Special Points on Orthogonal Symmetric Spaces

Andrew Fiori

Master of Science

Department of Mathematics and Statistics

McGill University

Montreal, Quebec

June 5, 2013

A thesis submitted to McGill University
in partial fulfilment of the requirements for an M.Sc. degree

Acknowledgements

There are a great number of people whose help, support and guidance over the past few years have made it possible for me to complete this thesis. Firstly, I would like to thank my supervisor, Eyal Goren, for both his mathematical guidance and his willingness to endure the long process of making this thesis what it is now.

I would like next to thank my various professors, my fellow students and other colleagues. The great many things I have learned from all of you, as well as the environment for mathematical study you create, have been a great asset.

I would also like to thank my friends and family: without the distractions you are able to provide I do not think I could have maintained sufficient sanity to complete this project.

Finally, I would like to thank the Mathematics and Statistics Department as well as the National Engineering and Science Council for their financial support during this time.

Abstract

The theory of complex multiplication has been a powerful tool for studying various aspects of classical modular forms along with their generalizations. With the recent work of Borcherds there has been an increase in the interest in studying modular forms on orthogonal groups of signature $(2, n)$ as well as the spaces on which they live. In this thesis, we study the special points (or CM-points) that exist on these spaces. We develop cohomological classifications relating the special points, their associated CM-fields and the spaces in which these points can be found.

Resumé

La théorie de la multiplication complexe nous donne des outils puissants pour étudier des aspects divers des formes modulaires classiques, ainsi que leurs généralisations. Les travaux récents de Borcherds donne une nouvelle motivation pour étudier les formes modulaires sur des groupes orthogonaux de signature $(2, n)$, ainsi que les espaces sur lesquels ils agissent. Dans cette thèse, nous étudierons les points spéciaux (ou points-CM) qui existent dans ces espaces. Nous développerons des classifications cohomologiques concernant les points spéciaux, les corps-CM associés et les espaces dans lesquels ces points peuvent être trouvées.

TABLE OF CONTENTS

CHAPTER 1
Motivation

The primary goal of this thesis is to attempt to understand the maximal $\mathbb{Q}$-defined algebraic tori with compact sets of real points that are contained in a given orthogonal group. The reason why this problem is of interest comes out of a particular generalization of the concept of modular forms, in particular a generalization of the domain for a space of modular forms.

A very general description of a modular form is a function f, defined on a hermitian symmetric domain $\mathbb{H}$, with values in $\mathbb{C}$. The space $\mathbb{H}$ comes equipped with the action of a group Γ, where the function f will be required to satisfy some sort of functional equation with respect to the action of Γ. Generally, f is not invariant under the action of Γ but instead changes by some constant power k (called the weight) of some factor of automorphy $j : \Gamma \times \mathbb{H} \to \mathbb{C}$. One typically takes $j \in H^1(\Gamma, \mathcal{O}(\mathbb{H})^\times)$ (so $f(\gamma \cdot h) = j(\gamma, h)^k f(h)$). One usually also has holomorphicity requirements defined by using the structure of $\mathbb{H}$ as a complex manifold.

In the classical case one has:

$$\mathbb{H} := \{z \in \mathbb{C} | \Im(z) > 0\} \simeq \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2)(\mathbb{R}) \simeq \ SO(2,1)(\mathbb{R})/\mathrm{SO}(2)(\mathbb{R}),$$

and Γ will be an arithmetic subgroup (more specifically a congruence subgroup) of SL_2, with the standard factor of automorphy $j\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z\right) := c \cdot z + d$.

In this setting there is a notion of points with complex multiplication (CM). These are points where we expect to be able to use arithmetic information about elliptic curves to study the values of modular forms; the CM-points are precisely the points τ such that $\mathbb{Q}(\tau)$ is a quadratic imaginary field, while under the $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2)(\mathbb{R})$ interpretation, the CM-points are those points whose stabilizer in $\mathrm{SL}_2(\mathbb{C})$ is a maximal algebraic torus, defined over $\mathbb{Q}$, having a compact set of $\mathbb{R}$ points.

When one generalizes the above construction to take $\mathbb{H} := G(\mathbb{R})/K(\mathbb{R})$, with G a reductive group over $\mathbb{Q}$, and K a maximal compact subgroup, one arrives at the generalized notion of CM-points as being those points in $G(\mathbb{R})$, whose stabilizer contains a maximal torus defined over $\mathbb{Q}$ having a compact set of real points. In the specific setting of taking G to be an orthogonal group of signature $(2, n)$, the problem we are interested in is precisely the classification and understanding of these CM-points.

To begin with we look at the problem more generally, developing a system for classifying certain conjugacy classes of k-defined subgroups contained in an algebraic group. We then apply this to the specific case we are interested in, that is classifying the tori in an orthogonal group. We next attempt to develop criterion for when a particular $\mathbb{Q}$-isomorphism class of a torus is embeddable into a given orthogonal group.

CHAPTER 2
Background Material

2.1 Introduction to Algebraic Groups

Most of the material in this section is covered in: A. Borel "Linear Algebraic Groups" [Bor91], T.A. Springer "Algebraic Groups" [Spr98] and Platonov and Rapinchuk "Algebraic Groups and Number Theory"[PR94]; though many other good references exist.

For the remainder of this section, let k be a perfect field and $\overline{k}$ be an algebraic closure (most of what follows would be true for non-perfect fields if one restricts to separable extensions).

Definition 2.1.1. An **algebraic group** G (over $\overline{k}$) is an algebraic variety over $\overline{k}$ together with a group structure where the group operations are morphisms of varieties. If G is a variety over k and the group operations are k-morphisms then G may be called a **k-group**, or said to be **defined over** k.

A homomorphism of algebraic groups is both a morphism of varieties and a group homomorphism. If the homomorphism is between two k-groups and is defined over k we may call it a k-homomorphism.

Definition 2.1.2. A **linear algebraic group** (over k) is an algebraic group over k that is affine as a variety over k.

Remark. Through the usual correspondence between affine varieties and rings, which associates to a variety its ring of regular functions, the extra morphisms that give a variety a group structure under this correspondence give the associated ring the structure of what is called a Hopf algebra. In general a Hopf algebra A over a ring R is an R algebra (with R algebra structure map $i : R \to A$, multiplication $m : A \otimes_R A \to A$) equipped additionally with a co-multiplication $\mu^* : A \to A \otimes_R A$, a co-unit $e^* : A \to R$ and an antipode $i^* : A \to A$ which satisfy the following commutative diagrams:

$$\begin{array}{ccc} A & \xrightarrow{\mu^*} & A \otimes_R A \\ \downarrow{\scriptstyle \mu^*} & & \downarrow{\scriptstyle id\otimes\mu^*} \\ A \otimes_R A & \xrightarrow{\mu^*\otimes id} & A \otimes_R A \otimes_R A \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\mu^*} & A \otimes_R A \\ \downarrow{\scriptstyle \mu^*} & \searrow^{id} & \downarrow{\scriptstyle id\otimes e^*} \\ A \otimes_R A & \xrightarrow{e^*\otimes id} & A \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\mu^*} & A \otimes_R A \\ \downarrow{\scriptstyle \mu^*} & \searrow^{i\circ e^*} & \downarrow{\scriptstyle m\circ(id\otimes i^*)} \\ A \otimes_R A & \xrightarrow{m\circ(i^*\otimes id)} & A \end{array}$$

One can check that such conditions on R-algebra maps would be equivalent to the associated variety having a group structure.

In the remainder of this thesis we shall generally restrict our attention to the case of linear algebraic groups, and as such the word "linear" shall often be omitted. That said, a number of the results do hold more generally.

Theorem 2.1.3. *[Bor91, 1.10] Every linear algebraic group G over $\overline{k}$ is isomorphic to a closed subgroup of $\mathrm{GL}_n(\overline{k})$ for some n. If moreover G is a k-group, then it is k-isomorphic to a closed subgroup, defined over k, of $\mathrm{GL}_n(\overline{k})$.*

Sketch of proof. The first step is to prove a series of lemmas concerning G actions on k-varieties. In particular one defines the actions of left/right translation of G on $\overline{k}[V]$ for any k-variety V on which G acts. That is $\lambda_g : \overline{k}[V] \to \overline{k}[V]$ via $\lambda_g(f)(v) = f(g^{-1} \circ v)$. One then proves that we can write $k[G] = k[f_1, \ldots, f_n]$ where $E := \overline{k}[f_1, \ldots, f_n]$ is stable under right translation. left translation

then gives us a representation of G into $\mathrm{GL}(E)$ which is defined over k. Finally, it is shown that this gives us a closed immersion, thus defining G as being a closed subvariety of $\mathrm{GL}_n(\overline{k})$. □

With the above theorem we will in general be viewing linear algebraic groups as being closed subgroups of some GL_n, most often $\mathrm{GL}_n(\mathbb{C})$.

As is often the case when talking about varieties, the notion of fields of definition come into play. As such the following characterization will be useful.

Theorem 2.1.4. *[Bor91, AG.14] Let $G \subseteq \mathrm{GL}_n(\overline{k})$ be an algebraic group, then the following are equivalent:*

1. *G can be defined over k as an algebraic group. ie:*
   The ideal defining G as a subvariety of $G \subseteq \mathrm{GL}_n(\overline{k})$ is generated by polynomials over k and the morphisms defining the group structure of G correspond to polynomials in k on the coordinate ring of G.
2. *G can be defined over k as a variety. ie:*
   The ideal $\mathfrak{a}$ defining G as a subvariety of $G \subseteq \mathrm{GL}_n(\overline{k})$ is generated by polynomials over k.
3. *$G(\overline{k})$ is invariant (as a subset of $\mathrm{GL}_n(\overline{k})$) under the action of $\mathrm{Gal}(\overline{k}/k)$.*

Sketch of proof. $1 \Rightarrow 2$ is obvious from the definition.
$2 \Rightarrow 1$ follows from observing that the group law on GL_n is defined by polynomials with integer coefficients and so are immediately k defined for any G.
$2 \Rightarrow 3$ is clear by applying the Galois action to the equation being satisfied.
$3 \Rightarrow 2$ we need only to check the criterion on the variety being a k-variety. The Galois criterion for varieties is proven by proving a similar statement about vector spaces then viewing the coordinate ring as a k-vector space.

Lemma 2.1.5. *Let V be a vector space over k and W be a subspace of $V_{\overline{k}} = V \otimes_k \overline{k}$ then W can be defined over k if and only if W is defined over $\overline{k}$ and $W(\overline{k})$ is Galois stable.*

Proof of lemma. The "only if" assertion is clear.
For the "if" assertion notice that $W_k := W^{\mathrm{Gal}(\overline{k}/k)}$ is defined over k so we only need to show that $W' := \mathrm{span}_{\overline{k}}(W_k) = W$. By considering W/W' we can reduce to the case $W_k = 0$ in which case we wish to prove $W = 0$. We remark that to show that the invariants of W/W' would be 0 one uses the additive version of Hilbert's Theorem 90.

Indeed, choose a k basis e_i for V. Choose an element $0 \neq w \in W$ such that the number of e_i involved in expressing w is minimal. By reindexing and rescaling we can arrange so that $w = e_1 + a_2 e_2 + \cdots + a_j e_j$. Since w is not in W_k, there exists $\sigma \in \mathrm{Gal}(\overline{k}/k)$ with $\sigma(w) \neq w$, but then $0 \neq w - \sigma(w) \in W$ is expressed in $j-1$ terms which is a contradiction. □

Returning to the theorem, we denote by $\mathfrak{m}_x$ the ideal of functions vanishing at x and consider $J = \bigcap_{x \in G} \mathfrak{m}_x$ the ideal of functions vanishing on G. Then J is defined as a subspace of $\overline{k}[\mathrm{GL}_n]$ over $\overline{k}$. For $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we have:

$$^{\sigma}J_{\overline{k}} = \bigcap_{x \in G(\overline{k})} {}^{\sigma}\mathfrak{m}_{x,\overline{k}} = \bigcap_{x \in G(\overline{k})} \mathfrak{m}_{\sigma(x),\overline{k}} = \bigcap_{x \in G(\overline{k})} \mathfrak{m}_{x,\overline{k}} = J_{\overline{k}}.$$

The last equality following from the stability of $G(\overline{k})$. Thus, by the Galois criterion for stability of vector spaces, J is defined over k, from which it follows that G is. □

We next note that as a consequence of the above we can show that for algebraic groups $H \subseteq G$ defined over k, the following objects will also be defined over k: the normalizer $N_G(H)$ of H in G,

the centralizer $C_G(H)$ of H in G, the commutator subgroup (G,G) and the connected component of the identity G^o.

Since an algebraic group is a homogeneous space (because: $\forall x, y \in G$, translation by yx^{-1} is an automorphism taking x to y) we conclude that algebraic groups are smooth varieties, and consequently their irreducible components are their connected components.

2.1.1 Characters, Co-Characters and Diagonalizable Groups

Definition 2.1.6. For an algebraic group G we define $X^*(G)$ and $X_*(G)$ to be the character group and co-character respectively. That is:

$$X^*(G) := \mathrm{Hom}(G, \overline{k}^*) \text{ and } X_*(G) := \mathrm{Hom}(\overline{k}^*, G).$$

There are two distinguished types of connected algebraic groups, tori and Borel subgroups. These are defined as follows:

Definition 2.1.7. An algebraic group G is said to be **diagonalizable** if $X^*(G)$ spans $\overline{k}[G]$ as a $\overline{k}$-vector space. A diagonalizable group D is called **split** over k if $X^*(D)_k := X^*(D) \cap k[D]$ spans $\overline{k}[D]$ or equivalently $X^*(D)_k$ spans $k[D]$. Conversely D is said to be **anisotropic** (over k) if $X^*(D)_k = 0$. A connected diagonalizable group is called an **algebraic torus**. These are precisely those groups that are isomorphic over $\overline{k}$ to $\mathbb{G}_m^n := \mathrm{GL}_1(\overline{k})^n$ for some n.

Remark. One should note that the conditions for an algebraic group to be diagonalizable are equivalent to saying that for any faithful representation into GL_n the group will in fact be diagonalizable in the sense that some conjugate over $\mathrm{GL}_n(\overline{k})$ will consist only of diagonal matrices. To see this fix a basis $\chi_1, \ldots, \chi_n$ for $X^*(D)$ as a $\mathbb{Z}$-module and consider the natural representation of D on $\mathrm{span}_{\overline{k}}(\chi_1, \ldots, \chi_n)$. This representation will map into the diagonal matrices. One can moreover check that diagonalizability in this sense is independent of the choice of representation.

It should be noted that every diagonalizable group is split over some finite algebraic extension of the base field (to see this just consider the element of $\mathrm{GL}_n(\overline{k})$ that diagonalize G, adjoining the entries of the matrix to k gives a splitting field). We call such a field a splitting field of the group.

We notice that for an algebraic group G defined over k we will have a natural action of $\mathrm{Gal}(\overline{k}/k)$ on $X^*(G)$. In particular for $\sigma \in \mathrm{Gal}(\overline{k}/k)$ and $\chi \in X^*(G)$ we have:

$$(\sigma \circ \chi)(g) := \sigma(\chi(\sigma^{-1}(g))).$$

Using this structure we can obtain the following:

Theorem 2.1.8. *[Bor91] Let K/k be a finite Galois extension with Galois group $\Gamma := \mathrm{Gal}(K/k)$. The functor from the category of diagonalizable groups defined over k split in K to the category of $\mathbb{Z}[\Gamma]$-Modules taking $D \mapsto X^*(D)$ is a contravariant equivalence of categories. Moreover, the full subcategory of tori corresponds to the subcategory of $\mathbb{Z}$-torsion free $\mathbb{Z}[\Gamma]$-Modules.*

Sketch of proof. The proof of the first statement amounts to understanding the Hopf algebra structure on the coordinate ring in relation to the fact that the character group spans the coordinate ring. The proof of the statements about the subcategory of tori amounts to checking that connected implies torsion free character module, which follows from fact that $\mathbb{G}_m$ has no non-trivial connected subgroups. □

Definition 2.1.9. Let T be an algebraic torus. Define T_a and T_d to be the maximal anisotropic and respectively split subtori of T. These can be shown to exist by construction or via the equivalence

of categories stated above. One can construct T_a, T_d as:

$$T_a := \bigcap_{\chi \in X^*(T)_k} \mathrm{Ker}(\chi) \qquad T_d := \langle \mathrm{im}(\chi) | \chi \in X_*(T)_k \rangle.$$

In order to see that these are tori one only needs to check that they are connected. For T_d this is obvious as it is the union of the continuous image of connected sets containing a common point. The character module for T_d is $X_k^*(T)$. To show that T_a is connected one uses that its character module $X^*(T_a) \simeq X^*(T)/X^*(T)_k$ is $\mathbb{Z}$-torsion free. Note that since $(T_a \cap T_d)^\circ$ is trivial. $T_a \cap T_d$ is finite. We should also note that T_a, T_d are functorial in their constructions.

Definition 2.1.10. A **Borel subgroup** of an algebraic group G is a subgroup which is maximal for the property of being connected and solvable.

We now mention an important property of Borel subgroups which is the basis for proving a number of results about them.

Theorem 2.1.11. *[Bor91, IV.11.2] Let G be a connected algebraic group and P a closed subgroup. Then G/P is projective (or complete) if and only if P contains a Borel subgroup.*

As a consequence of the above theorem we make the following definition:

Definition 2.1.12. A subgroup P of an algebraic group G is called **parabolic** if G/P is projective.

Theorem 2.1.13. *[Spr98, CH2 3.2.2] Let G be an algebraic group over k, then there exists a maximal torus T in G that is defined over k.*

In contrast to the above result, there need not exist Borel subgroups which are defined over k. When there is, the group G is said to be quasi-split over k.

Theorem 2.1.14 (Conjugacy of Maximal Tori)**.** *[Bor91, IV.11.3] Let G be a (linear) algebraic group over k. Then all maximal tori in G are conjugate over $G(\overline{k})$, that is to say, there is for any two tori an element of $G(\overline{k})$ which conjugates one to the other.*

Sketch of Proof. The important points of the proof are as follows:

1. All Borel subgroups are conjugate over G. [Bor91, IV.11.1]
2. Any two maximal tori in a solvable group are conjugate. [Bor91, III.10.6]
3. Every maximal torus is contained in a Borel subgroup (tori are connected and solvable, hence contained in maximal such objects).
4. Hence, any two maximal tori are conjugate.

□

One can say slightly more in the case of maximal k-split torus.

Theorem 2.1.15. *[Bor91, V.15.14] Let G be connected and k perfect. Then the maximal k-split tori of G are conjugate over $G(k)$.*

Examples. Examples of Algebraic Groups:

1. The first example is $G = \mathrm{GL}_n(\overline{k})$, in this case we have $\overline{k}[G] = \overline{k}[x_{ij}, \det(x_{ij})^{-1}]$ A maximal torus here is $D_n(\overline{k})$ the diagonal matrices. An example of a Borel subgroup is the upper triangular matrices. In general the Borel subgroups consist of those matrices which stabilize a maximal flag, that is which stabilize a sequence of subspaces $V_1 \subset V_2 \subset \cdots \subset V_n$ where $\dim(V_i) = i$. We define $\mathbb{G}_m := \mathrm{GL}_1(\overline{k})$.
2. The next is $G = \mathrm{SL}_n(\overline{k})$, where we have $\overline{k}[G] = \overline{k}[x_{ij}]/(\det(x_{ij}) - 1)$. A maximal torus here is $T \subset D_n(\overline{k})$ given by requiring the bottom right to be such that the determinant is 1. An example of a Borel subgroup consists of upper triangular matrices of determinant 1.
3. We also have the subgroup $\mathbb{G}_a \subset \mathrm{SL}_2(\overline{k})$ given by $\mathbb{G}_a := \left\{ \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) | x \in \overline{k} \right\}$. We have $\overline{k}[\mathbb{G}_a] = \overline{k}[x]$ A maximal torus here is trivial. The entire group is itself a Borel subgroup.

4. The next example is a general construction. Let $S \in \mathrm{GL}_n(\overline{k})$ then the matrices:

$$G := \{M \in \mathrm{GL}_n(\overline{k}) | {}^tMSM = S\}$$

form an algebraic group, the structure of which depends highly on the choice of S. If S has entries in k, then G is defined over k. It should be noted that the group G', defined in terms of ${}^tNSN$ where $N \in \mathrm{GL}_n(k)$, is related to G via $G' = N^{-1}GN$ and thus the resulting groups are k-isomorphic. As such, various similarity theorems can be used to convert our group to a 'nicer' form.

(a) If S is symmetric ($S = {}^tS$) with non-zero determinant then we get an orthogonal group ($char(k) \neq 2$). Specifically, if $S_m = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ we get the usual orthogonal group. A maximal torus is of the form:

$$\begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_m \end{pmatrix}$$

where the A_i are two by two blocks of the form:

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a^2 + b^2 = 1 \right\} = \left\{ \frac{1}{2} \begin{pmatrix} x + \frac{1}{x} & i(x - \frac{1}{x}) \\ -i(x - \frac{1}{x}) & x + \frac{1}{x} \end{pmatrix} | \ x \in \overline{k} \right\}$$

(where i is some square root of -1 in $\overline{k}$) along the diagonal. We remark that the character module for each of the A_i is generated by the map x. If n is odd then an additional 1 would appear in the lower right entry.

(b) If S is skew-symmetric ($S = -{}^tS$) with non-zero determinant then we get a symplectic group. If $S_m = \left(\begin{smallmatrix} 0 & 1_m \\ -1_m & 0 \end{smallmatrix} \right)$ we get the group Sp_{2m}. A maximal torus here consists of the matrices:

$$\begin{pmatrix} t_1 & & & & \\ & \ddots & & & \\ & & t_m & & \\ & & & t_1^{-1} & \\ & & & & \ddots \\ & & & & & t_m^{-1} \end{pmatrix}.$$

In both of the last two cases a Borel subgroup consists of the subgroup of matrices which stabilize a maximal flag of the form:

$$V_1 \subset V_2 \subset \cdots \subset V_m \subseteq V_m^{\perp} \subset \cdots \subset V_1^{\perp}$$

where each V_i has dimension i and the V_i are isotropic for the form on $\overline{k}^n$. For the case of Sp_{2m} an example is the subgroup of upper triangular matrices it contains.

2.1.2 Restriction of Scalars

The next section gives another method of constructing an algebraic group. It is a method of constructing one algebraic group from another via manipulation of the fields of definition. In particular the construction goes as follows: Let L/k be a finite field extension of degree d. Fixing a basis for L/k we may view L as a d-dimensional vector space over k. Then the action of L on L via multiplication on the left gives us a map $L \hookrightarrow \mathrm{GL}_d(k)$. Now, let G be an algebraic group defined over L. The set of equations defining both its variety and group structure have coefficients in L, We can translate these into matrix equations via the map $L \hookrightarrow \mathrm{GL}_d(k)$, expanding out the matrix equations will yield a set of equations over k. We then define $R_{L/k}(G)$ to be the algebraic group whose structure is given by these equations. Concretely, if $G \hookrightarrow \mathrm{GL}_n(L)$ then

$R_{L/k}(G) \hookrightarrow \mathrm{GL}_{nd}(k)$. We note that this construction is independent of the initial choice of basis for L up to k-isomorphism. The restriction of scalars construction enjoys a number of very nice properties.

1. If L/k is separable and N is the normal closure of L, then there exists an N-isomorphism $R_{L/k}(G) \simeq \prod_{\sigma} G^{\sigma}$ where σ ranges over the k-embeddings of L into N and G^{σ} is the same as G but with defining equations corresponding to the embedding of L into N by σ. In particular for any k-algebra A we have $R_{L/k}(G)(A) = G(L \otimes_k A)$.
2. The restriction of scalars operation can also be applied to morphisms of algebraic groups, thus becoming functorial. This functor is however not full. We can however conclude that, $X^*(R_{L/k}(G))_k = X^*(G)_L$, a statement which is particularly useful when applied to tori.

One special case of the restriction of scalars construction is in applying it to a non-algebraic group defined over one field to get an algebraic group defined over the base field.

Example. Let L/k be a finite Galois extension. Then the set $\{x \in L | N_{L/k}(x) = 1\}$ is not algebraic in L, however viewing L as a k vector space, the corresponding set is algebraic over k, and so the equations defining it give us a closed subvariety of $R_{L/k}(\mathbb{G}_m)$. Following the notation in Platinov & Rapinchuk we define:

$$R^{(1)}_{L/k}(\mathbb{G}_m) := \{x \in R_{L/k}(\mathbb{G}_m) |\ N_{L/k}(x) = 1\}$$

where $N_{L/k}$ is the $\overline{k}$-linear extension of the map defining $N_{L/k}$ on L as a k-vector space.

More specifically, we note that under the regular representation for L the norm map $N_{L/k}$ becomes the determinant map and so $R^{(1)}_{L/k} = \{x \in R_{L/k}(\mathbb{G}_m) |\ \det(x) = 1\}$. In particular one sees that this is indeed an algebraic condition.

Specifically, consider the case $L = k(\sqrt{D})$. If we fix the basis for L/k of $1, \sqrt{D}$ then the regular representation of L maps the element $a + b\sqrt{D} \mapsto \left(\begin{smallmatrix} a & bD \\ b & a \end{smallmatrix}\right)$. Consequently we have that $R_{L/k}(\mathbb{G}_m) = \{\left(\begin{smallmatrix} a & bD \\ b & a \end{smallmatrix}\right) | a^2 - b^2 D \neq 0\}$. Over L this diagonalizes to the form $\{\left(\begin{smallmatrix} a+b\sqrt{D} & 0 \\ 0 & a-b\sqrt{D} \end{smallmatrix}\right)\}$ with the characters thus corresponding to the two embeddings of L over k and the non-trivial Galois element acting on $X^*(R_{L/k}(\mathbb{G}_m))$ by interchanging them. The torus $R^{(1)}_{L/k}(\mathbb{G}_m)$ is then precisely $\{\left(\begin{smallmatrix} a & bD \\ b & a \end{smallmatrix}\right) | a^2 - Db^2 = 1\}$. The character module is generated by the character $\left(\begin{smallmatrix} a & bD \\ b & a \end{smallmatrix}\right) \mapsto a + b\sqrt{D}$ and the non-trivial Galois element maps this to the inverse $a - b\sqrt{D}$. We remark finally that a different choice of k basis for L would correspond to conjugation in $\mathrm{GL}_2(k)$.

2.2 The Lie Algebra of an Algebraic Group

There are many good references for the formal definitions of Lie algebras, for example see A. Borel "Linear Algebraic Groups" [Bor91], T.A. Springer "Linear Algebraic Groups"[Spr98] or Fulton and Harris "Representation Theory" [FH91]. The treatment we give below is less formal and primarily intended to give a framework for understanding the dimension of an algebraic group.

For a Lie group, the idea of the Lie algebra is that it is supposed to be the elements of the group that are infinitesimally close to the identity of the group. That is the elements X such that $(1 + X) \in G$ and X is "close" to 0. That is to say, it is precisely the tangent space to the "manifold" at the identity (T_e). One of the motivations for looking at this space is that in general one typically finds that a neighborhood of the identity generates most of the group, and as such understanding this infinitesimal neighborhood may give much information.

For the case of the algebraic group GL_n, the map $\mathrm{GL}_n \to \mathbb{A}^{n^2}$ makes it clear that the coordinate functions are just the components of the matrix. (To be pedantic one should look at first an embedding into M_{n+1}; we will not do this here.) It is also easy to see, since the condition of being

in GL_n is an open condition on $\mathbb{A}^{n^2}$ that you can travel in any direction (at least a small distance) from the identity and stay in GL_n and that these directions are all independent. Thus we have that $\mathrm{Lie}(\mathrm{GL}_n) = \mathrm{M}_n$. We note that the exponential map $\exp : A \mapsto 1 + A + A^2/2! + A^3/3! \ldots$ maps $\mathrm{Lie}(\mathrm{GL}_n)$ to GL_n. This phenomenon is in fact much more general.

