האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

The Faculty of Mathematics and Natural Science
the Einstein Institute of Mathematics

Generators for Finite Index Subgroups of $\mathrm{SL}_n(\mathcal{O}_k)$

יוצרים לתת-חבורות מאינדקס סופי של $\mathrm{SL}_n(\mathcal{O}_k)$

By

Amitai Assayag

Supervised by

Prof. Alex Lubotzky

A thesis submitted in partial fulfillment for the requirements for the degree of Master of Science

November 2019
חשוון תש״פ

Acknowledgments

I like to thank my beloved Linoy, who supplied all the love and faith I needed to complete this work. Thanks to my family, for the love and support. And thanks to my adviser Prof. Alex Lubotzky, for giving me a glimpse into his incredible mathematical world.

תקציר

לחבורה G, נגדיר את $r\left(G\right)$ להיות מספר היוצרים המינימלי שניתן למצוא בכל תת-חבורה מאינדקס סופי של G, כך שהם יוצרים תת-חבורה מאינדקס סופי. לחסימת $r\left(G\right)$ יש שימוש רב בחבורות דיסקרטיות, פרו-סופיות וחבורות-p [LM87a][Lub86] . בנוסף, דרכי מציאת היוצרים לחסימת $r\left(G\right)$, עוזרות להבין אילו איברים יצרו חבורות מאינדקס סופי. מידע זה שימושי למציאת חבורות דקות[Mei17]. חבורה דקה של חבורה אלגברית G פשוטה למחצה מעל הממשיים, הינה תת חבורה דיסקרטית צפופה זריצקי ב$G\left(\mathbb{R}\right)$, עם קו-נפח אינסופי.
נעשו הצלחות רבות בחסימת $r\left(G\right)$ בחבורות מסויימות, לובוצקי ומן הוכיחו כי לחוג השלמים ה-p-אדיים $\mathbb{Z}_p$, מתקיים $r\left(\mathrm{SL}_n\left(\mathbb{Z}_p\right)\right)=2$ [LM87b] . לובוצקי שאל את השאלה הבאה [Lub86] .

בעיה האם לכל $n\geq 3$ מתקיים $r\left(\mathrm{SL}_n\left(\mathbb{Z}\right)\right)=2$?

בעקבות שאלה זו, לונג ורייד הוכיחו זאת עבור $n=3$ [LR11] , ולאחרונה מאירי נתן תשובה חיובית לשאלה זו[Mei17]. כמו כן, ואנקטארמנה ושרמה הוכיחו עבור חבורה אלגברית מעל הרציונאלים G, קשירה ופשוטה למחצה, ללא תתי-חבורות אלגבריות קשירות ונורמליות מעל הרציונאלים ומדרגה ממשית גדולה מ 2. אזי, לכל תת-חבורה מאינדקס סופי של $G\left(\mathbb{Z}\right)$, שיש לה מרחב מנה לא קומפקטי מעל $G\left(\mathbb{R}\right)$, יש שלושה יוצרים לחבורה מאינדקס סופי [SV05] . באותו מאמר הם הוכיחו גם כי עבור שדה מספרים k ועבור $n\geq 3$ מתקיים $r\left(\mathrm{SL}_n\left(\mathcal{O}_k\right)\right)\leq 3$, כש$\mathcal{O}_k$ הוא אוסף השלמים האלגבריים בk.
לובוצקי הציג בפני את השאלה הבאה.

בעיה האם לכל חבורת שבליי מדרגה גבוהה, מתקיים $r\left(G\left(\mathbb{Z}\right)\right)=2$?

שאלה זו עדיין פתוחה , אך התוצאות שהוזכרו נותנות אינדקציה טובה לתשובה חיובית. במאמר זה היני מציג הוכחה לטענה הבאה. עבור α שלם אלגברי כלשהו ו$k=\mathbb{Q}\left(\alpha\right)$, מתקיים $r\left(\mathrm{SL}_n\left(\mathcal{O}_k\right)\right)\leq 3$ לכל $n\geq 3$. תוצאה זו אינה חידוש כפי שהוזכר, אך ההוכחה שונה מזו שהוצגה ע"י ואנקטארמנה ושרמה, והיא מתבססת על עבודתו של מאירי שמשתמשת בתכונות המבנה של SL_n.

בעבודה זו אני מציג חלק מהרכבן ותכונתן של חבורות שבליי, כמו כן אציג ואראה כמה תכונות בתחום השלמים האלגברים ותחום המטריצות. בשני החלקים האחרונים אראה איך תכונות אלו באות לידי ביטוי בSL_n, ואיך השימוש בהן גורר את הטענה המרכזית.

Contents

1 Introduction

For a group G we denote $r(G)$ to be the smallest integer such that for every finite index subgroup H of G, H has a subgroup of finite index generated by $r(G)$ elements. The attempt to bound $r(G)$ for certain algebraic groups has been very successful over the years. Lubotzky presented the following problem

Problem 1.1. [Lub86]For $n \geq 3$, does $r(\mathrm{SL}_n(\mathbb{Z})) = 2$?

This is not true when $n = 2$, since $\mathrm{SL}_2(\mathbb{Z})$ contains a finite index non-abelian free subgroup. A positive answer to this problem has been given for the case $n = 3$ by Long and Reid[LR11]. More recently, a positive answer to Problem 1.1 has been given by Meiri[Mei17]. Lubotzky and Mann proved in [LM87b], that for the p-adic integers $\mathbb{Z}_p$, $r(\mathrm{SL}_n(\mathbb{Z}_p)) = 2$. This result gave a good indication for a positive answer for Lubotzky's problem. Another indication has been given by Sharma and Venkataramana in [SV05]. They showed that for G, a connected semi-simple algebraic group over $\mathbb{Q}$, when G has no connected normal algebraic subgroups defined over $\mathbb{Q}$ and that $\mathrm{rank}_{\mathbb{R}}(G) \geq 2$, $r(G(\mathbb{Z})) \leq 3$ (when we restrict the finite index subgroups to have non compact quotient space over $G(\mathbb{R})$). In their paper they also showed that for any number field k and $n \geq 3$, that $r(\mathrm{SL}_n(\mathcal{O}_k)) \leq 3$.

I researched a generalized problem of Problem 1.1, presented to me by Lubotzky

Problem 1.2. For a Chevalley group G of high rank, does $r(G(\mathbb{Z})) = 2$?

This question is yet to be answered, but it has strong indications that the answer is positive, especially for the universal Chevalley groups. The conclusion from the main theorem of this paper (Theorem 6.2), is that for α an integral element over $\mathbb{Z}$, $k = \mathbb{Q}(\alpha)$ and $n \geq 3$, $r(\mathrm{SL}_n(\mathcal{O}_k)) \leq 3$. As mentioned this result is not new, but the proof is different then Sharma and Venkataramana's and based on Meiri's work, utilizing the more specific structure of SL_n.

1.1 Motivation

In the study of discrete groups and pro-finite groups, the bound on $r(G)$, bounds other functions on G and functions on groups derived from G. In the field of powerful groups, this bound has connections to a conjecture by Jones and Wiegold[Lub86, LM87a]. Another motivation for this problem derived from the study of the construction of thin groups, which are discrete Zariski-dense subgroups of $G(\mathbb{R})$ that have infinite covolume. There is not much known about the algebraic structure of thin groups and it seems difficult to construct new types of them. By understanding in what conditions, small number of elements creates Zariski-dense subgroups of $G(\mathbb{R})$ that has finite covolume, we might be able to find elements to create new thin group types[Mei17].

1.2 Organization

In Sections 2 and 4, I present definitions and results regarding certain algebraic groups. Sections 3 and 5 present relative subjects in ring theory and matrix theory respectively. Section 6, focuses on implementing the previous sections to SL_n, the main result is in Subsection 6.2.

