The Classification of Arithmetic Subgroups of $SO(n,1)$: DRAFT

William Jones

October 22, 2025

Contents

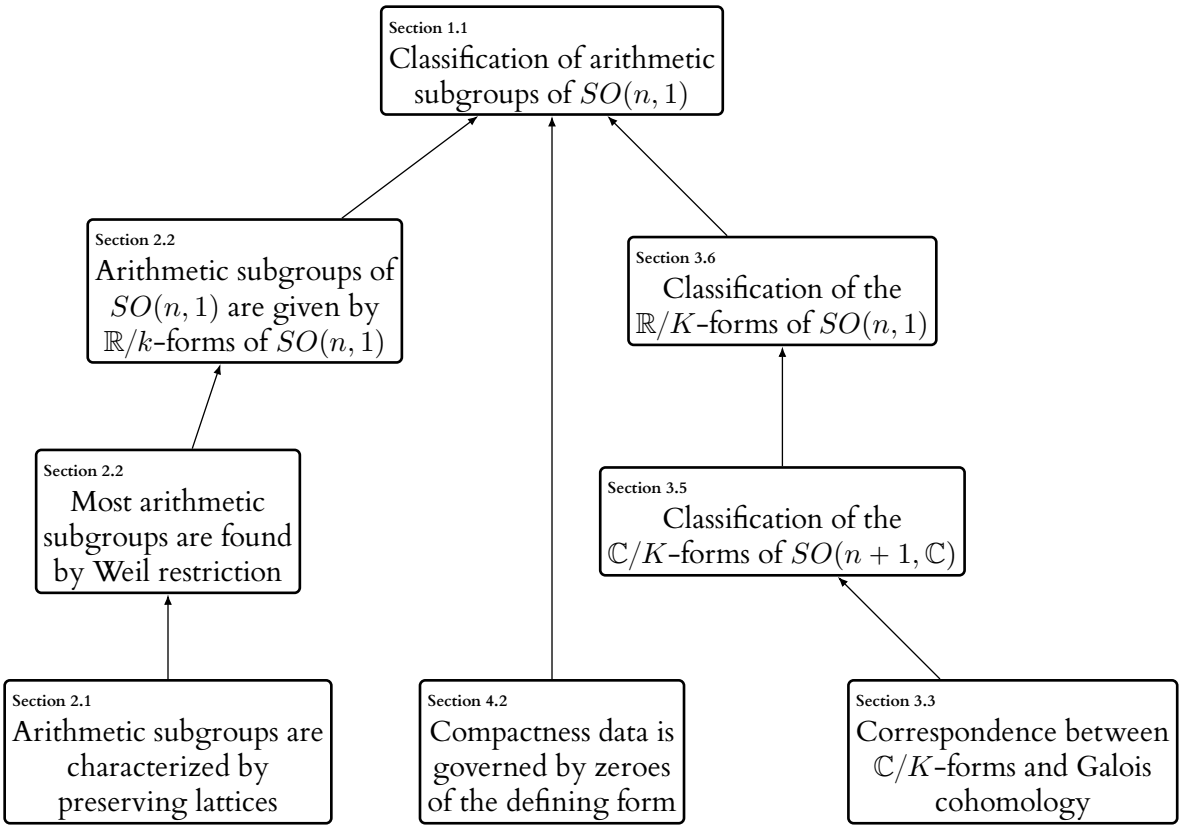

Fig 1: Logical dependency diagram for the classification.

1 Background

1.1 Introduction

The following note is an attempt at a (reasonably) self-contained proof of the following classification of arithmetic subgroups of the real Lie group $SO(n,1)$.

Theorem 0 (Classification Theorem for Arithmetic Lattices in $SO(n,1)$).

Let Γ be an arithmetic lattice in $SO(n,1)$, where $n \neq 7$. Then:

1. If Γ is non-cocompact, then it is an inner lattice defined over $\mathbb{Q}$: it is commensurable with the group of units of an admissible quadratic form defined over $\mathbb{Q}$
2. If Γ is cocompact, then there are two possibilities:
   (a) Γ is an inner lattice defined over a number field k. Moreover, if $n > 3$, k cannot be $\mathbb{Q}$.
   (b) n is odd, and Γ is an outer lattice: it is commensurable with the the group of units of an admissible skew-Hermitian form on a quaternion algebra.

If $n = 7$, then all relevant groups described above are arithmetic, but there are more of them.

The terminology in this theorem is defined in bold-text throughout this note, but the "new" terminology (e.g., inner, outer, admissible) is defined in §3.6.

As far as I've seen, people trace the origin of this classification to [9], in which the relationship between algebras with involution and the classical groups is studied; this serves a vital role in §3. However, the explicit proof I will be presenting is based primarily on various elements in [6], [5], and [1]. In particular, the notion of "arithmetic" subscribed to in this note is that described in [5], although at various times the (someteimes narrower) algebro-geometric notion will come into play.

A few facts will be assumed; e.g., about basic properties of Lie groups, or about semisimple algebras with involution; when the statements are (I think) believable and easy to find proofs of, but otherwise I will try to provide a proof of everything written.

Also, I might use results/definitions that hold true for $\mathbb{Q}$ on things defined over number fields. This is always fine, as $\mathbb{Q}$ is a finite index subgroup of k, so up to commensurability the "$\mathbb{Q}$-things" are the same as the "k-things."

Proofs end with $\square$, notable remarks end with $\diamondsuit$, and examples end with $\triangle$.

1.2 Basic Definitions: Arithmetic Subgroups and $SO(n,1)$

As mentioned in the introduction, we will be following the definition of an arithmetic group in [5]. In particular, all of the nice corollaries proved in that book hold true about the arithmetic groups we will be discussing.

For the purposes of this definition, let H be a semisimple subgroup of some $SL_n(\mathbb{R})$. We say that

H is **defined over** K, or is a K**-group** if there are polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_{n^2}]$ so that the variety $V = \mathbb{R}[x_1, \ldots, x_{n^2}]/(f_1, \ldots, f_m)$ is a subgroup of $SL_n(\mathbb{R})$, and H is commensurable to V.

Example. $SL(n,k)$ is a $\mathbb{Q}$-group for any field k, as it is given by $k[x_{11}, \ldots, x_{nn}]/(\det(-)-1)$. $GL(n,k)$ is a $\mathbb{Q}$-group for any field k; let $\det^*(-)$ be $\det$ of an $(n+1)\times(n+1)$ matrix restricted to the upper-left $n \times n$ block. Then one presentation of $GL(n,k)$ as an affine algebraic subvariety of $SL(n+1,k)$ is:

$$\frac{\mathbb{Q}[x_{11}, \ldots, x_{n+1,n+1}]}{(x_{n+1,1}, \ldots, x_{n+1,n}, x_{1,n+1}, \ldots, x_{n,n+1}, \det^*(-)x_{n+1,n+1} - 1)};$$

that is, we embed $GL(n,k)$ as the upper-left $n \times n$ block of those submatrices of $SL(n+1,k)$ of the form

$$\begin{bmatrix} M & 0 \\ 0 & \det(M)^{-1} \end{bmatrix}$$

for $M \in GL(n,k)$. The positive multiplicative group $\mathbb{R}^\times_{>0}$ is $\mathbb{Q}$-group; we may realize $\mathbb{R}^\times$ as $\mathbb{R}[x,y]/(xy-1)$, and $\mathbb{R}^\times_{>0}$ is the identity component. $\triangle$

In particular, H is a connected $\mathbb{Q}$-group if and only if H is the **identity component** H_0 of a group variety defined over $\mathbb{Q}$. When H is a $\mathbb{Q}$-group, it is reasonable to talk about its **integer points**: namely, $H_\mathbb{Z} = H \cap SL_n(\mathbb{Z})$, and in fact we have the following fundamental theorem in the theory of algebraic groups.

Theorem 1. *If H is defined over $\mathbb{Q}$, then $H_\mathbb{Z}$ is a discrete subgroup with finite covolume.*

Such subsets are called **lattices**. Now let G be a semisimple subgroup of some special linear group; the definition of arithmetic in [5] is as follows:

Definition (Arithmetic Subgroups of G)**.** We say a subgroup $\Gamma \leqslant G$ is **arithmetic** if and only if there is a closed, connected, semisimple $\mathbb{Q}$-subgroup H of some $SL_N(\mathbb{R})$, compact normal subgroups K, J of G_0 and H, and an isomorphism $\phi : G_0/K \to H/J$ so that $\phi(\Gamma \mod K)$ is commensurable to $H_\mathbb{Z} \mod J$.

We are interested primarily in the case that $G = SO(n,1)$, although the general definition of arithmetic will be relevant to us at times. To that end, since $SO(n,1)$ has no nontrivial compact normal subgroups (a normal subgroup of a connected simple Lie group lies in its center), it follows that we may make a small simplification in the above definition.