Algebraically, there are a variety of different definitions one may take for the Lie algebra. One may take the Lie algebra to be the space of left invariant derivations, the tangent space at the identity or define it to be the dual to the cotangent space which has a natural algebraic definition as $\mathfrak{m}_{id}/\mathfrak{m}_{id}^2$. We will try to avoid getting into the algebraic formalism here. For a group $G \subset \mathrm{GL}_n$ we will view $\mathrm{Lie}(G)$ as $X \in \mathrm{M}_n = \mathrm{Lie}(\mathrm{GL}_n)$ such that "$id_G + \epsilon X \in G$" where $\epsilon^2 = 0$.

We wish to compute the Lie algebra for O_V, this can be done in several ways. The seemingly informal ways we present now can actually be made rigorous. Essentially one needs to make the argument that the operations we perform on matrices, can be carried out componentwise with the same effect.

Example (Lie Algebra of an Orthogonal Group)**.** Let V be a vector space over k, a field of characteristic not 2; fix a basis for V and let S be a symmetric matrix with non-zero determinant. Let Q be the quadratic form given by $Q(x) := ({}^t x)Sx$.

The basis for V gives us an isomorphism, $\mathrm{Aut}(V) \simeq \mathrm{GL}_n(k)$, under which:

$$\mathrm{O}_V \simeq \{M \in \mathrm{GL}_n(k) | {}^t MSM = S\}.$$

We then wish to view the tangent space of O_V as a subspace of the tangent space of GL_n. The tangent space is then the elements $X \in \mathrm{M}_n(k)$ such that $(1 + X) \in \mathrm{O}_V$ "mod squares". that is: ${}^t(1 + X)S(1 + X) = S$ which gives the condition:

$${}^t XS + SX = 0$$

where we consider ${}^t XSX$ a square since "it has 2 Xs". Rigourously ${}^t XSX$ is actually a square in the sense we mean, componentwise all the functions it contains will be generated by products of 2 coordinate functions each from the maximal ideal, and it is this that we are modding out by.

We will now compute the dimension of the Lie algebra, which from general theory will also be the dimension of the orthogonal group (as a manifold).

It suffices to consider the situation over the algebraic closure of k since dimensions won't change under extension(flatness), and here we may assume our quadratic form is the most trivial one, given by $S = id_n$ the identity matrix. The condition ${}^t XS + SX = 0$ then just says X is skew-symmetric. The space of skew symmetric matrices in $\mathrm{M}_n(\overline{k})$ is easily seen to have dimension $n(n-1)/2$. Therefore,

$$\dim(\mathrm{O}_V) = \frac{n(n-1)}{2} \text{ where } \dim(V) = n.$$

2.3 Orthogonal Groups and their Symmetric Spaces

Much of the material for this section can be found in J. Brunier "The 1-2-3 of Modular forms" [Bru08]. The material on quadratic spaces can also be found in J.P. Serre "A Course in Arithmetic" [Ser73], and the construction of the Clifford algebra and spin group, at least for the complex case, is also done in Fulton and Harris "Representation Theory"[FH91]. A more detailed construction of the symmetric spaces can also be found in J. Brunier "Borcherds products on O(2,1) and Chern classes of Heegner divisors" [Bru02].

The purpose of this section is to develop more concretely an understanding of the spaces we are trying to work with. We have the goal of understanding the special points in certain hermitian symmetric domains, but what are these and which are we intending to look at?

2.3.1 Hermitian Symmetric Spaces

In this section we will attempt to quickly define the general sorts of spaces that one typically considers modular functions on, that is, hermitian symmetric spaces. The general definitions for hermitian spaces can be found in all sorts of sources; our definitions here are based on those from J. Milne "Introduction to Shimura Varieties" [Mil05]. Another source on the topic is J. Helgason "Differential Geometry and Symmetric Spaces" [Hel01].

Definition 2.3.1. A **real manifold** M of dimension n is a separated topological space M, locally isomorphic to $\mathbb{R}^n$, with a countable basis for the topology.

Definition 2.3.2. A **smooth** manifold M is a manifold together with a sheaf $\mathcal{O}_M$ of smooth $\mathbb{R}$-valued functions, such that $(M, \mathcal{O}_M)$ is locally isomorphic to $\mathbb{R}^n$ with its usual sheaf of smooth functions.

Remark. To give a complex structure on M amounts to giving instead of a sheaf of $\mathbb{R}$-valued functions a sheaf of $\mathbb{C}$-valued functions that makes M locally isomorphic to $\mathbb{C}^n$ with its sheaf of analytic functions.

To give a complex structure on an $\mathbb{R}$-vector space V amounts to giving a function $J : V \to V$ such that $J^2 = -1$.

Definition 2.3.3. Denote by $\mathcal{O}_{M,p}$ the germs of smooth functions at a point $p \in M$; T_pM the space of $\mathbb{R}$-derivations $\mathcal{O}_{M,p} \to \mathbb{R}$; and by $T_pM^\vee$ the vector space dual of T_pM.

A **smooth vector field** on an open set $U \subset M$ is a collection $(X_p \in T_pM)_{p\in U}$ such that for all $f \in \mathcal{O}_M(U)$ the map $p \mapsto X_p(f)$ is smooth.

A **smooth r-tensor field** on an open set $U \subset M$ is a collection $(t_p : T_pM^r \to \mathbb{R})_{p\in U}$ such that for all smooth vector fields $X^{(1)}, \ldots, X^{(r)}$ on U the map $p \mapsto t_p(X^{(1)}, \ldots, X^{(r)})$ is smooth.

A **smooth (r,s)-tensor field** on an open set $U \subset M$ is $(t_p : T_pM^r \times (T_pM^\vee)^s \to \mathbb{R})_{p\in U}$ with a similar smoothness condition.

Definition 2.3.4. A **riemannian metric** on M is a smooth 2-tensor field g on M such that for each $p \in M$ the pairing $g_p : T_pM \times T_pM \to \mathbb{R}$ is symmetric and positive definite.

Definition 2.3.5. An **almost complex structure** on a smooth manifold M is a smooth (1,1)-tensor field $J_p : T_pM \to T_pM$ on M such that $J_p^2 = -1$ for each p. That is, it is a smoothly varying family of complex structures on the tangent spaces.

Remark. An actual complex structure induces an almost complex structure.

Definition 2.3.6. A **hermitian metric** is a riemannian metric such that $g(JX, JY) = g(X, Y)$ for all vector fields X, Y.

Definition 2.3.7. A **hermitian space** is a smooth real manifold M with a complex structure and a hermitian metric.

Definition 2.3.8. A **homogeneous space** is a manifold M such that $\mathrm{Aut}(M)$ acts transitively on M.

Definition 2.3.9. A homogeneous space is called **symmetric** if for some point p (equivalently any point) there exists a symmetry s_p such that $s_p^2 = id$ and for some open neighborhood U of p, p is the only fixed point of s_p in U.

Example. We present a few examples of hermitian symmetric spaces:

- $\mathbb{H}$, the standard upper half plane, is a symmetric space with volume element $\frac{dxdy}{y^2}$ which has automorphism group $\mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$. $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ acts as a symmetry at i.

Concretely, at a point $p = (x, y)$ the tangent space has basis $\frac{\partial}{\partial x}, \frac{\partial}{\partial y}$. We then have that the pairing is given by the formula $g_p(a_1\frac{\partial}{\partial x} + a_2\frac{\partial}{\partial y}, b_1\frac{\partial}{\partial x} + b_2\frac{\partial}{\partial y}) = \frac{a_1b_1+a_2b_2}{y^2}$. One checks that the complex structure $J : \frac{\partial}{\partial x} \mapsto \frac{\partial}{\partial y}$, $J : \frac{\partial}{\partial y} \mapsto -\frac{\partial}{\partial x}$ preserves this pairing. Moreover, one can check that the action of $\mathrm{SL}_2(\mathbb{R})$ also preserves the form.

- More generally, the Hilbert modular spaces $\mathbb{H}^n$ are hermitian symmetric spaces.
- The Siegal upper half space $\mathcal{H}_g := \{Z = X + iY \in M_g(\mathbb{C}) | Z = {}^tZ, Y \gg 0\}$ is a hermitian symmetric space. The group Sp_{2g} acts blockwise analogously to the first example. That is for
$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \circ Z = (AZ + B)(CZ + D)^{-1}, \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_{2g}.$$
One must check that this action is well defined.

It is our goal in the coming sections to develop a further example of a hermitian symmetric space constructed from certain orthogonal groups.

2.3.2 Quadratic Spaces

The following definitions are in some sense far more general than what is needed. To simplify things one may generally assume in the following that $R = k$ is a field of characteristic not 2 and that M is a vector space over k. The only more general setting we should need, is to consider discrete modules contained in these (that is lattices).

Definition 2.3.10. Let R be a commutative ring with unity, R^* the group of units, V a finitely generated R-module. A **quadratic form** on V is a mapping $Q : V \to R$ such that:

1. $Q(rx) = r^2Q(x)$ for all $r \in R$ and $x \in V$;
2. $B(x, y) := Q(x + y) - Q(x) - Q(y)$ is bilinear.

The pair (V, Q) will be called a **quadratic module** (or quadratic space) over R. The space is said to be **non-degenerate** if for any $x \in V$ we have $B(x, y) = 0$ for all $y \in V$, then we have $x = 0$.

We remark that in general the first condition follows from the second if $2 \in R^*$ as in this case $Q(x) = \frac{1}{2}B(x, x)$.

Example. Let $R = \mathbb{R}$ be the real numbers, let $(p, q) \in \mathbb{N}^2$, let $V = \mathbb{R}^{p+q}$ have coordinates given by $x_1, \ldots, x_p, y_1, \ldots, y_q$. Define $Q(v) = x_1^2 + \cdots + x_p^2 - y_1^2 - \cdots - y_q^2$. Then this gives a quadratic form on V. We will denote this quadratic space (V, Q) by $\mathbb{R}^{p,q}$

It turns out, that up to isomorphism (to be defined) these give all non-degenerate quadratic spaces over $\mathbb{R}$. One often calls (p, q) the signature of such a quadratic space. Later on, we shall discuss the various invariants attached to quadratic forms over $\mathbb{Q}$ and thus their classification.

Definition 2.3.11. Two vectors $x, y \in V$ are said to be **orthogonal** if $B(x, y) = 0$.

Using this definition one can define the notion of the orthogonal complement to a set.

Definition 2.3.12. Let $A \subset V$ then $A^\perp := \{x \in V | B(x, y) = 0 \ \forall y \in A\}$ is called the **orthogonal complement** of A.

We now wish to define the notion of morphism between quadratic spaces; we use the most natural definition.

Definition 2.3.13. Let (V, Q) and (V', Q') be quadratic spaces over R. We call an R-linear map $\sigma : V \to V'$ an **isometry** if for all $x \in V$ we have $Q'(\sigma(x)) = Q(x)$.

Example. Reflections: for an element $x \in M$ such that $Q(x) \in R^*$, define $\tau_x : M \to M$ via:

$$\tau_x(y) = y - B(y, x)Q(x)^{-1}x.$$

This is an isometry and in the vector space case can be seen as the reflection in the hyperplane $x^\perp$. Namely it fixes $x^\perp$ and takes x to $-x$.

Eichler Elements: Let $u \in M$ be isotropic ($Q(u) = 0$) and let $v \in M$ be such that $B(u, v) = 0$. Define:

$$E_{u,v}(y) = y + B(y, u)u - B(y, v)v - B(y, u)Q(v)u.$$

$E_{u,v}$ leaves $\{u, v\}^\perp$ fixed and has $E_{u,v}(u) = u$, $E_{u,v}(v) = v - 2Q(v)v$. Moreover, for $v_1, v_2 \in u^\perp$ these elements satisfy $E_{u,v_1} \circ E_{u,v_2} = E_{u,v_1+v_2}$.

We now define the objects we actually wish to study, that is the orthogonal group for a quadratic space.

Definition 2.3.14. Let (V, Q) be a quadratic space. The **orthogonal group** of V is:

$$\mathrm{O}_V := \{\sigma \in \mathrm{Aut}(V) |\ \sigma \text{ is an isometry}\}.$$

Definition 2.3.15. Suppose V is free and $v_1, \ldots, v_n$ is a basis for V, let $S := (B(v_i, v_j))_{i,j}$ then the element $\det(S) \in R/(R^*)^2$ is independent of the choice of basis and is called the discriminant $d(V)$. One can show that the space is non-degenerate if and only if $d(V) \neq 0$.

Remark. When the characteristic is not 2 giving a symmetric matrix S and a basis for V is equivalent to giving a quadratic form since any bilinear form is determined by its evaluation on a basis.

Moreover, when we are working over a field the Gram Schmidt process allows for the construction of an orthogonal basis for non-degenerate spaces. Doing so allows us to always view our quadratic form as being given by $a_1v_1^2 + \cdots + a_nv_n^2$ for some elements $a_i \in R$. Over more general rings it may not always be possible to fully diagonalize.

Choosing a basis for V also allows us to view the elements of the orthogonal group as being contained in "$\mathrm{GL}_n(R)$" which allows us to make the following definition.

Definition 2.3.16. The **special orthogonal group** is the subgroup of the orthogonal group consisting of elements of determinant 1, that is:

$$\mathrm{SO}_V := \{\sigma \in \mathrm{O}_V \,|\, \det(\sigma) = 1\}.$$

Remark. One should remark that the above definition is independent of choice of basis and embedding into GL_n.

Example. Having a basis, and viewing the elements of V as column vectors we can express B as:

$$B(x, y) = {}^t xSy.$$

As such, the statement $M \in \mathrm{O}_V$ amounts to saying ${}^tMSM = S$. In the $S = id$ case this is just ${}^tMM = id$, which gives us the usual notion of orthogonal matrices.

Theorem 2.3.17. *Let $R = k$ be a field of characteristic not 2, M a regular quadratic space (that is, for all $x \in M, \{x\}^\perp \neq M$). Then O_M is generated by reflections and SO_M is the subgroup of elements that are products of an even number of reflections.*

Sketch of proof. The first step is to observe that if for $x, y \in V$ we have $Q(x) = Q(y) \neq 0$ then either $\tau_{x+y}(y) = x$ or $\tau_x(\tau_{x-y}(y)) = x$.

The next step is to observe that V must contain a non-isotropic vector x, and any orthogonal map M carries it to another vector y with $Q(x) = Q(y) \neq 0$. Then composing the orthogonal map with τ as appropriate from above, we get $\tau \circ M$ is an orthogonal map fixing x and thus stabilizing $x^\perp$. Since $\dim_k(x^\perp) < \dim_k(x)$ we can apply induction and conclude the result. □

Classification of Quadratic Forms (over $\mathbb{Q}$)

We now wish to define the invariants of quadratic forms that allows for their classification over $\mathbb{Q}$. Most of the material of this section can be found in J.P. Serre "A Course in Arithmetic"[Ser73]. First we introduce the Hilbert symbol.

The Hilbert Symbol

Definition 2.3.18. Let K be a (local) field then the Hilbert Symbol:

$$(-,-)_K : K^* \times K^* \to \pm 1$$

is defined via the rule:

$$(a,b)_K = 1 \Leftrightarrow x^2 - ay^2 - bz^2 = 0 \text{ has non-trivial solutions in } K.$$

Although the definition essentially makes sense for any field K, some of the following results require K to be a local field.

What the Hilbert symbol is computing in actuality is whether or not the quaternion algebra of type (a,b) is split over K. It is in this sense telling you information about the class of the quaternion algebra (a,b) in the Brauer group $Br(K)$.

One can check that the Hilbert Symbol satisfies the following properties:

Proposition 2.3.19. *[Ser73] For all $a,b,c \in K^*$ one has:*

1. $(a,b)_K = (b,a)_K$;
2. $(1,1)_K = (a,1)_K = (a,1-a)_K = (a,c^2)_K = 1$;
3. $(a,b)_K(a,c)_K = (a,bc)_K$.

The first two assertions are immediate, the last is a consequence of local class field theory.

Over the various completions of the rational numbers, the Hilbert symbol satisfies the following closed form:

Proposition 2.3.20. *[Ser73, 3.1.2] Let p be a prime, $a,b \in \mathbb{Q}$ with $a = p^\alpha u$, $b = p^\beta v$ where u,v coprime to p.*
if p is odd then:

$$(a,b)_{\nu_p} = (-1)^{\alpha\beta(p-1)/2} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$$

if $p = 2$ then:

$$(a,b)_{\nu_p} = (-1)^{(u-1)(v-1)/4 + \alpha\left(v^2-1\right)/8 + \beta\left(u^2-1\right)/8}$$

if $p = \infty$ then:

$$(a,b)_{\nu_p} = -1 \Leftrightarrow a,b < 0.$$

Moreover, for almost all valuations ν we have $(a,b)_\nu = 1$ and $\prod_\nu (a,b)_\nu = 1$.

In the above $\left(\frac{u}{p}\right)$ denotes the Legendre symbol.

There is also the following important result about the existence of rational numbers with prescribed Hilbert symbols.

Theorem 2.3.21. *[Ser73, 3.2.2] Let $(a_i)_{i\in I}$ be a finite collection of elements of $\mathbb{Q}^*$ and let $(e_{i,\nu})_{i\in I,\nu\in V} \in \{\pm 1\}$. In order that there exist $x \in \mathbb{Q}^*$ such that $(a_i,x)_\nu = e_{i,\nu}$ for all $i \in I$ and $\nu \in V$ it is necessary and sufficient that:*

1. *for almost all ν and i we have $e_{i,\nu} = 1$.*
2. *for all $i \in I$ we have $\prod_\nu e_{i,\nu} = 1$.*

3. for all $\nu \in V$ there exists $x_\nu \in \mathbb{Q}_\nu^*$ such that $(a_i, x_\nu)_\nu = e_{i,\nu}$ for each $i \in I$.

Invariants of Quadratic Forms (over $\mathbb{Q}$)

We now proceed to define the invariants of a quadratic form:

Definition 2.3.22. Let $q(x_1, \ldots, x_n) = \sum_{i=1}^n a_i x_i^2$ $a_i \in \mathbb{Q}$ then the invariants are:

1. The discriminant $d_q := \prod_{i=1}^n a_i \in \mathbb{Q}^*/\mathbb{Q}^{*2}$.
2. The Hasse-Witt invariants e_{ν_p} for each valuation ν_p of $\mathbb{Q}$, where $e_{\nu_p} := \prod_{i<j} (a_i, a_j)_{\nu_p}$.
3. The signature (r, s), where $r := \#\{a_i < 0\}$ and $s := \#\{a_i > 0\}$.

Remark. One should note that we can also view these as cohomological invariants (see 3.1 for the definition of group cohomology) via the identifications:

$$d_q \in \mathbb{Q}^*/\mathbb{Q}^{*2} = H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$$

$$(e_{\nu_p})_{\nu_p} \in H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z}) = Br(\mathbb{Q})[2].$$

The first identification comes via the exact sequences:

$$1 \to \{\pm 1\} \to \overline{\mathbb{Q}}^* \xrightarrow{x^2} \overline{\mathbb{Q}}^* \to 1$$

$$0 \to \{\pm 1\} \to \mathbb{Q}^* \xrightarrow{x^2} \mathbb{Q}^* \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z}) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \overline{\mathbb{Q}}^*) = 0.$$

Which gives:

$$H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Q}^*/\mathbb{Q}^{*2}.$$

The second identification comes out of the fact that the Brauer Group of a field K classifies finite dimensional central simple division algebras over K and moreover the 2-torsion classifies the quaternion algebras over that field. The primary invariant of a quaternion algebra over $\mathbb{Q}$ is how it splits at the various places. In particular the map:

$$H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z}) \to \prod_p H^2(\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p), \mathbb{Z}/2\mathbb{Z})$$

allows us to detect if a quaternion algebra is split at the various primes. It is in this way that one associates a collection of values ($e_{\nu_p} = \pm 1$) to a quaternion algebra. The element of the Brauer group associated to a quadratic form is the class of the algebra $\bigotimes_{i<j}(a_i, a_j)$.

One can also remark that under the general method of classifying forms which we shall describe (see 3.1) one has that quadratic spaces are classified by:

$$H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(V, Q)) = H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{O}_V).$$

One can use spectral sequences and other methods to construct maps:

$$H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{O}_V) \hookrightarrow \bigoplus_i H^i(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$$

which allow one to realize the above construction. For a more detailed account see "Cohomological Invariants in Galois Cohomology" [GMS03]. One can then interpret the following theorems as saying that this map remains injective even when we project onto the $i = 1, 2$ components. The result is true over $\mathbb{Q}$, more generally a similar statement holds for number fields.

We cite here some of the key theorems concerning the classification of quadratic forms over $\mathbb{Q}$ and their invariants.

Theorem 2.3.23. *[Ser73] Let $(V_1, q_1), (V_2, q_2)$ be quadratic spaces over $\mathbb{Q}$, then they are isomorphic (as quadratic spaces) if and only if q_1 and q_2 have all the same invariants.*

Theorem 2.3.24 (Existence of Quadratic Forms)**.** *[Ser73, p44] Let $d \in \mathbb{Q}^*/\mathbb{Q}^{*2}$, $e_{\nu_p} \in \{\pm 1\}_{\nu_p}$ for each ν_p and $(r, s) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$. Let $n = r + s$. In order that there exist a quadratic form q with this prescribed set of invariants. It is necessary and sufficient that:*

1. *$e_{\nu_p} = 1$ for almost all ν_p and $\prod_\nu e_\nu = 1$.*
2. *(a) if $n = 1$ then $e_{\nu_p} = 1$ for all ν_p;*
   (b) if $n = 2$ then either the image of d in $Q^*_{\nu_p}/{Q^*_{\nu_p}}^2 \neq -1$ or $e_{\nu_p} = 1$;
   (c) if $n \geq 3$ there are no additional conditions.
3. *$d_{\nu_\infty} = (-1)^s$ and $e_{\nu_\infty} = (-1)^{s(s-1)/2}$.*

Proposition 2.3.25. *Let q be a quadratic form as above, $\lambda \in \mathbb{Q}^*$, then the quadratic form $q_\lambda := \lambda q$ has invariants:*

1. *$d_\lambda = \lambda^n d$;*
2. *$e_{\nu_p \lambda} = e_{\nu_p}(\lambda, \lambda)^{n(n-1)/2}_{\nu_p}(\lambda, d^{n-1})_{\nu_p}$;*
3. *$(r_\lambda, s_\lambda) = (r, s)$ if $\lambda > 0$; (s, r) otherwise.*

Proof. The only difficult check is that of the Witt invariants, it follows from the computation:

$$\begin{aligned}
\prod_{i<j}(\lambda a_i, \lambda a_j)_{\nu_p} =& \prod_{i<j}(\lambda, \lambda)_{\nu_p}(\lambda, a_j)_{\nu_p}(a_i, \lambda)_{\nu_p}(a_i, a_j)_{\nu_p} \\
=& (\lambda, \lambda)^{n(n-1)/2}_{\nu_p}\prod_{i<j}(\lambda, a_i a_j)_{\nu_p}\prod_{i<j}(a_i, a_j)_{\nu_p} \\
=& (\lambda, \lambda)^{n(n-1)/2}_{\nu_p}(\lambda, \prod_{i<j} a_i a_j)_{\nu_p}\prod_{i<j}(a_i, a_j)_{\nu_p} \\
=& (\lambda, \lambda)^{n(n-1)/2}_{\nu_p}(\lambda, d^{n-1})_{\nu_p}\prod_{i<j}(a_i, a_j)_{\nu_p}
\end{aligned}$$

□

Proposition 2.3.26. *Let q_1, q_2 be quadratic forms over $\mathbb{Q}$. Let the quadratic forms q_i have invariants d_i, $e_{\nu_p i}$, (r_i, s_i), n_i. Then the quadratic form $q := q_1 \oplus q_2$ has invariants:*

1. *$d_q = d_1 d_2$;*
2. *$e_{\nu_p q} = (d_1, d_2)_{\nu_p} e_{\nu_p 1} e_{\nu_p 2}$;*
3. *$(r_q, s_q) = (r_1, s_1) + (r_2, s_2)$.*

Proof. The only non-immediate check is that of the Witt invariants, it follows from the computation:

$$\begin{aligned}
e_{\nu_p q} =& \prod_{i<j}(a_i, a_j)_{\nu_p}\prod_{i<j}(b_i, b_j)_{\nu_p}\prod_{i,j}(a_i, b_j)_{\nu_p} \\
=& e_{\nu_p 1} e_{\nu_p 2}\prod_{i,j}(a_i, b_j)_{\nu_p} \\
=& e_{\nu_p 1} e_{\nu_p 2}\prod_{i}(a_i, d_2)_{\nu_p} \\
=& e_{\nu_p 1} e_{\nu_p 2}(d_1, d_2)_{\nu_p}
\end{aligned}$$

□

Proposition 2.3.27. *Let q_1, q_2 be quadratic forms over $\mathbb{Q}$ with invariants as above, $\lambda \in \mathbb{Q}^*$, then the quadratic form $q := (\lambda q_1) \oplus q_2$ has the following invariants:*

1. $d_q = \lambda^{n_1} d_1 d_2$;
2. $e_{\nu_p q} = e_{\nu_p 1} e_{\nu_p 2} (\lambda, \lambda)_{\nu_p}^{n_1(n_1-1)/2} (\lambda^{n_1} d_1, d_2)_{\nu_p} (\lambda, d_1^{n_1-1})_{\nu_p}$;
3. $(r_q, s_q) = (r_1, s_1) + (r_2, s_2)$ *if* $\lambda > 0$, $(s_1, r_1) + (r_2, s_2)$ *otherwise.*

Proof. This follows immediately from previous two propositions. □

The Clifford Algebra of a Quadratic Space

As before, let R be a commutative ring with unity, and let (V, Q) be a finitely generated quadratic space over R. For an R algebra A we will denote $Z(A)$ its center.

Definition 2.3.28. Let T_V be the tensor algebra of V, that is $T_V := \bigoplus_{m=0}^{\infty} V^{\otimes m}$. Let I_V be the two-sided ideal in T_V generated by the elements $v \otimes v - Q(v)$ for $v \in V$. Then the **Clifford algebra** for V is

$$\mathrm{C}_V := T_V / I_V.$$

Remark. One should notice that V has a natural embedding into C_V via $v \mapsto v$. There may however be in some special cases more than one way to embed V into C_V. However, unless explicitly mentioned we always take $V \subset \mathrm{C}_V$ in the natural way.

One should also observe that the relation $v \otimes v - Q(v)$ implies $v_1 \otimes v_2 + v_2 \otimes v_1 = B(v_1, v_2)$ for $v_i \in V$. In particular, if R is a field (or a nice enough ring), and if we choose an orthogonal basis $\{v_1, \ldots, v_n\}$ for V, then we have the basis for C_V given by:

$$\{v_{i_1} \otimes \cdots \otimes v_{i_j} |\ 0 < i_1 < \cdots < i_j \leq n, 1 \leq j \leq n\}.$$

In particular C_V has dimension 2^n over R.