2 Chevalley Groups

In the past, defining and classifying families of simple groups was done mainly by careful consideration of simple complex Lie groups and root systems. But many groups, which were known to exist from an association to a Lie algebra or root system, failed to admit a simple definition. Despite the fact that algebraic groups can be considered as subgroups of GL_n satisfying some polynomial conditions, those conditions where hard to find. In 1995 Chevalley introduced in a ground-breaking paper[Che55], a method of constructing and defining such groups. This method can construct groups above arbitrary fields, including finite ones. In this section I will provide some background about the construction, build and properties of the Chevalley groups. I'll be writing about the Chevalley groups in the broadened general version treated by Steinberg [Ste67].

2.1 Construction

Let $\mathcal{L}$ be a semi-simple Lie algebra over $\mathbb{C}$ and let $\mathcal{H}$ be its Cartan subalgebra, then we can write $\mathcal{L} = \mathcal{H} \bigoplus_{\alpha\neq 0} \mathcal{L}_\alpha$ where $\alpha \in \mathcal{H}^*$ and

$$\mathcal{L}_\alpha = \{X \in \mathcal{L} | [H, X] = \alpha(H)X, \forall H{\in}\mathcal{H}\}.$$

The α's are linear functions on $\mathcal{H}$ called roots and generate $\mathcal{H}^*$ as a vector space over $\mathbb{C}$, every $\mathcal{L}_\alpha$ for $\alpha \neq 0$ has dimension 1. Denote the collection of all roots by Σ, then Σ is a root system in the vector space over $\mathbb{Q}$ generated by the roots marked as $\mathcal{H}^*_{\mathbb{Q}}$. Σ is irreducible if and only if $\mathcal{L}$ is simple[Hal15, Theorem 7.35]. Let $\{\alpha_1, \dots, \alpha_n\} \subset \Sigma$ be a system of simple roots and let $\{H_{\alpha_i}, X_\alpha | \alpha \in \Sigma, 1 \leq i \leq n\}$ be a Chevalley basis of the algebra $\mathcal{L}$. We denote $\mathcal{U}_{\mathbb{Z}}$ to be the $\mathbb{Z}$-algebra generated by all $X_\alpha^m/m!$ for $m \in Z^+; \alpha \in \Sigma$, $\mathcal{U}_{\mathbb{Z}}$ is called Kostant's $\mathbb{Z}$-form [Kos09].

Lemma 2.1. *[Ste67, p.16]Every finite-dimensional $\mathcal{L}$-module V contains a lattice M invariant under all $X_\alpha^m/m!$ for $m \in Z^+; \alpha \in \Sigma$ i.e., M is invariant under $\mathcal{U}_{\mathbb{Z}}$.*

Let φ be a faithful representation of the Lie algebra $\mathcal{L}$ in a finite-dimensional vector space V, from Lemma 2.1 V contains a lattice M invariant under all $\varphi(X_\alpha)^m/m!$ for $m \in Z^+; \alpha \in \Sigma$. For k an arbitrary field we denote $V^k = M \otimes_{\mathbb{Z}} k$, and for $\alpha \in \Sigma$, we define homomorphisms $x_\alpha : k^+ \to \mathrm{GL}(V^k)$ of the additive group k^+ of k into GL(V^k) by

$$x_\alpha(t) = exp(t\varphi(X_\alpha)) := \sum_{m=0}^{\infty} t^m \varphi(X_\alpha)^m / m!$$

and mark $\mathfrak{X}_\alpha$ as the group $\{x_\alpha(t) | t \in k\}$ ($x_\alpha(t)$ is additive in t), $\mathfrak{X}_\alpha$ is the root subgroup of α.

Definition 2.1. The subgroup of GL(V^k) generated by all $\mathfrak{X}_\alpha$, $\alpha \in \Sigma$ is the Chevalley group $G(k)$ related to the Lie algebra $\mathcal{L}$, the representation φ and the field k.

When the representation φ is the adjoint representation, the related Chevalley groups are those defined by Chevalley in 1955 [Che55].

2.2 Subgroups

2.2.1 Weyl Group

Definition 2.2. For each root $\alpha \in \Sigma$, let s_α denote the reflection about the hyperplane perpendicular to α in $\mathcal{H}^*_{\mathbb{Q}}$, the subgroup W of the orthogonal group $\mathrm{O}(\mathcal{H}^*_{\mathbb{Q}})$ generated by all s_α ($\alpha \in \Sigma$), is called the Weyl group of Σ. For every α_i ($1 \leq i \leq n$) the reflection s_{α_i} is called a simple reflection, the simple reflections creates W [Hal15, Proposition 8.24].

Remark 2.1. By the definition of a root system, each s_α preserves Σ , from which it follows that W is a finite group.

Definition 2.3. For every $\alpha \in \Sigma$ there are unique $a_i \in \mathbb{Z}, 1 \leq i \leq n$, in which the nonzero coefficients are either all positive or all negative, such that $\alpha = \sum_{i=1}^n a_i\alpha_i$, we define the height of α to be $ht(\alpha) := \sum_{i=1}^n a_i$.

Remark 2.2. When Σ is a irreducible root system there is a unique root with maximal height called the highest root [Hum90, p.40]. There are only nine classification types for irreducible root systems (and so, simple complex Lie algebras), $A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4$ and G_2.

Each element w in W has a length which is defined by the length of the shortest multiplication of simple reflections that creates w. The Weyl groups are a type of finite Coxeter groups which are groups that have a presentation in terms of reflections. In every finite Coxeter group there is a unique element w_0 with maximal length, w_0 has order 2 and $w_0 P = -P$ where $P \subset \Sigma$ is the set containing all positive roots [Hum90, p.15-16]. The elements created by product of all simple reflections in W are called Coxeter elements, different orderings produce conjugate elements, which have the same order. The order of the Coxeter elements h is called the Coxeter number. The Coxeter number can be calculated by $h = \frac{2|P|}{n}$, or when Σ is irreducible and h' is the height of the highest root, we have $h = h' + 1$ [Hum90, p.79,84]. When h is even there is a unique Coxeter element w such that $w_0 = w^{h/2}$.

Example 2.1. For the irreducible root system of type A_{n-1} the Weyl group is isomorphic to the symmetric group S_n, the Coxeter number is equal to n and the permutation $(12)(23)...((n-1)n) = (12...n)$ is a Coxeter element. For an even n the permutation $(246...(n-2)n(n-1)(n-3)...31)$ is the Coxeter element w for which $w^{n/2} = w_0 = (1n)(2(n-1))...\left(\frac{n}{2}\left(\frac{n}{2}+1\right)\right)$.

2.2.2 Borel and Cartan Subgroups

Proposition 2.1. *[Ste67, p.29]Let $U^+ = \mathfrak{X}_P := \langle \mathfrak{X}_\alpha | \alpha \in P\rangle$ then:*

(a) $U^+ = \prod \mathfrak{X}_\alpha$ with uniqueness of expression, where the product is taken over all $\alpha \in P$ arranged in any fixed order.

(b) U^+ is unipotent and is superdiagonal relative to an appropriate choice of basis for V^k. Similarly, $U^- = \mathfrak{X}_{-P}$ is unipotent and subdiagonal relative to the same choice of basis.

Remark 2.3. For every $\alpha, \beta \in \Sigma$ and $t, u \in k$ we have the following relations presented by Steinberg which are independent of the representation space chosen for G [Ste67, p.23]:

($R1$) $(x_\alpha(t), x_\beta(u)) = \prod x_{i\alpha+j\beta}\left(c_{i,j}t^iu^j\right)$ where the product is taken over all roots $i\alpha + j\beta \in \Sigma, i, j \in \mathbb{Z}^+$ arranged in some fixed but arbitrary order, and the $c_{i,j}$s are unique integers depending on α, β, and the chosen ordering, but not on t or u.

($R2$) $w_\alpha(t) := x_\alpha(t)x_{-\alpha}\left(-t^{-1}\right)x_\alpha(t), w_\alpha := w_\alpha(1)$.

($R3$) $w_\alpha x_\beta(t) w_\alpha^{-1} = x_{s_\alpha\beta}(ct)$ where $c = c(\alpha, \beta) = \pm 1$ is independent of t and k. s_α is the reflection in the Weyl group.