Definition (Arithmetic Subgroups of $SO(n,1)$)**.** We say a subgroup $\Gamma \leqslant SO(n,1)$ is **arithmetic** if there is a $\mathbb{Q}$-group $H \leqslant SL_\ell(\mathbb{R})$, a compact normal subgroup J of H, and an isomorphism $\phi : SO(n,1) \to H/J$ so that $\phi(\Gamma)$ is commensurable to $H_\mathbb{Z} \mod J$.

Remark. This definition shows that the data of an arithmetic subgroup is linked with the topological structure of the group, but we will soon see that there is an alternative definition which is more closely related to the algebraic data of the arithmetic group. $\Diamond$

If a lattice Γ in H is infinite (i.e., H is noncompact), we say Γ is **irreducible** if ΓN is dense in H, for every noncompact closed normal subgroup of H. If we squint, every semisimple Lie group looks like a product of simple Lie groups. This definition of irreducibility is equivalent to asking that in this product decomposition, the lattice Γ does not decompose as a product $\Gamma_1 \times \Gamma_2$ of two nontrivial lattices. In light of this interpretation, the following lemma is obvious.

Lemma 1. *If a connected $\mathbb{Q}$-group H is has a maximal compact normal subgroup K so that H/K is simple, then $H_{\mathbb{Z}}$ is irreducible.*

Proof. By Theorem 1, $H_{\mathbb{Z}}$ is a lattice in H.

Let N be a noncompact closed normal subgroup of H. Then N/K is a noncompact closed normal subgroup of H/K, and as H/K is simple, it follows that $N/K = H/K$. Thus $N = H$, and thus $H_{\mathbb{Z}}N = H_{\mathbb{Z}}H = H$ is (of course) dense in H. Thus $H_{\mathbb{Z}}$ is irreducible. □

2 Every Arithmetic Group is (almost) the Integer Points of Some Form

2.1 An Algebraic Characterization of Arithmetic Groups

The real-Lie-theoretic flavor of the definition of "arithmetic" in §1 is very useful for working with geometric properties of arithmetic groups, but is not immediately compatible with the algebraic properties. This is a problem, largely because the classification theorem is an algebraic claim. To address this, we will develop an alternative characterization of the theory, which is more in the style of [1].

In order to make things explicit, we will follow [5] in defining the following notions inside some ambient real space V. Note that most of this can be sidestepped by instead specifying a this data relative to some representation.

Given a number field k, we say that a k-vector space V_k is an **$\mathbb{R}/k$-form** of V if multiplication $V_k \otimes_k \mathbb{R} \to V$ is an isomorphism. A polynomial f on V is said to be **defined over k relative to V_k** if $f(V_k) \subset k$. If $\mathcal{O}$ is k's ring of integers, we say that a finitely generated subgroup $\mathcal{L}$ of V_k's additive group is a **$\mathcal{O}$-lattice of** V_k if multiplication $\mathcal{L} \otimes_{\mathcal{O}} k \to V_k$ is an isomorphism.

Note now that any vector space k-form of V produces a vector space k-form of $\operatorname{End} V$, via setting:

$$\operatorname{End}(V)_k = \{A : A(V_k) \subset V_k\}$$

We will say that a subgroup $G \leqslant SL(V)$ is a **k-group relative to** V_k if there are polynomials $f_1, \ldots, f_z$ on $\operatorname{End} V$ satisfying:

1. each f_i is k-defined relative to $\operatorname{End} V$,
2. the variety $V(f_1, \ldots, f_z)$ is a subgroup of $SL(V)$, and
3. H is commensurable to $V(f_1, \ldots, f_z)$.

The **standard k-form** of a vector space V with chosen basis $B = \{e_1, \ldots, e_n\}$ is $\oplus_i k e_i$, and the **standard $\mathcal{O}$-lattice** of the standard k-form of (V, B) is $\oplus_i \mathcal{O} e_i$.

Example. Suppose that G is a $\mathbb{Q}$-group as defined in §2. Then there are rational polynomials $f_1, \ldots, f_n$ so that $V(f_1, \ldots, f_n)$ is a subgroup of some $SL(\mathbb{R}^l)$, and G is commensurable to $V(f_1, \ldots, f_n)$.

Picking the standard $\mathbb{Q}$-form $V_{\mathbb{Q}}$ relative to the standard basis of $\mathbb{R}^l$, it follows that the induced $\mathbb{Q}$-form of $\operatorname{End}\mathbb{R}^l$ is just $\operatorname{End}\mathbb{Q}^l$, so each f_i is indeed $\mathbb{Q}$-defined relative to $\operatorname{End}(\mathbb{R}^l)_{\mathbb{Q}}$. Thus G is also a $\mathbb{Q}$-group relative to $V_{\mathbb{Q}}$.

Conversely, every $\mathbb{Q}$-group relative to a standard $\mathbb{Q}$-form of some $\mathbb{R}^l$ is a $\mathbb{Q}$-group. △

As was hinted at before the example, we may also define "arithmetic" in this setting. Indeed, suppose that G is a k-group relative to some k-form V_k. Given any $\mathcal{O}$-lattice $\mathcal{L}$ of V_k, we define

$$G_{\mathcal{L}} = \{g \in G : g\mathcal{L} = \mathcal{L}\}$$

to be the subgroup which preserves the lattice $\mathcal{L}$.

Example. If $G = SL_k(\mathbb{R})$, $V_{\mathbb{Q}} = \mathbb{Q}^k$ is the standard form, and $\mathcal{L} = \mathbb{Z}^k$ is the standard $\mathbb{Z}$-lattice, then $G_{\mathcal{L}} = SL_k(\mathbb{Z})$.

△

Indeed, we get something better than just integer points being (as expected) arithmetic— we also get commensurability.

Theorem 2. *Suppose that G is a k-group relative to a k-form V_k, and $\mathcal{L}_1, \mathcal{L}_2$ are two $\mathcal{O}$-lattices of V_k. Then $G_{\mathcal{L}_1}$ and $G_{\mathcal{L}_2}$ are commensurable arithmetic subgroups of G.*

Proof. Commensurability follows immediately from Lemma 2 below applied to the identity map. To see arithmeticity, apply an $\mathbb{R}$-automorphism of V which takes V_k to the standard k-form, thus taking $G_{\mathcal{L}}$ to G_k. This shows that $G_{\mathcal{L}}$ is arithmetic. □

Here is an advantage of this definition: if G is arithmetic, then we know that it preserves a lattice $\mathcal{L}$ in some k-form V_k. Thus we have the following **congruence subgroups**:

$$G_{\mathcal{L}}(N) = \{g \in G : g \equiv \mathrm{id} \pmod{N\mathcal{L}}\}.$$

All congruence subgroups are finite index, as they are the kernel of a natural homomorphism to the finite group $\operatorname{Aut}(\mathcal{L}/N\mathcal{L})$. Thus even this general class of arithmetic subgroups admit an intrinsic (and large) family of finite-index subgroups. Similarly to the definition of $G_{\mathcal{L}}$, if G is a k-group relative to the standard k-form, and $\mathcal{L}'$ is the standard $\mathcal{O}$-lattice, we define the following subgroup of G

$$G_k = \{g \in G : gV_k \subset V_k\}$$

as the **k-rational points of G**.

Example. If $G = SL_k(\mathbb{R})$, then $G_{\mathbb{Q}} = SL_k(\mathbb{Q})$. More generally, if G is a k-group, with respect to the standard k-form and $\mathcal{O}$-lattice we have that $G_k = G \cap SL_N(k)$, and $G_{\mathcal{O}} = G \cap SL_N(\mathcal{O})$. △

Recall than an **isogeny** from a connected Lie group is a surjective homomorphism with finite kernel. The following proof is modified from [5].

Lemma 2. *Suppose G, G' are $\mathbb{Q}$-groups, G connected, and $\phi : G \to G'$ is an isogeny so that $\phi(G_\mathbb{Q}) \subset G'_\mathbb{Q}$. Then $\phi(G_\mathbb{Z})$ is commensurable to $G'_\mathbb{Z}$.*

Proof. We will find that $\phi(G_\mathbb{Z})$ and $G'_\mathbb{Z}$ have a common finite-index subgroup; namely, the image of a congruence subgroup of $G_\mathbb{Z}$.

Suppose that $G' \leqslant SL_n(\mathbb{R})$. Then ϕ is a representation $G \to SL_n(\mathbb{R})$, and as $\phi(G_\mathbb{Q}) \subset G'_\mathbb{Q}$, it follows that the representation is given by polynomials in the entries of G.

As $\phi(I) = I$, we observe that $\psi(x) = \phi(x-I)$ is still given by polynomials, but these satisfy $\psi(I) = 0$, so they have no constant term. Picking a common denominator m of the polynomials, if $g - I \equiv 0 \pmod m$, then $\psi(g - I)$ therefore has integer coefficients, and so $\phi(g)$ has integer coefficients as well. Thus the image of the congruence subgroup $\phi(G_\mathbb{Z}(m))$ is contained in $G'_\mathbb{Z}$.