The Clifford algebra satisfies the following universal property:

Proposition 2.3.29. *Let A be any R-algebra and $f : V \to A$ an R-linear map with $f(v)^2 = Q(v)1_A$ for all $v \in V$. Then there exists unique R-algebra homomorphism $g : \mathrm{C}_V \to A$ such that $f(v) = g(v)$ for all $v \in V$.*

Proof. (Sketch) The proof of this fact is to appeal to the universal property of tensor products and to note that the map descends to the quotient by I_V because of the condition $f(v)^2 = Q(v)1_A$. □

Example. If we let $C_{p,q}$ be the Clifford algebra for $\mathbb{R}^{p,q}$ we can compute that:

$C_{0,0} \simeq \mathbb{R}$	$C_{1,0} \simeq \mathbb{R} \oplus \mathbb{R}$
$C_{0,1} \simeq \mathbb{C}$	$C_{2,0} \simeq \mathrm{M}_2(\mathbb{R})$
$C_{1,1} \simeq \mathrm{M}_2(\mathbb{R})$	$C_{0,2} \simeq \mathbb{H}$

(where $\mathbb{H}$ is the hamiltonian quaternions). To demonstrate the computation observe that $C_{0,2}$ is an algebra over $\mathbb{R}$ in two non-commuting indeterminants x, y with the relations $x^2 = y^2 = -1$, $xy = -yx$. This gives the usual presentation of the quaternions.

We next observe that because the relation defining I_V involves only tensors of even length, there is a natural $\mathbb{Z}/2\mathbb{Z}$ grading on C_V with $\mathrm{C}_V = \mathrm{C}_V^0 \oplus \mathrm{C}_V^1$ where $\mathrm{C}_V^0, \mathrm{C}_V^1$ are the even and odd length tensors respectively. Note that C_V^0 is a subalgebra, called the even Clifford algebra, but C_V^1 is just a vector subspace.

Since multiplication by -1 on V is an isometry we can use it to induce an automorphism J of the Clifford algebra called the **canonical automorphism**. It is easy to see that (if $2 \in R^*$) $\mathrm{C}_V^0 = \{x \in \mathrm{C}_V | J(x) = x\}$.

Next we define the **canonical involution** $x \mapsto {}^t x$ on C_V. It is defined by linearly extending ${}^t(x_1 \otimes \cdots \otimes x_n) = x_n \otimes \cdots \otimes x_1$. We can use this to define the **Clifford norm**:

$$N(x) = {}^t x x,$$

which extends Q from V to C_V.

We now fully restrict our attention to the case $R = k$ a field of characteristic not 2. Let (V, Q) be a non-degenerate quadratic space and let $v_1, \ldots, v_n$ be an orthogonal basis of V. Set:

$$\delta = v_1 \otimes \ldots \otimes v_n \in \mathrm{C}_V.$$

It follows from the fact that one can move from any one orthogonal basis to any other by steps which modify only two of the basis elements, and by inspecting what such changes can do, that the choice of δ is canoncial up to scaling by k^*.

Theorem 2.3.30. *The center of* C_V *is given by:* $Z(\mathrm{C}_V) = k$ *if* n *is even,* $k + \delta k$ *if* n *is odd. The center of* C_V^0 *is given by:*

$$Z(\mathrm{C}_V^0) = \begin{cases} k + \delta k & n \text{ even} \\ k & n \text{ odd.} \end{cases}$$

Sketch of Proof. The Clifford algebra is generated over k by the images of $x_1 \otimes \cdots \otimes x_l$. It is thus easy to check that the centers contain the given elements. To check that those elements are the entire center follows from the following observations:

1. If a basis vector v_i is to commute with a linear combination of the basis tensors described above it will need to commute with each individual basis tensor involved. (This is because failure to commute with such a basis tensor is only off by multiplication by -1).
2. A basis vector v_i commutes with a tensor of the form $v_{l_1} \otimes \cdots \otimes v_{l_j}$ if and only if it does not appear it in and the tensor is of even length or it does appear and the tensor is of odd length. (this follows from inspecting when you do/don't have the -1 error).

Thus, if an elementary tensor is to commute with every basis vector, it must either contain none and be of odd length or all and be of even length. This completes the argument. □

Example. Let V be a non-degenerate vector space over k of dimension n and $v_1, \ldots, v_n$ an orthogonal basis for V.

1. if $n = 1$ then $\mathrm{C}_V \simeq k[X]/(X^2 - Q(v_1)/2)$;
2. if $n = 2$ then C_V is a quaternion algebra of type $(Q(v_1), Q(v_2))$ and moreover we have that $\mathrm{C}_V^0 \simeq k[X]/(X^2 + Q(v_1)Q(v_2))$;
3. if $n = 3$ then C_V^0 is a quaternion algebra of type $(-Q(v_1)Q(v_2), -Q(v_2)Q(v_3))$;
4. if $n = 4$ then C_V^0 is a quaternion algebra of type $(-Q(v_1)Q(v_2), -Q(v_2)Q(v_3))$ over the ring $Z(\mathrm{C}_V^0) = k + \delta k$.

Moreover in all the above cases the conjugation and norm on C_V^0 correspond to the main involution and Clifford norm respectively. To see how one shows this, observe that for the $n = 4$ case, every even length tensor can be arrived at by taking products of v_1v_2, v_2v_3 and δ, Thus v_1v_2, v_2v_3 generate C_V^0 over $Z(\mathrm{C}_V^0)$. It remains then only to check that the relations give the quaternion algebra structure. Moreover, one can see that $\delta^2 = Q(v_1)Q(v_2)Q(v_3)Q(v_4)$.

The Spin Group

The goal of this section is to define the spin group, which will be the covering space of the special orthogonal group.

We would like to make two remarks. Firstly, given any semi-simple (connected) algebraic group G, there are two natural other groups to consider. These are the adjoint group, $G/Z(G)$ where $Z(G)$ is the center of G, and the universal covering space of G. In general (for semi-simple groups) the former always has finite index in the latter, and many of the properties of one are shared by the others. In particular, they share Lie algebras. Both groups are often easier to study than the original. The spin group shall arise as the universal covering space of the special orthogonal group.

Secondly, the term spin group arises from physics. The notion is that physical laws should be independent of choices made by observers and so any coordinate system an observer uses to model the universe should be equally valid. As a consequence of this one concludes that the laws ought to be preserved under isometric transformations. It turned out that under appropriate modeling of certain subatomic particles there was an extra degree of freedom for the configuration space that did not seem to correspond to vector valued locations or directions but was rather a binary property of individual particles. This property was labeled as the "spin" of the particle. Once one applies mathematical language to this model, this extra spin parameter corresponds to what is additionally captured by the covering space of an orthogonal group. For examples of the spin group in physics see S. Weinberg "Quantum Theory of Fields" [Wei99].

The first step towards the construction of this covering is to define the Clifford group.

Definition 2.3.31. The **Clifford group** CG_V is defined to be:

$$\mathrm{CG}_V := \{x \in \mathrm{C}_V | x \text{ invertible and } xVJ(x)^{-1} = V\}.$$

It is easy to check that this is a group.

Notice that for each $x \in \mathrm{CG}_V$ the function:

$$\alpha_x(v) = xvJ(x)^{-1}$$

is an automorphism of V. We thus have a representation:

$$\alpha : \mathrm{CG}_V \to \mathrm{Aut}_R(V),$$

called the vector representation. We observe that ${}^t : x \mapsto {}^t x$ takes CG_V to itself and thus so does the Clifford norm.

Example. Starting with a vector space V over a field k of characteristic not 2, and given an orthogonal basis $v_1, \ldots, v_n$ then every elementary tensor $v_{i_1} \otimes \cdots \otimes v_{i_j}$ is invertible and moreover for each k we have $(v_{i_1} \otimes \cdots \otimes v_{i_j}) v_k J(v_{i_1} \otimes \cdots \otimes v_{i_j})^{-1} = \pm Q(v_{i_1}) \cdots Q(v_{i_j}) v_k$ and so $v_{i_1} \otimes \cdots \otimes v_{i_j} \in \mathrm{CG}_V$.

Lemma 2.3.32. *If $R = k$ a field of characteristic not 2, then $\mathrm{Ker}(\alpha) = k^*$ and the Clifford norm gives a homomorphism $N : \mathrm{CG}_V \to k^*$.*

Proof. It is easy to see that because the J map acts trivially on C_V^0 we have $k^* \subset \mathrm{Ker}(\alpha)$.

Conversely let $x \in \mathrm{Ker}(\alpha)$. we can then write $x = x_0 + x_1$ with $x_0 \in \mathrm{C}_V^0$ and $x_1 \in \mathrm{C}_V^1$. Using that for all $v \in V$ we have $xvJ(x)^{-1} = v$ we get $(x_0 + x_1)v(x_0 - x_1)^{-1} = v$ and so rearranging this we have $x_0 v + x_1 v = v x_0 - v x_1$. Looking at the C_V^0 and C_V^1 components and noting that V generates C_V as an algebra we can conclude:

$$x_0 \in Z(\mathrm{C}_V) \cap \mathrm{C}_V^0 = k^*.$$

The implication $x_1 v = v x_1 \Rightarrow x_1 = 0$ is proven similarly to computing the center of C_V. This completes the first assertion that $\mathrm{Ker}(\alpha) = k^*$.

Now, for $v \in V$ we have $\alpha_x(v) \in V$ and so $\alpha_x(v) = -{}^tJ(\alpha_x(v))$; it follows then that we have $xvJ(x)^{-1} = {}^tx^{-1}vJ({}^tx)$ and so:

$$N(x)vJ(N(x))^{-1} = v.$$

In particular $N(x) \in \mathrm{Ker}(\alpha) = k^*$. □

Lemma 2.3.33. *For each $x \in \mathrm{CG}_V, \alpha_x$ is an isometry.*

Proof. For $v \in V$ we have:

$$Q(a_x(v)) = N(a_x(v)) = ({}^tJ(x^{-1}))({}^tv)({}^tx)xvJ(x^{-1}) = Q(v).$$

□

In particular this gives us a homomorphism $\alpha : \mathrm{CG}_V \to \mathrm{O}_V$ with kernel k^*. Moreover, if $x \in \mathrm{CG}_V \cap V$, then $Q(x) \in k^*$ and thus we have:

$$\alpha_x(v) = xv(-x)Q(x)^{-1} = (vx - B(x,v))Q(x)^{-1}x = v - B(x,v)Q(x)^{-1}x$$

corresponds to the reflection in the plane $x^\perp$.

Definition 2.3.34. We define the groups GSpin_V and Spin_V as follows:

$$\mathrm{GSpin}_V := \mathrm{CG}_V \cap \mathrm{C}_V^0 \qquad \mathrm{Spin}_V := \{x \in \mathrm{GSpin}_V \,|N(x) = 1\}.$$

In the case where reflections generate the orthogonal group (which is the case when V is a regular quadratic space) we get the exact sequence:

$$1 \to k^* \to \mathrm{CG}_V \xrightarrow{\alpha} \mathrm{O}_V \to 1$$

and since SO_V is the subgroup of elements which are products of an even numbers of reflections we also have:

$$1 \to k^* \to \mathrm{GSpin}_V \xrightarrow{\alpha} \mathrm{SO}_V \to 1.$$

Using that $N : \mathrm{CG}_V \to k^*$, we can construct an induced homomorphism

$$\theta : \mathrm{O}_V \to k^*/(k^*)^2,$$

called the **spinor norm**. It is defined by taking a section of α and computing the norm in CG_V. One must check that different choices of sections give the same result up to elements of $(k^*)^2$. Indeed, since $\mathrm{Ker}(\alpha) = k^*$, a different section of α will give a k-multiple of the original choice, since the norm map acts on k by squaring, this is the desired result.

We observe next that for $x \in V$ and τ_x the associated reflection we get $\theta(\tau_x) = Q(x)$. To see this recall that $\tau_x = \alpha_x$ and thus can be lifted to x and $N(x) = Q(x)$.

We then obtain the exact sequence:

$$1 \to \mu_2 \to \mathrm{Spin}_V \xrightarrow{\alpha} \mathrm{SO}_V \xrightarrow{\theta} k^*/(k^*)^2.$$

Remark. We remark that the sequence:

$$1 \to \mu_2 \to \mathrm{Spin}_V \to \mathrm{SO}_V \to 1$$

is exact as a sequence of algebraic groups over k in the sense that $\mathrm{SO}_V \simeq \mathrm{Spin}_V/\mu_2$. This statement implies that for any k algebra L the sequence on points:

$$1 \to \mu_2(L) \to \mathrm{Spin}_V(L) \to \mathrm{SO}_V(L)$$

is exact. However, the mapping $\mathrm{Spin}_V(L) \to \mathrm{SO}_V(L)$ is not in general surjective. However, given any L there exists a finite extension L' of L such that the image of $\mathrm{Spin}_V(L')$ contains $\mathrm{SO}_V(L)$. Consequently we have that:

$$1 \to \mu_2(\overline{k}) \to \mathrm{Spin}_V(\overline{k}) \to \mathrm{SO}_V(\overline{k}) \to 1$$

is exact. Taking $\mathrm{Gal}(\overline{L}/L)$ invariants we find:

$$1 \to \mu_2(L) \to \mathrm{Spin}_V(L) \to \mathrm{SO}_V(L) \to H^1(\mathrm{Gal}(\overline{L}/L), \mu_2)$$

is exact. This tells us that the obstruction to exactness lies in $H^1(\mathrm{Gal}(\overline{L}/L), \mu_2) \simeq L^*/L^{*2}$.

The following example shall be of some use to us later:

Example. Consider the quadratic space $\mathbb{R}^{2,n}$ and consider a positive definite plane $V \subset \mathbb{R}^{2,n}$ and its orthogonal complement $V^\perp$ which is a negative definite space. Let V have orthogonal basis x_1, x_2 and $V^\perp$ have orthogonal basis $x_3, \ldots, x_{n+2}$. Consider the orthogonal maps M_i which sends $x_i \mapsto -x_i$ and $x_j \mapsto x_j$ for $i \neq j$. Then we note that $\det(M_i) = -1$ for each i.

However, we have that since M_i is the reflection τ_{x_i} we get $\theta(M_i) = Q(x_i) = 1$ for $i = 1, 2$ and $\theta(M_i) = Q(x_i) = -1$ otherwise.

In particular, $\det(M_i) = \theta(M_i)$ whenever the reflection preserves the orientation of a positive definite plane. Since reflections generate the orthogonal group, this statement is in fact true for all orthogonal maps.

For the purpose of doing computations in low dimensions, the following lemma is useful.

Lemma 2.3.35. *If* $\dim(V) \leq 4$ *then* $\mathrm{GSpin}_V = \{x \in \mathrm{C}_V^0 | N(x) \in k^*\}$, $\mathrm{Spin}_V := \{\mathrm{C}_V^0 | N(x) = 1\}$.

Proof. The first observation is that for $\dim(V) \leq 4$ we have:

$$V = \{g \in \mathrm{C}_V^1 | {}^t g = g\}.$$

This follows by checking that a tensor of length 3 of orthogonal elements satisfies $x^t = -x$.

The next observations is that if $N(x) \in k^*$ then $x^t N(x)^{-1}$ is the inverse of x. Consequently, the equation $N(x) v N(x)^{-1} = v$ implies that $xvx^{-1} = (xvx^{-1})^t$ which implies that x satisfies the conditions to be in C_V^0. This completes the result. □

Example. From the examples of the previous section we get that the groups Spin_n for $n = 1, \ldots, 4$ correspond to the elements of norm 1 from particular algebras. Specifically, in the cases $n = 3, 4$ we had the norm 1 elements of a particular quaternion algebra.

2.3.3 The Symmetric Space of an Orthogonal Group

Let (V, Q) be a quadratic space over $\mathbb{Q}$. The real quadratic space $V(\mathbb{R}) := V \otimes \mathbb{R}$ is isomorphic to $\mathbb{R}^{p,q}$ for some choice of p, q.

If $K \subset \mathrm{O}_V(\mathbb{R})$ is a maximal compact subgroup, then it will turn out that $\mathrm{O}_V(\mathbb{R})/K$ is a symmetric space (every point has a symmetry for which it is the unique local fixed point). It turns out that these only have complex structures (and thus are hermitian) if one of p or q is 2. Since interchanging p, q does not change the orthogonal group (it amounts to replacing Q by $-Q$) we

suppose that $p = 2$. We wish to construct these spaces along with their complex structure for this case.

Remark. For the next while, we will be discussing the structure of $\mathbb{R}$ points, and as such the only invariants of significance are these values p, q. However, when we mention rational boundary points the remaining details about the structure over $\mathbb{Q}$ become important. So although topologically, the spaces we define in what follows may be isomorphic, the rational structures on them may not be so simple.

The Grassmannian - Maximal Compacts

Let (V, Q) be a quadratic space over $\mathbb{Q}$ of type $(2, n)$. We consider the Grassmannian of 2-dimensional subspaces of $V(\mathbb{R})$ on which the quadratic form Q restricts to one which is positive definite, that is:

$$\mathrm{Gr}(V) := \{v \subseteq V(\mathbb{R}) |\ \dim(v) = 2, Q|_v > 0\}.$$

Theorem 2.3.36. *(Witt's Extension Theorem) [Ser73, IV.1.5] If (V, Q) and (V', Q') are non-degenerate isometric quadratic spaces, then every injective isometry $s : U \hookrightarrow V'$ from a subspace $U \subset V$ extends to an isometry $s : V \to V'$.*

Proof. For simplicity of notation we may assume that $V = V'$ since they are isomorphic.

We first handle the case where U is degenerate by extending s to some U' containing U which is non-degenerate. Let $x \in U$ such that $B(x, u) = 0$ for all $u \in U$. Then since V is non-degenerate there exists $y \in V$ such that $B(x, y) \neq 0$, we can replace y by $\frac{y}{B(x,y)}$ so that $B(x, y) = 1$ and we can then replace y by $y - \frac{1}{2}B(y, y)x$ so that $B(y, y) = 0$. We now consider the linear operator on $s(U)$ defined by $l(u') = B(s^{-1}(u'), y)$. By non-degeneracy of V this linear operator takes the form $B(u', y')$ for some $y' \in V$. As with y we may arrange so that $B(y', y') = 0$. We may now extend the original map to $U \oplus \mathrm{span}(y)$ by taking $y \mapsto y'$. The conditions on y' guarantee this map is an isometry. We can perform this process repeatedly so long as U is degenerate.

We may now assume U is non-degenerate. We proceed by induction on the dimension of U.

- $\dim(U) = 1$
  Fix $x \in U$ and let $y = s(x)$ then one can check that one of $x + y$, $x - y$ is non-isotropic call this z. Let $H = z^\perp$. Let s' be the map which sends $z \mapsto -z$ and fixes H, that is the reflection in $z^\perp$. Then s' extends s to V.
- $\dim(U) > 1$
  We can non-trivially orthogonally decompose $U = U_1 \oplus U_2$, then by induction $s|_{U_1}$ extends to a map σ on V. take $r = \sigma^{-1} \circ s$ then r acts as the identity on U_1 and so $r : U_2 \to U_2 = U_1^\perp$. By induction $r|_{U_2}$ extends to a map $r' : U_1^\perp \to U_1^\perp$. We extend r' to V by having it act as the identity on U_1. The map $s' = \sigma \circ r'$ then extends s to V.

Induction then completes the result. □

By Witt's extension theorem, the group $\mathrm{O}_V(\mathbb{R})$ acts transitively on $\mathrm{Gr}(V)$.

Claim. *Fix $v_0 \in \mathrm{Gr}(V)$ and let K_{v_0} be the stabilizer of v_0 in $\mathrm{O}_V(\mathbb{R})$. Then $K_{v_0}(\mathbb{R})$ is a maximal compact subgroup of $\mathrm{O}_V(\mathbb{R})$.*

Proof. First observe that since K_{v_0} preserves the plane v_0 it also preserves its orthogonal complement, consequently by correct choice of basis we can write $K_{v_0} \simeq \mathrm{O}_2 \times \mathrm{O}_n$ over $\mathbb{R}$.

Lemma 2.3.37. *Let (V', q') be a quadratic space, then $\mathrm{O}_{q'}(\mathbb{R})$ is compact if and only if q' is definite.*

Proof. The forward direction is clear. Indeed, if q' is indefinite then it must contain as a subgroup the image of $\mathrm{SO}(1, 1) = \{\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right) |\ a^2 - b^2 = 1\}$ which is non-compact as it is unbounded. This is

because once we diagonalize the form over $\mathbb{R}$ we find there is a two dimensional subspace where the quadratic form must take the shape $q'(x_1v_1+x_2v_2) = x_1^2 - x_2^2$. We can consider the subgroup of $\mathrm{O}_{q'}$ that acts on this subspace as $\mathrm{SO}(1,1)$ and stabilizes the orthogonal complement, this subgroup is not compact.

For the reverse direction, observe that for a matrix $M \in \mathrm{O}_{q'}(\mathbb{R})$, expressed via an orthogonal basis $v_1, \ldots, v_n$, we have that the columns c_i of M viewed as vectors in $\mathbb{R}^n$ satisfy $\|c_i\| = \pm Q(v_i)$ in particular the norms of the columns are bounded in the usual Euclidean norm. Consequently $\mathrm{O}_{q'}$ is bounded in the real topology in $\mathbb{R}^{n^2}$. Since $\mathrm{O}_{q'}(\mathbb{R})$ is a closed subset of $\mathrm{M}_n(\mathbb{R})$ it is thus compact. □

It follows from the claim that $K_{v_0}(\mathbb{R})$ is compact as it is the product of two compact sets.

To see that it is maximal, we first remark that a maximal $\mathbb{R}$ compact in $\mathrm{GL}_{n+2}(\mathbb{R})$ is given by the usual orthogonal group $\mathrm{O}_{n+2}(\mathbb{R})$. To see this remark that any strictly larger subgroup contains an element which does not preserve the metric on $\mathbb{R}^{n+2}$, thus we can construct an element g and find an $x \in \mathbb{R}^{n+2}$ such that $g(x) = ax$ with $a > 1$. Consequently g^n is unbounded. We remark further that any two maximal compacts in $\mathrm{GL}_{n+2}(\mathbb{R})$ are conjugate (this is a consequence of the Iwasawa decomposition) and that this corresponds to a different choice of inner product on $\mathbb{R}^n$.

From this we conclude that the compact group $\mathrm{O}_2(\mathbb{R}) \times \mathrm{O}_n(\mathbb{R})$ must be contained in some maximal compact subgroup of $\mathrm{GL}_{n+2}(\mathbb{R})$. Indeed $\mathrm{O}_2(\mathbb{R}) \times \mathrm{O}_n(\mathbb{R}) = \mathrm{O}_{n+2}(\mathbb{R}) \cap \mathrm{O}_V(\mathbb{R})$. It follows from the proof of Lemma 4.1.1 that $\mathrm{O}_2(\mathbb{R}) \times \mathrm{O}_n(\mathbb{R})$ preserves no other inner products except for independent re-scalings of the inner product on the 2 and n dimensional subspaces. Any of these re-scalings would give the same intersection. This completes the result. □

In addition to being maximal compact, having chosen a basis so that $K_{v_0} \simeq \mathrm{O}_2 \times \mathrm{O}_n$, if we denote the action of conjugation by $\mathrm{diag}(-1,-1,1,\ldots,1)$ on O_V as σ then we observe that $\mathrm{Stab}_\sigma(\mathrm{O}_V) = K_{v_0}$. We can describe the corresponding action of σ on $\mathrm{Gr}(V) \simeq \mathrm{O}_V / K_{v_0}$ as follows. Suppose the plane v_0 has basis X, Y and that $Z_1, Z_2 \in \{X,Y\}^\perp$, then we have that $\sigma \circ \mathrm{span}\{X+Z_1, Y+Z_2\} = \mathrm{span}\{X-Z_1, Y-Z_2\}$. Under a suitable metric on $\mathrm{Gr}(V)$ such a map would be isometric and so by [Hel01] $\mathrm{Gr}(V) \simeq \mathrm{O}_V / K_{v_0}$ will realize a symmetric space.

Remark. Though this is a simple and useful realization of the space, it is not clear from this construction what the complex structure should be.

The Projective Model - Complex Structure

We consider the complexification $V(\mathbb{C})$ of the space V and the projectivization $P(V(\mathbb{C}))$. We then consider the zero quadric:

$$N := \{[Z] \in P(V(\mathbb{C})) | B(Z,Z) = 0\}.$$

It is a closed algebraic subvariety of the projective space. We now define:

$$\kappa := \{[Z] \in P(V(\mathbb{C})) | B(Z,Z) = 0, B(Z,\overline{Z}) > 0\};$$

κ is a complex manifold of dimension n consisting of 2 connected components.

Remark. One must check that these spaces are in fact well defined, that is that the conditions do not depend on a representative Z. Indeed $B(cZ,cZ) = c^2 B(Z,Z)$ and $B(cZ,\overline{cZ}) = c\bar{c}B(Z,\overline{Z})$.

The assertions about the dimension and connected components is easily seen once we consider the tube domain model later. However one can see that projectivization removes one dimension as does the $B(Z,Z) = 0$ condition. Moreover, the $B(Z,\overline{Z}) > 0$ condition disconnects the space into two components separating Z from $\overline{Z}$ via removing the real points which all satisfy $B(Z,\overline{Z}) = 0$.

Remark. The orthogonal group $\mathrm{O}_V(\mathbb{R})$ acts transitively on κ.

We can reformulate the condition that a given $Z \in V(\mathbb{C})$ will have $[Z] \in \kappa$ by observing that: $B(X+iY, X+iY) = B(X,X) - B(Y,Y) + 2iB(X,Y)$ and $B(X+iY, X-iY) = B(X,X) + B(Y,Y)$. And so the conditions $B(X+iY, X+iY) = 0$ and $B(X+iY, X-iY) > 0$ give us that:

$$[Z] \in \kappa \Leftrightarrow B(X,X) = B(Y,Y) > 0 \text{ and } B(X,Y) = 0.$$

It follows from this then that $\mathrm{O}_V(\mathbb{R})$ will in fact act on κ. To show that it acts transitively observe that we can get a transformation M in $\mathrm{O}_V(\mathbb{R})$ that maps $X \mapsto X'$ and maps $Y \mapsto Y'$ by appealing to Witt's extension theorem. This transformation will then map $[Z]$ to $[Z']$.

Consider the subgroup $\mathrm{O}_V^+(\mathbb{R})$ of elements whose spinor norm equals the determinant. As was discussed in the example following the definition of the spinor norm, this consists of those elements which preserve the orientation of any, and hence all, positive definite planes. Then $\mathrm{O}_V^+(\mathbb{R})$ preserves the 2 components of κ whereas $\mathrm{O}_V \setminus \mathrm{O}_V^+(\mathbb{R})$ interchanges them. To see this, note that any element of $\mathrm{O}_V(\mathbb{R})$ which takes $[X+iY]$ to $[X-iY]$ will have spinor norm not equal to its determinant. This is because it changes the orientation on the positive definite plane generated by X, Y.

Pick one component of κ denote it κ^+. For $Z \in V(\mathbb{C})$ we will write $Z = X + iY$ where $X, Y \in V(\mathbb{R})$.

Lemma 2.3.38. *The assignment $[Z] \mapsto v(Z) := \mathbb{R}X + \mathbb{R}Y$ defines a real analytic isomorphism $\kappa^+ \to \mathrm{Gr}(V)$.*

Proof. The first step is to check that this map is well defined. To see that the assignment gives us a positive definite plane we appeal to the arguments made in the preceeding remark about the conditions for an element to be in κ.

To see that the map does not depend on the choice of representative notice that multiplying a representative $[Z] \in \kappa$ by $\mathbb{C}^*$ just rotates and rescales the resulting plane. Indeed, if we rescale to chose a different representative we find that $(a+ib)(X+iY) = (aX - bY) + i(aY + bX)$ so the result is that we have just changed the basis for the plane.

The next step is to check that the map is surjective. Indeed, the condition for inclusion of elements in κ in the remark was an if and only if condition. Additionally we note that we can pick either $[X+iY]$ or $[Y-iX]$ at least one of which shall be is in κ^+.