($R4$) $h_\alpha(t) := w_\alpha(t) w_\alpha(1)^{-1}$.

Corollary 2.1. *[Ste67, p.24]Let N be the group generated by all $w_\alpha(t)$, H be the subgroup generated by all $h_\alpha(t)$ and B be the group generated by U^+ and H. Then:*

(a) U^+ is normal in B and $B = U^+H$.

(b) H is abelian and normal in N.

(c) If $|k| > 3$, N is the normalizer in G of H.

(d) There exists an epimorphism $\varphi : W \longrightarrow N/H$ such that $\varphi(s_\alpha) = Hw_\alpha(t)$ for all roots α.

Remark 2.4. From relation ($R1$) and Corollary 2.1, when α is a root with maximal height, $\mathfrak{X}_\alpha$ is normal in U^+. Under the same base of Proposition 2.1(b) H is diagonal and $\mathfrak{X}_\alpha$ is normal in B.

Theorem 2.1. *[Ste67, Theorem 6]If k is an algebraically closed field, k_0 is the prime subfield and M is the lattice as in Proposition 2.1 used to define G, then:*

(a) G is a semisimple algebraic group relative to M.

(b) B is a maximal connected solvable subgroup.

(c) H is a maximal connected group and diagonalizable under the same base as in Proposition 2.1(b).

(d) φ as defined in Corollary 2.1 is an isomorphism.

(e) $G, B, H,$ and N are defined over k_0 relative to M.

Remark 2.5. The groups B and N form a BN pair as defined by J. Tits [Tit64, Definition 2.1].

A maximal connected solvable closed subgroup of an algebraic group, is called a Borel subgroup, and a maximal connected abelian subgroup of an algebraic groups, is called a Cartan subgroup and is usually defined as the centralizer of a maximal torus. When k is an algebraically closed field, B and H are a Borel subgroup and a Cartan subgroup of G respectively. In this case there is a single conjugacy class of Borel subgroups and a single conjugacy class of Cartan subgroups.

Definition 2.4. A proper subgroup $P \subset G$ is called a parabolic subgroup if it contains some Borel subgroup of G. The unipotent radical of such P is a horospherical subgroup U of G. The Lie algebra $\mathfrak{u}$ of U is called a horospherical subalgebra and the Lie algebra $\mathfrak{p}$ of P is called a parabolic subalgebra. An opposite horospherical subgroup of U is a horospherical subgroup U^- of G, such that the algebra $\mathcal{L} = \mathfrak{p} \oplus \mathfrak{u}^-$. The opposite horospherical subgroup U^- always exist.

Example 2.2. U^+, U^- are a pair of opposite horospherical subgroups of G.

2.3 Bruhat Decomposition

Throughout this paper, for $n \in N$ that represents $w \in W$ under $\varphi : W \longrightarrow N/H$, I will write wB (Bw) in place of nB (Bn).

Theorem 2.2. *(Bruhat decomposition)*

(a) $\bigcup_{w \in W} BwB = G$, BwB is called the Bruhat cell of w.

(b) If k is algebraically closed the union is disjoint.

Remark 2.6. From the Bruhat decomposition, many questions about G can be reduce to questions about W and B.

Theorem 2.3. *[Ste67, Theorem 4']Let $w \in W$ let n_w be a representative of w in N, and set $Q_w = P \bigcap w^{-1}(-P)$ (P denotes the set of positive roots). Then $BwB = Bn_w\mathfrak{X}_{Q_w}$ with uniqueness of expression on the right.*

Example 2.3. For the orthogonal algebra $\mathcal{L} = \mathfrak{so}_{2n}(\mathbb{C})$, which is the Lie algebra consisting of the matrices $\left\{X \in Mat_{2n}(\mathbb{C}) | X^T J_{2n} + J_{2n} X = 0\right\}$, where J_n is the n-by-n matrix with one on the anti-diagonal and zero elsewhere. The indexing of the rows and columns of our matrices from top to bottom and left to right is by $1, \ldots, n, -n, \ldots, -1$. The root system is of type D_n, the roots are denoted by $\alpha_{\pm_1 i, \pm_2 j} = \pm_1 e_i \pm_2 e_j, (1 \leq i < j \leq n)$, the positive roots are $\alpha_{i \pm j} = e_i \pm e_j$ for $(1 \leq i < j \leq n)$. For a certain representation we have $G = \mathrm{SO}_{2n}(\mathbb{C}) = \left\{X \in \mathrm{SL}_{2n}(\mathbb{C}) | X^T J_{2n} X = J_{2n}\right\}$. The root elements $x_{\alpha_{i,j}}(t); (-n \leq i, j \leq n)$ in G correspond to the matrices $e_{i,j}(t) = Id + \widetilde{e}_{i,-j}(t) - \widetilde{e}_{j,-i}(t)$, where $\widetilde{e}_{i,j}(t)$ has t at the (i,j) entry and zeros elsewhere. B can be chosen to be the superdiagonal matrices in G, representative for elements of W in G consists of all permutations and an even number sign changes in n coordinates. So for $w \in W$ matching the permutation $((n-1) \ldots 1 (1-n) \ldots (-1))(n(-n))$, which is a Coxeter element, we have $Q_w = \{\alpha_{1,n}, \alpha_{1,-i} | 2 \leq i \leq n\}$, so every element $g \in BwB$ can be written as $g = bp_w e_{1,n}(t_{1,n}) \prod_{i=2}^{n} e_{1,-i}(t_{1,-i})$, where p_w is a permutation matrix representing w.

2.4 Representation Spaces and Properties

Definition 2.5. Let V be a representation space for $\mathcal{L}$, a vector $v \in V$ is a weight vector if there is a linear functional λ on $\mathcal{H}$ such that $Hv = \lambda(H) v$ for all $H \in \mathcal{H}$. If such a $v \neq 0$ exists, we call the corresponding λ a weight of the representation.

Lemma 2.2. *[Ste67, Lemma 27]Let V be a representation space for $\mathcal{L}$.*

(a) The additive group generated by all the weights of all representations forms a lattice L_1.

(b) The additive group generated by all roots is a sublattice L_0 of L_1.

(c) The additive group generated by all weights of a faithful representation on V forms a lattice L_V between L_0 and L_1.

All lattices between L_0 and L_1 can be realized as in Lemma 2.2(c) by an appropriate choice of V. For example, $L_V = L_0$ if V corresponds to the adjoint representation. The Chevalley groups G_0 and G_1 corresponding to the lattices L_0 and L_1, are called the adjoint group and the universal group respectively. The property of the nesting lattices can be expanded to a property of the Chevalley groups in the following way.

Corollary 2.2. *[Ste67, p.30]If G, G' are Chevalley groups constructed from the same $\mathcal{L}$ and k but using V' for G' in place of V, such that $L_V \subseteq L_{V'}$. Then there exists a homomorphism $\phi : G' \to G$ such that $\phi(x'_\alpha(t)) = x_\alpha(t)$ for all α, t and $ker\phi \subseteq Z(G')$. If $L_V = L_{V'}$ then ϕ is an isomorphism.*

Remark 2.7. This gives us a useful tool to go between types of Chevalley groups. The center $Z(G)$, is finite and when G is the adjoint group, $Z(G) = \{1\}$. When $\mathcal{L}$ is simple, ${}^{G}\!/_{Z(G)}$ is simple, so G is almost simple.

Lemma 2.3. *[Ste67, Lemma 32']Assume $\mathcal{L}$ is simple and $|k| > 3$, then $[G, G] = G$.*

Remark 2.8. If $k = \mathbb{C}$ then G has the structure of a complex Lie group, and all the preceding statements have natural modifications in the language of Lie groups.

Theorem 2.4. *[Ste67, Theorem 13]If G is a universal Chevalley group over $\mathbb{C}$ viewed as a Lie group, then G is simply connected.*

Example 2.4. $\mathrm{SL}_n(\mathbb{C})$, $\mathrm{Sp}_n(\mathbb{C})$, and $\mathrm{Spin}_n(\mathbb{C})$ are simply connected. These cases can also be proved by induction on n. [Che46, Chapter II]

3 The Ring of S-Integers

In this section I will introduce some information regarding a finitely-generated $\mathbb{Z}$-module, the ring of S-integers over certain fields.

