^k$-th congruence subgroup of $GL_D(R)$ by $GL_D(R;m^k)$, and denote $H[m^k] := H \cap GL_D(R;m^k)$.

**Lemma 3.20.** In Setting 3.19 there are constants $c = c(F, D, H, H)$, $N = N(F, D, H, H)$ such that

1. For every $n$, if $g \in H \setminus (Z(H) \cdot H[m^n])$, then $gcl_H(g)^{\dim_H Z(H)[m^n]} \subseteq H[m^{n+c}]$.

2. For any $g \in H$, $gcl_H(g)^N = \langle gcl_H(g) \rangle$.
3. For any normal subgroup $L$ of $H$, there are $h_1, \ldots, h_N \in L$ such that $L = \text{gcl}_H(h_1) \cdots \text{gcl}_H(h_N)$.

Proof. Denote $d = \dim_F H$, $q = |R/m|$, and $b = \text{val}_m |Z(H)|$.

1. Let $c_1$ be the constant from Lemma 3.13 applied to $X = R^d$ and $Y = H$. By enlarging $c_1$, we can assume that

   (a) The series $\exp$ converges on $m^{c_1}g$ and $\exp(m^{c_1}g) = H[m^{c_1}]$ (and, hence, $\exp(m^k g) = H[m^k]$, for every $k \geq c_1$).

   (b) $[g, g] \supseteq m^{c_1}g$.

By Lemma 3.16, there is $c_2$ such that, for every $g \in H \setminus Z(H) \cdot H[m^{c_1}]$, $\text{gcl}_H(g)^d \supseteq H[m^{c_2}]$. We will prove that the claim holds with $c = \max \{2c_1 + b, c_2\}$.

Suppose $g \in H \setminus Z(H) \cdot H[m^n]$, and let $a$ be the minimal number such that $g \in H \setminus Z(H) \cdot H[m^a]$. Then $1 \leq a \leq n$. There are two cases:

Case 1: $a \leq c_1$. In this case, $g \in H \setminus Z(H) \cdot H[m^{c_1}]$ and, by the definition of $c_2$, we have $\text{gcl}_H(g)^d \supseteq H[m^{c_2}] \supseteq H[m^{a+c}]$.

Case 2: $a \geq c_1 + 1$. In this case, $g \in Z(H) \cdot H[m^{a-1}] \subseteq Z(H) \cdot H[m^{c_1}]$, so $g = \zeta \exp(X)$, where $\zeta \in Z(H)$ and $X \in m^{a-1}g \setminus m^a g$. Denoting $Y = |Z(H)| X$, we get that $g^{Z(H)}|X = \exp(Y)$ and $Y \in m^{a-1+b}g \setminus m^{a+b}g$. By the definition of $c_1$, there are $X_1, \ldots, X_d \in m^{c_1}g$ such that the elements $[X_i, Y]$ are in $m^{a-1+b+2c_1}g$ and their reduction modulo $m^{a+b+2c_1}$ is a basis. Let $\Phi : R^d \to H$ be the function

$$\Phi(t_1, \ldots, t_d) = [\exp(-t_1 X_1), g^{Z(H)}] \cdots [\exp(-t_d X_d), g^{Z(H)}]$$

Then $\Phi(0, \ldots, 0) = 1$ and $d\Phi(0, \ldots, 0)(R^d) \supseteq m^{a+b+2c_1-1}g$. By Lemma 3.13 $\text{gcl}_H(g)^{Z(H)}|d \supseteq \Phi(R^d) \supseteq H[m^{a+b+2c_1+c}]$.

2. Let $c$ be the constant from Claim 1. We will show that Claim 2 holds with $N = |Z(H)| \dim_F H + q^{cD^2}$. If $g \in Z(H)$, then $\text{gcl}_H(g)^{Z(H)} = \langle \text{gcl}_H(g) \rangle$. Assume now that $g \notin Z(H)$ and let $n$ be the minimal natural number such that $g \in H \setminus Z(H) \cdot H[m^n]$. We have

$$H[m^{c+n}] \subseteq \text{gcl}_H(g)^{Z(H)}|\dim_F H \subseteq \langle \text{gcl}_H(g) \rangle \subseteq Z(H) \cdot H[m^{a-1}].$$

Since $|H[m^{a-1}]|/|H[m^{c+n}]| < q^{(c+1)D^2}$, we get the result.
Let \( c \) be the constant from Claim \( 3 \). We show that Claim \( 3 \) holds with \( N = |Z(H)|q^{(c+1)D^2} \). If \( L \subset Z(H) \) then the claim holds. Otherwise, let \( n \) be the minimal natural number such that \( L \setminus Z(H) \cdot H[m^n] \neq \emptyset \), and choose \( h_1 \in L \setminus Z(H) \cdot H[m^n] \). By definition of \( c \),

\[
H[m^{n+c}] \subseteq \text{gcl}_H(h_1)|Z(H)|^{\dim_F G} \subseteq L \subseteq Z(H) \cdot H[m^{n-1}].
\]

Since \( |Z(H) \cdot H[m^{n-1}]/H[m^{n+c}]| < |Z(H)|q^{(c+1)D^2} \), the result follows.

\[ \square \]

**Lemma 3.21.** In Setting 3.19, assume that \( H \) is good. Let \( k \geq 1 \). Suppose \( g \in H(R) \) and \( (\text{Ad}(g) - \text{Id})h(R) \subseteq m^k h(R) \). Then \( g \in Z(H(R)) \cdot H(R; m^k) \).

**Proof.** For \( k = 1 \), this follows from the assumption that the action of \( H(R/m) \) on \( h(R/m) \) is faithful.

Assume now that \( k > 1 \). By the case \( k = 1 \), we know that \( g \in H(R; m) \). By assumption, \( g = \exp(Y) \), for some \( Y \in m h(R) \). Since \( \text{Ad}(g) = \exp(ad(Y)) \), we get that \( [Y, h(R)] \subseteq m^k h(R) \). Since \( h(R/m) \) has no center, we get by induction on \( k \) that \( Y \in m^k h(R) \), so \( g = \exp(Y) \in H(R; m^k) \).

\[ \square \]

**Lemma 3.22.** In Setting 3.19, assume that \( H \) is good. For every \( g \in H(R) \),

\[
\text{gcl}_{H(R)}(g)^{|Z(H(R))|^{\dim_H}} = \langle \text{gcl}_{H(R)}(g) \rangle.
\]

If \( g \in H(R) \setminus Z(H(R)) \cdot H(R)[m] \), then \( \langle \text{gcl}_{H(R)}(g) \rangle = H(R) \).

**Proof.** Denote \( d = \dim_H H \). If \( g \in Z(H(R)) \), the claim is clear. Assume now that \( g \in H(R) \setminus Z(H(R)) \cdot H(R)[m] \). By the smoothness assumption, \( h(R) \) is a free \( R \)-module of rank \( d \). By Lemma 3.21, the submodule \( V := (\text{Ad}(g) - \text{Id})(h(R)) \subseteq h(R) \) is not contained in \( m h(R) \). By the irreducibility of the action of \( H(R/m) \) and by Nakayama’s lemma, there are \( h_1, \ldots, h_d \in H(R) \) such that \( \text{Ad}(h_1)V + \ldots + \text{Ad}(h_d)V = h(R) \). Define \( \Psi : H(R)^d \to H(R) \) by

\[
\Psi(x_1, \ldots, x_d) = \prod_{i=1}^d (h_i^{-1}g^{-1}x_igx_i^{-1}h_i).
\]

We get that \( h(R) = d|\Psi|_{(1, \ldots, 1)}(h(R)^d) \), and, by Lemma 3.13, we get that \( H(R;m) \subseteq \Psi(H(R)^d) \subseteq \text{gcl}_{H(R)}(g)^d \). Since \( H \subseteq \text{gcl}_{H(R)}(g)^d \cdot H(R; m) \), the result follows.

Finally, assume \( g \in Z(H(R)) \cdot H(R)[m] \setminus Z(H(R)) \). Let \( k \geq 1 \) be the number such that \( g \in Z(H(R)) \cdot H(R; m^k) \setminus Z(H(R)) \cdot H(R; m^{k+1}) \). Since \( H \)
is good, $g^{[\mathcal{H}(R)]} \in \mathcal{H}(R; m^k) \setminus \mathcal{H}(R; m^{k+1})$. The same arguments as above imply that $\mathcal{H}(R; m^{k+1}) \subseteq \text{gcl}_{\mathcal{H}(R)}(g^{[\mathcal{H}(R)]})^d$.

Denote the image of $g^{[\mathcal{H}(R)]}$ in $\mathcal{H}(R; m^k)/\mathcal{H}(R; m^{k+1}) = \mathfrak{h}(R/m)$ by $X$. By Lemma 3.12

$$\text{Ad}(\mathcal{H}(R))X + \cdots + \text{Ad}(\mathcal{H}(R))X = \mathfrak{h}(R/m).$$

Taking exponents, we get that

$$(\text{gcl}_{\mathcal{H}(R)}(g^{[\mathcal{H}(R)]}))^{4d} \cdot \mathcal{H}(R; m^k) = \mathcal{H}(R; m^k),$$

so $\text{gcl}_{\mathcal{H}(R)}(g^{[\mathcal{H}(R)]})^{5d} \supseteq \text{gcl}_{\mathcal{H}(R)}(g^{[\mathcal{H}(R)]})^{4d} \text{gcl}_{\mathcal{H}(R)}(g^{[\mathcal{H}(R)]})^d \supseteq \mathcal{H}(R; m^k)$, from which the result follows.

### 3.4 Proofs of Propositions 3.8, 3.10, and 3.11

**Proof of Proposition 3.8.** By [PR, Theorem 6.16], for any local field $F$ and integer $D$, there are only finitely many connected semisimple algebraic subgroups of $\text{GL}_D$ up to isomorphism. Therefore, given $K, S, D$, there are finitely many locally compact groups $L_1, \ldots, L_M$ such that, if $G \subseteq \text{GL}_D$ is a connected, simply connected semisimple algebraic group defined over $K$ and $v \in S$, then $G(K_v)$ is isomorphic to one of the $L_j$s. Applying Lemmas 3.17 (for compact Lie groups), 3.18 (for non-compact groups), and 3.20 (for compact totally disconnected groups) to the groups $L_i$, there is $N_1$, depending only on $K, S, D, \epsilon$ such that

$$(\forall v \in S) \quad \text{gcl}_{G(K_v)}(g)^{N_1} = \langle \text{gcl}_{G(K_v)}(g) \rangle. \tag{1}$$

Let $N = \max \{N_1, 5D^3\}$. We will show that the claim holds for $N$. Indeed, given $g$, applying Lemma 3.16 for every $v \in T_1$, we get a neighborhood $W_v$ of 1 in $G(K_v)$ such that

$$(\forall v \in T_1) \quad \text{gcl}_{G_v}(g)^{N} \supseteq W_v. \tag{2}$$

Finally, by Lemma 3.22, we get

$$(\forall v \notin T_1 \cup S) \quad \text{gcl}_{G_v}(g)^{N} = \langle \text{gcl}_{G_v}(g) \rangle. \tag{3}$$
By the assumptions, $G$ satisfies strong approximation, so $\Gamma$ is dense in $\prod_{v \neq w} \Gamma_v$. It follows that the closure of $\text{gcl}_{\Gamma}(g)$ in $\prod_{v \neq w} \Gamma_v$ is $\prod_{v \neq w} \text{gcl}_{\Gamma_v}(g)$.

Since $\Gamma_v = G(K_v)$, for every $v \in S$, we get from (1), (2), and (3) that

$$
\prod_{v \neq w} \text{gcl}_{\Gamma_v}(g) \supseteq \prod_{v \in \mathcal{T}_\Gamma} W_v \times \prod_{v \notin \mathcal{T}_\Gamma \cup \{w\}} \langle \text{gcl}_{\Gamma_v}(g) \rangle.
$$

\[\qed\]

**Proof of Proposition 3.10.** The proof is almost identical to the proof of Proposition 3.8 except we apply Lemma 3.20 for the groups $\Gamma_v$, for $v \in T_\Gamma$, and get that there is $N_2$ (this time, depending on $\Gamma$) such that

$$(\forall v \in T_\Gamma) \quad \text{gcl}_{\Gamma_v}(g)^{N_2} = \langle \text{gcl}_{\Gamma_v}(g) \rangle. \quad (4)$$

Taking $N = \max \{N_1, N_2, 5D^2\}$, the result follows when we use (1) instead of (2).

**Proof of Proposition 3.11.** By the assumption that such $\Delta$ exists, we get that $\Gamma$ is a congruence subgroup. By replacing $\Gamma$ by a finite-index subgroup, we can assume that $\Gamma$ is a principal congruence subgroup. Let $N_1$ the constant from Proposition 3.11 applied with $\Gamma$ and $\epsilon = \frac{1}{2}$. For every $v \in T_\Gamma$, apply Lemma 3.20 to $\Gamma_v$ to get a number $N_{2,v}$, and let $N_2 = \max \{N_{2,v} \mid v \in T_\Gamma\}$. We will show that the claim holds with $N = 2N_1 + N_2$.

Let $\Delta$ be a principal congruence subgroup. For a place $v$, denote the closure of $\Delta$ in $\Gamma_v$ by $\Delta_v$.

By Strong Approximation, there is a non-central $\frac{1}{2}$-separated element $\alpha \in \Delta$. By the definition of $N_1$, $\text{gcl}_{\Gamma}(\alpha)^{N_1}$ is dense in $\prod_{v \notin S} \langle \text{gcl}_{\Gamma_v}(\alpha) \rangle$. For every $v \in T_\Gamma$, choose a natural number $k_v$ such that $\Gamma_v[p_v^{k_v}] \subseteq \langle \text{gcl}_{\Gamma_v}(\alpha) \rangle$. Let $T$ be the finite set of places $v \notin T_\Gamma \cup S$ such that $\alpha \in Z(\Gamma_v) \cdot \Gamma_v[p_v]$.

For $v \notin S \cup T \cup T_\Gamma$, $\text{gcl}_{\Gamma_v}(\alpha)^{N_1} = \langle \text{gcl}_{\Gamma_v}(\alpha) \rangle = \Gamma_v$. For every $v \in T$, there is a natural number $k_v$ such that $\Delta_v = \Gamma_v[p_v^{k_v}]$. By Strong Approximation, there is an element $\beta \in \Delta$ such that $\beta \in \Gamma_v[p_v^{k_v}]\setminus Z(\Gamma_v) \cdot \Gamma_v[p_v^{k_v+1}]$. We have that $\text{gcl}_{\Gamma_v}(\beta)^{N_1} = \langle \text{gcl}_{\Gamma_v}(\beta) \rangle = \Delta_v$. For every $v \in T_\Gamma$, there are elements $\gamma_{v,1}, \ldots, \gamma_{v,N} \in \Delta_v$ such that $\Delta_v = \text{gcl}_{\Gamma_v}(\gamma_{v,1}) \cdots \text{gcl}_{\Gamma_v}(\gamma_{v,N})$. By Strong Approximation, choose elements $\gamma_1, \ldots, \gamma_{N_2} \in \Gamma$ such that $\gamma_i \equiv \gamma_{v,i} \pmod {\Gamma_v[p_v^{k_v}]}$, for all $i = 1, \ldots, N_2$. For every $v \notin S$,

$$
\text{gcl}_{\Gamma_v}(\alpha)^{N_1} \cdot \text{gcl}_{\Gamma_v}(\beta)^{N_1} \cdot \text{gcl}_{\Gamma_v}(\gamma_1) \cdots \text{gcl}_{\Gamma_v}(\gamma_{N_2}) = \Delta_v
$$

and the claim holds.

\[\qed\]
4 Definability of congruence subgroups

Definition 4.1. Under Setting 1.1, for every \( q \vartriangleleft A \), let \( G(A; q) \) be the \( q \)th congruence subgroup of \( G(A) \) and let \( G^*(A; q) \) consists of the elements whose images in \( G(A)/G(A; q) \) are central. Then \( \{\alpha G(A; q) \mid q \not= 0\} \) is a basis to the congruence topology of \( G(A) \) and \( \{\alpha G^*(A; q) \mid q \not= 0\} \) is a basis to a topology of \( G(A) \) which we call the projective congruence topology. Finally, denote \( \Gamma[q] := \Gamma \cap G(A; q) \) and \( \Gamma^*[q] := \Gamma \cap G^*(A; q) \).

Theorem 4.2. Let \( \Gamma \) be as in Setting 1.1. If \( G = \text{Spin}_q \), assume further that \( n \geq 9 \). The exists a definable collection \( \mathcal{F} \) of normal congruence subgroups of \( \Gamma \) which contains \( \{\Gamma^*[q] \mid A \not= q \vartriangleleft A\} \).

Proof. Proposition 4.3 below implies that there exists a definable collection \( \mathcal{D} \) which is a basis of neighborhoods of identity under the projective congruence topology. Let \( N \) be the constant given by Proposition 3.11. Let \( \mathcal{F} \) be the collection of normal subgroups of \( \Gamma \) which are of the form \( \prod_{1 \leq i \leq N} \text{gcl}_{\Gamma}(\alpha_i)\Lambda \) for some \( \alpha_1, \ldots, \alpha_N \in \Gamma \) and some \( \Lambda \in \mathcal{D} \). \( \square \)

Proposition 4.3. Let \( \Gamma \) be as in Setting 1.1. If \( G = \text{Spin}_q \), assume further that \( n \geq 9 \). There exists a uniformly definable collection of subsets of \( \Gamma \) which is a base of neighborhoods of identity under the projective congruence topology.

Remark 4.4. By a base of neighborhoods of identity in Proposition 4.3 we mean a collection \( \mathcal{A} \) of (not necessarily open) sets, that satisfies the following conditions:

1. For every \( A \in \mathcal{A} \), the identity is in the interior of \( A \).

2. For every open set \( B \) containing the identity, there is an element \( A \in \mathcal{A} \) such that \( A \subseteq B \).

4.1 Proof of Proposition 4.3 for non-uniform \( \Gamma \)

Lemma 4.5. Let \( \Phi \) be a reduced and irreducible root system. Fix a lexicographic order on \( \Phi \) and let \( \Delta \) be the set of simple roots. For any \( \alpha \in \Delta \), \( \text{Span}_Q \left\{ r \in \Phi^+ \mid r = \sum_{\gamma \in \Delta} c_{\gamma} \gamma \text{ with } c_{\alpha} > 0 \right\} = \text{Span}_Q \Phi \).
Proof. By the assumptions, the Dynkin diagram of \( \Phi \) is connected. We claim that, for every \( \beta \in \Delta \), \( \beta \) is in the \( \mathbb{Q} \)-span of \( \left\{ r \in \Phi^+ \mid r = \sum_{\gamma \in \Delta} c_{\gamma} \gamma \text{ with } c_\alpha > 0 \right\} \).

We show this by induction on the distance between \( \alpha \) and \( \beta \) on the Dynkin diagram. The basis case \( \alpha = \beta \) is clear. Assume that \( \beta \neq \alpha \), and let \( \alpha = \alpha_0, \ldots, \alpha_n = \beta \) be a sequence of elements of \( \Delta \) such that \( \langle \alpha_i, \alpha_j \rangle \neq 0 \) iff \( i = j \pm 1 \). By induction, we have that \( \alpha_0, \ldots, \alpha_{n-1} \in \mathbb{Q} \left\{ r \in \Phi^+ \mid r = \sum_{\gamma \in \Delta} c_{\gamma} \gamma \text{ with } c_\alpha > 0 \right\} \).

Denoting the reflection in the root \( \alpha_i \) by \( s_{\alpha_i} \), the element \( r = s_{\alpha_n} \circ \cdots \circ s_{\alpha_1}(\alpha_0) \) is of the form \( \sum_{i=0}^n c_i \alpha_i \), with \( c_0, c_n > 0 \), and the claim is proved. \( \square \)

Lemma 4.6. Let \( G \) be a connected and simple algebraic group over \( \mathbb{C} \), let \( P \subseteq G \) be a maximal parabolic, and let \( P = L \cdot U \) be a Levi decomposition. Then, the kernel of the conjugation action map \( \rho : L \rightarrow \text{Aut}(U) \) is \( Z(G) \).