Finally we must check analyticity. First remark that since $\mathrm{Gr}(V)$ does not yet have a complex structure we must only show real analycity and then use this to transport a complex structure under which we will then have a complex analytic map.

The mappings $Z \mapsto X$ and $Z \mapsto Y$ are real analytic as maps from $V(\mathbb{C})$ to $V(\mathbb{R})$. From this it follows that outside the region where $aX = bY$ the assignment of the plane generated by X, Y in $\mathrm{Gr}(V)$ is then a real analytic map from $V(\mathbb{C})$ into $\mathrm{Gr}(V)$. The mapping $\kappa \to \mathrm{Gr}(V)$ we have described can be defined by giving a covering of $P(V(\mathbb{C}))$ by affine opens $U_i = \{[z_1, \ldots, z_n] | z_i \neq 0\}$ and taking the analytic section $[z_1, \ldots, z_n] \mapsto (z_1/z_i, \cdots, z_n/z_i)$ into $V(\mathbb{C})$ and composing with this map.

If we wish to show that the inverse map is also real analytic, we must show that our choice of orientation, that was the choice of $[X+iY]$ or $[Y-iX]$ to land in κ^+ can be done analytically. Indeed, by observing that $\mathrm{O}_V^+(\mathbb{R})$ acts transitively on $\mathrm{Gr}(V)$ and real analytically on V it can be used to continuously analytically assign an orientation to each plane, that is, by fixing one plane P and an ordered basis X_0, Y_0 we can for $M \in \mathrm{O}_V^+(\mathbb{R})$ assign the orientation MX_0, MY_0 to MP. $\square$

The "Tube Domain" Model

Pick e_1 a non-zero isotropic vector in V, pick e_2 such that $B(e_1, e_2) = 1$ (note that e_i may not be defined over $\mathbb{Q}$ when $n \leq 4$ though for computations it is useful to when possible pick ones that are). Define $W := V \cap e_2^{\perp} \cap e_1^{\perp}$, we then may express elements of $V(\mathbb{C})$ as (z, a, b), where $z \in W$,$a, b \in \mathbb{C}$ via the decomposition:

$$V = W \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_1.$$

Note that W is a quadratic space of type $(1, n-1)$ ("Lorentzian").

Definition 2.3.39. We define the tube domain $H := \{z \in W(\mathbb{C}) | Q(\Im(z)) > 0\}$. where $\Im(z)$ is the imaginary part of the complex vector z.

Lemma 2.3.40. *The map $\psi : H \to \kappa$ given by:*

$$\psi(z) = [(z, 1, -Q(z) - Q(e_2))]$$

is bi-holomorphic.

Proof. Observing that $Q(ae_1 + be_2) = \frac{1}{2}(B(ae_1, ae_1) + 2B(ae_1, be_2) + B(be_2, be_2)) = ab + b^2 Q(e_2)$ allows us to check that this is well defined. Indeed we have that:

$$Q(z + e_2 + (-Q(z) - Q(e_2))e_1) = Q(z) + Q(e_2) + B(e_2, e_1)(-Q(z) - Q(e_2)) = 0.$$

Additionally:

$$\begin{aligned}
&B(z + e_2 + (-Q(z) - Q(e_2))e_1, \overline{z + e_2 + (-Q(z) - Q(e_2))e_1}) \\
&= B(z + e_2 + (-Q(z) - Q(e_2))e_1, \overline{z} + e_2 + (-Q(\overline{z}) - Q(e_2))e_1) \\
&= B(z, \overline{z}) + 2Q(e_2) + (-Q(z) - Q(e_2)) + (-Q(\overline{z}) - Q(e_2)) \\
&= B(z, \overline{z}) - (1/2)B(z, z) - (1/2)B(\overline{z}, \overline{z}) \\
&= (1/2)(B(z, \overline{z} - z) + B(z - \overline{z}, \overline{z})) \\
&= (1/2)(B(2\Im(z), z) - B(2\Im(z), \overline{z})) \\
&= 2B(\Im(z), \Im(z)) \\
&= Q(\Im(z)) \\
&> 0.
\end{aligned}$$

Given an element $[Z] \in \kappa$ with $Z = X + iY$ the condition that X, Y span a positive definite plane tells us that under the decomposition $V(\mathbb{C}) = W(\mathbb{C}) \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_1$ we have $Z = (z, a, b)$ with $b \neq 0$. We can see this fact by observing first that $W(\mathbb{Q})$ contains no positive definite plane, and so under the decomposition not both a, b are zero. However, since e_1 is isotropic it is an easy check that $W(\mathbb{Q}) \oplus \mathbb{Q}e_1$ also contains no positive definite planes and so we conclude $a \neq 0$. We can thus rescale and write $[Z] = [(z, 1, b)]$. Reversing the above calculations allows us to conclude that $b = -Q(z) - Q(e_2)$ and $Q(\Im(z)) > 0$.

The bi-holomorphicity of the map follows from the fact that in one direction the map is a polynomial mapping $z \mapsto (z, 1, Q(z) - Q(e_2))$. In the reverse direction we may cover $P(V(\mathbb{C}))$ by open affines. one of which, U, is the one corresponding to the requirement that the a component of $[(z, a, b)]$ has $a \neq 0$. The complex structure on such an affine can be defined by the mapping $U \to \mathbb{C}^{n-1}$ given by $[(z, a, b)] \mapsto (z/a, b/a)$ this mapping is then, by definition holomorphic, and

consequently so to is the projection onto z/a. For this appropriate choice of affine covering, $\kappa \subset U$ and consequently this 'projection' is holomorphic on κ. □

H, like κ, has 2 components. This follows from the fact that $W(\mathbb{R})$ is a space of type $(1, n-1)$ and by inspecting the defining conditions. That is Q has the form $Q(x_1, \ldots, x_n) = a_1x_1^2 - a_2x_2^2 - \cdots - a_nx_n^2$ with $a_i > 0$ and the condition is that $Q(\Im(Z)) > 0$ writing $\Im(Z) = (x_1, \ldots, x_n)$ we see that we have 2 components corresponding to the cases $x_1 > 0$ and $x_1 < 0$. Under the map one of these thus corresponds to κ^+ we shall label that one H^+.

It is this H^+ that is the analog of the usual upper half plane, we have an action of $\mathrm{O}_V^+(\mathbb{R})$ acting on it through its action on κ. This action as before is transitive.

The advantage to viewing the symmetric space under this interpretation is that it corresponds far more directly to some of the more classically constructed symmetric spaces. This shall be made more explicit once we construct the correspondence between the classical SL_2 case and the (2,1) case as well as the correspondences of the Hilbert modular surfaces for real quadratic fields to orthogonal groups of signature (2,2).

Discrete Subgroups - Lattices

Let V be a non-degenerate quadratic space over $\mathbb{Q}$ of type $(2, n)$.

Definition 2.3.41. A **lattice** in V is a $\mathbb{Z}$-module L such that $V = L \otimes_{\mathbb{Z}} \mathbb{Q}$. The lattice L is said to be **integral** if $B(x, y) \in \mathbb{Z}\ \forall x, y \in L$. It is moreover called **even** if $Q(x) \in \mathbb{Z}\ \forall x \in L$.

We define the **dual lattice** to be $L^\vee := \{x \in V | B(x, y) \in \mathbb{Z}\ \forall y \in L\}$. Note that L is integral if and only if $L \subset L^\vee$ in which case $L^\vee/L$ is a finite abelian called the **discriminant group**. A lattice is said to be **unimodular** if $|L^\vee/L| = |\det(S)| = 1$ where S is the matrix for Q coming from a lattice basis for L.

The following along with more thorough descriptions and proofs, can be found in Brunier and Frietag "Local Borcherds Products" [BF01].

For the remainder L is an even lattice. Then $\mathrm{O}_L \subset \mathrm{O}_V$ is a discrete subgroup. Let $\Gamma \subset \mathrm{O}_L$ be the subgroup of finite index corresponding to elements which act trivially on $L^\vee/L$ then Γ acts properly discontinuously on $\mathrm{Gr}(V)$ in the sense that every element x of the space has a neighborhood U such that for all $g \in \Gamma$ we have $g(U) \cap U = \{x\}$.

We then consider the space: $Y(\Gamma) := \Gamma \setminus H^+$, it is a normal complex space and is compact if and only if V is anisotropic (recall that this means that Q does not take on the value 0 on $V(\mathbb{Q})$). If it is not compact, it can be compactified by adding rational boundary components. In the κ^+ model the boundary components are precisely the non-trivial isotropic subspaces of $V(\mathbb{R})$. The rational boundary components are those which are defined over $\mathbb{Q}$.

If an isotropic boundary component is a line in $V(\mathbb{R})$ then we call it a special boundary point. If an isotropic boundary component is a plane in $V(\mathbb{R})$ then we shall call it a generic boundary component. We note that by the choice of signature $(2, n)$ all isotropic subspaces have dimension at most 2.

We then define $(\kappa^+)^*$ to be $\kappa^+ \cup \{\text{rational boundary components}\}$.

We have that $\mathrm{O}_V(\mathbb{Q}) \cap \mathrm{O}_V^+(\mathbb{R})$ acts on $(\kappa^+)^*$ and by the theory of Baily-Borel, $X(\Gamma) := (\kappa^+)^*/\Gamma$ together with Baily-Borel topology is a compact hausdorff space which can be given a complex structure. Moreover, using modular forms one can construct an ample line bundle, hence it is projective algebraic.

2.3.4 Modular Forms for O(2,n)

Let $\overline{\kappa}^+ = \{Z \in V(\mathbb{C}) | [Z] \in \kappa^+\}$ be the cone over κ^+.

Definition 2.3.42. Let $k \in \mathbb{Z}$, χ be a character of Γ. A meromorphic function on $\overline{\kappa}^+$ is a **modular form** of weight k and character χ for the group Γ if:

1. F is homogeneous of degree $-k$, i.e. $F(cZ) = c^{-k}F(Z)$ for $c \in \mathbb{C} - \{0\}$.
2. F is invariant under Γ, i.e. $F(gZ) = \chi(g)F(Z)$ for any $g \in \Gamma$.
3. F is meromorphic on the boundary.

If F is holomorphic on $\overline{\kappa}^+$ and on the boundary, we call it a holomorphic modular form.

Remark. The Koecher principle (see for example Freitag "Hilbert Modular Forms" [Fre90]), which says that if the codimension of the cusps is sufficiently large then analyticity at the cusps is automatic, implies condition (3) is automatic if the Witt rank of V (the dimension of maximal isotropic subspace) is less than n, where the dimension of V was $n+2$. Note that for type $(2, n)$ the Witt rank is always at most 2, and will often be less whenever $n \leq 2$.

One should find this definition a bit troubling in that our function F isn't defined as being a function on κ^+ which is largely counter to the usual situation one expects. However, we do have that $H^+ \simeq \kappa^+$ sits quite naturally inside $\overline{\kappa}^+$ in that $H^+ \hookrightarrow V(\mathbb{C})$ via $[Z] \mapsto (z, 1, -Q(z) - Q(e_2))$. It is when we restrict F to H^+ in this way that we can get a function on H^+. We shall denote the function on H constructed in this way as f. Moreover, it is under this interpretation that a factor of automorphy will appear. That is, there is a unique action of $\mathrm{O}_V^+(\mathbb{R})$ on H (denoted by σ_g) so that for each $g \in \mathrm{O}_V^+(\mathbb{R})$ the diagram:

$$\begin{array}{ccc} \kappa^+ & \xrightarrow{[Z]\mapsto[gZ]} & \kappa^+ \\ {\scriptstyle\psi}\uparrow & & \uparrow{\scriptstyle\psi} \\ H^+ & \xrightarrow{\sigma_g} & H^+ \end{array}$$

becomes commutative. We know that:

$$\psi^{-1} \circ g([Z]) = \psi^{-1} \circ g([z, 1, -Q(z) - Q(e_2)]) = \psi^{-1}([z', a', b']) = z'/a'$$

and so:

$$\sigma_g(z) = B(g \circ (z, a, -Q(z) - Q(e_2)), e_1)^{-1} \rho_W(g \circ (z, a, -Q(z) - Q(e_2))).$$

Where ρ_W is the projection onto the W component. We then have that the function $j : \mathrm{O} \times H \to \mathbb{C}$ given by:

$$j(g, z) = B(g \circ (z, a, -Q(z) - Q(e_2)), e_1)$$

defines a factor of automorphy. That is, it satisfies the cocycle condition:

$$j(g_1 g_2, z) = j(g_1, \sigma_{g_2} z) j(g_2, z).$$

When we reinterpret conditions (1) and (2) when viewing F as a function on H we find that F is not invariant under the action of Γ on H through σ. Indeed, for $\gamma \in \Gamma$ we have:

$$\begin{aligned} f(\sigma_\gamma z) &= f(B(\gamma \circ (z, 1, -Q(z) - Q(e_2)), e_1)^{-1} \rho_W(\gamma \circ (z, 1, -Q(z) - Q(e_2)))) \\ &= F(j(\gamma, z)^{-1}(\gamma \circ (z, 1, -Q(z) - Q(e_2)))) \\ &= j(\gamma, z)^k F(\gamma \circ (z, 1, -Q(z) - Q(e_2))) \\ &= j(\gamma, z)^k F((z, 1, -Q(z) - Q(e_2))) \\ &= j(\gamma, z)^k f(z). \end{aligned}$$

Example. The first standard example of modular forms are the Eisenstein series. We will first describe the general construction somewhat vaguely and then explain how this relates to the classical Eisenstein series for SL_2.

The idea is that one first fixes a Borel subgroup $B \subset \mathrm{O}$ (recall that for an orthogonal group the Borel subgroups are those which stabilize a maximal isotropic flag in V) or more generally one can fix a parabolic subgroup $P \subset \mathrm{O}$ (that is a proper subgroup containing a Borel subgroup). One then fixes a function Φ that will be invariant under the action of P. One then averages this function over $(P \cap \mathrm{O}_L) \backslash \mathrm{O}_L$ (remark here that we are using the discrete subgroup O_L and not the full group). What we arrive at is the formula:

$$f(z) = \sum_{\gamma \in (P \cap \mathrm{O}_L) \backslash \mathrm{O}_L} j(\gamma, z)^{-k} \Phi(\gamma z).$$

If we ignore issues of absolute convergence then it is an easy check that under the action of O_L on this function we would pull out the factor of automorphy to the k^{th} power and rearrange the summation. Consequently if we do have absolute and uniform convergence on a sufficiently nice neighborhood then this would define a modular form.

In the classical SL_2 case, one can use the Borel subgroup of upper triangular matrices, that is $\{\left(\begin{smallmatrix} a & t \\ 0 & a^{-1} \end{smallmatrix}\right)\}$. One then considers the function Φ to be the constant function 1. The observation that an element $\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ can be written uniquely as a product:

$$\begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & c^{-1} \\ -c & d \end{pmatrix}$$

allows us to write the sum:

$$\sum_{\gamma \in (B \cap \mathrm{O}_L) \backslash \mathrm{O}_L} j(\gamma, z)^{-k} \Phi(\gamma z) = \sum_{(c,d)} (cz + d)^{-k}$$

which recovers the classical weight k Eisenstein series. Remark in particular though that for $k = 2$ this does not converge absolutely, and it turns out that consequently this case does not give a modular form.

Borcherds Products

The next construction of modular forms for these orthogonal spaces comes out of fairly recent results of Borcherds. For details on the theory see R. Borcherds' article "Automorphic forms on $O_{s+2,2}(\mathrm{R})$ and infinite products" [Bor95] or J. Brunier's article and book "Infinite Products in Number Theory and Geometry" [Bru04] and "Borcherds Products on O(2,l) and Chern classes of Heegner divisors" [Bru02].

A **nearly holomorphic** modular form for $\mathrm{SL}_2(\mathbb{Z})$ is a holomorphic function on the upper half plane, with the usual transformation behavior but with the relaxed requirement that the function may have a pole of finite order at the cusp. Such a function f has a fourier expansion at the cusp at infinity of the form:

$$f(q) = \sum_{n > n_0 > -\infty} c(n) q^n.$$

The non-holomorphic part of the fourier expansion:

$$\sum_{0 > n > n_0} c_n q^n$$

is called the principal part.

On $\Gamma\backslash \mathrm{O}_V(\mathbb{R})/K(\mathbb{R})$ there is a notion of certain special divisors, 'Heegner divisors', these arise through the embedding of sub-orthogonal groups of type (2,$n-1$) (where O_V has type (2,n)) into O_V.

Borcherds discovered a lifting from nearly holomorphic modular forms of weight $1-n/2$ to meromorphic modular forms on orthogonal spaces of type (2,n).

Suppose $L \subset V$ is an even unimodular lattice. Let $K = L \cap W$ where $V(\mathbb{C}) = W \oplus \mathbb{C}e_1 \oplus \mathbb{C}e_2$ as in the construction of the tube domain model. For a function f as above, we consider the product:

$$\Psi(Z) = e^{B(\varrho_f(M),Z)} \prod_{\substack{\lambda \in K \\ B(\lambda,M)>0}} \left(1 - e^{B(\lambda,Z)}\right)^{c(Q(\lambda))}$$

where $\varrho_f(M) \in K \otimes \mathbb{Q}$ is a Weyl vector (see [Bru02, 3.5] for a definition of this). The variable Z is taken to be in the orthogonal upper half space H.

Theorem 2.3.43. *(Borcherds) [Bru04] Let f be a nearly holomorphic modular form for $\mathrm{SL}_2(\mathbb{Z})$ whose fourier expansion is as above and whose principal part has integral coefficients. Then the product $\Psi(Z)$ converges for $\Im(Z)$ sufficiently large, and $\Psi(Z)$ can be continued to a meromorphic function of the symmetric space H associated to O_V. Moreover, this function satisfies the following:*

1. *The function is a meromorphic modular form for O_L with a finite multiplier system.*
2. *The weight of Ψ is $c(0)/2$.*
3. *The divisor of Ψ is determined explicitly by the principal part of f.*

Remark. It should be remarked that the construction of this lifting can be realized as a regularized theta lift via the dual reductive pairing of $\mathrm{SL}_2 \simeq \mathrm{Sp}_2$ and $\mathrm{O}_{2,n}$ (see [Bru02] for details on this).

Example. We now briefly present a few examples of this lifting.

- Consider the weight 1/2 Jacobi theta series give by $12\theta(q) = 12\sum_{n\in\mathbb{Z}} q^{n^2}$. By the theorem this lifts to the modular form:
$$\Delta(q) = q\prod_{n>0}(1-q^n)^{24}$$
for an orthogonal group of type (2,1). Once we have seen that the (2,1) case corresponds to the classical upper half space we see that we recover the classic weight 12 cusp form Δ.
- For the next example we consider the j function, that is $j = \frac{E_4^3}{\Delta}$ where E_4 is the normalized weight 4 Eisenstein series. Consider now $J := j - 724$. Since J has weight 0 it lifts to a modular form on an orthogonal group of type (2,2). It turns out that under the isomorphism between this space and $\mathbb{H}\times\mathbb{H}$ (that we shall see shortly) this lifting gives us the modular function $j(z_1) - j(z_2)$ which then has q-expansion:
$$q_1^{-1}\prod_{\substack{m>0 \\ n\in\mathbb{Z}}}(1-q_1^m q_2^n)^{c(mn)}$$
where $c(mn)$ gives us the fourier coefficients of the function J.
- It can be shown that E_k for $k = 4, 6, 8, 10, 14$ are Borcherds lifts of certain half integral weight modular forms.

2.3.5 The Isomorphism of O(2,1) and SL_2

It turns out, that as a consequence of some exceptional isomorphisms between Lie groups in low dimension that there is an isomorphism between SL_2 and Spin_V where V is a quadratic space of type (2,1). We wish now to present this isomorphism.

Consider the vector space V of traceless matrices in M_2. That is $V = \{\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)\}$. The determinant then defines a quadratic form on V of type (2,1). SL_2 acts on V through conjugation and this action preserves the determinant and hence the quadratic form. The kernel of the map is $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and one can check that the images all have determinant 1 and thus lie in $\mathrm{SO}(2,1)$. Hence this gives us a map of SL_2 to $\mathrm{SO}(2,1)$. By connectedness and for dimension reasons we see that this map is surjective. Moreover, in this case we know that the even Clifford algebra C_V^0 is a quaternion algebra and we can check that it is split, thus $\mathrm{C}_V^0 \simeq \mathrm{M}_2$. Consequently since the Clifford norm is the determinant we have that $\mathrm{Spin}_V \simeq \mathrm{SL}_2$.

Consider the basis for V given by:

$$v = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \qquad e_1 = \left(\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}\right) \qquad e_2 = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right).$$

The action of Spin_V on V is through conjugation. Computing what this means on $\overline{\kappa}^+$ we have that for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2$ and $(z, 1, z^2) \in \overline{\kappa}^+$ we get:

$$\begin{aligned}
\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \circ (z, 1, -z^2) &= \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \left(\begin{smallmatrix} z & -z^2 \\ 1 & -z \end{smallmatrix}\right) \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) \\
&= \left(\begin{smallmatrix} az+b & -az^2-bz \\ cz+d & -cz^2-dz \end{smallmatrix}\right) \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) \\
&= \left(\begin{smallmatrix} adz+bd+acz^2+bcz & -abz-b^2-a^2z^2-abz \\ cdz+d^2+c^2z^2+cdz & -cbz-db-acz^2-adz \end{smallmatrix}\right) \\
&= (cz+d)^2 \left(\begin{smallmatrix} \frac{az+b}{cz+d} & -(\frac{az+b}{cz+d})^2 \\ 1 & -\frac{az+b}{cz+d} \end{smallmatrix}\right).
\end{aligned}$$

Consequently then the action on H is given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \circ z = \frac{az+b}{cz+d}$. However we notice that the factor of automorphy is now $(cz+d)^2$ rather than the usual $(cz+d)$. This means that our notion of weight is off by a multiple of 2 from the classical case (That there are no classical modular forms of odd weight and trivial character is perhaps reassuring).

2.3.6 The Isomorphism of O(2,2) and the Hilbert Modular Space

We would now like to explain how the exceptional isomorphism of $\mathrm{SL}_2 \times \mathrm{SL}_2 \simeq \mathrm{Spin}_4$ relates to the isomorphism of Hilbert modular spaces for real quadratic fields and with spaces of type (2,2).

We recall quickly the definitions for the Hilbert modular space in the real quadratic case. Let $F/\mathbb{Q}$ be the real quadratic field $F = \mathbb{Q}(\sqrt{d})$, where $d > 0$ and square free. Let a' denote the conjugate of a in F. The Hilbert modular space is $\mathbb{H} \times \mathbb{H}$ together with the diagonal action of $\mathrm{SL}_2(F)$ via fractional linear transformation on each component via the two distinct embeddings of $F \hookrightarrow \mathbb{C}$. A Hilbert modular form of (parallel) weight k is a holomorphic function $f : \mathbb{H} \times \mathbb{H} \to \mathbb{C}$ satisfying holomorphicity conditions as well as modularity with respect to the action of $\mathrm{SL}_2(\mathcal{O}_F)$. That is:

$$f\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \circ (z_1, z_2)\right) := f\left(\frac{az_1+b}{cz_1+d}, \frac{a'z_2+b'}{c'z_2+d'}\right) = (cz_1+d)^k (c'z_2+d')^k f(z_1, z_2), \ \forall \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_F).$$

What we wish to do now, is to show that these spaces can be realized as a special case of the previous construction for certain quadratic forms of signature (2,2).

As above, let $F/\mathbb{Q}$ be the real quadratic field $F = \mathbb{Q}(\sqrt{d})$. Consider the 4-dimensional $\mathbb{Q}$ vector space $\mathbb{Q} \oplus \mathbb{Q} \oplus F$, with the quadratic form given by:

$$Q(a, b, x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) - ab.$$

Then V is a rational quadratic space of type (2,2) so all of the proceeding constructions apply.

We consider the basis $v_1 = (1,1,0)$, $v_2 = (1,-1,0)$, $v_3 = (0,0,1)$, $v_4 = (0,0,\sqrt{d})$. We then have (as in the notation of Clifford algebras) that $\delta^2 = d$ and so $Z := Z(\mathrm{C}_V^0) = \mathbb{Q} + \mathbb{Q}\delta \simeq F$ and moreover $\mathrm{C}_V^0 = Z + Zv_1v_2 + Zv_2v_3 + Zv_1v_3$ is isomorphic to the split quaternion algebra $\mathrm{M}_2(F)$. The isomorphism is obtained by linearly extending the mapping:

$$1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \quad v_1v_2 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \quad v_2v_3 \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \quad v_1v_3 \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right).$$

The canonical involution in C_V^0 is given by: $* : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^* = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.
The Clifford norm is given by the determinant: $N : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto ad - bc$.

We thus have that $\mathrm{Spin}_V \cong \mathrm{SL}_2(F) \cong R_{F/\mathbb{Q}}(\mathrm{SL}_2)$. Thus $\Gamma_F = \mathrm{SL}_2(\mathcal{O}_F)$ is an arithmetic subgroup of Spin_V. In fact, one can show that $\Gamma_F = \mathrm{Spin}_L$ where L is the lattice $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathcal{O}_F \subset V$.

We now explicitly describe the vector representation (that is, how does Spin_V act on V). let $\sigma : x \mapsto v_1 x v_1^{-1}$ be $\mathrm{Ad}(v_1)$. Then $\delta^\sigma = -\delta$ and so σ agrees with conjugation on F when acting on the center of C_V^0. On $\mathrm{M}_2(F)$ the action is expressed as:

$$\sigma : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^\sigma = \left(\begin{smallmatrix} d' & -c' \\ -b' & a' \end{smallmatrix}\right).$$

Let $\overline{V} = \{X \in \mathrm{M}_2(F) | X^* = X^\sigma\} = \{X \in \mathrm{M}_2(F) |\ {}^tX = X'\} = \left\{\left(\begin{smallmatrix} a & v' \\ v & b \end{smallmatrix}\right) \mid a, b \in \mathbb{Q}, v \in F\right\}$, Where the quadratic and bilinear forms are given by:

$$\overline{Q}(X) = -\det(X) \text{ and } \overline{B}(X,Y) = -tr(XY^*).$$

Moreover, we see that $\mathrm{Spin}_V \cong \mathrm{SL}_2(F)$ acts on $\overline{V}$ via $g \circ X = gXg^{-\sigma} = gX({}^tg')$. We observe in particular that V is isometric to $\overline{V}$ with compatible action of Spin_V. So from now on we work with $\overline{V}$. We next notice that we have: $\overline{V}(\mathbb{C}) = \mathrm{M}_2(\mathbb{C})$ (that is the entire algebra and not a sub-algebra) and so:

$$\kappa = \{[Z] \in P(\mathrm{M}_2(\mathbb{C})) | \det(Z) = 0, -tr(Z\overline{Z}^*) > 0\}.$$

Take $e_1 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $e_2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Observe that we have $Q(e_1) = 0$ and $B(e_1, e_2) = 1$ as in the construction of H. As before we set $W = \overline{V} \cap e_1^\perp \cap e_2^\perp$. Noting that $B\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), e_1\right) = d$ and $B\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), e_2\right) = -a$ we conclude that $W = \{\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) \in V\}$. From this we see that $W(\mathbb{C}) \cong \mathbb{C}^2$ and $H \cong \{(z_1, z_2) \in \mathbb{C}^2 | \operatorname{im}(z_1 z_2) > 0\}$.