Definition 3.1. Let k be an algebraic number field, an integral element is a root of a monic polynomial with integer coefficients. The ring of integers of k is the ring of all integral elements contained in k, is denoted by $\mathcal{O}_k$.

Let S_∞ be the set of all archimedean valuations of an algebraic number field k, let S be a finite set of absolute values of k containing S_∞. The ring $\mathcal{O}_S := \{x \in k | v(x) \geq 0 \text{ for every valuation } v \notin S\}$ is the ring of S-integers of k and $\mathcal{O}_{S_\infty} = \mathcal{O}_k$.[RP94, p.11]

Theorem 3.1. *Let α be an integral element over $\mathbb{Z}$ and $k = \mathbb{Q}(\alpha)$, then for every $(0) \neq I \lhd \mathbb{Z}[\alpha]$ there is an ideal $(0) \neq J \lhd \mathcal{O}_k$ such that $J \subset I$.*

Proof. First we claim that $I \cap \mathbb{Z} \neq \{0\}$, let $0 \neq \beta \in I$ it is integral so there is a monic polynomial $p(x) = x^r + a_{r-1}x^{r-1} + \ldots + a_0 \in \mathbb{Z}[x]$ and $a_0 \neq 0$ such $p(\beta) = 0$. $a_0 = -\left(\beta^{r-1} + a_{r-1}\beta^{r-2} + \ldots + a_1\right)\beta \in I$ because I is an ideal. Now it is known that there is a $\mathbb{Z}$ basis for $\mathcal{O}_k$, $\omega_1, \ldots, \omega_n \in \mathcal{O}_k \setminus \{0\}$, such $\mathcal{O}_k = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$. For every $1 \leq i \leq n$ there are $p_i, q_i \in \mathbb{Z}[\alpha] \setminus \{0\}$ such $\omega_i = \frac{p_i}{q_i}$ since $\mathcal{O}_k \subset k = \mathbb{Q}(\alpha)$. We mark $q = \prod_{i=1}^{n} q_i$ and let $0 \neq a \in \mathbb{Z} \cap I$ so $q\omega_i \in \mathbb{Z}[\alpha] \subset \mathcal{O}_k$. From I being an ideal we have $q\omega_i a \in I$ for every $1 \leq i \leq n$ and so if we denote $h := aq \in \mathbb{Z}[\alpha]$ we get $h\mathbb{Z}\omega_i \subset I$. Since I closed under the sum operator we have $I \supset J := h\sum_{i=1}^{n} \mathbb{Z}\omega_i = h\mathcal{O}_k$ and J is a non zero ideal of $\mathcal{O}_k$. □

4 Finite Index Subgroups

Let k be some field and let G be a connected k-algebraic group with a faithful k-representation of G in some $\mathrm{GL}_n(k)$. We identify G with its image under this representation. For any ring $R \subset k$ and subgroup $H \leq G$, we define $H(R) := H \cap \mathrm{GL}_n(R)$. More generally for an ideal $I \lhd R$, we set

$$H(I) = \{x \in H(R) | x \equiv Id \pmod{I}\}. \tag{4.1}$$

Notice that $H(I)$ is the kernel of the projection $\Pi : H(R) \to H\left({}^{R}\!/_{I}\right)$.

4.1 Zariski Density of Finite Index Subgroups

In this subsection, let $\mathcal{L}$ be a simple complex Lie algebra and let G be the Chevalley group related to $\mathcal{L}$, $\mathbb{C}$, and some representation. Also let α be an integral element over $\mathbb{Z}$ and $k := \mathbb{Q}(\alpha)$. The purpose of this section is to give a quick explanation for the following proposition.

Proposition 4.1. *Every finite index subgroup of $G(\mathcal{O}_k)$ is Zariski dense in G.*

Remark 4.1. For every finite index subgroup H of $G(\mathcal{O}_k)$, $H \cap G(\mathbb{Z})$ has a finite index in $G(\mathbb{Z})$, so it's enough to prove Proposition 4.1 for $G(\mathbb{Z})$.

Theorem 4.1. *[BHC61, Theorem 1]Let G be a connected complex algebraic group defined over $\mathbb{Q}$. Then there exists an open set U in $G(\mathbb{R})$ with the following properties:*

(a) $G(\mathbb{R}) = UG(\mathbb{Z})$.

(b) if G has no nontrivial rational character defined over $\mathbb{Q}$, U has finite Haar measure.

A character of G is a homomorphism from G to the multiplicative group of a field, which is abelian, then from Lemma 2.3 we can see that every character of G is trivial. This theorem by Borel and Harish-Chandra, implies that ${}^{G(\mathbb{R})}\!/_{G(\mathbb{Z})}$ has a finite Haar measure and since $G(\mathbb{Z})$ is a discrete subgroup, that means that $G(\mathbb{Z})$ is a lattice in $G(\mathbb{R})$. So every finite index subgroup of $G(\mathbb{Z})$ is a lattice in $G(\mathbb{R})$.

Theorem 4.2. *(Borel density theorem)Let G be a connected semisimple real algebraic group without compact factors and let Γ be a lattice in G. Then Γ is Zariski dense in G.*

A slightly more general form of this theorem was first presented by Borel in his paper [Bor60], the way this version derived from Borel's original paper can be found in Raghunathan's book [Rag72, Chapter V]. The real Chevalley groups have no compact factors, this comes from the construction, specifically from the fact that the Cartan subalgebra has the same dimension over $\mathbb{R}$ as it has over $\mathbb{C}$. This dimension is the rank of G (over a selected field) and when $\mathcal{L}$ is simple, is equals to the number of simple roots. The interested reader is referred to [Mor15, Chapter 2], [Pet17, Lemma 3.11] for more details. So from Theorem 4.2, every finite index subgroup of $G(\mathbb{Z})$ is Zariski dense in $G(\mathbb{R})$.

Theorem 4.3. *[Ros57, p.44]If the connected linear algebraic group G is defined over the infinite perfect field k, then the points of G that are rational over k are dense in G.*

From Theorem 2.1 G is semisimple, in particular G is connected. Since $\mathbb{C}$ is perfect, from this Rosenlicht's theorem we get that $G(\mathbb{Q})$ is Zariski dense in G. Obviously that mean that $G(\mathbb{R})$ is Zariski dense in G, so every finite index subgroup of $G(\mathbb{Z})$ is Zariski dense in G.

4.2 Generating Pairs of Opposite Horospherical Subgroups

Here let k be a global field and G a connected, absolutely almost simple, simply connected k-algebraic group of $\mathrm{rank}_k(G) \geq 2$. We fix a faithful k-representation of G in some $\mathrm{GL}_n(k)$ and identify G with its image under this representation. Let S be a finite set of valuations of k containing all the archimedean valuations and $\mathcal{O}_S$ be the ring of S-integers in k. We fix a maximal $k-$split torus T in G. Let Σ denote the root system of G with respect to T. Let $\Pi \subset \Sigma$ be a system of simple roots and denote by P^+ (resp. P^-) the positive (resp. negative) roots. For $A \subset \Sigma$, let $\mathfrak{X}_A$ denote the group generated by all root subgroups $\mathfrak{X}_\alpha$, $\alpha \in A$.

Theorem 4.4. *Let $\Gamma(I)$ be the group generated by $\mathfrak{X}_{P^+}(I)$ and $\mathfrak{X}_{P^-}(I)$. Then for any non-zero ideal $I \lhd \mathcal{O}_S$, $\Gamma(I)$ has a finite index in $G(\mathcal{O}_S)$.[Rag92, Theorem 1.2]*

This result was first presented for classical groups with $\mathrm{rank}_k(G) \geq 2$ by Vaserstein in[Vas73], and then for Chevalley groups for $\mathrm{rank}_k(G) \geq 2$ by Tits in [Tit76]. Venkataramana expanded this result for some groups with $\mathrm{rank}_k(G) \geq 1$ [Ven94]. This result is true for an arbitrary pair of opposite horospherical k-subgroups.