Proof. Let \( T \subseteq L \) be a maximal torus. Let \( \Phi \) be the root system corresponding to the action of \( T \) on the Lie algebra of \( G \), and, for \( \chi \in \Phi \), denote the root space by \( g^\chi \). There is a lexicographic order on \( \Phi \), with corresponding set \( \Phi^+ \) of positive roots and set \( \Delta \) of simple roots, and a simple root \( \alpha \in \Delta \) such that \( P \) is the parabolic attached to \( \{ \alpha \} \). In particular, it follows that the Lie algebra of \( U \) is

\[
\text{Lie } U = \bigoplus \left\{ g^\chi \mid \chi = \sum_{\gamma \in \Delta} c_{\gamma} \gamma \text{ with } c_\alpha > 0 \right\}.
\]

By Lemma 4.5, \( \ker \rho \cap T = \bigcap_{\beta \in \Delta} \ker \beta = Z(G) \). Since \( L \) is semisimple and \( \ker \rho \) is normal in \( L \), if \( \ker \rho \neq Z(G) \), then ker \( \rho \cap T \neq Z(G) \), a contradiction. \( \square \)

Lemma 4.7. Let \( G \) be a connected simple algebraic group defined over \( \mathbb{C} \), let \( P \subseteq G \) be a parabolic, and let \( U \) be the unipotent radical of \( P \). Then

1. \( \text{Cent}_G(U) \subset U \cdot Z(G) \).
2. \( \text{Cent}_G(U) = Z(U) \cdot Z(G) \).

Proof. 1. If \( Q \) is a parabolic containing \( P \) and \( V \) is the unipotent radical of \( Q \), then \( V \subseteq U \) and \( \text{Cent}_G(U) \subseteq \text{Cent}_G(V) \). Hence, it is enough to prove the claim assuming \( P \) is maximal. Let \( P = L \cdot U \) be a Levi decomposition of \( P \). Since \( \text{Cent}_G(U) \subseteq N_G(U) = P \), the claim now follows by Lemma 4.6.
2. This is an immediate consequence of the first claim. \hfill \Box

**Lemma 4.8.** In Setting 1.1, assume that $P \subseteq G$ is a maximal $K$-parabolic defined over $K$, and let $U \subseteq P$ be the unipotent radical of $P$. Then

1. $\text{Cent}_\Gamma(U \cap \Gamma) = (Z(U) \cdot Z(G)) \cap \Gamma$.
2. $(Z(U) \cdot Z(G)) \cap \Gamma$ is definable.

**Proof.** 1. Since $P$ is defined over $K$, so is $U$. It follows that $U \cap \Gamma$ is Zariski-dense in $U$. By Lemma 4.7

$$\text{Cent}_\Gamma(U \cap \Gamma) = \text{Cent}_G(U \cap \Gamma) \cap \Gamma = \text{Cent}_G(U) \cap \Gamma = (Z(U) \cdot Z(G)) \cap \Gamma.$$

2. There are finitely many elements in $U \cap \Gamma$ that generate a Zariski dense subgroup of $U$. The result now follows from the first claim. \hfill \Box

The following follows from [Rag, Claim 2.11]

**Lemma 4.9.** In Setting 1.1, assume that $P \subseteq G$ is a maximal $K$-parabolic, and let $P = L \cdot U$ be a Levi decomposition defined over $K$. Denote the connected component of the Zariski closure of $L \cap \Gamma$ by $Z$. Then $Z$ acts non-trivially on $Z(U)$.

**Remark 4.10.** The assumption that the $S$-rank of $G$ is at least two is used in a crucial way in Lemma 4.9. However, if $|S| > 1$, then the claim is easier. Indeed, in this case, if $T \subseteq L$ is a maximal $K$-split torus, then $T \cap \Gamma$ is commensurable with $T(A)$, so it is Zariski dense in $T$. It is known that $T$ acts non-trivially on $Z(U)$, so the claim follows.

**Lemma 4.11.** In Setting 1.1, assume that $P \subseteq G$ is a maximal $K$-parabolic, and denote the unipotent radical of $P$ by $U$. For every $v \notin S$ and every natural number $n$ there is a natural number $m$ such that, for any $g \in \Gamma \setminus G^*(A; p^n_v)$, the set $\text{gcl}_\Gamma(g)^{4\dim G}$ contains an element in $Z(U) \setminus G(A; p^n_v)$.

**Proof.** Choose a Levi decomposition $P = L \cdot U$ and a maximal $K$-split torus $T \subseteq L$. There is a lexicographic ordering of the roots of $T$ acting on the Lie algebra of $G$ and a simple root $\alpha$ of $T$ such that $P$ is the parabolic corresponding to $\alpha$. By [BT65, §5], there is an element $w \in N_G(T)(K)$ that
switches the positive and negative roots; the image of \( w \) in the Weyl group has order 2. This implies that \( P^{w^2} = P \) and, in particular, that \( P \cap P^w \) is \( w \)-invariant.

Let \( \alpha' = -w(\alpha) \) (so \( \alpha' \) is positive), let \( P' \) be the maximal parabolic corresponding to \( \alpha' \), and let \( U' \) be its unipotent radical. By Bruhat decomposition, the map \( \beta : U' \times P \to G \) given by \( \beta(u, p) = uwp \) is a \( K \)-isomorphism between \( U' \times P \) and a Zariski open set in \( G \).

Denote the connected component of the identity in the Zariski closure of \( P \cap P^w \cap \Gamma \) by \( M \). Let \( f : U' \times P \times M \to P \) be the function \( f(u, p, x) = p^{-1}w^{-1}x^{-1}wpuxu^{-1} \). By [Rag, Lemma 2.8], the subgroup generated by \( f(U' \times P \times M) \) contains \( \left( \Gamma \cap L^{-1} \right)^0 \). By Lemma 3.9 there is an element \( u_0 \in Z(U) \cap \Gamma \) such that \( [f(U' \times P \times M), u_0] \neq 1 \). Since \( U' \times P \times M \) is connected and \( [f(1, 1, 1), u_0] = 1 \), we get that \( f(U' \times P \times M) \to Z(U) \) given by \( h(u, p, x) = [f(u, p, x), u_0] \) is not constant.

Given \( v \) and \( n \), by Lemma 3.10 there is a constant \( a \) such that, for every \( g \in \Gamma \setminus G^*(A_v; p^o_v) \), the set \( gcl_\Gamma (g)^{dim G} \) is dense in \( G(A_v; p^o_v) \). Since \( h \) is non-constant but \( h(u, p, 1) = 1 \), for every \( u, p \), there is a point \( (u_1, p_1) \in \beta^{-1}(G(A_v; p^o_v)) \) such that the function \( x \in M \mapsto h(u_1, p_1, x) \) is non-constant. Since \( u_1 \in U(K) \), there is a natural number \( b \) such that \( [u_1, \Gamma \cap M(A_v; p^o_v)] \subseteq \Gamma \). It follows that there is a natural number \( c \) such that \( f(u_1, p_1, M(A_v; p^o_v)) \not\subseteq U(A_v; p^o_v) \). By continuity, there is a neighborhood \( V \subseteq \beta^{-1}(G(A_v; p^o_v)) \) of \( (u_1, p_1) \) such that, for every \( (u, p) \in V \), \( f(u, p, M(A_v; p^o_v)) \not\subseteq U(A_v; p^o_v) \) and \( [u_1, \Gamma \cap M(A_v; p^o_v)] \subseteq \Gamma \). We will show that the claim of the lemma holds with \( m = c \).

Indeed, suppose that \( g \in \Gamma \setminus G(A_v; p^o_v) \). Then, there is an element \( g_1 \in gcl_\Gamma (g)^{dim G} \cap \beta(V) \). Writing \( g_1 = uwp \), there is an element \( x \in \Gamma \cap M(A_v; p^o_v) \) such that \( h(u, p, x) \notin U(A_v; p^o_v) \). We have that

\[
wxuwpuxu^{-1}x^{-1} = xg_1x^{-1} \in gcl_\Gamma (g)^{dim G}
\]

and, since \([x, u] \in \Gamma \), we get that

\[
xpx^{-1}wpuxu^{-1}x^{-1} = [x, u]g_1[x, u]^{-1} \in gcl_\Gamma (g)^{dim G}.
\]

We get that

\[
xf(u, p, x)x^{-1} = xp^{-1}w^{-1}x^{-1}wpuxu^{-1}x^{-1} = (xg_1^{-1}x^{-1}) ([x, u]g_1[x, u]^{-1}) \in gcl_\Gamma (g)^{2dim G}.
\]

Therefore, \( f(u, p, x) \in gcl_\Gamma (g)^{2dim G} \), so \( h(u, p, x) \in gcl_\Gamma (g)^{4dim G} \). By construction, \( h(u, p, x) \notin U(A_v; p^o_v) \), and the claim is proved.
Corollary 4.12. Under Setting 1.1, assume that \( P \varsubsetneq G \) is a maximal \( K \)-parabolic, and denote the unipotent radical of \( P \) by \( U \). For every ideal \( I \triangleleft A \), there is an ideal \( J \triangleleft A \) such that, if \( \gamma \notin \Gamma[I] \), then \( \text{gcl}_\Gamma(\gamma)^{4\dim G} \) contains an element in \( Z(U)(A) \setminus Z(U)(A; J) \).

Lemma 4.13. There is an ideal \( J_0 \) such that \( \Gamma[J_0] \cap \text{Cent}_G(U) \subseteq Z(U) \).

Proof. It is known that there is an algebraic representation of \( G \) and a vector \( a \) such that \( U = \text{Stab}_G(a) \). It follows that there is a regular function \( f \) on \( G \) such that \( f(xu) = f(x) \) for every \( x \in G \) and \( u \in Z(U) \), and such that \( f(z) \neq f(1) \), for every \( z \in Z(G) \setminus \{1\} \). We can also assume that \( f \) is defined over \( A \). Let \( J_0 \) be an ideal such that \( f(z) \equiv f(1) \mod J_0 \), for any \( z \in Z(G) \setminus \{1\} \). If \( x \in \Gamma[J_0] \cap \text{Cent}_G(U) \), then \( x = zu \), where \( z \in Z(G) \) and \( u \in Z(U) \) and also \( f(z) = f(x) \equiv f(1) \mod J_0 \), so \( z = 1 \).

Proof of Proposition 4.3 for non-uniform \( \Gamma \). By assumption, there is a proper, maximal \( K \)-parabolic \( P \varsubsetneq G \). Let \( U \) be its unipotent radical. We need to show that there is a uniformly-definable collection \( X \subseteq (\Gamma \setminus Z(\Gamma)) \times \Gamma \) such that

1. For each \( \delta \in \Gamma \setminus Z(\Gamma) \), \( X_\delta \) is a symmetric, conjugation-invariant subset that contains some congruence subgroup.

2. For each ideal \( I \), there is a \( \delta \in \Gamma \) such that \( X_\delta \subseteq \Gamma[I] \).

By [ALM, Theorem 5.1], there is a constant \( N_1 \) such that, for any non-central element \( \gamma \in \Gamma \), there is an ideal \( I(\gamma) \) such that \( \text{gcl}_\Gamma(\gamma)^{N_1} \supseteq U(I(\gamma)) \). Let \( N = \max \{N_1, 4\dim G\} \) and let \( X \subseteq \Gamma \times \Gamma \) be the definable set consisting of all pairs \( (x, y) \) such that \( \text{gcl}_\Gamma(y)^N \cap \text{Cent}_G(U) \subseteq \text{gcl}_\Gamma(x)^N \). If \( \delta \in \Gamma \) is non-central, then, by Lemma 4.13, \( \Gamma[J_0I(\delta)] \subseteq X_\delta \), proving (1). On the other hand, given an ideal \( I \) of \( A \), let \( J \) be the ideal obtained by applying Corollary 4.12 to \( I \), and let \( \delta \in \Gamma[J] \setminus \{1\} \). By the definition of \( J \), if \( \gamma \notin \Gamma[I] \), then \( \text{gcl}_\Gamma(\gamma)^N \cap U \not\subseteq \Gamma[J] \), and, in particular, \( \gamma \notin X_\delta \). This proves (2).

4.2 Proof of Proposition 4.3 for \( G = \text{Spin} \)

Setting 4.14. Under Setting 1.1, assume that \( G = \text{Spin}_q \) and \( n \geq 9 \). Let \( c_1, c_2, c_3 \in A^n \) be non-isotropic orthogonal vectors such that \( q \left( (K_w c_0 + K_w c_1)\right)^\perp \geq \)

\[ \]
and $i_q(C_w) = 1$ where $C := Kc_0 + Kc_1 + Kc_2$. Let $\Lambda$ be the subgroup of $\Gamma$ consisting of the elements which act on $C$ as $\pm 1$.

**Lemma 4.15.** Under Setting 4.14, $\Lambda$ is definable.

**Proof.** Let $\Delta$ be the subgroup of $\Gamma$ consisting of the elements which act as the identity on $C^\perp$. Then $\Delta$ is a congruence subgroup of $\text{Spin}_{q|C}(K)$ so $\Delta$ is finitely generated and the action of $\Delta$ on $C$ is absolutely irreducible. Thus, $\text{Cent}_\Gamma(\Delta) = \Lambda$ is definable. $\square$

We will need the following lemma which follows from Theorem 1.11. The proof of will be given §8.2 below.

**Lemma 4.16.** Under Setting 4.14, for every $\epsilon > 0$, there exists $N = N(\Gamma, \epsilon)$ such that the following holds:

If $\alpha \in \Gamma$ is $\epsilon$-separated, then $\text{gcl}_\Gamma(\alpha)^N(c_0, c_1, c_2)$ contains an open neighborhood of of $\bar{c}$ in $\Gamma(c_0, c_1, c_2)$ with respect to the $S$-adelic topology.

**Corollary 4.17.** Under Setting 4.14, let $\alpha \in \Gamma$ be a non-identity element. If $\text{gcl}_\Gamma(\alpha)^M\Lambda = \text{gcl}_\Gamma(\alpha)^{M+1}\Lambda$, then $\text{gcl}_\Gamma(\alpha)^M\Lambda$ is a congruence subgroup of $\Gamma$.

**Proof.** The assumption implies that $\text{gcl}_\Gamma(\alpha)^M\Lambda = \langle \text{gcl}_\Gamma(\alpha) \rangle \Lambda$. Fix non-central $\beta \in \langle \text{gcl}_\Gamma(\alpha) \rangle$. Lemma 4.16 implies that there exists $N$ and $0 \neq q \triangleleft A$ such that

$\text{gcl}_\Gamma(\alpha)^M\Lambda = \langle \text{gcl}_\Gamma(\alpha) \rangle \Lambda \supseteq \text{gcl}_\Gamma(\beta)^N\Lambda \supseteq \Gamma[q].$ $\square$

**Corollary 4.18.** Under Setting 4.14, for every $\epsilon > 0$ there exists $N = N(\epsilon, \Gamma)$ such every for every $\epsilon$-separated $\alpha \in \Gamma$,

$\text{gcl}_\Gamma(\alpha)^N\Lambda = \text{gcl}_\Gamma(\alpha)^{N+1}\Lambda = \langle \text{gcl}_\Gamma(\alpha) \rangle \Lambda.$

**Proof.** Lemma 4.16 implies that there are $N_1$ and $q \neq 0$ such that $\text{gcl}_\Gamma(\alpha)^{N_1}\bar{c}$ contains the $q$-congruence neighborhood of of $\bar{c}$ in $\Gamma\bar{c}$. Let $N_2$ be the constant given by Proposition 3.10. For $N = N_1 + N_2$, we have $\text{gcl}_\Gamma(\alpha)^N\Lambda = \langle \text{gcl}_\Gamma(\alpha) \rangle \Lambda$. $\square$

**Proof of Proposition 4.3.** We use Setting 4.14. Let $N$ be the natural number obtained by applying Corollary 4.18 with $\epsilon = \frac{1}{2}$. Then for every $\gamma \in \Gamma$,
\[ \gamma \Lambda \gamma^{-1} \] is the subgroup of \( \Gamma \) which acts on \( \gamma C \) as \( \pm 1 \). Moreover, for every \( \alpha, \gamma \in \Gamma \) and every \( M \), \( \text{gcl}_{\Gamma}(\alpha)^M(\gamma \Lambda \gamma^{-1}) = \gamma(\text{gcl}_{\Gamma}(\alpha)^M \Lambda)\gamma^{-1} \).

Choose \( \gamma_1, \ldots, \gamma_{n+1} \in \text{Spin}_q(A) \) such that \( \gamma_1 c_1, \ldots, \gamma_{n+1} c_1 \) are in general position in \( K^{n+1} \) (this means that every \( n \) of them are linearly independent). Lemma 4.15 implies that \( Y := \{ \alpha \in \Gamma \mid \text{gcl}_{\Gamma}(\alpha)^N \Lambda = \text{gcl}_{\Gamma}(\alpha)^{N+1} \Lambda \} \) is a definable subset of \( \Gamma \). Let \( X \subseteq \Gamma \times \Gamma \) be the definable subset

\[ X := \{ (\alpha, \beta) \in \Gamma \times \Gamma \mid \alpha \in Y \text{ and } \beta \in \cap_{1 \leq i \leq n+1} \gamma_i (\text{gcl}_{\Gamma}(\alpha)^N \Lambda) \gamma_i^{-1} \}. \]

We will show that \( \{ X_\alpha \mid \alpha \in Y \} \) is a uniformly definable collection of subgroups of \( \Gamma \) which is a basis of neighborhoods of identity under the projective congruence topology.

Corollary 4.17 implies that, for every \( \alpha \in Y \), \( X_\alpha \) is a congruence subgroup.

Let \( 0 \neq q < A \). We want to show that there exists \( \alpha \in Y \) such that \( X_\alpha \subseteq \Gamma^*[q] \).

Let \( p \) be a prime ideal of odd residue characteristic such that the reductions of \( a_i \) modulo \( p \) are in general position in \( (A/p)^n \). Let \( m \geq 1 \) be such that \( mA^n \subseteq \text{Span}_A \{ \gamma_i c_1 \mid 1 \leq i \leq n \} \). Choose a \( \frac{1}{2} \)-separated \( \alpha \in \Gamma[mpq] \).

Corollary 4.18 implies that \( \alpha \in Y \). We will show that \( X_\alpha \subseteq \Gamma^*[q] \).

Let \( \beta \in X_\alpha \). For every \( 1 \leq i \leq n+1 \) there exists \( \epsilon_i \in \{ \pm 1 \} \) such that \( \beta \gamma_i c_1 = \epsilon_i \gamma_i c_1 (\text{mod } mpq) \). By the choice of \( p \), \( \epsilon_1 = \epsilon_2 = \cdots = \epsilon_{m+1} = \pm 1 \). Since \( mA^n \subseteq \text{Span}_A \{ \gamma_i c_1 \mid 1 \leq i \leq n \} \), \( \beta \in \Gamma^*[pq] \).

\section{Interpretation of \( \mathbb{Z} \)}

**Theorem 5.1.** Let \( \Gamma \) be as in Setting 1.1. Then, there is an element \( \alpha \in \Gamma \) of infinite order such that

1. \( \langle \alpha \rangle \) is definable.
2. The map \( (\alpha^r, \alpha^s) \mapsto \alpha^{rs} \) is definable.

In particular, \( \Gamma \) interprets \( \mathbb{Z} \).

