Bounded Generation of Two Families of S-Arithmetic Groups

Andrea Heald
Charlottesville, Virginia

B.S., Harvey Mudd College, 2007

A dissertation presented to the Graduate Faculty
of the University of Virginia in Candidacy for the Degree of
Doctor of Philosophy

Department of Mathematics

University of Virginia
August, 2013

Abstract

The objective of this work is to establish bounded generation for two families of S-arithmetic groups. We first establish bounded generation for the special linear group over certain S-orders of a quaternion algebra. We also establish bounded generation for certain special unitary groups.

This thesis consists of three chapters. The first chapter provides much of the background necessary as well as providing some applications of bounded generation. The second chapter contains the proof of bounded generation for some special linear groups, and the third chapter contains the proof of bounded generation for some special unitary groups.

Acknowledgments

I would like to thank my advisor, Andrei Rapinchuk, for all the assistance and advice he has given me. I would also like to thank everyone in the University of Virginia math department for providing support through my years here. Most of all, I would like to thank my husband, Ben, for being an unending source of support and encouragement.

Contents

Introduction

This work demonstrates that two different families of S-arithmetic groups have bounded generation.

Definition. A group G has *bounded generation* if there exist elements $a_1, \ldots, a_m$ of G such that $G = \langle a_1 \rangle \langle a_2 \rangle \cdots \langle a_m \rangle$, where $\langle a_i \rangle$ is the cyclic group generated by a_i.

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. In [3] Carter and Keller showed that for $n \geq 3$ any element in $SL_n(\mathcal{O}_K)$ is a product of a bounded number of elementary matrices. This implies that $SL_n(\mathcal{O}_K)$ has bounded generation (see Section 2.1). Theorem 2.7 extends this result to SL_n over an order of a quaternion algebra (see Section 1.2).

Let S be a finite subset of the set V^K of all valuations of K which contains V_∞^K, the set of all archmidean valuations. Let V be a quadratic space of Witt index at least 2 or assume S contains at least one nonarchimedean valuation and V has Witt index at least 1. (We refer to Section 0.1 for all unexplained notations.) In this case Rapinchuk and Erovenko showed in [7] that $\mathrm{Spin}(V)_{\mathcal{O}_S}$ (and thus the corresponding orthogonal group) has bounded generation. In Chapter 3 we extend their method to establish bounded generation for certain unitary groups.

We now give precise statements of our theorems. Let K be an algebraic number field, $\alpha, \beta \in K$ and let $\mathcal{D} = \left(\dfrac{\alpha, \beta}{K}\right)$ be a quaternion algebra with standard basis

$1, i, j, k$ (see Section 1.2). Assume $S \subset V^K$ is such that $\alpha, \beta \in \mathcal{O}_S$, then let

$$\mathcal{O}_{S,\mathcal{D}} := \{x + yi + zj + wk \mid x, y, z, w \in \mathcal{O}_S\}.$$

For $n \geq 1$, $SL_n(\mathcal{D})$ denotes the subset of elements of $M_n(\mathcal{D})$ with reduced norm 1. We set $SL_n(\mathcal{O}_{S,\mathcal{D}}) = M_n(\mathcal{O}_{S,\mathcal{D}}) \cap SL_n(\mathcal{D})$. (See Section 1.2.)

Theorem (Main Theorem 1)**.** *Let S be a finite subset of V^K such that S contains V_∞^K and at least one nonarchimedean valuation. Then $SL_n(\mathcal{O}_{S,\mathcal{D}})$ has bounded generation.*

The proof involves reducing the general case of $n \geq 2$ to the case where $n = 2$, and then showing $SL_2(\mathcal{O}_{S,\mathcal{D}})$ has bounded generation by giving an isomorphism to a spin group which has bounded generation by [7].

For our second result we let $L = K[\sqrt{d}]$ be a quadratic extension of K. For a Hermitian matrix $F \in M_n(L)$ we let $SU_{n,F}$ denote the associated special unitary group (see Section 1.4).

Theorem (Main Theorem 2)**.** *Let f be a nondegenerate sesquilinear form on L^n and let F be the associated matrix, and $G = SU_{n,F}$. Fix $S \subset V^K$ such that $V_\infty^K \subset S$. If f has Witt index at least 2 then $G_{\mathcal{O}_S}$ has bounded generation.*

Similarly to the proof of the first main theorem, this result is proved by reducing the general case to $SU_{4,f}$ and then obtaining bounded generation by exhibiting an isomoprhism to a spin group with bounded generation.

Chapter 1 contains the necessary background material for the proofs of the main theorems. Section 1.1 introduces bounded generation, some theorems related to it, and contains some applications of bounded generation to other problems. Section 1.2 discusses general properties of quaternion algebras, including the definition of $SL_n(\mathcal{D})$. Section 1.3 gives a brief overview of orthogonal groups. Section 1.4 discusses properties of unitary groups including Witt's theorem for lattices. Section 1.5

defines a Clifford algebra and the spin group. Finally, Section 1.6 introduces the concept of strong approximation. Chapter 2 contains the proof of Main Theorem 1, and Chapter 3 contains the proof of Main Theorem 2.

0.1 Notations

We introduce some standard notations and provide some basic facts about the corresponding structures; see for example [17]. Let K be an algebraic number field. Two valuations on K are called equivalent if they induce the same topology on K. We let V^K denote the set of equivalence classes of valuations. There are two subsets of V^K that we will frequently refer to: V_∞^K, the set of all archimedean valuations, and $V_f^K = V^K \setminus V_\infty^K$, the set of all nonarchimedean valuations. For $v \in V^K$ we let $|\cdot|_v$ denote an absolute value corresponding to v. The completion of K with respect to the metric induced by v will be denoted by K_v. For any $v \in V_f^K$ we define $\mathcal{O}_v := \{k \in K_v \mid |k|_v \leq 1\}$. For a finite subset $S \subset V^K$ containing V_∞^K we define the ring of S integers,

$$\mathcal{O}_S := \{k \in K \mid |k|_v \leq 1 \text{ for all } v \notin S\}.$$

For $\alpha \in K^\times$ we define

$$V(\alpha) := \{v \in V_f^K \mid |\alpha|_v \neq 1\}.$$

We now define the ring of adeles, A_K, which will be needed in Section 1.6. We define

$$A_K = \{(x_v) \in \prod_{v \in V^K} K_v \mid x_v \in \mathcal{O}_v \text{ for all but finitely many } v \in V^K\}$$

with addition and multiplication defined componentwise.

Let S be a finite subset of V^K containing V_∞^K, and for each $v \in S$ let W_v be an

open set in K_v. We define a topology on A_K by taking sets of the form

$$\prod_{v\in S} W_v \times \prod_{v\in V^K\setminus S} \mathcal{O}_v$$

as a basis.

Let $S \subset V^K$. Define $A_{K,S}$ as the image of the projection map

$$\pi\colon A_K \to \prod_{v\in V^K\setminus S} K_v.$$

There is a topology on $A_{K,S}$ given by taking as open sets the sets $U \subseteq A_{K,S}$ with $\pi^{-1}(U)$ open in A_K.

Consider the diagonal map $\delta\colon K \to \prod_{v\in V^K} K_v$. Since $x \in \mathcal{O}_v$ for all but finitely many $v \in V_f^K$, we have that $\delta(K) \subset A_K$, and composing with the projection map we can define a diagonal map into $A_{K,S}$ for any S.

Proposition 0.1 ([17]). *For any nonempty $S \subset V^K$ the image of δ is dense in $A_{K,S}$.*

We now define some notations related to varieties. Let F be an algebraically closed field and let T be a subset of $F[x_1, \ldots, x_n]$. We define

$$V(T) = \{a \in F^n \mid f(a) = 0 \text{ for all } f \in T\}$$

and say $X \subset F^n$ is a variety if $X = V(T)$ for some T. Let X be a variety, we can define

$$I(X) = \{f \in F[x_1, \ldots, x_n] \mid f(a) = 0 \text{ for all } a \in X\}.$$

We say that X is defined over a ring R if $I(X) \cap R[x_1, \ldots, x_n]$ generates $I(X)$. If X is defined over R, we can consider

$$X_R = \{a \in R^n \mid f(a) = 0 \text{ for all } f \in I(X)\}.$$

If X, Y are both varieties an R-defined morphism $X \to Y$ is a map given by polynomials belonging to $R[x_1, \ldots, x_n]$. Notice that we can view the special linear group

SL_n as a variety in $M_n(F) = F^{n^2}$, since the determinant is a polynomial. We can view GL_n as a variety by indentifying it with

$$\{(x_{ij}) \in SL_{n+1} \mid x_{in} = x_{ni} = 0 \text{ for all } i \neq n\}.$$

Throughout this work we will be considering linear algebraic groups, i.e., subgroups of GL_n which are also varieties.

Two subgroups G_1, G_2 of a group G are *commensurable* if

$$[G_1 : G_1 \cap G_2] < \infty$$

and

$$[G_2 : G_1 \cap G_2] < \infty.$$

If G is an algebraic group a subgroup $\Gamma \subset G$ is called S-arithmetic if Γ and $G_{\mathcal{O}_S}$ are commensurable. If S is the set of all archimedean valuations then Γ is called arithmetic.

Chapter 1

Background Material

1.1 Bounded Generation

1.1.1 Definition and some Basic Properties

We start with a discussion of the definition and some basic properties of bounded generation.

Definition. A group G has *bounded generation* if there exist $a_1, \ldots, a_n \in G$ such that $G = \langle a_1 \rangle \langle a_2 \rangle \cdots \langle a_n \rangle$, where $\langle a_i \rangle$ denotes the cyclic group generated by a_i.

In other words, any element g in G can be written in the form $g = a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n}$ with $m_i \in \mathbb{Z}$. Notice that the definition does not require that the a_i's be distinct. It is clear that any finite group has bounded generation, and that groups with bounded generation are finitely generated. However, there are finitely generated groups without bounded generation (for instance F_n the free group on $n \geq 2$ generators [24]).

One example of an infinite group with bounded generation is the infinite dihedral group, $G = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} = \langle a, b \mid a^2 = b^2 = 1 \rangle$, since $G = \langle a \rangle \langle ab \rangle \langle b \rangle$.

On the other hand, the free product $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$ does not have bounded generation. In fact Tavgen showed in [24] that a non-trivial free product $A * B$ does not

have bounded generation unless both factors are isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

We now prove a useful fact about bounded generation.

Proposition 1.1 ([6],[11])**.** *Let $H \subset G$, $[G : H] < \infty$. Then H has bounded generation if and only if G does.*

Proof. Assume H has bounded generation; then $H = \langle a_1 \rangle \langle a_2 \rangle \cdots \langle a_n \rangle$ for some $a_i \in H$. Since H is of finite index in G, there exist $b_1, \ldots, b_m \in G$ such that $G = \bigcup_i b_i H$. Thus $G = \langle b_1 \rangle \cdots \langle b_m \rangle \langle a_1 \rangle \cdots \langle a_n \rangle$, and therefore G has bounded generation.

Assume that G has bounded generation. Since every subgroup of finite index contains a finite index normal subgroup, we only need to consider the case where H is normal in G. Let $m := [G : H]$ and $G = \langle g_1 \rangle \cdots \langle g_n \rangle$. The image of g_i in G/H has order divisible by m, so for $h_i := g_i^m$ we have that $h_i \in H$. Let

$$S = \{I = (i_1, \ldots, i_n) | 0 \leq i_j \leq m \text{ for all } 1 \leq j \leq n\},$$

and for $I = (i_1, \ldots, i_n)$ let g_I denote $g_1^{i_1} \cdots g_n^{i_n}$. Define $T := \{I \in S | g_I \in H\}$. We claim

$$H = \prod_{J \in T} \langle g_J \rangle \prod_{j=1}^{n} \prod_{I \in S} \left\langle g_I^{-1} h_j g_I \right\rangle.$$

Let $h \in H$. Then $h = g_1^{r_1} \cdots g_n^{r_n}$. We can write each r_j as $i_j + m a_j$ where $0 \leq i_j < m$. Then

$$\begin{aligned} h &= g_1^{i_1} h_1^{a_1} \cdots g_n^{i_n} h_n^{a_n} \\ &= g_{(i_1,\ldots,i_n)} g_{(0,i_2,\ldots,i_n)}^{-1} h_1^{a_1} g_{(0,i_2,\ldots,i_n)} g_{(0,0,i_3,\ldots,i_n)}^{-1} h_2^{a_2} \cdots h_n^{a_n} \\ &= g_{(i_1,\ldots,i_n)} \prod_{j=1}^{n} g_{(0,\ldots,0,i_{j+1},\ldots,i_n)}^{-1} h_j^{a_j} g_{(0,\ldots,0,i_{j+1},\ldots,i_n)} \in \prod_{J \in T} \langle g_J \rangle \prod_{j=1}^{n} \prod_{I \in S} \left\langle g_I^{-1} h_j g_I \right\rangle \end{aligned}$$

as desired. □

Corollary 1.2. *Assume $H, K \subset G$ are commensurable. Then H has bounded generation if and only if K does.*

Proof. If H has bounded generation then since H and K are commensurable by Proposition 1.1 $H \cap K$ has bounded generation and thus by Proposition 1.1 K does. □

Corollary 1.3. *Assume H, G are algebraic groups, and let K be an algebraic number field, assume there is a K-isomorphism $\phi\colon H_K \to G_K$. Then $H_{\mathcal{O}_K}$ has bounded generation, if and only if $G_{\mathcal{O}_K}$ does.*

Proof. By proposition 4.1 in [17] $\phi(H_{\mathcal{O}_K})$ is commensurable with $G_{\mathcal{O}_K}$ and thus by Corollary 1.2, we have that $\phi(H_{\mathcal{O}_K})$ has bounded generation if and only if $G_{\mathcal{O}_K}$ does. □

1.1.2 Applications

We now discuss various applications of the property of bounded generation. We first define bounded generation for profinite groups. One reference for profinite groups is [5].

Definition. A profinite group Γ is said to have bounded generation if there exist $a_1, \ldots, a_n \in G$ such that $G = \overline{\langle a_1 \rangle}\,\overline{\langle a_2 \rangle} \cdots \overline{\langle a_n \rangle}$, where $\overline{\langle a_i \rangle}$ denotes the closure of $\langle a_i \rangle$.

There is a connection between the property of bounded generation for an abstract group G, and its profinite completion, $\hat{G} := \varprojlim_{N \in I} G/N$, where I is the set of all finite index normal subgroups of G.

Lemma 1.4. *Let G be a group. If G has bounded generation then its profinite completion $\hat{G}$ has bounded generation as profinite groups.*

Proof. Let $G = \langle g_1 \rangle \cdots \langle g_n \rangle$, and let $\iota : G \to \hat{G}$ denote the canonical homomorphism. Notice that for each g_i, $\overline{\langle \iota(g_i) \rangle}$ is compact. This implies that $\overline{\langle \iota(g_1) \rangle} \cdots \overline{\langle \iota(g_n) \rangle}$ is compact, and therefore closed. However $\iota(G) \subset \overline{\langle \iota(g_1) \rangle} \cdots \overline{\langle \iota(g_n) \rangle}$ implying that $\hat{G} = \overline{\langle \iota(g_1) \rangle} \cdots \overline{\langle \iota(g_n) \rangle}$ since $\iota(G)$ is dense in $\hat{G}$. □

Bounded generation for profinite groups allows for a nice characterization of all analytic pro-p groups. A pro-p group is called analytic if it is an analytic manifold over $\mathbb{Q}_p$, the field of p-adic rationals, and the group operations are analytic functions, i.e., it has the structure of a p-adic Lie group.

Theorem 1.5 ([19])**.** *A pro-p group is analytic if and only if it has bounded generation as a profinite group.*

Bounded generation is also closely connected to the congruence subgroup property. Let G be an algebraic group defined over an algebraic number field K. Fix $S \subset V^K$ such that $V_\infty^K \subseteq S$ and fix an embedding $G \hookrightarrow GL_n$. Recall that $G_{\mathcal{O}_S} = G \cap GL_n(\mathcal{O}_S)$. For any nonzero ideal $\mathfrak{a} \subset \mathcal{O}_S$, we define that congruence subgroup $G(\mathfrak{a})$ by

$$G(\mathfrak{a}) = \{g \in G_{\mathcal{O}_S} \mid g \equiv I_n \pmod{\mathfrak{a}}\}.$$

Lemma 1.6. *The congruence subgroup $G(\mathfrak{a})$ has finite index in $G_{\mathcal{O}_S}$.*

Proof. Notice that $G_{\mathcal{O}_S}/G(\mathfrak{a}) \subseteq GL_m(\mathcal{O}_S/\mathfrak{a})$ for some m, and as $\mathcal{O}_S/\mathfrak{a}$ is finite, so is $G_{\mathcal{O}_S}/G(\mathfrak{a})$. □

To describe the congruence subgroup property we consider two different topologies on G_K. Define a topology on G_K by taking all normal subgroups of $G_{\mathcal{O}_S}$ of finite index as a base of neighborhoods of the identity. Let $\hat{G}^S$ denote the completion of G_K with respect to this topology. We can define an alternative topology by taking all congruence subgroups of $G_{\mathcal{O}_S}$ as a base of neighborhoods of the identity. Let $\bar{G}^S$ denote the completion of G_K with respect to this alternative topology. Since the first topology is stronger, there exists a natural, continuous, surjective homomorphism $\hat{G}^S \to \bar{G}^S$. The kernel of this map is called the S-congruence kernel and is denoted by $C^S(G)$. If $C^S(G)$ is finite we say that $G_{\mathcal{O}_S}$ has the congruence subgroup property. For an overview of developments on the congruence subgroup problem see [21].

To illustrate the connection between the congruence subgroup property and bounded generation we will need to focus on groups which satisfy the Margulis-Platonov conjecture (MP). This states: If

$$T = \{v \in V^K \setminus V_\infty^K \mid G \text{ is } K_v\text{-anisotropic}\},$$

then for any non-central normal subgroup $N \subset G_K$ there exists an open normal subgroup $W \subset \prod_{v \in T} G_{K_v}$ such that $N = G_K \cap W$. This has been proved in most cases; see Appendix A of [22] for a survey of this conjecture. With this condition it was proved in [16] that:

Theorem 1.7. *Let G be an algebraic group over a field K satisfying (MP), and let $S \subset V^K$ with $V_\infty^K \subset S$ and $S \cap T = \emptyset$. If $G_{\mathcal{O}_S}$ has bounded generation, $C^S(G)$ is finite.*

Another application involves the commensurator-normalizer property. A subgroup G_1 is commensurated by the conjugation action of G if for all $g \in G$, $g^{-1}G_1g$ and G_1 are commensurable. A group G has the outer commensurator-normalizer property if for any group H, and a homomorphism $\phi\colon G \to H$, any subgroup Γ of H which is commensurated by the conjugation action of $\phi(G)$, is almost normalized by $\phi(\Gamma)$,i.e, there exists a subgroup $H' \subset G$ commensurable with H which is normalized by $\phi(\Gamma)$. In [23] Shalom and Willis used bounded generation to show that certain S-arithmetic groups have the outer commensurator-normalizer property. Let K be a global field, with ring of integers $\mathcal{O}$, and G an absolutely simple, simply connected algebraic group over K. Then let G be K-isotropic of rank at least two, and $\Gamma \subset G(K)$ commensurable with $G(\mathcal{O})$. With these assumptions they showed (Theorem 6.12) that if $G(\mathcal{O})$ is boundedly generated by unipotents then Γ has the outer commensurator-normalizer property.

Bounded generation is also related to the notion of SS-rigidity. We say that a

group G has SS-rigidity if it has only finitely many equivalence classes of complex fully reducible representations in each dimension.

Theorem 1.8 ([19])**.** *Let G be a group with the property that every finite index subgroup of G has finite abelianization. If G has bounded generation, then G is SS-rigid.*

Another application involves right-orderability. Morris and Lifschitz used bounded generation in [14] to show that certain groups are not right orderable, and thus have no nontrivial action on the line. Let K be an algebraic number field which is neither $\mathbb{Q}$ nor an imaginary quadratic extension of $\mathbb{Q}$. Let Γ be a finite index subgroup of $SL_2(\mathcal{O}_K)$. They showed that Γ has no nontrivial orientation preserving action on $\mathbb{R}$, using the bounded generation of $SL_2(\mathcal{O}_K)$. A discrete subgroup Γ of a Lie group G is called a lattice if G/Γ has finite volume, for example $SL_2(\mathbb{Z})$ is a lattice in $SL_2(\mathbb{R})$. It was shown that if it is true that any noncocompact lattice in $SL_3(\mathbb{R})$ or $SL_3(\mathbb{C})$ is boundedly generated by unipotents, then for any connected, semisimple Lie group G with finite center and $\mathbb{R}$-rank $G \geq 2$ if Γ is a noncocompact, irreducible lattice in G, then Γ has no nontrivial orientation-preserving action on $\mathbb{R}$.