Since ϕ has finite kernel, it is a finite-sheeted covering map, and thus $\phi(G_\mathbb{Z}(m))$ is a lattice in G'. But so is $G'_\mathbb{Z}$, so $\phi(G_\mathbb{Z}(m))$ is a finite-index subgroup of G'. □

Corollary 1. *Fix a real vector space V. If V_1 and V_2 are two $\mathbb{Q}$-forms of V and $\mathcal{L}_1, \mathcal{L}_2$ two $\mathbb{Z}$-lattices in V_1 and V_2, respectively, and G is a $\mathbb{Q}$-group relative to both $\mathbb{Q}$-forms, then*

$$G_{\mathcal{L}_1} \text{ is widely commensurable to } G_{\mathcal{L}_2}$$

Proof. By an $\mathbb{R}$-automorphism of V we may take V_1 onto V_2; this induces an automorphism of G which takes $G_{\mathcal{L}_1}$ onto a $\mathbb{Z}$-lattice relative to V_2. By Lemma 2 applied to this automorphism, the image of $G_{\mathcal{L}_1}$ is commensurable to $G_{\mathcal{L}_2}$. □

2.2 Restriction of Scalars

Everything in this section is in [5] in one form or another, but the following treatment is not always the same.

We will motivate this section with an example.

Example. Let $q : \mathbb{Q}[\sqrt{2}]^3 \to \mathbb{Q}[\sqrt{2}]$ be the quadratic form $q(x) = x_0^2 + x_1^2 - \sqrt{2}x_2^2$, and let $P = SO(q, \mathbb{Q}[\sqrt{2}])$. We *cannot* use P as the certifying group H in the definition of arithmeticity, as P is not defined over $\mathbb{Q}$! That is, one of P's defining equations as a variety has a $\sqrt{2}$, so P is defined only over $\mathbb{Q}[\sqrt{2}]$.

Nonetheless, we would like the subgroup $SO(q, \mathbb{Z})$, interpreted somehow as a subgroup of $SO(n, 1)$ to be an arithmetic lattice (if this isn't "arithmetic", what would be?). Moreover, we also need to figure out how to interpret $SO(q, \mathbb{Z})$ as sitting inside $SO(n, 1)$ in a natural way. After all, from the perspective of $\mathbb{Q}$ there is no difference between $\sqrt{2}$ and $-\sqrt{2}$.

Miraculously, the solution to both of these conceptual difficulties (not being defined over $\mathbb{Q}$, and finding a natural embedding) is to be found in one construction: just take both embeddings! Recall

that if k is a number field, then the (infinite) **places** of K are the distinct real embeddings $K \hookrightarrow \mathbb{R}$ and conjugate-pairs of (non-real) complex embeddings $K \hookrightarrow \mathbb{C}$. We will refer to the set of (infinite) places by V_∞. In this case, $\mathbb{Q}[\sqrt{2}]$ has two places, the identity 1 and conjugation ν. Defining a **k-group** in the same way as a $\mathbb{Q}$-group, the places of k induce embeddings of a k-group into real space by embedding the coefficients of the defining equations. In particular, we have two embeddings of P, namely $P_1 = SO(q, \mathbb{R})$ and $P_\nu = SO(q_\nu, \mathbb{R})$, where

$$q_\nu = x_0^2 + x_1^2 - \nu(\sqrt{2})x_2^2 = x_0^2 + x_1^2 + \sqrt{2}x_2^2.$$

Note that these embeddings really are distinct: $P_1 \cong SO(2,1)$, while $P_\nu \cong SO(3)$! One can make sense of $P_1 \times P_\nu$ being defined over $\mathbb{Q}$ in the sense of algebraic geometry, which gives us the $\mathbb{Q}$-points as in the standard $\mathbb{Q}$-form, but it is also possible to make sense of it being defined over $\mathbb{Q}$ in the sense of §3; namely, relative to a vector space $\mathbb{R}/\mathbb{Q}$-form that is not the usual one. This will be desirable because the $\mathbb{Q}$-form we construct will partly encode the arithmetic data of $\mathbb{Q}[\sqrt{2}]$.

Setting $H = P_1 \times P_\nu$, one can check directly that H is defined over $\mathbb{Q}$, and if ϕ is an isomorphism $P_1 \to SO(2,1)$, it follows that $\phi(H_\mathbb{Z} \mod P_\nu)$ is an arithmetic subgroup of $SO(2,1)$.

Letting Δ be the embedding $SO(q, \mathbb{R}) \to SO(q, \mathbb{R}) \times SO(q_\nu, \mathbb{R})$, we may also find a relation between $\Delta(SO(q, \mathbb{R})_{\mathbb{Z}[\sqrt{2}]})$ and $(SO(q, \mathbb{R}) \times SO(q_\nu, \mathbb{R}))_\mathbb{Z}$. Namely, given the basis $B = \{1, \sqrt{2}\}$ of $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$, we have that $\Delta(B) = \{(1,1), (\sqrt{2}, -\sqrt{2})\}$ is a $\mathbb{Q}$-basis for $\Delta(F)$, and an $\mathbb{R}$-basis for $\mathbb{R}^2$. In the language of §3, we have that $\Delta(F)$ is an $\mathbb{R}/\mathbb{Q}$-form of $\mathbb{R}^2$. Then $\Delta(F^3) = \{(v, \sigma(v)) : v \in F^3\}$ is an $\mathbb{R}/\mathbb{Q}$-form of $\mathbb{R}^6$, and $SO(q, \mathbb{R}) \times SO(q_\nu, \mathbb{R})$ is defined over $\mathbb{Q}$ relative to this $\mathbb{Q}$-form.

Moreover, $\Delta(\mathcal{O}^3)$ is a $\mathbb{Z}$-lattice in $\Delta(F^3)$, so by Corollary 1:

$$(SO(q, \mathbb{R}) \times SO(q_\nu, \mathbb{R}))_{\Delta(\mathbb{Z}[\sqrt{2}]^3)} \text{ is widely commensurable to } (SO(q, \mathbb{R}) \times SO(q_\nu, \mathbb{R})_\mathbb{Z};$$

in fact, one may calculate that $SO(q, \mathbb{R}) \times SO(q_\nu, \mathbb{R}))_{\Delta(\mathbb{Z}[\sqrt{2}]^3)} = \Delta SO(q, \mathbb{Z}[\sqrt{2}])$, so we have about as nice a relationship between the diagonal embedding of the integer points and the integer points of the product as we would like. △

We will now discuss a general construction, of which this example is a special case. Let k be a number field, and let G be a k-group. If we were to produce a $\mathbb{Q}$-group which captures G's structure, it would have to be blind in distinguishing the $k/\mathbb{Q}$ Galois conjugates of elements of k. In other words, all of the places $v \in V_\infty$ of k would have to be equally preferred. This leads us to the following construction: define the *Weil restriction*, or the *restriction of scalars* of G to be the $\mathbb{Q}$-group (!) given by

$$\mathrm{Res}_{k/\mathbb{Q}} G = \prod_{v \in V_\infty} G_v$$

Three comments.

1. Since k is a number field, it follows that k is a z-dimensional vector space over $\mathbb{Q}$, so the affine k-line $\mathbb{A}^1_k$ may be interpreted as affine $\mathbb{Q}$-space $\mathbb{A}^z_\mathbb{Q}$. If we are to interpret the k-variety G as living

inside of affine k-space $\mathbb{A}_k^m$, then the Weil restriction of G is what we obtain when we intepret how G sits inside of $\mathbb{A}_{\mathbb{Q}}^{mz}$. This is suggestive of how we cook up $\mathrm{Res}_{k/\mathbb{Q}} G$'s defining equations.

Indeed, as $[k : \mathbb{Q}] = z$, it follows that the regular representation of k on itself as $\mathbb{Q}$-vector space realizes k as a subvariety of $M_z(\mathbb{Q})$. If $G = V(f_1, \ldots, f_l)$, where each $f_i \in k[x_1, \ldots, x_d]$, then under this identification we obtain matrix polynomials $F_1, \ldots, F_l$ on $M_z(\mathbb{Q})$. Then as $G \leqslant M_n(k)$ for some k, we have that $G \hookrightarrow M_n(M_z(\mathbb{Q})) = M_{nz}(\mathbb{Q})$, as the variety cut out by the F_i and the equations cutting k out of $M_z(\mathbb{Q})$.

2. Given a $\mathbb{Q}$-group H, we may think of H as a k-group by looking at H in affine k-space. In a suitable sense, we have that Weil restriction is (the unique up to unique isomorphism) right adjoint to extending scalars in this way. In fact, in sufficiently general settings we have that Weil restriction is right adjoint basically by definition; see e.g. [?].

3. As is suggested by Theorem 3, in various sources we have that being realized as the integer points of a Weil restriction is the *definition* of arithmetic; see e.g. [?].

This construction will serve the role of $P_1 \times P_\nu$ in the above example. The following theorem shows that the example is a special case of a relation which holds in great generality; the key idea of the proof is based off of the one in [5].