Claim 4.1. Let I be a nonzero ideal in $\mathcal{O}_S$ and $\Gamma(I)$ denote the subgroup of $G(\mathcal{O}_S)$ generated by $\mathfrak{X}_{P^+}(I)$ and $\mathfrak{X}_{P^-}(I)$. Then for any $g \in G(k)$ there is a non-zero ideal I' in $\mathcal{O}_S$ such that $g\Gamma(I')g^{-1} \subset \Gamma(I)$.[Rag92]

The universal Chevalley groups over $\mathbb{C}$ has the S-congruence subgroup property. That means that every finite index subgroup of $G(\mathcal{O}_S)$ contains a $G(I)$, for I a non zero ideal of $\mathcal{O}_S$, such $G(I)$ is called a principal S-congruence subgroup. The proof of Theorem 4.4 is connected to the congruence subgroup problem, which asks if the S-congruence subgroup property applies. By studding the group under two topologies, called the S-congruence topology and the profinite topology, we can find connection between the finite index subgroups and the principal S-congruence subgroups.

5 Matrix Discriminant

Definition 5.1. The companion matrix of the monic polynomial $p(x) = x^r + a_{r-1}x^{r-1} + \ldots + a_0 \in k[x]$, for k a field, is the matrix

$$C(p) := \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{r-1} \end{pmatrix}.$$

Claim 5.1. If A is an n-by-n matrix with entries from some field k, then the following are equivalent[HJ12, p.194-195]:

(a) A is similar to the companion matrix over k of its characteristic polynomial.

(b) The characteristic polynomial of A coincides with the minimal polynomial of A.

(c) There exists a cyclic vector v in $V = k^n$ for A, meaning that $\{v, Av, A^2v, \ldots, A^{n-1}v\}$ is a basis of V.

Definition 5.2. For matrices $A \in M_n(k), B \in M_m(k)$ their direct sum is

$$A \oplus B := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

Theorem 5.1. *Every matrix $A \in M_n(k)$ is similar over k to a direct sum of companion matrices $C(p_1) \oplus \ldots \oplus C(p_r)$ where $p_i \in k[x]$ monic polynomials such that for every $1 \leq i \leq r-1$, $p_i | p_{i+1}$. [DF03, Chap .12 Theorem 14.]*

Remark 5.1. We can see that the characteristic polynomial of A is equal to $\prod_{i=1}^{r} p_i$.

Definition 5.3. For two polynomials $p(x) = \sum_{i=0}^{n} a_i x^i, q(x) = \sum_{i=0}^{m} b_i x^i$ with respective roots $\alpha_1, \ldots \alpha_n; \beta_1, \ldots \beta_m$ the resultant is defined by

$$Res(p,q) := a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$$

Definition 5.4. The discriminant of the polynomial $p(x) = a_n x^n + \ldots + a_0$, where $a_n \neq 0, a_i \in R$ a commutative ring, is

$$disc(p) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n} Res(p, p').$$

The discriminant of a matrix $A \in M_n(k)$ is the discriminant of its characteristic polynomial.

Remark 5.2. Form Definition 5.3, the resultant of two polynomials with coefficients in an integral domain, is zero if and only if they have a common divisor of positive degree. If for a polynomial p we have $disc(p) \neq 0$ then $Res(p, p') \neq 0$, this is true if and only if there are no common roots for p and p' and that is if and only if p has distinct roots.

6 The SL_n Group

When $\mathcal{L}$ is the simple Lie algebra $sl_n(k)$; $(n\geq 2)$, the Lie algebra of $n\times n$ matrices of trace 0 with multiplication $[X,Y]=XY-YX$, the universal Chevalley group G over $\mathcal{L}$ and k is the $\mathrm{SL}_n(k)$ group. The roots are the maps $\mathrm{diag}(a_1,a_2,...,a_n)\to a_i-a_j,(1\leq i,j\leq n,i\neq j)$, the positive roots are for $(1\leq i<j\leq n)$ and the root system is of type A_{n-1}. We denote the roots by $\alpha_{i,j}$ and we have $ht(\alpha_{i,j})=j-i$. We can choose the root elements $x_{\alpha_{i,j}}(t)$ in G, to correspond to the matrices $e_{i,j}(t)=Id+\widetilde{e}_{i,j}(t)$, where $\widetilde{e}_{i,j}(t)$ has t at the (i,j) entry and zeros elsewhere. Under this choice, we have that U^+, B and H (as defined in Proposition 2.1 and Corollary 2.1) are the unipotent superdiagonal, superdiagonal and diagonal matrices respectively. The root subgroups are denoted by $E_{i,j}:=\mathfrak{X}_{\alpha_{i,j}}=\langle e_{i,j}(t)\,|t\in k\rangle$ and for $1\leq i\lneq j\leq n$ and we define

$$U_{i,j}:=\langle E_{r,s}|\,(j\lneq s)\,or\,(j=s\wedge r\leq i)\rangle \tag{6.1}$$

Notice that

$$U_{1,2}=\begin{pmatrix}1&*&*&*&\cdots&*\\&1&*&*&\cdots&*\\&&1&*&\cdots&*\\&&&1&\ddots&\vdots\\&&&&\ddots&*\\&&&&&1\end{pmatrix},U_{2,3}=\begin{pmatrix}1&0&*&*&\cdots&*\\&1&*&*&\cdots&*\\&&1&*&\cdots&*\\&&&1&\ddots&\vdots\\&&&&\ddots&*\\&&&&&1\end{pmatrix}$$

$$,U_{1,3}=\begin{pmatrix}1&0&*&*&\cdots&*\\&1&0&*&\cdots&*\\&&1&*&\cdots&*\\&&&1&\ddots&\vdots\\&&&&\ddots&*\\&&&&&1\end{pmatrix}\ldots,U_{1,n}=\begin{pmatrix}1&0&0&\cdots&0&*\\&1&0&\cdots&0&0\\&&1&\ddots&0&0\\&&&1&\ddots&\vdots\\&&&&\ddots&0\\&&&&&1\end{pmatrix}$$

also notice that for $(i,j)=(1,2)$, $U_{1,2}=\langle E_{i,j}|1\leq i\lneq j\leq n\rangle=:U^+$. From Theorem 2.1, if $k=\mathbb{C}$ then the Weyl group $W\cong {}^{\mathrm{N}_G(H)}\!/_{H}\cong S_n$. Representative for elements of W in G can be the matching permutation matrices. However, since the determinant of a permutation matrix is the sign of the permutation, to represent an odd permutation in G, we can take one of the nonzero elements to be -1 instead of 1. In this section I'll assume $G=\mathrm{SL}_n(\mathbb{C})$, and will prove some results regarding G. Notice since $\mathcal{L}$ is simple and G is the universal Chevalley group over $\mathcal{L}$ and $\mathbb{C}$, G is simply connected and so, all the conclusions in Section 4 applies.

6.1 Open Set in a Conjugacy Class of a Bruhat Cell

In the Weyl group $W\cong S_n$, the element that correspond to the permutation $\sigma:=(12)(23)...((n-1)n)=(12\ldots n)$, is a Coxeter element. For a representative of the coset of σ in G (as defined in Corollary 2.1(d)), we can take the matrix

$$w := \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ -1 & 0 & & & 0 \\ 0 & -1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & -1 & 0 \end{pmatrix} \tag{6.2}$$

Notice that for Q_σ as defined in Theorem 2.3, we have $Q_\sigma = \{\alpha_{i,n} | 1 \leq i \leq n-1\}$, $\mathfrak{X}_{Q_\sigma} = U_{n-1,n}$. So every element $g \in BwB$ can be written as $g = bw \prod_{i=1}^{n-1} e_{i,n}(t_i) \in BwU_{n-1,n}$.