Bounded generation has also been related to Kazhdan's Property (T). In particular it has been used to show that $SL_n(\mathbb{Z})$ has Property (T) without using the property that $SL_n(\mathbb{Z})$ is a lattice in $SL_n(\mathbb{R})$ and to give an explict Kazhdan constant. (This is explained in Chapter 4 of [2].)

1.2 Quaternion Algebras

In this section we introduce (generalized) quaternion algebras, some of their basic properties and the notion of an order. One reference for these basics is Chapter 1 of [8].

Definition. Let K be a field (of characteristic not 2) and $\alpha, \beta \in K^\times$. The quaternion algebra $\mathcal{D} = \left(\frac{\alpha, \beta}{K}\right)$ is the 4-dimensional K-algebra with basis $\{1, i, j, k\}$ and multiplication determined by $i^2 = \alpha$, $j^2 = \beta$, $ij = k$ and $ji = -k$.

There is a standard involution on $\mathcal{D}$, denoted by $\bar{\cdot}$, defined by

$$\overline{x_0 + x_1 i + x_2 j + x_3 k} = x_0 - x_1 i - x_2 j - x_3 k.$$

Notice that if $x \in K$, then $\bar{x} = x$, and if $x = x_1 i + x_2 j + x_3 k$, then $\bar{x} = -x$. We can show that $\overline{ab} = \bar{b}\bar{a}$. A simple computation verifies this for basis elements, and since $\bar{\cdot}$ is additive and K-linear the result follows.

For $x \in \mathcal{D}$ we can define its norm $N\colon \left(\frac{\alpha, \beta}{K}\right) \to K$ by $N(x) = x\bar{x}$. Taking $x = x_0 + x_1 i + x_2 j + x_3 k$ and multiplying we can see that

$$N(x) = x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2.$$

Notice that this can be viewed as a quadratic form on K^4.

Lemma 1.9. *For any $x, y \in \mathcal{D}$, $N(xy) = N(x)N(y)$.*

Proof. We can see that

$$N(xy) = xy\overline{xy} = xy\bar{y}\bar{x} = xN(y)\bar{x} = x\bar{x}N(y) = N(x)N(y)$$

since $N(y) \in K$. □

Notice that if $N(q) \neq 0$, then by construction we have $\frac{1}{N(q)} q\bar{q} = 1$, so $q^{-1} = \frac{1}{N(q)}\bar{q}$. If $q \neq 0$ and $N(q) = 0$ then q is a zero divisor and thus not invertible. This implies:

Lemma 1.10. *An element $q \in \left(\frac{\alpha, \beta}{K}\right)$ is invertible if and only if $N(q) \neq 0$. In particular, $\left(\frac{\alpha, \beta}{K}\right)$ is a division algebra if and only if $x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 = 0$ has no nonzero solutions over K.*

We first consider a simple example where $\mathcal{D}$ is not a division algebra.

Lemma 1.11. *Let* $\mathcal{D} = \left(\frac{\alpha^2, \beta}{K}\right)$, *for* $\alpha, \beta \in K^\times$. *Then* $\mathcal{D} \cong M_2(K)$.

Proof. We define a homomorphism $\phi\colon \left(\frac{\alpha^2, \beta}{K}\right) \to M_2(K)$ by taking

$$\phi(i) = \begin{bmatrix} \alpha & 0 \\ 0 & -\alpha \end{bmatrix}, \ \phi(j) = \begin{bmatrix} 0 & 1 \\ \beta & 0 \end{bmatrix}.$$

Then $\phi(i)^2 = \alpha^2 I$, $\phi(j)^2 = \beta I$ and $\phi(j)\phi(i) = -\phi(i)\phi(j)$. Since $\phi(i)$ and $\phi(j)$ satisfy the relations of the quaternion algebra this defines a homomorphism. We can also see that

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \frac{1}{2}(I + \frac{1}{\alpha}\phi(i)), \ \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2}(I - \frac{1}{\alpha}\phi(i)),$$
$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \frac{1}{2}(\phi(j) + \frac{1}{\alpha}\phi(i)\phi(j)), \ \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \frac{1}{2\beta}(\phi(j) - \frac{1}{\alpha}\phi(i)\phi(j))$$

so ϕ is surjective. Since the dimensions of $\mathcal{D}$ and $M_2(K)$ are both 4, ϕ is an isomorphism. □

We will later use that if $\tau_k : \mathcal{D} \to \mathcal{D}$ is a K-linear map fixing $1, i, j$ such that $\tau_k(k) = -k$, then

$$\phi(\tau_k(\phi^{-1}(X))) = \begin{bmatrix} \frac{1}{\beta} & 0 \\ 0 & 1 \end{bmatrix} X^t \begin{bmatrix} \beta & 0 \\ 0 & 1 \end{bmatrix}$$

since we can see from the proof of the previous lemma that $\phi \circ \tau_k \circ \phi^{-1}$ will fix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ and take $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ to $\begin{bmatrix} 0 & 0 \\ \beta & 0 \end{bmatrix}$.

Lemma 1.12. *Let* $\mathcal{D}$ *be a quaternion algebra, then either* $\mathcal{D}$ *is a division algebra, or* $\mathcal{D} \cong M_2(K)$.

Proof. Given Lemma 1.11 and Lemma 1.10 it suffices to show that if

$$x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2$$

has a nontrivial solution in K, then $\left(\frac{\alpha,\beta}{K}\right) \cong \left(\frac{y^2,z}{K}\right)$ for some $y, z \in K$. Let y_0, y_1, y_2, y_3 be such that

$$y_0^2 - \alpha y_1^2 - \beta y_2^2 + \alpha\beta y_3^2 = 0.$$

Then

$$y_0^2 - \alpha y_1^2 = \beta(y_2^2 - \alpha y_3^2),$$

implying that

$$N(y_0 + y_1 i) = \beta N(y_2 + y_3 i).$$

If $N(y_2 + y_3 i) = 0$ then α is a square in K and thus by Lemma 1.11, $\mathcal{D} \cong M_2(K)$. Assume $N(y_2 + y_3 i) \neq 0$, then

$$\beta = N(y_0 + y_1 i)N(y_2 + y_3 i)^{-1}.$$

Since N is multiplicative there exists $a, b \in K$ such that $\beta = N(a + bi)$. Let $j' = \frac{1}{\beta}(a + bi)j$, then

$$(j')^2 = \frac{1}{\beta^2} N(a + bi)j^2 = 1.$$

Notice that $ij' = -j'i$, and so $1, j', i, j'i$ forms a basis for a quaternion algebra, implying that $\mathcal{D} \cong \left(\frac{1,\alpha}{K}\right)$. Therefore by Lemma 1.11 we have that$\mathcal{D} \cong M_2(K)$. □

We now define the reduced norm for quaternions, and matrix algebras over quaternions. Notice that if L is a field extension of K and $\mathcal{D} = \left(\frac{\alpha,\beta}{K}\right)$, then

$$\mathcal{D} \otimes_K L \cong \left(\frac{\alpha,\beta}{L}\right).$$

Thus by Lemma 1.11 we have that

$$\mathcal{D} \otimes K(\sqrt{\alpha}) \cong M_2(K(\sqrt{\alpha})).$$

In particular there is an injective homomorphism $\phi\colon\ \mathcal{D} \to M_2(K(\sqrt{\alpha}))$, given by

$$x_0 + x_1 i + x_2 j + x_3 k \mapsto \begin{bmatrix} x_0 + x_1\sqrt{\alpha} & x_2 + x_3\sqrt{\alpha} \\ \beta(x_2 - x_3\sqrt{\alpha}) & x_0 - x_1\sqrt{\alpha} \end{bmatrix}.$$

We can extend this to an injective homomorphism $\phi_n\colon M_n(\mathcal{D}) \to M_{2n}(K(\sqrt{\alpha}))$. Define a determinant on $M_n(\mathcal{D})$ by $\det X = \det \phi(X)$ for $X \in M_n(\mathcal{D})$. This is also known as the reduced norm (note that the standard notation is Nrd not det). We notice that if $q \in M_1(\mathcal{D}) = \mathcal{D}$, the reduced norm

$$\begin{aligned} \det[q_0 + q_1 i + q_2 j + q_3 k] &= \det \phi(q) \\ &= (q_0 + q_1\sqrt{\alpha})(q_0 - q_1\sqrt{\alpha}) - \beta(q_2 - q_3\sqrt{\alpha})(q_2 + q_3\sqrt{\alpha}) \\ &= q_0^2 - \alpha q_1^2 - \beta q_2^2 + \alpha\beta q_3^2 \\ &= N(q). \end{aligned}$$

So it corresponds with our original norm. We define

$$SL_n(\mathcal{D}) = \{X \in M_n(\mathcal{D}) \mid \det X = 1\}.$$

To prove that $SL_n(\mathcal{O}_{\mathcal{D},S})$ has bounded generation, we will analyze its structure using elementary matrices. For ease of notation we let $[X]_{ij}$ denote the ijth entry of the matrix X.

An elementary matrix is a matrix with 1s on the diagonal, 0s elsewhere except for a single nonzero entry. We will use $E_{ij}(a)$ with $i \neq j$ to denote the elementary matrix given by

$$[E_{ij}(a)]_{lk} = \begin{cases} 1 & \text{if} \quad l = k \\ a & \text{if} \quad l = i \text{ and } k = j \\ 0 & \text{otherwise} \end{cases}.$$

We can see that $\phi(E_{ij}(\alpha))$ will be an upper or lower triangular matrix with 1s along the diagonal, so $\phi(E_{ij}(\alpha))$ has determinant 1, implying that $E_{ij}(a) \in SL_n(\mathcal{D})$ for all $a \in \mathcal{D}$, $i \neq j$.

Our first main result involves SL_n for an $\mathcal{O}_{K,S}$-order of a quaternion algebra, which we will now define. Let A be a finite-dimensional algebra over an algebraic number field K. An order in A is a subring O that is also an $\mathcal{O}_{K,S}$ lattice, i.e., O is a finitely generated $\mathcal{O}_{K,S}$-module which contains a basis for A as a vector space. An order is maximal if it is not contained in a larger order. (See section 1.5 in [17].)

In our case we let $\mathcal{D} = \left(\frac{\alpha,\beta}{K}\right)$ with $\alpha, \beta \in \mathcal{O}_{K,S}$. Let $S \subset V^K$ be finite with $V_\infty^K \subset S$. Define

$$\mathcal{O}_{\mathcal{D},S} = \{x_0 + x_1 i + x_2 j + x_3 k \mid x_i \in \mathcal{O}_S\}.$$

We define $SL_n(\mathcal{O}_{\mathcal{D},S}) = SL_n(\mathcal{D}) \cap M_n(\mathcal{O}_{\mathcal{D},S})$. Clearly $E_{ij}(\alpha) \in SL_n(\mathcal{O}_{\mathcal{D},S})$ for all α in $\mathcal{O}_{\mathcal{D},S}$.

As a preliminary lemma for Main Theorem 1 we prove a result concerning $E_{ij}(\mathcal{O}_{\mathcal{D},S}) := \{E_{ij}(\alpha) \mid \alpha \in \mathcal{O}_{\mathcal{D},S}\}$.

Lemma 1.13. *Fix i, j and S. There exists $g_1, \ldots, g_m \in SL_n(\mathcal{O}_{\mathcal{D},S})$ such that $E_{ij}(\mathcal{O}_{\mathcal{D},S}) \subset \langle g_1 \rangle \cdots \langle g_m \rangle$.*

Proof. If $S = V_\infty^K$ then $\mathcal{O}_{\mathcal{D},S} = \mathcal{O}_{\mathcal{D}}$ and $E_{ij}(\mathcal{O}_{\mathcal{D},S}) \cong \mathcal{O}_{\mathcal{D}}^+$ the additive group of $\mathcal{O}_{\mathcal{D}}$, which is a finitely generated abelian group and thus has bounded generation so $E_{ij}(\mathcal{O}_{\mathcal{D},S}) = \langle g_1 \rangle \cdots \langle g_m \rangle$ for $g_i \in E_{ij}(\mathcal{O}_{\mathcal{D},S})$. Assume that $S \neq V_\infty^K$. Then by Lemma 6 in [24] there exists $a \in \mathcal{O}_K$ such that $\mathcal{O}_S = \mathcal{O}_K\left[\frac{1}{a}\right]$, which implies that for any $x \in \mathcal{O}_{\mathcal{D},S}$ there exists $x_i \in \mathcal{O}_{\mathcal{D}}$ such that

$$x = \sum_{i=0}^{M} x_i a^{-i}.$$

Let $A = \mathrm{diag}(1, \ldots, 1, a, \ldots, 1/a, \ldots, 1)$ (i.e. $[A]_{ii} = a$, $[A]_{jj} = 1/a$ and $[A]_{ll} = 1$ for $l \neq i, j$.) Notice that $A \in SL_n(\mathcal{O}_{\mathcal{D},S})$ and that

$$E_{ij}(x) = A^{-M} E_{ij}\left(\sum_{i=0}^{n} x_i a^{2M-i}\right) A^M.$$

Thus $E_{ij}(\mathcal{O}_{\mathcal{D},S}) \subset \langle A \rangle \langle g_1 \rangle \cdots \langle g_m \rangle \langle A \rangle$ as desired. □

1.3 Orthogonal Groups

In this section we define properties that are used in [6] to show that some orthogonal groups have bounded generation. In the next section we introduce analogous properties for unitary groups. Throughout, K will be a field and W a finite-dimensional K-vector space.

Definition. A map $W \times W \to K$ denoted by $(x, y) \mapsto \langle x, y \rangle$ is a *bilinear form* if

$$\langle \alpha x, y \rangle = \alpha \langle x, y \rangle = \langle x, \alpha y \rangle ,$$

$$\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle ,$$

and

$$\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$$

for all $\alpha \in K$ and $x, y, z \in W$.

If we also have that $\langle x, y \rangle = \langle y, x \rangle$ for all $x, y \in W$, then $\langle \cdot, \cdot \rangle$ is called *symmetric*. We say $\langle \cdot, \cdot \rangle$ is *nondegenerate* if for every nonzero $x \in W$ there exists $y \in W$ such that $\langle x, y \rangle \neq 0$. A vector $x \in W$ is called *anisotropic* if $\langle x, x \rangle \neq 0$. The space W is called anisotropic if every nonzero vector in W is anisotropic, and is called isotropic otherwise.

Let $e_1, \ldots, e_n$ be a basis for W. Define $a_{ij} = \langle e_i, e_j \rangle$ and form the matrix

$$F = (a_{ij})_{1 \leq i,j \leq n}.$$

With respect to this basis we have that

$$\langle x_1 e_1 + \cdots + x_n e_n, y_1 e_1 + \cdots + y_n e_n \rangle = [x_1, \ldots, x_n] F \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} .$$

Notice that if $\langle \cdot, \cdot \rangle$ is symmetric then $F^t = F$. For any matrix F, we may define a bilinear form by $\langle x, y \rangle_F = x^t F y$.

Definition. Let $\langle \cdot, \cdot \rangle$ be a symetric bilinear form. We define the orthogonal group $O(W) = \{\sigma \in GL(W) \mid \langle \sigma x, \sigma y \rangle = \langle x, y \rangle \text{ for all } x, y \in W\}$.

If we fix a basis, then $O(W)$ can be identified with:

$$\begin{aligned} O_{n,F}(K) &= \{M \in GL_n(K) \mid \langle Mx, My \rangle = \langle x, y \rangle \text{ for all } x, y \in K^n\} \\ &= \{M \in GL_n(K) \mid M^t F M = F\}. \end{aligned}$$

We can also define $SO_{n,F}(K) = \{M \in O_{n,F}(K) \mid \det M = 1\}$.

Theorem 1.14 (Witt's Theorem version 1)**.** *Let W be a finite-dimensional K-vector space with a symmetric nondegenerate bilinear form $\langle \cdot, \cdot \rangle_F$. Assume we have two linearly independent sets of vectors $x_1, \ldots, x_r$, and $y_1, \ldots, y_r$ with $\langle x_i, x_j \rangle = \langle y_i, y_j \rangle$ for $1 \leq i, j \leq r$. Then there exists $\sigma \in O_{n,F}(K)$ such that $\sigma(x_i) = y_i$ for $1 \leq i \leq n$.*

This is Theorem 5.2 in [9].

Let $M \subset W$ be a maximal subspace of W such that all vectors of M are isotropic. Assume that N is another such subspace and $\dim M \leq \dim N$. There exists a subspace $N' \subseteq N$ with $\dim N' = \dim M$. By Witt's theorem there exists $\sigma \in O_{n,F}(K)$ such that $\sigma(N') = M$. Then $M \subseteq \sigma(N)$ and all vectors in $\sigma(N)$ are isotropic, so since M is maximal $M = \sigma(N)$ and $\dim M = \dim N$. Thus all such subspaces have the same dimension. We call this dimension the *Witt index* of W. Notice also that if V is nondegenerate that the Witt index is at most half the dimension of V since

$$\dim M^\perp = \dim V - \dim M,$$

but $M \subset M^\perp$ implying that

$$\dim M^\perp \leq \dim V - \dim M^\perp$$

so $2 \dim M^\perp \leq \dim V$.

Corollary 1.15. *Let W, $x_1, \ldots, x_r$, $y_1, \ldots, y_r$ be as in the theorem, and further assume that $2r + 1 \leq n$. Then there exists $\sigma \in SO_{n,F}(K)$ such that $\sigma(x_i) = y_i$ for $1 \leq i \leq n$.*

Proof. From the theorem we have that there is $\sigma' \in O_{n,F}(K)$ such that $\sigma'(x_i) = y_i$ for all $1 \leq i \leq r$. Since $\sigma' \in O_{n,F}(K)$, $\det \sigma' = \pm 1$. Assume $\det \sigma' = -1$. For any anisotropic $u \in W$ we can define a map $\sigma_u : W \to W$ by

$$\sigma_u(v) = v - 2\frac{\langle u, v\rangle}{\langle u, u\rangle}u.$$

Then $\sigma_u(u) = -u$, and if $\langle u, v\rangle = 0$, $\sigma_u(v) = v$, implying $\det \sigma_u = -1$. We can also see that $\sigma_u \in O_{n,F}(K)$, since for arbitrary vectors $v_1, v_2 \in W$,

$$\begin{aligned}\langle \sigma_u(v_1), \sigma_u(v_2)\rangle &= \left\langle v_1 - 2\frac{\langle u, v_1\rangle}{\langle u, u\rangle}u, v_2 - 2\frac{\langle u, v_2\rangle}{\langle u, u\rangle}u \right\rangle \\ &= \langle v_1, v_2\rangle - 2\frac{\langle u, v_1\rangle \langle u, v_2\rangle}{\langle u, u\rangle} - 2\frac{\langle u, v_2\rangle \langle v_1, u\rangle}{\langle u, u\rangle} + 4\frac{\langle u, v_1\rangle \langle u, v_2\rangle}{\langle u, u\rangle} \\ &= \langle v_1, v_2\rangle .\end{aligned}$$

Thus it suffices to show there exists $w \in \operatorname{span}(x_1, \ldots, x_r)^\perp$ which is anisotropic, since then $\sigma = \sigma'\sigma_w$ will have the desired properties. The dimension of $\operatorname{span}(x_1, \ldots, x_r)^\perp$ is at least $n - r$, but this means that the dimension is at least $r + 1$, and thus contains anisotropic vectors since the Witt index of W is at most r, so the desired w exists. □

Now assume K is an algebraic number field. Let W be a vector space with a nondegenerate, symmetric bilinear form and basis $e_1, \ldots, e_n$. Let $\mathcal{L}$ be the $\mathcal{O}_K$-lattice defined by this basis. Then we can define $GL_n(\mathcal{L})$ and $O_{n,F}(\mathcal{L})$ as the subgroups of $GL_n(K)$ and $O_{n,F}(K)$, respectively, that fix this lattice. Similarly we can consider the lattice $\mathcal{L}_v$ over $\mathcal{O}_v$ with $v \in V_f^K$. Let $\bar{x}$ denote the image of $x \in \mathcal{L}_v$ under the map $\mathcal{L}_v \to \mathcal{L}_v / \mathfrak{p}_v \mathcal{L}_v$ and let $k_v = \mathcal{O}_v / \mathfrak{p}_v$.

Theorem 1.16 (Witt's Theorem for local lattices)**.** *Let* $\{a_1, \ldots, a_m\}$ *and* $\{b_1, \ldots, b_m\}$ *be elements of* $\mathcal{L}_v$ *such that* $\{\bar{a}_1, \ldots, \bar{a}_m\}$ *and* $\{\bar{b}_1, \ldots, \bar{b}_m\}$ *are each linearly independent sets over* k_v *and* $\langle a_i, a_j \rangle_F = \langle b_i, b_j \rangle_F$ *for all* $1 \leq i \leq j \leq m$*. Then if* $\det F \in \mathcal{O}_v^\times$ *and* $|2|_v = 1$ *then there exists* $\sigma \in O_{n,F}(\mathcal{L}_v)$ *such that* $\sigma(a_i) = b_i$ *for all* $i = 1, \ldots, m$*.*

This is theorem 2.24 in [6].