We now define the map $M : H \to \kappa$. For $z = (z_1, z_2) \in H$ we define:

$$M(z) := \begin{pmatrix} z_1 z_2 & z_1 \\ z_2 & 1 \end{pmatrix}.$$

This corresponds to the map $H \to \kappa$ from before. If we choose for H^+ the component where $\operatorname{im}(z_1), \operatorname{im}(z_2) > 0$ then it is immediately clear we have an isomorphism $\mathbb{H}^2 \cong H^+ \cong \kappa^+$. This map commutes with the action of $\mathrm{SL}_2(F)$ where the action on κ^+ is given as before (that is through $\mathrm{Spin}_V \cong \mathrm{SL}_2(F)$). In particular, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(F)$ acts on $M(z) \in \kappa^+$ as:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z_1 z_2 & z_1 \\ z_2 & 1 \end{pmatrix} \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \begin{pmatrix} (az_1z_2 + bz_2)a' + (az_1 + b)b' & (az_1z_2 + bz_2)c' + (az_1 + b)d' \\ (cz_1z_2 + dz_2)a' + (cz_1 + d)c' & (cz_1z_2 + dz_2)c' + (cz_1 + d)d' \end{pmatrix}$$

and acts on H as:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ (z_1, z_2) = \left(\frac{az_1 + b}{cz_1 + d}, \frac{a'z_2 + b'}{c'z_2 + d'}\right).$$

Applying M gives:

$$\begin{pmatrix} \frac{az_1+b}{cz_1+d}\frac{a'z_2+b'}{c'z_2+d'} & \frac{az_1+b}{cz_1+d} \\ \frac{a'z_2+b'}{c'z_2+d'} & 1 \end{pmatrix} = N(cz+d)\begin{pmatrix} (az_1+b)(a'z_2+b') & (az_1+b)(c'z_2+d') \\ (a'z_2+b')(cz_1+d) & (cz_1+d)(c'z_2+d') \end{pmatrix}.$$

In particular this shows that $\gamma M(z) = N(cz+d)M(\gamma z)$. Moreover, we see that for parallel weight modular forms, our definitions agree.

CHAPTER 3
Tori and Galois Cohomology

When we looked at the Grassmannian model of the symmetric space we saw that maximal compact subgroups came from stabilizers of points of the Grassmannian. Moreover, we saw that the stabilizers of positive definite planes were isomorphic (over $\mathbb{R}$) to $\mathrm{O}_2 \times \mathrm{O}_n$. Conversely, if we have a subgroup of the orthogonal group isomorphic to $O_{V_2} \times O_{V_n}$, where V_i is some i dimensional quadratic space, it will stabilize some plane. The plane however may not in general be positive definite. However, we have seen the statement that $\mathrm{O}_{V_i}(\mathbb{R})$ is compact is equivalent to the statement that the quadratic form is definite. Consequently, if we require a compact set of real points, this will correspond to a positive definite plane in the space.

By virtue of the fact that $\mathrm{O}_2 \times \mathrm{O}_n$ contains maximal $\mathbb{R}$-compact tori and that stabilizers of points in $\mathrm{Gr}(V)$ are $\mathbb{R}$ conjugates of these, we have that any point in the Grassmannian model is stabilized by a torus whose $\mathbb{R}$ points are compact, and vice-versa, any torus whose $\mathbb{R}$ points are compact is contained in the stabilizer of a point on the Grassmannian. What makes the points we are interested in special is that one expects algebraicity results concerning the values of modular forms or related functions at these points. In order to hope to get these results the criterion we add is that the torus be defined over $\mathbb{Q}$.

These above facts contribute to the reasons that the points we are interested in are those points x which satisfy $\exists\, T \subset \mathrm{Stab}_x$ such that T is a maximal algebraic torus in O_q, is defined over $\mathbb{Q}$. It is a consequence of the fact that $T(\mathbb{R})$ lies in the $\mathbb{R}$-compact set Stab_x that $T(\mathbb{R})$ will be $\mathbb{R}$-compact.

In the case of the usual upper half plane viewed via the isomorphism to the $(2,1)$ case, one finds that the points satisfying the above correspond to the quadratic imaginary points in the upper half plane. To see this consider $\tau = x + iy \in \mathbb{H}$ and suppose $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Q})$ stabilizes τ. We then have that:

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \circ \tau = \frac{a\tau + b}{c\tau + d} = \tau.$$

Then, provided $c \neq 0$ we have τ satisfies a quadratic equation over $\mathbb{Q}$. In the case $c = 0$ then either $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\tau \in \mathbb{Q}$ which was not allowed. We now claim that any maximal rational torus in SL_2 has rational points other than $\pm id$. Indeed, by 2.1.8 we have that one dimensional tori correspond to $\mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \{\pm 1\})$. But picking such a homomorphism corresponds to picking a quadratic extension L of $\mathbb{Q}$, and the corresponding torus is then isomorphic to $R_{L/\mathbb{Q}}(\mathbb{G}_m)$. All of these tori have infinitely many rational points.

Conversely, if we consider the the quadratic imaginary point $\tau = y\sqrt{-D}$ we see that it is fixed by the torus $T = \{\left(\begin{smallmatrix} a & -y^2 Db \\ b & a \end{smallmatrix}\right) \mid a^2 + y^2 Db^2 = 1\}$, the point $\tau = x + y\sqrt{-D}$ is then fixed by the torus $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) T \left(\begin{smallmatrix} 1 & -x \\ 0 & 1 \end{smallmatrix}\right)$.

In the Hilbert modular case (the (2,2) case) the CM-points can be seen to correspond to 'quadratic imaginary' points as well. However, in this case, they will be quadratic imaginary over the real quadratic field used to construct the Hilbert modular surface.

In both the (2,1) and (2,2) cases these points are the subject of rather spectacular phenomenon related to the fields in which the results of evaluating modular forms at these points lie. Specifically,

there is a relation to class field theory in that the values are associated to the Hilbert class field of the quadratic imaginary field.

It is our goal to study these points for general orthogonal groups of type (2,l) with the eventual goal of evaluating modular forms at these points and of observing similar phenomenon, making use of Shimura's reciprocity law.

3.1 Galois Cohomology of Algebraic Groups

Most of the material in this section can be found in J.P Serre "Galois Cohomology" [Ser02] and "Local Fields" [Ser79] as well as numerous other sources.

We intend to treat several cases simultaneously, so in the following consider Γ to be a group, and M to be either a $\mathbb{Z}[\Gamma]$-module or a group acted upon by Γ via homomorphisms (or a Γ-set). The first case corresponds to abelian Galois cohomology and the second is the non-abelian case.

Let $C^n(\Gamma, M)$ be the group (or pointed set) of all functions $f : \Gamma^n \to M$.

We define the coboundary maps $d^n : C^n(\Gamma, M) \to C^{n+1}(\Gamma, M)$ via:

$$d^n(\phi)(x_0, \ldots, x_n) = x_0\phi(x_1, \ldots, x_n) + \sum_{i=0}^{n-1}(-1)^{i+1}\phi(x_0, \ldots, x_{i-1}x_i, \ldots, x_n) + (-1)^{n+1}\phi(x_0, \ldots, x_{n-1}).$$

The important property of the function d^n is that $d^{n+1} \circ d^n = 0$. We then define: $Z^n(\Gamma, M) := \mathrm{Ker}(d^n)$ and $B^n(\Gamma, M) := \mathrm{im}(d^{n-1})$ (or $\{0\}$ if $n = 0$). Finally:

$$H^n(\Gamma, M) := Z^n(\Gamma, M)/B^n(\Gamma, M).$$

We note that this definition doesn't always make sense, in particular in the case of a Γ-set only $H^0(\Gamma, M)$ makes sense, and in the case of M a non-abelian group things become ill-defined for $n > 1$ (and for the $n = 1$ case the definition would better be phrased using multiplicative notation).

In the case of a non-abelian group M, what we end up with is the following:

$$\begin{aligned}
&B^0(\Gamma, M) = \{0\}\\
&Z^0(\Gamma, M) = \{m \in M |\ {}^\sigma m = m\ \forall \sigma \in \Gamma\} = M^\Gamma\\
&H^0(\Gamma, M) = \{m \in M |\ {}^\sigma m = m\ \forall \sigma \in \Gamma\} = M^\Gamma\\
&B^1(\Gamma, M) = \{\phi_m |\ \phi_m(\sigma) = m^{-1}({}^\sigma m),\ m \in M\}\\
&Z^1(\Gamma, M) = \{\xi |\ \xi_\sigma := \xi(\sigma),\ \xi_{\sigma\tau} = \xi_\sigma {}^\sigma\xi_\tau\ \forall \sigma, \tau \in \Gamma\}\\
&H^1(\Gamma, M) = \{\xi \in Z^1(\Gamma, G)\}/\{\xi \sim \xi' \Leftrightarrow \exists m \in M \text{ such that } \xi_\sigma = m^{-1}\xi'_\sigma {}^\sigma m\ \forall \sigma \in \Gamma\}
\end{aligned}$$

In the cases we are most interested in, Γ will be a topological group (for example a Galois group) and M will be an algebraic group. In this case, we add the requirement that the action of Γ be continuous (with the topology on M being the discrete topology) and that the functions defining the cohomology also be continuous.

One of the important results of this construction is that if we have an exact sequence of objects on which Γ acts appropriately,

$$0 \to A \to B \to C \to 0,$$

then we get a long exact sequence:

$$0 \to H^0(\Gamma, A) \to H^0(\Gamma, B) \to H^0(\Gamma, C) \xrightarrow{\delta_0} H^1(\Gamma, A) \to H^1(\Gamma, B) \to H^1(\Gamma, C) \xrightarrow{\delta_1} H^2(\Gamma, A) \cdots$$

which continues for as long as the terms involved are defined. In particular it stops early if $H^2(\Gamma, A)$ does not exist because A is not an abelian group. (And is only an exact sequence of pointed sets.)

One constructs the connecting homomorphisms using the snake lemma, concretely it goes as follows:

We are given $[\rho : \Gamma^n \to C] \in H^n(\Gamma, C)$, We let $\overline{\rho} : \Gamma^n \to B$ be any lifting of ρ coming from the surjectivity of $B \to C$. We now set $\varrho := d^n(\overline{\rho}) : \Gamma^{n+1} \to B$. We now have $[\varrho] \in H^{n+1}(\Gamma, B)$ (one should check that $[\varrho]$ does not depend on choice of lifting) and moreover it will be in $\mathrm{Ker}(H^{n+1}(\Gamma, B) \to H^{n+1}(\Gamma, C))$. It follows (once one proves exactness at the middle terms) that we can lift this to an element of $H^{n+1}(\Gamma, A)$. The added complexity of continuous cohomology is that in order for this to make sense we need to end up with continuous cocycles, this is equivalent to requiring that there exists a continuous section from $C \to B$. (which for our purposes we always have).

Classification of Forms

One common use for cohomology is to allow us to classify the various "forms" of an object. That is to say, two objects, M, M' in some category $\mathcal{C}$, may not be isomorphic. However, there may exist a "Γ-extension" $\mathcal{C}_\Gamma$ of the category to which M, M' belong in which they are isomorphic. We might then call these objects "$\mathcal{C}_\Gamma$-Forms". It turns out that one often has that "$\mathcal{C}_\Gamma$-forms" of M are classified by $H^1(\Gamma, \mathrm{Aut}(M))$. One useful construction for this purpose is the concept of a twisted object. Let Γ be a group, M a Γ-module. Now, let $\xi \in H^1(\Gamma, \mathrm{Aut}(M))$ we can define M twisted by ξ to be ${}_\xi M := M$ except we replace the usual action of Γ on M with a new one. In particular for $\tau \in \Gamma$ if we denote the action on M (respectively ${}_\xi M$) by τ_M (respectively $\tau_{{}_\xi M}$) we have the formula:

$$\tau_{{}_\xi M}(a) = \xi_\tau(\tau_M(a)).$$

To see this is a group action we observe that:

$$\tau_{{}_\xi M} \circ \sigma_{{}_\xi M}(a) = \xi_\tau(\tau_M(\xi_\sigma(\sigma_M(a)))) = \xi_\tau({}^\tau\xi_\sigma(\tau_M(\sigma_M(a)))) = \xi_{\tau\sigma}((\tau\sigma)_M(a)) = (\tau\sigma)_{{}_\xi M}(a).$$

This construction is useful for allowing $H^1(\Gamma, \mathrm{Aut}(M))$ to classify the forms of M. In general one would want to show that whatever sort of object M is, so too is ${}_\xi M$. For example, if we consider the case $\Gamma = \mathrm{Gal}(\overline{k}/k)$, $M = G$ an algebraic group, then we would like ${}_\xi M$ to also be an algebraic group, This requires some work in general (we actually do this for tori later). Assuming this has been done, one then gets that ${}_\xi M$ will be a "Form" of M. In particular, they shall be isomorphic in the category where we allow the additional morphisms corresponding to this twisting.

With the vaguely defined terms of "form", "extension" as above, it may seem obvious that this construction will always give all the possible forms (as we have seemed to define "forms" as those things you get from twisting by H^1). The real work arises when one specifies first the definition of the categories, extensions and forms and then tries to show that they correspond to some particular Γ.

Typically, we have been (and will be) working with the category of algebraic groups defined over k. The extensions of the category we are working with corresponds to algebraic groups over L, a Galois extension of k. We would like to say (in terms of the vague language above) that this is a $\mathrm{Gal}(L/k)$ extension of the category and thus that the L/k-forms of an algebraic group G are classified by $H^1(\mathrm{Gal}(L/k), \mathrm{Aut}(G))$.

One important tool in the proof that this makes sense is Hilbert's Theorem 90. An important part of the proof of which is the following lemma:

Lemma 3.1.1 (Independence of Characters)**.** *[Hun80, V.7.5] If $S \subset \mathrm{Aut}(F)$ is a set of distinct automorphisms of a field F, then S is linearly independent in that if we have for any a_i in any integral domain containing F that $\sum_{i=1}^{n} a_i \sigma_i(u) = 0$ for all $u \in F$ then $a_i = 0$ for all i.*

Proof. Suppose $\sum_{i=1}^{n} a_i \sigma_i(u)$ is a minimal counterexample. Pick $v \in F$ such that $\sigma_1(v) \neq \sigma_2(v)$. Then we have:

$$\sum_{i=1}^{n} a_i \sigma_i(uv) = 0$$

and

$$\sigma_1(v) \sum_{i=1}^{n} a_i \sigma_i(u) = 0.$$

The difference of these equations then gives a smaller counterexample. □

Remark. One should note that the proof as above goes through almost completely unchanged if we replace $\mathrm{Aut}(F)$ by $\mathrm{End}(F^*)$ or $\mathrm{Hom}(F^*, \mathbb{C}^*)$.

We now give Hilbert's Theorem 90.

Theorem 3.1.2 (Hilbert's Theorem 90)**.** *Let L/k be a Galois extension, then:*

$$H^1(\mathrm{Gal}(L/k), \mathrm{GL}_n(L)) = 1.$$

Proof. We follow [Ser79].

Let $[\alpha] \in H^1(\mathrm{Gal}(L/k), \mathrm{GL}_n(L))$ consider the map $L_\alpha : L^n \to L^n$ given by:

$$L_\alpha(f) = \sum_{\sigma \in \mathrm{Gal}(L/k)} \alpha(\sigma)\sigma(f),$$

where we view L^n as column vectors.

Observe that $\tau(L_\alpha(f)) = \alpha(\tau)^{-1} L_\alpha(f)$. We claim that the image of L_α contains a basis for L^n. If not, then there is a non-zero linear map on $\lambda : L^n \to L$ such that $\lambda(L_\alpha(v)) = 0 \ \forall v \in L^n$. But we can then compute that for any fixed v and for all $f \in L$ we have:

$$0 = \lambda(L_\alpha(fv)) = \sum_{\sigma} \lambda(\alpha(\sigma)\sigma(f)\sigma(v)) = \sum_{\sigma} \sigma(f)\lambda(\alpha(\sigma)\sigma(v)).$$

Then, by linear independence of the $\sigma(f)$ we find that for any fixed v and for all σ we have that $\lambda(\alpha(\sigma)\sigma(v)) = 0$. Using that $\alpha(\sigma)$ is invertible this then implies $\lambda = 0$ which is a contradiction.

We can thus choose a basis $v_i = L_\alpha(x_i)$ for L^n. The map which sends $e_i \to v_i$ corresponds to some matrix $M \in \mathrm{GL}_n(L)$. Moveover, we can by checking the behavior on the columns of M see that:

$$\tau(M) = \tau\left(L_a(x_i)\right)_j = \alpha(\tau)^{-1}\left(L_a(x_i)\right)_j = \alpha(\tau)^{-1} M.$$

From which it follows that $\alpha(\tau) = M\tau(M^{-1})$ is a coboundary which completes the result. □

Example. As a particular example of this classification at work, we consider the isomorphism classes of rank n algebraic tori defined over k, split over a finite Galois extension L of k. Fix T a k-split torus ($T := \mathbb{G}_m^n$). We then expect to have that the forms of T, which become isomorphic to it over L, are classified (up to k-isomorphism) by $H^1(\mathrm{Gal}(L/k), \mathrm{Aut}(T))$. But we have from

equivalence of categories for diagonalizable groups (Theorem 2.1.8) that:

$$H^1(\mathrm{Gal}(L/k), \mathrm{Aut}(T)) \simeq H^1(\mathrm{Gal}(L/k), \mathrm{Aut}(X^*(T))).$$

Furthermore, from the description of the character module:

$$H^1(\mathrm{Gal}(L/k), \mathrm{Aut}(X^*(T))) \simeq H^1(\mathrm{Gal}(L/k), \mathrm{GL}_n(\mathbb{Z})).$$

On the other hand, since the action of $\mathrm{Gal}(L/k)$ is trivial:

$$H^1(\mathrm{Gal}(L/k), \mathrm{GL}_n(\mathbb{Z})) \simeq \mathrm{Hom}(\mathrm{Gal}(L/k), \mathrm{GL}_n(\mathbb{Z})).$$

But $\mathrm{Hom}(\mathrm{Gal}(L/k), \mathrm{GL}_n(\mathbb{Z}))$ precisely classifies all the possible Galois module structures of $\mathbb{Z}^n$. In particular via the equivalence of categories (Theorem 2.1.8) this does classify tori. Consequently we see that $H^1(\mathrm{Gal}(L/k), \mathrm{Aut}(T))$ classifies the tori we were interested in.

3.2 Classification of Maximal Tori over k in G

Let k be a perfect field. We have the goal of trying to classify the k-defined maximal algebraic tori in a given algebraic group over k. We know that at least one exists and that they are all conjugate over $\overline{k}$. As such, we first develop some tools for dealing with conjugates of k-defined subgroups.

Proposition 3.2.1 (Criteria for Field of Definition)**.** *Let G be an algebraic group over k, $H \subseteq G$ a subgroup defined over k. For $g \in G$, the subgroup gHg^{-1} is defined over k if and only if $g^{-1}\sigma(g) \in N_G(H), \forall \sigma \in \mathrm{Gal}(\overline{k}/k)$.*

Proof. Suppose first that both H and gHg^{-1} are defined over k. Then for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we get:

$$gHg^{-1} = \sigma(gHg^{-1}) = \sigma(g)\sigma(H)\sigma(g^{-1}) = \sigma(g)H\sigma(g^{-1}).$$

Rearranging then yields $H = g^{-1}\sigma(g)H\sigma(g^{-1})g$ and so then we get: $g^{-1}\sigma(g) \in N_G(H)$.

For the converse we have that: $\forall \sigma \in \mathrm{Gal}(\overline{k}/k), g^{-1}\sigma(g) \in N_G(H)$, thus $H = g^{-1}\sigma(g)H\sigma(g^{-1})g$. Rearranging and applying $H = \sigma(H)$ gives that for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we get:

$$gHg^{-1} = \sigma(g)H\sigma(g^{-1}) = \sigma(gHg^{-1}).$$

And so by Theorem 2.1.4 we have that gHg^{-1} is defined over k. □

Before proceeding with the next few results we would like to introduce and explain some notation. for $H \subseteq G$ and $g \in G$ we make the following notation:

$H_g := gHg^{-1}$

$g_\sigma := [\sigma \mapsto g^{-1}\sigma(g)] \in H^1(\mathrm{Gal}(\overline{k}/k), H)$ where $g^{-1}\sigma(g) \in H \subseteq G$ for each σ (though H need not contain g). That g_σ actually gives a cocycle follows from the following computation:

$$g_{\tau\sigma} = g^{-1}(\tau\sigma(g)) = g^{-1}\tau(gg^{-1}\sigma(g)) = g^{-1}\tau(g)\tau(g^{-1}\sigma(g)) = g_\tau{}^\tau g_\sigma.$$

Through abuse of notation we may view g_σ as being in $H^1(\mathrm{Gal}(\overline{k}/k), H)$ for more than one H; we shall always make it clear in which cohomology any expression involving a cocycle takes place.

More generally, for $[\xi] \in H^1(\mathrm{Gal}(\overline{k}/k), M)$ we shall often drop the [ ]. Moreover, we shall denote $\xi_\sigma = \xi(\sigma) \in M$. By Hilbert's Theorem 90 for GL_n, we know that for any $H' \subseteq \mathrm{GL}_n(\overline{k})$ and any $[\xi] \in H^1(\mathrm{Gal}(\overline{k}/k), H')$ we can write $[\xi_\sigma] = [g^{-1}\sigma(g)]$ for some $g \in \mathrm{GL}_n(\overline{k})$. Consequently, $[\xi_\sigma] = g_\sigma$ and so by taking $\xi = g$ we remove the ambiguity in the notation.

We shall generally use Latin characters $g_\sigma, f_\sigma, \cdots$ when it is clear that f, g come from some G. We shall generally use Greek characters $\xi_\sigma, \cdots$ when the cocycles are not from some algebraic group.

Corollary 3.2.2 (Classification of Forms)**.** *Let $H \subseteq G$ be as before, then we get a map:*

$$\{H_g | g \in G(\overline{k}), H_g \text{ defined over } k\} \xrightarrow{\phi} H^1(\mathrm{Gal}(\overline{k}/k), N_G(H))$$
$$\phi\colon H_g \longmapsto g_\sigma.$$

Proof of Corollary. The only thing to check is that this map is well defined, We already know that g_σ is a cocycle in the appropriate group, so it remains only to check that: $H_g = H_f \Rightarrow g_\sigma = f_\sigma$ in $H^1(\mathrm{Gal}(\overline{k}/k), N_G(H))$. Indeed, the following proves slightly more.

Lemma 3.2.3. *Let H, G be as above and let $f, g \in G$ then $\exists r \in G(k)$ such that $H_g = H_{rf}$ if and only if $g_\sigma = f_\sigma$ in $H^1(\mathrm{Gal}(\overline{k}/k), N_G(H))$.*

Proof of Lemma.

$$\begin{aligned} g_\sigma = f_\sigma &\Leftrightarrow \exists s \in N_G(H) \text{ such that } g_\sigma = s^{-1} {f_\sigma}^\sigma s, \forall \sigma \in \mathrm{Gal}(\overline{k}/k) \\ &\Rightarrow s g^{-1} \sigma(g) = f^{-1}\sigma(f)\sigma(s), \forall \sigma \in \mathrm{Gal}(\overline{k}/k) \\ &\Rightarrow \sigma(g s^{-1} f^{-1}) = g s^{-1} f^{-1}, \forall \sigma \in \mathrm{Gal}(\overline{k}/k) \\ &\Rightarrow g s^{-1} f^{-1} \in G(k). \end{aligned}$$

Then taking $r = g s^{-1} f^{-1}$ we get:

$$\begin{aligned} gHg^{-1} = (g s^{-1} f^{-1}) f H f^{-1} (g s^{-1} f^{-1})^{-1} &= r f H f^{-1} r^{-1} \\ \Rightarrow \exists r \in G(k) &\text{ such that } H_g = H_{rf}. \end{aligned}$$

Conversely, if $H_g = H_{rf}$ we will have $f^{-1} r^{-1} g \in N_G(H)$ so that:

$$(f^{-1} r^{-1} g)^{-1} {f_\sigma}^\sigma (f^{-1} r^{-1} g) = g^{-1} r f f^{-1} \sigma(f) \sigma(f^{-1}) r^{-1} \sigma(g) = g_\sigma.$$

Which implies $g_\sigma = f_\sigma$. □

Taking r as the identity we thus have a well defined map. □

Claim. *With the map as above,*

$$H_g \xmapsto{\phi} g_\sigma,$$

we have $\ker \phi = \{H_r | r \in G(k)\}$ *and* $\operatorname{im} \phi = \ker \left[H^1(\mathrm{Gal}(\overline{k}/k), N_G(H)) \to H^1(\mathrm{Gal}(\overline{k}/k), G) \right]$.

Proof. The statement about the kernel follows from the lemma in corollary. The statement about the image follows from the fact that ϕ by definition maps to coboundaries in G. That ϕ surjects onto this kernel is obvious, since if $\xi_\sigma \in H^1(\mathrm{Gal}(\overline{k}/k), N_G(G))$ becomes a coboundary in $H^1(\mathrm{Gal}(\overline{k}/k), G)$ then $\xi_\sigma = g^{-1}\sigma(g)$ for some $g \in G$ and thus ξ_σ is the image of gHg^{-1} in $H^1(\mathrm{Gal}(\overline{k}/k), N_G(H))$. □

In the case we are most interested in, that is maximal tori, the fact that they are all conjugate in $G(\overline{k})$ means that this construction gives us a complete classification of the k-defined maximal tori in G up to $G(k)$-conjugation.

Corollary 3.2.4. *Let $H \subset G$ be a subgroup with both H, G defined over k. Consider the set $R(H)$ of $G(\overline{k})$ conjugates of H that are defined over k, modulo conjugation by $G(k)$. $R(H)$ is a pointed set with base point H and there is a bijective map of pointed sets:*

$$\phi : R(H) \to \mathrm{Ker}\left[H^1(\mathrm{Gal}(\overline{k}/k), N_G(H)) \to H^1(\mathrm{Gal}(\overline{k}/k), G)\right].$$

Proof. This is simply a restatement of the previous claim. □

Remark. We have proven the above using direct computations, however one can understand this result conceptually by looking at the meaning of objects in the exact sequence of cohomology corresponding to the exact sequence:

$$1 \to N_G(H) \to G \to G/N_G(H) \to 1$$

where $G/N_G(H)$ is viewed as a pointed set with Galois action. In particular one has that as pointed sets:

$$(G/N_G(H))(k)/G(k) \simeq \mathrm{Ker}[H^1(\mathrm{Gal}(\overline{k}/k), N_G(H)) \to H^1(\mathrm{Gal}(\overline{k}/k), G)]$$

where $(G/N_G(H))(k)$ is a pointed set with a $G(k)$ action so the quotient makes sense.

Since we have that all maximal tori in G are conjugate, we find:

Corollary 3.2.5 (Classification of Maximal Tori)**.** *Let G/k be an algebraic group, fix a maximal torus $T_0 \subseteq G$ defined over k. Then we have a bijection:*

$$\{T \subset G |\ T \text{ maximal } k\text{-defined torus}\}/G(k) \leftrightarrow \mathrm{Ker}\left[H^1(\mathrm{Gal}(\overline{k}/k), N_G(T_0)) \mapsto H^1(\mathrm{Gal}(\overline{k}/k), G)\right],$$

Moreover, $gTg^{-1} \simeq {}_{g_\sigma}T$, where ${}_{g_\sigma}T$ is the torus T with twisted Galois action (see page 38).