Remark. The careful reader may be surprised that we are looking at the $\mathcal{O}$-points of a k-group in the below theorem, as we have only been looking at $\mathbb{Z}$-points so far. The difference between $\mathbb{Z}$-points and $\mathcal{O}$-points is largely superficial: we are looking at finite-dimensional matrix groups, so as $[\mathcal{O} : \mathbb{Z}] = [k : \mathbb{Q}] < \infty$, it follows that $G \cap SL_n(\mathbb{Z})$ is a finite-index subgroup of $G \cap SL_n(\mathcal{O})$. Thus up to commensurability, there is no difference between $\mathcal{O}$-points and $\mathbb{Z}$-points; on the other hand, in practice there can be computational advantages to looking at the (more natural) $\mathcal{O}$-points. $\Diamond$

Theorem 3. *Suppose that G is a $\mathbb{Q}$-group whose integer points $H_{\mathbb{Z}}$ are an irreducible lattice. Then there is a number field F and an F-group H, and an isogeny $\eta : \mathrm{Res}_{F/\mathbb{Q}}(H) \to G$ so that $\eta\Delta(H_{\mathcal{O}})$ is commensurable to $G_{\mathbb{Z}}$.*

Proof. We will work over the complex numbers; indeed, if the theorem is proved over $\mathbb{C}$, then by tracking where the real parts of the complexifications go proves the theorem for $\mathbb{R}$ (since we are always viewing complex-coefficient groups are real Lie groups).

First take $L = G \times_{\mathbb{R}} \mathbb{C}$, the complexification of G. Note that as G is a $\mathbb{Q}$-group, then L is a $\mathbb{Q}[i]$-group, and so $L_{\mathbb{Z}[i]}$ is a lattice in L. Take $\mathcal{G} = \mathrm{Gal}(\mathbb{C}/\mathbb{Q}[i])$. As L is semisimple, it is isogenous to a product of simple groups $P = L_1 \times \cdots \times L_k$ (note that the L_i are in general not defined over $\mathbb{Q}[i]$), via the quotient map

$$\phi : P \to L$$

given by modding out by a finite subgroup of the center. Note that $\phi(P_{\mathbb{Q}[i]}) \subset L_{\mathbb{Q}[i]}$, as any $\mathbb{Q}[i]$-point of the domain is $\mathcal{G}$-invariant, hence so is its image. Thus by Lemma 2, we have that $\phi(P_{\mathbb{Z}[i]})$ is commensurable to $L_{\mathbb{Z}[i]}$.

As P is defined over $\mathbb{Q}[i]$, we have that $\sigma(P) = P$ for any $\sigma \in \mathcal{G}$. Thus $\mathcal{G}$ permutes the factors L_i of P. We claim this action is transitive; indeed, if $\{L_{j_1}, \dots, L_{j_r}\}$ is an orbit under this Galois action, it follows that $L_{j_1} \times \cdots \times L_{j_r}$ is defined over $\mathbb{Q}[i]$. Thus if the Galois action has at least two orbits, it follows that $L_1 \times \cdots \times L_k$ is a product of two groups defined over $\mathbb{Q}[i]$, and by Theorem 1 in each group the $\mathbb{Z}[i]$-points are a lattice. This implies that $L_{\mathbb{Z}[i]}$ is reducible, which contradicts the hypothesis.

Let $\mathrm{Stab}(L_1)$ be the stabilizer under this action, and let F be the fixed field of $\mathrm{Stab}(L_1) \leqslant \mathcal{G}$. Since the Galois action is transitive, it follows that $[\mathcal{G} : \mathrm{Stab}(L_1)] = k$, the number of factors in the product, so $[F : \mathbb{Q}[i]] = k$ by Galois theory. Moreover, $\mathrm{Stab}(L_1) = \mathrm{Gal}(\mathbb{C}/F)$, so as L_1 is held fixed by this Galois group, it follows that L_1 is defined over F.

Let $\sigma_1, \dots, \sigma_k$ be coset representatives of $\mathrm{Gal}(\mathbb{C}/F)$ in $\mathcal{G}$. Then interpreting each σ_i as a function from F into some completion, it follows that the places of F are given by the σ_i. Further assume that $\sigma_i(L_1) = L_i$ and set $H = L_1$ to be an F-group; then $\prod_{v \in V_\infty} H_v = \mathrm{Res}_{k/\mathbb{Q}[i]} H$ is precisely equal to P as a $\mathbb{Q}[i]$-group.

This shows that our original isogeny ϕ is of the form we want; i.e., we can now write $\phi : \mathrm{Res}_{k/\mathbb{Q}[i]} H \to L$. Now note that $\Delta(F)$ is a $\mathbb{Q}[i]$-form of $\mathbb{R}^p$, and so $\Delta(\mathcal{O}^k)$ is a $\mathbb{Z}[i]$-lattice of the $\mathbb{Q}[i]$-form $\Delta(F^k)$. By Corollary 1, it follows that there is an automorphism ψ so that $\psi\Delta(H_{\mathcal{O}}) = \psi \,\mathrm{Res}_{F/\mathbb{Q}[i]}(H)_{\Delta(\mathcal{O}^k)}$ is commensurable with $P_{\mathbb{Z}[i]}$, and thus $\phi\psi(\Delta(\mathcal{O}))$ is commensurable with $L_{\mathbb{Z}[i]}$ by Lemma 2.

But then we may simply take our isogeny to be $\eta := \phi\psi$, thereby finishing the proof. □

Corollary 2. *Suppose that Γ is an arithmetic subgroup of $SO(n,1)$. Then there is a number field k, a simple connected k-group G', and an isogeny $\phi : G' \to SO(n,1)$ so that $\phi(G'_{\mathcal{O}})$ is commensurable to Γ.*

In particular, the simple connected k-group $G = G'/\ker\phi$ is isomorphic to $SO(n,1)$, and its integer points are commensurable with Γ.

Proof. Let Γ be an arithmetic subgroup of $SO(n,1)$, so that there is some $\mathbb{Q}$-group H with maximal compact factor K such that $H_{\mathbb{Z}} \mod K$ is taken by an isomorphism $H \to SO(n,1)$ to a subgroup commensurable with Γ.

Then by Lemma and Theorem 1, $H_{\mathbb{Z}}$ is irreducible, so by Theorem 3 there is a number field F, a simple F-group G, and an isogeny $\eta : \mathrm{Res}_{F/\mathbb{Q}}(G) \to H$ so that $\eta\Delta(G_{\mathcal{O}})$ is commensurable with $H_{\mathbb{Z}}$. Composing this with the isomorphism $H \to PO(n,1)$ produces a continuous surjection $\phi : \mathrm{Res}_{F/\mathbb{Q}}(G) \to PO(n,1)$ with compact kernel; but as each factor of the restriction is simple, it follows that there is some simple factor G' so that $\phi : G' \to PO(n,1)$ is an isogeny which takes $G'_{\mathcal{O}}$ to a subgroup commensurable with Γ. □

By examining the proof of Corollary 2 closely, we have proved:

Theorem 4 (Half of the Classification)**.** *Suppose that Γ is an arithmetic subgroup of $SO(n,1)$. Then there is a number field k and a k-group G isomorphic to $SO(n,1)$, so that all factors but G in $\mathrm{Res}_{k/\mathbb{Q}} G$ are compact, and $G_{\mathcal{O}}$ is commensurable to Γ under this isomorphism.*

To complete the other half of the classification then, we must find the k-groups which are isomorphic to $SO(n,1)$. These are known as $\mathbb{R}/k$**-forms** of $SO(n,1)$, and classifying them will take us somewhat afield of what we have done so far.

Remark. It is not at all obvious from the above proof, but if G is noncompact we may actually assume that G is defined over $\mathbb{Q}$ (see e.g. [5] Cor. 5.3.2 for a general statement)— and moreover when $G = SO(n,1)$ the converse holds too (this is the content of §4). $\Diamond$

3 Classifying the Forms

As suggested by Theorem 4, in order to complete this classification of arithmetic subgroups of $SO(n,1)$ we should determine what possible k-groups can be isomorphic to $SO(n,1)$. Amazingly, the answer ends up being only *two* classes of k-groups: orthogonal groups over fields, and special unitary groups over quaternion algebras.

A word of caution: in this part of the proof we are interested *only* in isomorphism classes, so we will not be directly viewing these algebraic groups as being subsets of some real special linear group; instead, they will be abstract group varieties over a number field, or $\mathbb{R}$ or $\mathbb{C}$.

Importantly, the "fixed-point set" of a Galois action can be seen two equivalent ways,

1. We could mean that H may be *embedded* inside of G as a k-group, even if pointwise it is not a subset. For example, the quaternions are not themselves a subset of $GL_2(\mathbb{C})$, but they can be embedded as such, and the subgroup is isomorphic to the quaternions as a central simple algebra over $\mathbb{R}$.

2. We could mean an abstract group variety obtained by applying a dual Galois action to the defining polynomial equations of the variety.

Both perspectives are useful in different circumstances (e.g., it is transparent from the second that the fixed-point set is defined over the base field), and as they are equivalent in our circumstances we will not worry too much about distinguishing them. In particular, we hope that the reader will forgive us for repeatedly saying "fixed-point *set*."