1.4 Unitary Groups

We now consider unitary groups. Let K be a field, $L = K(\sqrt{d})$ be a quadratic extension, and τ be the involution taking $\sqrt{d}$ to $-\sqrt{d}$. We also fix a finite-dimensional vector space W over L.

Definition. A map $\langle \cdot, \cdot \rangle : W \times W \to L$ is called a *sesquilinear form* if it satisfies the following:

- $\langle \alpha x, y \rangle = \tau(\alpha) \langle x, y \rangle$
- $\langle x, \alpha y \rangle = \alpha \langle x, y \rangle$
- $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$
- $\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$

for all $x, y, z \in W$, $\alpha \in L$.

We call $\langle \cdot, \cdot \rangle$ *Hermitian* if

$$\tau(\langle y, x \rangle) = \langle x, y \rangle$$

and *skew-Hermitian* if

$$\tau(\langle y, x \rangle) = - \langle x, y \rangle .$$

All our forms will be Hermitian or skew-Hermitian.

As for bilinear forms, we call $\langle \cdot, \cdot \rangle$ *nondegenerate* if for every nonzero $x \in W$, there exists $y \in W$ such that $\langle x, y \rangle \neq 0$. An element $x \in W$ is called *anisotropic* if $\langle x, x \rangle \neq 0$ and *isotropic* if $\langle x, x \rangle = 0$. A subspace $V \subset W$ is called *anisotropic* if every element of V is anisotropic, and is called *isotropic* otherwise; if all elements of V are isotropic the space is called *totally isotropic*.

We now prove a useful fact about isotropic spaces that will be used in Chapter 3.

Lemma 1.17. *Let W be a finite-dimensional L-vector space with a non-degenerate Hermitian sesquilinear form $\langle \cdot, \cdot \rangle$. If W is isotropic, then for any $k \in K$, there exists an element $w \in W$ such that $\langle w, w \rangle = k$.*

Proof. Since W is isotropic there exists nonzero $v \in W$ such that $\langle v, v \rangle = 0$. Let $e_1, \ldots, e_n$ be an orthogonal basis of W (see Theorem 10.10 in [18] for the existence of such a basis and write $v = v_1 e_1 + \cdots + v_n e_n$. Since $v \neq 0$, $v_i \neq 0$ for some i. Define

$$v' = v_1 e_1 + \cdots + (-v_i) e_i + \cdots + v_n e_n.$$

Then $\langle v', v' \rangle = 0$, and $\langle v, v' \rangle \neq 0$. Set $w = v + \dfrac{k}{2 \langle v, v' \rangle} v'$. Then we can see that

$$\begin{aligned} \langle w, w \rangle &= \left\langle v + \frac{k}{2 \langle v, v' \rangle} v', v + \frac{k}{2 \langle v, v' \rangle} v' \right\rangle \\ &= \frac{k}{2\tau(\langle v, v' \rangle)} \langle v', v \rangle + \frac{k}{2 \langle v, v' \rangle} \langle v, v' \rangle \\ &= k \end{aligned}$$

as desired. □

We define the unitary group

$$U(W) = \{ g \in GL(W) \mid \langle gx, gy \rangle = \langle x, y \rangle \text{ for all } x, y \in W \}.$$

Fix a basis $e_1, \ldots, e_n$ of W and let $F = (\langle e_i, e_j \rangle)$. For a matrix $M = (m_{ij})$ let $\tau(M) = (\tau(m_{ij}))$ and $M^* = \tau(M)^t$. Then we can express the unitary group as

$$U_{n,F}(L) = \{ M \in GL_n(L) \mid M^* F M = F \}.$$

We define

$$SU_{n,F} = \{M \in U_{n,F} \mid \det M = 1\}.$$

Theorem 1.18 (Witt's theorem for unitary groups)**.** *Let W be a finite-dimensional vector space over L with a Hermitian (or skew-Hermitian) nondegenerate sesquilinear form $\langle \cdot, \cdot \rangle$. Assume we have two linearly independent sets of vectors $x_1, \dots x_r$ and $y_1, \dots, y_r$ of W such that $\langle x_i, x_j \rangle = \langle y_i, y_j \rangle$ for $1 \leq i, j \leq r$. Then there exists $\sigma \in U(W)$ such that $\sigma x_i = y_i$ for all $1 \leq i \leq r$.*

This is Theorem 10.12 in [9].

As before, we define the notion of the Witt index. If $M \subset W$ is a maximal totally isotropic subspace of W, then $\dim_L M$ is called the *Witt index* of W. The same argument used in the orthogonal case shows that Witt's theorem implies that the Witt index is well-defined.

Corollary 1.19. *Let $x_1, \dots x_r$, $y_1, \dots, y_r$ be as in Theorem 1.18. If $2r + 1 \leq n$ then there exists $\sigma \in SU_{n,F}(L)$ such that $\sigma x_i = y_i$ for all $1 \leq i \leq r$.*

Proof. Let σ' be an element of $U_{n,F}(L)$ given by Theorem 1.18. Let $w \in L^n$ be anisotropic with $\langle x_i, w \rangle = 0$ for all $1 \leq i \leq r$. Such an element exists because $2r + 1 \leq n$ and W is nondegenerate. For $l \in L$, $w \in W$ define $\sigma_{l,w} \colon W \to W$ by

$$\sigma_{l,w}(v) = v + l\frac{\langle w, v \rangle}{\langle w, w \rangle} w.$$

Then $\sigma_{l,w}$ is a linear map which fixes all $v \in W$ with $\langle w, v \rangle = 0$. We also can see that $\sigma_{l,w}(w) = (1 + l)w$. Thus $\det \sigma_{l,w} = 1 + l$ and $\sigma_{l,w} \in U(W)$ if $(1 + \tau(l))(1 + l) = 1$. Let

$$l = (\det \sigma')^{-1} - 1,$$

then

$$\begin{aligned}(1+\tau(l))(1+l) &= (\det\tau(\sigma'))^{-1}(\det\sigma')^{-1} \\ &= (\det(\tau(\sigma')\sigma'))^{-1} \\ &= (\det(\tau(\sigma')F\sigma'F^{-1}))^{-1} \\ &= 1\end{aligned}$$

since $\sigma' \in U(W)$. By construction $\det\sigma_{l,w} = (\det\sigma')^{-1}$. Thus $\sigma = \sigma'\sigma_{l,w}$ has the desired properties. □

Define an injective homomorphism $\phi\colon L^\times \to GL_2(K)$ by

$$\phi(x+\sqrt{d}y) \mapsto \begin{bmatrix} x & dy \\ y & x \end{bmatrix}.$$

Note that the image of this map is an algebraic group as it can be described as the set of $X \in GL_n$ such that $[X]_{11} = [X]_{22}$ and $[X]_{12} = d[X]_{21}$. The map ϕ extends to an injective homomorphism $GL_n(L) \to GL_{2n}(K)$ given by $(x_{ij}) \mapsto (\phi(x_{ij}))$. By identifying $U_{n,F}$ with its image under this map we can see that $U_{n,F}$ is an algebraic group over K.

Alternatively we can view $U_{n,F}$ as a variety defined over K by expressing the hermitian matrix F as

$$F = F_1 + \sqrt{d}F_2$$

(with $F_1 \in M_n(K)$ symmetric, $F_2 \in M_n(K)$ skew-symmetric.) Then the map $U_{n,F}(L) \to (M_n(K))^2$ given by $X + Y\sqrt{d} \mapsto (X,Y)$ is an injection whose image is

$$\begin{aligned}&\{(X,Y) \in (M_n(K))^2 \mid (X-\sqrt{d}Y)^tF(X+\sqrt{d}Y) = F\} \\ &= \{(X,Y) \in (M_n(K))^2 \mid X^tF_1X - dY^tF_1Y + dX^tF_2Y - dY^tF_2X = F_1 \\ &\qquad\qquad \text{and } X^tF_1Y - Y^tF_1X + X^tF_2X - dY^tF_2Y = F_2\}.\end{aligned}$$

We define the multiplication on $(M_n(K))^2$ by $(X,Y)*(Z,W) = (XZ + dYW, XW + YZ)$.

We will need a lattice version of Witt's Theorem for unitary groups. Let $v \in V_f^K$. Let $L_v := L \otimes_K K_v$ (note that this is not necessarily a field), and define $\tau_v \colon L_v \to L_v$ by $\tau_v(x \otimes y) = \tau(x) \otimes y$. The unitary group $U_{n,F}(L_v)$ acts on a n-dimensional L_v-module (which is a $2n$-dimensional K_v-vector space). Let $\mathcal{O}_{v,L} := \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_v$. We let $\mathcal{L}_v = (\mathcal{O}_{v,L})^n$, an n-dimensional free $\mathcal{O}_{v,L}$-module. Let $\mathfrak{p}_{v,L}$ be the ideal generated by $1 \otimes \mathfrak{p}_v$ in $\mathcal{O}_{v,L}$, $\ell_v = \mathcal{O}_{v,L}/\mathfrak{p}_{v,L}$, and for $a \in \mathcal{L}_v$ let $\bar{a}^{(v)}$ denote the image of a under the map $\mathcal{L}_v \to \mathcal{L}_v / \mathfrak{p}_{v,L}\mathcal{L}_v$.

Theorem 1.20 (Witt's theorem for local lattices, unitary case)**.** *Let $v \in V_f^K$ such that $|2|_v = 1$, and $|d|_v = 1$. Let $F \in M_n(\mathcal{O}_{v,L})$ be a Hermitian matrix with $\det F \in \mathcal{O}_v^\times$. Let $a_1, \ldots, a_m,\ b_1, \ldots, b_m \in \mathcal{L}_v$ with $\langle a_i, a_j\rangle = \langle b_i, b_j\rangle$ for all $1 \le i, j \le m$. Assume $\operatorname{span}_{\ell_v}(\bar{a}_1^{(v)}, \ldots, \bar{a}_m^{(v)})$ and $\operatorname{span}_{\ell_v}(\bar{b}_1^{(v)}, \ldots, \bar{b}_m^{(v)})$ are m-dimensional free modules. Then there exists $g \in U_{n,F}(\mathcal{O}_{v,L})$ such that $ga_i = b_i$ for all $1 \le i \le m$.*

We consider two cases. In the first case L_v is a field. In the second case we have $L_v \cong K_v \otimes K_v$.

Case 1: $v \in V_f^K$ is such that L_v is a field, i.e., $L_v = K_v[\sqrt{d}]$. In this case the proof is built from a proposition and a few lemmas. Notice that in this case ℓ_v is a field which is a quadratic extension of k_v. Throughout we will let π_v denote a fixed generator of $\mathfrak{p}_{v,L}$. Notice that since $|d|_v = 1$ we may take $\pi_v \in \mathcal{O}_v$.

Proposition 1.21. *Let L be a field with involution τ, $K = L^\tau$ and $[L : K] = 2$. Let W be an n-dimensional vector space over L with non-degenerate Hermitian inner product $\langle \cdot, \cdot \rangle$. Let*

$$R = \{Y \in \operatorname{End}(V) \mid \langle x, Yy\rangle + \langle Yx, y\rangle = 0 \text{ for all } x, y \in V\}.$$

For $x_1, \ldots, x_m \in V$ linearly independent, let

$$\Omega = \{(y_1, \ldots, y_m) \in V^m \mid \langle x_i, y_j \rangle + \langle y_i, x_j \rangle = 0 \text{ for all } 1 \leq i, j \leq m\}$$

and

$$\Gamma = \{(Yx_1, \ldots, Yx_m) \mid Y \in R\}.$$

Then $\Omega = \Gamma$.

Proof. Notice that R, Ω and Γ are K-vector spaces. By the construction of R it is clear that $\Gamma \subset \Omega$. Thus if we show that $\dim_K \Gamma = \dim_K \Omega$ then the two are equal. Let $V = \operatorname{span}_L(x_1, \ldots, x_m)$,

$$T = \{Y \in R \mid Yx_1 = \cdots = Yx_m = 0\}.$$

Then $\dim_K \Gamma = \dim_K R - \dim_K T$. We first compute $\dim_K R$. Fix a basis of W and let F be the matrix of $\langle \cdot, \cdot \rangle$ in this basis. We can see that R consists of matrices $Y \in M_n(L)$ such that $Y^*F = -FY$. Let H (respectively H') denote the subspace of Hermitian (respectively skew-Hermitian) matrices in $M_n(L)$. Then $M_n(L) = H \oplus H'$ since $H \cap H' = 0$ and for every $X \in M_n(L)$, $X = (\frac{X+X^*}{2}) + (\frac{X-X^*}{2})$, i.e., X is the sum of an element of H and an element of H'. We can also see that $\dim_K H = \dim_K H'$ since the map $X \mapsto \sqrt{d}X$ takes the space H to H'. Therefore $\dim_K H' = \frac{1}{2} \dim_K M_n(L) = n^2$. Finally $\dim_K H' = \dim_K R$ since the map $X \mapsto F^{-1}X$ takes the space H' to R. Therefore $\dim_K R = n^2$.

We can view T as

$$\{Y \in M_n(L) \mid Y^*F = -FY \text{ and } Yv = 0 \text{ for all } v \in V\}$$

and express V as $V_1 \perp V_0$ where V_1 is nondegenerate and $V_0 = V^{\perp}$. Fix an orthogonal basis $e_1, \ldots, e_k$ for V_1 and let $v_{k+1}, \ldots v_m$ be an arbitrary basis of V_0. By the construction of V_0, $v_{k+1}, \ldots, v_m \in V_1^{\perp}$ which is nondegenerate. Therefore there exist

$\hat{v}_{k+1}, \ldots, \hat{v}_m \in V_1^{\perp}$ such that

$$\mathrm{span}_L(v_{k+1}, \ldots v_m, \hat{v}_{k+1}, \ldots \hat{v}_m) \cong \mathrm{span}(v_{k+1}, \hat{v}_{k+1}) \perp \cdots \perp \mathrm{span}(v_m, \hat{v}_m)$$

where each $v_k, \hat{v}_j$ forms a hyperbolic pair. Thus W can be written as

$$W = V_1 \perp (V_0 \oplus \mathrm{span}(\hat{v}_{k+1}, \ldots, \hat{v}_m) \perp V_2.$$

Since Y anhilates V there exists a basis and matrices F_1, F_2 and Y_{ij} with $1 \leq i \leq 4$, $j = 1, 2$ such that:

$$F = \begin{bmatrix} F_1 & 0 & 0 & 0 \\ 0 & 0 & I_{m-k} & 0 \\ 0 & I_{m-k} & 0 & 0 \\ 0 & 0 & 0 & F_2 \end{bmatrix}, Y = \begin{bmatrix} 0 & 0 & Y_{11} & Y_{12} \\ 0 & 0 & Y_{21} & Y_{22} \\ 0 & 0 & Y_{31} & Y_{32} \\ 0 & 0 & Y_{41} & Y_{42} \end{bmatrix}$$

so

$$Y^*F = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ Y_{11}^*F_1 & Y_{31}^* & Y_{21}^* & Y_{41}^*F_2 \\ Y_{12}^*F_1 & Y_{32}^* & Y_{22}^* & Y_{42}^*F_2 \end{bmatrix}$$

and

$$FY = \begin{bmatrix} 0 & 0 & F_1Y_{11} & F_1Y_{12} \\ 0 & 0 & Y_{31} & Y_{32} \\ 0 & 0 & Y_{21} & Y_{22} \\ 0 & 0 & F_2Y_{41} & F_2Y_{42} \end{bmatrix}.$$

Since F is invertible we have that Y_{11}, Y_{12}, Y_{31} and Y_{32} are all 0. We also have that $Y_{21} = -Y_{21}^*$, $F_2Y_{41} = -Y_{22}^*$ and $F_2Y_{42}^* = -Y_{42}^*F_2$. It is clear Y_{41} is completely determined by Y_{22}, and Y_{22} can be aribtrary, so the dimension of the K-subspace consisting of possible Y_{22}s is $Y_{22} = 2(m-k)(n-2m+k)$. By our previous argument the dimension

of the K-subspace consisting of possible Y_{21}s is $(m-k)^2$ and $\dim_K Y_{42} = (n-2m+k)^2$. Therefore

$$\begin{aligned}\dim_K T &= (m-k)^2 + 2(m-k)(n-2m+k) + (n-2m+k)^2 \\ &= ((m-k) + (n-2m+k))^2 \\ &= (n-m)^2\end{aligned}$$

and thus

$$\dim_K \Gamma = \dim_K R - \dim_K T = n^2 - (n-m)^2 = 2mn - m^2.$$

For each i from 1 to m define a linear map $f_i \colon W \to L$ by $f_i(w) = \langle x_i, w\rangle$ for all $w \in W$. Because the x_is are linearly independent and W is nondegenerate, the f_is are linearly independent. We define $\Phi \colon W^m \to M_m(L)$ by

$$\Phi(w_1, \ldots, w_m) = (f_i(w_j))_{1\le i,j\le m}.$$

Since the f_i are linearly independent their span is an m-dimensional L-vector space and $\dim_L(\Phi(W^m)) = m^2$, so Φ is surjective. We can express

$$\Omega = \{(y_1, \ldots, y_m) \in W^m \mid \Phi(y_1, \ldots, y_m) + \Phi(y_1, \ldots, y_m)^* = 0\}$$

since

$$f_i(y_j) + \tau(f_j(y_i)) = \langle x_i, y_j\rangle + \tau(\langle x_j, y_i\rangle) = \langle x_i, y_j\rangle + \langle y_j, x_i\rangle .$$

Let

$$U = \{X \in M_m(L) \mid X + X^* = 0\}.$$

Then

$$\dim_K \Omega = \dim_K \ker \Phi + \dim_K U.$$

From previous arguments $\dim_K U = m^2$. Since

$$\ker \Phi = \{(w_1, \ldots, w_m) \mid f_i(w_j) = 0 \text{ for all } i, j\},$$

we have that $\dim_K \ker \Phi = m \dim_K V^\perp = 2m(n-m)$. Therefore

$$\dim \Omega = 2mn - 2m^2 + m^2 = 2mn - m^2$$

which is the dimension of Γ. □

Lemma 1.22. *Let $v \in V_f^K$ be as in the theorem and satisfying $L_v = K_v[\sqrt{d}]$. Let $F \in M_n(\mathcal{O}_{v,L})$ be a Hermitian matrix and suppose that $\det F \in \mathcal{O}_v^\times$. Given an integer $l \geq 0$ and a matrix X in $M_n(\mathcal{O}_{v,L})$ satisfying*

$$X^*FX \equiv F \pmod{\mathfrak{p}_{v,L}^l}$$

there exists $Y \in M_n(\mathcal{O}_{v,L})$ such that

$$Y^*FY \equiv F \pmod{\mathfrak{p}_{v,L}^{l+1}}$$

and $Y \equiv X \pmod{\mathfrak{p}_{v,L}^l}$.

Proof. By assumption $X^*FX - F = \pi_v^l A$ for some matrix $A \in M_n(\mathcal{O}_{v,L})$. Clearly, $A^* = A$. The requirement that $Y \equiv X \pmod{\mathfrak{p}_{v,L}^l}$ implies that Y must be of the form $X + \pi_v^l Z$ for $Z \in M_n(\mathcal{O}_{v,L})$. Computing, we see that

$$\begin{aligned} Y^*FY &= X^*FX + \pi_v^l(Z^*FX + X^*FZ) + \pi_v^{2l} Z^*FZ \\ &\equiv F + \pi_v^l(-A + Z^*FX + X^*FZ) \pmod{\mathfrak{p}_{v,L}^{l+1}}. \end{aligned}$$

Thus, it remains to find a matrix Z such that

$$Z^*FX + X^*FZ \equiv A \pmod{\mathfrak{p}_{v,L}}.$$

Since $\det F \in \mathcal{O}_v^\times$ and

$$F^{-1}X^*FX \equiv I \pmod{\mathfrak{p}_{v,L}^l}$$

we have that $X^{-1} \in M_n(\mathcal{O}_{v,L})$. Let $Z = ((FX)^*)^{-1}(\frac{1}{2}A)$. Since $|2|_v = 1$ we have that $Z \in M_n(\mathcal{O}_{v,L})$. Then

$$Z^*FX + X^*FZ = (\frac{1}{2}A^*) + \frac{1}{2}A = A$$

as desired. □

Lemma 1.23. *Let $v \in V_f^K$ as in Lemma 1.22. For any integer $l \geq 1$ and any matrix $X \in M_n(\mathcal{O}_{v,L})$ such that $X^*FX \equiv F \pmod{\mathfrak{p}_{v,L}^l}$ there exists $\hat{X} \in U_{n,F}(\mathcal{O}_{v,L})$ satisfying $\hat{X} \equiv X \pmod{\mathfrak{p}_{v,L}^l}$.*

Proof. Applying Lemma 1.22 iteratively we construct a sequence $X = X_l, X_{l+1}, \ldots$ such that

$$X_k^* F X_k \equiv F \pmod{\mathfrak{p}_{v,L}^k}$$

and $X_k \equiv X_{k+1} \pmod{\mathfrak{p}_{v,L}^k}$. This is a Cauchy sequence since $|X_k - X_{k+1}|_v \leq |\pi_v|_v^k$. Since L_v is complete the sequence has a limit, $\hat{X}$. Since each X_k is contained in $M_n(\mathcal{O}_{v,L})$, we have that $\hat{X}$ is in $M_n(\mathcal{O}_{v,L})$. Similarly, since $\hat{X} \equiv X_k \pmod{\mathfrak{p}_{v,L}^k}$, we have that $\hat{X}^* F \hat{X} \equiv F \pmod{\mathfrak{p}_{v,L}^k}$ for all $k \geq l$, so $\hat{X}^* F \hat{X} = F$ and $\hat{X} \in U_{n,F}(\mathcal{O}_{v,L})$.