The proof of Theorem 5.1 is based on the following two propositions:

**Proposition 5.2.** Under Setting 1.1, there are a definable subgroup \( \Lambda \) of \( \Gamma \), a regular quadratic form \( f \) on \( K^3 \) such that \( i_f(K^3) = 1 \) and a homomorphism \( \rho : \text{Spin}_f \rightarrow G \) which is an isogeny over its image such that \( \rho(\text{Spin}_q) \cap \Gamma \) has finite index in \( \Lambda \).
Proposition 5.3. Under Setting 1.1 denote $\mathcal{P} = \{ p^k \mid p < A \text{ is prime and } k \geq 1 \}$. Let $f$, $\rho$, and $\Lambda$ be as in Proposition 5.2. For every infinite order semisimple $\alpha \in \Lambda$, there exist $d, e \geq 1$ such that, for every cofinite $\mathcal{R} \subseteq \mathcal{P}$, the set
\[
\{ \gamma \in Z(\text{Cent}_\Lambda(\alpha)) \mid (\forall 1 \leq i \leq d \forall t \in \mathcal{R}) (\gamma \alpha^{-i})^e \not\in \Gamma^\ast[t]\}
\]
is finite.

5.1 Proof of Proposition 5.2 for non-uniform $\Gamma$

We will need the following straightforward extension of the notions of definable sets, imaginaries, and interpretations from a single structure to a sequence of structures.

Definition 5.4. Let $L$ be a first order language, let $(M_n)_{n \in \mathbb{N}}$ be a sequence of $L$-structures, and let $k \in \mathbb{N}$. We say that a sequence of subsets $A_n \subseteq M_n^k$ is definable if there is an $L$-formula $F(x_1, \ldots, x_k, y_1, \ldots, y_m)$ and, for each $n$, an $m$-tuple $(c_1^n, \ldots, c_m^n) \in M_n^m$ such that $A_n = \{(x_1, \ldots, x_k) \in M_n^k \mid F(x_1, \ldots, x_k, c_1^n, \ldots, c_m^n)\}$; for every $n$. In this case, we also say that the sequence $(A_n)$ is a definable sequence of sets in $(M_n)$. In a similar manner, define the notions of definable sequence of functions between definable sequences of sets in $(M_n)$, and the notion of a sequence of imaginary sets in $(M_n)$.

Definition 5.5. Let $L, L'$ be first order languages, let $(M_n)_{n \in \mathbb{N}}$ be a sequence of $L$-structures, and let $(M'_n)_{n \in \mathbb{N}}$ be a sequence of $L'$-structures.

1. An interpretation of $(M'_n)$ in $(M_n)$ is a pair $(F, f)$, where $F = (F_n)$ is a sequence of imaginaries in $(M_n)$ and $f = (f_n)$ is a sequence of bijections $f_n : F_n \to M'_n$ such that
   
   (a) For each $k$-ary relation symbol $r$ of $L_2$, the sequence of imaginaries $(f_n^{-1}(r^{M'_n}))$ is a definable sequence of subsets of $F_n^k$.

   (b) For every function symbol $g$ of $L_2$, say of arity $(r, s)$, the sequence of functions $(f_n^{-1} \circ g^{M_n} \circ f_n)$ is definable.

2. An interpretation $(F, (f_n))$ of $(M'_n)$ in $(M_n)$ is called trivial if the sequence of functions $(f_n)$ is definable.

3. A pair $(\mathcal{F}_{1,2}, \mathcal{F}_{2,1})$ consisting of an interpretation $\mathcal{F}_{1,2}$ of $(M_n)$ in $(M'_n)$ and an interpretation $\mathcal{F}_{2,1}$ of $(M'_n)$ in $(M_n)$ is called a bi-interpretation if the compositions $\mathcal{F}_{1,2} \circ \mathcal{F}_{2,1}$ and $\mathcal{F}_{2,1} \circ \mathcal{F}_{1,2}$ are trivial.
Proposition 5.6. Let $Q$ be the set of prime powers. The sequence $(\text{PSL}_2(\mathbb{F}_q))_{q \in Q}$ is in bi-interpretation with the sequence $(\mathbb{F}_q)_{q \in Q}$.

Proof. It is clearly enough to restrict the sequence to $q > 3$, which we will do in the rest of the proof. We first construct an interpretation $\mathcal{F}$ of $(\mathbb{F}_q)_{q \in Q}$ in $(\text{PSL}_2(\mathbb{F}_q))_{q \in Q}$. For every $q > 3$, let $u_q = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \text{PSL}_2(\mathbb{F}_q)$ and choose $t_q = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \in \text{PSL}_2(\mathbb{F}_q)$, for some $\epsilon \in \mathbb{F}_q \setminus \{0, 1, -1\}$. The sequences $U_q = \text{Cent}_{\text{PSL}_2(\mathbb{F}_q)}(u_q)$ and $T_q = \text{Cent}_{\text{PSL}_2(\mathbb{F}_q)}(t_q)$ are definable, as well as the sequence of functions $U_q \times U_q \to U_q$ taking $\left( \begin{pmatrix} 1 & x \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & y \\ 1 & 1 \end{pmatrix} \right)$ to $\begin{pmatrix} 1 & x + y \\ 1 & 1 \end{pmatrix}$. For every $q$ and every $a := \begin{pmatrix} 1 & x \\ 1 & 1 \end{pmatrix}, b := \begin{pmatrix} 1 & y \\ 1 & 1 \end{pmatrix} \in U_q \setminus \{1\}$, there are $s_1, s_2 \in T_q$ such that $(s_1^{-1}u_q s_1)(s_2^{-1}u_q s_2) = a$; for every such $s_1, s_2$, we have $(s_1^{-1}b s_1)(s_2^{-1}b s_2) = \begin{pmatrix} 1 & xy \\ 1 & 1 \end{pmatrix}$. This shows that the bijection $U_q \to \mathbb{F}_q$ given by $\begin{pmatrix} 1 & x \\ 1 & 1 \end{pmatrix} \mapsto x$ is an interpretation.

In the other direction, let $\mathcal{G}$ be the interpretation of $\text{PSL}_2(\mathbb{F}_q)$ in $\mathbb{F}_q$ whose imaginary is the set of 4-tuples $(x, y, z, w) \in \mathbb{F}_q$ satisfying the equation $xw - yz = 1$ (modulo $\pm 1$), and whose bijection is $(x, y, z, w) \mapsto \begin{pmatrix} x & y \\ z & w \end{pmatrix}$.

The inverse of composition $\mathcal{F} \circ \mathcal{G}$ is the function $x \mapsto (1, x, 0, 1)$ from $\mathbb{F}_q$ to $\mathbb{F}_q^4$, which is clearly definable.

Finally, the inverse of the composition $\mathcal{G} \circ \mathcal{F}$ is the sequence of functions $h_q : \text{PSL}_2(\mathbb{F}_q) \to \text{PSL}_2(\mathbb{F}_q)^4$ given by

$$h_q \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left( \begin{pmatrix} 1 & a \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & b \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & c \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & d \\ 1 & 1 \end{pmatrix} \right).$$

We need to show that $h_q$ is definable. Let $v_q = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \text{PSL}_2(\mathbb{F}_q)$, and let $V_q = \text{Cent}_{\text{PSL}_2(\mathbb{F}_q)}(v_q)$. The restriction of $h_q$ to $U_q$ is definable, as well as its restriction to $V_q$. Using the definability of addition and multiplication operations in $U_q$, we get that the restriction of $h_q$ to $U_q V_q U_q V_q$ is definable, but $U_q V_q U_q V_q = \text{PSL}_2(\mathbb{F}_q)$. \qed
Proposition 5.7. Let $Q$ be the set of prime powers. Let $G$ be a connected, simply connected and split simple group scheme over $\mathbb{Z}$. Then the sequence $(G(\mathbb{F}_q)/Z(G(\mathbb{F}_q)))_{q \in Q}$ is bi-interpretable with the sequence $(\mathbb{F}_q)_{q \in Q}$.

Proof. Let $r$ be the rank of $G$. It is enough to restrict the claim to the subsequence $q > r + 1$. Choose a maximal split torus $T$, and, for every $q > r + 1$, choose a regular element $t_q \in T(\mathbb{F}_q)$. The sequence $T(\mathbb{F}_q) = \text{Cent}_{G(\mathbb{F}_q)}(t_q)$ is definable. Let $\alpha$ be a root of $(G,T)$, let $U_{\alpha} \cong \mathbb{G}_a$ be the root subgroup, and choose $u_{q,\alpha} \in U_{\alpha}(\mathbb{F}_q)$. Since $\alpha$ is a non-trivial character, there is a constant $k$ such that $\alpha(T(\mathbb{F}_q))$ contains the collection of all $k$th powers in $\mathbb{F}_q^\times$. It follows that there is a constant $C$ (independent of $q$) such that $\alpha(T(\mathbb{F}_q)) + \cdots + \alpha(T(\mathbb{F}_q)) = \mathbb{F}_q$. It follows that every element in $U_{\alpha}(\mathbb{F}_q)$ is a product of $C$ conjugates of $u_{q,\alpha}$ by elements of $T(\mathbb{F}_q)$. This implies that the sequence $U_{\alpha}(\mathbb{F}_q)$ is definable. The proof now continues in the same way as in Proposition 5.6. \hfill \square

Definition 5.8. Let $d \in \mathbb{N}$, let $R$ be a domain whose characteristic is bigger than $d$, and let $u \in \text{GL}_d(R)$ be a unipotent element. Denote the fraction field of $R$ by $\text{Frac}(R)$. We define $u^R$ to be the set $\exp (R \log(u)) \subseteq \text{GL}_d(\text{Frac}(R))$. Note that $u^R$ is a group.

Corollary 5.9. Let $G$ be a simply connected Chevalley group scheme over $\mathbb{Z}$. There is an integer $d$ and a first order formula $F(x,y)$ in the language of groups such that, for every finite field $\mathbb{F}_q$ of characteristic larger than $d$, every unipotent element $u \in G(\mathbb{F}_q)/Z(G(\mathbb{F}_q))$, and every $g \in G(\mathbb{F}_q)/Z(\mathbb{F}_q)$, we have $G(\mathbb{F}_q)/Z(\mathbb{F}_q)$ satisfies $F(g,u)$ if and only if $g \in u^R$.

Proof. Using the bi-interpretation of $G(\mathbb{F}_q)/Z(\mathbb{F}_q)$ and $\mathbb{F}_q$, the sequence of Lie algebras $\mathfrak{g}(\mathbb{F}_q)$, as well as the exponential and logarithm maps, are definable. \hfill \square

The following is well known (the first claim follows from generic flatness and [SGA3, Expose XIX, Proposition 3.8]; the second claim follows from Strong Approximation and the construction of the finite simple groups of Lie type):

Lemma 5.10. Under Setting [LA]

\begin{enumerate}
\item For all but finitely many prime ideals $p \triangleleft A$, $G_{A/p}$ is a simple and connected algebraic group.
\end{enumerate}
2. For all but finitely many prime ideals $p \triangleleft A$, we have $\Gamma/\Gamma^*[p] = G(A/p)/Z(G(A/p))$ is a simple group of the Lie type of $G$.

In particular, the sets

\[
\{ \Delta \subseteq \Gamma \mid \Delta \text{ is a maximal normal congruence subgroup} \}
\]

and

\[
\{ \Gamma^*[p] \mid p \triangleleft A \text{ is a prime ideal} \}
\]

are commensurable.

Lemma 5.11. Let $n, C$ be natural numbers greater than 1. If $F$ is a field and $x, y \in \text{GL}_n(F)$ satisfy $x^{-1}yx = y^C$, then $y^{C^n!}$ is a unipotent.

Proof. Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of $y$. Since $\{ \lambda_i \} = \{ \lambda_i^C \}$, all $\lambda_i$ are roots of unity of order at most $C^n$, and the claim follows. \qed

Corollary 5.12. Under Setting 1.1, there is an infinite set $Q$ of primes of $A$ such that

1. For every $q \in Q$, $G_{A/q}$ is split.

2. The collection $\{ \Gamma^*[q] \mid q \in Q \}$ is uniformly definable.

Proof. By Theorem 4.2 there is a collection $\mathcal{F}_1$ of normal congruence subgroups of $\Gamma$ that contains all subgroups of the form $\Gamma^*[q]$. Taking the elements of $\mathcal{F}_1$ which are maximal, we get a uniformly definable collection $\mathcal{F}_2$ which, by Lemma 5.10, is commensurable with $\{ \Gamma^*[q] \mid q \triangleleft A \}$. By imposing a lower bound on the index of the subgroup, we get a uniformly definable collection $\mathcal{F}_3$ consisting of almost all subgroups of the form $\Gamma^*[q]$.

Let $n$ be such that there is an embedding $G \hookrightarrow \text{GL}_n$. Let $r$ be the rank of $G$ and let $\Phi \subseteq X^*(\mathbb{G}_m)$ be the absolute root system of $G$. Choose a basis $\beta_1, \ldots, \beta_r$ to $X_*(\mathbb{G}_m)$ such that $\alpha(\beta_i) \geq 0$, for all $\alpha \in \Phi^+$, and denote $C = \max \{ 2^{\alpha(\beta_i)} \mid \alpha \in \Phi, i = 1, \ldots, r \}$. By Chebotarev Density Theorem, there are infinitely many prime ideals $p \triangleleft A$ such that $p \not| C^n!$, $G_{A/p}$ is split, and $A/p$ contains a primitive $(r + 1)$ root of unity, which we denote by $\zeta_p$. In this case, let $\mathbb{G}_m \cong T \subseteq G_{A/p}$ be a split torus defined over $A/p$ and let $t \in T(A/p)$ be the element corresponding to $(1, \zeta_p, \ldots, \zeta_p^r)$. For each $\alpha \in \Phi^+$, choose a non-trivial element $u_\alpha$ in the root subgroup of $\alpha$ and, for each $i = 1, \ldots, r$, let $t_i = \beta_i(2) \in T(A/p)$. Then, the following hold:
(1) $t^{r+1} = 1$ and $\text{Cent}_{G(A/p)}(t)$ is abelian.

(2) $t_i^{-1}u_\alpha t_i = u_\alpha^{2^\alpha(i)}$.

(3) $u_\alpha^{C_n!} \neq 1$.

Now assume that $p < A$ is such that the characteristic of $A/p$ is greater than $\max \{ r+1, n, C_n!, D, 2^{\alpha(i)} | \alpha \in \Phi, i = 1, \ldots, r \}$ and there are elements $t, t_i, u_\alpha \in \Gamma/\Gamma^*[p]$, for $i = 1, \ldots, r$ and $\alpha \in \Phi^+$ satisfying the conditions (1), (2), and (3). By Condition (1), $t$ is regular and semisimple, so $S = \text{Cent}_{G(A/p)}(t)$ is a torus defined over $A/p$. By Conditions (2), (3), and Lemma 5.11, the elements $u_\alpha^{C_n!}$ are non-trivial unipotents. Every element of $S$ acts on the line $A/p \cdot \log(u_\alpha)$ by scalar multiplication, so we get a map $f : S \to \mathbb{G}_m$. Finally, Condition (2) implies that $f$ is an embedding. Hence, $S$ is split. Letting $\mathcal{F}_i$ be the collection of all subgroups $\Delta \in \mathcal{F}_3$ for which there are elements in $\Gamma/\Delta$ satisfying Conditions (1), (2), and (3), we get the claim of the Corollary.

**Proof of Proposition 5.2 for non-uniform $\Gamma$.** We will show that there is a homomorphism $\rho : \text{SL}_2 \to G$ which is an isogeny over its image and such that $\rho(\text{SL}_2) \cap \Gamma$ is definable. Since $\text{SL}_2$ is isomorphic to the spin group of the form $x^2 + y^2 - z^2$, this will prove the claim.

Choose $u \in \Gamma$ unipotent. We have that $u^A \cap \Gamma$ is a subgroup of finite index in $u^A$, so, after replacing $u$ by some integral power of itself, we can assume that $u^A \subset \Gamma$. Let $X = \log(u) \in \mathfrak{g}(K)$. By Jacobson–Morozov, there is $Y \in \mathfrak{g}(K)$ such that $(X, Y)$ is an $\mathfrak{sl}_2$-pair. There is a natural number $m$ such that $\exp(mAY) \subset \Gamma$. Let $v = \exp(mY)$. We have that $u^A, v^A \subset \Gamma$ and the Zariski closure of the subgroup generated by $u^A, v^A$, which we denote by $S$, is isogenous to $\text{SL}_2$.

It remains to show that $S \cap \Gamma$ is definable. For any prime $q$ of $A$, let $S_q$ be the image of $S(A/q)$ in $\Gamma/\Gamma^*[q]$, and let $u_q, v_q$ be the images of $u, v$ in $\Gamma/\Gamma^*[q]$. Let $\mathcal{Q}$ be the set of primes given by Corollary 5.12. For all but finitely many primes $q$, $S_q = u_q^{A/q} v_q^{A/q} u_q^{A/q} v_q^{A/q}$. Using this and Corollary 5.9, the sequence $(S_q)_{q \in \mathcal{Q}}$ is a definable sequence of subsets of $(\Gamma/\Gamma^*[q])_{q \in \mathcal{Q}}$. It follows that there is a first order formula $F$ such that $F(g)$ holds if and only if $g \Gamma^*[q] \subset S_q$, for every $q \in \mathcal{Q}$. If $g \in \Gamma \setminus S$, then, for almost all primes $p$, the reduction of $g$ modulo $p$ is not in $S_p$. Thus, $F(g)$ holds if and only if $g \in S \cap \Gamma$.

**Proof of Proposition 5.2 for $G = \text{Spin}$.** Choose a regular 3-dimensional subset $U$ of $K^n$ such that $i_q(U_w) \geq 1$. We view $\text{Spin}_{q(U_w)}(K)$ as a subgroup of 30
Spin\(_q(K)\). Denote \( f = q \upharpoonright_U \). There is an isomorphism \( \rho : \text{Spin}_f(K) \to \text{Spin}_{q|_U}(K) \). Let \( \Lambda \) be the subgroup of \( \Gamma \) consisting of the elements which act on \( U^\perp \) as \( \pm 1 \). Then \( \rho(\text{Spin}_f(K)) \cap \Gamma \) is of finite index in \( \Lambda \). The proof of Lemma 4.15 shows that \( \Lambda \) is definable.

### 5.2 Proof of Proposition 5.3

In the first few lemmas, we will use the following setting:

**Setting 5.13.**

1. \( A \) is the ring of \( S \)-integers in a number field \( K \) and \( \mathcal{P} = \{ p^k \mid p \triangleleft A \) is prime and \( k \geq 1 \} \).

2. \( f \) is a quadratic from on \( K^3 \), \( \alpha \in \text{SO}_f(A) \) is an infinite order semisimple element, \( \Delta \) is a subgroup of \( \text{Cent}_{\text{SO}_f(A)}(\alpha) \) and, for every ideal \( q \), \( \Delta[q] := \Delta \cap \text{SO}_f(A; q) \).

3. \( L \) is the splitting field of the characteristic polynomial of \( \alpha \), \( T \) is the set of places of \( L \) that lie above \( S \), and \( B \) is the ring of \( T \)-integers in \( L \).

4. \( \beta \mapsto \lambda_\beta \) is a non-trivial homomorphism from \( \Delta \) to \( B^\times \) such that, for every \( \beta \), \( \lambda_\beta \) is an eigenvalue of \( \beta \). It follows that for every \( \beta \in \Delta \) the eigenvalues of \( \beta \) are \( \{ \lambda_\beta, \lambda_\beta^{-1}, 1 \} \).

The following is Theorem 2.0 of [Nos]:

**Theorem 5.14** (Noskov). Let \( B \) be a finitely generated integral domain. There exists a number \( d \) such that, for every distinct elements \( c_1, \ldots, c_d \in B \) and every \( 0 \neq a \in B \), the set \( \{ b \in B \mid (\forall 1 \leq i \leq d) \ b - c_i|a \} \) is finite.

The following Lemma is clear.

**Lemma 5.15.** Under Setting 5.13, assume that \( K = L \). For every non-zero \( a \in A \) and \( \lambda \in A^\times \) such that \( \lambda - 1 \) does not divides \( a \), there exist a prime ideal \( p \triangleleft A \) and a natural number \( m \geq 1 \) such that \( a \notin Bp^m \) and \( \lambda - 1 \in Bp^m \).