Also, the following work will be over $\mathbb{C}$; this is because we need the extension to be Galois for the algebraic machinery to work (we could also work over the algebraic closure $\overline{k}$, but $\mathbb{C}$ has the advantage that $\mathbb{R} \subset \mathbb{C}$, and that it is very easy to determine the $\mathbb{C}/\mathbb{R}$-forms of $SO(n+1,\mathbb{C})$). We will obtain the results for $SO(n,1)$ by studying the results for $SO(n+1,\mathbb{C})$, and seeing what possible $\mathbb{C}/k$-forms of $SO(n+1,\mathbb{C})$ are indeed $\mathbb{R}/k$-forms of $SO(n,1)$; thankfully, this is fairly easy to verify, and will be largely omitted.

3.1 The General Strategy

In order to determine the possible k-groups, we will follow a common principle: that subthings of a $\mathbb{C}$-thing are defined over k whenever they are invariant under a suitable $\mathrm{Gal}(\mathbb{C}/k)$ action. What is a suitable $\mathrm{Gal}(\mathbb{C}/k)$ action? It is an action by the Galois group which is compatible with the algebraic structure of the $\mathbb{C}$-thing; i.e., it commutes with its automorphism group. Once we have a suitable Galois action, we will simply take the fixed points of this action; due to the compatibility, it will have the right

kind of algebraic structure, and it will be defined over k because it is $\mathrm{Gal}(\mathbb{C}/k)$-invariant. Our strategy then is as follows:

Determine the compatible Galois actions on $SO(n,1)$ for a given number field k, and then calculate their fixed points.

3.2 Twisting

This section (based off of [7]) will show that finding the compatible Galois actions is a special instance of a very general construction, known as *twisting*. Namely, in order to justifiably call an action a "Galois" action, it should be related to the canonical Galois action on a field (after all, as abstract groups Galois groups can act in many "unnatural" ways). It turns out that following the procedure of pulling back G-bundles along principal G-bundles leads us directly to all of the possible associated actions (for the reader that is surprised by this, see the remark at the end of this section).

The setup is as follows:

- Let G be a group,
- A a G-group; i.e., a group with a left G-action $a \mapsto {}^g a$ so that ${}^g(ab) = {}^g a {}^g b$;
- X a left G-set with a faithful and transitive right A-action so that ${}^g(x \cdot a) = {}^g x \cdot {}^g a$.

Such a triple (G, A, X) will be called a **compatible action on** X.

Example. Let $X = \mathbb{C}^n$ be a complex vector space, $A = GL_n(\mathbb{C})^{op}$ the opposite group of $GL_n(\mathbb{C})$, and $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Then G acts on A via conjugation and X via componentwise Galois action, and A acts on the right via $v \cdot A = Av$. Clearly A with this action is a G-group, and one computes that

$$ {}^g(x \cdot A) = g(Ax) = gAg^{-1}gx = {}^g x \cdot {}^g A $$

so $(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), GL_n(\mathbb{C}), \mathbb{C}^n)$ is a compatible action on $\mathbb{C}^n$. △

Example. Let $N \rtimes H$ be a semidirect product of groups. Then H acts on N via conjugation and on itself by right multiplication. Then (H, N, H) is a compatible triple. △

We will now classify the compatible actions on sufficiently nice X, modulo a mild equivalence. Mimicking the study of G-bundles via *principal* G-bundles, we will assume that the action of A on X is *free*; such an X is called an A**-torsor**. Now suppose X has a compatible G-action; then for any $x \in X$ and $g \in G$, there is a unique $a(x)_g \in A$ so that

$$ {}^g x = x \cdot a(x)_g. \tag{1} $$

One readily computes that for any fixed x_0, we have the relation:

$$ a(x_0)_{gh} = a(x_0)_g {}^g a(x_0)_h \tag{2} $$

and we have that:

$$a(x \cdot b)_g = b^{-1}a(x)^g b. \tag{3}$$

Any function $f : G \to A$ satisfying (2) is called a **cocycle**, and we say two cocycles are **cohomologous** if they differ by a twisted conjugation $g \mapsto b^{-1}(-)^g b$ for some $b \in A$, as in (3).

Thus given the action ${}^g(-)$, we obtain for every $x \in X$ a cocycle. However, as A acts transitively on X, it follows that all of these cocycles are cohomologous, so the action ${}^g(-)$ gives rise to a well-defined **cohomology class** $a : g \mapsto a_g$. One may also check that for any fixed $b \in A$, the translated action $g * (-) = {}^g(- \cdot b)$ gives rise the same cohomology class.

We thus obtain a well-defined map Φ from the compatible actions (modulo translation) on the A-torsor X to the set of cohomology classes, $H^1(G, A)$. In fact, Φ is a bijection; given $a \in H^1(G, A)$, we may fix some $x_0 \in X$, so that any $x \in X$ may be written uniquely as $x_0 \cdot b(x)$, and then set:

$${}^g x = x_0 \cdot a_g {}^g b(x),$$

which is a compatible action. This inverse map is well-defined, as by (3) we have that cohomologous cocycles give rise to translated actions.

Summarizing all of this, we have the following theorem.

Theorem 5. *Suppose X is an A-torsor. Then there is a bijection between compatible actions modulo translation and $H^1(G, A)$.*

We will now be able to generalize Theorem 5 to any A-set as follows, via a pullback trick: namely, any A-set may be "twisted" by the action of an A-torsor.

If S is an *left* A-set, let X be any A-torsor. Given a cocycle $a \in H^1(G, A)$, denote by ${}_aX$ the twisted A-torsor; i.e., X with the action given by a. Observe that the relation $(xb, b^{-1}s) \sim (x, s)$ on ${}_aX \times S$ is compatible with the G-action, and setwise we have that ${}_aX \times S/\sim$ is precisely S. However, we have a different G action on S, so we denote by

$${}_aS = {}_aX \times S/\sim$$

the **twisted set** ${}_aS$. What is the action on ${}_aS$? We may fix some $x \in X$; then under the G-equivariant identification $s \mapsto (x, s)$

$${}_g s \approx {}_g(x, s) = (x \cdot a_g, {}^g s) = (x, a_g \cdot {}^g s) \approx a_g \cdot {}^g s$$

so the action on ${}_aS$ may be said to be S's given G-action **twisted by the cocycle** a.

This construction produces a canonical family of associated actions, parameterized by $H^1(G, A)$.

Remark (Informal Remark for Intuition)**.** The idea of mimicking bundles is classical, see e.g. [7]; however, the fact that this is a sensible strategy is more than a coincidence. This (very informal) remark, based off of [2], is to give an indication as to why that is.

There are various analogues of **nice covering maps** in algebraic geometry (e.g., fppf, fpqc, or étale morphisms), and if one is willing to expand their notion of "topology" so that a "cover by open sets" is given (i.e., replaced by) by the data of a family of nice covering maps, then one may define a G**-bundle**, or a G**-torsor** (where G is a group scheme over k in the category of schemes over k) to be the data of a k-scheme P with a G-equivariant nice covering map $P \to k$ that is locally trivializable in the chosen topology (i.e., there is a cover $\{Y_i \to k\}$ so that the pullback G-bundle $Y_i \times_k P \to Y_i$ is trivial for each i). A **principal** G**-bundle** is a trivial G-bundle.

The theory of topological principal G-bundles tells us (essentially by definition of a bundle) that principal G-bundles over B are classified by the first Čech cohomology group $\check{H}^1(B, G)$ when G is abelian. With some more work, one can show that this is true when G is not abelian as well.

The upshot of considering principal G-bundles in the scheme setting is that a similar result holds: if G is an abelian group k-scheme in a sufficiently nice site over k, it follows that the principal G-bundles over k are classified by a cohomology theory $\widehat{H}^1(k, G)$, which one may check is isomorphic to the group cohomology $H^1(\mathrm{Gal}(k_s/k), G(k_s))$! And just as in the topological case, this is true as well when G is nonabelian: the principal G-bundles over k are classified by $H^1(\mathrm{Gal}(k_s/k), G(k_s))$, now a cohomology *set*. Thus the work we have done in §3.2 is not classifying some artificial notion of "associated G-action;" rather, it is classifying the algebro-geometric analogue of principal bundles. ◊

3.3 Finding the Forms Through Twisting

Now let $\mathcal{G} = \mathrm{Gal}(\mathbb{C}/k)$. In §3.2 we found a canonically defined family of actions associated to the standard Galois action of $\mathcal{G}$ on G and $\mathrm{Aut}_{\mathbb{C}}(G)$, the *twists* of the standard action. As suggested by the remark at the end of §3.2, there is good reason to think that these are the right objects, but don't take our word for it: the following theorem is much more trustworthy.

Theorem 6. *If G is a $\mathbb{C}$-group, then the k-isomorphism classes of the $\mathbb{C}/k$-forms of G are in bijection with the twists ${}_aG$ of the standard Galois action; the bijection is given by taking the fixed point set ${}_aG^{\mathcal{G}}$.*

Proof Sketch. One can check directly (e.g., by looking at the induced action on the ring of functions on G) that the fixed-point set under a compatible action is an algebraic group defined over k; by virtue of it being a bona-fide subset of G, it follows that ${}_aG^{\mathcal{G}} \times_k \mathbb{C} = G$, so ${}_aG^{\mathcal{G}}$ is a $\mathbb{C}/k$-form of G.