Proof. The only new statement here is the one about twisting. If we consider the group isomorphism (that it is an isomorphism is essentially by definition):

$$\psi\colon {}_{g_\sigma}T \longrightarrow gTg^{-1}, \qquad t \longmapsto gtg^{-1}.$$

Then the only thing to check is that it preserves the k-structure. To do this it suffices to check that it is equivariant with respect to $\mathrm{Gal}(\overline{k}/k)$. Indeed, on ${}_{g_\sigma}T$ the group $\mathrm{Gal}(\overline{k}/k)$ acts as:

$$\sigma(t) = g_\sigma * {}^\sigma t = g_\sigma {}^\sigma t g_\sigma^{-1}$$

where $*$ denotes the action of an automorphism; in this case the automorphism corresponding to g_σ is the inner automorphism of conjugation by g_σ. We get:

$$\begin{aligned}
\psi(\sigma(t)) &= \psi(g_\sigma * {}^\sigma t) \\
&= g \cdot g_\sigma \sigma(t) g_\sigma^{-1} \cdot g^{-1} \\
&= g \cdot g^{-1} \sigma(g) \sigma(t) \sigma(g^{-1}) g \cdot g^{-1} \\
&= \sigma(gtg^{-1}) \\
&= \sigma(\psi(t)),
\end{aligned}$$

which is the desired result. □

Remark. The next few results involve certain seemingly difficult to describe groups. The groups themselves turn out to have simple descriptions over an algebraically closed field. In particular we shall eventually prove (Lemma 4.1.1) that we have $N_{\mathrm{GL}_n}(\mathrm{O}) = \mathbb{G}_m \cdot \mathrm{O}$. From this it shall follow

that $N_{N_{\mathrm{GL}_n}(O)}(T) = N_{\mathrm{GL}_n}(O) \cap N_{\mathrm{GL}_n}(T) = \mathbb{G}_m \cdot N_O(T)$. One should remark that these are not direct products, in particular $-Id$ is in both groups.

One should also remark that in general for a maximal torus $T \subset G$ where G is a semi-simple group we have $N_G(T)/T$ is what is called the **Weyl Group** and this object has a strong connection to the classification of semi-simple algebraic groups. Moreover, for the case of a maximal torus T in GL_n we have that over $\overline{k}$ we find $N_{\mathrm{GL}_n}(T) \simeq T \rtimes S_n$ where S_n acts as the permutation group on the characters. One should note well that the rational structure of this group is non-trivial if T is not chosen to be the split torus.

For an orthogonal group, though it is not semi-simple, the structure of $N_{\mathrm{O}_n}(T)$ can still be worked out (either via ideas in Theorem 4.4.2 or by working first with SO_n). When one does this one finds that for n even we have that over $\overline{k}$ we get $N_{\mathrm{O}_n}(T) \simeq T \rtimes (\mathbb{Z}/2\mathbb{Z})^{n/2} \rtimes S_{n/2}$. Here $S_{n/2}$ acts by permuting in a compatible fashion the characters along with their inverses and the $\mathbb{Z}/2\mathbb{Z}$ act by interchanging a character and its inverse (a similar formula exists for n odd with an extra $\mathbb{Z}/2\mathbb{Z}$ term which acts as a reflection along the line fixed by T). Again one should note that the rational structure of these groups will not in general be trivial to describe. It is for this reason we continue to use $N_{\mathrm{O}_n}(T)$ rather than $T \rtimes (\mathbb{Z}/2\mathbb{Z})^{n/2} \rtimes S_{n/2}$ as the latter seems to imply a trivial Galois actions on the $(\mathbb{Z}/2\mathbb{Z})^{n/2} \rtimes S_{n/2}$ factor.

Similarly to the result above about tori, arising from the fact that we can diagonalize any form over an algebraically closed field, we have that all orthogonal groups are conjugate in $\mathrm{GL}_n(\overline{k})$ and thus we have the following:

Corollary 3.2.6. *Let $O_0 \subset \mathrm{GL}_n$ be any k-defined orthogonal group of dimension n. Consider the set:*

$$R(O) = \{O \subset \mathrm{GL}_n |\ O \text{ a } k\text{-defined orthogonal group}\}/\mathrm{GL}_n(k).$$

Then we have a bijection:

$$R(O) \leftrightarrow H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(O_0)).$$

Proof. That all orthogonal groups are conjugate allows us to apply the theorem. Hilbert's Theorem 90 tells us that $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{GL}_n)$ is trivial, as such we do not need to take the kernel of the map to $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{GL}_n)$ as this would be all of $H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(O_0))$ anyways. □

As a further consequence of the fact that any two orthogonal groups are conjugate and the fact that any two tori in them are conjugate we have the following:

Corollary 3.2.7. *Let $T_0 \subset O_0$ be a maximal k-defined torus contained in the k-defined orthogonal group O_0. Consider the set:*

$$R(T) = \{T \subset \mathrm{GL}_n |\ T \subset O \text{ maximal } k\text{-defined torus in } O \text{ an orthogonal group}\}/\mathrm{GL}_n(k)$$

Then we have a bijection:

$$R(T) \leftrightarrow H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(T_0)).$$

Proof. We remark first that the orthogonal groups in which the various T are contained are not necessarily defined over k. The proof follows from the observation that any conjugate of T_0 is automatically contained in the conjugate of O_0 and that any two maximal tori in any two orthogonal groups of the same dimension are conjugate. □

We now combine the above two results:

Corollary 3.2.8. *Let $T_0 \subset O_0$ be a maximal k-defined torus contained in the k-defined orthogonal group O_0. Consider the set:*

$$R(O,T) = \{(O,T) |\ T \subset O \subset \mathrm{GL}_n, \text{ with } T, O \text{ both defined over } k\}/\sim .$$

The equivalence condition is to consider orthogonal groups up to $\mathrm{GL}_n(k)$ *conjugacy and the tori that each orthogonal group* O *contains up to* $N_{\mathrm{GL}_n}(O)(k)$ *conjugacy (we shall see later that* $N_{\mathrm{GL}_n}(O)$ *is only larger than* O *through the inclusion of scalar matrices). We then have a bijection:*

$$R(O,T) \leftrightarrow H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0)).$$

Proof. We first make a few observations about why we would expect such a result before proceeding to give the full proof of it. that since every k-rational orthogonal group contains a k-rational maximal torus, every k-rational orthogonal group contains a k-rational conjugate of T_0.

Now, the inclusion $N_{N_{\mathrm{GL}_n}(O_0)}(T_0) \subset N_{\mathrm{GL}_n}(T_0)$ Gives us the map of cohomology:

$$H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0)) \to H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(T_0)).$$

This allows us to get a map:

$$\phi_T : H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0)) \to R(T).$$

Likewise the inclusion $N_{N_{\mathrm{GL}_n}(O_0)}(T_0) \subset N_{\mathrm{GL}_n}(O_0)$ gives us a map:

$$\phi_O : H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0)) \to R(O).$$

However, the method of associating to a cohomological element $g_\sigma \in H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0))$ an element of $R(T)$ was to took at gT_0g^{-1}, and to get an element of $R(O)$ we have gO_0g^{-1}. It follows then that the image of $\phi'_{OT} := \phi_T \times \phi_O$ lands in $R(O,T)'$ (where $R(O,T)'$ is the natural image of $R(O,T)$ in $R(O) \times R(T)$). Moreover, the map:

$$\phi'_{OT} : H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0)) \to R(O,T)'$$

will be surjective. For any k-defined maximal torus T in a k-defined orthogonal group O we can consider first the element $h_1 \in \mathrm{GL}_n$ which conjugates O_0 to O then the element $h_2 \in O$ which conjugates $h_1T_0h_1^{-1}$ to T. The element $g = h_2h_1 \in \mathrm{GL}_n$ then conjugates both O_0 to O and T_0 to T. Consequently $g_\sigma \in H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0))$ and moreover $\phi_T(g_\sigma) = T$ and $\phi_O(g_\sigma) = O$.

All that would then remain is to check that the map ϕ'_{OT} factors through $R(O,T)$, that is, that the equivalence conditions we put on $R(O,T)$ are in fact correct.

Now, by our previous theorems and the fact that the conjugates of T_0 in $N_{\mathrm{GL}_n}(O_0)$ are all in fact inside O_0 we have that $R(O,T)$ can be decomposed as follows:

$$R(O,T) = \bigsqcup_{g_\sigma} \mathrm{Ker}\left[H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(gO_0g^{-1})}(gT_0g^{-1})) \xrightarrow{\alpha} H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(gO_0g^{-1}))\right]$$

where the disjoint union runs over one representative $[g_\sigma] \in H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(O_0))$ conjugacy class of orthogonal group k-rational orthogonal group (we remark we can choose g so that gT_0g^{-1} is k-rational). However we also know that via the cohomological map:

$$H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0)) \to H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(O_0))$$

that every element of $H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0))$ must be in the kernel of the map:

$$H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0)) \xrightarrow{\beta} H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(gO_0g^{-1}))$$

for precisely one choice of base-point gO_0g^{-1}. In particular we can decompose the cohomology $H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0))$ as:

$$\bigsqcup_{g_\sigma} \mathrm{Ker}\left[H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0)) \xrightarrow{\beta} H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(gO_0g^{-1}))\right].$$

With this we note that the map:

$$H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(O_0)}(T_0)) \to H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(gO_0g^{-1})}(gT_0g^{-1}))$$

via twisting by g_σ makes it so that the combined diagram with α and β will be commutative. We then see that we have the desired result. □

Corollary 3.2.9. *Fix an n-dimensional orthogonal group O_q and a maximal torus T and both of which are defined over k with $T \subset \mathrm{O}_q \subset \mathrm{GL}_n$. Consider the natural maps:*

$$\phi_1 : H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(\mathrm{O}_q)}(T)) \to H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}(T))$$

$$\phi_2 : H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(\mathrm{O}_q)}(T)) \to H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(T))$$

$$\phi_3 : H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(\mathrm{O}_q)}(T)) \to H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{GL}_n}(\mathrm{O}_q))$$

Then we have correspondences:

$\mathrm{Ker}(\phi_1) \leftrightarrow \{$ *k-rational orthogonal groups containing a k-rationally isomorphic copy of T* $\}/\sim$
$\mathrm{Ker}(\phi_2) \leftrightarrow \{$ *k-rational orthogonal groups containing a k-conjugate of T* $\}/\sim$
$\mathrm{Ker}(\phi_3) \leftrightarrow \{$ *k-rational conjugates of T contained in O_q* $\}/\sim$

where the objects on the right are considered up to conjugation in $\mathrm{GL}_n(k)$ (potentially with a multiplicity).

Proof. By the previous theorem $H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(\mathrm{O}_q)}(T))$ classifies up to some equivalence pairs $T \subset O \subset \mathrm{GL}_n$ such that T, O are both defined over k. By taking kernels of these various maps we pick out specific subsets of these. Consequently the first assertions amounts to understanding what the trivial elements on the right hand sides of the maps corresponds to. In the first case we get pairs (O', T') where T' is rationally isomorphic to T. In the second T' must be rationally conjugate to T. In the third case we require that O' be rationally conjugate to O.

On the issue of equivalence conditions and multiplicities, these follow by comparing our stated equivalence condition with those of the previous theorem and observing that the map may not be one to one. For the first correspondence, we have one copy of each O' for each class of non-$N_{N_{\mathrm{GL}_n}(O)}(T)(k)$-equivalent representation of T into O. For the second correspondence you will have one copy of each O' for each class of non-$N_{N_{\mathrm{GL}_n}(O)}(T)(k)$-conjugate embedding of T into O that is $\mathrm{GL}_n(k)$ conjugate to T in O. □

Remark. The distinction between understanding into which orthogonal groups a given torus can embed and understanding which contain a rational conjugate of some fixed embedding into GL_n comes down to a question about the rational representations of tori.

One might ask that if $T_1, T_2 \subset \mathrm{GL}_n$ are conjugate over $\overline{k}$ and are k-isomorphic (via some map that is not necessarily conjugation) then are they conjugate in GL_n over k? The answer to this question is known to be true for the special case of split tori. However, in general we know that

not all representations of a torus need to be linearly equivalent over $\overline{k}$ (let alone over k), but what we are asking is if under some conditions the images of these representation are.

A related question to ask is, suppose $T_1, T_2 \subset G \subset \mathrm{GL}_n$ are defined over k are conjugate by $g \in G(\overline{k})$ and $g' \in \mathrm{GL}_n(k)$ does this imply that they are conjugate over k in G? The answer to this second question is in general no, consider for example conjugation by $\begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$ and $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ on tori in SL_2.

One might then ask even if it fails for general G, are there groups for which it is true, and in particular is it true for O_q or $N_{\mathrm{GL}_n}(\mathrm{O}_q)$? In particular if these statements where true, then this would imply the multiplicities mentioned in the previous theorem are 1.

3.2.1 Twisting and Characters of Tori

Now that we have a classification of the maximal tori in terms of cohomology, we are interested in which properties of a torus can be extracted just from information about the base tori and the corresponding cohomology class of the torus. We start by trying to understand the character group of the torus. Let T be a k-defined torus.

If we define the action of $M \in \mathrm{Aut}(T)$ on $\chi \in X^*(T)$ to be:

$$M \circ \chi(t) := \chi(M^{-1}(t))$$

then we can twist the character module $X^*(T)$ via the elements of $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}(T))$ and thus also by $H^1(\mathrm{Gal}(\overline{k}/k), N_G(T))$. Namely, for a cocycle ξ we have ${}_\xi X^*(T)$ is the Galois module with underlying group $X^*(T)$ but with twisted Galois action. For $\sigma \in \mathrm{Gal}(\overline{k}/k)$ and $\chi \in {}_\xi X^*(T)$ denote the action of σ on χ as σ_ξ and define it as:

$$\sigma_\xi(\chi)(a) = \xi_\sigma(\sigma(\chi))(a) = \sigma(\chi(\sigma^{-1}(\xi_\sigma^{-1}(a)))).$$

Doing this we get the following result:

Theorem 3.2.10. *Let $T \subseteq G$ be a torus defined over k, let $\xi_\sigma \in H^1(\mathrm{Gal}(\overline{k}/k), N_G(T))$ then we have that $X^*({}_{\xi_\sigma}T) \simeq {}_{\xi_\sigma}X^*(T)$ as Galois Modules. Moreover, this isomorphism is realized via the map: $\psi : \chi \mapsto \chi$, that is essentially the identity map.*

Proof. Since ${}_{\xi_\sigma}T$ and T are isomorphic as groups, ψ is certainly an isomorphism of the character modules viewed only as $\mathbb{Z}$-modules. So the only thing to check is that ψ is Galois equivariant. Indeed, for each $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we get (in $\chi({}_{\xi_\sigma}T)$):

$$\begin{aligned} ({}^\sigma\chi)(t) &= \sigma \circ \chi({}^{\sigma^{-1}}t) \\ &= \sigma \circ \chi(\xi_{\sigma^{-1}}(\sigma^{-1}(t))). \end{aligned}$$

If we now apply ψ to this we get that:

$$\begin{aligned} (\psi({}^\sigma\chi))(t) &= \sigma \circ \chi(\xi_{\sigma^{-1}}(\sigma^{-1}(t))) \\ &= \sigma \circ \chi(\xi_{\sigma^{-1}}({}^{\sigma^{-1}}t)). \end{aligned}$$

If we were currently working in $X^*(T)$ this would give ${}^{\sigma}(\chi \circ \xi_{\sigma^{-1}})(t)$. However, we are in ${}_{\xi_\sigma}X^*(T)$ so we have a twisted action and get: $({}^{\sigma}X^*)(t)$. This is because we have:

$$\begin{aligned}
({}^{\sigma_\xi}\chi) &= \xi_\sigma \cdot ({}^{\sigma}\chi) \text{ so that:} \\
({}^{\sigma_\xi}\chi)(t) &= \xi_\sigma \cdot ({}^{\sigma}\chi)(t) \\
&= \sigma(\chi(\sigma^{-1}(\xi_\sigma^{-1}(t)))) \\
&= \sigma(\chi(\sigma^{-1}(\sigma(\xi^{-1})\xi t \xi^{-1}\sigma(\xi)))) \\
&= \sigma(\chi(\xi^{-1}\sigma^{-1}(\xi)\sigma^{-1}(t)\sigma^{-1}(\xi^{-1})\xi)) \\
&= \sigma \circ \chi(\xi_{\sigma^{-1}}({}^{\sigma^{-1}}t)),
\end{aligned}$$

which completes the result. □

Once we know how to compute the character groups for the torus corresponding to our cohomological elements we can then use this information to determine other properties that depend only on the character group. In particular we know that the splitting field of the torus is the field of definition for the character module. And thus by understanding the character module we know the splitting field. For a more direct method of determining this we note that if the original torus T were split, then a torus corresponding to ξ_σ will be split over the fixed field of $\mathrm{Ker}(\xi : \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(T))$. If T where not split, then ${}_{\xi_\sigma}T$ will split over the composite field of that field and the splitting field of T, but that will in general not be minimal. We do however know that there is a conjugate of T that is split somewhere in GL_n, and in some situations we can arrange that it will be contained in a conjugate of G that is defined over k (every orthogonal group is conjugate to an orthogonal group containing a split maximal torus). In particular we want, $\exists s \in \mathrm{GL}_n(\overline{k})$ such that sTs^{-1} is k-split, and sGs^{-1} is defined over k. We then have that $s^{-1}\sigma(s) =: s_\sigma \in H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n(\overline{k})}(G)}(T))$. We then wish to study the image of ξ_σ in $H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n(\overline{k})}({}_{s_\sigma}G)}({}_{s_\sigma}T))$. The map coming via:

$$\begin{array}{ccccc}
H^1(\mathrm{Gal}(\overline{k}/k), N_G(T)) & \longrightarrow & H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}(G)}(T)) & \longrightarrow & H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}({}_{s_\sigma}G)}({}_{s_\sigma}T)) \\
\xi_\sigma & \longmapsto & \xi_\sigma & \longmapsto & s\xi_\sigma\sigma(s^{-1})
\end{array}$$

Claim. *With notation as above, a splitting field of the torus corresponding to ξ_σ is the fixed field in $\overline{k}$ of* $\mathrm{Ker}(s\xi_\sigma\sigma(s^{-1}))$ *where we fix a representative of the cocycle and view $s\xi_\sigma\sigma(s^{-1})$ as a map of pointed sets* $\mathrm{Gal}(\overline{k}/k) \to N_{N_{\mathrm{GL}_n}({}_{s_\sigma}G)}({}_{s_\sigma}T))$.

Proof. By construction the torus corresponding to $\xi_\sigma \in H^1(\mathrm{Gal}(\overline{k}/k), N_G(T))$ is the same as the one corresponding to $s\xi_\sigma\sigma(s^{-1}) \in H^1(\mathrm{Gal}(\overline{k}/k), N_{N_{\mathrm{GL}_n}({}_{s_\sigma}G)}({}_{s_\sigma}T))$. By Hilbert's Theorem 90 we may write $s\xi_\sigma\sigma(s^{-1}) = g^{-1}\sigma(g)$. We observe that g is then an element of GL_n which splits the torus, and that the kernel we describe is precisely the field generated by the entries of g. □

3.3 Tori with Compact $\mathbb{R}$-points

We have the requirement that the tori we are interested in should have that their set of points over $\mathbb{R}$ be compact. Our current goal is to understand which tori these are.

3.3.1 Classification of Tori over $\mathbb{R}$

A first step towards understanding which tori over $\mathbb{Q}$ have compact sets of real points is to classify all tori over $\mathbb{R}$ and then inspect which are compact. Once we have done this we will be able to develop a criterion for which tori defined over $\mathbb{Q}$ will have a compact set of real points.

Example. We have the following examples of tori over $\mathbb{R}$.

1. $\mathbb{G}_m$ is the most trivial case, its character module is generated by $\chi : t \mapsto t$. We have $\mathbb{G}_m(\mathbb{R}) = \mathbb{R}^*$.
2. $R_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m) = \left\{ \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mid a^2 + b^2 \neq 0 \right\}$, over $\mathbb{C}$ this becomes isomorphic to $\mathbb{G}_m \times \mathbb{G}_m$ and has characters χ_1, χ_2 given by $\chi_1 \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mapsto a + bi$ and $\chi_2 \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mapsto a - bi$. These generate the character module and complex conjugation in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts by interchanging them.
3. $R^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m) = \left\{ \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) | a^2 + b^2 = 1 \right\} = \left\{ \frac{1}{2} \left(\begin{smallmatrix} x + \frac{1}{x} & -i(x - \frac{1}{x}) \\ i(x - \frac{1}{x}) & x + \frac{1}{x} \end{smallmatrix}\right) \right\}$. This torus is a sub-torus of the one above, one notices that its $\mathbb{R}$-points form a compact set, the character module is a quotient of the one in case (2) by the relation $\chi_1 = \chi_2^{-1}$. Either of the characters $\chi_1 = x$ or $\chi_2 = \frac{1}{x}$ will generate the character module. Complex conjugation in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts by sending characters to their inverse. We remark that this is isomorphic to $\mathrm{SO}(2)$.

The following result is essentially stated in Platinov & Rapinchuk "Algebraic Groups and Number Theory" [PR94].

Theorem 3.3.1 (Classification of Tori over $\mathbb{R}$)**.** *Every torus over $\mathbb{R}$ is some finite product of tori in the form of the above examples. That is of the form:*

$$\mathbb{G}_m^i \times R_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)^j \times R^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)^k.$$

Proof. Tori over $\mathbb{R}$ are all forms of the torus $T = (\mathbb{G}_m)^n$ for some n and are thus classified by:

$$H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathrm{Aut}(T))$$

But we have chosen T to be split over $\mathbb{R}$ so that the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on $\mathrm{Aut}(T)$ is trivial and thus understanding the cohomology is equivalent to classifying n dimensional integral representations of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, i.e.

$$H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathrm{GL}_n(\mathbb{Z})) = \mathrm{Hom}(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathrm{GL}_n(\mathbb{Z})).$$

By observing that each such homomorphism ϕ turns $\mathbb{Z}^n$ into a $\mathbb{Z}$-torsion free finitely generated $\mathbb{Z}[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$-module the problem reduces to classifying these modules, which (as we shall prove shortly) it turns out are all of the form:

$$\mathbb{Z}^i \oplus \mathbb{Z}[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]^j \oplus I^k,$$

where I is the kernel of the augmentation map $\mathbb{Z}[\mathrm{Gal}(\mathbb{C}/\mathbb{R})] \to \mathbb{Z}$. Once we have this, we know that via a different choice of basis for $\mathbb{Z}^n$ our homomorphism ϕ can be written in the form:

$$\sigma \mapsto \mathrm{diag}\left(\underbrace{1, \cdots, 1}_{i}, \underbrace{\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \cdots, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)}_{j}, \underbrace{-1, \cdots, -1}_{k} \right)$$

where σ represents complex conjugation. Since, complex conjugation acts this way on the character modules of $\mathbb{G}_m, R_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m), R^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)$, we can conclude by Theorem 2.1.8 that these are all the tori.

It remains only to prove the following lemma:

Lemma 3.3.2. *Every $\mathbb{Z}$-torsion free finitely generated $\mathbb{Z}[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$-module is of the form*

$$\mathbb{Z}^i \oplus \mathbb{Z}[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]^j \oplus I^k.$$

Proof. Let M be a finitely generated $\mathbb{Z}$-torsion free $\mathbb{Z}[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$-module. Then M can be viewed as being a free finitely generated $\mathbb{Z}$ module with an involution τ. In particular then, $M \simeq \mathbb{Z}^n$ and

$\tau \in \mathrm{GL}_n(\mathbb{Z})$ satisfies $\tau^2 = id_n$. To get the desired result we need to show that any such τ is similar over $\mathbb{Z}$ to one of the form:

$$\mathrm{diag}\left(\underbrace{1,\cdots,1}_{i},\underbrace{\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right),\cdots,\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)}_{j},\underbrace{-1,\cdots,-1}_{k}\right).$$

It is worth noting that if $\mathbb{Z}$ were a field, this result would follow immediately from the theory of rational canonical forms, moreover if $\mathbb{Z}[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$ were either a principle ideal domain or if it were split, general theory would yield the results. Unfortunately, $\mathbb{Z}[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$ is not a principle ideal domain as it has zero divisors, and does not split, though $\mathbb{Z}[\frac{1}{2}][\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$ does.

Claim (1)**.** *Let M be a free $\mathbb{Z}$-module, then $\{x_1,\cdots,x_n\} \subset M$ extends to a basis for M if and only if $\{x_1,\cdots,x_n\}$ is linearly independent and for all $z \in M$ such that there exists $0 \neq n \in \mathbb{Z}$ with $nz \in \langle x_1,\cdots,x_n\rangle_{\mathbb{Z}}$ we have $z \in \langle x_1,\cdots,x_n\rangle_{\mathbb{Z}}$.*

Proof. The forward direction is proven by considering some extension to a basis and showing that if $nz \in \langle x_1,\cdots,x_n\rangle_{\mathbb{Z}}$ but z is not then we will have a linear dependence in our extended basis.

The reverse direction is proven by considering any basis for M and showing inductively that we can perform a change of basis to include the x_i. This requires showing that the subsets $\{x_1,\ldots,x_m\}$ satisfy the same conditions, which is to say that if $az \in \langle x_1,\cdots,x_m\rangle_{\mathbb{Z}}$ then $az \in \langle x_1,\cdots,x_n\rangle_{\mathbb{Z}}$ so $z \in \langle x_1,\cdots,x_n\rangle_{\mathbb{Z}}$ we then get two expressions for az in terms of the $\{x_1,\cdots,x_n\}$ linear independence will then imply $z \in \langle x_1,\cdots,x_m\rangle_{\mathbb{Z}}$.
Now inductively suppose we have included the first m elements into a basis $\{x_1,\cdots,x_m,y_1,\cdots y_l\}$, write x_{m+1} in terms of this basis $x_{m+1} = a_1x_1 + \cdots + a_mx_m + b_1y_1 + \cdots + b_ly_l$. the divisibility condition on the x_i implies that $\gcd(b_i) = 1$ we can thus perform a change of basis within the y_j to arrange so that at least one $b_j = 1$, replacing the corresponding y_j with x_{m+1} is then a valid integral change of basis and allows us to complete the result. □

Claim (2)**.** *Let M be a free $\mathbb{Z}$-module and suppose the set $\{x_1,\cdots,x_n\} \subset M$ extends to a basis for M. Let $y \in M \setminus \langle x_1,\cdots,x_m\rangle_{\mathbb{Z}}$, then there exists $z \in M, 0 \neq a \in \mathbb{Z}$ such that $az \in \langle x_1,\cdots,x_m,y\rangle_{\mathbb{Z}}$ and $\{x_1,\cdots,x_n,z\}$ extends to a basis for M. Moreover, we have that:*

$$\{x \in M |\ \exists 0 \neq a \in \mathbb{Z} \text{ such that } ax \in \langle x_1,\cdots,x_m,y\rangle_{\mathbb{Z}}\} = \langle x_1,\cdots,x_n,z\rangle_{\mathbb{Z}}.$$

Proof. Consider the $\mathbb{Z}$-module $M' = \{x \in M |\ \exists 0 \neq a \in \mathbb{Z} \text{ such that } ax \in \langle x_1,\cdots,x_m,y\rangle_{\mathbb{Z}}\}$. Since $\{x_1,\cdots,x_n\}$ extends to a basis of M, by the conditions of claim 1 it extends to one for M'. Let z be any element in this extension to a basis for M', then again by claim 1 we have $\{x_1,\cdots,x_n,z\}$ extends to a basis for M. The assertion $M' = \langle x_1,\cdots,x_n,z\rangle_{\mathbb{Z}}$ is checked that if $z' \in M' \setminus \langle x_1,\cdots,x_n,z\rangle_{\mathbb{Z}}$ then for some $0 \neq a,b \in \mathbb{Z}$ we would have $\langle x_1,\cdots,x_n,az,bz'\rangle_{\mathbb{Z}}$ a rank $n+2$ submodule of M'. □

Claim (3)**.** *τ is upper triangularizable over $\mathbb{Z}$.*

Proof. We proceed inductively to produce a set $\{x_1,\cdots,x_m\}$ that extends to a basis for M and $\langle x_1,\cdots,x_n\rangle_{\mathbb{Z}}$ is τ stable and τ acts upper triangularly. So, suppose we have completed this process up to step m and suppose $y \in M \setminus \langle x_1,\cdots,x_m\rangle_{\mathbb{Z}}$. We consider first the case that $\{x_1,\cdots,x_m,y,\tau(y)\}$ is linearly independent. In this case replace y by $y + \tau(y)$ (note that the "new y" is still in $M \setminus \langle x_1,\cdots,x_n\rangle_{\mathbb{Z}}$).