**Lemma 5.16.** Under Setting 5.13, assume that \( K \neq L \). Let \( c \in A \) be a non-zero element that belongs to every prime ideal of \( A \) that is ramified in \( L \). For every non-zero \( a \in A \) and \( \lambda \in U \) such that \( \lambda - 1 \) does not divide \( ac \), there exist a prime ideal \( p \triangleleft A \) and a natural number \( m \geq 1 \) such that \( a \notin Bp^m \) and \( \lambda - 1 \in Bp^m \).
Proof. Since $\lambda - 1$ does not divide $ac$, there exist a prime ideal $q$ of $B$ and $m \geq 1$ such that $\lambda - 1 \in q^m$ and $ac \not\in q^m$. Denote $p := q \cap A$. We divide the proof into four cases:

1. Assume that $p$ is inert in $L$. Then $p^m = q^m \cap A$ and $Bp^m = q^m$ so $a \not\in Bp^m$ and $\lambda - 1 \in Bp^m$.

2. Assume that $p$ splits in $L$ and let $\sigma$ be the non-identity element of $\text{Gal}(L/K)$. Then $p^m = q^m \cap A$ and $Bp^m \cap A = q^m$ so $a \not\in Bp^m$. Since $\sigma(\lambda) = \lambda^{-1}$, $\lambda - 1 = \sigma(-\lambda^{-1}(\lambda - 1)) \in \sigma(q)^m$. It follows that $\lambda - 1 \in q^m \cap \sigma(q)^m = (q\sigma(q))^m = Bp^m$.

3. Assume that $p$ ramifies in $L$ and $m = 2l$. Then $p^l = q^m \cap A$ and $Bp^l = q^m$ so $a \not\in Bp^l$ and $\lambda - 1 \in Bp^l$.

4. Assume that $p$ ramifies in $L$ and $m = 2l + 1$. Then $\lambda - 1 \in Bp^l = q^{2l}$. Since $p^{l+1} = q^m \cap A$, $ac \not\in p^{l+1}$. Since $c \in p$ and $Bp^l \cap A = p^l$, $a \not\in Bp^l$.

\[\square\]

Lemma 5.17. Under Setting 5.13, let $p \triangleleft A$ be a prime ideal and define $n \geq 0$ to be minimal such that $\lambda_2^2 \not\equiv_{Bp^{n+1}} 1$. If $\beta \in \Delta$ and, for some $m \geq 2n + 1$, $\lambda_\beta \equiv_{Bp^m} 1$, then $\beta \in \Delta[p^{m-2n}]$.

Proof. Since all the eigenvalues of $\alpha$ belong to $B$, it follows from a variant of the structure theorem of finitely generated modules over principal ideal domains (see [Caš Lemma 3.2]) that there exists $\gamma \in \text{SL}_3(B_p)$ such that $\gamma \alpha \gamma^{-1}$ is an upper triangular matrix. Since $\Delta$ is abelian and all the eigenvalues of $\alpha$ are distinct, $\gamma \Delta \gamma^{-1}$ consists of upper triangular matrices. We can assume that $(\gamma \alpha \gamma^{-1})_{1,1} = \lambda_\alpha,$ $(\gamma \alpha \gamma^{-1})_{2,2} = \lambda_\alpha^{-1}$ and $(\gamma \alpha \gamma^{-1})_{3,3} = 1$.

Let $\beta \in \Delta$ and $m \geq 2n + 1$ be such that $\lambda_\beta \equiv_{Bp^m} 1$. For every $1 \leq i < j \leq 3$, let $b_{i,j}$ be the $(i,j)$-entry of $\gamma \beta \gamma^{-1}$. Since $\alpha$ and $\beta$ commute, $b_{1,2} \equiv_{Bp^m} \lambda_\alpha b_{1,2}$ and $b_{2,3} \equiv_{Bp^m} \lambda_\alpha^{-1} b_{2,3}$. Since $\lambda_\alpha^2 \not\equiv_{Bp^{n+1}} 1$, $b_{1,2}$ and $b_{2,3}$ belong to $Bp^{m-n}$. By the same argument, $b_{1,3} \equiv_{Bp^{m-n}} \lambda_\alpha b_{1,3}$. Since $\lambda_\alpha^2 \not\equiv_{Bp^{n+1}} 1$, $b_{1,3}$ belongs to $Bp^{m-2n}$. Thus, $\gamma \beta \gamma^{-1} \in \text{SL}_3(B; Bp^{m-2n})$ and $\beta \in \Delta[p^{m-2n}]$. \[\square\]

Lemma 5.18. Under Setting 5.13, let $d$ be as in Theorem 5.14. Let $Q$ be a cofinite subset of $\mathcal{P}$. Then

\[Q := \{\beta \in \Delta \mid (\forall q \in Q \forall 1 \leq i \leq d) \beta \alpha^{-i} \not\in \Delta[q]\}\]
is finite.

Proof. For every prime $p \triangleleft A$, let $m_p \geq 0$ be minimal such that $p^{m_p+k} \in Q$, for every $k \geq 1$. For every prime $p \triangleleft A$, let $n_p \geq 0$ be minimal such that $\lambda^2_\beta \not\equiv_{Bp^{n_p+1}} 1$. There exists a finite set $\mathcal{P}$ of prime ideals of $A$ such that for every $p \notin \mathcal{P}$, $m_p = n_p = 0$. Choose a non-zero element $a \in \prod_{p \in \mathcal{P}} p^{m_p+2n_p}$.

We claim that if $\beta \in \Delta$ and there are a prime ideal $p$, an integer $k \geq 1$, and an integer $1 \leq i \leq d$ such that $a \notin p^k$ and $\lambda^i_{\beta \alpha - i} \equiv_{Bp^k} 1$, then $\beta \not\in Q$. Indeed, since $a \in \prod_{p \in \mathcal{P}} p^{m_p+k}, k \geq m_p+2n_p+1$. Lemma 5.17 implies that $\beta^i_{\alpha - i} \in \Delta[p^{k-2n_p}]$. Since $p^{k-2n_p} \in Q$, $\beta \not\in Q$.

If $K = L$, define $c = 1$ and, if $K \neq L$, let $c$ be as in Lemma 5.16. We will show that $$Q \subseteq \{\beta \in \Delta \mid \forall 1 \leq i \leq d, \lambda^i_{\beta} - \lambda^i_{\alpha^{i+1}}ac\},$$ so Theorem 5.14 implies that $Q$ is finite. Indeed, let $\beta \in \Delta$ and $1 \leq i \leq d$ be such that $\lambda^i_{\beta} - \lambda^i_{\alpha^{i+1}} = \lambda^i_{\alpha^{i+1}}(\lambda^{i+1}_{\beta \alpha - i} - 1)$ does not divide $ac$. Lemmas 5.15 and 5.16 imply that there exist a prime ideal $p \triangleleft A$ and $k \geq 1$ such that $\lambda^i_{\beta \alpha - i} \equiv_{Bp^k} 1$ and $a \notin p^k$. The second paragraph implies that $\beta \not\in Q$. \hfill \Box

Lemma 5.19. Let $K$ be a number field, $S$ a finite set of places containing all archimedean ones, $A$ the ring of $S$-integers in $K$ and $\mathcal{P} = \{p^k \mid p \triangleleft A$ is prime and $k \geq 1\}$. Let $G_1, G_2 \subseteq (\text{SL}_n)_A$ be group schemes such that $(G_1)_K$ and $(G_2)_K$ are semisimple, and let $\rho : (G_1)_K \to (G_2)_K$ be an isogeny (of algebraic groups over $K$). Then:

1. $\rho^{-1}(G_2(A))$ is commensurable with $G_1(A)$.

2. For almost all prime ideals $p \triangleleft A$ and for every $k \geq 1$, $G_2(A_p; p^k) \subseteq \rho(G_1(A_p; p^k))$.

3. For every prime ideal $p \triangleleft A$ there exists $m_p \geq 0$ such that for every $k \geq 1$, $G_2(A_p; p^{m_p+k}) \subseteq \rho(G_1(A_p; p^k))$.

Proof. 1. Let $\tau : (\text{Mat}_n)_A \to (\text{Mat}_n)_A$ be the map $\tau(X) = X + I$. The map $\tau^{-1} \circ \rho \circ \tau : \tau^{-1}(G_1) \to \tau^{-1}(G_2)$ is given by polynomials with coefficients in $K$. Since $\tau^{-1} \circ \rho \circ \tau(0) = 0$, all these polynomials vanish at 0. Let $N \in A$ be the product of all denominators of all coefficients of all polynomials in $\tau^{-1} \circ \rho \circ \tau$. For any ideal $q \triangleleft A$, we have $\tau^{-1} \circ \rho \circ \tau(NqA^{n^2}) \subseteq qA^{n^2}$, which implies that $\rho(G_1(A; Nq)) \subseteq G_2(A; q)$. In particular, taking $q = A$, we get that $\rho(G_1(A; N)) \subseteq G_2(A)$. Since
$\rho^{-1}(G_2(A))$ is discrete and contains a lattice, it is a lattice. Hence, $[\rho^{-1}(G_2(A)) : G_1(A; N)] < \infty$. Since $[G_1(A) : G_1(A; N)] < \infty$, they are commensurable.

2. Let $\mathfrak{g}_1$ (respectively, $\mathfrak{g}_2$) be the Lie ring of $G_1$ (respectively, $G_2$). We show that the claim holds for all prime ideals $p < A$ for which both $G_1$ and $G_2$ have good reductions modulo $p$ and the map $d\rho|_1 : \mathfrak{g}_1(A_p) \rightarrow \mathfrak{g}_2(A_p)$ is an isomorphism. Let $k \geq 1$ and let $q \in G_1(A_p)$ be such that $\rho(q) \in G_2(A_p;p^k)$. Since, by assumption, $d\rho|_q$ is an isomorphism, Hensel’s lemma implies that there is $h \in G_1(A_p;p^k)$ such that $\rho(gh) = 1$, so $gh \in \ker \rho$ and the claim follows.

3. There is a natural number $a$ such that the power series $\log(x)$ and $\exp(x)$ converge on $G_1(A_p;p^a)$ and $\mathfrak{g}_1(K_p) \cap \mathfrak{p}^\mathfrak{n} \mathfrak{l}_n(A_p)$ and define inverse bijections between the two sets. Fix $\varpi \in \mathfrak{p}A_p \setminus \mathfrak{p}^2A_p$ and, for each natural number $t$, let $\delta_t : G_1(A_p;p^a) \rightarrow G_1(A_p;p^a)$ be the dilation map $\delta_t(g) = \exp(\varpi^t \log(g))$. For any $k \geq a$, we have that $\delta_t(G_1(A_p;p^k)) = G_1(A_p;p^{k+t})$. There is a natural number $b$ such that $\varphi := \rho \circ \delta_b$ is equal to a convergent power series with coefficients in $A_p$. Let $c$ be the constant obtained by applying Lemma 3.13 with $R = A_p$, $X = G_1(A_p;p^a)$, and $Y = G_2(A_p)$. Finally, since $d\varphi|_1 = \varpi^b d\rho|_1$, there is a natural number $d$ such that $d\varphi|_1(\mathfrak{g}_1(K_p) \cap \mathfrak{s}l_n(A_p)) \supseteq \mathfrak{p}^d (\mathfrak{g}_2(K_p) \cap \mathfrak{s}l_n(A_p))$. By Lemma 3.13 for every $k \geq a + b$,

$$
\rho(G_1(A_p;p^k)) = \varphi(G_1(A_p;p^{k-b})) \supseteq G_2(A_p;p^{d+k-b+c}),
$$

and the result follows.

\[ \square \]

**Proof of Proposition 5.3.** Denote $H := \rho(\text{Spin}_f)$. Since $H \subseteq G$, we have $\rho(\text{Spin}_f) \cap G(A) = H(A)$. The only finite and non-trivial normal subgroup of $\text{Spin}_f$ is the center $Z(\text{Spin}_f)$ and this center has order two. We get that $\rho : \text{Spin}_f \rightarrow H$ is either isomorphism or $\ker \rho = Z(\text{Spin}_f)$. In any case, we have an isogeny $\psi : H \rightarrow SO_f$ of algebraic groups over $K$ and $\ker \psi$ is either trivial or central of order 2. Lemma 5.19 implies that there exists a finite index normal subgroup $\Lambda^* \leq \Lambda$ such that $\Lambda^* \leq \Lambda \cap H(A)$ and $\psi(\Lambda^*)$ is contained in $SO_f(A)$. By Lemma 5.19 for every prime ideal $p < A$, there exists $m_p \geq 0$ such that for every $k \geq 1$, $\psi(H(A_p;p^k))$ contains $SO_f(A_p;p^{k+m_p})$. We can further assume that $m_p = 0$ for all but finitely many prime ideals.
Let $\beta \in \Lambda^*$. We claim that, for every prime ideal $p$ and every $k \geq 1$, if $\beta^2 \notin \Gamma^*[p^k]$, then $\psi(\beta) \notin SO_f(A; p^{k+mp})$. Assume otherwise. Lemma 5.19 implies that $\beta \in H(A) \cap ((\ker \rho) \cdot H(A_p, p^k))$ so $\beta^2 \in H(A) \cap H(A_p, p^k) = H(A; p^k) \subseteq \Gamma^*[p^k]$, a contradiction.

Let $\alpha \in \Lambda^*$ be an infinite order semisimple element. Then $\text{Cent}_{\Lambda^*}(\alpha)$ is an abelian subgroup whose torsion subgroup is finite. Let $d$ be the constant given in 5.18 with respect to $\psi(\alpha)$ and $\Delta := \psi(\text{Cent}_{\Lambda^*}(\alpha))$. Let $\mathcal{R} \subseteq \mathcal{P}$ be a cofinite subset and denote $\mathcal{Q} := \{p^{k+mp} | p \text{ prime and } p^k \in \mathcal{R}\}$. Note that $\mathcal{Q}$ is cofinite in $\mathcal{P}$. We claim that

$$D := \{\gamma \in \text{Cent}_{\Lambda^*}(\alpha) | (\forall 1 \leq i \leq d \forall r \in \mathcal{R}) (\gamma \alpha^{-i})^2 \notin \Gamma^*[r]\}$$

is finite. Let $\gamma \in D$. The previous paragraph implies that for every $q \in \mathcal{Q}$ and every $1 \leq i \leq d$, $\psi(\gamma \alpha^{-i}) \notin SO_f(A; q)$. Since $\mathcal{Q}$ is cofinite in $\mathcal{P}$ and $\ker \psi$ is finite, Lemma 5.18 implies that $D$ is finite.

Denote $e = [\Lambda : \Lambda^*]$. Let $\alpha \in \Lambda$ be an infinite order semisimple element. Then $\alpha^e \in \Lambda^*$ is an infinite order semisimple element. Let $d$ be the constant given in Lemma 5.18 with respect to $\psi(\alpha^e)$. In order to finish the proof it suffices to show that the set

$$E := \{\gamma \in Z(\text{Cent}_{\Lambda}(\alpha)) | (\forall 1 \leq i \leq d \forall r \in \mathcal{R}) (\gamma \alpha^{-i})^{2e} \notin \Gamma^*[r]\}$$

is finite. If $\gamma \in Z(\text{Cent}_{\Lambda}(\alpha))$ then $\gamma^e \in \text{Cent}_{\Lambda^*}(\alpha^e)$ so the previous paragraph implies that $\{\gamma^e | \gamma \in E\}$ is finite. Since $Z(\text{Cent}_{\Lambda}(\alpha))$ is an abelian group whose torsion subgroup is finite, then map $x \mapsto x^e$ has finite fibers so $E$ is finite.

### 5.3 Proof of Theorem 5.1

**Proof of Theorem 5.1.** Let $f$ and $\rho$ and $\Lambda$ be as in Proposition 5.2. Fix an infinite order semisimple $\alpha \in \Lambda$ and denote $\Theta := Z(\text{Cent}_{\Lambda}(\alpha))$. Robinson [Rob1] proved that $(\mathbb{Z}, +, \times)$ is definable in $(\mathbb{Z}, +, |)$ where $|$ is the divisibility relation. For every non-zero $r, s \in \mathbb{Z}$, $r | s$ if and only if $\alpha^s \in \langle \alpha^r \rangle$. Thus, in order to prove Theorem 5.1 it is enough to show that there exists a definable subset $C \subseteq \Theta \times \Theta$ such that for every $\beta \in \Theta$ of infinite order, $C_\beta = \langle \beta \rangle$.

Theorem 4.2 implies that there exists a uniform definable collection $\mathcal{F}$ of normal congruence subgroups in $\Gamma$ which contains $\{\Gamma^*[q] | q < A\}$. Let $d, e \geq 1$ be as in Proposition 5.3. Denote $\Psi := \{\beta \in \Theta | \exists (1 \leq i \leq d) (\beta \alpha^{-i})^e = 1\}$. 

35
Since the torsion subgroup of $\Theta$ is finite, $\Psi$ is a finite. Let $D \subseteq \Gamma \times \Theta$ be the definable subset

$$D := \{ (\gamma, \beta) \in \Gamma \times \Theta \mid (\forall \Delta \in F \forall 1 \leq i \leq d) \gamma \notin \Delta \rightarrow ((\beta \in \Psi) \lor (\beta \alpha^{-i})^e \notin \Delta) \}.$$ 

Then for every non-identity $\gamma \in \Gamma$, $D_\gamma$ is finite.

**Claim 5.20.** Let $\Phi \subseteq \Theta$ be finite. There exists a non-identity $\gamma \in \Gamma$ such that $\Phi \subseteq D_\gamma$.

**Proof.** There exists a finite set $C \subseteq F$ such there for every $\Delta \in F \setminus C$, $\Delta \cap \{(\phi \alpha^{-i})^e \mid \phi \in \Phi$ and $1 \leq i \leq d\} = 1$. For every non-trivial $\gamma \in \cap \Delta \in C \Delta$, $\Phi \subseteq D_\gamma$. \(\square\)

Let $E \subseteq \Gamma^3 \times \Theta$ be the definable subset

$$\{((\gamma, \delta_1, \delta_2), \beta) \in \Gamma^3 \times \Theta \mid (\beta \in D_\gamma) \land ((\forall \Delta \in F) \delta_2 \notin \Delta \rightarrow \beta \notin \delta_1 \Delta)\}.$$ 

**Claim 5.21.** Let $\Phi \subseteq \Theta$ be finite. There exist non-identity $\gamma, \delta_1, \delta_2 \in \Gamma$ such that $\Phi = E_{(\gamma, \delta_1, \delta_2)}$.

**Proof.** Choose non-identity $\gamma \in \Gamma$ such that $\Phi \subseteq D_\gamma$. Assume that $D_\gamma = \{\beta_i \mid 1 \leq i \leq r + s\}$ and $\Phi = \{\beta_i \mid 1 \leq i \leq r\}$. Choose distinct prime ideals $p_1, \ldots, p_s$ such that for every $1 \leq j \leq s$, $\Gamma/\Gamma^*[p_j]$ is non-abelian and simple and the map $\beta_i \mapsto \beta_i \Gamma^*[p_j]$ is injective on $D_\gamma$.

By the strong approximation theorem, $\Gamma$ projects onto $\prod_{1 \leq j \leq s} \Gamma/\Gamma^*[p_j]$. Hence, there exists $\delta_1 \in \Gamma$ such that for every $1 \leq j \leq s$, $\beta_{r+j} \Gamma^*[p_j] = \delta_1 \Gamma^*[p_j]$. Let $C \subseteq F$ consists of the $\Delta \in F$ for which there exits $1 \leq i \leq r$ such that $\delta_1 \Delta = \beta_i \Delta$. Then $C$ is finite and every $\Delta \in C$ is not contained in any of the subgroups $\Gamma^*[p_1], \ldots, \Gamma^*[p_s]$. Since for every $1 \leq j \leq s$, $\Gamma/\Gamma^*[p_j]$ is simple and every $\Delta \in C$ is normal in $\Gamma$, $\cap_{\Delta \in C} \Delta$ projects onto $\prod_{1 \leq j \leq s} \Gamma/\Gamma^*[p_j]$. Thus, there exists $\delta_2 \in \cap_{\Delta \in C} \Delta$ such that for every $1 \leq j \leq s$, $\delta_2 \notin \Gamma^*[p_j]$.