□

Lemma 1.24. *Let v be as in Lemma 1.22 and let $a_1, \ldots, a_m, b_1, \ldots, b_m$ be as in the theorem. If $a_i - b_i \in \mathfrak{p}_{v,L}^l \mathcal{L}_v$, for all $1 \leq i \leq m$, then there exists $X \in M_n(\mathcal{O}_{v,L})$ such that*

$$X \equiv E_n \pmod{\mathfrak{p}_{v,L}^l}, \; X^* F X \equiv F \pmod{\mathfrak{p}_{v,L}^{l+1}}$$

and $X a_i \equiv b_i \pmod{\mathfrak{p}_{v,L}^{l+1}}$ for all $1 \leq i \leq m$.

Proof. We can write $b_i = a_i + \pi_v^l c_i$ for some c_i in $\mathcal{L}_v$. Then

$$\langle b_i, b_j \rangle = \left\langle a_i + \pi_v^l c_i, a_j + \pi_v^l c_j \right\rangle = \langle a_i, a_j \rangle + \pi_v^l (\langle c_i, a_j \rangle + \langle a_i, c_j \rangle) + \pi_v^{2l} \langle c_i, c_j \rangle,$$

so $\langle c_i, a_j \rangle + \langle a_i, c_j \rangle \equiv 0 \pmod{\mathfrak{p}_{v,L}}$. It sufficies to find a matrix $Y \in M_n(\mathcal{O}_{v,L})$ such that $Y a_i \equiv c_i \pmod{\mathfrak{p}_{v,L}}$ and $Y^* F + F Y \equiv 0 \pmod{\mathfrak{p}_{v,L}}$, because in that case $X = E_n + \pi_v^l Y$ has the desired qualities. The existence of such a Y follows from Proposition 1.21 by leting $x_i = a_i$, $L = \ell_v$, $K = k_v$. Since

$$\left\langle \bar{a}_i^{(v)}, \bar{c}_j^{(v)} \right\rangle + \left\langle \bar{c}_i^{(v)}, \bar{a}_j^{(v)} \right\rangle = 0,$$

we have that $(\bar{c_1}^{(v)}, \ldots, \bar{c_m^{(v)}}) \in \Omega$, and thus is in Γ so there exists $\bar{Y}^{(v)} \in M_n(\ell_v)$ such that $\bar{Y}^{(v)}(\bar{a}_i^{(v)}) = \bar{c}_i^{(v)}$ and

$$(\bar{Y}^{(v)})^* \bar{F}^{(v)} + \bar{Y}^{(v)} \bar{F}^{(v)} = 0.$$

Lifting we get an appropriate $Y \in M_n(\mathcal{O}_{v,L})$. □

Proof. (of the first case of Theorem 1.20) Applying Theorem 1.18 to the $\bar{a_i}^{(v)}$s, $\bar{b_i}^{(v)}$s gives an $\bar{X} \in U_{n,\bar{F}}(\ell_v)$ such that $\bar{X}\bar{a_i}^{(v)} = \bar{b_i}^{(v)}$. Lifting we obtain $X_0 \in M_n(\mathcal{O}_{v,L})$ such that $X_0 a_i \equiv b_i \pmod{\mathfrak{p}_{v,L}}$ and $X_0^* F X_0 \equiv F \pmod{\mathfrak{p}_{v,L}}$. By Lemma 1.23 there exists $X_1 \in U_{n,F}(\mathcal{O}_{v,L})$ such that $X_0 \equiv X_1 \pmod{\mathfrak{p}_{v,L}}$, so $X_1 a_i \equiv b_i \pmod{\mathfrak{p}_{v,L}}$. Assume that we have found $X_1, \ldots, X_k \in U_{n,F}(\mathcal{O}_{v,L})$ such that $X_l \equiv X_{l+1} \pmod{\mathfrak{p}_{v,L}^{l+1}}$ and $X_l(a_i) \equiv b_i \pmod{\mathfrak{p}_{v,L}^{l}}$. By applying the Lemma 1.24 to $\{X_k(a_1), \ldots, X_k(a_m)\}$ and $\{b_1, \ldots, b_m\}$ there exists Y such that

$$Y \equiv E_n \pmod{\mathfrak{p}_{v,L}^{k}},$$

$$Y^* F Y \equiv F \pmod{\mathfrak{p}_{v,L}^{k+1}}$$

and

$$Y(X_k(a_i)) \equiv b_i \pmod{\mathfrak{p}_{v,L}^{k+1}}.$$

Then by Lemma 1.23 there exists $X_{k+1} \in U_{n,F}(\mathcal{O}_{v,L})$ such that $X_{k+1} \equiv Y X_k \pmod{\mathfrak{p}_{v,L}^{k+1}}$. The X_i's form a cauchy sequence. Let X be the limit of the X_is. We have that X is in $U_{n,F}(\mathcal{O}_{v,L})$ and $Xa_i = b_i$ for all i as desired.

Before proving case 2 we prove a lemma which has a similar flavor to the proof of case 1.

Lemma 1.25. *Let $f_1, \ldots, f_n \in \mathcal{O}_v[x_1, \ldots, x_m]$ such that $f_i = a_{i0} + \sum a_{ij} x_j$ and $n \leq m$. Assume the image of $\{f_1, \ldots, f_n\}$ under the map $\mathcal{O}_v \to k_v$ has rank n. For any $y_1, \ldots, y_m \in \mathcal{O}_v$ such that $f_i(y_1, \ldots, y_m) \equiv 0 \pmod{\mathfrak{p}_v}$ for all $1 \leq i \leq n$ there*

exists $\hat{y}_1, \ldots, \hat{y}_m \in \mathcal{O}_v$ *such that* $f_i(\hat{y}_1, \ldots, \hat{y}_m) = 0$ *and* $y_i \equiv \hat{y}_i \pmod{\mathfrak{p}_v}$ *for all* $1 \leq i \leq n$.

Proof. First we note that since the image of $f_1, \ldots, f_n$ has rank n in k_v there exists linear equations $f_{n+1}, \ldots, f_m$, with $f_i = a_{i0} + \sum a_{ij}x_j$ such that $f_i(y_1, \ldots, y_m) = 0$ for all $n+1 \leq i \leq m$ and $\{f_1, \ldots, f_m\}$ has rank n. Let $A = (a_{ij})$ be the matrix of coefficients, $x = \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$, $a = \begin{bmatrix} a_{10} \\ \vdots \\ a_{m0} \end{bmatrix}$ and $y = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$. With this notation, we are trying to find a solution to $Ax + a = 0$ such that $x \equiv y \pmod{\mathfrak{p}_v}$. Since $f_1, \ldots, f_m$ has rank m in k_v, there exists $A' \in M_m[\mathcal{O}_v]$ such that $AA' \equiv I \pmod{\mathfrak{p}_v}$. We claim that given $y^{(k)}$ such that $Ay^{(k)} + a \equiv 0 \pmod{\mathfrak{p}_v^k}$ there exists $y^{(k+1)}$ such that $y^{(k)} \equiv y^{(k+1)} \pmod{\mathfrak{p}_v^k}$ and $Ay_{k+1} + a \equiv 0 \pmod{\mathfrak{p}_v^{k+1}}$. Since $Ay^{(k)} + a \equiv 0 \pmod{\mathfrak{p}_v^k}$, there exists $b \in \mathcal{O}_v^n$ such that $Ay^{(k)} + a = \pi_v^k b$. Let $y^{(k+1)} = y^{(k)} - \pi_v^k A'b$. Then

$$Ay^{(k+1)} + a = Ay^{(k)} + a - \pi_v^k AA'b = \pi_v^k(b - AA'b)$$

and since $AA' \equiv I \pmod{\mathfrak{p}_v}$ we have that $Ay^{(k+1)} + a \equiv 0 \pmod{\mathfrak{p}_v^{k+1}}$. Thus we can construct a Cauchy sequence $y^{(1)} = y, y_2, \ldots$. Let $\hat{y}$ be the limit of this sequence, we can see that $A\hat{y} + a = 0$ as desired. □

Case 2 of the proof of Theorem 1.20: Let $v \in V_f^K$ such that $L_v \cong K_v \oplus K_v$. We now give the isomorphism explicitly. Assume $v \in V_f^K$ is a valuation such that d is square in K_v. Let $t \in K_v$ be an element such that $t^2 = d$. Define an isomorphism $\phi\colon L_v \to K_v \oplus K_v$ by $\phi((a + b\sqrt{d}) \otimes k) = (k(a+bt), k(a-bt))$. Notice that $\phi(\tau(\phi^{-1}(x,y))) = (y,x)$. and that if $x \in \mathcal{O}_{v,L}$, we have that $\phi(x) \in \mathcal{O}_v \oplus \mathcal{O}_v$.

Since the $\bar{a}_i^{(v)}$ are linearly independent there exists a basis $e_1, \ldots, e_n$ such that $e_i = a_i$ for all $1 \leq i \leq m$.

Notice that the isomorphism defined above extends to a map $L_v^n \to (K_v \oplus K_v)^n$ via $\phi(\sum c_i e_i) = \sum \phi(c_i)(e_i, e_i)$, and similarly extends to a map $M_n(L_v) \to M_n(K_v) \oplus$

$M_n(K_v)$. Let $(F_1, F_2) = \phi(F)$. Since F is Hermitian, we have that $F_1^t = F_2$. For $x, y \in \mathcal{L}_v$, if $\phi(x) = (x_1, x_2)$ and $\phi(y) = (y_1, y_2)$ then

$$\phi(\langle x, y\rangle) = (x_2^t F_1 y_1, y_1^t F_2 x_2).$$

Let $X \in U_{n,F}(L_v)$. We have $X^* F X = F$, thus if $\phi(X) = (X_1, X_2)$ we see that

$$(X_2^t, X_1^t)(F_1, F_2)(X_1, X_2) = (F_1, F_2)$$

implying $X_2^t F_1 X_1 = F_1$. Therefore $X_2 = F_2^{-1}(X_1^t)^{-1} F_2$. This implies that finding $g \in U_{n,F}(\mathcal{O}_{v,L})$ such that $g a_i = b_i$, is equivalent to finding $G \in GL_n(\mathcal{O}_v)$ such that

$$(G, F_2^{-1}(G^t)^{-1} F_2)(e_i, e_i) = \phi(b_i)$$

for $1 \leq i \leq m$. Let $\phi(b_i) = (b_i^{(1)}, b_i^{(2)})$. The condition now reduces to constructing $G \in GL_n(\mathcal{O}_v)$ such that $G e_i = b_i^{(1)}$ and $F_2^{-1}(G^t)^{-1} F_2 e_i = b_i^{(2)}$. Notice that the second condition may be rewritten as $F_2 e_i = G^t F_2 b_i^{(2)}$. From the first condition, we see we should take

$$G = \begin{bmatrix} b_1^{(1)} & \cdots & b_m^{(1)} & x_{m+1} & \cdots & x_n \end{bmatrix}$$

where

$$x_j = \begin{bmatrix} x_{1j} \\ \vdots \\ x_{nj} \end{bmatrix}$$

for some x_{ij}. With this it is clear that $G e_i = b_i$ for all $1 \leq i \leq m$. Then

$$G^t F_2 b_i^{(2)} = \begin{bmatrix} (b_1^{(1)})^t \\ \vdots \\ (b_m^{(1)})^t \\ x_{m+1}^t \\ \vdots \\ x_n^t \end{bmatrix} F_2 b_i^{(2)} = \begin{bmatrix} (b_1^{(1)})^t F_2 b_i^{(2)} \\ \vdots \\ (b_m^{(1)})^t F_2 b_i^{(2)} \\ x_{m+1}^t F_2 b_i^{(2)} \\ \vdots \\ x_n^t F_2 b_i^{(2)} \end{bmatrix} = \begin{bmatrix} \langle b_i, b_1\rangle \\ \vdots \\ \langle b_i, b_n\rangle \\ x_{m+1}^t F_2 b_i^{(2)} \\ \vdots \\ x_n^t F_2 b_i^{(2)} \end{bmatrix}.$$

We also can see that

$$F_2 e_i = \begin{bmatrix} \langle e_i, e_1 \rangle \\ \vdots \\ \langle e_i, e_n \rangle \end{bmatrix}$$

but $\langle e_i, e_j \rangle = \langle b_i, b_j \rangle$ for $1 \leq i, j \leq m$, so

$$F_2 e_i = \begin{bmatrix} \langle b_i, b_1 \rangle \\ \vdots \\ \langle b_i, b_m \rangle \\ \langle e_i, e_{m+1} \rangle \\ \vdots \langle e_i, e_n \rangle \end{bmatrix}.$$

Therefore $F_2 e_i = G^t F_2 b_i$ for all $1 \leq i \leq m$, if $x_j^t F_2 b_i^{(2)} = \langle e_i, e_j \rangle$ for all $m+1 \leq j \leq n$ and $1 \leq i \leq n$. Thus there exists an appropriate G if there is a solution to the system of equations $\sum_{l=1}^{n} x_{jl} \langle b_i, e_l \rangle = \langle e_i, e_j \rangle$ for all $1 \leq i \leq m$, $m+1 \leq j \leq n$ in $\mathcal{O}_v$. Note that if $m = n$ the system is empty and since $\operatorname{span}_{\ell_v}(\bar{b}_1^{(v)}, \ldots, \bar{b}_m^{(v)})$ is an m-dimensional free module we have that G is invertible. Consider this system modulo $\mathfrak{p}_v$ and add if $m < n$ add the requirement that $\det G \equiv 1 \pmod{\mathfrak{p}_v}$. Since $\det F \in \mathcal{O}_v^{\times}$ (implying that its determinant is nonzero mod $\mathfrak{p}_v$) there is a solution to this system in k_v, and by Lemma 1.25 this lifts to a solution in $\mathcal{O}_v$. Since $\det G \equiv 1 \pmod{\mathfrak{p}_v}$, $G \in GL_n(\mathcal{O}_v)$ as desired. □

Corollary 1.26. *Let a_i, b_i be as in the previous two theorems, $v \in V_f^K$ such that $|2|_v = 1$, $|d|_v = 1$, and further assume that $2m+1 \leq n$. Then there exists $g \in SU_{n,F}(\mathcal{O}_{v,L})$ such that $ga_i = b_i$ for all i.*

Proof. Let σ' be the element of $U_{n,F}(\mathcal{O}_{v,L})$ found in Theorem 1.20. Since $2m+1 \leq n$ there exists an element $w \in L_v^n$ such that $\langle w, w \rangle \neq 0$ and $\langle a_i, w \rangle = 0$. By multiplying by an appropriate constant we can guarentee $w \in \mathcal{O}_{v,L}^n$. Then $g = \sigma' \sigma_{(\det \sigma')^{-1}-1,w}$ (where $\sigma_{l,w}$ is as defined in Corollary 1.19) has the desired properties. □

We will also need the following fact about $U_{n,F}$.

Proposition 1.27. *Assume $\langle \cdot, \cdot \rangle_F$ is a hermitian form with Witt index Milliat least 2. If $n \geq 3$ we have $[U_{n,F}(L), U_{n,F}(L)] = SU_{n,F}(L)$.*

This is proved by combining statements 2 and 4 on pages 48-49 in [4]

1.5 Clifford Algebras

The structure of Clifford algebras and spin groups are key in establishing the base case for both main theorems. One reference for the basic definitions and properties is Chapter 5 in [13]. To construct the Clifford algebra we will need the following notations. Let K be a field with characteristic not 2, V a finite-dimensional vector space over K, $\langle \cdot, \cdot \rangle$ a nondegenerate symmetric bilinear form on V, and let $q \colon V \to K$ given by $q(v) = \langle v, v \rangle$ be then corresponding quadratic form.

Definition. The Clifford algebra defined by V, denoted $Cl(V)$, is $T(V)/I$, where $T(V)$ is the tensor algebra, and I is the two-sided ideal generated by $\{v \otimes v - q(v)\}$ for all $v \in V$.

Henceforth we will suppress the tensor notation and write vw for $v \otimes w$. We claim that for any $v, w \in V$, $vw + wv = 2\langle v, w \rangle$. By construction of $Cl(V)$,

$$(v + w)(v + w) = q(v + w) = q(v) + 2\langle v, w \rangle + q(w).$$

By expanding the expression on the left we also have that

$$(v + w)(v + w) = v^2 + wv + vw + w^2 = q(v) + wv + vw + q(w).$$

Therefore by setting the two expressions equal we get $wv + vw = 2\langle v, w \rangle$. Thus if $\langle v, w \rangle = 0$, then $vw = -wv$.

Let $e_1, \ldots, e_n$ be an orthogonal basis for V, and let $I = (i_1, \ldots, i_m)$ be a sequence of integers, $1 \leq i_j \leq n$. Define $e_I = e_{i_1} e_{i_2} \cdots e_{i_m}$, and $e_{()} = 1$. Let S be the set of all strictly increasing sequences consisting of integers between 1 and n including the empty sequence.

Proposition 1.28. *The set $\{e_I\}_{I \in S}$ is a basis for $Cl(V)$, and $\dim_K Cl(V) = 2^n$.*

A proof can be found in [13].

We define an involution $\tau_{Cl(V)}$ on $Cl(V)$. If $I = (i_1, \ldots, i_m)$, let $\bar{I}$ denote $(i_m, \ldots, i_1)$. Then define $\tau_{Cl(V)}(\sum a_I e_I) = \sum a_I e_{\bar{I}}$. When the algebra is clear from context we will write τ instead of $\tau_{Cl(V)}$.

Lemma 1.29. *For all $x, y \in CL(V)$, we have that $\tau(xy) = \tau(y)\tau(x)$.*

Proof. Define an involution τ' on $T(V)$ by

$$\tau'(\sum v_{i_1} \otimes \cdots \otimes v_{i_{r_i}}) = \sum v_{i_{r_i}} \otimes \cdots \otimes v_{i_1}$$

Notice that $\tau'(v \otimes v - q(v)) = v \otimes v - q(v)$, and if p is the quotient map $T(V) \to Cl(V)$, $\tau \circ p = p \circ \tau'$. We can see that for arbitrary basis elements of $T(V)$, $a = v_1 \otimes \cdots \otimes v_r$, $b = w_1 \otimes \cdots \otimes w_s$,

$$\begin{aligned} \tau'(ab) &= \tau'(v_1 \otimes \cdots \otimes v_r \otimes w_1 \otimes \cdots w_s) \\ &= w_s \otimes \cdots \otimes v_1 \\ &= \tau'(w_1 \otimes \cdots \otimes w_s)\tau'(v_1 \otimes \cdots \otimes v_r) \\ &= \tau'(b)\tau'(a). \end{aligned}$$

Since τ' is additive, this means for any $a, b \in T(V)$, $\tau'(ab) = \tau'(b)\tau'(a)$. Let $x, y \in Cl(V)$, $a \in p^{-1}(x)$ and $b \in p^{-1}(y)$. Then

$$\tau(xy) = \tau(p(ab)) = p(\tau'(ab))$$

and thus

$$\tau(xy) = p(\tau'(b)\tau'(a)) = p(\tau'(b))p(\tau'(a)) = \tau(p(b))\tau(p(a)) = \tau(y)\tau(x)$$

as desired. □

For $I = (i_1, \ldots, i_m)$ define $|I| := m$. We define $Cl^0(V)$ to be the K-subalgebra generated by the e_J with $|J|$ even, and $Cl^1(V)$ to be the K-subspace spanned by the e_J with $|J|$ odd. Then $Cl(V) = Cl^0(V) \oplus Cl^1(V)$ making $Cl(V)$ a $\mathbb{Z}/2$-graded algebra. We can see that $Cl^0(V)$ has dimension 2^{n-1}.