We may now suppose we are in the case where $\{x_1,\cdots,x_m,y,\tau(y)\}$ is linearly dependant. We now apply claim (2) to $\{x_1,\cdots,x_m,y\}$ and find there exists $z \in M$ such that $\{x_1,\cdots,x_m,z\}$

extends to a basis of M and

$$\langle x_1, \cdots, x_m, z\rangle_{\mathbb{Z}} = \{x \in M | \ \exists 0 \neq a \in \mathbb{Z} \text{ such that } ax \in \langle x_1, \cdots, x_m, y\rangle_{\mathbb{Z}}\}.$$

Notice that because of the linear dependance we assumed we find $\tau(y) \in \langle x_1, \cdots, x_m, z\rangle_{\mathbb{Z}}$. Moreover, notice then that since $\langle x_1, \cdots, x_m, y, \tau(y)\rangle_{\mathbb{Z}}$ was τ stable so too is $\langle x_1, \cdots, x_m, z\rangle_{\mathbb{Z}}$. It follows then that τ will act upper triangularly with the basis $\{x_1, \ldots, x_m, z\}$. The result follows by induction. □

Since τ is upper triangularizable we can write:

$$\tau = \begin{pmatrix} \pm 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \pm 1 \end{pmatrix}.$$

Claim (4)**.** *We can sort the diagonal of τ via a change of basis so that all the $+1$ appear before the -1 while maintaining upper triangularity.*

Proof. It suffices to prove that the blocks $\left(\begin{smallmatrix} 1 & a \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & a \\ 0 & 1 \end{smallmatrix}\right)$ are all similar since we could then interchange the 1's and -1's one at a time preserving upper triangularity. The computation:

$$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a \\ 0 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a-2 \\ 0 & -1 \end{smallmatrix}\right)$$

allows us to reduce a $(mod\ 2)$, the case of $a = 0$ is seen via the identity:

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

and the computations:

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

give us the result in the $a = 1$ case. □

We now conclude that we have τ in the form:

$$\tau = \begin{pmatrix} 1 & * & \cdots & * \\ & \ddots & & \\ & & 1 & \vdots \\ & & & -1 & \\ & & & & \ddots & * \\ & & & & & -1 \end{pmatrix}.$$

the condition $\tau^2 = id_n$ can be used to iteratively show that the entries above the 1's on the diagonal and those to the right of the -1's are all 0. This is done by computing the $a_{i+j,i}$ entry of τ^2 starting at $j = 1, i = 1$ then $j = 1, i = 2$ and so on. Consequently we may assume we have:

$$\tau = \begin{pmatrix} id_n & A \\ 0_{m,n} & -id_m \end{pmatrix}$$

where A is some potentially non-square matrix. It is then an easy check that:

$$\begin{pmatrix} P & 0_{m,n} \\ 0_{n,m} & Q \end{pmatrix} \begin{pmatrix} id_n & A \\ 0_{m,n} & -id_m \end{pmatrix} \begin{pmatrix} P^{-1} & 0_{m,n} \\ 0_{n,m} & Q^{-1} \end{pmatrix} = \begin{pmatrix} id_n & PAQ^{-1} \\ 0_{m,n} & -id_m \end{pmatrix}$$

so that by the theory of Smith normal form, that is that invertible row and column operations allow diagonalizing any matrix, we may assume that A is a diagonal matrix. It immediately follows that τ can be broken into blocks of the form $\left(\begin{smallmatrix} 1 & a \\ 0 & -1 \end{smallmatrix}\right)$. The computations in claim (4) then allow us to conclude the desired result. □

This concludes the proof of the theorem. □

As a natural consequence of the above classification, we get the following characterizations of when the real points of a torus are compact.

Corollary 3.3.3. *Let T be an algebraic torus defined over $k \subset \mathbb{R}$ then the following are equivalent:*

1. *$T(\mathbb{R})$ is compact.*
2. *T is isomorphic over $\mathbb{R}$ to $R^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)^a$ for some a.*
3. *T is anisotropic over $\mathbb{R}$, that is $X^*(T)_{\mathbb{R}} = \{0\}$.*
4. *Complex conjugation acts as inversion on $X^*(T)$.*

Proof. (1) $\Leftrightarrow$ (2) in the theorem this is the only case where $T(\mathbb{R})$ is compact.

(2) $\Leftrightarrow$ (3) in the theorem this is the only case where T is anisotropic over $\mathbb{R}$.

(3) $\Leftrightarrow$ (4) follows from fact that for any character τ we know that the character $\tau\overline{\tau}$ will have be in $X^*(T)_{\mathbb{R}}$. Consequently, $X^*(T)_{\mathbb{R}} = \{0\}$ implies $\tau^{-1} = \overline{\tau}$. Conversely, for $\tau \in X^*(T)_{\mathbb{R}}$ we have $\overline{\tau} = \tau$ and so $\tau = \tau^{-1}$ implies $\tau = id$ (as the character module is $\mathbb{Z}$-torsion free.

□

Remark. The previous theorem suggests, that if we understand which of the above types of tori have compact sets of real points (in particular only the last type) and construct the map:

$$\phi : H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_G(T_0)) \to H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathrm{Aut}(T_0)),$$

by first associating to an element of $N_G(T)$ the automorphism it induces through conjugation, and then via fixing an embedding $\overline{\mathbb{Q}} \to \mathbb{C}$ view $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and restricting the map to this set. We could use the map to understand which tori over $\mathbb{Q}$ will have $T(\mathbb{R})$ compact.

Claim. *Fix T_0 any $\mathbb{Q}$-defined maximal torus in G such that $T_0(\mathbb{R})$ is compact. Let T be any other $\mathbb{Q}$-defined maximal torus in G with associated cocycle $g_\sigma \in H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_G(T))$ then $T(\mathbb{R})$ is compact if and only if $g_\sigma \in \mathrm{Ker}(\phi)$.*

Proof. The map ϕ associates to the torus T first its isomorphism class as a torus over $\mathbb{Q}$. Then via restricting to $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ we consider only its isomorphism class over $\mathbb{R}$. Since all tori with $T(\mathbb{R})$ compact of the same rank are $\mathbb{R}$-isomorphic the result then follows. □

3.3.2 Structure of Tori with Compact $\mathbb{R}$-points

Now that we have some criterion for detecting compactness, we wish to describe more explicitly the possible structure of these tori.

Definition 3.3.4. An algebraic torus T/k is said to be **quasi-split** if it is k-isomorphic to $\prod_{i=1}^{n} R_{L_i/k}(\mathbb{G}_m)$ for L_i/k finite extensions.

Remark that a split torus is quasi-split in the sense that one can take the fields L_i to be k.

The following general result can be found in Platinov and Rapinchuk "Algebraic Groups and Number Theory" [PR94].

Theorem 3.3.5. *Every algebraic torus T/k can be embedded into a quasi-split torus. Moreover, if T splits over L we can arrange so that T embeds into $R_{L/k}(\mathbb{G}_m)^l$ for some l.*

Proof. Let L be a finite Galois extension of k over which T splits. Then $X^*(T)$ is a $\mathbb{Z}[\mathrm{Gal}(L/k)]$-module. Writing $X^*(T)$ as a quotient of a free $\mathbb{Z}[\mathrm{Gal}(L/k)]$-module we get the exact sequence:

$$0 \to \Delta \to \mathbb{Z}[\mathrm{Gal}(L/k)]^l \to X^*(T) \to 0$$

Applying the contravariant functor from Galois modules to tori we get the exact sequence:

$$1 \to T \to R_{L/k}(\mathbb{G}_m)^l \to S \to 1$$

which proves the result. □

We now focus more specifically on our setting.

Proposition 3.3.6. *Let k be a totally real field and $T \subset R_{L/k}(\mathbb{G}_m)^l$ have a compact set of real points then T splits over a CM-field.*

Proof. The criterion for $T(\mathbb{R})$ to be compact was that the action of the element induced by complex conjugation in $\mathrm{Gal}(\overline{k}/k)$ acts as inversion on $X^*(T)$. However, which element of $\mathrm{Gal}(\overline{k}/k)$ complex conjugation corresponds to depends on the embedding of $\overline{k}$ in $\mathbb{C}$ whereas compactness depends only on the embedding of k into $\mathbb{R}$. Consequently, we conclude any potential representative of complex conjugation acts by inversion on $X^*(T)$.

Next, we know that a torus $T \subset \mathrm{GL}_n$ is a form of SO_2^l. By the classification of forms, there exists some cocycle $\xi_\sigma \in H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}(\mathrm{SO}_2^l))$ that corresponds to the isomorphism class of T and that the isomorphism $T \to \mathrm{SO}_2^l$ is defined over the fixed field in $\overline{k}$ of $\mathrm{Ker}(\xi_\sigma)$. We moreover know that in general the character module of T is the same as that of SO_2^l except with a twisted action of the Galois group.

Now, for any potential representative of complex conjugation $\tau \in \mathrm{Gal}(\overline{k}/k)$ we have that the action of τ on $X^*(T)$ agrees with that of τ on $X^*(\mathrm{SO}_2^l)$, In particular it acts as inversion on both modules. Consequently, by computing the twisted action we have that $\chi(t) = \chi(\xi_\tau(t))$ for all $\chi \in X^*(T)$ and $t \in T$. From this we conclude for τ, any representative of complex conjugation, ξ_τ is the identity map. This implies that $\tau \in \mathrm{Ker}(\xi_\sigma)$. From this we conclude that the field L' over which T is isomorphic to SO_2^l, that is the fixed field of $\mathrm{Ker}(\xi_\sigma)$ in $\overline{k}$, is fixed by every representative of complex conjugation. Consequently this field is totally real. Since SO_2^l splits over $k(i)$ we conclude that T splits over a $L'(i)$ which is a CM-field. □

Combining Proposition 3.3.6 and Theorem 3.3.5, we conclude that every torus over $\mathbb{Q}$ with $T(\mathbb{R})$ compact embeds in $R_{L/\mathbb{Q}}(\mathbb{G}_m)^l$ where $L/\mathbb{Q}$ is CM.

Theorem 3.3.7. *Every torus T defined over $\mathbb{Q}$ with $T(\mathbb{R})$ compact embeds in $R_{K/\mathbb{Q}}(R^{(1)}_{L/K}(\mathbb{G}_m))^l$ where $L/\mathbb{Q}$ is a CM-field, and K is the maximal totally real subfield of L.*

Proof. By the above we know that T embeds in $R_{K/\mathbb{Q}}(R_{L/K}(\mathbb{G}_m))^l$ for some l where L is a Galois CM splitting field of T. Let σ represent complex conjugation in $\mathrm{Gal}(L/\mathbb{Q})$, then since we know σ acts as -1 on $X^*(T)$ we have that $X^*(T)$ is a module over the ring $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]/(\sigma + 1)$. Then as in previous theorem writing:

$$0 \to \Delta \to (\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]/(\sigma + 1))^l \to X^*(T) \to 0$$

we get the sequence of tori:

$$1 \to T \to R_{K/\mathbb{Q}}(R^{(1)}_{L/K}(\mathbb{G}_m))^l \to S \to 1$$

Which completes the result. □

Remark. We comment that the above result is a long way from saying that all such tori are isomorphic to tori of this form. If it were true that all sub-tori of $R_{K/\mathbb{Q}}(R^{(1)}_{L/K}(\mathbb{G}_m))$ where of a similar form but for a smaller CM-field we could perhaps conclude this. But such a claim is dubious since the similar claim is certainly not true for a general quasi-split torus.

We do however note that the embedding $T \hookrightarrow R_{K/\mathbb{Q}}(R^{(1)}_{L/K}(\mathbb{G}_m))$ gives us a representation $\mathrm{Gal}(L/Q) \to \mathrm{GL}(X^*(T))$. If this representation is not faithful, it must factor through a quotient, and thus corresponds to a smaller subfield of $L' \subset L$ and then $T \hookrightarrow R_{K'/\mathbb{Q}}(R^{(1)}_{L'/K'}(\mathbb{G}_m))$. In this way, since we can bound the size of finite subgroups of GL_n, we may bound the size of extensions we consider when looking at these tori.

CHAPTER 4
Special Points on Hermitian Symmetric Spaces of Orthogonal Type

Recall from the beginning of Chapter 3 that our goal is to understand the special points that appear on the symmetric spaces attached to orthogonal groups. To each special point we have an associated torus of compact type and it was the appearance of these tori in our groups that we have been looking at. The question we now pose is, given an algebraic torus T, for which orthogonal groups O_q can we have $T \subset \mathrm{O}_q$? We are most interested in tori with a compact set of real points.

4.1 Criterion for embedding O_q in $\mathrm{O}_{q'}$

We are interested in the problem of determining which tori can inject into a given orthogonal group. We would like to restrict this to the easier problem of studying this problem for specific types of tori, in particular those that come from a single field and not from a product of fields. However, in doing so, we seem to go from the problem of embedding tori maximally, to embedding them non-maximally. To resolve this we would like to say that, whenever $T \subset \mathrm{O}_q$ then $\exists q'$ such that $T \subset \mathrm{O}_{q'} \subset \mathrm{O}_q$ and T is maximal in $\mathrm{O}_{q'}$. This is however in general not true. We do however have the following results:

Claim. *Let T be a rank n torus defined over a field k suppose $T \hookrightarrow \mathrm{O}_q$ where q is a non-degenerate quadratic form on V a k-vector space then:*

- *T acts on $V \otimes \overline{k}$ via some subset S of its characters. This set S spans the character module.*

  Proof. Diagonalizability implies T acts via characters, that it injects into O_q, and thus into GL_n implies the action is faithful and thus T acts by a spanning set of characters (but not necessarily a basis). □

- *If $W \subset V \otimes \overline{k}$ is a 1-dimensional subspace and T acts on W via $t \circ w \mapsto \chi(t)w$ then either $\chi = 1$ or $q|_W = 0$.*

  Proof. This is because the action of T preserves the form and $q(t \circ v) = \chi(t)^2 q(v)$. □

- *For each character $\chi \in S \setminus \{1\}$ there is a 2-dimensional subspace $W_\chi \in V \otimes \overline{k}$ with a basis w_1, w_2 such that $t \circ w_1 = \chi(t)w_1$ and $t \circ w_2 = \chi(t)^{-1}w_2$. Moreover $q|_W(x_1w_1 + x_2w_2) = ax_1x_2$.*

  Proof. By diagonalizing T over $\mathrm{GL}_n(\overline{k})$ we may suppose that each character acts linearly. We may thus fix $w_1 \in V \otimes \overline{k}$ on which T acts linearly via χ. By non-degeneracy there exists an element $w_2 \in V \otimes \overline{k}$ on which T acts linearly via another character χ' and such that q is not trivial on $W_\chi := \mathrm{span}(w_1, w_2)$. By the previous claim however $q(w_1) = 0$. If $q(w_2) \neq 0$ then $\chi' = 1$ and so $B(t \circ w_1, t \circ w_2) = \chi(t)B(w_1, w_2)$. Thus we conclude also that $q(w_2) = 0$. Consequently $q|_{W_\chi}(x_1w_1 + x_2w_2) = ax_1x_2$. It follows then that since $a \neq 0$ that $\chi' = \chi^{-1}$. □

- *For $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we can take $W_{{}^\sigma\chi} = \sigma(W_\chi)$ in particular, if $\chi \in S$ then ${}^\sigma\chi \in S$.*

  Proof. For w a χ eigenvector of T have:

  $$t \circ \sigma(w) = \sigma((\sigma^{-1}(t) \circ w) = \sigma(\chi(\sigma^{-1}(t))w) = {}^\sigma\chi(\sigma(w)).$$

  This gives us the desired action. □

- *Fixing a Galois stable linearly independent subset $S' \subset S$ and considering $V' := \bigoplus_{\chi \in S'} W_\chi$ yields a k-rational, subspace of V. If we consider the torus T' whose Galois module is $\mathbb{Z}\langle S' \rangle$ then it acts k-rationally on this space.*

  Proof. V' is rational over k since it is Galois stable. T' is rational over k since it is the image of T acting on $\mathrm{GL}(V')$ under a k-rational morphism. □

- *If we can arrange so that S' spans $X^*(T)$ then moreover T' and T will be isogenous.*

  Proof. This follows from the fact that $X^*(T')$ would be a maximal rank $\mathbb{Z}$-submodule of $X^*(T)$. □

Remark. The reason we don't get the desired result from the above is that it is possible that no subset of S forms a $\mathbb{Z}$-basis for the character module. Consider for example the torus:

$$T' = \left\{ \begin{pmatrix} t^2 & 0 & 0 & 0 \\ 0 & t^{-2} & 0 & 0 \\ 0 & 0 & t^3 & 0 \\ 0 & 0 & 0 & t^{-3} \end{pmatrix} \right\}$$

It will inject into an orthogonal group for a 4 dimensional space, is rational, but it doesn't act by a basis of characters. However, in this case the only maximal torus that can contain it inside any orthogonal group is of the form:

$$T = \left\{ \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & s & 0 \\ 0 & 0 & 0 & s^{-1} \end{pmatrix} \right\}.$$

And this torus could be broken up in such a way that it preserves sub-orthogonal groups.

Our general hope was that if we have $T = T_1 \times T_2 \times \cdots \times T_s$, where each T_i cannot be further decomposed as products of k-defined subtori, that whenever $T \hookrightarrow \mathrm{O}_q$ we can decompose $\mathrm{O}_q \supset \prod O_{q_i}$ where $T_i \hookrightarrow O_{q_i}$. The above example shows that not all decompositions of T may work, that is $T \simeq T' \times \mathbb{G}_m$ fails to decompose the space but $T \simeq \mathrm{SO}_2 \times \mathrm{SO}_2$ does. It is hoped that there always exists one that does.

The problem that this uncertainty gives us, is that one may not be able to fully understand the embedding problem for non-maximal tori in terms of the problem for maximal tori together with the embedding problem of orthogonal groups. This restricts what we can say about the embedding problem for tori coming from CM-algebras (rather than just CM-fields). The embeddings of these that we can understand in this way require us to assume that the action is "almost-regular" in the sense that it decomposes into something sufficiently like the regular representation for each constituent field.

If we wish to perform the program as indicated above, one of the first questions that comes up is when can we embed one orthogonal group into another. This problem will turn out to be of interest for another reason in the special case where the orthogonal groups have the same rank. The reason for this is that we shall eventually be able to give some explicit descriptions of quadratic forms that certain tori shall naturally preserve. By doing this, we obtain an embedding of the torus into the orthogonal group associated to the form. A question that then arises is 'how general is this construction?'. If two orthogonal groups are isomorphic, constructing a torus in one group would give us a torus in the other even if we did not a priori see a natural embedding of it. As such, we will be interested in the question of to what extent are the isomorphism classes of orthogonal groups controlled by the quadratic forms defining them? That is we will have maps:

$$\{\text{quadratic forms over } \mathbb{Q} \text{ up to scaling}\} \twoheadrightarrow \{\text{orthogonal groups over } \mathbb{Q} \text{ up to isomorphism}\}$$

$$\{\text{orthogonal groups in } \mathrm{GL}_n \text{ over } \mathbb{Q}\} \hookrightarrow \{\text{forms of } \mathrm{O}_n \text{ over } \mathbb{Q} \text{ up to isomorphism}\}$$

What we would like somehow to know is that the first of these maps is in fact also injective and though not totally relevant to our objectives it is interesting to ask if the second map is surjective.

We first prove a lemma which allows us to understand the structure of $N_{\mathrm{GL}_n}(\mathrm{O}_n)$.

Lemma 4.1.1. *For O_n a orthogonal group (for an n-dimensional space) we get:*

$$N_{\mathrm{GL}_n}(\mathrm{O}_n) = \{\alpha M | \alpha \in \mathbb{C}, M \in \mathrm{O}_n\}.$$

Proof. It suffices to consider the case of the usual orthogonal group coming from ${}^t gg = I_n$.

The containment $\{\alpha M | \alpha \in \mathbb{C}, M \in \mathrm{O}_n\} \subset N_{\mathrm{GL}_n}(\mathrm{O}_n)$ is obvious. Conversely, to say that $M \in N_{\mathrm{GL}_n}(\mathrm{O}_n)$ is to say that $MgM^{-1}I_n{}^t(MgM^{-1}) = I_n$ in GL_n for all $g \in \mathrm{O}_n$. That is equivalent to saying ${}^t g({}^t MM)g = {}^t MM$ for all $g \in \mathrm{O}_n$.

We first consider the case $n = 2$. Take ${}^t MM = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and the element $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{O}_2$. The identity:

$$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} c & d \\ a & b \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} d & c \\ b & a \end{smallmatrix}\right)$$

tells us that $a = d$ and $b = c$ and then using the element $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{O}_2$ we get:

$$\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} b & a \\ -a & -b \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & -b \\ -b & a \end{smallmatrix}\right)$$

which then tells us that $b = c = 0$.

We can reduce the general case to the $n = 2$ case by observing that we can embed $\mathrm{O}_2 \hookrightarrow \mathrm{O}_n$ in sufficiently many ways to get the result that ${}^t MM = \alpha Id$. That is the map which takes $\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right) \in \mathrm{O}_2$ to the matrix $X \in \mathrm{O}_n$ which is equal to the identity except that $X_{ii} = X_{jj} = x$ and $X_{ij} = -X_{ji} = y$ allows us to use the identical argument to show that $({}^t MM)_{ij} = ({}^t MM)_{ji} = 0$ and $({}^t MM)_{ii} = ({}^t MM)_{jj}$. We can thus conclude that $(\frac{1}{\alpha^{(1/2n)}})M \in \mathrm{O}_n$. □

The next thing we need to understand is the structure of $\mathrm{Aut}(\mathrm{O}_q)$. We know that for a connected reductive group the automorphism group is precisely the semi-direct product of the inner automorphisms and the automorphism group of the associated Dynkin diagram [Spr98]. O_q is not connected, however we do have the following:

Claim. *If the dimension n for the quadratic space of q is odd then $\mathrm{Aut}(\mathrm{O}_q) \simeq \mathrm{Aut}(\mathrm{SO}_q)$ and if it is even we have that $\mathrm{Aut}(\mathrm{O}_q) \simeq \mathrm{Aut}(\mathrm{SO}_q) \times \{\pm 1\}$ and in particular the automorphism corresponding to $id \times -1$ is the map $\phi : g \mapsto \det(g)g$.*

Proof. There is a natural map $\mathrm{Aut}(\mathrm{O}_q) \to \mathrm{Aut}(\mathrm{SO}_q)$ coming via restriction using the fact that maps must take the connected component of the identity, in this case SO_q, to itself. It suffices to show that the kernel of this map is precisely ϕ when n is even and trivial when n is odd.

Pick any element $x \in V$ where V is the underlying space of q. Let τ_x be the reflection at x. Then τ_x interchanges the connected components of O_q and thus we have $\mathrm{O}_q = \mathrm{SO}_q \bigsqcup \tau_x \mathrm{SO}_q$. Consequently, any map on O_q trivial on SO_q is determined entirely by its action on τ_x.

Consider a map $\sigma \in \mathrm{Ker}(\mathrm{Aut}(\mathrm{O}_q) \to \mathrm{Aut}(\mathrm{SO}_q))$. For all $h \in \mathrm{SO}_q$ we have $\tau_x h \tau_x = \sigma(\tau_x) h \sigma(\tau_x)$ and so we have that $\tau_x \sigma(\tau_x^{-1})$ is in the center of SO_q. Since for $n > 2$ the center is precisely I_n when n is odd or $\pm I_n$ otherwise we conclude $\sigma(\tau_x) = \pm \tau_x$. In the $n = 2$ we can use that $\sigma(\tau_x)^2 = I_2$ to get the same result. It is easy to see that $\sigma(\tau_x) = \tau_x$ corresponds to the identity and $\sigma(\tau_x) = -\tau_x$ corresponds to ϕ. This completes the result. □

Proposition 4.1.2. *For the dimension $n \neq 8$ we have that the map:*

$$H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(\mathrm{O}_q)) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{O}_q))$$

which takes a rational conjugacy class to its rational isomorphism class is injective.

Proof. Since $N_{\mathrm{GL}_n}(\mathrm{O}_q) \to \mathrm{Aut}(\mathrm{O}_q)$ factors through $\mathrm{Inn}(\mathrm{O}_q)$ this is simply a basic property of sequence of cohomology attached to the exact sequence:

$$0 \to \mathrm{Inn}(\mathrm{O}_q) \to \mathrm{Aut}(\mathrm{O}_q) \to \mathrm{Aut}(\mathrm{O}_q)/\mathrm{Inn}(\mathrm{O}_q) \to 0$$

which tells us that the kernel of the map $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Inn}(\mathrm{O}_q)) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{O}_q))$ is precisely given by $H^0(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{O}_q)/\mathrm{Inn}(\mathrm{O}_q))/\operatorname{im}\left[H^0(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{O}_q))\right]$. In all cases other than $n = 8$ the group $\mathrm{Aut}(\mathrm{SO}_q)/\mathrm{Inn}(\mathrm{O}_q)$ is trivial as the outer automorphism of SO_q is conjugation by O_q. We thus need only consider the morphism ϕ from the previous claim. The map ϕ is Galois equivariant and thus gives an element of $H^0(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{O}_q))$. It follows from this that:

$$H^0(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{O}_q)/\mathrm{Inn}(\mathrm{O}_q))/\operatorname{im}\left[H^0(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{O}_q))\right]$$

is trivial.

We next consider the exact sequence:

$$0 \to \mathbb{Q}^* \to N_{\mathrm{GL}_n}(\mathrm{O}_q) \to \mathrm{Inn}(\mathrm{O}_q) \to 0$$

Hilbert's Theorem 90 tells us that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(\mathrm{O}_q)) \hookrightarrow H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Inn}(\mathrm{O}_q))$. This completes the result. □

Corollary 4.1.3. *For the dimension $n \neq 8$ we have that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(\mathrm{O}_q))$ classifies the rational isomorphism classes of forms of the orthogonal group which are defined by quadratic forms.*

Proof. We know that any two forms of orthogonal groups for dimension n which are defined by a quadratic form in the usual way are conjugate over $\overline{\mathbb{Q}}$. Thus if we consider the map $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(\mathrm{O}_q)) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{O}_q))$ viewing $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{O}_q))$ as the classifying space for rational forms of orthogonal groups we have the image will contain all those isomorphism classes coming from quadratic forms. That this map is also injective gives the result. □

Remark. If one wanted to handle the cases of $n = 8$ as above one would need to look first at the outer automorphism group $\mathrm{Aut}(\mathrm{SO}_q)/\mathrm{Inn}(\mathrm{SO}_q)$ and determine if

$$H^0(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{SO}_q)/\mathrm{Inn}(\mathrm{SO}_q))/H^0(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(\mathrm{SO}_q))$$

is trivial. To do this one must understand the spin representations as it is exceptional isomorphisms of these that give rise to the extra automorphisms. For example in the $n = 4$ case it was the spin representation that gave us the isomorphism to $\mathrm{SL}_2 \times \mathrm{SL}_2$. One can see that an outer automorphism arises by interchanging the two factors. If one looks at the case $n = 8$, one would find that in general the set may seem not be trivial for the cases $n = 8$ depending on the choice of quadratic form. One then needs to investigate if these automorphisms descend to SO_q.