It follows that $\Phi = E_{(\gamma, \delta_1, \delta_2)}$. \(\square\)

Claim 5.21 implies that the collection $E$ of finite subsets of $\Gamma$ is uniformly definable. Let $C$ be the subset of $\Theta \times \Theta$ such that for every $\beta, \gamma \in \Theta$, $(\beta, \gamma) \in C$ if and only if there exists $\Phi \in E$ for which the following two conditions hold:

a) $\beta \in \Phi$.
If \( \delta \in \Phi \) then either \( \delta = \gamma \pm 1 \) or \( \beta \delta \in \Phi \).

We claim that \( C \) is the desired definable subset. Let \( \beta \in \Theta \) be of infinite order. For every \( r \in \mathbb{N} \), the set \( \Phi := \{ \beta^i \mid 0 \leq |i| \leq |r| \} \) satisfies items [a] and [b] so \( (\beta, \beta^r) \in C \). On the other hand, if \( \gamma \notin \langle \beta \rangle \) then every set which satisfies items [a] and [b] contains all positive powers of \( \beta \) and thus is not finite. The proof of Theorem 5.1 is now complete. \( \square \)

6 Bi-interpretation

The goal of this section is to prove Theorem 1.2. The following Lemma follows from Corollary 2.8 of [AKNS]:

Lemma 6.1. Every self interpretation of \( \mathbb{Z} \) is trivial.

Robinson [Rob2] proved that \( \mathbb{Z} \) is a definable subset in the ring of integers of any number field. Using the fact that every such ring is a free \( \mathbb{Z} \)-module, the following lemma can be easily proved for rings of integers. A similar argument works for rings of \( S \)-integers. Alternatively, it follows from the main Theorem of [AKNS] that every finitely generated infinite integral domain is bi-interpretable with \( \mathbb{Z} \).

Lemma 6.2. Every ring of \( S \)-integers of a number field is in bi-interpretation with \( \mathbb{Z} \).

The following is a well known theorem of Gödel:

Theorem 6.3. Every recursive function \( \mathbb{N} \rightarrow \mathbb{Z}^m \) and every recursively enumerable subset \( B \subseteq \mathbb{Z}^m \) are definable in \( \mathbb{Z} \).

Lemma 6.4. Let \( A, G \) and \( \Gamma \) be as in Setting 1.1. If \( G = \text{Spin}_q \), assume further that \( n \geq 9 \). There exist an interpretation \( \mathcal{R} = (R, r) \) of \( \mathbb{Z} \) in \( \Gamma \), an interpretation \( \mathcal{E} = (E, e) \) of \( \Gamma \) in \( \mathbb{Z} \) and an infinite order element \( \alpha \in \Gamma \) such that for \( \mathcal{H} = (H, h) := \mathcal{E} \circ \mathcal{R} \) the restriction of \( h^{-1} \) to \( \langle \alpha \rangle \) is definable.

Proof. Theorem 5.1 implies that there is an infinite order element element \( \alpha \in \Gamma \) and an interpretation \( \mathcal{R} = (R, r) \) of \( \mathbb{Z} \) in \( \Gamma \) such that \( R = \langle \alpha \rangle \) and \( r(\alpha^m) = m \).

Lemma 6.2 gives an interpretation \( \mathcal{B} = (B, b) \) of \( A \) in \( \mathbb{Z} \). Let \( \mathcal{C} := (C, c) \) be the standard interpretation of \( G(A) \) in \( A \). Then \( \mathcal{D} = (D, d) := \mathcal{C} \circ \mathcal{B} \) is
an interpretation of $G(A)$ in $\mathbb{Z}$. Since $\Gamma$ is finitely generated, $E := d^{-1}(\Gamma)$ is recursively enumerable subset of $D$. Denote $e := d \upharpoonright E$. Theorem 6.3 implies that:

a) $E$ is definable so $\mathcal{E} = (E, e)$ is an interpretation of $\Gamma$ in $\mathbb{Z}$.

b) The map $p : \mathbb{Z} \to E$ given by $p(m) = e^{-1}(\alpha^m)$ is definable in $\mathbb{Z}$.

Item b) implies that the map $R^*p : R \to R^*E$ is definable in $\Gamma$. Denote $H := (H, h) := \mathcal{E} \circ \mathcal{R}$. Then $H = R^*E$ and the restriction of $h^{-1}$ to $\alpha$ is $R^*p$.

The following is Theorem 2 of [PS]. It can also be deduced from Theorem 2.3 of [BGT] under the assumption that $X$ is symmetric.

**Theorem 6.5** ([PS]). Let $G$ be a finite simple group of Lie type of rank $r$ and $X$ a generating set of $L$. Then either $X^3 = G$ or $|X^3| > |A|^{1+\epsilon}$ where $\epsilon$ depends only on $r$.

**Lemma 6.6.** Let $\Gamma$ be as in Setting 1.1 and let $\alpha \in \Gamma$ be of infinite order. There exist infinitely many prime ideals $p \triangleleft A$ such that the order of $\alpha$ in $\Gamma/\Gamma[p]$ is at least $|A/p|^\frac{1}{3[K:\mathbb{Q}]}$.

**Proof.** Assume first that $\alpha$ is virtually-unipotent. Then there exists $m > 0$ such that $\alpha^m$ is unipotent. If $\alpha^m \notin \tilde{\Gamma}[p]$ then the order of the image of $\alpha^m$ in $\Gamma/\Gamma[p]$ is at least $p = \text{char}(A/p)$. The claim follows since $p^{[K:\mathbb{Q}]} \geq |A/p|$.

For every rational prime $p$ there exists a prime ideal of $p \triangleleft A$ for which $\text{char}(A/p) = p$. Moreover, if $p \triangleleft A$ and $\text{char}(A/p) = p$ then $|A/p| \leq p^{[K:\mathbb{Q}]}$. It follows from the prime number theorem that for a large enough $m$, the number of prime ideals $p \triangleleft A$ for which $|A/p| \leq m^{3[K:\mathbb{Q}]}$ is at least $\frac{m^3}{6 \log m}$. Therefore, in order to prove the lemma it is enough to show that if $\alpha$ is not virtually-unipotent, then the number of prime ideals $p \triangleleft A$ for which the image of $\alpha$ in $\Gamma/\Gamma[p]$ has order at most $m$, is bounded by a quadratic function of $m$. In order to show this it is enough to show that the number of prime ideals $p \triangleleft A$ for which the image of $\alpha$ in $\Gamma/\Gamma[p]$ has order exactly $m$, is bounded by a linear function of $m$.

Assume that $\alpha$ is not virtually-unipotent. Then $\alpha$ has an eigenvalue $\lambda$ which is not a root of unity. Let $E$ be a finite extension of $K$ which contains $\lambda$ and let $B$ be the ring of integers of $E$. Then $B$ contains $\lambda$. If $p \triangleleft A$ is a prime ideal and the order of the image of $\alpha$ in $\Gamma/\Gamma[p]$ is $m$, then $\lambda^m - 1 \in pB$. 38
If follows that $|B/pB| \text{ divides } |B/((\lambda^m - 1)B)| = N_{E/Q}(\lambda^m - 1)$. In particular, $\text{char}(A/p) \text{ divides } N_{E/Q}(\lambda^m - 1)$. The number of distinct prime divisors of $N_{E/Q}(\lambda^m - 1)$ is at most $\log_2(N_{E/Q}(\lambda^m - 1))$ so it is bounded by a linear function in $m$. The result follows since for every prime $p$, there exists at most $|K : \mathbb{Q}|$ prime ideals $p \triangleleft A$ such that $\text{char}(A/p) = p$.

**Corollary 6.7.** Let $\Gamma$ be as in Setting [1.1] and let $\alpha \in \Gamma$ be of infinite order. There are $\beta_1, \ldots, \beta_d \in \Gamma$ such that the set $\prod_{1 \leq i \leq d} \langle \beta_i \alpha \beta_i^{-1} \rangle$ projects onto $\Gamma/\Gamma[p]$, for infinitely many prime ideals $p \triangleleft A$.

**Proof.** By Margulis’s Normal Subgroup Theorem, $[\Gamma : \langle \text{gcl}_\Gamma(\alpha) \rangle] < \infty$, so $\langle \text{gcl}_\Gamma(\alpha) \rangle$ is generated by finitely many conjugates of $\alpha$. By the strong approximation theorem, for all but finitely many prime ideals $p$, the normal subgroup generated by $\alpha$ projects onto $\Gamma/\Gamma[p]$. The result follows from Theorem 6.5, Lemma 5.10 and Lemma 6.6.

**Lemma 6.8.** Let $G$ be a group and let $L, M$ be normal subgroups of $G$. Let $\Phi \subseteq G$ be a symmetric generating subset which contains the identity and projects onto $G/L$ and $G/M$. If the quotients maps $\Phi^2 \to G/L$ and $\Phi^2 \to G/M$ have the same fibers then $L = M$.

**Proof.** Assume that the fibers are the same. Define a map $\rho : G/L \to G/M$ by setting $\rho(\phi L) := \phi M$, for every $\phi \in \Phi$. Every $g \in G$ is a product of elements in $\Phi \cup \Phi^{-1}$ and induction on the length of this product shows that $\rho(gL) = gM$. It follows that $\rho$ is an isomorphism. In particular, $g \in L$ if and only if $gL \in \ker \rho$ if and only if $g \in M$.

**Proof of Theorem 1.2.** Lemma 6.4 implies that there exist an interpretation $\mathcal{R} = (R, r)$ of $\mathbb{Z}$ in $\Gamma$, an interpretation $\mathcal{E} = (E, e)$ of $\Gamma$ in $\mathbb{Z}$ and an infinite order element $\alpha \in \Gamma$ such that for $\mathcal{H} = (H, h) := \mathcal{E} \circ \mathcal{R}$ the restriction of $h^{-1}$ to $\langle \alpha \rangle$ is definable. Lemma 6.1 states that every self interpretation of $\mathbb{Z}$ is trivial. Therefore, in order to show that $\Gamma$ is bi-interpretable with $\mathbb{Z}$, it is enough to prove that the isomorphism $h^{-1} : \Gamma \to H$ is definable. Since $h^{-1}$ is a homomorphism, if $D_1, D_2$ are definable subsets of $\Gamma$ and the restrictions of $h^{-1}$ to each $D_i$ is definable, then the restriction of $h^{-1}$ to $D_1^{-1}$ and $D_1 D_2$ are definable.

Margulis’s Normal Subgroup Theorem implies that non-trivial normal subgroups of $\Gamma$ have finite index. Since finite index subgroups of $\Gamma$ are finitely generated, we can choose $\beta_1, \ldots, \beta_d \in \Gamma$ such that $\Lambda := \langle \beta_i \alpha \beta_i^{-1} \mid 1 \leq i \leq d \rangle$
is a normal finite index subgroup of $\Gamma$. Corollary 6.7 allows us to further assume that $D_1 := \langle \beta_1 \alpha_{1} \beta_1^{-1} \rangle \langle \beta_2 \alpha_{2} \beta_2^{-1} \rangle \cdots \langle \beta_d \alpha_{d} \beta_d^{-1} \rangle$ projects onto $\Gamma/\Gamma[p]$ for infinitely many prime ideals $p \triangleleft A$. Choose a finite representative set $D_2$ for $\Gamma/\Lambda$ which contains the identity and denote $D := D_1 \cup D_1^{-1} \cup D_2 \cup D_2^{-1}$. Since the restriction of $h^{-1}$ to $\langle \alpha \rangle$ is definable, the previous paragraph implies that the restriction of $h^{-1}$ to $D^2$ is also definable.

Every ideal of $A$ is generated by two elements. Therefore, there exist definable sets $I$ and $X \subseteq I \times H$ such that $H := \{ h^{-1}(\Gamma^*[q]) \mid q \triangleleft A \} = \{ X_i \mid i \in I \}$. Theorem 4.2 implies that there exists a uniformly definable collection $F$ of normal congruence subgroups of $\Gamma$ which contains $\{ \Gamma^*[q] \mid q \triangleleft A \}$. Let $J$ be the definable subset such that $j \in J$ if and only if, for every $i \in I$ and $j \in \tilde{J}$, denote $H[i] = X_i$ and $\Gamma^*[j] = Y_j$.

Let $J \subseteq \tilde{J}$ be the definable subset such that $j \in J$ if and only if the following condition holds:

a) $D \Gamma^*[j]/\Gamma^*[j] = \Gamma/\Gamma^*[j]$.

By the construction of $D$ we get that

b) The set $\{ \Gamma^*[j] \mid j \in J \}$ is infinite.

We claim that the set $W := \{(i,j) \in I \times J \mid H[i] = h^{-1}(\Gamma^*[j])\}$ is definable. We first show that if the claim is true then $h^{-1}$ is definable. Since $\Gamma$ is centerless, two elements of $\Gamma$ are equal if and only if they are equal modulo infinitely many $\Gamma^*[q]$. Thus, for every $\gamma \in \Gamma$ and $\eta \in H$, $h^{-1}(\gamma) = \eta$ if and only if, for every $(i,j) \in W$, there exists $\delta \in D$ such that $\delta \Gamma^*[j] = \gamma \Gamma^*[j]$ and $h^{-1}(\delta) H[i] = \eta H[i]$. Since $h^{-1} |_{D}$ is definable, the later statement can be expressed as a first order statement.

It remains to show that $W$ is definable. Let $U \subseteq I \times J$ be the set such that $(i,j) \in U$ if and only if the following two conditions hold:

c) $h^{-1}(D) H[i]/H[i] = H/H[i]$.

d) For every $\delta_1, \delta_2 \in D^2$, $\delta_1 \Gamma^*[j] = \delta_2 \Gamma^*[j]$ if and only if $h^{-1}(\delta_1) H[i] = h^{-1}(\delta_2) H[i]$.

Since $h^{-1}$ is definable on $D^2$, conditions [c] and [d] are first order conditions. Thus, $U$ is definable. Clearly, $W \subseteq U$ so in order to complete the proof it is enough to show that $U \subseteq W$. Item [d] implies that, for every $(i,j) \in U$, $h^{-1}$ induces a bijection between the fibers of the reduction map $D^2 \to \Gamma/\Gamma^*[j]$. 

40
and the fibers of the reduction map $h^{-1}(D^2) \to H/H[i]$. Moreover, items a) and c) imply that, for every $(i, j) \in U$, $D$ and $h^{-1}(D)$ project onto $\Gamma/\Gamma^*[j]$ and $H/H[i]$, respectively. Thus, Lemma 6.8 implies that $U \subseteq W$. □

7 Width of squares and bi-interpretation

The following Lemma is well known, we include a proof for the convenient of the reader.

Lemma 7.1. The ring $\mathbb{Z}$ interprets every finitely presented group.

Proof. We first claim that for every $d \geq 1$, the ring $\mathbb{Z}$ interprets a finitely generated free group of rank at least $d$. This could be proved directly using Gödel’s encoding or in the following way: For every $d$, there exists $p \triangleleft \mathbb{Z}$ such that $\text{SL}_2(\mathbb{Z}; p)$ is a free group of rank at least $d$. Clearly, $\mathbb{Z}$ interprets $\text{SL}_2(\mathbb{Z}; p)$.

Let $\Gamma$ be a finitely presented group and let $\rho : F \to \Gamma$ be an epimorphism where $F$ is a free group of finite rank. Since $\Gamma$ is finitely presented, $\ker \rho$ is a recursively enumerable subset of $F$. The result follows from Theorem 6.3. □

Lemma 7.2. Let $\Gamma$ be a finitely presented group which is bi-interpretable with the ring $\mathbb{Z}$. Let $k \geq 2$ and assume that the word $x^k[y, z]$ has finite width in $\Gamma$. If $\Delta$ is a finite central extension of $\Gamma$ by a group of size $k$ then $\Delta$ is bi-interpretable with $\mathbb{Z}$.

Proof. Since bi-interpretability is an equivalence relation, it is enough to show that $\Gamma$ and $\Delta$ are bi-interpretable. Identifying $\Gamma$ with a quotient of $\Delta$ by a central subgroup of size $k$, we can view $\Gamma$ as an imaginary in $\Delta$. Then $\mathcal{C} := (\Gamma, \text{id}_\Gamma)$ is an interpretation of $\Gamma$ in $\Delta$. Lemma 7.1 implies that there exists an interpretation $\mathcal{D} := (D, d)$ of $\Delta$ in $\Gamma$. Since $\Gamma$ is an imaginary in $\Delta$, $D$ is also an imaginary in $\Delta$.

We want to show that $\mathcal{D} \circ \mathcal{C} = \mathcal{D}$ and $\mathcal{C} \circ \mathcal{D} = ([\mathcal{D}^* \Gamma, d_\Gamma]$ are trivial. Since $\Gamma$ is bi-interpretable with $\mathbb{Z}$, every self interpretation, in particular $\mathcal{C} \circ \mathcal{D}$, is trivial. Thus, $d_\Gamma$ is definable in $\Gamma$. Since we view $\Gamma$, and thus also $\mathcal{D}^* \Gamma$, as imaginaries of $\Delta$, $d_\Gamma$ is also definable as a function between two imaginaries in $\Delta$. Let $\rho : \Delta \to \Gamma$ be the quotient map. We have a commutative square:
Since \( \rho \) is definable in \( \Delta \), \( \mathcal{G}^* \rho \) is definable as a function between imaginaries of \( \Gamma \) and thus also as a function between imaginaries of \( \Delta \). It follows that \( \rho \circ d = \mathcal{G}^* \rho \circ d \Gamma \) is definable in \( \Delta \).

Recall that the bijection \( d : D \to \Delta \) induces a group structure on \( D \) and that the induced multiplication \( D \times D \to D \) is definable in \( \Delta \). Denote \( w = x^k[y, z] \). For every \( \delta_1, \delta_2, \delta_3, \delta'_1, \delta'_2, \delta'_3 \in D \) satisfying \( \rho \circ d(\delta_i) = \rho \circ d(\delta'_i) \), for \( 1 \leq i \leq 3 \), we have

\[
d(w(\delta_1, \delta_2, \delta_3)) = w(d(\delta_1), d(\delta_2), d(\delta_3)) = w(d(\delta'_1), d(\delta'_2), d(\delta'_3)) = d(w(\delta'_1, \delta'_2, \delta'_3)).
\]

It follows that if \( \alpha = w(\alpha_1, \alpha_2, \alpha_3) \in w(\Delta) \), \( \delta = w(\delta_1, \delta_2, \delta_3) \in w(D) \) and, for every \( 1 \leq i \leq 3 \), \( \rho \circ d(\delta_i) = \rho(\alpha_i) \), then \( d(\delta) = \alpha \). Thus, the restriction of \( d^{-1} \) to \( w(\Delta) \) is definable. Since \( w \) has finite width in \( \Gamma \) and, thus, in \( \Delta \), the restriction of \( d^{-1} \) to \( \langle w(\Delta) \rangle \) is definable. Since \( \Delta \) is finitely generated, \( [\Delta : \langle w(\Delta) \rangle] \) \(< \infty \) so \( d^{-1} \) is definable.

**Definition 7.3.** Suppose that \( L \) is a first order language and that \( M \) is an \( L \)-structure. We denote by \( \text{Aut}_L(M) \) the group of automorphisms of \( M \) as an \( L \)-structure. In particular, the elements of \( \text{Aut}_L(M) \) point-wise fix the constants.

For every \( \varphi \in \text{Aut}_L(M) \) and every imaginary \( I \) in \( M \), we also denote by \( \varphi_I \) the automorphism that \( \varphi \) induces on \( I \). Note that, if \( F : I \to J \) is a definable function between imaginaries, then, for every \( x \in I \), \( F(\varphi_I(x)) = \varphi_J(F(x)) \).

**Definition 7.4.** Suppose that \( L \) is a first order language, \( M \) is an \( L \)-structure and \( I \) is a definable subset of \( M \). Denote the \( L \)-theory of \( M \) by \( \text{Th}_M \) and let \( \phi \) be an \( L_M \)-formula such that \( I = \phi(M) \). Then for every \( \text{Th}_M \) model \( M' \), \( I' := \phi(M') \) is a definable subset of \( M' \) which is independent of the choice of the formula \( \phi \). Thus, there is no ambiguity in denoting the set \( I' \) by \( I(M') \).