Lemma 1.30. *Let $e_1, \ldots, e_n$ be an orthogonal basis of a vector space V with nondegenerate quadratic form q. Then $Cl^0(V)$ is generated (as an algebra) by $e_1e_2, \ldots, e_1e_n$.*

Proof. First we claim that $\{e_ie_j\}_{1\leq i<j\leq n}$ generates $Cl^0(V)$. We can write an arbitrary basis element of $Cl^0(V)$ $e_I = e_{i_1} \cdots e_{i_{2m}}$ as $(e_{i_1}e_{i_2}) \cdots (e_{i_{2m-1}}e_{i_2m})$, a product of e_ie_j's. Now we notice that since $(e_1e_i)(e_1e_j) = -q(e_1)e_ie_j$, the e_1e_i's generate $Cl^0(V)$. □

For $\dim_K V \leq 3$ we have the following explicit descriptions of $Cl(V)$.

Example 1.31. *Let $V = \operatorname{span}(e_1)$ with $q(e_1) = a_1$. Then $Cl(V) \cong K[x]/\langle x^2 - a_1\rangle$.*

Notice that if a_1 is a square in $K^\times$ $K[x]/\langle x^2 - a_1\rangle$ is isomorphic to $K \oplus K$, since the homomorphism $\phi\colon K[x]/\langle x^2 - a_1\rangle \to K \oplus K$ given by

$$a + bx \mapsto (a + b\sqrt{a_1}, a - b\sqrt{a_1}$$

is an isomorphism. Further, though the involution on the clifford algebra is trivial in this case, if τ is the involution taking x to $-x$ then $\phi(\tau(\phi^{-1}(x, y))) = (y, x)$. (These facts are used in later proofs).

Example 1.32. *Let $V = \operatorname{span}(e_1, e_2)$ with $\langle e_1, e_2\rangle = 0$, $q(e_1) = a_1$, $q(e_2) = a_2$. Then $Cl(V) \cong \left(\frac{a_1, a_2}{K}\right)$, a quaternion algebra.*

To prove this fact, we define a map ϕ: $\left(\frac{a_1, a_2}{K}\right) \to Cl(V)$ by

$$\phi(x_0 + x_1 i + x_2 j + x_3 k) = x_0 + x_1 e_1 + x_2 e_2 + x_3 e_1 e_2,$$

which is K-linear isomorphism of vector spaces. Since $i^2 = a_1 = e_1^2$, $j^2 = a_2 = e_2^2$, $\phi(ij) = \phi(k) = e_1 e_2 = \phi(i)\phi(j)$, and $\phi(ji) = \phi(-k) = -e_1 e_2 = e_2 e_1 = \phi(j)\phi(i)$ we have that ϕ is a K-algebra isomorphism.

We also notice that the involution on $Cl(V)$ does not correspond to the usual quaternion involution, since

$$\tau(x_0 + x_1 e_1 + x_2 e_2 + x_3 e_1 e_2) = x_0 + x_1 e_1 + x_2 e_2 - x_3 e_1 e_2.$$

We can see that $\phi^{-1} \circ \tau \circ \phi$ fixes i and j and sends k to $-k$.

Example 1.33. *Let $V = \text{span}(e_1, e_2, e_3)$ with the e_i's orthogonal, and $q(e_i) = a_i$. Then $Cl^0(V) \cong \left(\frac{-a_1 a_2, -a_1 a_3}{K}\right)$.*

We define a map ϕ: $\left(\frac{-a_1 a_2, -a_1 a_3}{K}\right) \to Cl^0(V)$ by

$$\phi(x_0 + x_1 i + x_2 j + x_3 k) = x_0 + x_1 e_1 e_2 + x_2 e_1 e_3 - x_3 a_1 e_2 e_3$$

which is an isomorphism of vector spaces. Since

$$i^2 = -a_1 a_2 = (e_1 e_2)^2,$$

$$j^2 = -a_1 a_3 = (e_1 e_3)^2,$$

$$\phi(ij) = \phi(k) = -a_1 e_2 e_3 = (e_1 e_2)(e_1 e_3) = \phi(i)\phi(j)$$

and

$$\phi(ji) = \phi(-k) = a_1 e_2 e_3 = (e_1 e_3)(e_1 e_2) = \phi(j)\phi(i),$$

thus ϕ is a K-algebra isomorphism.

We also note that $\tau(x_0 + x_1e_1e_2 + x_2e_1e_3 + x_3e_2e_3) = x_0 - x_1e_1e_2 - x_2e_1e_1 - x_3e_2e_3$ implying $\phi^{-1} \circ \tau \circ \phi$ is the standand quaternion involution.

For an arbitrary quadratic form, we define the discriminants,

$$d(q) = \prod_{i=1}^{n} q(e_i),$$

and $d_{\pm}(q) = (-1)^{n(n-1)/2} d(q)$ where $n = \dim_K V$. Further, for a Clifford algebra defined by this form it can be seen that $d_{\pm}(q) = (e_1e_2 \cdots e_n)^2$. For $m \in \mathbb{Z}$ we define a K-algebra homomorphism $\psi_m \colon Cl(V) \to Cl(V)$ by $\psi_m(\sum a_I e_I) = \sum (-1)^{m|I|} a_I e_I$. Notice that for m even this is the identity homomorphism, and for m odd this is the homomorphism from $Cl(V) = Cl^0(V) \oplus Cl^1(V)$ to itself which fixes $Cl^0(V)$ and is multiplication by -1 on $Cl^1(V)$.

The following two lemmas can be found as Corollary 2.7, and Corollary 2.9 on page 113 in [12].

Lemma 1.34. *Let V_1 be a vector space of dimension $2m$ with quadratic form q_1, V_2 a vector space with quadratic form q_2. Then there is an isomorphism*

$$\phi \colon Cl(V_1 \perp V_2) \to Cl(V_1) \otimes_K Cl(V_2')$$

where V_2' is the vector space V_2 with quadratic form given by $q_2' = d_{\pm}(q_1)q_2$. We obatin an involution on $Cl(V_1) \otimes_K Cl(V_2')$, $\phi \circ \tau \circ \phi^{-1}$, which is given by

$$(\tau_{Cl(V_1)} \otimes \psi_m) \circ (id \otimes \tau_{Cl(V_2')}).$$

Proof. Let $V_1 = \operatorname{span}(f_1, \ldots, f_{2m})$ where the f_i's are orthogonal. Let A be the subalgebra of $Cl(V_1 \perp V_2)$ generated by $f_1, \ldots, f_{2m}$. Let $V_2 = \operatorname{span}(e_1, \ldots, e_n)$ where the e_i's are orthogonal. Let B be the subalgebra of $Cl(V_1 \perp V_2)$ generated by

$f_1 f_2 \cdots f_{2m} e_1, \ldots, f_1 f_2 \cdots f_{2m} e_n$. Notice that

$$\begin{aligned} f_i(f_1 f_2 \cdots f_{2m} e_j) &= (-1)^{i-1}(f_1 \cdots f_i^2 \cdots f_{2m} e_j) \\ &= (-1)^{2m-1} f_1 \cdots f_{2m} f_i e_j \\ &= (f_1 f_2 \cdots f_{2m} e_j) f_i \end{aligned}$$

for any f_i, e_j, so any element of A commutes with any element of B. We claim that any basis element of $Cl(V_1 \perp V_2)$ can be expressed as an element of A times an element of B. Any basis element is a product of f_i's and e_j's, but the f_i's are all elements of A, and the e_j's can be expressed as

$$e_j = \frac{1}{d_\pm(q_1)} f_1 f_2 \cdots f_{2m}(f_1 f_2 \cdots f_{2m} e_j).$$

Thus by dimension counting $Cl(V_1 \perp V_2) = A \otimes_K B$. Clearly $A \cong Cl(V_1)$. To show $B \cong Cl(V_2')$ we define a map $\phi\colon B \to Cl(V_2')$ by $\phi(f_1 \cdots f_{2m} e_i) = e_i$. Since

$$(f_1 \cdots f_{2m} e_i)(f_1 \cdots f_{2m} e_j) = -(f_1 \cdots f_{2m} e_j)(f_1 \cdots f_{2m} e_i)$$

and

$$(f_1 \cdots f_{2m} e_i)^2 = d_\pm(q_1) q_2(e_i) = q_2'(e_i),$$

ϕ is a K-algebra isomorphism, establishing the lemma. Furthermore,

$$\begin{aligned} \phi(\tau_{Cl(V_1 \perp V_2)}(\phi^{-1}(e_i))) &= \phi(\tau_{Cl(V_1 \perp V_2)}(f_1 \cdots f_{2m} e_i)) \\ &= \phi(e_i f_{2m} \cdots f_1) \\ &= \phi((-1)^m e_i (f_{2m-1} f_{2m}) \cdots (f_1 f_2)) \\ &= \phi((-1)^m e_i (f_1 f_2) \cdots (f_{2m-1} f_{2m})) \\ &= \phi((-1)^m f_1 \cdots f_{2m} e_i) \\ &= (-1)^m e_i \\ &= \psi_m(\tau_{Cl(V_2')}(e_i)) \end{aligned}$$

so the induced involution is as described. □

Lemma 1.35. *Let V_1 be a vector space of dimension $2m+1$ with quadratic form q_1, V_2 a finite-dimensional vector space with quadratic form q_2. Then there is an isomorphism*

$$\phi\colon Cl^0(V_1 \perp V_2) \to Cl^0(V_1) \otimes_K Cl(V_2')$$

where V_2' is V_2 with quadratic form $q_2' = -d_\pm(q_1)q_2$. Further,

$$\phi \circ \tau \circ \phi^{-1} = (\tau_{Cl(V_1)} \otimes_K \psi_{m+1}) \circ (id \otimes \tau_{Cl(V_2')}).$$

Proof. Let $V_1 = \operatorname{span}(f_1, \ldots, f_{2m+1})$, $V_2 = \operatorname{span}(e_1, \ldots, e_n)$. Let A be the subalgebra generated by $f_1f_2, \ldots, f_1f_{2m+1}$ and let B be the subalgebra generated by $f_1 \cdots f_{2m+1}e_1, \ldots, f_1 \cdots f_{2m+1}e_n$. Then

$$f_1f_i(f_1 \cdots f_{2m+1}e_j) = (f_1 \cdots f_{2m+1}e_j)f_1f_i$$

so every element of A commutes with every element of B. We also notice that for any j,

$$\frac{1}{q_1(f_1)^{m-1}d_\pm(q_1)}(f_1f_2)(f_1f_3)\cdots(f_1f_{2m+1})(f_1 \cdots f_{2m+1}e_j) = f_1e_j,$$

and so every generator of $Cl^0(V_1 \perp V_2)$ can be expressed as an element of A times an element of B, so by dimension count $Cl^0(V_1 \perp V_2) = A \otimes B$. It is clear that $A \cong Cl^0(V_1)$. As in the proof of Lemma 1.34 we define a map $B \to Cl(V_2')$ by $\phi(f_1 \cdots f_{2m+1}e_j) = e_j$. Then

$$(f_1 \cdots f_{2m+1}e_i)(f_1 \cdots f_{2m+1}e_j) = -(f_1 \cdots f_{2m+1}e_j)(f_1 \cdots f_{2m+1}e_i)$$

and

$$\begin{aligned}(f_1 \cdots f_{2m+1}e_i)^2 &= -d_\pm(q_1)q_2(e_i)\\ &= q_2'(e_i)\end{aligned}$$

so ϕ is a K-algebra isomorphism, establishing the lemma. As in the previous lemma

$$\tau_{Cl(V_1 \perp V_2)}(f_1 \cdots f_{2m+1} e_i) = (-1)^{m+1} f_1 \cdots f_{2m+1} e_i$$

implying that

$$\phi(\tau_{Cl(V_1 \perp V_2)}(\phi^{-1}(e_i))) = \psi_{m+1}(\tau_{Cl(V_2')}(e_i)).$$

□

The following theorem can be found as Proposition 1 in [15].

Theorem 1.36. *Let V be a vector space with nondegenerate quadratic form*

$$q(\sum x_i e_i) = \sum a_i x_i^2,$$

and $\dim_K V = 4n + 2$. *Then there is an isomorphism*

$$\phi \colon Cl^0(V) \to \mathcal{D}_1 \otimes \mathcal{D}_2 \otimes \cdots \otimes \mathcal{D}_{2n} \otimes K[x] / \left\langle x^2 + a_1 \cdots a_{4n+2} \right\rangle$$

where $\mathcal{D}_i = \left(\dfrac{(-1)^i a_1 \cdots a_{2i}, (-1)^i a_1 \cdots a_{2i-1} a_{2i+1}}{K} \right)$. *Further,* $\phi \circ \tau_{Cl(V)} \circ \phi^{-1}$ *gives the standard quaternion algebra involution on* $\mathcal{D}_i$ *with* i *odd, the involution given in Example 1.32 on* $\mathcal{D}_i$ *with* i *even, and takes* x *to* $-x$.

Proof. Let $V = \operatorname{span}(e_1, \ldots, e_{4n+2})$ and $q(\sum x_i e_i) = \sum a_i x_i^2$. Define $V_1 = \operatorname{span}(e_1, e_2, e_3)$, $V_2 = \operatorname{span}(e_4, \ldots, e_{4n+2})$, then $V = V_1 \perp V_2$. By Lemma 1.35

$$Cl^0(V) \cong Cl^0(V_1) \otimes_K Cl(V_2').$$

By Example 1.33 we have that $Cl^0(V) \cong \left(\dfrac{-a_1 a_2, -a_1 a_3}{K} \right) \otimes_K Cl(V_2')$. The quadratic form on $V_2' = \operatorname{span}(e_4, \ldots, e_{4n+2})$ is given by

$$\sum_{i=4}^{4n+2} x_i e_i \mapsto a_1 a_2 a_3 \sum_{i=4}^{4n+2} a_i x_i^2,$$

and the involution is the standard quaternion involution on $\mathcal{D}_1 = \left(\frac{-a_1a_2, -a_1a_3}{K}\right)$ and $\psi_2 \circ \tau_{Cl(V_2')} = \tau_{Cl(V_2')}$ on $Cl(V_2')$. We now let $V_{21} = \text{span}(e_4, e_5)$ and $V_{22} = \text{span}(e_6, \ldots, e_{4n+2})$, so $V_2' = V_{21} \perp V_{22}$. By Lemma 1.34

$$Cl(V_2') \cong Cl(V_{21}) \otimes Cl(V_{22}')$$

and by Example 1.2 we have

$$Cl(V_2') \cong (\frac{a_1a_2a_3a_4, a_1a_2a_3a_5}{K}) \otimes_K Cl(V_{22}').$$

The quadratic form on V_{22}' is given by

$$\sum_{i=6}^{4n+2} x_i e_i \mapsto -a_1a_2a_3a_4a_5 \sum_{i=6}^{4n+2} x_i^2$$

and the involution is the involution given in Example 1.2. The involution on $Cl(V_{22}')$ is $\psi_1 \circ \tau_{Cl(V_{22}')}$. We continue in this manner until we are left with $Cl(\text{span}(e_{4n+2}))$ with quadratic form given by

$$x_{4n+2}e_{4n+2} \mapsto -a_1a_2 \cdots a_{4n+2}x_{4n+2}^2.$$

By Example 1.1 this is isomorphic to $K[x]/\langle x^2 + a_1a_2 \cdots a_{4n+2} \rangle$ with an involution given by $x \mapsto -x$. Thus we have the desired isomorphism and involutions. □

Define

$$Cl^+(V) = \{x \in Cl(V) \mid \tau(x)x = 1\}$$

and

$$\text{Spin}(V) = \{x \in Cl^+(V) \cap Cl^0(V) \mid xvx^{-1} \in V \text{ for all } v \in V\}.$$

There is a natural map $\phi\colon \text{Spin}(V) \to O(V)$, the orthogonal group on V given by $\phi(x)(v) = xvx^{-1}$. The map given by $\phi(x)$ is clearly in $GL(V)$, and by construction of the clifford algebra

$$q(xvx^{-1}) = (xvx^{-1})^2 = xv^2x^{-1} = xq(v)x^{-1} = q(v)$$

, thus we have that $\phi(x) \in O(V)$. In fact $\operatorname{Im}\phi = SO(V)$ and $\ker\phi = \{-1, 1\}$ (There is a discussion of this in Chapter 5 of [1].)

We shall need the following for the base case of the second main theorem:

Theorem 1.37. *Let $V = K^n$ with $n \geq 3$ and K algebraically closed. Then the commutator subgroup,* $[\mathrm{Spin}(V), \mathrm{Spin}(V)] = \mathrm{Spin}(V)$.

Proof. We first note that by statement 2a on page 56 of [4] we have that $SO(V)/[SO(V), SO(V)] \cong K^\times/K^{\times 2}$, which is $\{1\}$ since K is algebraically closed, implying that $SO(V) = [SO(V), SO(V)]$. Since $\mathrm{Spin}(V)$ surjects onto $SO(V)$ with kernel $\{-1, 1\}$ the statement of the theorem reduces to showing that $-1 \in [\mathrm{Spin}(V), \mathrm{Spin}(V)]$, which holds if there are elements of $x, y \in \mathrm{Spin}(V)$ such that $xy = -yx$. We take a orthonormal basis of V, $f_1, \ldots, f_n$, which exists since K is algebraically closed. Let $x = f_1 f_2$, $y = f_2 f_3$. We can see $x\tau(x) = 1$, x fixes f_i for all $i > 2$, $xf_1\tau(x) = -f_1$ and $xf_2\tau(x) = -f_2$. Therefore $x \in \mathrm{Spin}(V)$. Similarly $y \in \mathrm{Spin}(V)$ and

$$xy = f_1 f_2 f_2 f_3 = -f_2 f_3 f_1 f_2 = -yx$$

as desired. □

We will also need bounded generation for spin groups.

Theorem 1.38. *Let V be a vector space over a number field K with* $\dim_K V \geq 5$. *Let S be a finite subset of V^K containing V_∞^K. Then* $\mathrm{Spin}(V)_{\mathcal{O}_S}$ *has bounded generation if the Witt index of V is at least 2, or the Witt index of V is one, and S contains at least one nonarchimdean place.*

This is the main theorem of [7]

Assume K is an algebraic number field and let S be a finite subset of V^K containing V_∞^K. Let V be a vector space, and fix a basis, $e_1, \ldots, e_n$ such that $q(e_i) \in \mathcal{O}_S$ for all i. We define $Cl(V)_{\mathcal{O}_S}$ as the set of $\mathcal{O}_S$-linear combinations of the basis of $Cl(V)$ formed by the e_i's.

1.6 Strong Approximation

One of the useful properties of the special unitary group used in the proof of the second main result is strong approximation. We define this property by first extending the notion of adeles (Section 0.1) to affine varieties. If X is the set of zeroes of a system of polynomial equations in $K[x_1, \ldots, x_n]$, then X_{A_K} is the set of zeroes of the same system of polynomials in A_K. This is equivalent to setting

$$X_{A_K} = \{(x_v) \in \prod X_{K_v} \mid x_v \in X_{\mathcal{O}_v} \text{ for almost all } v \in V\}.$$

The set $X_{A_{K,S}}$ is defined similarly.

Definition. Let X be an affine variety, and $S \subset V^k$ containing V_∞^K. We say X has *strong approximation* with respect to S if the image of the diagonal map

$$\delta \colon X \to X_{A_{K,S}}$$

is dense.

Example 1.39. *SL_n has strong approximation with respect to $S = V_\infty^K$.*

Proof. The proof relies on the fact that SL_n is generated by elementary matrices. Take a basic open set U in $SL_n(A_{K,S})$. Without loss of generality we may assume

$$U = \prod_{v \in T} B_{r_v}(g_v) \times \prod_{v \notin T} SL_n(\mathcal{O}_v)$$

where $T \subset V_f^K$ is finite and

$$B_{r_v}(g_v) := \{g \in SL_n(K_v) \mid g - g_v \in M_n(\mathfrak{p}_v^{r_v})\}.$$

For each $v \in T$ note that $g_v = \prod_{l=1}^{m_v} E_{i_{lv}j_{lv}}(\alpha_{lv})$. Since T is finite, there exists some $m \in \mathbb{Z}$ such that $g_v = \prod_{l=1}^{m} E_{i_l j_l}(\alpha_{lv})$ for all $v \in T$. Notice that for each $v \in T$ there exists s_v such that

$$\prod_{l=1}^{m} E_{i_l j_l}(\alpha_{lv} + \mathfrak{p}_v^{s_v}) \subseteq B_{r_v}(g_v).$$

Let

$$U_l = \prod_{v \in T} (\alpha_{lv} + \mathfrak{p}_v^{s_v}) \times \prod_{v \notin T} \mathcal{O}_v \,.$$

This is an open set in $A_{K,S}$, so by Proposition 0.1 we have that there exists $\alpha_l \in K$ whose image under the diagonal map lies in U_l. Set $g = \prod_{l=1}^{m} E_{i_l j_l}(\alpha_l)$. Then the image of g under the diagonal map lies in U, and thus SL_n has strong approximation. □

We note the following fact concerning strong approximation:

Proposition 1.40. *If X and Y are biregularly isomorphic varieties over K, then X has strong approximation if and only if Y does.*

(This is part 1 from proposition 7.1 in [17].)