Theorem 6.1. *The conjugacy class in $G(\mathbb{Z})$ of the Bruhat cell $B(\mathbb{Q}) wB(\mathbb{Q})$ contains a Zariski open set.*

Proof. We define the Zariski open set $J := \{g \in \mathrm{SL}_n(\mathbb{Z}) \,|\, disc(g) \neq 0\}$, it is Zariski open since it is a complement of an algebraic set. Let $g \in J$, we'll show that g is conjugate in $\mathrm{SL}_n(\mathbb{Z})$ to a matrix in $B(\mathbb{Q}) wB(\mathbb{Q})$. From Theorem 5.1 we have that g is conjugate to $\bigoplus_{i=1}^{r} C(f_i)$ in $\mathrm{GL}_n(\mathbb{Q})$ for f_i rational monic polynomials such that $f_i | f_{i+1}$. The characteristic polynomial for conjugate matrices is the same, so the characteristic polynomial of g is $f := \prod_{i=1}^{r} f_i$. Since $disc(g) \neq 0$, form Remark 5.2 we have that f has distinct roots. That means that $f_1, \ldots, f_r$ are pairwise coprime, and from the assumption that $f_i | f_{i+1}$, we get that $r = 1$ so g is conjugate to a companion matrix in $\mathrm{GL}_n(\mathbb{Z})$. From Claim 5.1 there is a $v \in \mathbb{Q}^n$ such that $\mathcal{V} = \{v, gv, \ldots, g^{n-1}v\}$ is a $\mathbb{Q}$ basis for $\mathbb{Q}^n$. So under the basis $\mathcal{V}$ we have

$$[g]_{\mathcal{V}} = C(f) = \begin{pmatrix} & & & a_0 \\ 1 & & & a_1 \\ & \ddots & & \vdots \\ & & 1 & a_{n-1} \end{pmatrix}$$

for $a_i \in \mathbb{Z}$ and since $g \in \mathrm{SL}_n(\mathbb{Z})$ we have $a_0 = (-1)^{n+1}$ and for

$$\widetilde{b} = \begin{pmatrix} -1 & & & \frac{-a_1}{a_0} \\ & -1 & & \vdots \\ & & \ddots & \frac{-a_{n-1}}{a_0} \\ & & & a_0 \end{pmatrix} \in B(\mathbb{Z})$$

we get $[g]_{\mathcal{V}} \widetilde{b} = w$. We can construct a $\mathbb{Z}$ basis $\mathcal{W} = \{w_1, \ldots, w_n\}$ for $\mathbb{Z}^n$ such that for every $1 \leq k \leq n$

$$\mathrm{span}_{\mathbb{Q}} \{w_i | 1 \leq i \leq k\} = \mathrm{span}_{\mathbb{Q}} \{g^{i-1}v | 1 \leq i \leq k\} \tag{6.3}$$

and so g is conjugated to $[g]_{\mathcal{W}}$ in $\mathrm{GL}_n(\mathbb{Z})$. Since we can change $w_1 \to -w_1$, we may assume the conjugation is in $\mathrm{SL}_n(\mathbb{Z})$. From Equation (6.3), the change of basis matrix between $\mathcal{V}$ and $\mathcal{W}$ is an upper triangular matrix b. We can set $b' = \frac{1}{det(b)} b \in B(\mathbb{Q})$ and we get $[g]_{\mathcal{W}} = b' [g]_{\mathcal{V}} b'^{-1} = b' w \widetilde{b}^{-1} b'^{-1} \in B(\mathbb{Q}) w B(\mathbb{Q})$. As g is conjugated to $[g]_{\mathcal{W}}$ in $\mathrm{SL}_n(\mathbb{Z})$, we are done. □

Corollary 6.1. *Let H be a subgroup with finite index of $G(\mathbb{Z})$, then $H \cap B(\mathbb{Q}) w U_{n-1,n}(\mathbb{Q}) \neq \emptyset$.*

Proof. Every finite index subgroup contains a normal subgroup of finite index, so we may assume that H is normal in $G(\mathbb{Z})$. From Subsection 4.1, H is Zariski dense in G, so from Theorem 6.1 H contains an element of the conjugacy class over $G(\mathbb{Z})$ of $B(\mathbb{Q}) w B(\mathbb{Q})$. Since H is normal in $G(\mathbb{Z})$, it contains an element g of $B(\mathbb{Q}) w B(\mathbb{Q})$. From Theorem 2.3, we conclude that $g \in H \cap B(\mathbb{Q}) w B(\mathbb{Q}) = H \cap B(\mathbb{Q}) w U_{n-1,n}(\mathbb{Q})$ as needed. □

6.2 Finite Index Subgroup Construction

The following Theorem demonstrate a method of using the Chevalley group structure and certain elements, to generate a finite index subgroup. The method is to use the fact that the Weyl group's representatives, act on the root elements as in Remark 2.3 ($R3$). So by having a root element, and a Weyl group's element representative with high enough order, we can create more root elements. For example, for a root element $e_{i,j}(t)$ in G and w as defined in 6.2, we have ${}^{w}e_{i,j}(t) = e_{\sigma(i),\sigma(j)}(-t), {}^{w^{-1}}e_{i,j}(t) = e_{\sigma^{-1}(i),\sigma^{-1}(j)}(-t)$, for $\sigma = (1 \ldots n)$. Since the root elements are unipotent elements and are the image of the additive group of the field, it is not difficult to find root elements in finite index groups of $G(\mathbb{Z})$. The representative for the Weyl group in $G(\mathbb{Z})$, are only in the form of $w_\alpha(\pm 1)$, as defined in Remark 2.3 ($R2$). So it is more difficult to find such elements in our subgroups of $G(\mathbb{Z})$. We go around this by finding more general elements, specifically we use elements present in the Bruhat cells. In their composition, those elements include a representative of an element in the Weyl group. By having an element of a Bruhat cell, that is constructed from a Coxeter element using a root element, we can generate most of the time a Coxeter number of root elements. Once we have enough root elements, we use relation ($R1$) in Remark 2.3, to create more. In this section we set $n \geq 3$, α an integral element over $\mathbb{Z}$ and $k := \mathbb{Q}(\alpha)$.

Theorem 6.2. *There are unipotent element $u_1 \in \mathrm{SL}_n(\mathbb{Z}), u_2 \in \mathrm{SL}_n(\mathcal{O}_k)$ such that for every $g \in \mathrm{SL}_n(\mathbb{Z}) \cap B(\mathbb{Q}) w U_{n-1,n}(\mathbb{Q})$ and every $m_1, m_2 \in \mathbb{Z}^+$, $\langle g, u_1^{m_1}, u_2^{m_2} \rangle$ is of finite index in $\mathrm{SL}_n(\mathcal{O}_k)$.*

Proof. We take $u_1 := e_{1,n}(1), u_2 = e_{2,n}(\alpha)$ and write $g = bwu \in B(\mathbb{Q}) w U_{n-1,n}(\mathbb{Q})$ (where w as in (6.2) and B is upper triangular matrices and $U_{n-1,n}$ is as Equation (6.1) both over k). Let $m, l \in \mathbb{Z}^+$ and define $\Lambda := \langle g, u_1^m, u_2^l \rangle$ and show that for every $r \in \mathbb{N}$ there is a $k_r \in \mathbb{Z}^+$ such that

$$U_{1,2}^{(r)}(k_r\mathbb{Z}) := Id + (U_{1,2}(k_r\mathbb{Z}) - Id)\alpha^r \subset \Lambda \tag{6.4}$$

(where $U_{1,2}(I)$ as in Equation 4.1). We'll show this by induction on r, in each level we will use the relation in Remark 2.3 to create more root elements.

$r=0$ This case has a proof given by Meiri in [Mei17], I'll show a variation of it. I'll show that for every $1 \le i < j \le n$ we have $k_{i,j} \in \mathbb{Z}^+$ such that $U_{i,j}^{(0)}(k_{i,j}\mathbb{Z}) = U_{i,j}(k_{i,j}\mathbb{Z}) \subset \Lambda$ by induction on j.

$j=n$ Again by induction on $1 \le i \le n-1$ we'll show that there are $k_{i,n} \in \mathbb{Z}^+$ such that $U_{i,n}(k_{i,n}\mathbb{Z}) \subset \Lambda$.