We use similar definition and notation in the case where \( I \) is an imaginary.
Lemma 7.5. Suppose that $L$ is a first order language, $M$ is an $L$-structure and $I$ is an imaginary. Let $Th_M$ be the $L$-theory of $M$. Then a necessary condition for the existence of a definable surjective function from $I$ onto $M$ is that for every $Th_M$ model $M'$ and every automorphism $\varphi \in Aut_L(M')$, if $\varphi_{I(M')} = \text{id}_{I(M')}$ then $\varphi = \text{id}$.

Proof. Assume that $F : I \to M$ is a definable surjective function. Let $M'$ be a $Th_M$ model and $\varphi \in Aut_L(M')$ be such that $\varphi_{I(M')} = \text{id}_{I(M')}$. Then for every $x \in I(M')$, $F(M')(x) = F(M')(\varphi_I(x)) = \varphi(F(M')(x))$. Since $F(M') : I(M') \to M'$ is surjective, $\varphi = \text{id}$.

Proof of Theorem 1.7. The if part is Lemma 7.2. For the only if part, assume that the word $w = x^d[y,z]$ has infinite width in $\Gamma$ and, thus, also in $\Delta$. View $\Gamma$ as the quotient of $\Delta$ by a central subgroup $\Lambda$ of size $d$. In particular, $\Gamma$ is an imaginary in $\Delta$. By Lemma 7.1, there exists an interpretation $C = (C,c)$ of $\Delta$ in $\Gamma$. Since $\Gamma$ is an imaginary of $\Delta$, $C$ is also an interpretation of $\Delta$ in itself. If $\Delta$ is bi-interpretable with $\mathbb{Z}$ then Lemma 6.1 implies that $C$ is trivial so $C : C \to \Delta$ is definable. Lemma 7.5 implies that, in order to show that $c$ is not definable, it is enough to show that there exists a $Th_\Delta$-model $\Delta'$ and a non-identity automorphism $\varphi \in Aut_{L_\Delta}(\Delta')$ such that $\varphi_{C(\Delta')} = \text{id}_{C(\Delta')}$. Note that $Aut_{L_\Delta}(\Delta')$ is the subgroup of $Aut(\Delta')$ consisting of the group automorphisms which fix every element of $\Delta$ and that, if $\varphi_{\Delta'/\Lambda} = \text{id}_{\Delta'/\Lambda}$, then $\varphi_{C(\Delta')} = \text{id}_{C(\Delta')}$. Let $U$ be a non-principal ultrafilter on $\mathbb{N}$ and denote $\Delta' := \prod_{n \in \mathbb{N}} \Delta'/U$. Identify $\Delta$ as a subgroup of $\Delta'$ via the diagonal embedding so $\Delta'$ is a $Th_\Delta$-model. Since the width of $w$ in $\Delta$ is infinite, $[\Delta' : \langle w(\Delta') \rangle] = \infty$ and $\Delta'/\langle w(\Delta') \rangle$ is an uncountable abelian group of exponent $d$. Since $\Delta$ is finitely generated, there exists a non-trivial homomorphism $\rho : \Delta' \to \Lambda$ such that $\rho_{\Delta} = \text{id}_{\Delta}$. The automorphism $\varphi \in Aut_{L_\Delta}(\Delta')$ defined by $\varphi(x) = x\rho(x)$ is the desired automorphism.

8 Proof of Theorem 1.11 and Lemma 4.16

Setting 8.1. $K$ is a number field, $S$ is a finite set of places containing all archimedean ones, $A$ is the ring of $S$-integers, $\Theta_q = \text{Spin}_q$, where $q$ is a regular integral quadratic form on $A^n$ and $w \in S$ is a place such that $i_q(K^n_w) \geq 1$. Finally, $\Gamma$ is a congruence subgroup of $G(A)$.
For every subspace $C$ of $K^n$, we view $\Theta_{q|C}(K) := \text{Spin}_{q|C}(K)$ as a subgroup of $\Theta_q(K)$.

For every place $v$, let $K_v$ be the $v$-completion of $K$. For a subset $C \subseteq K^n$ let $C_v$ be its closure in $(K_v)^n$. In particular, $A_v = K_v$ for $v \in S$. For $v \notin S$, let $k_v$ be the residue field of $A_v$ and $p_v : A_v \to k_v$ be the residue map. The kernel of $p_v$ is denote by $p_v$.

**Remark 8.2.** In some places we assume the stronger condition $i_q(K^n_w) \geq 2$. In particular, in the proofs of Theorem 1.11 and Lemma 4.16 we assume that $i_q(K^n_w) \geq 2$.

### 8.1 Proof of Theorem 1.11

The following definition is essential in what follows.

**Definition 8.3.** Under Assumption 8.1, let $a_1 \in A^n$ be non-isotropic and $a_2, a_3 \in \Gamma a_1$. We say that $(a_1, a_2, a_3)$ is $A$-good if there exist $a_4 \in A^n$ and $\sigma, \tau \in \Gamma$ such that $\sigma(a_1, a_3) = (a_1, a_4)$ and $\tau(a_1, a_3) = (a_2, a_4)$. Similarly, for any place $v$, if we replace $A$ by $A_v$ and $\Gamma$ by $\Gamma_v$, we get the notion of an $A_v$-good triple.

The following lemma is the motivation for Definition 8.3.

**Lemma 8.4.** Under Setting 8.1, let $a_1, a_2 \in A^n$ and let $M$ be a symmetric normal subset of $\Gamma$. If there are $\beta, \gamma \in M$ such that $(a_1, \beta(a_2), \gamma(a_1))$ is $A$-good, then $a_2 \in M^3a_1$.

**Proof.** If $\sigma(a_1, \gamma(a_1)) = (a_1, a_4)$ and $\tau(a_1, \gamma(a_1)) = (\beta(a_2), a_4)$ then $\delta(a_1) = a_2$ where $\delta := \beta^{-1}\tau\gamma^{-1}\tau^{-1}\sigma\gamma^{-1} \in M^3$.

Lemma 8.4 implies that, in order to prove Theorem 1.11 it is enough to show that there exists $N$ such that, for every non-isotropic $a_1$, there exists an $S$-adelic neighborhood $V$ of $a_1$ in $\Gamma a_1$ such that, for every $a_2 \in V$, there exist $\beta, \gamma \in \text{gcl}_\gamma(\alpha)^N$ for which $(a_1, \beta(a_2), \gamma(a_1))$ is $A$-good.

We start by stating a local-to-global condition for being $A$-good. Recall that if $B$ is a commutative ring then a matrix $M \in M_k(B)$ is said to be in general position if for every non-empty $I \subseteq \{1, \ldots, k\}$, $\det M_I \neq 0$ where $M_I$ is the principal $I$-minor of $M$. The following lemma is a reformulation of Lemma 8.1 of [Kne].
Lemma 8.5 (Local-to-global principle for \(A\)-good triplets, \([\text{Kne}, \text{Lemma 8.1}]\)). Under Setting 8.1, assume that \(n \geq 6\) and \(i_q(K_v^n) \geq 2\). Let \(a_1, a_2, a_3 \in A^n\) be non-isotropic vectors such that \(i_q((K_wa_1 + K_wa_2)^\perp) \geq 1\), \(i_q((K_wa_1 + K_wa_3)^\perp) \geq 1\), and the matrix

\[
M(a_1, a_2, a_3) = \begin{pmatrix}
q(a_1, a_1) & q(a_1, a_2) & q(a_1, a_3) \\
q(a_2, a_1) & q(a_2, a_2) & q(a_2, a_3) \\
q(a_3, a_1) & q(a_3, a_2) & q(a_3, a_3)
\end{pmatrix}
\]

is in general position (note that the \((2,3)\) and \((3,2)\) entries of the above matrix are equal to \(q(a_1, a_3)\) and not to \(q(a_2, a_3)\)). Assume that, for every place \(v\), \((a_1, a_2, a_3)\) is \(A_v\)-good. Then \((a_1, a_2, a_3)\) is \(A\)-good.

The next task is to find local conditions for being \(A_v\)-good. The following Lemma is a reformulation of Lemmas 7.1, 7.2, 7.3 and 7.4 of \([\text{Kne}]\).

Lemma 8.6 (Local conditions for being \(A_v\)-good). Under Assumption 8.7, assume that \(n \geq 5\). Let \(M(a_1, a_2, a_3)\) be the matrix defined in Equation (5).

Let \(v\) be a place.

1. Let \(a_1, a_2, a_3 \in A_v^n\) be non-isotropic vectors that belong to the same \(\Gamma_v\)-orbit. If \(v \in S\), the matrix \(M(a_1, a_2, a_3)\) is in general position, and 
\(i_q((K_v a_1 + K_v a_3)\perp) \geq 1\), then \((a_1, a_2, a_3)\) is \(A_v\)-good.

2. Let \(a_1 \in A_v^n\) be non-isotropic, and let \(\Delta_v\) be an open subgroup of \(\Gamma_v\). Then there are open sets \(U_v^2, U_v^3 \subset A_v^n\) such that \(U_v^2 \cap \Delta_v a_1 \neq \emptyset\), \(U_v^3 \cap \Delta_v a_1 \neq \emptyset\) and, for every \(a_2 \in U_v^2 \cap \Delta_v a\) and \(a_3 \in U_v^3 \cap \Delta_v a_1\), the matrix \(M(a_1, a_2, a_3)\) is in general position and \((a_1, a_2, a_3)\) is \(A_v\)-good.

3. Assume that \(v \notin S\), that \(v\) is not dyadic and that \(q\) is regular on \(A_v^n\). Let \(a_1, a_2, a_3 \in A_v^n\) be in the same \(\Gamma_v\) orbit such that \(M(a_1, a_2, a_3)\) is in general position and \(q(a_1) \in A_v^\times\). Then \((a_1, a_2, a_3)\) is \(A_v\)-good if the following two conditions hold:

(i) At least one of \(\text{disc}_q(a_1, a_2)\) or \(\text{disc}_q(a_1, a_3)\) belongs to \(A_v^\times\).

(ii) \(p_v(a_1), p_v(a_2),\) as well as \(p_v(a_1), p_v(a_3),\) are linearly independent over \(k_v\).

Let \(a_1 \in A^n\) be non-isotropic vector. We will apply part 1 of Lemma 8.6 only for \(v = w\). Part 2 will be used for a finite set of places with bad
properties, and part 3 will be used for the remaining places. Note that, if $T \supseteq S$ is a finite set of places, then the set consisting of the vectors $a_2 \in A^n$ such that for every $v \not\in T$, $p_v(a_1), p_v(a_2)$ are linearly independent over $k_v$, is not open in the $S$-adic topology. Thus, if $a_1 \in A^n$ is non-isotropic, then the subset of $(\Gamma a_1)^3$ consisting of the triplets that satisfy the conditions of Lemma 8.6 is not open in the $S$-adic topology and we cannot directly use Lemmas 8.5 and 8.6 in order to prove Theorem 1.11. Lemma 8.8 below allows us to overcome this issue.

**Definition 8.7.** Under Assumption 8.1,

1. Let $T_\Gamma$ be as in Definition 3.3 with respect to $G := \Theta_q$.
2. For $\alpha \in \Gamma$, let $T_\alpha$ be the set of places $v \not\in S$ for which $\langle \text{gcl}_\Gamma(\alpha) \rangle \neq \Theta_q(A_v)$.
3. For $a \in A^n$, let $T_a$ be the set of places $v \not\in S$ for which $q(a) \neq 0$.
4. For $\alpha \in \Gamma$ and $a \in A^n$, denote $T_{\Gamma,a,\alpha} := T_\Gamma \cup T_a \cup T_\alpha$.

The following lemma is an effective version of Lemma 5.2 of [Kne].

**Lemma 8.8 (cf. Lemma 5.2 of [Kne]).** Under Setting 1.1, for every $n \geq 7$ and every $\epsilon > 0$ there exists $N = N(n, \epsilon)$ such that the following claim holds:

If $\alpha \in \Gamma$ is $\epsilon$-separated, then there exists an open neighborhood of the identity, $W \subseteq \prod_{v \in T_\Gamma} \langle \text{gcl}_\Gamma(\alpha) \rangle$, such that, for every $b_1, b_2 \in A^n$ with $q(b_1) = q(b_2) \neq 0$ and every finite set of places $T \supseteq T_{\Gamma,b_1,\alpha} \cup S$, the set of elements $\beta \in \text{gcl}_\Gamma(\alpha)^N$ for which

1. $i_q(K\omega b_1 + K\omega \beta b_2) = 1$.
2. $p_v(b_1), p_v(\beta b_2)$ are linearly independent, for every $v \not\in T$.

contains a dense subset of $W \times \prod_{v \in T_\Gamma \setminus (T_{\Gamma,b_1,\alpha} \cup \{w\})} \langle \text{gcl}_\Gamma(\alpha) \rangle$.

The proof of Lemma 8.8 is given in the next subsection.

**Proof of Theorem 1.11.** The proof closely follows the proof of Theorem 6.1 of [Kne].

Denote $a_1 := a \in A^n$, $\Delta = \langle \text{gcl}_\Gamma(\alpha) \rangle$, $T := T_{\Gamma,a_1,\alpha} \cup S$. Lemma 8.8 implies that there are a constant $N$ and an open neighborhood of the identity $W \subseteq$
\( \prod_{v \in T_{\Gamma}} (\text{gcl}_{T}(\alpha)) \) such that, for any \( b_1, b_2 \in A^n \) such that \( q(b_1) = q(b_2) = q(a) \), and any finite \( T' \) containing \( T \),

the set of \( \beta \in \text{gcl}_{T}(\alpha)^N \) for which \( i_q(K_w b_1 + K_w \beta b_2) = 1 \)
and \( p_v(b_1), p_v(\beta b_2) \) are linearly independent, for every \( v \notin T' \), contains a dense subset of \( W_{T'} := W \times \prod_{v \in T \setminus (T_{\Gamma} \cup \{w\})} (\text{gcl}_{T}(\alpha)) \).

For every \( v \in T_{\Gamma} \), choose an open normal subgroup \( \Delta_v^* \subseteq \Delta_v \) such that \( \prod_{v \in T_{\Gamma}} \Delta_v^* \subseteq W \). For every \( v \in T \setminus T_{\Gamma} \), denote \( \Delta_v^* = \Delta_v \). Item 2 of Lemma 8.4 implies that for every \( v \in T \setminus \{w\} \), there are open sets \( U_v^2, U_v^3 \subseteq A^n_v \) such that \( U_v^2 \cap \Delta_v^* a_1 \neq \emptyset \), \( U_v^3 \cap \Delta_v^* a_1 \neq \emptyset \) and, for every \( a_2 \in U_v^2 \cap \Delta_v^* a \) and \( a_3 \in U_v^3 \cap \Delta_v^* a_1 \), the matrix \( M(a_1, a_2, a_3) \) is in general position and \( (a_1, a_2, a_3) \) is \( A_v \)-good.

Let \( V = \Gamma a_1 \cap \bigcap_{v \in T \setminus S} U_v^2 \). We will show that \( \text{gcl}(\alpha)^{3N} a_1 \supseteq V \), which implies that \( \text{gcl}(\alpha)^{6N} a_1 \) contains an \( S \)-adic neighborhood of \( a \) in \( \Gamma a \).

Let \( a_2 \in V \). Lemma 8.4 implies that it is enough to find \( \beta, \gamma \in \text{gcl}_{T}(\alpha)^N \) such that \( (a_1, \beta a_2, \gamma a_3) \) is \( A \)-good. We start by finding \( \beta \). Applying \( (6) \) with \( b_1 = a_1, b_2 = a_2, \) and \( T' = T \), and since \( \{ \beta \in \Gamma \cap W_T \mid \beta a_2 \in U_v^2 \} \) is non-empty and open, we can find \( \beta \in \text{gcl}_{T}(\alpha)^N \) such that:

1. (c) For every \( v \in T \setminus \{w\} \), \( \beta \in \Delta_v^* \) and \( \beta a_2 \in U_v^2 \).
2. (d) \( i_q(K_w a_1 + K_w \beta a_2) = 1 \) so \( i_q((K_w a_1 + K_w \beta a_2)^+) \geq 1 \).
3. (e) \( p_v(a_1), p_v(\beta a_2) \) are linearly independent, for every \( v \notin T \).

Item \( (b) \) and the choice of \( U_v^2, U_v^3 \) imply that, for every \( v \in T \setminus \{w\} \) and \( a_3 \in U_v^3 \cap \Delta_v^* a_1 \), the triple \( (a_1, \beta a_2, a_3) \) is \( v \)-good and \( M(a_1, \beta a_2, a_3) \) is in general position.

We now find \( \gamma \). One of the requirements on \( \gamma \) will be that \( \gamma a_1 \in U_v^3 \cap \Delta_v^* a_1 \), for every \( v \in T \setminus \{w\} \). It then follows that the triple \( (a_1, \beta a_2, \gamma a_1) \) is \( v \)-good, for every \( v \in T \setminus \{w\} \).

Since \( M(a_1, \beta a_2, a_3) \) is in general position, \( \text{disc}(a_1, \beta a_2) \neq 0 \). It follows that the set \( T(\beta) \) consisting of the places \( v \notin T \) for which \( \text{disc}(a_1, \beta a_2) \notin A_v^x \) is finite. For every \( v \in T(\beta) \), \( q(a_1) \in A_v^* \) and \( \Delta_v = \Theta_q(A_v) \). Thus, for every \( v \in T(\beta) \), the set of \( \gamma_v \in \Delta_v \) such that \( \text{disc}(a_1, \gamma_v a_1) \in A_v^* \) is non-empty and open. Applying \( (6) \) with \( b_1 = b_2 = a_1 \) and \( T' = T \cup T(\beta) \), there is \( \gamma \in \text{gcl}_{T}(\alpha)^N \) such that
(f) For every $v \in T \setminus \{w\}$, $\gamma \in A^\times_v$ and $\gamma a_1 \in U^3_v$.

(g) $\text{disc}(a_1, \gamma a_1) \in A^\times_v$ for $v \in T(\beta)$.

(h) $i_q(K_w a_1 + K_w \gamma a_1) = 1$ so $i_q((K_w a_1 + K_w \gamma a_1)^\perp) \geq 1$.

(i) $p_v(a_1), p_v(\gamma a_1)$ are linearly independent, for every $v \notin T \cup T(\beta)$. It follows from item (g) that $p_v(a_1), p_v(\gamma a_1)$ are linearly independent also for $v \in T(\beta)$.

Since $\gamma a_1 \in U^3_v \cap A^\times_v a_1$, $M(a_1, \beta a_2, \gamma a_1)$ is in general position and $(a_1, \beta a_2, \gamma a_1)$ is $A_v$-good for every $v \in T \setminus \{w\}$. Item [d] of Lemma 8.6 and item [h] imply that $(a_1, \beta a_2, \gamma a_1)$ is $w$-good. Item [b] of Lemma 8.6 items [e], [g], [i], and the definition of $T(\beta)$ imply that $(a_1, \beta a_2, \gamma a_1)$ is $A_v$-good for every $v \notin T$. We conclude that $(a_1, \beta a_2, \gamma a_1)$ is $A_v$-good for every $v$. Lemma 8.9 and items [d] and [h] imply that $(a_1, \beta a_2, \gamma a_1)$ is $A$-good. Lemma 8.10 shows that $a_2 \in \text{gcl}_\Gamma(\alpha)^A$.

### 8.2 Proof of Lemma 8.8

**Lemma 8.9** (Lemmas 4.2, 4.3, 4.4, 4.5 and 4.6 of [Kne]). Under Setting 8.1, assume that $n = 3$ or $n \geq 5$. Let $\alpha \in \Gamma \setminus Z(\Gamma)$ and denote $\Delta := \langle \text{gcl}_\Gamma(\alpha) \rangle$.