We will also need the following facts about strong approximation specific to algebraic groups.

Proposition 1.41. *If an algebraic group G has strong approximation, then $G_{A_{K,S}} = \delta(G_K) \prod_{v \notin S} G_{\mathcal{O}_v}$.*

Proof. By definition of the adele topology, $U = \prod_{v \notin S} G_{\mathcal{O}_v}$ is an open subgroup of $G_{A_{K,S}}$. Let $g \in G_{A_{K,S}}$. Since G has strong approximation, $gU \cap \delta(G_K)$ is nonempty, implying that $g \in \delta(G_K)U$, so $G_{A_{K,S}} \subseteq \delta(G_K) \prod_{v \notin S} G_{\mathcal{O}_v}$ and so the two sets are equal. □

Theorem 1.42 (Strong Approximation Theorem)**.** *Let G be a reductive algebraic group over an algebraic number field K, and let S be a finite subset of V^K. Then G has strong approximation with respect to S if and only if*

1. *G is simply connected*
2. *G does not contain any K-simple component G^i with G^i_S compact.*

This is Theorem 7.38 in [17].

Proposition 1.43. *$SU_{n,F}$ where F is Hermitian with Witt index at least 1 has strong approximation.*

Proof. We let $SU_{n,F} = G$ and apply the strong approximation theorem. We first claim that $G_{\bar{K}} \cong SL_n(\bar{K})$, where $\bar{K}$ denotes the algebraic closure of K. Since SL_n is simply connected, we have that G is also simply connected. Further, since the Witt index is at least 1, G contains a nontrivial K-split torus, so G_S is noncompact and thus G has strong approximation.

It remains to be shown that $G_{\bar{K}} = SU_{n,F}(L \otimes \bar{K})$ is isomorphic to $SL_n(\bar{K})$. To do so we use the second characterization of $U_{n,F}$ as a variety in Section 1.4. It is clear that if $(X, Y) \in G_{\bar{K}}$ (note that $X, Y \in M_n(\bar{K})$ and satisfy the equations given in Section 1.4), then $X + \sqrt{d}Y \in SL_n(L)$ and this is an injective map of varieties. What remains to be seen is whether this map is surjective. Let $M \in SL_n(L)$, the map is surjective if there exists $(X, Y) \in \bar{G}$ such that $X + \sqrt{d}Y = M$. Let

$$X = \frac{1}{2}(M + F^{-1}(M^t)^{-1}F)$$
$$Y = \frac{\sqrt{d}}{2d}(M - F^{-1}(M^t)^{-1}F).$$

It is clear that $X + \sqrt{d}Y = M$.

$$X^t F X = \frac{1}{4}(M^t F M + 2F + F M^{-1} F^{-1} (M^t)^{-1} F),$$

$$Y^t F Y = \frac{1}{4d}(M^t F M - 2F + F M^{-1} F^{-1} (M^t)^{-1} F)$$

so $X^t F X - d Y^t F Y = F$. Also

$$X^t F Y = \frac{1}{4}(M^t F M - F M^{-1} F^{-1} (M^t)^{-1} F) = Y^t F X.$$

Thus $(X, Y) \in G_{\bar{K}}$, so $\bar{G} \cong SL_n(\bar{K})$ as needed. □

We will also need strong approximation for "spheres."

Proposition 1.44. *([20]) Let G' be a simply connected K-subgroup of a connected algebraic K-group G. Suppose $V_\infty^K \subset S$ and G has strong approximation with respect to S. Then the homogeneous space $X = G/G'$ also has strong approximation with respect to S.*

Combining the previous two propositions, we obtain the following corollary.

Corollary 1.45. *Let $f(x) = \langle x, x\rangle$ where $\langle \cdot, \cdot \rangle$ is a nondegerate hermitian form with Witt index at least 1. Fix $c \in K^\times$ and let $C = \{x \mid f(x) = c\}$. If $C_K \neq 0$, then C has strong approximation.*

Proof. Let $G = SU_{n,F}$ and fix $x \in C_K$. By Theorem 1.18 the map $G \to C$ given by $g \mapsto gx$ is surjective. Therefore, if we let $G(x)$ denote the stabilizer of x, we have a bijective morphism $\phi\colon C \to G/G(x)$. However, $G(x) \cong SU_{n-1,F'}$ for some hermitian matrix F', and so is simply connected. By Proposition 1.43, G has strong approximation and therefore by Proposition 1.44 C does. □

Chapter 2

$SL_n(\mathcal{O}_{\mathcal{D},S})$ has bounded generation

2.1 Special Linear Groups

The goal of this chapter is to demonstrate that under certain conditions SL_n over an order of a quaternion algebra has bounded generation. We first reduce the general case to SL_2 and then demonstrate that this group has bounded generation by showing it is isomorphic to a spin group.

We fix K, an algebraic number field, $S \subset V^K$ such that $V_\infty^K \subset S$, and let $\mathcal{D} = \left(\frac{\alpha,\beta}{K}\right)$ be a non-split quaternion algebra with $\alpha, \beta \in \mathcal{O}_S$. Recall that $SL_n(\mathcal{D}) = \{X \in GL_n(\mathcal{D}) \mid \det X = 1\}$, where the determinent is defined by the reduced norm. Let $\phi\colon M_n(\mathcal{D}) \to M_{2n}(K(\sqrt{\alpha}))$ denote the homomorphism defined in Section 1.2. We define $SL_n(\mathcal{O}_{\mathcal{D},S}) = SL_n(\mathcal{D}) \cap M_n(\mathcal{O}_{\mathcal{D},S})$ where $\mathcal{O}_{\mathcal{D},S}$ is as defined at the end of Section 1.2.

In the argument we will use the properties of elementary matrices from Section 1.2. We notice that if $A = (a_{lk})_{1\le l,k\le n}$, then mulitplying by an elementary matrix gives

$$[AE_{ij}(x)]_{lk} = \begin{cases} a_{lk} & \text{if} \quad k \neq j \\ a_{li}x + a_{lj} & \text{if} \quad k = j \end{cases},$$

and

$$[E_{ij}(x)(A)]_{lk} = \begin{cases} a_{lk} & \text{if} \quad l \neq i \\ xa_{jk} + a_{ik} & \text{if} \quad l = i \end{cases}.$$

We use these types of calculations extensively in the proof of Theorem 2.3.

We start our proof of Main Theorem 1 by proving a basic lemma necessary for the induction step.

Lemma 2.1. *Let V be a finite-dimensional vector space over a field K, and let $f, g\colon V \to V$ be linear transformations. Then there exists $h \in \mathrm{End}_K(V)$ such that $\mathrm{Im}(f + gh) = \mathrm{Im}\, f + \mathrm{Im}\, g$.*

Proof. Let $v_1, \ldots, v_n$ be a basis of V such that $f(v_1), \ldots, f(v_r)$ form a basis of $\mathrm{Im}\, f$. Let W be a subspace of V such that $g|_W$ is injective and

$$\mathrm{Im}\, f + \mathrm{Im}\, g = \mathrm{Im}\, f \oplus g(W).$$

Let $n := \dim V$, $r := \dim \mathrm{Im}\, f$ and $t := \dim W$. We can see that $t \leq n - r$. There exists $h \in \mathrm{End}_K(V)$ be such that $h(v_i) = 0$ for $i = 1, \ldots, r$ and $h(v_{r+1}), \ldots, h(v_{r+t})$ form a basis of W. Then $(f + gh)(v_i) = f(v_i)$ for $i = 1, \ldots, r$, so $\mathrm{Im}(f + gh) \supseteq \mathrm{Im}\, f$. Since

$$(f + gh)(v_i) = f(v_i) + g(h(v_i))$$

for $i = r + 1, \ldots, r + t$, we have that $\mathrm{Im}(f + gh) \supset g(W)$, and thus $\mathrm{Im}(f + gh) \supset \mathrm{Im}\, f + \mathrm{Im}\, g$. Therefore $\mathrm{Im}(f + gh) = \mathrm{Im}\, f + \mathrm{Im}\, g$. □

Corollary 2.2. *With V as before, and $f_1, \ldots, f_n\colon V \to V$ linear transformations, there exist $h_2, \ldots, h_n \in \mathrm{End}_K(V)$ such that*

$$\mathrm{Im}(f_1 + f_2h_2 + \cdots + f_nh_n) = \mathrm{Im}\, f_1 + \cdots + \mathrm{Im}\, f_n.$$

Proof. This follows directly by induction on n, the previous lemma providing the base case. □

Theorem 2.3. *Let $\mathcal{D}$ be a non-split quaternion algebra over an algebraic number field K, and let S be a finite subset of V^K containing V_∞^K. Then $SL_n(\mathcal{O}_{\mathcal{D},S}) = E_1 \cdots E_r X E_{r+1} \cdots E_s$ where for each $1 \leq i \leq s$, $E_i = E_{l_i k_i}(\mathcal{O}_{\mathcal{D},S})$ for some l_i, k_i, and X is the group of matrices of the form $\begin{bmatrix} X' & 0 \\ 0 & I \end{bmatrix}$ where X' is in $SL_2(\mathcal{O}_{\mathcal{D},S})$. Further $s \leq 2n^2 + 2n - 12$.*

Proof. By induction on n. We will prove the theorem by showing that for an arbitrary $A \in SL_n(\mathcal{O}_{\mathcal{D},S})$ we have that $A = E_{l_1 k_1}(\alpha_1) \cdots E_{l_i k_i}(\alpha_i) C E_{l_{i+1} k_{i+1}}(\alpha_{i+1}) \cdots E_{l_{4n} k_{4n}}(\alpha_{4n})$ where $l_1, \ldots, l_{4n}, k_1, \ldots, k_{4n}$ are not dependent on A and C is of the form $\begin{bmatrix} C' & 0 \\ 0 & 1 \end{bmatrix}$ with $C' \in SL_{n-1}(\mathcal{O}_{\mathcal{D},S})$.

Let

$$A = (a_{ij})_{1 \leq i,j \leq n}.$$

Since A is invertible, there exists a matrix

$$B = (b_{ij})_{1 \leq i,j \leq n} \in SL_n(\mathcal{O}_{\mathcal{D},S})$$

such that $AB = I$. Thus,

$$a_{n1} b_{1n} + \cdots + a_{nn} b_{nn} = 1.$$

Case 1: $a_{n2} = 0$. Let

$$A' = A E_{12}(b_{1n}) \prod_{j=3}^{n} E_{j2}(b_{jn}).$$

We can see that

$$[A']_{n2} = \sum a_{nj} b_{jn} = 1.$$

Now let

$$A'' = A' E_{2n}(1 - a_{nn}) \prod_{j=1}^{n-1} E_{nj}(-a_{nj}).$$

Computing, we find that $[A'']_{nj} = 0$ for all $j < n$. Finally if

$$A''' := (\prod_{j=1}^{n-1} E_{jn}(-[A'']_{jn}))A''$$

we have that $[A''']_{nj} = [A''']_{jn} = 0$ for all $j < n$ and $[A''']_n n = 1$. Notice that the total number of E_{lk}'s in this case is $3n - 2$.

Case 2: $a_{n2} \neq 0$. We will need to use a few facts about the Jacobson radical of a ring. The Jacobson radical of a ring R, denoted $J(R)$, is the intersection of all maximal left ideals of R.

Lemma 2.4. *1. The Jacobson radical is a 2-sided ideal.*

2. If R is Artinian, $R/J(R)$ is semsimple.

3. Let $x \in R$, and let $\bar{x}$ denote the image of x in $R/J(R)$. If $\bar{x}$ is invertible then x is invertible.

Proof. 1. See Theorem 4.1 in [10].

2. Proposition 4.4 and the theorem on page 203 in [10] show that if a ring A is artinian and $J(A) = 0$ then A is semi-simple. Since R is Artinian, $R/J(R)$ is also Artinian. Notice that $J(R/J(R)) = 0$. Thus $R/J(R)$ is semisimple.

3. By Theorem 4.1 in [10] every element $y \in J(R)$ has the property that $1 - y$ has an inverse. Let $z = \bar{x}^{-1}$, then $1 - zx \in J(R)$. Then $1 - (1 - zx) = zx$ has an inverse, and thus x does.

□

We now continue our consideration of case 2. If $a_{nn} = 0$ then by replacing A with $AE_{2n}(1)$ we may assume $a_{nn} = a_{n2} \neq 0$. Let $a \in a_{nn}\,\mathcal{O}_{\mathcal{D},S} \cap \mathcal{O}_K$ be nonzero. Such an a exists since $N(a_{nn}) \neq 0$ ($\mathcal{D}$ is non-split and $a \neq 0$) and is in $\mathcal{O}_K$. Let

$C := \mathcal{O}_{\mathcal{D},S}/a\,\mathcal{O}_{\mathcal{D},S}$, which is finite. By part 2 of the lemma, $C/J(C)$ is a semisimple ring. Thus there is an isomorphism

$$\psi\colon C/J(C) \to M_{m_1}(k_1) \oplus \cdots \oplus M_{m_r}(k_r)$$

for finite fields k_i, $1 \le i \le r$. Thus for each $1 \le i \le r$ there exists a homomorphism $\phi_i\colon \mathcal{O}_D \to M_{m_i}(k_i)$. We use this to view $\phi_i(a_{nj})$ as a linear transformation $k_i^{m_i} \to k_i^{m_i}$ for any i, $1 \le i \le n$. Since $\sum a_{nj}b_{jn} = 1$, its image, $\sum \phi_i(a_{ni})\phi_i(b_{in})$, is the identity endomorphism. Therefore

$$\operatorname{Im}\phi_i(a_{n1}) + \cdots + \operatorname{Im}\phi_i(a_{nn}) = k_i^{m_i}.$$

By Corollary 2.2 there exist $c_{2i}, \ldots c_{ni} \in M_{n_i}(k_i)$ such that

$$\operatorname{Im}\big(\phi_i(a_{n1}) + \phi_i(a_{n2})c_{2i} + \cdots + \phi_i(a_{nn})c_{ni}\big) = k_i^{m_i}.$$

Thus

$$\phi_i(a_{n1}) + \phi_i(a_{n2})c_{2i} + \cdots + \phi_i(a_{nn})c_{ni}$$

is invertible for all ϕ_i. Pick $c_2, \ldots, c_n \in C/J(C)$ such that $c_j \in \psi^{-1}(c_{j1}, \ldots, c_{jr})$. Thus if $\phi\colon \mathcal{O}_{\mathcal{D},S} \to C/J(C)$ is the quotient map,

$$\phi(a_{n1}) + \phi(a_{n2})c_2 + \cdots + \phi(a_{nn})c_n$$

is invertible. Further, there exist $c_2', \ldots, c_n' \in C$ such that $\phi(c_i') = c_i$.

Thus

$$\phi(a_{n1} + a_{n2}c_2' + \cdots + a_{nn}c_n')$$

is invertible. By part 3 of the lemma this implies that $a_{n1} + a_{n2}c_2' + \cdots + a_{nn}c_n'$ is invertible in $C = \mathcal{O}_{\mathcal{D},S}/a\,\mathcal{O}_{\mathcal{D},S}$. Taking A' to be $A\prod_2^n E_{i1}(c_i')$ we may assume that $[A']_{n1}$ is invertible mod a. Therefore there exists d such that

$$[A']_{n1}d + a_{n2} \equiv 0 \pmod{a}.$$

Let $A'' = A'E_{12}(d)$, we have that

$$[A'']_{n2} \equiv 0 \pmod{a}.$$

This implies that there exists x such that $ax = [A'']_{n_2}$, but by construction $a = a_{nn}z$ for some z. Thus $[A''E_{n2}(-zx)]_{n2} = 0$. Thus after multiplying by $n+2$ elementary matrices we may apply case 1. Therefore multiplying by $4n$ elementaries reduces $SL_n(\mathcal{O}_{\mathcal{D},S})$ to $SL_{n-1}(\mathcal{O}_{\mathcal{D},S})$ and thus multiplying by $2n^2+2n-12$ elementaries reduces $SL_n(\mathcal{O}_{\mathcal{D},S})$ to $SL_2(\mathcal{O}_{\mathcal{D},S})$. □

Let V be a 6-dimensional vector space over K with basis $e_1, \ldots, e_6$. Define a quadratic form on V by

$$q(x_1e_1 + \cdots + x_6e_6) = -\alpha x_1^2 + x_2^2 + \alpha\beta x_3^2 - \beta x_4^2 + \beta x_5^2 - \beta x_6^2.$$

Notice that $q(e_5 + e_6) = 0$, implying that the Witt index is at least 1. We can also see that $V = \text{span}(e_1, e_2, e_3, e_4) \perp \text{span}(e_5, e_6)$ and q restricted to the first component gives $x_2^2 - \alpha x_1^2 - \beta x_4^2 + \alpha\beta x_3^3$ which has no solutions since $\mathcal{D}$ is nonsplit. Thus the Witt index of q is exactly 1.

Theorem 2.5. *There is an isomorphism*

$$\phi\colon M_2(\mathcal{D}) \oplus M_2(\mathcal{D}) \to Cl^0(V).$$

Furthermore, if τ is the involution on $Cl(V)$, the isomorphism can be constructed such that

$$\phi^{-1}(\tau(\phi(X,Y))) = (F\overline{Y}^tF^{-1}, F\overline{X}^tF^{-1}),$$

where $F = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

Proof. Define an alternative quadratic form on V by

$$q'(x_1e_1 + \cdots + x_6e_6) = -\alpha x_1^2 + x_2^2 + \frac{\beta}{\alpha}x_3^2 - \frac{1}{\beta}x_4^2 + \frac{1}{\beta}x_5^2 - \beta x_6^2.$$

Let V' denote V with this quadratic form.

We construct a map $\phi'\colon M_2(\mathcal{D}) \oplus M_2(\mathcal{D}) \to Cl^0(V')$ as the composition of several algebra isomorphisms. We then note that there is an isomorphism $\psi\colon Cl^0(V') \to Cl^0(V)$ which commutes with the involution given by $e_1 \mapsto e_1$, $e_2 \mapsto e_2$, $e_3 \mapsto \frac{1}{\alpha}e_3$, $e_4 \mapsto \frac{1}{\beta}e_4$, $e_5 \mapsto \frac{1}{\beta}e_5$ and $e_6 \mapsto e_6$.

By Theorem 1.36 we have an isomorphism

$$\phi_1\colon \left(\frac{\alpha,\beta}{K}\right) \otimes_K \left(\frac{1,-1}{K}\right) \otimes_K K[t]/\left\langle t^2-1\right\rangle \to Cl^0(V),$$

with an involution induced on the tensor product given by $\tau_1 \otimes \tau_2 \otimes \tau_3$ where τ_1 is the ordinary quaternion involution, τ_2 is the involution given in Example 1.32 and $\tau_3(a+bt) = a - bt$.

By Example 1.31 we have an isomorphism

$$\phi_2\colon K \oplus K \to K[t]/\left\langle t^2-1\right\rangle,$$

and $\phi_2^{-1}(\tau_3(\phi_2(x,y))) = (y,x)$.

Let

$$\phi_3\colon \mathcal{D} \oplus \mathcal{D} \to \mathcal{D} \otimes_K (K \oplus K)$$

be the isomorphism given by

$$\phi_3(x_0{+}x_1i{+}x_2j{+}x_3k, y_0{+}y_1i{+}y_2j{+}y_3k) = 1{\otimes}(x_0,y_0){+}i{\otimes}(x_1,y_1){+}j{\otimes}(x_2,y_2){+}k{\otimes}(x_3,y_3).$$

(where $1, i, j, k$ is the basis of $\mathcal{D}$.)

By Lemma 1.11 there exists an isomorphism,

$$\phi_4\colon M_2(K) \to \left(\frac{1,-1}{K}\right).$$

By examining the map we can see that $\phi_4^{-1}(\tau_2(\phi_4(X))) = FX^tF$.