If two actions differ by a translation by $\mathrm{Aut}_l\, G$, then their respective fixed-points differ by a k-isomorphism, given by taking the fixed points of the Galois action on $\mathrm{Aut}_l\, G$, so the map is well-defined.

On the other hand, given a $\mathbb{C}/k$-form H of G, there is a $\mathbb{C}$-isomorphism $f : G \to H \times_k \mathbb{C}$. One can check that $f^{-1\sigma} f$ is a cocycle, and its induced action has fixed-point set k-isomorphic to H. □

None of these facts are particularly hard to check in our setting, so we won't go through the grimy details. Those interested in seeing a proof can consult [6]. We have thus obtained:

Corollary 3. *If k is a number field, the k-isomorphism classes of $\mathbb{C}/k$-forms of the real Lie group $SO(n, \mathbb{C})$ are parameterized by the set $H^1(\mathcal{G}, \mathrm{Aut}_{\mathbb{C}}(SO(n, \mathbb{C})))$.*

We must thus embark on a better understanding of this cohomology group, as we will have to compute the fixed points of cocycles.

3.4 Simple Algebras: Basics, Involutions, and the Brauer Group

This and §3.5 are almost entirely from [6], modified to be more "concrete."

In order to understand the fixed point sets of cocycles, we will need to work with a slightly better behaved algebraic object: if ι is an involutive antihomomorphism on an (associative but not necessarily commutative) algebra A, we call ι an **involution**. We will say that (A, ι) is a **simple** algebra with involution if it contains no nontrivial subalgebras stable under ι. If (D, ι) is a division algebra with involution and $V = D^n$ is a free module over D, then given $M = (m_{ij})$ in $GL_n(D)$, we define ${}^*M = (\tau(m_{ji}))$, the "conjugate transpose" over D.

The Artin-Wedderburn theorem informs us that finite-dimensional central simple algebras over k are $n \times n$ matrix algebras over some central division k-algebra D, and $\dim_k A = n^2 \dim_k D$. There is a unique integer d called the **index** of D so that $\dim_k D = d^2$.

Over an algebraically closed field $\overline{k}$, there is only one finite-dimensional central division $\overline{k}$-algebra over $\overline{k}$, namely $\overline{k}$, so we have that the only finite-dimensional central simple algebra is the matrix algebra. This implies that for any f.d. central simple algebra A over k, we have that $A \otimes_k \overline{k} \cong M_n(\overline{k})$, so in particular we may define the **reduced norm** of an element of A as

$$\mathrm{Nrd}_{A/k}(a) := \det(a \otimes 1),$$

and is in fact independent of the field F so that $A \otimes F \cong M_n(F)$.

We may also define (skew) Hermitian forms on V relative to an involution τ in the expected manner. Then if F is the matrix of a (skew) Hermitian form f in a basis of V, we have that the **unitary group** of f over D is:

$$U_n(D, f) = \{X \in GL_n(D) : {}^*XFX = F\}$$

and the **special unitary group** of f over D is the subgroup of elements of reduced norm 1:

$$SU_n(D, f) = \{X \in U_n(D, f) : \mathrm{Nrd}_{M_n(D)/Z(D)} X = 1\}$$

For simplicity let $\mathcal{H}^1 = H^1(\mathcal{G}, \mathrm{Aut}_{\mathbb{C}}(SO_n(\mathbb{C})))$, and let Ψ be the map taking $a \in \mathcal{H}^1$ to the associated form of $SO(n, \mathbb{C})$. If (A, ι) is an algebra with involution over $\mathbb{C}$, we may also define the analogue of $\mathbb{C}/k$-forms for (A, ι), and by mimicking the proof of Theorem 6 we obtain that the $\mathbb{C}/k$-forms of (A, ι) are also parameterized by a cohomology set taking values in $\mathrm{Aut}_{\mathbb{C}}(A, \iota)$. We will find that they are simpler to compute than the $\mathbb{C}/k$-forms of $SO(n, \mathbb{C})$, and this is useful for the following crucial relationship:

The $\mathbb{C}/k$-forms of $SO(n, \mathbb{C})$ are found as special unitary groups of forms of a simple algebra with involution. That is, the following diagram commutes.

$$\begin{array}{ccc} SO(n,\mathbb{C}) & \xleftarrow{\quad SU \quad} & (M(n,\mathbb{C}), {}^t(-)) \\ \uparrow \text{form of} & & \uparrow \text{form of} \\ \{\mathbb{C}/k\text{-forms of } SO(n,\mathbb{C})\} & \xleftarrow{SU} & \{\mathbb{C}/k\text{-forms of } (M(n,\mathbb{C}), {}^t(-))\} \end{array}$$

The reason why this should work in theory is because the automorphisms of $SO(n,\mathbb{C})$ are (mostly) all automorphisms of the matrix algebra which commute with the transpose. This strategy also works for the other classical groups, and might be easier to track in the following easy case of classifying some forms of $SL(n,\mathbb{C})$.

Example. Fix k, and consider a form H of $SL_n(\mathbb{C})$. We know that it is the fixed-point set of a cocycle $a \in H^1(\mathcal{G}, PSL_2(\mathbb{C}) \rtimes \langle t \rangle)$, where t is transpose-inverse. Suppose further that this cocycle does *not* land in $\langle t \rangle$, so really we have $a \in H^1(\mathcal{G}, PSL_2(\mathbb{C}))$. It so happens that $PSL_2(\mathbb{C})$ is the automorphism group of the matrix algebra $M_n(\mathbb{C})$ with trivial involution, which by the theory of simple algebras has $\mathbb{C}/k$-forms of the form $M_m(D)$ where D is a central simple division algebra over k of degree $d = n/m$. With the trivial involution we have that $SU(M_m(D)) = SL_m(D)$, which is a $\mathbb{C}/k$-form of $SL_n(\mathbb{C})$.

By the calculation in the proof of Theorem 7, we have that $SL_m(D)$ is indeed the $\mathbb{C}/k$-form of associated with a; namely, $SL_m(D) = {}_aSL_n(\mathbb{C})^{\mathcal{G}}$. △

We will also need an object which records data about algebras over a given field. If A_1 and A_2 are central simple k-algebras, we know that there are division algebras D_1 and D_2 so that $A_1 \cong M_{n_1}(D_1)$ and $A_2 \cong M_{n_2}(D_2)$. We will say that $A_1 \sim A_2$ if and only if $D_1 \cong D_2$, and denote by $[A]$ the equivalence class of A. Observe that for any A, we have that $A \otimes k \cong A$, so if we define a product $[A][B] = [A \otimes B]$, it follows that the set of classes has an identity element (the tensor product of two central simple algebras is indeed central simple). In fact, under the equivalence $\sim$, there is an inverse element: define for a given A the **opposite algebra** A^{op} with the same underlying abelian group, but with $a \cdot b = ba$. Using the fact that A is central simple if and only if $A \otimes_k A^{op} \cong M_n(k)$, have that $[A][A^{op}] = [k]$, so the set of central simple algebras over k forms a *group*, known as the **Brauer group of** k $\mathrm{Br(k)}$. The following fact can be found in [6].

Lemma 3. *Suppose K is a number field. Then if A is a central simple algebra over K, with index d, then the order of $[A]$ in $\mathrm{Br}(K)$ is equal to d.*

3.5 Classifying the $\mathbb{C}/k$-forms of $SO(n,\mathbb{C})$

We now have the tools under our belt to prove the following theorem.

Theorem 7. *Suppose $n \neq 8$.*

The $\mathbb{C}/k$-forms of $SO(n,\mathbb{C})$ are either special orthogonal groups over k of a quadratic form, or are special unitary groups over a quaternion algebra over k with standard involution, with respect to a skew-hermitian form.

Proof. Following the example in §3.4, we will realize automorphisms of $SO(n,\mathbb{C})$ as automorphisms of a simple algebra with involution. Indeed, let $A = M(n,\mathbb{C})$ and τ the matrix transpose. Then if $n \neq 8$,

the theory of algebraic groups (or even Lie groups) tells us that $\mathrm{Aut}_{\mathbb{C}}(SO_n(\mathbb{C}))$ is given by conjugation by elements of $O(n,\mathbb{C})$. In particular, this tells us that any cocycle $a \in H^1(\mathrm{Gal}(\mathbb{C}/k), \mathrm{Aut}_{\mathbb{C}}(SO(n,\mathbb{C}))$ is also a cocycle in $H^1(\mathrm{Gal}(\mathbb{C}/k), \mathrm{Aut}_{\mathbb{C}}(M(n,\mathbb{C}),\tau))$, and thereby indexes a $\mathbb{C}/k$-form of $(M(n,\mathbb{C}),\tau)$. Explicitly, we have that τ induces an involution ν of ${}_aM(n,\mathbb{C})$ with commutes with $\mathrm{Gal}(\mathbb{C}/k)$, thus ν restricts to an involution θ of ${}_aM(n,\mathbb{C})^{\mathrm{Gal}(\mathbb{C}/k)}$. The Wedderburn-Artin theorem tells us that as a k-algebra this fixed set is $M(m,D)$, where D is a degree d central division algebra over k, and as τ fixes the center of $M_n(\mathbb{C})$, it follows that θ fixes the center of $M(m,D)$.