Then:

1. $\Delta$ is dense in $\prod_{v \neq w} \Delta_v$.
2. Let $v \in S$. Then, $\Delta_v = \Gamma_v = \Theta_q(K_v)$.
3. For every $v \notin S$, $\Delta_v$ is open in $\Theta_q(K_v)$.
4. For all but finitely many $v \notin S$, $\Delta_v = \Gamma_v = \Theta_q(A_v)$.
5. If $v \notin S \cup T_\Gamma$, then $p_v(\Theta_q(A_v)) = \Theta_q(k_v)$.

**Lemma 8.10** (Lemma 4.7 of [Kne]). Under Assumption 8.4, assume that $n = 3$ or $n \geq 5$. Let $b_1, b_2 \in K^n$ be non-zero vectors and let $U$ be a non-empty open subset of $\Theta_q(A^w)$ for every $r > 0$, there is a non-empty open subset $W \subseteq U$ such that every element $\alpha \in \Theta_q(K) \cap W$, $|q(b_1, \alpha b_2)|_w > r$. In particular, if $r$ is large enough then $i_q(K_w b_1 + K_w \alpha b_2) = 1$. 

48
Definition 8.11. For an element $\alpha \in \Theta_q(K)$, the support of $\alpha$ is the subspace 
$$\text{supp}(\alpha) := \{ a \in K^n \mid \alpha(a) = a \}^\perp.$$ We say that $\alpha$ is strongly $\epsilon$-separated if $\alpha \restriction_{\text{supp}(\gamma)}$ is $\epsilon$-separated in $\Theta_q|_{\text{supp}(\gamma)}(K)$.

For example, any reflection is $\sqrt{2}$-separated, but not strongly $\epsilon$-separated, for any $\epsilon > 0$. The following lemma is an effective version of Lemma 4.8 of [Kne].

Lemma 8.12 (cf. Lemma 4.8 of [Kne]). For every $n \geq 5$ and every $\epsilon > 0$ there exists $N = N(n, \epsilon)$ such that the following claim holds:

If $\alpha \in \Gamma$ is $\epsilon$-separated then the set $\text{gcl}_\Gamma(\alpha)^N$ contains a strongly $1$-separated element $\beta$ such that $\text{supp}(\beta)$ is a 5-dimensional regular subspace and $i_q(\text{supp}(\beta)_w) \geq 1$.

Proof. The proof is by induction on $n$. Assume that $n = 5$. Let $N = N(5, \epsilon)$ be the constant in Proposition 3.8. For every $v \in S_{\text{def}}$, choose $\beta_v \in \Theta_v(K_v)$ such that $\text{dist}_v(\beta_v, Z(\Theta_v)) > 1$ and $\text{supp}(\beta_v) = K_v^5$. The definition of $N$ implies that there exists $\beta \in \text{gcl}_\Gamma(\alpha)^N$ such that $\beta$ is arbitrary close to $\beta_v$, for every $v \in S_{\text{def}}$. If the approximation is good enough, then $\beta$ has the required properties.

Assume $n > 5$ and let $M = M(n, \epsilon)$ be the constant in Proposition 3.8. For every $v \in S \setminus \{w\}$, choose $a_v \in A_v^n$ and $\beta_v \in \langle \text{gcl}_\Gamma(\alpha) \rangle_v = \Theta_q(K_v)$ such that, for $c_{v,i} := \beta_v^i a_v$, the following hold:

(a) For every $v \in S_{\text{def}}$, $c_{v,0}, c_{v,1}, c_{v,2}, c_{v,3}, c_{v,4}$ is an orthonormal basis to a regular 5-dimensional subspace.

(b) For every $v \in S \setminus (S_{\text{def}} \cup \{w\})$, $\text{Span}_{K_v}\{c_{v,i} \mid 0 \leq i \leq 4\}$ is a regular isotropic subspace.

A straightforward computation shows that, for every $v \in S_{\text{def}}$ and every $\gamma_v \in \Theta_q(K_v)$, if supp$(\gamma_v) = \text{Span}_{K_v}\{c_{v,0}, c_{v,1}\}$, $\gamma_v(c_{v,0}) = c_{v,1}$ and $\gamma_v(c_{v,1}) = -c_{v,0}$ then, for $\delta_v = \beta_v \gamma_v \beta_v^{-1} \gamma_v^{-1}$, we have dist$_v(\delta_v \restriction_{\text{supp}(\delta_v)}, Z(\Theta_q|_{\text{supp}(\delta_v)}(K_v)))) = \sqrt{2}$. Lemma 8.10 implies that we can choose $a \in A_v^n$ and $\beta \in \text{gcl}_\Gamma(\alpha)^M$ which are arbitrary close to $a_v$ and $\beta_v$, for every $v \in S \setminus \{w\}$, such that $i_q(K_w a + K_w \beta a) \geq 1$. If the approximation is good enough, then for $c_i := \beta^i a$, the following hold:

(c) $C := \text{Span}_K\{c_i \mid 0 \leq i \leq 2\}$ and $D := \text{Span}_K\{c_i \mid 0 \leq i \leq 4\}$ are regular.
(d) For every $v \in S_{def}$ and every $\gamma_v \in \Theta_q(K_v)$ satisfying $\text{supp}(\gamma_v) = \text{Span}_{K_v}\{c_0, c_1\}$, $\gamma_v(c_0) = c_1$, and $\gamma_v(c_1) = -c_0$, we have $\text{supp}(\beta\gamma_v\beta^{-1}\gamma_v^{-1}) \subseteq C$ (because $\text{supp}(\beta\gamma_v\beta^{-1}) = \text{Span}_{K_v}\{c_1, c_2\}$) and $\text{dist}_v(\beta\gamma_v\beta^{-1}\gamma_v^{-1} \mid C, Z(\Theta_q(K_v))) > 1$.

(e) For every $v \in S \setminus (S_{def} \cup \{w\})$, $D_v$ is an isotropic subspace.

The group $\Gamma \cap \Theta_{q,\mu}(K)$ is a congruence subgroup in $\Theta_{q,\mu}(K)$ and $i_q(C_w) \geq 1$. Hence, the strong approximation theorem and item (d) imply that there exists $\gamma \in \Gamma \cap \Theta_{q,\mu}(K)$ such that $\delta := \beta\gamma\beta^{-1}\gamma^{-1} \in \text{gcl}_\Gamma(\alpha)^{2M} \cap \Theta_{q,\mu}(K)$ is 1-separated in $\Theta_{q,\mu}(K)$. Since $\Gamma \cap \Theta_{q,\mu}(K)$ is a congruence subgroup in $\Theta_{q,\mu}(K)$ and $i_q(D_w) \geq 1$, the induction basis implies that $\text{gcl}_{\Theta_{q,\mu}(K)\cap \mu}(\delta)^N \subseteq \text{gcl}_\Gamma(\alpha)^{2NM}$ contains the required element. $\square$

**Proof of Lemma 8.8.** The proof closely follows the proof of Theorem 5.2 of \[Kne\]. Lemma 8.12 implies that there is $N_1$ for which there exists an $\beta \in \text{gcl}_\Gamma(\alpha)^{N_1}$ such that:

(a) $C := \text{supp}(\beta)$ is a regular 5-dimensional plane.

(b) $\beta$ is strongly 1-separated.

(c) $i_q(C_w) = 1$.

By replacing $\beta$ with a conjugate element, we can assume that $b_1 \notin C \cup C^\perp$. Denote $\Lambda := \Gamma \cap \Theta_{q,\mu}(K)$, then $\Lambda$ is a congruence subgroup of $\Theta_{q,\mu}(K)$ and $\beta \in \Lambda$. By choosing a free $A$-lattice $M \subseteq C$, we get a form $\Theta_{M,q,\mu}(K)$ of $\Theta_{q,\mu}(K)$ defined over $A$. There is a finite set $T'$ of places, disjoint form $T$, a constant $N_2$ and a neighborhood of the identity $W' \subseteq \prod_{v \in (T \cup T') \setminus \{w\}} \Theta_{q,\mu}(K_v)$ such that the following items hold:

(d) For every $v \notin T \cup T'$, $A_v \cap C_v = M_v$ and $q$ is regular on $p_v(M_v)$. In particular, $k_v^n$ is an orthogonal sum of $p_v(M_v)$ and $p_v(M_v)^\perp$.

(e) For every $v \notin T \cup T'$, $p_v(b_1) \notin p_v(M_v)^\perp$.

(f) For every $v \notin T \cup T'$, $(\text{gcl}_\Lambda(\beta))_v = \Theta_{M,q,\mu}(A_v)$ and $\pi_{M,v}(\Theta_{M,q,\mu}(A_v)) = \Theta_{M,q,\mu}(k_v)$.

(g) $\text{gcl}_\Lambda(\beta)^{N_2}$ contains a dense subset of $W' \times \prod_{v \notin T \cup T' \cup \{w\}} (\text{gcl}_\Lambda(\beta))_v$.  

50
Indeed, item (d) follows from the fact that for all but finitely many places \( v \), \( A_v^n \cap C_v = M_v \) and \( q \) is regular on \( M_v \). Item (e) follows from the assumption that \( b_1 \notin C^\perp \). Item (f) follows from Lemma 8.9 applied to \( \beta \) and \( \Lambda \). The existence of \( N_2 \) and \( W' \) for which Item (g) holds follows from Proposition 3.8 applied to \( \beta \) and \( \Lambda \).

Proposition 3.8 applied to \( \Gamma \) and \( \alpha \) shows that there exit a constant \( N_3 \) and an open neighborhood of the identity \( W \subseteq \prod_{v \in T'} \Theta_q(K_v) \) such that \( \text{gcl}_1(\alpha)^{N_3} \) contains a dense subset of \( W \times \prod_{v \notin T' \cup \{ w \}} \langle \text{gcl}_1(\alpha) \rangle_v \). Let \( U \) be a non-empty open subset of \( W \times \prod_{v \in T \setminus (T' \cup \{ w \})} \langle \text{gcl}_1(\alpha) \rangle_v \). We will show that the intersection of \( \text{gcl}_1(\alpha)^{N_1N_2+N_3} \) with \( U \) contains an element which satisfies the desired properties.

Fix some place \( u \notin T \cup T' \). Then \( q(b_1) = q(b_2) \in A_v^\times \) so \( p_v(b_2) \neq 0 \). Since \( \langle \text{gcl}_1(\alpha) \rangle_v = \Theta_u \) and \( \dim C^\perp \geq 2 \), there exist \( \gamma_u \in \langle \text{gcl}_1(\alpha) \rangle_v \) such that \( b_1 + C_u \) and \( \gamma_u b_2 + C_u \) are linearly independent in \( K_v^n / C_u \). For every \( v \in T' \), \( p_v(\langle \text{gcl}_1(\alpha) \rangle_v) = \Theta_q(K_v) \), \( q \) is regular on \( k_v^n \) and \( q(b_1) = q(b_2) \in A_v^\times \), thus \( p_v(b_2) \neq 0 \) and there exists \( \gamma_v \in \langle \text{gcl}_1(\alpha) \rangle_v \) for which \( p_v(b_1) \) and \( p_v(\gamma_v b_2) \) are linearly independent over \( k_v \). Approximation at the places in \( T \cup T' \cup \{ u \} \) implies that there is \( \gamma \in \text{gcl}_1(\alpha)^{N_3} \) with the following properties:

(h) \( \gamma \in U \).

(i) \( b_1 + C \) and \( \gamma b_2 + C \) are linearly independent in \( K^n / C \).

(j) \( p_v(b_1) \) and \( p_v(\gamma b_2) \) are linearly independent over \( k_v \) for \( v \in T' \).

Item (i) implies that there is a finite set of places \( T'' \) which is disjoint from \( T \cup T' \) such that:

(k) For every \( v \notin T \cup T' \cup T'' \), the images \( p_v(b_1) + p_v(M_v) \) and \( p_v(\gamma b_2) + p_v(M_v) \) are linearly independent in \( k_v^n / p_v(M_v) \).

For every \( v \in T'' \), \( q(b_1) = q(b_2) \in A_v^\times \) so \( p_v(b_2) \neq 0 \). If \( v \in T'' \) and \( p_v(\gamma b_2) \in p_v(M)^\perp \), denote \( \gamma_v = \text{id} \). Item (e) implies that \( p_v(b_1) \) and \( p_v(\gamma_v b_2) \) are linearly independent over \( k_v \). If \( v \in T'' \) and \( p_v(\gamma b_2) \notin p_v(M)^\perp \), then items (d), (e) and (f) imply that there is \( \gamma'_v \in \Theta_{\mathcal{M} q|C}(A_v) \) such that \( p_v(b_1) \) and \( p_v(\gamma'_v b_2) \) are linearly independent over \( k_v \). Let \( V \) be an open subset of \( \Theta_{q|C}(A_v \setminus \{ w \}) \) such that for every \( \gamma' \in \Theta_{q|C}(K) \cap V \):

(l) For every \( v \in T \setminus \{ w \} \), \( \gamma' \) is so close to 1 such that \( \gamma' \gamma \in U \).
(m) For every $v \in T'$, $\gamma'$ is so close to 1 such that $p_v(b_1)$ and $p_v(\gamma'\gamma b_2)$ are linearly independent over $k_v$.

(n) For $v \in T''$, $\gamma'$ is so close to $\gamma'_v$ such that $p_v(b_1)$ and $p_v(\gamma'\gamma b_2)$ are linearly independent over $k_v$.

Let $c_1$ and $c_2$ be the orthogonal projections of $b_1$ and $\gamma(b_2)$ to $C$. Items (f) and (g) and Lemma 8.10 applied to $\beta$ and $\Lambda$, imply that there exists $\gamma' \in \text{gcl}_1(\beta N_2 \cap V)$ such that $q(c_1, \gamma' c_2)$ is arbitrary large. If $q(c_1, \gamma' c_2)$ is large enough then $i_q(K_w b_1 + K_w \gamma' b_2) = 1$. Denote $\delta := \gamma' \gamma \in \text{gcl}_1(\beta N_2 \cap V)$ such that $\gamma' \gamma \in \text{gcl}_1(\beta N_2 \cap V)$. Item (l) implies that $\delta \in U$. The linear independence of $p_v(b_1)$ and $p_v(\delta b_2)$ follows for $v \in T'$ from item (m), for $v \in T''$ from item (n) and for $v \notin T \cup T' \cup T''$ from item (k).

8.3 Proof of Lemma 4.16

Lemma 8.13 (cf. Lemma 4.10 of [Kne]). Under Setting 8.4, assume that $i_q(K_w) \geq 2$ and $n \geq 6$. For every $\epsilon > 0$ there exists a constant $N = N(n, \epsilon)$ (in particular, $N$ does not depend on $q$ nor on $\Gamma$) such that the following claim hold:

If $\alpha$ is $\epsilon$-separated and $a \in \mathbb{K}^n$ is non-isotropic, then $\text{gcl}_1(\alpha)^N$ contains an element which fixes $a$ and is strongly 1-separated.

Proof. Let $N := N(n, \epsilon)$ be as in Proposition 3.8. Lemma 8.10 and approximation imply that there exist $\beta \in \text{gcl}_1(\alpha)^N$ and $\gamma_v \in \Theta_q(K_{v+b_1+b_2}) \cap (K_v)$, for every $v \in S_{def}$, such that:

(a) $K_a + K\beta a + K\beta^2 a$ is a regular 3-dimensional subspace.

(b) $i_q(K_{v+a} + K_v \beta a) = 1$.

(c) For every $v \in S_{def}$, $\text{dist}_v((\beta^{-1} \gamma_v^{-1} \beta \gamma_v) |_{(K_{v+a})^1}, Z(\Theta_q|_{(K_{v+a})^1}(K_v))) > 1$.

Since $i_q((K_{v+a} + K_v \beta a)^1) \geq 1$ and $\Lambda := \Gamma \cap \Theta_q(K_{v+b_1+b_2}) \cap (K)$ is a congruence subgroup of $\Theta_q(K_{v+b_1+b_2}) \cap (K)$, the strong approximation theorem implies that there exists $\gamma \in \Lambda$ which is arbitrary close to $\gamma_v$, for every $v \in S_{def}$. If the approximation is good enough, then $\delta := \beta^{-1} \gamma^{-1} \beta \gamma \in \text{gcl}_1(\alpha)^{2N}$ fixes $a$ and the restriction of $\delta$ to $(K \gamma)^1$ is 1-separated in $\Theta_q(K_{v+a+b_2}) \cap (K)$. Lemma 8.12 implies that there exists $M = M(n)$ such that $\text{gcl}_1(\Gamma \cap \Theta_q(K_{v+a+b_2}) \cap (K))^{\delta M} \subseteq \text{gcl}_1(\alpha)^{2NM}$ contains the required element. \qed
Corollary 8.14. Under Setting 8.14, assume that $i_q(K_w) \geq 2$ and $n \geq 6$. For every $\epsilon > 0$ there exists a constant $N = N(n, \epsilon)$ such that the following claim hold:

Let $d \leq n - 6$ and let $a_0, a_1, \ldots, a_d \in K^n$ be non-isotropic orthogonal vectors such that $i_q((K_w a_0 + \ldots K_w a_{d-1})^\perp) \geq 2$. If $\alpha \in \Gamma$ is $\epsilon$-separated and $q \ll A$, then there exists $\beta \in \text{gcl}_\Gamma(\alpha)^N \cap \Theta_q(A; q)$ which is strongly 1-separated and fixes $a_0, \ldots, a_d$.

**Proof.** Denote $\epsilon' = \min(1, \epsilon)$. For every $0 \leq k \leq d$, denote $U_k := (\text{Span}_K \{a_i \mid 0 \leq i \leq k - 1\})^\perp$ and $\Gamma_k := \Gamma \cap \Theta_{q_0U_k}(K)$. For every $6 \leq n' \leq n$ let $N(n', \epsilon')$ be the constant given by Lemma 8.13 with respect to $n'$ and $\epsilon'$. Denote $N := \max\{N(n', \epsilon') \mid 6 \leq n' \leq n\}$.

We will prove by induction on $1 \leq k \leq d$ that there exists a strongly 1-separated $\alpha_k \in \text{gcl}_\Gamma(\alpha)^N \cap \Theta_{q_0U_k}(K)$. The case $k = 1$ follows from the definition of $N$. Assume that the claim is true for some $1 \leq k < d$. Since $\Gamma_k$ is a congruence subgroup in $\Theta_{q_0U_k}(K)$, by the definition of $N$, there exists a strongly 1-separated

$$\alpha_{k+1} \in \text{gcl}_{\Gamma_k}(\alpha_k)^N \cap \Theta_{q_0U_{k+1}}(K) \subseteq \text{gcl}_\Gamma(\alpha)^{N_{k+1}} \cap \Theta_{q_0U_{k+1}}(K).$$

For every $5 \leq n' \leq n$ let $M(n', 1)$ be the constant given by Proposition 8.13 and denote $M = \max_{n'} M(n', 1)$. By the definition of $M$, there exists a strongly 1-separated

$$\beta \in \text{gcl}_\Gamma(\alpha_d)^M \cap \Theta_q(A; q) \subseteq \text{gcl}_\Gamma(\alpha)^{N_{d}M} \cap \Theta_{q_0U_d}(K) \cap \Theta_q(A; q).$$

□

**Proof of Lemma 4.16.** Denote $\epsilon' = \min(1, \epsilon)$ and let $N := N(n, \epsilon')$ be the the constant given by Corollary 8.14. For every $n - 2 \leq n' \leq n$, let $M(n', \epsilon')$ be the constant given by Theorem 11.11 and denote $M := \max_{n'} M(n', \epsilon')$. For every $0 \leq r \leq 2$, let $U_r := (\text{Span}_K \{c_i \mid 0 \leq i \leq r - 1\})^\perp$ and $\Gamma_r := \Gamma \cap \Theta_{q_0U}(K)$. Note that $\Gamma_r$ is a congruence subgroup in $\Theta_{q_0U}(K)$, that $U_0 = K^n$, and that $\Gamma_0 = \Gamma$.