$i=1$ In this case we have $u_1^m = e_{1,n}(m) \in \Lambda$ and notice that $\langle e_{1,n}(m)\rangle = E_{1,n}(m\mathbb{Z}) = U_{1,n}(m\mathbb{Z}) \subset \Lambda$.

i Assume for i and we prove for $i+1$. From the assumption we have $e_{i,n}(k_{i,n}), e_{1,n}(m) \in \Lambda$ and notice that ${}^{b^{-1}}e_{1,n}(m) = b^{-1}e_{1,n}(m)\,b = e_{1,n}(qm)$ for some $0 \ne q \in \mathbb{Q}$. Since $U_{n-1,n}$ is abelian we have $\Lambda \cap \mathrm{SL}_n(\mathbb{Z}) \ni h := [{}^{g}e_{i,n}(k_{i,n}), e_{1,n}(m)] = \left[{}^{b}e_{i+1,1}(-k_{i,n}), {}^{b}e_{1,n}(qm)\right] = {}^{b}\left[e_{i+1,1}(-k_{i,n}), e_{1,n}(qm)\right] = {}^{b}e_{i+1,n}(-k_{i,n}qm) = Id + \sum_{c=1}^{i+1} \widetilde{e}_{c,n}(t_c)$ where $t_c \in \mathbb{Z}, t_{i+1} \ne 0$ and $\widetilde{e}_{i,j}(t)$ is the matrix with t in the (i,j) position and zero everywhere else. Then since from the induction assumption $e_{c,n}(-k_{i,n}t_c) \in \Lambda$ for every $1 \le c \le i$ we have $\left(\prod_{c=1}^{i} e_{c,n}(-k_{i,n}t_c)\right) h^{k_{i,n}} = e_{i+1,n}(t_{i+1}k_{i,n}) \in \Lambda$ and so $U_{i+1,n}(t_{i+1}k_{i,n}\mathbb{Z}) \subset \Lambda$.

j Assume for j and we prove for $j-1$, let $1 \le i < j-1$ from the assumption there is a $k_{i+1,j} \in \mathbb{Z}^+$ such that $U_{i+1,j}(k_{i+1,j}\mathbb{Z}) \subset \Lambda$. $U_{i+1,j}$ is normalized by b so $e_{i+1,j}(1) \in {}^{b^{-1}} U_{i+1,j}$, from that we have that ${}^{u^{-1}}e_{i,j-1}(1) = Id + \widetilde{e}_{i,j-1}(1) + \widetilde{e}_{i,n}\left(\frac{z_1}{z_2}\right) \in {}^{g^{-1}}U_{i+1,j}$ for $z_i \in \mathbb{Z}, z_2 \ne 0$. We define the projection $\Pi_{k_{i+1,j}} : \mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n\left(\mathbb{Z}/k_{i+1,j}\mathbb{Z}\right)$ and notice that for $u' \in U_{i+1,j}(\mathbb{Z})$, if ${}^{g^{-1}}u' \in \ker\left(\Pi_{k_{i+1,j}}\right)$, then $u' \in \ker\left(\Pi_{k_{i+1,j}}\right)$. So

$$\left({}^{g^{-1}}U_{i+1,j}\right)(k_{i+1,j}\mathbb{Z}) \subset {}^{g^{-1}}\left(U_{i+1,j}(k_{i+1,j}\mathbb{Z})\right) \subset \Lambda. \tag{6.5}$$

Then we know that $\left({}^{u^{-1}}e_{i,j-1}(1)\right)^{z_2 k_{i+1,j}} \in \left({}^{g^{-1}}U_{i+1,j}\right)(k_{i+1,j}\mathbb{Z}) \subset \Lambda$. Since the assumption give us $e_{i,n}(-z_1k_{i+1,j}) \in \Lambda$,

$e_{i,n}(-z_1k_{i+1,j})\left({}^{u^{-1}}e_{i,j-1}(1)\right)^{z_2k_{i+1,j}} = e_{i,j-1}(z_2k_{i+1,j}) \in \Lambda$,

so $U_{i,j-1}(z_2k_{i+1,j}) \subset \Lambda$.

$r-1$ We now assume (6.4) for every $1 \le r' < r$. So for every $1 \le i < j \le n$ we need to find $k_{i,j}^{(r)} \in \mathbb{Z}^+$ such that $U_{i,j}^{(r)}\left(k_{i,j}^{(r)}\mathbb{Z}\right) \subset \Lambda$, we'll do it by induction on j.

$j=n$ We will show that for every $1 \le i \le n-1$ there is a $k_{i,n}^{(r)} \in \mathbb{Z}^+$ such that $U_{i,n}^{(r)}\left(k_{i,n}^{(r)}\mathbb{Z}\right) \subset \Lambda$, by induction on i.

$i=1$ Since $U_{1,2}^{(r-1)}(k_{r-1}\mathbb{Z}) \subset \Lambda$ we have $\left[e_{1,2}\left(k_{r-1}\alpha^{r-1}\right), u_2^l\right] = e_{1,n}\left(k_{r-1}l\alpha^r\right) \in \Lambda$ and so $U_{1,n}^{(r)}(k_{r-1}l\mathbb{Z}) \subset \Lambda$.

i We assume for i and prove for $i+1$, from the assumption we deduce that $\Lambda \ni h'' := \left[{}^g e_{i,n}\left(k_{i,n}^{(r)}\alpha^r\right), e_{1,n}(m)\right] =^b e_{i+1,n}\left(-qmk_{i,n}^{(r)}\alpha^r\right) = Id + \sum_{c=1}^{i+1}\widetilde{e}_{c,n}\left(t_c'\alpha^r\right)$ for $t_c' \in \mathbb{Z}, t_{i+1}' \neq 0$. We can have now $\left(\prod_{c=1}^{i} e_{c,n}\left(-k_{i,n}^{(r)}t_c'\alpha^r\right)\right) h''^{k_{i,n}^{(r)}} = e_{i+1,n}\left(t_{i+1}'k_{i,n}^{(r)}\alpha^r\right) \in \Lambda \Rightarrow U_{i+1,n}^{(r)}\left(t_{i+1}'k_{i,n}^{(r)}\mathbb{Z}\right) \subset \Lambda$.

j We assume for j and prove for $j-1$, let $1 \leq i < j-1$ from the assumption there is a $k_{i+1,j} \in \mathbb{Z}^+$ such that $U_{i+1,j}^{(r)}\left(k_{i+1,j}^{(r)}\mathbb{Z}\right) \subset \Lambda$. Since $U_{i+1,j}$ is normalized by b we have ${}^{g^{-1}}U_{i+1,j}^{(r)} = Id + \left({}^{g^{-1}}U_{i+1,j} - Id\right)\alpha^r \ni \bar{h} :=^{u^{-1}} e_{i,j-1}(\alpha^r) = Id + \widetilde{e}_{i,j-1}(\alpha^r) + \widetilde{e}_{i,n}\left(\frac{z_3}{z_4}\alpha^r\right)$ for $z_i \in \mathbb{Z}, z_4 \neq 0$. Similar to (6.5) we have $\bar{h}^{z_4 k_{i+1,j}} \in \left({}^{g^{-1}}U_{i+1,j}^{(r)}\right)(k_{i+1,j}\mathbb{Z}) \subset^{g^{-1}} \left(U_{i+1,j}^{(r)}(k_{i+1,j}\mathbb{Z})\right) \subset \Lambda$. Since $e_{i,n}(-z_3 k_{i+1,j}\alpha^r) \in \Lambda$, we have $e_{i,n}(-z_3 k_{i+1,j}\alpha^r)\,\bar{h}^{z_4 k_{i+1,j}} = e_{i,j-1}(z_4 k_{i+1,j}\alpha^r) \in \Lambda$. So we can deduce that $U_{i,j-1}^{(r)}(z_4 k_{i+1,j}\mathbb{Z}) \subset \Lambda$ as needed.