However, an involution θ which fixes the center of a central simple algebra is precisely the data of an isomorphism to its opposite algebra; thus $M(m,D) \cong M(m,D)^{op}$, and thus has order at most two in the Brauer group Br(k). But $[D] = [M(m,D)]$ in $\mathrm{Br}(k)$, so D has order at most two, and hence the isomorphism to the opposite algebra D^{op} furnishes D with an involution δ which fixes k. By the Skolem-Noether theorem, this implies that in a given basis of D over k, there is a matrix F so that the involution θ on $M(m,D)$ is given by

$$\theta(X) = F^{-1*}XF$$

where $*(-)$ is δ-conjugate-transpose.

The fact that $(M(m,D),\theta)$ is a $\mathbb{C}/k$-form of $(M(n,\mathbb{C}),\tau)$ implies there is an isomorphism $\varphi : M(n,\mathbb{C}) \to M(m,D) \otimes_k \mathbb{C}$ which commutes with the involutions, and moreover by the proof of Theorem 6, the cocycle $a : \mathrm{Gal}(\mathbb{C}/k) \to \mathrm{Aut}_{\mathbb{C}}(SO(n,\mathbb{C}))$ is given by $a_\sigma = \varphi^{-1\sigma}\varphi$. We may now compute that the fixed set of $SO(n,\mathbb{C})$ by a is:

$$\begin{aligned}
{}_aSO(n,\mathbb{C})^{\mathrm{Gal}} &= \{X \in SO(n,\mathbb{C}) : {}_\sigma X = X, \forall \sigma \in \mathrm{Gal}(\mathbb{C}/k)\} \\
&= \{X \in SO(n,\mathbb{C}) : a_\sigma \cdot {}^\sigma X = X, \forall \sigma\} \\
&= \{X \in SO(n,\mathbb{C}) : {}^\sigma(\varphi X)) = \varphi(X), \forall \sigma\}
\end{aligned}$$

but if $\varphi(X) = \sum_i Y_i \otimes z_i$, where $Y_i \in M(m,D)$ and $z_i \in \mathbb{C}$, we have that ${}^\sigma(\varphi(X)) = \sum_i Y_i \otimes {}^\sigma z_i$, so the condition that ${}^\sigma\varphi(X) = \varphi(X)$ for all $\sigma \in \mathrm{Gal}(\mathbb{C}/k)$ implies that the z_i are in k, so in fact $\varphi(X) = \sum_i k_i Y_i \in M(m,D)$.

As the isomorphism φ preserves the reduced norm and satisfies $\varphi\tau = (\theta \otimes_k \mathbb{C})\varphi$, it also follows that if $\varphi(X)$ is Gal-invariant, then $\theta\varphi(X) = \varphi(X)$, and $\mathrm{Nrd}_{M(m,D)/k}\,\varphi(X) = 1$. Since φ restricted to the Galois-fixed set defines a k-morphism, it therefore follows that φ is a k-isomorphism between the fixed set and a unitary group

$$\varphi : {}_aSO(n,\mathbb{C})^{\mathrm{Gal}} \xrightarrow{\cong} SU_m(F,D),$$

as desired.

Now we will pare down the possibilities for F and D to prove the theorem. If n is odd, then as $n = md$, neither m nor d can be even. But as noted above, we know that D has order at most two in the Brauer group, so by Lemma 3, it follows that $d \leqslant 2$. Since d is odd, it follows that $d = 1$, so $\dim_k D = 1$ and thus $D = k$. We also know that δ is trivial in D's center, so δ is trivial on all of D, hence the (skew) Hermitian form defined by F is just a bilinear form, and so we have that $SU_m(F,D) = SO_n(F,k)$.

If n is even, then if $d = 1$ we have the same result. If $d = 2$, then D is a quaternion algebra, and as the fixed set of δ is D's center k, it follows that for all $a \in D$, $a\delta(a)$ is in k, as it is fixed by δ. Thus δ must be the standard involution on D (cf. [8]), which must satisfy $F = -F$, so we have that $SU_m(F, D) = SU_{n/2}(F, D)$, where F defines a skew-hermitian form relative to the standard involution, and D is a quaternion algebra.

This finishes the proof, but we note an aside: by reading off the fixed set, we see that the orthogonal groups correspond precisely to cocycles landing in $PSO(n, \mathbb{C})$, while the unitary groups correspond to those cocycles meeting the (order two) outer automorphism group of $SO(n, \mathbb{C})$. □

Other than compactness criteria, combining Theorem 7 with Corollary 2 and some work tracing when tensoring with $\mathbb{R}$ produces $SO(n, 1)$ "on the way" to $SO(n, \mathbb{C})$ proves Theorem 1. We will omit the thorough proof to §4.2, but the worst of the work has now been done.

Note also that the proof of Theorem 7 allows us to read off precisely what subgroup of $SO(n, \mathbb{C})$ we want our special unitary groups to be: we pick an identification $\varphi : M(n/2, D) \otimes_k \mathbb{C} \to M(n, \mathbb{C})$, and read off the restriction. The most common identification is through the following: writing out quaternion algebra D as $(x, y \mid k)$, we have that $D \otimes_k \mathbb{C}$ embeds in $M_2(\mathbb{C})$ via the identification

$$a + bi + cj + dk \mapsto \begin{pmatrix} a + b\sqrt{x} & y(c + d\sqrt{x}) \\ c - d\sqrt{x} & a - b\sqrt{x} \end{pmatrix}$$

Repeating this for each element produces a k-identification of $M(n/2, D)$ with a subalgebra of $M(n, \mathbb{C})$, which when tensored with $\mathbb{C}$ gives precisely $M(n, \mathbb{C})$; we thus obtain the map φ, and the fixed set under the Galois action in this case is $\varphi^{-1}(SU_{n/2}(F, D))$; i.e., interpreting the $n/2 \times n/2$ matrices of quaternions in the special unitary group as $n \times n$ matrices of complex numbers.

3.6 Restating Theorem 4 and Completing the Classification

At the end of §2.2, we stated half of the classification. Now we may use Theorem 7 to complete it.

Theorem 8. *Suppose Γ is an arithmetic subgroup of $SO(n, 1)$, and $n \neq 7$. Then there is a number field k and an $\mathbb{R}/k$-form G of $SO(n, 1)$ so that all factors but G in $\mathrm{Res}_{k/\mathbb{Q}} G$ are compact, and $G_{\mathbb{O}}$ is commensurable to Γ when we quotient out by these compact factors.*

In particular, we have that G must be $SO(f, k)$ or $SU(g, D)$, where f is a quadratic form defined over k which is definite outside of the identity, and $D = (a, b \mid k)$ is a quaternion division algebra with $a, b \in \mathbb{R}$ so that all but one place of the embedding of the skew-Hermitian form g is definite.

Moreover, any projection of integers in this fashion produces an arithmetic group.

We have thus classified the arithmetic subgroups of $SO(n, 1)$ when $n \neq 8$. This isn't quite Theorem 0, as it is missing the compactness data, but that will follow straightforwardly from Godement's criterion.

Note that there are stringent conditions in Theorem 8 characterizing the types of orthogonal and unitary groups which give rise to arithmetic subgroups of $SO(n, 1)$; we will call these types **admissible**.

Last, a piece of terminology: the arithmetic groups obtained via the orthogonal groups are known as the **lattices of simplest type**, and those obtained via unitary groups are known as **non-simplest type**. Note that the lattices of simplest type are obtained from $\mathbb{R}/k$-forms which are twisted by cocycles landing in $SO(n,\mathbb{C})$'s inner automorphism group, known as , **inner forms**, and non-simplest type are twisted by cocycles which take value in the outer automorphism group, known as **outer forms**. Since "simple" is an overdetermined word in mathematics, we wish to avoid the former terminology, so we will refer to the lattices of simplest type as **inner lattices**, and non-simplest type as **outer lattices**.

4 Proving Theorem 0

All that remains now is to prove the compactness criteria in Theorem 0. Namely, we must prove that:

- when $n > 3$, inner lattices are non-cocompact if and only if they are defined over $\mathbb{Q}$,
- and outer lattices are always compact.

This will boil down to a fact about quadratic forms, but first we should provide some background theory which will make the second item easy.

4.1 Representing Zeroes: A Smidge of Number Theory

Earlier we defined a *place* v to be an equivalence class of embeddings into $\mathbb{R}$ or $\mathbb{C}$. These are better described as **infinite places**; a **finite place** v is an equivalence class of an embedding into the $\mathfrak{p}$-adic completion of k, where $\mathfrak{p}$ is a prime of $\mathcal{O}$. Note that if k_v is such an $\mathfrak{p}$-adic completion of k, then its ring of integers is $\mathcal{O}_v$, the $\mathfrak{p}$-adic completion of the local ring $\mathcal{O}_\mathfrak{p}$.