Define an isomorphism

$$\phi_5\colon M_2(\mathcal{D}) \oplus M_2(\mathcal{D}) \to M_2(K) \otimes (\mathcal{D} \oplus \mathcal{D})$$

by

$$\phi_5([\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}],[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}]) = [\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}] \otimes (x,a) + [\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}] \otimes (y,b) + [\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}] \otimes (z,c) + [\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}] \otimes (w,d).$$

Now define

$$\phi' = \phi_1 \circ (id \otimes id \otimes \phi_2) \circ (id \otimes \phi_3) \circ (\phi_4 \otimes id) \circ \phi_5.$$

It is an isomorphism because it is a composition of isomorphisms. Finally, we see that $\phi = \psi \circ \phi'$ is an isomorphism $M_2(\mathcal{D}) \otimes M_2(\mathcal{D}) \to Cl^0(V)$ and following the maps we see that $\phi^{-1}(\tau(\phi(X,Y))) = (F\overline{Y}^t F, F\overline{X}^t F)$ as desired. □

Remark. Following the maps in the proof of the previous theorem, we can see that $\phi^{-1}(Cl^0(V)_{\mathcal{O}_S}) \subset M_2(\mathcal{O}_{\mathcal{D},S}) \oplus M_2(\mathcal{O}_{\mathcal{D},S})$. Further, if $X, Y \in M_2(\mathcal{O}_{\mathcal{D},S})$ such that $X \equiv I \pmod{(2\alpha\beta)}$ and $Y \equiv I \pmod{(2\alpha\beta)}$ then $\phi(X,Y) \in Cl^0(V)_{\mathcal{O}_S}$.

Corollary 2.6. $SL_2(\mathcal{D}) \simeq \mathrm{Spin}(V)$ *(with the associated quadratic form as before).*

Proof. Define

$$\psi \colon GL_2(\mathcal{D}) \to M_2(\mathcal{D}) \oplus M_2(\mathcal{D})$$

by

$$X \mapsto (X, F(\overline{X}^t)^{-1}F^{-1})$$

for $X \in GL_2(\mathcal{D})$. I claim that $\phi \circ \psi$ defines an isomorphism from $GL_2(\mathcal{D})$ to the set of elements $x \in Cl^+(V) \cap Cl^0(V)$, i.e., the set of x in $Cl^0(V)$ such that $x\tau(x) = 1$. Since ϕ and ψ are injective, $\phi \circ \psi$ is injective. To establish surjectivity it is enough to show that the image of ψ is

$$\{(X,Y) \mid (X,Y)\tau'(X,Y) = (I,I)\}$$

where $\tau' = \phi^{-1} \circ \tau \circ \phi$. Let $X, Y \in M_2(\mathcal{D})$ with $(X,Y)\tau'(X,Y) = I$. Then

$$(X,Y)(F\overline{Y}^t F, F\overline{X}^t F) = (I,I),$$

so $YF\overline{X}^tF = I$, implying $Y = F(\overline{X}^t)^{-1}F$ therefore $\psi(X) = (X, Y)$, and thus ψ is surjective.

We now verify that $\phi(\psi(SL_2(\mathcal{D}))) = \mathrm{Spin}(V)$. Let $X = \left[\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right]$ for an arbitrary $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{D}$. Then

$$\phi(\psi(X)) = 1 + \frac{1}{2}(\frac{x_0}{\beta}e_4 - \frac{x_1}{\beta}e_3 + x_2e_2 + x_3e_1)(-e_5 + e_6) =: \xi$$

is in $\mathrm{Spin}(V)$ since for any e_i, $1 \leq i \leq 6$, $\xi e_i \tau(\xi) \in V$. Explicitly,

$$\begin{aligned}
\tau(\xi)e_1\xi &= e_1 + \alpha x_3 e_5 - \alpha x_3 e_6 \\
\tau(\xi)e_2\xi &= e_2 - x_2 e_5 + x_2 e_6 \\
\tau(\xi)e_3\xi &= e_3 + \alpha x_1 e_5 - \alpha x_1 e_6 \\
\tau(\xi)e_4\xi &= e_4 + x_0 e_5 - x_0 e_6 \\
\tau(\xi)e_5\xi &= \beta x_3 e_1 + \beta x_2 e_2 - x_1 e_3 + x_0 e_4 + (1 + \frac{1}{2}N(x))e_5 - \frac{1}{2}N(x)e_6 \\
\tau(\xi)e_6\xi &= \beta x_3 e_1 + \beta x_2 e_2 - x_1 e_3 + x_0 e_4 + \frac{1}{2}N(x)e_5 + (1 + \frac{1}{2}N(x))e_6
\end{aligned}$$

Similarly if $X' = \left[\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right]$ then $\phi(\psi(X')) \in \mathrm{Spin}(V)$ since

$$\phi(\psi(X')) = 1 - \frac{1}{2}(-\frac{x_0}{\beta}e_4 - \frac{x_1}{\beta}e_3 + x_2e_2 + x_3e_1)(e_5 + e_6)) =: \xi$$

satisfies

$$\begin{aligned}
\tau(\xi)e_1\xi &= e_1 + \alpha x_3 e_5 + \alpha x_3 e_6 \\
\tau(\xi)e_2\xi &= e_2 - x_2 e_5 - x_2 e_6 \\
\tau(\xi)e_3\xi &= e_3 + \alpha x_1 e_5 + \alpha x_1 e_6 \\
\tau(\xi)e_4\xi &= e_4 - x_0 e_5 - x_0 e_6 \\
\tau(\xi)e_5\xi &= \beta x_3 e_1 + \beta x_2 e_2 - x_1 e_3 - x_0 e_4 + (1 - \frac{1}{2}N(x))e_5 - \frac{1}{2}N(x)e_6 \\
\tau(\xi)e_6\xi &= -\beta x_3 e_1 - \beta x_2 e_2 + x_1 e_3 + x_0 e_4 + \frac{1}{2}N(x)e_5 + (1 + \frac{1}{2}N(x))e_6.
\end{aligned}$$

For any $g \in GL_2(\mathcal{D})$, $g = XZ$ where $X = \left[\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right]$ for some $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{D}^\times$ and Z is a product of elementary matrices [4]. Set $\xi := \phi(\psi(X))$ and

$$\theta = (1 + \frac{1}{N(x)} + \frac{1}{\alpha\beta^2}(1 - \frac{1}{N(x)})e_1e_2e_3e_4e_5e_6.$$

Computing we see that

$$\xi = \frac{1}{2}(1 - \frac{1}{\alpha\beta}e_1e_2e_3e_4) + \frac{1}{4}(x_0 + x_1e_1e_2 + \frac{1}{\alpha}x_2e_1e_3 + x_3e_2e_3)(1 + \frac{1}{\alpha\beta}e_1e_2e_3e_4)\theta$$

and

$$\tau(\xi)e_1\xi = e_1(\frac{1}{2}(x_0 + x_1e_1e_2 + \frac{1}{\alpha}x_2e_1e_3 - x_3e_1e_4)\theta$$

which is in V if and only if $N(x) = 1$. In this case we have that $\xi \in \mathrm{Spin}(V)$. Therefore $X \in SL_2(\mathcal{D})$ if and only if $N(x) = 1$. Since elementary matrices are are in $SL_2(\mathcal{D})$, this proves that $SL_2(\mathcal{D}) \cong \mathrm{Spin}(V)$. □

Theorem 2.7 (Main Theorem 1)**.** *Let S be a finite subset of V^K such that $V_\infty^K \subset S$ and S contains at least one nonarchimedean place. Let $\mathcal{D} = \left(\frac{\alpha, \beta}{K}\right)$ with $\alpha, \beta \in \mathcal{O}_S$. Then $SL_n(\mathcal{O}_{S,\mathcal{D}})$ has bounded generation.*

Proof. By Theorem 2.3 $SL_n(\mathcal{O}_{S,\mathcal{D}}) = E_1 \cdots E_r X E_{r+1} \cdots E_m$ and $X \cong SL_2(\mathcal{O}_{S,\mathcal{D}})$. Thus by Lemma 1.13 it is enough to show that $SL_2(\mathcal{O}_{S,\mathcal{D}})$ has bounded generation. Let

$$C := \{X \in SL_n(\mathcal{O}_{S,\mathcal{D}}) \mid X \equiv I \pmod{(2\alpha\beta)}\}.$$

This is a congruence subgroup and thus has finite index in $SL_n(\mathcal{O}_{S,\mathcal{D}})$ by Lemma 1.6. By our previous remark and theorem,

$$\phi(C) \subset \mathrm{Spin}(V)_{\mathcal{O}_S} \cap \phi(SL_n(\mathcal{O}_{\mathcal{D},S}),$$

and since $\mathrm{Spin}(V)_{\mathcal{O}_S} \subset \phi(SL_n(\mathcal{O}_{S,\mathcal{D}}))$, $\phi(C)$ has finite index in $\mathrm{Spin}(V)_{\mathcal{O}_S}$ so it and $\phi(SL_n(\mathcal{O}_{S,\mathcal{D}}))$ are commensurable. Since S contains a nonarchimedean valuation, and the Witt index of the relevant form is 1, by Theorem 1.38 $\mathrm{Spin}(V)_{\mathcal{O}_S}$ has bounded generation. Then by Corollary 1.2 $SL_n(\mathcal{O}_{\mathcal{D},S})$ has bounded generation. □

Chapter 3

SU_n has bounded generation

3.1 Induction Step

In this chapter we prove that special unitary groups of hermitian forms over $L|K$ with Witt index at least 2 over a ring of S-integers have bounded generation. We first reduce the problem to the case SU_4 and then show this group is isomorphic to a spin group and then again use Theorem 1.38.

Let K be an algebraic number field, $L = K(\sqrt{d})$ a quadratic extension. We fix a finite subset $S \subset V^K$ containing V_∞^K.

Let $\langle \cdot, \cdot \rangle$ be a non-degenerate sesquilinear Hermitian form on L^n and define the quadratic form $f(x) = \langle x, x \rangle$. Throughout we assume that the Witt index is at least one and $n \geq 5$.

Fix a basis $e_1, \ldots, e_n$ of L^n such that

$$f(x_1e_1+\cdots+x_ne_n) = x_1\tau(x_2)+x_2\tau(x_1)+x_3\tau(x_4)+x_4\tau(x_3)+\alpha_5x_5\tau(x_5)+\cdots+\alpha_nx_n\tau(x_n).$$

Let F denote the matrix corresponding to $\langle \cdot, \cdot \rangle$. Throughout $G = SU_{n,F}$ and thus $G_K = SU_{n,F}(L)$. For $v \in V_f^K$,

$$G_{\mathcal{O}_v} = SU_{n,F}(\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_v)$$

and for $S \subset V^K$,

$$G_{\mathcal{O}_S} = SU_{n,F}(\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_S).$$

For $a \in L^n$, $G(a)$ denotes the stabilizer of a in G.

Lemma 3.1. *Assume that $n \geq 5$ and f has Witt index at least 1. Let $a, b \in L^n$ with $\langle a, b\rangle = 0$, $f(a) \neq 0$ and $f(b) \neq 0$. If $\operatorname{span}_L(a,b)^\perp$ is isotropic, then we have following for every extension $K'|K$ we have that $G_{K'} = G(a)_{K'}G(b)_{K'}G(b)_{K'}$.*

Proof. We define the K-varieties

$$\begin{aligned} X &= G(a) \times G(b) \times G(a), \\ Y &= \{t \mid f(t) = f(a)\}, \\ Z &= \{(g,t) \in G \times Y \mid \langle t, a\rangle = \langle g(a), a\rangle, \langle t, b\rangle = \langle a, b\rangle\}. \end{aligned}$$

The product map $\mu\colon X \to G$ factors through the maps $\phi\colon X \to Z$ given by $\phi(x,y,z) = (xyz, y(a))$ and $\psi\colon Z \to G$ given by $\psi(g,t) = g$.

To prove the lemma we must consider two cases.

Case 1: Assume $K' \otimes_K L$ is a field. We show that $G_{K'} = G(a)_{K'}G(b)_{K'}G(a)_{K'}$ by showing that ϕ and ψ are surjective on K'-points. Let $g \in G_{K'}$ and define $t' := \dfrac{\langle g(a), a\rangle}{f(a)} a$. Since $\operatorname{span}_{L\otimes K'}(a,b)^\perp$ is isotropic, by Lemma 1.17 it contains a vector t'' such that $f(t'') = f(a) - f(t')$. Let $t = t'' + t'$. Since t' and t'' are orthogonal we can see that $f(t) = f(t'') + f(t') = f(a)$. We also have that

$$\begin{aligned} \langle t, a\rangle &= \langle t', a\rangle \\ &= \frac{\langle g(a), a\rangle}{f(a)} \langle a, a\rangle \\ &= \langle g(a), a\rangle \end{aligned}$$

and $\langle t, b\rangle = 0 = \langle a, b\rangle$. Thus $(g,t) \in Z_{K'}$ implying that $\psi^{-1}(g)_{K'}$ is nonempty.

Let $(g,t) \in Z_{K'}$. Assume $g(a) = \lambda a$ for some $\lambda \in K' \otimes L$. Then since $\langle g(a), g(a)\rangle = \langle a, a\rangle$, $\lambda\tau(\lambda) = 1$. Let $c \in \operatorname{span}_{K'\otimes L}(a,b)^\perp$ such that $\langle c, c\rangle \neq 0$. Let $h = \sigma_{\lambda-1,c}\sigma_{\bar{\lambda}-1,a}$

where $\sigma_{l,w}$ is as defined in the proof of Corollary 1.19. We can see that $h \in G(b)_{K'}$ and $gh \in G(a)_{K'}$ so $g \in G(a)_{K'}G(b)_{K'}G(a)_{K'}$. Therefore we may assume that $g(a) \neq \lambda a$ and the spaces $\text{span}_{K'\otimes L}(t, a)$ and $\text{span}_{K'\otimes L}(g(a), a)$ are isometric and 2-dimensional. By Corollary 1.19 there exists $x \in G_{K'}$ such that $x(t) = g(a)$ and $x(a) = a$. Similarly, there exists $y \in G_{K'}$ such that $y(a) = t$ and $y(b) = b$. Let $z = (xy)^{-1}g$. By construction, $xyz = g$, $x \in G(a)_{K'}$, $y \in G(b)_{K'}$ and

$$\begin{aligned} z(a) &= y^{-1}(x^{-1}(g(a))) \\ &= y^{-1}(t) \\ &= a \end{aligned}$$

so $z \in G(a)_{K'}$. Since $y(a) = t$ we have that $(x, y, z) \in \phi^{-1}(g, t)_{K'}$.

Thus μ is surjective on K'-points, implying $G_{K'} = G(a)_{K'}G(b)_{K'}G(a)_{K'}$.

Case 2: Assume $K' \otimes L \cong K' \oplus K'$. In this case by the argument in Proposition 1.43 there is an isomorphism $\phi\colon G_{K'} \to SL_n(K')$. Notice that under this map the requirement that $ga = a$ for $g \in G_{K'}$ becomes $\phi(g)v = v$ for some $v \in K'^n$. Thus there is a change of basis such that

$$A := \phi(G(a)_{K'}) = \begin{bmatrix} SL_{n-1}(K') & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$B := \phi(G(b)_{K'}) = \begin{bmatrix} 1 & 0 \\ 0 & SL_{n-1}(K') \end{bmatrix}.$$

The result is then equivalent to showing that for any $X \in SL_n$ there exists $a_1, a_2 \in A$ such that $a_1Xa_2 \in B$. Let $r_1, \ldots, r_n$ denote the rows of X and let $c_1, \ldots c_n$ denote the colums. Notice that the following operations are equivalent to multiplying X by an element of A:

- $r_i \mapsto mr_j + r_i$ for any $i \neq j$, $i, j > 1$ and $m \in K'$ (RA),

- $c_i \mapsto mc_j + c_i$ for any $i \neq j$, $i, j > 1$ and $m \in K'$ (CA),
- $r_i \mapsto r_j$ and $r_j \mapsto -r_i$ for any $i \neq j$, $i, j > 1$(RS),
- $c_i \mapsto c_j$ and $c_j \mapsto -c_i$ for any $i \neq j$, $i, j > 1$(CS),
- $c_i \mapsto nc_i$ and $c_j \mapsto \frac{1}{n}c_j$ for any $i \neq j$, $i, j > 1$ and $n \neq 0$ (Sc).

If for all $1 < i < n$, $[X]_{1i} = 0$ and $[X]_{1n} \neq 0$, we perform a (CS) so $[X]_{1n} = 0$, and if for all $1 < i < n$ $[X]_{i1} = 0$ and $[X]_{n1} \neq 0$ we perform a (RS) so $[X]_{n1} = 0$. After possibly performing a (RS) and (CS), we can guarentee that $[X]_{nn} \neq 0$. (Note that since $n \geq 4$, we can guarentee that the action does not effect the result of the first two operations). By adding appropriate multiples of r_n to r_i for $1 < i < n$ we obtain $[X]_{in} = 0$. If $[X]_{n1} \neq 0$, there exists i such that $[X]_{i1} \neq 0$ and by adding a multiple of r_i to r_n we now have that $[X]_{n1} = 0$. (Note that this will not change the value of $[X]_{nn}$.) By adding multiples of c_n to c_i for $1 < i < n$ we obtain $[X]_{ni} = 0$ for $1 \leq i < n$. If $[X]_{1n} \neq 0$ there exists i such that $[X]_{1i} \neq 0$ and by adding a multiple of c_i to c_n we now have that $[X]_{1n} = 0$. (Note that this did not change the value of $[X]_{ni}$ for $1 \leq i \leq n$.) As before by adding multiples of r_n to r_i we have that $[X]_{in} = 0$ for $1 \leq i < n$. By performing a (Sc) operation we can obtain $[X]_{nn} = 1$ and $X \in B$. Thus $SL_n = ABA$ implying $G_{K'} = G(a)_{K'}G(b)_{K'}G(a)_{K'}$. □

Corollary 3.2. *Let $v \in V^K$, $A, C \subset G(a)_{K_v}$ open, $B \subset G(b)_{K_v}$ open, then there exists a open subset of $\mu(A, B, C) = ABC$ in G_{K_v}.*

Proof. Lemma 3.1 shows that the product map is surjective, so the claim follows from Corollary 1 in section 3.1 of [17]. □

Fix $V_0 := V(d) \cup_{i=5}^{n} V(\alpha_i)$. Let $a := e_n$, $b := e_{n-1}$. By the previous corollary there exists an open compact subset U of $G_{V_0} = \prod_{v \in V_0} G_{K_v}$ contained in $\prod_{v \in V_0} G(a)_{\mathcal{O}_v}G(b)_{\mathcal{O}_v}G(a)_{\mathcal{O}_v}$. We can further assume that $U \subset \{g \in G \mid g(a) \text{ and } a \text{ are linearly independent}\}$.

Theorem 3.3. *Let $\Delta = G(a)_{\mathcal{O}_S} G(b)_{\mathcal{O}_S} G(a)_{\mathcal{O}_S}$, then $G_{\mathcal{O}_S} \cap U \subset \Delta\Delta\Delta$.*

We first prove several lemmas.

Lemma 3.4. *Let $(g,t) \in Z_{\mathcal{O}_S}$. Suppose that*

1) $\phi^{-1}(g,t)_K$ and $\phi^{-1}(g,t)_{\mathcal{O}_v}$ are non-empty for all $v \notin S$.

2) The subspace spanned by a and t is two-dimensional and nondegenerate.

Then $\phi^{-1}(g,t)_{\mathcal{O}_S}$ is nonempty, hence $g \in \Delta$.

Proof. By condition 1 there exists $(x_K, y_K, z_K) \in \phi^{-1}(g,t)_K$ and $(x_v, y_v, z_v) \in \phi^{-1}(g,t)_{\mathcal{O}_v}$ for each $v \notin S$. By construction $x_K(t) = g(a)$ and $x_v(t) = g(a)$ with $x_K \in G(a)_K$ and $x_v \in G(a)_{\mathcal{O}_v}$. Therefore we have that $(x_K^{-1} x_v)_{v \notin S} \in G(a,t)_{A_{K,S}}$. By Proposition 1.41, $G(a,t)_{A_{K,S}} = G(a,t)_K \prod_{v \notin S} G(a,t)_{\mathcal{O}_v}$, so there exists $h_K \in G(a,t)_K$, $h_v \in G(a,t)_{\mathcal{O}_v}$ such that $(h_K h_v)_{v \notin S} = (x_K^{-1} x_v)_{v \notin S}$. Then $x_K h_K = x_v h_v^{-1} \in G(a)_{\mathcal{O}_v}$ for all $v \notin S$, so $x_K h_K \in G(a)_{\mathcal{O}_S}$. Similarly we have that $y_K(a) = t$ and $y_v(a) = t$ with $y_K \in G(b)_K$ and $y_v \in G(b)_{\mathcal{O}_v}$ implying that $(y_K^{-1} y_v) \in G(a,b)_{A_{K,S}}$ and that there exists $j_K \in G(a,b)_K$ such that $y_K j_K \in G(b)_{\mathcal{O}_S}$. Let $x = x_K h_K$, $y = y_K j_K$, $z = (xy)^{-1} g$. Then $(x,y,z) \in \phi^{-1}(g,t)_{\mathcal{O}_S}$ as desired. □

We use the same notations as in Theorem 1.20.