By the definition of $N$, there exists a strongly 1-separated element $\alpha_2 \in \text{gcl}_\Gamma(\alpha)^N \cap \Theta_{q_0U_2}(K)$. By the definition of $M$, there exists $0 \neq q_2 \ll A$ such that $\text{gcl}_{\Gamma_2}(\alpha_q)^M \cap \Theta_{q_0U_2}(K)$ contains the $q_2$-th neighborhood of $c_2$ in $\Gamma_2c_2$.

By the definition of $N$, there exists a strongly 1-separated element $\alpha_1 \in \text{gcl}_\Gamma(\alpha)^N \cap \Theta_{q_0U_1}(K) \cap \Theta_q(A; q_2)$. By the definition of $M$, there exists $0 \neq q_2$...
\( q_1 \vartriangleleft A \) such that \( q_1 \subseteq q_2 \) and \( \text{gcl}_{\Gamma_1}((\alpha_1)^M)_{c_1} \) contains the \( q_1 \)-th neighborhood of \( c_1 \) in \( \Gamma_1 c_1 \).

By the definition of \( N \), there exists a strongly 1-separated element \( \alpha_0 \in \text{gcl}_{\Gamma}(\alpha)^N \cap \Theta_{q_0}(K) \cap \Theta_{q}(A; q_1) \). By the definition of \( M \), there exists \( 0 \neq q_0 \vartriangleleft A \) such that \( q_0 \subseteq q_1 \) and \( \text{gcl}_{\Gamma_0}((\alpha_0)^M)_{c_0} \) contains the \( q_0 \)-th neighborhood of \( c_0 \) in \( \Gamma_0 c_0 \).

We claim that the \( q_0 \)-th neighborhood \( J \) of \((c_0, c_1, c_2)\) in \( \Gamma(c_0, c_1, c_2) \) is contained in \( \text{gcl}_{\Gamma}(\alpha)^{3M}(c_0, c_1, c_2) \). For every \( 0 \leq r \leq 2 \), denote the \( q_r \)-th neighborhood of \( c_r \) in \( \Gamma_r c_r \) by \( J_r \). Let \((b_0, b_1, b_2) \in J \). There exists \( \beta_0 \in \text{gcl}_{\Gamma_0}(\alpha_0)^M \) such that \( \beta_0 c_0 = b_0 \). Since \( \alpha_0 \in \Theta_{q}(A; q_1) \), \( \beta_0^{-1}b_1 \in J_1 \).

Thus, there exists \( \beta_1 \in \text{gcl}_{\Gamma_1}(\alpha_1)^M \) such that \( \beta_1 c_1 = \beta_0^{-1}b_1 \). Since \( \alpha_0, \alpha_1 \in \Theta_{q}(A; q_2) \), \( \beta_1^{-1}\beta_0^{-1}b_2 \in J_2 \). Thus, there exists \( \beta_2 \in \text{gcl}_{\Gamma_2}(\alpha_2)^M \) such that \( \beta_2 c_2 = \beta_1^{-1}\beta_0^{-1}b_2 \). It follows that \( \beta_0\beta_1\beta_2(c_0, c_1, c_2) = (b_0, b_1, b_2) \) and \( \beta_0\beta_1\beta_2 \in \text{gcl}_{\Gamma}(\alpha)^{3M} \).

\[ \Box \]

### A Bi-interpretability of \( A \) and \( \text{PSL}_n(A) \)

**Setting A.1.** \( n \geq 3 \) is an integer, \( A \) is an infinite integral domain of Krull dimension \( d < \infty \) which has trivial Jacobson radical and \( \text{PSL}_n(A) := \text{SL}_n(A)/\text{Z}(\text{SL}_n(A)) \).

1. For every \( q \vartriangleleft A \), \( \rho_q : \text{SL}_n(A) \to \text{SL}_n(A/q) \) is the quotient map, \( \text{SL}_n(A; q) := \ker \rho_q \) is the \( q \)-th congruence subgroup and \( \text{SL}_n^*(A; q) := \rho_q^{-1}(\text{Z}(\text{SL}_n(A/q))) \).

2. For every \( 1 \leq i \neq j \leq n \), \( a \in A \) and \( q \vartriangleleft A \), \( e_{i,j}(a) \in \text{SL}_n(A) \) is the matrix with 1 on the diagonal, a in the \((i, j)\)-entry and zero elsewhere, \( e_{i,j} := e_{i,j}(1), E_{i,j}(A) := \{ e_{i,j}(b) \mid b \in A \}, U(A) := E_{1,2}(A)E_{1,3}(A)\cdots E_{1,n}(A), E_{i,j}(A; q) := E_{i,j}(A) \cap \text{SL}_n(R; q) \) and \( U(A; q) := U(A) \cap \text{SL}_n(A; q) \). Finally, for every \( 1 \leq i \neq j \leq n \), let \( p_{i,j} \in \text{SL}_n(A) \) be a permutation matrix such that for every \( a \in A \), \( p_{i,j} e_{1,n}(a) p_{i,j}^{-1} = e_{i,j}(a) \).

3. \( \text{PSL}_n(A; q) \) and \( \text{PSL}_n^*(A; q) \) are the images in \( \text{PSL}_n(A) \) of \( \text{SL}_n(A; q) \) and \( \text{SL}_n^*(A; q) \) respectively. By abuse of notation, we denote by \( e_{i,j}(a), e_{i,j}, p_{i,j}, E_{i,j}(A), U(A), E_{i,j}(A; q) \) and \( U(A; q) \) the images of \( e_{i,j}(a), e_{i,j}, p_{i,j}, E_{i,j}(A), U(A), E_{i,j}(A; q) \) and \( U(A; q) \) in \( \text{PSL}_n(A) \).

**Lemma A.2.** Under Setting [A.1], let \( q \vartriangleleft A \) be a maximal ideal and let \( e_1, \ldots, e_n \) be the standard basis of \( A^n \). Let \( \beta \in \text{SL}_n(A) \) be such that \( \beta \) is
equivalent to \( e_{2,1} \) modulo \( q \). Then there exists \( \gamma \in \operatorname{SL}_n(A) \) which fixes the vectors \( e_1 \) and \( \beta e_1 \) and is equivalent to \( e_{1,3} \) modulo \( q \).

**Proof.** Let \( K \) be the field of fractions of \( A \). Denote \( e_1^* = \beta e_1 \) and for every \( 1 \leq i \neq 2 \leq n \), \( e_i^* := e_i \). Then \( e_1^* \), \ldots, \( e_n^* \) is a basis of \( K^n \). Let \( \delta \) be the matrix such that, for every \( 1 \leq i \leq n \), the \( i \)th column of \( \delta \) is \( e_i^* \). Then \( \delta \in M_n(A) \cap \operatorname{GL}_n(K) \) and \( \delta \) is equivalent to \( e_{1,2} \) modulo \( q \). Denote the \((2,2)\)-coordinate of \( \delta \) by \( a \). Then \( a \) is equivalent to 1 modulo \( q \) and \( \gamma := \delta e_{1,3}(a)^{-1} \in \operatorname{SL}_n(A) \) is the required matrix.

\[ \square \]

**Lemma A.3.** Under Setting \([A.1]\), if \( q \triangleleft A \) is a maximal ideal and \( \alpha \notin \operatorname{SL}_n(A; q) \) then \( \gcd_{\operatorname{SL}_n(A)}(\alpha)^{32} \cap U(A) \) is not contained in \( U(A; q) \).

**Proof.** By Gauss elimination, \( \operatorname{SL}_n(A) \) projects onto \( \operatorname{SL}_n(A/q) \). It is easy to see that, if \( F \) is a field and \( g \in \operatorname{SL}_n(F) \) in not-central, then \( e_{2,1} \in \gcd_{\operatorname{SL}_n(F)}(g)^8 \) (cf. the proof of Lemma 2.9 in [ALM]). Choose \( \beta \in \gcd_{\operatorname{SL}_n(A)}(\alpha)^8 \) such that \( \beta \) is equivalent to \( e_{2,1} \) modulo \( q \). Lemma A.2 implies that there exists \( \gamma \in \operatorname{SL}_n(A) \) that fixes \( e_1 \) and \( \beta e_1 \) and is equivalent to \( e_{1,3} \) modulo \( q \). Then \( \eta := [\beta, \gamma] := \beta^{-1} \gamma^{-1} \beta \gamma \in \gcd_{\operatorname{SL}_n(A)}(\alpha)^{16} \) fixes \( e_1 \) and is equivalent to \( e_{2,3} \) modulo \( q \). It follows that \([e_{1,2}, \eta] \in \gcd_{\operatorname{SL}_n(A)}(\alpha)^{32} \cap U(A) \) is equal to \( e_{1,3} \) modulo \( q \).

\[ \square \]

**Lemma A.4.** Under Setting \([A.1]\)

1. \( Z(\operatorname{Cent}_{\operatorname{PSL}_n(A)}(e_{1,n})) = E_{1,n}(A) \).
2. For every \( a, b \in A \), \( e_{1,n}(a)e_{1,n}(b) = e_{1,n}(a + b) \).
3. For every \( a, b \in A \), \([p_{1,n-1}e_{1,n}(a)p_{1,n-1}^{-1}, p_{n-1,n}e_{1,n}(b)p_{n-1,n}^{-1}] = e_{1,n}(ab) \).

In particular, \( \operatorname{PSL}_n(A) \) interprets the ring \( A \).

**Proof.** The proof consists of simple computations which are omitted.

\[ \square \]

**Lemma A.5.** Under Setting \([A.1]\). The collections \( \{U(A; q) \mid q \triangleleft A \text{ is maximal}\} \) and \( \{\operatorname{PSL}_n(A; q) \mid q \triangleleft A \text{ is maximal}\} \) are uniformly definable.

**Proof.** Lemma 1.5 of [AKNS] implies that \( \{q \triangleleft A \mid q \text{ is maximal}\} \) is uniformly definable in \( A \). Lemma A.4 implies that the family \( \{E_{1,n}(A; q) \mid q \triangleleft A \text{ is maximal}\} \) is uniformly definable in \( \operatorname{PSL}_n(A) \). For every ideal \( q \triangleleft A \),

\[
U(A; q) = \prod_{2 \leq j \leq n} E_{1,j}(A; q) = \prod_{2 \leq j \leq n} p_{1,j}E_{1,n}(A; q)p_{1,j}^{-1}
\]
so \( \{U(A; q) \mid q \triangleleft A \text{ is maximal} \} \) is uniformly definable. Lemma \[3\] implies that for every maximal ideal \( q \triangleleft A, \alpha \in \text{PSL}_n^*(A; q) \) if and only if \( \text{gcl}_{\text{PSL}_n(A)}(\alpha)^{32} \cap U(A) \subseteq U(A; q) \). Thus, \( \{\text{PSL}_n^*(A; q) \mid q \triangleleft A \text{ is maximal} \} \) is uniformly definable.

\[\Box\]

**Theorem A.6.** Under Setting \[4\], \( A \) and \( \text{PSL}_n(A) \) are bi-interpretable.

**Proof.** Denote \( E = E_{1,n}(A) \) and let \( \mathcal{E} = (E, e) \) be the interpretation of \( A \) in \( \text{PSL}_n(A) \) given by Lemma \[4\]. Let \( \mathcal{J} = (S, s) \) be the standard interpretation of \( \text{PSL}_n(A) \) in \( A \) (i.e. as \( n \times n \) matrices with determinant 1, up to scalars).

Viewing \( \text{PSL}_n(A) \) as an imaginary in \( \text{SL}_n(A) \), we get that \( \mathcal{P} = (\text{PSL}_n(A), \text{Id}) \) is an interpretation of \( \text{PSL}_n(A) \) in \( \text{SL}_n(A) \) and \( \mathcal{C} = (C, c) := \mathcal{P} \circ \mathcal{J} \) is an interpretation of \( \text{PSL}_n(A) \) in \( A \). It is easy to see that \( \mathcal{E} \circ \mathcal{C} \) is trivial. Therefore, in order to show that \( A \) and \( \text{PSL}_n(A) \) are bi-interpretable, it is enough to show that \( \mathcal{D} = (D, d) := \mathcal{C} \circ \mathcal{E} \) is trivial.

By construction, the restriction of \( d^{-1} \) to \( E_{1,n}(A) \) is definable. Therefore, the restriction of \( d^{-1} \) to \( V := \prod_{1 \leq j \leq n} \prod_{1 \leq i \neq j \leq n} p_{i,j} E_{1,n}(A) p_{i,j}^{-1} \) is definable. By Gauss elimination, there is a constant \( C \) such that, for every maximal ideal \( q \), \( V^C \) projects onto \( \text{PSL}_n(A) / \text{PSL}_n^*(A; q) \cong \text{PSL}_n(A;q) \).

Lemma \[5\] implies that there are definable sets \( I, J, X \subseteq I \times \text{PSL}_n(A) \) and \( Y \subseteq J \times D \) such that \( \{X_i \mid i \in I\} = \{\text{PSL}_n^*(A; q) \mid q \triangleleft A \text{ is maximal} \} \) and \( \{Y_j \mid j \in J\} = \{d^{-1}(X_i) \mid i \in I\} \). We claim that there exists a definable \( Z \subseteq I \times J \) such that \( (i, j) \in Z \) if and only if \( Y_j = d^{-1}(X_i) \).

Indeed, \( d^{-1} \) is definable on \( U(A) \subseteq V \) and \( Y_j = d^{-1}(X_i) \) if and only if \( Y_j \cap d^{-1}(U(A)) = d^{-1}(X_i \cap U(A)) \).

Finally, \( d^{-1} \) is definable since for every \( \alpha \in \text{PSL}_n(A) \) and \( \delta \in D \), \( d^{-1}(\alpha) = \delta \) if and only if for every \( (i, j) \in Z \), there exists \( \nu \in V \) such that \( \alpha X_i = \nu X_i \) and \( \delta Y_j = d^{-1}(\nu) Y_j \).

\[\Box\]

**References**

[AKNS] M. Aschenbrenner, A. Khelif, E. Naziazeno and T. Scanlon, *The logical complexity of finitely generated commutative rings*. Int. Math. Res. Not. IMRN 2020, no. 1, 112–166.

[ALM] N. Avni, A. Lubotzky and C. Meiri *First order rigidity of non-uniform higher rank arithmetic groups*. Invent. Math. 217 (2019), no. 1, 219–240.
[AM] N. Avni and C. Meiri, *Words have bounded width in SL(n, Z)*. Compos. Math. 155 (2019), no. 7, 1245–1258.

[BBF] M. Bestvina, K. Bromberg, K. Fujiwara, *The verbal width of acylindrically hyperbolic groups*. Algebr. Geom. Topol. 19 (2019), no. 1, 477–489.

[BT65] A. Borel, J. Tits, *Groupes réductifs*. Inst. Hautes Etudes Sci. Publ. Math. No. 27 (1965), 55–150.

[BGT] E. Breuillard, B. Green and T. Tao, *Approximate subgroups of linear groups*. Geom. Funct. Anal. 21 (2011), no. 4, 774–819.

[Cas] J. W. S. Cassels, *Rational quadratic forms*. London Mathematical Society Monographs, 13. Academic Press, Inc. 1978.

[Khe] A. Khelif, *Bi-interprétabilité et structures QFA: étude de groupes résolubles et des anneaux commutatifs*, C. R. Math. Acad. Sci. Paris 345 (2007), no. 2, 59–61.

[KM1] O. Kharlampovich and A. Myasnikov, *Elementary theory of free non-abelian groups*. J. Algebra 302 (2006), no. 2, 451–552.

[KM2] O. Kharlampovich and A. Myasnikov, *Definable sets in a hyperbolic group*. Internat. J. Algebra Comput. 23 (2013), no. 1, 91–110.

[KM3] O. Kharlampovich and A. Myasnikov, *Decidability of the Elementary Theory of a Torsion-Free Hyperbolic Group*. [arXiv:1303.0760](https://arxiv.org/abs/1303.0760).

[Kne] M. Kneser, *Normalteiler ganzzahliger Spingruppen*. (German) J. Reine Angew. Math. 311(312) (1979), 191–214.

[Las1] C. Lasserre, *Polycyclic-by-finite groups and first-order sentences* J. Algebra 396 (2013), 18–38.

[Las2] C. Lasserre, *R. J. Thompsons groups F and T are bi-interpretable with the ring of the integers*. J. Symbolic Logic 79 (2014), no. 3, 693–711.

[LM] A. Lubotzky and C. Meiri, *Sieve methods in group theory I: Powers in linear groups*. J. Amer. Math. Soc. 25 (2012), no. 4, 11191148.
[Mar] G.A. Margulis, *Discrete Subgroups of Semisimple Lie Groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 17. Springer-Verlag, Berlin, 1991.

[MM] M. Sohrabi and A. Myasnikov, *Bi-interpretability with Z and models of the complete elementary theories of SLₙ(O), Tₙ(O) and GLₙ(O), n ≥ 3*. arXiv:2004.03585.

[Nie1] A. Nies. *Separating classes of groups by first-order sentences*. Intern. J. Algebra Comput. 13 (2003), 287–302.

[Nie2] A. Nies. *Comparing quasi-finitely axiomatizable and prime groups*. J. Group Theory 10 (2007), no. 3, 347–361.

[Nie3] A. Nies. *Describing groups*. Bull. Symbolic Logic 13 (2007), no. 3, 305–339.

[Nos] G.A. Noskov, *The elementary theory of a finitely generated almost solvable group*. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 47 (1983), no. 3, 498–517.

[OS] F. Oger and G. Sabbagh, *Quasi-finitely axiomatizable nilpotent groups*. J. Group Theory 9 (2006), no. 1, 95–106.

[PR] V. Platonov and A. Rapinchuk, *Andrei Algebraic groups and number theory*. Translated from the 1991 Russian original by Rachel Rowen. Pure and Applied Mathematics, 139. Academic Press, Inc., Boston, MA, 1994. xii+614 pp.

[PS] L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type*. J. Amer. Math. Soc. 29 (2016), no. 1, 95–146.

[Rag] M. S. Raghunathan, *On the congruence subgroup problem*. Inst. Hautes Etudes Sci. Publ. Math. No. 46 (1976), 107–161.

[Rob1] J. Robinson, *Definability and decision problems in arithmetic*. J. Symbolic Logic 14 (1949), 98–114.

[Rob2] J, Robinson, *The undecidability of algebraic rings and fields*. Proc. Amer. Math. Soc. 10 (1959), 950–957.
[Seg] D. Segal, *Words: notes on verbal width in groups*. London Mathematical Society Lecture Note Series, 361. Cambridge University Press, Cambridge, 2009. xii+121 pp.

[Sel1] Z. Sela, *Diophantine geometry over groups and the elementary theory of free and hyperbolic groups*. Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), 87–92, Higher Ed. Press, Beijing, 2002.

[Sel2] Z. Sela, *Diophantine geometry over groups. VII. The elementary theory of a hyperbolic group*. Proc. Lond. Math. Soc. (3) 99 (2009), no. 1, 217–273.

[Sha] A. Shalev, *Some results and problems in the theory of word maps*. Erdős centennial, 611–649, Bolyai Soc. Math. Stud., 25, Jňos Bolyai Math. Soc., Budapest, 2013.

[SGA3] Schemas en groupes (SGA 3). Tome III. Structure des schemas en groupes reductifs. Seminaire de Geometrie Algebrique du Bois Marie 1962–64. Documents Mathematiques (Paris), 8. Societe Mathematique de France, Paris, 2011.

[SGA4\frac{1}{2}] P. Deligne, *Cohomologie etale*. Seminaire de geometrie algebrique du Bois-Marie SGA 4\frac{1}{2}. Lecture Notes in Mathematics, 569. Springer-Verlag, Berlin, 1977.

[Sm] P. Smith, *An introduction to Gödel’s theorems*. Second edition. Cambridge Introductions to Philosophy. Cambridge University Press, Cambridge, 2013. xvi+388 pp.

[ST] D. Segal and K. Tent, *Defining R and G(R)*. [arXiv:2004.13407](https://arxiv.org/abs/2004.13407).

[VW] L. Vaserstein, E. Wheland, *Products of conjugacy classes of two by two matrices*. Linear Algebra Appl. 230 (1995), 165–188.