The following theorem is the archetypal example of a *local-global principal* in number theory, where some fact holds over k if and only if it holds over all k_v.

Theorem (Hasse-Minkowski Theorem)**.** *Let q be a quadratic form over k. Then the equation $q(x) = 0$ has a solution in $\mathcal{O}^n$ if and only if the equation $q_v(x) = 0$ has a solution in $\mathcal{O}_v^n$ for all places v of k.*

When such an equation $q(x) = 0$ has a solution in integers, we will say that it **represents zero**. Note that because q is homogeneous it represents zero if and only if $q(x) = 0$ has a solution in k.

See e.g., [3] for a partial proof, or [8] for a general, short proof using some high-powered machinery.

Lemma. *Let $n \geqslant 5$, k a number field, and v be a finite place of k. Then any quadratic form in n variables over k_v represents zero.*

This may also be found in [3]. Combining these two theorems gives us:

Theorem (Meyer's Theorem)**.** *Suppose $n \geqslant 5$, k a number field, and q a quadratic form over k in n variables. Then q represents zero if and only if q_v represents zero for every real place v, if and only if q_v is indefinite for every real place v.*

Proof. If v is a finite place, we know by the lemma as $n \geqslant 5$ that q_v represents zero. On the other hand, if v is a complex place, then q_v represents zero as well. Thus by the Hasse-Minkowksi theorem, q represents zero if and only if q_v represents zero at the real places of q. This is clearly true if and only if q_v is indefinite at each real place. □

Combining Meyer's theorem with our study of admissible quadratic forms produces the following interesting corollary, which will be of use in the following section.

Corollary 4. *Suppose that q is an admissible quadratic form. Then q represents zero if and only if it is defined over $\mathbb{Q}$.*

Proof. We have defined an admissible quadratic form to be definite at all but one real place of its field k of definition. By Meyer's theorem, q represents zero if and only if all of its real completions are indefinite, so k has only one real place. As k is totally real, it follows that $k = \mathbb{Q}$. □

4.2 Compactness Criteria and Proving Theorem 0

We now depart from number theory, and return to algebraic groups over $\mathbb{R}$. Given a $\mathbb{R}/k$-form G of $SO(n,1)$, we there is an $\mathbb{R}$-isomorphism $G \times_k \mathbb{R} \to SO(n,1)$, so we may consider G to be a subgroup of $SO(n,1)$. In particular $G_{\mathcal{O}}$ is also a subgroup of $SO(n,1)$ and is a lattice, which raises the question: when is $SO(n,1)/G_{\mathcal{O}}$ compact? If this is the case, we will call $G_{\mathcal{O}}$ a **cocompact** lattice.

The goal of this section is to prove the following theorem:

Theorem 9. *Let G be as above, and assume $n \neq 7$. The lattice $G_{\mathcal{O}}$ is non-cocompact if and only if G is an inner form of $SO(n,1)$ defined over $\mathbb{Q}$.*

Since cocompactness of a lattice is invariant under commensurability, combining Theorem 9 with Theorem 8 proves the following corollary.

Corollary 5. *Suppose Γ is an arithmetic lattice of $SO(n,1)$, $n \neq 7$. Then Γ is non-cocompact if and only if Γ is commensurable to an inner lattice of $SO(n,1)$ defined over $\mathbb{Q}$.*

To prove Theorem 9, we will need two compactness criteria.

Theorem 10 (Godement Compactness Criterion)**.** *Let G be a real Lie group defined over a number field k. The homogeneous space $G/G_{\mathcal{O}}$ is compact if and only if $G_{\mathcal{O}}$ has no nontrivial unipotent (all complex eigenvalues $= 1$) elements.*

Theorem 11 (Mahler Compactness Criterion)**.** *Let M be a subset of $SL(n,\mathbb{R})$, and k a number field. The coset space $M/SL(n,\mathcal{O})$ has compact closure in $SL(n,\mathbb{R})/SL_n(\mathcal{O})$ if and only if 0 is not an accumulation point of $M\mathcal{O}^n$.*

Both of these theorems' proofs may be found (essentially) in [5]. The following lemma is the crucial bridge between algebra and geometry; its proof is based off of elements from [5] and [1].

Lemma 4. *Suppose that $G = SO(q,k)$ is an admissible orthogonal group. Then $G_{\mathcal{O}}$ is cocompact if and only if q does not represent zero over k.*

Proof. We set $\Gamma = G_{\mathcal{O}}$, $G = SO(n,1)$, and M a fundamental domain for Γ in G. Note that G/Γ is naturally a closed subspace of $SL(n+1,\mathbb{R})/SL(n+1,\mathcal{O})$, so Theorem 11 tells us that G/Γ is compact if and only if 0 is not an accumulation point of $M\mathcal{O}^n$.

First suppose that G/Γ is not compact. Then $\|g(x)\|$ is not bounded away from zero on $M \times \mathcal{O}_k^n - 0$, so there are sequences $(g_i)_i \subset M$ and $(v_i)_i \subset \mathcal{O}_k^n - 0$ so that $g_i(v_i) \to 0$ as $i \to \infty$. Since $g_i \in G = SO(q,\mathbb{R})$, we have that $qg_i = q$ for all i, so $q(v_i) = q(g_i(v_i)) \to 0$. But $q(\mathcal{O}^n)$ is a discrete subset of $\mathbb{R}$, so for some large n we have that $q(v_n) = 0$.

Now suppose that q represents zero. Then by the Witt theory of split quadratic forms, it follows that q is equivalent to a form $q = x_0x_1 + p$ over k, so as k-groups we have that $SO(q,k) \cong SO(xy+p,k)$—this lifts to an isomorphism of $\mathbb{R}$-groups as well. Taking the subgroup H of elements which are constant on the lower diagonal representing p, it follows that H is isomorphic as a k-group to $SO(xy+z^2,k)$, which is $SL(2,k)/kI$. Thus gives us a continuous homomorphism $\rho : SL(2,\mathbb{R}) \to G$ which takes $SL(2,k)$ into G_k; in particular $\rho(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix})$ is a nontrivial unipotent element of $G_{\mathcal{O}}$. Thus G/Γ is noncompact by Theorem 10. □

All that remains for the proof of Theorem 9 is to address the case that the $\mathbb{R}/k$-form is outer. This argument is from [4].

Lemma 5. *Suppose that $G = SU(q,D)$, where q is skew-Hermitian relative to the standard involution on the admissible quaternion algebra D. Then $G_{\mathcal{O}}$ is cocompact in $SO(n,1)$.*

Proof. Here by $G_{\mathcal{O}}$ we mean the image of G's integer points under the embedding $D \hookrightarrow M_2(\mathbb{R})$ as described at the end of §3.5.

Suppose for the sake of contradiction that $G_{\mathcal{O}}$ is non-cocompact. We have that $G_{\mathcal{O}}$ is realized as an admissible orthogonal group $SU(q,D) \times_k \mathbb{R} \cong SO(f,\mathbb{R})$, q defined over k, so by Lemma 4 it follows that f represents zero over k. Reading off the identification, this implies that the skew-Hermitian form q represents zero in D, which then implies that there is a two-dimensional subspace W of k^n on which f vanishes.

However, by construction we have that f is signature $(n,1)$, and by the theory of quadratic forms we know that the maximal dimension of a subspace on which f vanishes is $\min\{n,1\} = 1$. This contradicts the existence of W, so $G_{\mathcal{O}}$ is indeed compact. □

We may now prove Theorem 9.

Proof of Theorem 9. By Lemma 5 we know that no outer lattice is non-cocompact. Thus by Lemma 4 $G_{\mathcal{O}}$ is non-cocompact if and only if it is an inner lattice with admissible quadratic form representing zero over k, which occurs if and only if $k = \mathbb{Q}$ by Corollary 4. □

This finishes the proof of Theorem 0: by Theorem 8 we have a complete classification of the commensurability types of arithmetic lattices in $SO(n,1)$, and by Corollary 5 we know exactly when they are cocompact.

References

[1] A. Borel. *Introduction to arithmetic groups*, volume 73 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2019. Translated from the 1969 French original [MR0244260] by Lam Laurent Pham, Edited and with a preface by Dave Witte Morris.

[2] C. Halleck-Dube. Some Remarks on Galois Cohomology and Linear Algebraic Groups.

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

[4] J.-S. Li and J. J. Millson. On the first Betti number of a hyperbolic manifold with an arithmetic fundamental group. *Duke Mathematical Journal*, 71(2), Aug. 1993.

[5] D. W. Morris. *Introduction to Arithmetic Groups*. 2015.

[6] V. Platonov, A. Rapinchuk, and I. Rapinchuk. *Algebraic Groups*, page 53–123. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2023.

[7] J.-P. Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[8] J. Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, [2021] 2021.

[9] A. Weil. Algebras with Involutions and the Classical Groups. *The Journal of the Indian Mathematical Society*, 24:589–623, 1960.