Lemma 3.5. *Let $(g,t) \in Z_{\mathcal{O}_S}$. Assume that:*

1) The space spanned by a and t is two-dimensional and nondegenerate.

2) $\phi^{-1}(g,t)_{\mathcal{O}_v}$ is nonempty for all $v \in V_0$.

3) For any $v \in V^K \setminus (S \cup V_0)$ the ℓ_v-modules $\mathrm{span}_{\ell_v}(\bar{a}^{(v)}, \overline{g(a)}^{(v)})$, $\mathrm{span}_{\ell_v}(\bar{a}^{(v)}, \bar{t}^{(v)})$, and $\mathrm{span}_{\ell_v}(\bar{b}^{(v)}, \bar{t}^{(v)})$ are free and 2-dimensional.

Then $\phi^{-1}(g,t)_{\mathcal{O}_S}$ is not empty and thus $g \in \Delta$.

Proof. Let $v \in V^K \setminus (S \cup V_0)$. Since $\mathrm{span}_{\ell_v}(\overline{g(a)}^{(v)}, \bar{a}^{(v)})$ and $\mathrm{span}_{\ell_v}(\bar{t}^{(v)}, \bar{a}^{(v)})$ are free 2-dimensional modules, $f(t) = f(a) = f(g(a))$, and $\langle g(a), a \rangle = \langle t, a \rangle$, by Theorem 1.20 there exists $x \in G_{\mathcal{O}_v}$ such that $x(t) = g(a)$ and $x(a) = a$. Similarly since

$\text{span}_{\ell_v}(\bar{t}^{(v)}, \bar{b}^{(v)})$ and $\text{span}_{\ell_v}(\bar{a}^{(v)}, \bar{b}^{(v)})$ are free 2-dimensional modules and $\langle t, b\rangle = \langle a, b\rangle$ there exists $y \in G_{\mathcal{O}_v}$ such that $y(t) = a$ and $y(b) = b$. Let $z = (xy)^{-1}g$. Then $(x, y, z) \in \phi^{-1}(g, t)_{\mathcal{O}_v}$ so $\phi^{-1}(g, t)_{\mathcal{O}_v}$ is nonempty for all $v \in V^K \setminus (S \cup V_0)$ and by condition 2), $\phi^{-1}(g, t)_{\mathcal{O}_v}$ is nonempty for all $v \in V^K \setminus S$. Thus by condition 1) and Lemma 3.4 $\phi^{-1}(g, t)_{\mathcal{O}_S}$ is not empty. □

Lemma 3.6. *Given $g \in G_{\mathcal{O}_S} \cap U$ there exists $\delta \in \Delta\Delta$ such that $\text{span}_{\ell_v}(\bar{a}^{(v)}, \overline{\delta g(a)}^{(v)})$ is a 2-dimensional free module for all $v \in V^K \setminus (S \cup V_0)$.*

Proof. Choose an open subgroup $\Omega \subseteq G_{V_0}$ such that $\Omega U = U$. We first verify that such an Ω exists. Notice that the multiplication map $\mu : G_{V_0} \times G_{V_0} \to G_{V_0}$ is continuous, implying $\mu^{-1}(U)$ is open. For any $x \in U$, the element $(1, x)$ is in $\mu^{-1}(U)$ so there exists a basic open set $T_x \times U_x \subset \mu^{-1}(U)$ such that T_x contains 1 and U_x contains x. The U_x's form an open cover for U. By construction U is compact so there exists $x_1, \ldots, x_m$ with $U_{x_1} \cup \cdots \cup U_{x_m} = U$. Let $T := \cap_{i=1} T_{x_i}$. We can see that $TU = U$ since T contains 1 and thus $U \subseteq TU$, and we also have that $T_{x_i} U_{x_i} \subseteq U$. Thus an appropriate open subgroup $\Omega \subseteq T$ exists.

Let

$$\Delta_\Omega = (G(a)_{\mathcal{O}_S} \cap \Omega)(G(b)_{\mathcal{O}_S} \cap \Omega)(G(a)_{\mathcal{O}_S} \cap \Omega).$$

By the Borel Density Theorem (Theorem 4.33 in [17]) $G(a)_{\mathcal{O}_S} \cap \Omega$ and $G(b)_{\mathcal{O}_S} \cap \Omega$ are Zariski-dense in $G(a)$ and $G(b)$ respectively, and thus by Lemma 3.1 Δ_Ω is dense in G. Let

$$(x)_m = \langle x, e_m\rangle \,/\, \langle e_m, e_m\rangle .$$

The set of all $g' \in G$ with the property that $(g'g(a))_{n-1} \neq 0$ is Zariski-open and nonempty. Therefore there is a $\delta_1 \in \Delta_\Omega$ such that $\beta := (\delta_1 g(a))_{n-1} \neq 0$. If $\bar{\beta}^{(v)}$ is invertible, then clearly $\bar{a}^{(v)}$ and $\overline{\delta g(a)}^{(v)}$ are linearly independent and generate a 2-dimension free ℓ_v-module. Let

$$V_1 = (V^K \setminus (S \cup V_0)) \cap V(\beta\tau(\beta)).$$

For each $v \in V_1$ the set $W_v \subset G(b)_{\mathcal{O}_v}$ such that for every $h_v \in W_v$, $\mathrm{span}_{\ell_v}(\overline{h_v \delta_1 g(a)}^{(v)}, \bar{a}^{(v)})$ is a 2-dimensional free module is open. The subgroup $G(b)$ has strong approximation so there exists

$$\delta_2 \in G(b)_{\mathcal{O}_S} \cap \prod_{v \in V_1} W_v \times \Omega.$$

Then for all $v \in V^K \setminus (S \cup V_0)$, we have that $\mathrm{span}_{\ell_v}(\overline{\delta_2 \delta_1 g(a)}^{(v)}, \bar{a}^{(v)})$ is a 2-dimensional free ℓ_v-module. Taking $\delta = \delta_1 \delta_2$ proves the lemma. □

Lemma 3.7. *Let $g \in G_{\mathcal{O}_S} \cap U$. There exists $t \in Y_{\mathcal{O}_S}$ such that $(g,t) \in Z_{\mathcal{O}_S}$, satisfies conditions 1 and 2 of Lemma 3.5, and in addition both $\mathrm{span}_{\ell_v}(\bar{a}^{(v)}, \bar{t}^{(v)})$ and $\mathrm{span}_{\ell_v}(\bar{b}^{(v)}, \bar{t}^{(v)})$ are 2-dimensional free modules.*

Proof. Let $t' = (g(a))_n a$ and

$$r = \frac{f(a)^2 - \langle g(a), a \rangle \, \tau(\langle g(a), a \rangle)}{f(a)} = f(a) - f(t').$$

Since $g \in U$, $\langle g(a), a \rangle \neq \lambda f(a)$ with $\lambda \bar{\lambda} = 1$, thus we have that $r \neq 0$.

Let

$$C = \{(x_1, \ldots, x_{n-2}, 0, 0) \mid f(x_1, \ldots, x_{n-2}, 0, 0) = r\}$$

and

$$V_2 = (V^K \setminus (S \cup V_0)) \cap V(r).$$

Since $g \in U$ for all $v \in V_0$ there exists $x_v, z_v \in G(a)_{\mathcal{O}_v}$, $y_v \in G(b)_{\mathcal{O}_v}$ such that

$g = x_v y_v z_v$. Let $s_v := y_v(a) - t'$. Computing $f(s_v)$ we get:

$$\begin{aligned}
f(s_v) &= \langle y_v(a) - t', y_v(a) - t' \rangle \\
&= \langle y_v(a), y_v(a) \rangle - \langle y_v(a), t' \rangle - \langle t', y_v(a) \rangle + \langle t', t' \rangle \\
&= \langle a, a \rangle - \langle y_v(a), (g(a))_n a \rangle - \langle (g(a))_n a, y_v(a) \rangle + \langle (g(a))_n a, (g(a))_n, a \rangle \\
&= f(a) - \tau((g(a))_n \langle g(a), a \rangle - (g(a))_n \langle a, g(a) \rangle + (g(a))_n \tau((g(a))_n) f(a) \\
&= f(a) - (g(a))_n \tau((g(a))_n) f(a) \\
&= f(a) - \langle a, g(a) \rangle \langle g(a), a \rangle \frac{1}{f(a)} \\
&= \frac{f(a)^2 - \langle g(a), a \rangle \tau(\langle g(a), a \rangle)}{f(a)} \\
&= r
\end{aligned}$$

Since $(s_v)_n = (y_v(a))_n - (t')_n = 0$ and $(s_v)_{n-1} = 0$, $s_v \in C_{\mathcal{O}_v}$.

For each $v \in V_0$ define $R_v := G(a, b)_{\mathcal{O}_v} s_v$. By Corollary 2 of Proposition 3.3 in [17] we have that R_v is open in $C_{\mathcal{O}_v}$. For each $v \in V_2$ define

$$R_v := \{ s \in C_{\mathcal{O}_v} \mid (s)_1 \in (\mathcal{O}_L \otimes_{K_v} \mathcal{O}_v)^* \}.$$

This set is also open, and it contains $(1, \frac{r}{2}, 0, \ldots, 0)$ so it is nonempty. The variety C has strong approximation with respect to S by Corollary 1.45 so there exists $t'' \in C_{\mathcal{O}_S} \cap \prod_{v \in V_0 \cup V_2} R_v$. Set $t := t'' + t'$, then

$$f(t) = f(t'') + f(t') + \langle t'', t' \rangle + \langle t', t'' \rangle = f(a),$$

and therefore t is in $Y_{\mathcal{O}_S}$. Computing, we see that

$$\langle t, a \rangle = \langle t', a \rangle = \langle g(a), a \rangle$$

and

$$\langle t, b \rangle = \langle t', b \rangle = 0,$$

so $(g,t) \in Z_{\mathcal{O}_S}$. By construction $\mathrm{span}_{\ell_v}(a,t) = \mathrm{span}_{\ell_v}(a,t'')$ which is 2-dimensional and nondegenerate.

For each $v \in V_0$, $t'' = h_v s_v$ with $h_v \in G(a,b)_{\mathcal{O}_v}$. Then

$$h_v y_v = h_v(t' + s_v) = t' + t'' = t$$

implying that $(x_v h_v^{-1}, h_v y_v, z_v) \in \phi^{-1}(g,t)_{\mathcal{O}_v}$. For all $v \notin S \cup V_0$, we have $\bar{t}^{(v)} \neq 0$. Therefore $\mathrm{span}_{\ell_v}(\bar{a}^{(v)}, \bar{t}^{(v)})$ and $\mathrm{span}_{\ell_v}(\bar{b}^{(v)}, \bar{t}^{(v)})$ are 2-dimensional free modules for all $v \in V^K \setminus (S \cup V_0)$ as desired. □

3.2 Base Case

Theorem 3.8. *Let* $G = SU_{4,F}$ *where* $F = \begin{bmatrix} r & 0 & 0 & 0 \\ 0 & -r & 0 & 0 \\ 0 & 0 & -s & 0 \\ 0 & 0 & 0 & s \end{bmatrix}$ *and* $r, s \in \mathcal{O}_S$ *nonzero. Let* $V = K^6$ *with quadratic form* $q = dx_1^2 - x_2^2 - dx_3^2 + x_4^2 - rsx_5^2 + rsdx_6^2$, $H = \mathrm{Spin}(V)$. *Then* $H_K \cong G_K$.

Proof. We begin by demonstrating an explicit isomorphism $\phi : Cl^0(V) \to M_4(L)$ and showing that the involution on the Clifford algebra induces an involution on $M_4(L)$ taking $X \to F^{-1}X^*F$. Given such an isomorphism, the image of its restriction to $Cl^+(V) \cap Cl^0(V)$ is $U_{4,F}(L)$. Let $\phi' = \phi|_{U_{4,F}}$. This map extends to an isomorphism

$$U_{4,F}(\bar{K}) \to (Cl^+(V) \cap Cl^0(V))_{\bar{K}}.$$

By Theorem 1.37 the commutator subgroup of $(Cl^+(V) \cap Cl^0(V))_{\bar{K}}$ contains $\mathrm{Spin}(V)_{\bar{K}}$. By Proposition 1.27 the commutator subgroup of $U_{4,F}$ is $SU_{4,F}$. Therefore $\mathrm{Spin}(V)_{\bar{K}}$ is contained in the image of $\phi'(G_{\bar{K}})$. As varieties $\dim \mathrm{Spin}(V) = \dim SU_{4,f} = 15$ (see [18]) so we have $\mathrm{Spin}(V)_K = \phi'(SU_{4,F}(L))$.

It remains to show that there exists an appropriate isomorphism $Cl^0(V) \to M_4(L)$. We do this by composing a few isomorphisms. Define V' as the vector space V with quadratic form given by

$$q = dx_1^2 - x_2^2 - \frac{1}{d}x_3^2 + x_4^2 - \frac{r}{s}x_5^2 + \frac{s}{r}dx_6^2.$$

Then there is an isomorphism $Cl^0(V) \to Cl^0(V')$. By Theorem 1.36 we have that

$$Cl^0(V') \cong \mathcal{D}_1 \otimes_K \mathcal{D}_2 \otimes_K A$$

where $\mathcal{D}_1 = \left(\frac{1, d}{K}\right)$, $\mathcal{D}_2 = \left(\frac{1, -\frac{r}{s}}{K}\right)$ and

$$A = K[t]/\left\langle t^2 - d \right\rangle \cong K[\sqrt{d}] = L.$$

The induced involution, τ_1, on $\mathcal{D}_1$ is the standard quaternion involution, the induced involution, τ_2, on $\mathcal{D}_2$ is the involution given in Example 1.32, and the induced involution, τ_3, on A takes t to $-t$.

By Lemma 1.11 there exists an isomorphism $\phi_2 \colon \mathcal{D}_2 \to M_2(K)$ with

$$\phi_2(\tau_2(\phi_2^{-1}(X))) = \begin{bmatrix} -\frac{1}{r} & 0 \\ 0 & \frac{1}{s} \end{bmatrix} X^t \begin{bmatrix} -r & 0 \\ 0 & s \end{bmatrix}.$$

Similarly, we construct an isomorphism $\mathcal{D}_1 \otimes L \to M_2(L)$. Let $1, i, j, k$ be the standard basis for $\mathcal{D}_1$. We can see that the elements $i' := i \otimes \sqrt{d}$, $j' := \frac{1}{d}j \otimes \sqrt{d}$ and $1 \otimes \sqrt{d}$ generate $\mathcal{D}_1 \otimes L$, and the subalgebra generated by i' and j' is isomorphic to the quaternion algebra $\mathcal{D}_1' = \left(\frac{d^2, -1}{K}\right)$, therefore we have an isomoprhism $\phi_1' \colon \mathcal{D}_1 \otimes L \cong \mathcal{D}_1' \otimes L$, and

$$\phi_1' \circ (\tau_1 \otimes \tau_3) \circ (\phi_1')^{-1} = \tau_2' \otimes \tau_3$$

where τ_2' is the involution given in Example 1.32. By Lemma 1.11 there exists an isomorphism $\phi_1 \colon D_1' \to M_2(K)$ with

$$\phi_1(\tau_2'(\phi_1^{-1}(X))) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} X^t \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Combining these maps we can we that there is a map $Cl^0(V) \to M_2(L) \otimes M_2(K)$, which is isomorphic to $M_4(L)$. Following the maps we see that the induced involution is given by $F^{-1}X^*F$. So by the previous argument there exists an isomorphism $\phi\colon \mathrm{Spin}(V) \to U_{4,F}(L)$. □

We can now prove

Theorem 3.9 (Main Theorem 2)**.** *Let $\langle \cdot, \cdot \rangle$ be a nondegenerate sesquilinear form on L^n, let F be the associated matrix, and let $G = SU_{n,F}$. Fix $S \subset V^K$ finite such that $V_\infty^K \subset S$. If f has Witt index at least 2 then $G_{\mathcal{O}_S}$ has bounded generation.*

Proof. If $G(a)_{\mathcal{O}_S}$ and $G(b)_{\mathcal{O}_S}$ have bounded generation then $\Delta\Delta\Delta$ will have bounded generation. Since G has Witt index 2, there exists an open U such that $G_{\mathcal{O}_S} \cap U \subset \Delta\Delta\Delta \subset G_{\mathcal{O}_S}$, implying that $\Delta\Delta\Delta$ has finite index in $G_{\mathcal{O}_S}$. Therefore $G_{\mathcal{O}_S}$ has bounded generation by Proposition 1.1. If $n > 4$ we can always choose a, b such that the sesquilinear forms associated to $G(a)$ and $G(b)$ have Witt index at least 2. If $n = 4$ then having Witt index 2 implies that there exists a change of basis such that F is of the form given in Theorem 3.8. Therefore the problem reduces to showing $G_{\mathcal{O}_S}$ has bounded generation in that case. By Theorem 3.8 and Corollary 1.3, $G_{\mathcal{O}_S}$ has bounded generation if and only if $\mathrm{Spin}(V)_{\mathcal{O}_S}$ does, but q has Witt index 2 so by Theorem 1.38 $\mathrm{Spin}(V)_{\mathcal{O}_S}$ has bounded generation. □

Bibliography

[1] E. Artin. *Geometric algebra*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1988. Reprint of the 1957 original, A Wiley-Interscience Publication.

[2] Bachir Bekka, Pierre de la Harpe, and Alain Valette. *Kazhdan's property (T)*, volume 11 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2008.

[3] David Carter and Gordon Keller. Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$. *Amer. J. Math.*, 105(3):673–687, 1983.

[4] Jean Dieudonné. *La géométrie des groupes classiques*. Seconde édition, revue et corrigée. Springer-Verlag, Berlin, 1963.

[5] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.

[6] Igor V. Erovenko. *Bounded generation of S-arithmetic orthogonal groups*. ProQuest LLC, Ann Arbor, MI, 2002. Thesis (Ph.D.)–University of Virginia.

[7] Igor V. Erovenko and Andrei S. Rapinchuk. Bounded generation of some S-arithmetic orthogonal groups. *C. R. Acad. Sci. Paris Sér. I Math.*, 333(5):395–398, 2001.

[8] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[9] Larry C. Grove. *Classical groups and geometric algebra*, volume 39 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.

[10] Nathan Jacobson. *Basic algebra. II*. W. H. Freeman and Company, New York, second edition, 1989.

[11] V. Kumar Murty. Bounded and finite generation of arithmetic groups. In *Number theory (Halifax, NS, 1994)*, volume 15 of *CMS Conf. Proc.*, pages 249–261. Amer. Math. Soc., Providence, RI, 1995.

[12] T. Y. Lam. *The algebraic theory of quadratic forms*. W. A. Benjamin, Inc., Reading, Mass., 1973. Mathematics Lecture Note Series.

[13] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[14] Lucy Lifschitz and Dave Witte Morris. Bounded generation and lattices that cannot act on the line. *Pure Appl. Math. Q.*, 4(1, Special Issue: In honor of Grigory Margulis. Part 2):99–126, 2008.

[15] V. P. Platonov. Birational properties of spinor varieties. *Trudy Mat. Inst. Steklov.*, 157:161–169, 236–237, 1981. Number theory, mathematical analysis and their applications.

[16] V. P. Platonov and A. S. Rapinchuk. Abstract properties of S-arithmetic groups and the congruence problem. *Izv. Ross. Akad. Nauk Ser. Mat.*, 56(3):483–508, 1992.

[17] Vladimir Platonov and Andrei Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.

[18] Ian R. Porteous. *Clifford algebras and the classical groups*, volume 50 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1995.

[19] A. S. Rapinchuk. Combinatorial theory of arithmetic groups. Preprint, Institute of Mathematics, Academy of Sciences of Belarus, 1990.

[20] A. S. Rapinchuk. The congruence subgroup problem for algebraic groups and strong approximation in affine varieties. *Dokl. Akad. Nauk BSSR*, 32(7):581–584, 668, 1988.

[21] Andrei S. Rapinchuk and Gopal Prasad. Developments on the congruence subgroup problem after the work of bass, milnor and serre, 2008. arXiv:0809.1622.

[22] Andrei S. Rapinchuk and Yoav Segev. Valuation-like maps and the congruence subgroup property. *Invent. Math.*, 144(3):571–607, 2001.

[23] Yehuda Shalom and George A. Willis. Commensurated subgroups of arithmetic groups, totally disconnected groups and adelic rigidity, 2009. arXiv:0911.1966v1.

[24] O. I. Tavgen. Bounded generation of Chevalley groups over rings of algebraic S-integers. *Izv. Akad. Nauk SSSR Ser. Mat.*, 54(1):97–122, 221–222, 1990.