Let $d \in \mathbb{Z}$ the degree of the minimal polynomial of α over $\mathbb{Z}$. We define $k = \prod_{i=0}^{d} k_i$, then from previous part we have $U_{1,2}^{(i)}(k\mathbb{Z}) \subset \Lambda$ for every $0 \leq i \leq d$. We denote $0 \neq I := \sum_{i=0}^{d} k\mathbb{Z}\alpha^i \triangleleft \mathbb{Z}[\alpha]$. From Theorem 3.1 there is a non zero ideal $0 \neq J \triangleleft \mathcal{O}_k$ such that $J \subset I$, so we have $U^+(J) \subset \Lambda$. Since $U_{n-1,n}$ is abelian we have ${}^g e_{n-1,n}(J) =^b e_{n,1}(J)$, we denote $\Lambda^* :=^{b^{-1}} \Lambda$ then $e_{n,1}(J) \subset \Lambda^*$. Since $n \geq 3$ $\mathrm{rank}_k(G) \geq 2$, so we can use Section 4.2. From Claim 4.1 there is a non zero ideal $0 \neq J' \triangleleft \mathcal{O}_k$ such that $\Gamma(J') := \left\langle \mathfrak{X}_{\alpha_{i,j}}(J') | 1 \leq i \neq j \leq n \right\rangle \subset b^{-1}\Gamma(J)\,b$. Since b is an upper triangular matrix and $U^+(J) \subset \Gamma(J) \cap B \Rightarrow U^+(J') \subset \Lambda^*$, for every $1 \leq i \leq n-1$, we have $[e_{i,n}(J'), e_{n,1}(J)] = e_{i,1}(J'J) \subset \Lambda^*$. So for every $1 < i \neq j \leq n$, $[e_{i,1}(J'J), e_{1,j}(J')] = e_{i,j}\left(J'^2 J\right) \subset \Lambda^*$. Now we have $\left\{\Gamma_{\alpha_{i,j}}\left(J'^2 J\right) | 1 \leq i \neq j \leq n\right\} \subset \Lambda^*$ and from Theorem 4.4 Λ^* has a finite index $\mathrm{SL}_n(\mathcal{O}_k)$. Since conjugated subgroup have the same index, so does Λ. □

Corollary 6.2. *For every finite index subgroup Γ of $\mathrm{SL}_n(\mathcal{O}_k)$ there are $a, b, c \in \Gamma$ such that $[\mathrm{SL}_n(\mathcal{O}_k) : \langle a, b, c\rangle] < \infty$.*

Proof. Since Γ of finite index there is a normal subgroup $\Gamma \supset N \triangleleft \mathrm{SL}_n(\mathcal{O}_k)$ with finite index, then from the second isomorphism theorem we have

$$[\mathrm{SL}_n(\mathbb{Z}) : \Gamma \cap \mathrm{SL}_n(\mathbb{Z})] \leq [\mathrm{SL}_n(\mathbb{Z}) : N \cap \mathrm{SL}_n(\mathbb{Z})] \leq [\mathrm{SL}_n(\mathcal{O}_k) : N] < \infty$$

so $\Gamma \cap \mathrm{SL}_n(\mathbb{Z})$ has a finite index in $\mathrm{SL}_n(\mathbb{Z})$. From Corollary 6.1, $\Gamma \cap \mathrm{SL}_n(\mathbb{Z}) \cap B(\mathbb{Q})\,wU_{n-1,n}(\mathbb{Q}) \neq \emptyset$, so there is a $g \in \Gamma \cap \mathrm{SL}_n(\mathbb{Z}) \cap B(\mathbb{Q})\,wU_{n-1,n}(\mathbb{Q})$. For the elements $u_1, u_2 \in \mathrm{SL}_n(\mathcal{O}_k)$ as defined in Theorem 6.2, since N is normal with finite index, there are $m, l \in \mathbb{Z}^+$such that $u_1^m, u_2^l \in N \subset \Gamma$, and so from Theorem 6.2 $\left\langle g, u_1^m, u_2^l\right\rangle \subset \Gamma$ has a finite index in $\mathrm{SL}_n(\mathcal{O}_k)$. □

Remark. Notice that for $\alpha \in \mathbb{Z}$, we can omit the u_2 elements in this section and get a two generated finite index subgroup of $\mathrm{SL}_n(\mathbb{Z})$ as Meiri did.

References

[BHC61] Armand Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Bull. Amer. Math. Soc.*, 67:579–583, 1961.

[Bor60] Armand Borel. Density properties for certain subgroups of semi-simple groups without compact components. *Ann. of Math. (2)*, 72:179–188, 1960.

[Che46] Claude Chevalley. Theory of lie groups princeton univ. *Press, Princeton, NJ*, 1, 1946.

[Che55] C. Chevalley. Sur certains groupes simples. *Tohoku Math. J. (2)*, 7(1-2):14–66, 1955.

[DF03] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.

[Hal15] Brian Hall. *Lie groups, Lie algebras, and representations: an elementary introduction*, volume 222. Springer, 2015.

[HJ12] Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, New York, NY, USA, 2nd edition, 2012.

[Hum90] James E Humphreys. *Reflection groups and Coxeter groups*, volume 29. Cambridge university press, 1990.

[Kos09] Bertram Kostant. *Groups Over* $\mathbb{Z}$, pages 483–491. Springer New York, New York, NY, 2009.

[LM87a] Alexander Lubotzky and Avinoam Mann. Powerful p-groups. I. Finite groups. *J. Algebra*, 105(2):484–505, 1987.

[LM87b] Alexander Lubotzky and Avinoam Mann. Powerful p-groups. II. p-adic analytic groups. *J. Algebra*, 105(2):506–515, 1987.

[LR11] D. D. Long and A. W. Reid. Small subgroups of $\mathrm{SL}(3,\mathbb{Z})$. *Exp. Math.*, 20(4):412–425, 2011.

[Lub86] Alexander Lubotzky. Dimension function for discrete groups. In *Proceedings of groups—St. Andrews 1985*, volume 121 of *London Math. Soc. Lecture Note Ser.*, pages 254–262. Cambridge Univ. Press, Cambridge, 1986.

[Mei17] Chen Meiri. Generating pairs for finite index subgroups of $\mathrm{SL}(n,\mathbb{Z})$. *J. Algebra*, 470:420–424, 2017.

[Mor15] Dave Witte Morris. *Introduction to arithmetic groups.* Deductive Press, 2015.

[Pet17] Chris Peters. Rigidity of spreadings and fields of definition. *EMS Surv. Math. Sci.*, 4(1):77–100, 2017.

[Rag72] M. S. Raghunathan. *Discrete subgroups of Lie groups.* Springer-Verlag, New York-Heidelberg, 1972. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 68.

[Rag92] M. S. Raghunathan. A note on generators for arithmetic subgroups of algebraic groups. *Pacific J. Math.*, 152(2):365–373, 1992.

[Ros57] Maxwell Rosenlicht. Some rationality questions on algebraic groups. *Ann. Mat. Pura Appl. (4)*, 43:25–50, 1957.

[RP94] Andrei Rapinchuk and Vladimir Platonov. Algebraic groups and number theory, 1994.

[Ste67] R. Steinberg. *Lectures on Chevalley groups.* Lectures on Chevalley Groups. Yale University, 1967.

[SV05] R. Sharma and T. N. Venkataramana. Generations for arithmetic groups. *Geometriae Dedicata*, 114(1):103–146, Aug 2005.

[Tit64] J. Tits. Algebraic and abstract simple groups. *Annals of Mathematics*, 80(2):313–329, 1964.

[Tit76] J. Tits. Systèmes générateurs de groupes de congruence. *C. R. Acad. Sci. Paris Sér. A-B*, 283(9):Ai, A693–A695, 1976.

[Vas73] L. N. Vaseršteĭn. Structure of the classical arithmetic groups of rank greater than 1. *Mat. Sb. (N.S.)*, 91(133):445–470, 472, 1973.

[Ven94] T. N. Venkataramana. On systems of generators of arithmetic subgroups of higher rank groups. *Pacific J. Math.*, 166(1):193–212, 1994.