If they do descend, one might then try to argue that:

$$H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(\mathrm{O}_q)) \hookrightarrow H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Inn}(\mathrm{SO}_q))$$

is not surjective in precisely the cases where we had a kernel in the map with which it would be composed.

Because we have not proved the result for the cases $n = 4, 6, 8$ we shall assume for the remainder of this section that the dimensions of quadratic spaces are not one of these.

Remark. A few final remarks are in order just to give a summary of which cohomology classifies what. We have that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{SO}_q)$ classifies quadratic forms with the same dimension and discriminant as q. We know that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{O}_q)$ classifies quadratic forms of the same dimension as q. The connection between these two facts is that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mu_2)$ classifies quadratic extensions of $\mathbb{Q}$ which is essentially to say it classifies square free integers which are the possible discriminants. We know that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(\mathrm{O}_q) = \mathrm{GO}_q)$ classifies both quadratic forms of the same dimension as q up to rescaling as well as rational conjugacy classes of O_q in GL_n. And we have also just proved that this classifies (for $n \neq 4, 6, 8$) the rational isomorphism classes of the conjugates of O_q in GL_n.

The next thing we would like to describe are the invariants of orthogonal groups that control embeddings. The invariants we are looking at come not directly from the orthogonal groups, but rather from the associated quadratic forms. In order to see to what extent the invariants of an orthogonal group can be tied to those of a defining quadratic form we have the following:

Proposition 4.1.4. *Let $\mathrm{O}_{q_1}, \mathrm{O}_{q_2} \subset \mathrm{GL}_n(\mathbb{C})$ be orthogonal groups defined over $\mathbb{Q}$ with q_1, q_2 any quadratic forms defining them (over $\mathbb{Q}$), then $\mathrm{O}_{q_1} \simeq \mathrm{O}_{q_2}$ over $\mathbb{Q} \Leftrightarrow \exists \lambda \in \mathbb{Q}$ such that $q_1 \sim \lambda q_2$ (over $\mathbb{Q}$).*

Proof. We have that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(\mathrm{O}_q))$ classifies orthogonal groups in dimension n. Moreover we know that $N_{\mathrm{GL}_n}(\mathrm{O}_q)(\mathbb{C}) = \mathbb{C}\,\mathrm{O}_q$.

Now, we know that $\mathrm{O}_q = \mathrm{Aut}(V, q)$ are the automorphisms of V preserving q, additionally we have $\mathbb{C}\,\mathrm{O}_q = \mathrm{Aut}(V, P(q))$ are the automorphisms of V that preserve q up to rescaling. In particular then $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(V, P(q))) = H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(\mathrm{O}_q))$ classifies quadratic spaces up to rescaling of the quadratic form. This gives us the desired correspondence between the forms of orthogonal groups and quadratic forms up to rescaling. □

We would like to consider the conditions on having an orthogonal group be contained in another, however we are only really interested in cases where the embedded orthogonal group is acting as an orthogonal group. As such we make the following non-standard definition:

Definition 4.1.5. Let $\mathrm{O}_q, \mathrm{O}_{q'}$ be the orthogonal groups for the spaces (V, q) and (V', q') respectively. Then $\mathrm{O}_{q'} \subset \mathrm{O}_q$ is a **sub-orthogonal group** if there exists an $\mathrm{O}_{q'}$ stable subspace $U \subset V$ such that $\mathrm{O}_{q'}$ acts faithfully on U, $(U, q|_U)$ is non-degenerate and $\dim(U) = \dim(V')$.

From the above result, we conclude the following general result about the embedding of orthogonal groups:

Proposition 4.1.6. *Let $\mathrm{O}_{q_1}, \mathrm{O}_{q_2}$ be orthogonal groups defined over $\mathbb{Q}$ with q_1, q_2 any quadratic forms defining them (over $\mathbb{Q}$). Then O_{q_2} is a sub-orthogonal group of O_{q_1} if and only if $\exists \lambda \in \mathbb{Q}, q_3$ such that $q_1 \simeq (\lambda q_2) \oplus q_3$ (what we mean is an isomorphism of $\mathbb{Q}$ vector spaces with quadratic forms where the right hand side is the direct sum of spaces).*

Proof. The injection $\mathrm{O}_{q_2} \hookrightarrow \mathrm{O}_{q_1}$ allows us to decompose the vector space on which O_{q_1} is acting into subspace which O_{q_2} acts trivially (V_3) and its orthogonal complement (V_2). Restricting q_1 when restricted to V_2 and V_3 must give quadratic forms q_2' and q_3, by the above result q_2' is a multiple of q_2. This completes the result. (One must of course also make a dimension argument about V_2, V_3). □

Proposition 4.1.7. *Let $\mathrm{O}_{q_1}, \mathrm{O}_{q_2}$ be orthogonal groups over $\mathbb{Q}$ with q_1, q_2 any rational quadratic forms defining them. Let the quadratic forms q_i have invariants d_i, $e_{\nu_p i}$, (r_i, s_i), n_i. Then $\mathrm{O}_{q_1} \simeq \mathrm{O}_{q_2}$ over $\mathbb{Q}$ if and only if $(r_1, s_1) = (r_2, s_2)$ or $(s_1, r_1) = (r_2, s_2)$ (in latter case replace q_1 by $-q_1$ to be in former case for the remainder) and*

- *if $n \equiv 0 (mod 2)$ then $d_1 = d_2$ and $\exists \lambda \in \mathbb{Q}$ such that $e_{\nu_p 1} e_{\nu_p 2} = (\lambda, (-1)^{n/2} d)_{\nu_p}$.*

- *if* $n \equiv 1(mod4)$ *then* $e_{\nu_p 1} = e_{\nu_p 2}$.
- *if* $n \equiv 3(mod4)$ *then* $e_{\nu_p 1}(d_1, d_1)_{\nu_p} = e_{\nu_p 2}(d_2, d_2)_{\nu_p}$.

Proof. By applying our criterion for the isomorphism of Orthogonal groups and the proposition above we immediately get the following conditions:

1. $(r_1, s_1) = (r_2, s_2)$ or $(s_1, r_1) = (r_2, s_2)$
   in the latter case replace q_1 by $-q_1$ to be in former.
2. $\exists \lambda \in \mathbb{Q}$ such that $d_1 = \lambda^n d_2$ and $e_{\nu_p 1} = e_{\nu_p 2}(\lambda, \lambda)_{\nu_p}^{n(n-1)/2}(\lambda, d^{n-1})_{\nu_p}$.

By using the properties of the Hilbert Symbol and the discriminant we arrive at these cases:

- if $n \equiv 0(mod4)$ then $d_1 = d_2$ and $\exists \lambda \in \mathbb{Q}$ such that $e_{\nu_p 1} e_{\nu_p 2} = (\lambda, d)_{\nu_p}$
- if $n \equiv 1(mod4)$ then $e_{\nu_p 1} = e_{\nu_p 2}$
- if $n \equiv 2(mod4)$ then $d_1 = d_2$ and $\exists \lambda \in \mathbb{Q}$ such that $e_{\nu_p 1} e_{\nu_p 2} = (\lambda, -d)_{\nu_p}$
- if $n \equiv 3(mod4)$ then $e_{\nu_p 1} e_{\nu_p 2} = (d_1 d_2, d_1 d_2)_{\nu_p}$

The extra conditions in the first and third case are in fact automatic in many cases by appealing to the existence of rational numbers with given Hilbert symbol. The failure for the existence of a global λ, such that $(\lambda, d)_{\nu_p} = -1$ is an entirely local problem at p and says that $(\lambda, d)_{\nu_p} = 1$ for all $\lambda \in \mathbb{Q}_p$. In particular it would imply d is a square in $\mathbb{Q}_p$. □

Proposition 4.1.8. *Let* $\mathrm{O}_{q_1}, \mathrm{O}_{q_2}$ *be orthogonal groups over* $\mathbb{Q}$ *with* q_1, q_2 *any rational quadratic forms defining them. Let the quadratic forms* q_i *have invariants* d_i, $e_{\nu_p i}$, (r_i, s_i), n_i. *Then we can embed* $\mathrm{O}_{q_2} \hookrightarrow \mathrm{O}_{q_1}$ *as a sub-orthogonal group if and only if* $(r_2, s_2) < (r_1, s_1)$ *or* $(s_2, r_2) < (r_1, s_1)$ *(in the latter case, replace* q_2 *with* $-q_2$*) and further conditions detailed in the proof of the theorem.*

Proof. The literal requirement is $\exists \lambda \in \mathbb{Q}, q_3$ such that $q_1 \simeq (\lambda q_2) \oplus q_3$. In particular this can be checked on the level of invariants. The condition $(r_2, s_2) < (r_1, s_1)$ or $(s_2, r_2) < (r_1, s_1)$ correspond to the signature condition.

The discriminant of $(\lambda q_2) \oplus q_3$ would be: $\lambda^{n_2} d_2 d_3$ thus we must have that:

$$d_3 \lambda^{n_2} = d_1 d_2 (\text{mod squares}).$$

The condition on Hilbert symbols in general is:

$$e_{\nu_p 1} = e_{\nu_p 2} e_{\nu_p 3} (\lambda, \lambda)_{\nu_p}^{n_2(n_2-1)/2} (\lambda^{n_2} d_2, d_3)_{\nu_p} (\lambda, d_2^{n_2-1})_{\nu_p}$$

Supposing now that the signature condition is met we can simplify this in the following cases:

1. $n_1 - n_2 \geq 3$ then take $\lambda = 1$ condition is $d_3 = d_1 d_2$, $e_{\nu_p 3} = e_{\nu_p 1} e_{\nu_p 2} (d_2, -d_1)_{\nu_p}$.
   Condition for the existence of quadratic form is automatic in this case.
2. $n_1 - n_2 = 2$
   (a) $n_1 \cong 0$ $(mod4)$: Then $d_3 = d_1 d_2$, $e_{\nu_p 3} = e_{\nu_p 1} e_{\nu_p 2} (d_2, -d_1)_{\nu_p} (\lambda, -1)_{\nu_p} (d_2, \lambda)_{\nu_p}$
   Requirement is $\forall p$ with $d_1 d_2 = -1$ in $\mathbb{Q}_p / \mathbb{Q}_p^2$ then $\exists \lambda_p \in Q_p$ with

   $$(\lambda_p, -d_2)_{\nu_p} = e_{\nu_p 1} e_{\nu_p 2} (d_2, -d_1)_{\nu_p}$$

   Or equivalently $d_1 d_2 = -1$ in $\mathbb{Q}_p / \mathbb{Q}_p^2$ implies $d_2 \neq -1$ in $\mathbb{Q}_p / \mathbb{Q}_p^2$
   (b) $n_1 \cong 1$ $(mod4)$ Then $d_3 \lambda = d_1 d_2$, $e_{\nu_p 3} = e_{\nu_p 1} e_{\nu_p 2} (d_2, -d_1)_{\nu_p} (\lambda, -1)_{\nu_p} (d_2, \lambda)_{\nu_p}$
   Then take $\lambda = d_1 d_2$ and condition the condition is then automatic.
   (c) $n_1 \cong 2$ $(mod4)$ Then $d_3 = d_1 d_2$, $e_{\nu_p 3} = e_{\nu_p 1} e_{\nu_p 2} (d_2, -d_1)_{\nu_p} (d_2, \lambda)_{\nu_p}$
   Requirement is $\forall p$ with $d_1 d_2 = -1$ in $\mathbb{Q}_p / \mathbb{Q}_p^2$ then $\exists \lambda_p \in Q_p$ with

   $$(\lambda_p, d_2)_{\nu_p} = e_{\nu_p 1} e_{\nu_p 2} (d_2, -d_1)_{\nu_p}$$

Or equivalently $d_1d_2 = -1$ in $\mathbb{Q}_p/\mathbb{Q}_p^2$ implies $d_2 \neq 1$ in $\mathbb{Q}_p/\mathbb{Q}_p^2$

(d) $n_1 \cong 3\ (mod 4)$ Then $d_3\lambda = d_1d_2$, $e_{\nu_p 3} = e_{\nu_p 1}e_{\nu_p 2}(d_2, -d_1)_{\nu_p}(d_2, \lambda)_{\nu_p}$
Then take $\lambda = d_1d_2$ and condition the condition is then automatic.

3. $n_1 - n_2 = 1$
   (a) $n_1 \cong 0\ (mod 4)$: Then $d_3\lambda = d_1d_2$, $e_{\nu_p 3} = e_{\nu_p 1}e_{\nu_p 2}(d_2, -d_1)_{\nu_p}(\lambda, -1)_{\nu_p}(d_2, \lambda)_{\nu_p}$
   Requirement is $\forall p \exists \lambda_p$ with $(\lambda_p, -d_2)_{\nu_p} = e_{\nu_p 1}e_{\nu_p 2}(d_2, -d_1)_{\nu_p}$
   (b) $n_1 \cong 1\ (mod 4)$: Then $d_3 = d_1d_2$, $e_{\nu_p 3} = e_{\nu_p 1}e_{\nu_p 2}(d_2, -d_1)_{\nu_p}(d_2, \lambda)_{\nu_p}$
   Requirement is $\forall p \exists \lambda_p$ with $(\lambda_p, d_2)_{\nu_p} = e_{\nu_p 1}e_{\nu_p 2}(d_2, -d_1)_{\nu_p}$
   (c) $n_1 \cong 2\ (mod 4)$: Then $d_3\lambda = d_1d_2$, $e_{\nu_p 3} = e_{\nu_p 1}e_{\nu_p 2}(d_2, -d_1)_{\nu_p}(d_2, \lambda)_{\nu_p}$
   Requirement is $\forall p \exists \lambda_p$ with $(\lambda_p, d_2)_{\nu_p} = e_{\nu_p 1}e_{\nu_p 2}(d_2, -d_1)_{\nu_p}$
   (d) $n_1 \cong 3\ (mod 4)$: Then $d_3 = d_1d_2$, $e_{\nu_p 3} = e_{\nu_p 1}e_{\nu_p 2}(d_2, -d_1)_{\nu_p}(\lambda, -1)_{\nu_p}(d_2, \lambda)_{\nu_p}$
   Requirement is $\forall p \exists \lambda_p$ with $(\lambda_p, -d_2)_{\nu_p} = e_{\nu_p 1}e_{\nu_p 2}(d_2, -d_1)_{\nu_p}$
4. $n_1 = n_2$ then as in the previous theorem.

□

The cases in the above that we are most interested in are those where n_2 is even. This is because it is more natural to first embed tori into even dimension orthogonal groups. The case where we have $n_1 = n_2 + 1$ really describes the extra sort of freedom we have when trying to embed tori into orthogonal groups of odd dimension. In comparison to the $n_1 = n_2$ case we have essentially removed the condition that the discriminants be equal and are left only with a lesser condition on Witt invariants. One can in a sense view this as replacing a condition about having the same ramification and splitting behavior at all primes with one about the quadratic forms having the same splitting behavior whenever a prime splits over either $\sqrt{d_2}$ or $\sqrt{-d_2}$ as appropriate. In the $n_1 = n_2 + 2$ case we have even milder conditions. The $n_1 - n_2 \geq 3$ case tells us that any 'small' CM-algebra will always be embeddable into a sufficiently large orthogonal group. Though there are still conditions on what one can pair such a CM-algebra with so that it becomes a maximal torus.

4.2 Quadratic forms for the Tori $R_{K/\mathbb{Q}}(R^{(1)}_{E/K}(\mathbb{G}_m))$

We will now look at a particular set of examples of tori and the orthogonal groups into which they embed.

Consider a CM-field $E/\mathbb{Q}$ (of degree $2n$), with maximal totally real subfield K (so $E = K(\sqrt{\delta})$ where δ is a totally negative). Fix an element $\lambda \in K$ then viewing E as a $\mathbb{Q}$-vector space we get the quadratic form q_λ on E attached to the bilinear form $B_\lambda(x, y) := Tr_{E/\mathbb{Q}}(\lambda x\overline{y})$.

Now we can fix two basis for $K/\mathbb{Q}$. Let $a_1, \ldots, a_n$ be such that $B_\lambda(a_i, a_j) = 0$ for $i \neq j$ and $a'_1, \ldots, a'_n$ be such that $B_{-\lambda\delta}(a'_i, a'_j) = 0$. Then $a_1, \ldots, a_n, a'_1\sqrt{\delta}, \ldots, a'_n\sqrt{\delta}$ is a basis for $E/\mathbb{Q}$ with respect to which the matrix for q_λ will be of the form $diag(2Tr_{K/\mathbb{Q}}(\lambda a_i^2)_{i=1..n}, 2Tr_{K/\mathbb{Q}}(-\lambda\delta a_i'^2)_{i=1..n})$. In particular, if we define a quadratic Q form on K via the bilinear form$Q_\alpha(x, y) := Tr_{K/\mathbb{Q}}(\alpha xy)$ then q_λ decomposes as $q_\lambda = 2Q_\lambda \oplus 2Q_{-\lambda\delta}$ via the natural decomposition $E = K \oplus K\sqrt{\delta}$. So to study the invariants of q_λ it shall suffice to look at the invariants of Q_α and combine them appropriately.

One thing to observe about q_λ (which explains our interest in it) is that the algebraic tori $R_{K/\mathbb{Q}}(R^{(1)}_{E/K}(\mathbb{G}_m))$ embeds naturally into O_{q_λ} for any choice of $\lambda \in K$. So that this construction then gives us a method of embedding these tori into not just one, but instead a family of orthogonal groups.

We now go about describing the invariants of the form Q_α. We recall that the important invariants of a quadratic form Q are its discriminant $D(Q) \in \mathbb{Q}/\mathbb{Q}^2 \cong H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})), \mathbb{Z}/2\mathbb{Z})$, it's

Hasse-Witt invariants, which can either be viewed as the collection $e_\nu \in \{\pm 1\}$ for each valuation ν of $\mathbb{Q}$ or as $W(Q) \in H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$, and finally its signature $(r, s) \in \mathbb{N} \otimes \mathbb{N}$. We shall use the following result of Serre "Invariant de Witt de la forme $Tr(x^2)$" [Ser84].

Theorem 4.2.1. *[Ser84]*
The quadratic form Q_α has the following invariants:
$D(Q_\alpha) = N_{K/\mathbb{Q}}(\alpha)$
$W(Q_\alpha) = e^*_\alpha(s'_n) + (2)(d_K)$
The signature is (#of positive embeddings of α, #of negative embeddings of α).

Remark. We now define the various terms that appear in the statement of the theorem:

d_K is the discriminant of the field $K/\mathbb{Q}$.

(x) is the element of $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$ corresponding to $x \in \mathbb{Q}^*/\mathbb{Q}^{*2}$.

$(x)(y)$ means the cup product as an element of $H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$.

Now if $\sigma_1, \ldots, \sigma_n$ are the embeddings of K in $\mathbb{C}$, and $\pm\beta_i$ the square roots of $\sigma_i(\alpha)$. Then we may map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to S(n, 2)$ (where $S(n, 2)$ are the Schur multipliers [DM74]) via the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\pm\beta_i$. $e^* : H^2(S(n, 2), \mathbb{Z}/2\mathbb{Z}) \to H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$ is then the map induced from $e : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to S(n, 2)$.

The element $s'_n \in H^2(S(n, 2), \mathbb{Z}/2\mathbb{Z})$ corresponds to a specific central extension of $S(n, 2)$. The complete description of the cohomology $H^2(S(n, 2), \mathbb{Z}/2\mathbb{Z})$ can be found in [DM74], we shall only describe the element s'_n which we need.

The group $S(n, 2)$ can be described as $(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$ where this is a semi-direct product with S_n acting as permutations on the $(\mathbb{Z}/2\mathbb{Z})^n$. This can be described in terms of generators and relations as:

$r_i, i = 1..(n-1)$ corresponds to $(i, i+1) \in S_n$ and $w_i, i = 1..n$ corresponds to 1 in the i^{th} copy of $\mathbb{Z}/2\mathbb{Z}$. $r_i^2 = 1$, $r_i r_{i+1}^3 = (r_i r_j)^2 = 1$ for $j \neq i, i+1$, $w_i^2 = 1$, $w_j w_i = w_i w_j$, $r_i w_i = w_{i+1} r_i$, $r_i w_j = w_j r_i$ for $j \neq i, i+1$.

The central extension we would like to consider we shall denote A and is the one whose generators are the same as before except with the inclusion of (-1) which shall commute with all other generators. We modify the other relations as follows:

$r_i^2 = 1$, $r_i r_{i+1}^3 = 1$, $(r_i r_j)^2 = -1$ for $j \neq i, i+1$, $w_j w_i = (-1) w_i w_j$ for $j \neq i, i+1$, $r_i w_i = w_{i+1} r_i$, $r_i w_j = (-1) w_j r_i$ for $j \neq i, i+1$.

The actual proof of Serre's result involves reducing to the case $\alpha = 1$ by replacing K by $E = K[X]/(X^2 - \alpha)$ and observing that:

$$Q_{E,1} \simeq 2Q_{K,1} \oplus 2Q_{K,\alpha}$$

and proceeding to relate the invariants of the participating quadratic forms.

The proof for the case $\alpha = 1$ in the general case is fairly technical.

We now proceed to compute the invariants for the form we were originally interested in $q_\lambda(x, y)$. Using that $q_\lambda = 2Q_\lambda \oplus 2Q_{-\lambda\delta}$ and the properties of combining invariants for direct sums we find the following:

Claim. *With notation as above, the invariants of the quadratic form $q_\lambda = Tr_{E/\mathbb{Q}}(\lambda x \bar{x})$ are:*

$$\begin{aligned}
D(q_\lambda) &= 2^{2n} N_{K/\mathbb{Q}}(\lambda) N_{K/\mathbb{Q}}(-\lambda\delta) = N_{K/\mathbb{Q}}(-\delta) \\
W(q_\lambda) &= e^*_\lambda(s'_n) + (2)(d_K) + e^*_{-\lambda\delta}(s'_n) + (2)(d_K) + (D(2Q_\lambda))(D(2Q_{-\lambda\delta})) \\
&= e^*_\lambda(s'_n) + e^*_{-\lambda\delta}(s'_n) + (2^n N_{K/\mathbb{Q}}(\lambda))(2^n N_{K/\mathbb{Q}}(-\lambda\delta)) \\
&= e^*_\lambda(s'_n) + e^*_{-\lambda\delta}(s'_n) + (2^n N_{K/\mathbb{Q}}(\lambda))(-N_{K/\mathbb{Q}}(-\delta))
\end{aligned}$$

The signature is (2× #of negative embeddings of λ,2× #of positive embeddings of λ).

What the above result tells us, is that given some quadratic form q in order to verify that the associated orthogonal group is equivalent to the one coming from a quadratic form of the shape $Tr_{E/\mathbb{Q}}(\lambda x\overline{x})$ then one needs to find a totally real field K of degree n which contains a totally negative δ such that $N_{K/\mathbb{Q}}(-\delta) = d_q$. In addition, the field must contain an element λ that provides for the correct Witt invariants. It is entirely unclear that any such field or elements δ, λ will always exist.

Example. We present briefly the example of how to use the formula in the case of dimension 4. That is where we have a real quadratic extension $K = \mathbb{Q}(\sqrt{D})$ a totally negative element δ and an arbitrary element λ in K.

One of the first things we might try to do is to evaluate a cocycle representative of $e^*_\lambda(s'_n)(\sigma, \tau)$, to do this we must fix a section $\phi : S(2,2) \to A$ (this shall not be a homomorphism). We then have that for a representative of the cohomology class we can compute:

$$e^*_\lambda(s'_n)(\sigma, \tau) = \phi(e(\sigma))\phi(e(\tau))\phi(e(\sigma\tau)^{-1}) = \pm 1.$$

What we see is that this element essentially detects the extent to which σ, τ commute less in A than in $S(2,2)$. We observe that in the case of $n = 2$ the only new failure to commute is in w_1, w_2 so when describing our section it is enough to specify a canonical ordering of w_1, w_2 for describing words in $S(2,2)$ we choose the natural lexical order. We can then check for example that: $e^*_\lambda(s'_n)(w_1, w_2) = -1$, $e^*_\lambda(s'_n)(w_2, w_1) = 1$, $e^*_\lambda(s'_n)(w_1w_2, w_1) = -1$, ...

We next wish to know when such a cocycle is in a non-trivial class of $H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$. By inspecting the coboundary condition we make the observation that because $e^*_\lambda(s'_n)(w_1, w_2) \neq e^*_\lambda(s'_n)(w_2, w_1)$ so that provided $w_1, w_2 \in \mathrm{im}(e)$ we will have that the cocycle is non-trivial. We remark that such a condition implies $\lambda \in K \setminus \mathbb{Q}$ and $\lambda \in K \setminus K^2$. By checking all the cases one can establish that this is in fact a necessary and sufficient condition for $e^*_\lambda(s'_n)$ to be non-trivial.

The above tells us a bit about the global perspective on how to view the formula. What we would like to do next is to give the local interpretation, that is to describe how to extract the local Hasse-Witt invariants e_{ν_p}. The most naive thing to try is to simply apply the above directly with $\lambda \in \mathbb{Q}_p(\sqrt{D})$. This of course does not really make sense, what you really want to do is study the situation in the localization of $K = \mathbb{Q}(\sqrt{D})$ at the prime ideal p. It turns out that Serre's Theorem above is true as stated for étale extensions of algebras over fields of characteristic not 2. So provided that $\mathbb{Q}(\sqrt{D})_p$ is étale over $\mathbb{Q}_p$, all the analysis above tells us precisely how to interpret all the terms in the formula and thus compute e_{ν_p}. The only difficulty that remains is the cases where $\mathbb{Q}(\sqrt{D})_p$ is not étale, that is the cases where $p|D$ so that the extension is ramified.

To see the explicit computations of the Hasse-Witt invariants for this case see 4.3 (page 67).

4.3 The Hilbert Modular Case and $O(2,2)$

In this section we will do some explicit computations to relate the classical results of the Hilbert Modular Case with that of the case $O(2,2)$.

Notation

For the remainder of this section, we fix the following notation:
Let $D \in \mathbb{Z}^+$ be a square free positive integer.
Let $K = \mathbb{Q}(\sqrt{D})$.
Let $\delta = \delta_1 + \delta_2\sqrt{D} \in K$ be a totally positive element of K ($\delta' = \delta_1 - \delta_2\sqrt{D}$ and $\delta, \delta' > 0$).
Let $\lambda \in K$.
Let $F = K(\sqrt{-\delta})$.

Let N be the normal closure of F.

Fix once and for all, an embedding $N \hookrightarrow \mathbb{C}$ so that we may think of the elements of $\mathrm{Gal}(N/\mathbb{Q})$ as both automorphisms of N but also as the various embeddings of N into $\mathbb{C}$.

Remark. N will be a CM-field of degree 4 or 8, this will be shown and the cases analyzed a bit later

The Torus $F^{(1)}$

We consider the algebraic torus $F^{(1)} := R_{K/\mathbb{Q}}(R^{(1)}_{F/K}(\mathbb{G}_m))$ of complex norm 1 elements of F. We shall first look at the restriction of scalars down to K.

$$R^{(1)}_{F/K}(\mathbb{G}_m)(K) = \{a + b\sqrt{-\delta} | a, b \in K, (a + b\sqrt{-\delta})(a - \sqrt{-\delta}) = a^2 + \delta b^2 d = 1\}.$$

The general construction of restriction of scalars gives us:

$$R^{(1)}_{F/K}(\mathbb{G}_m) \simeq \left\{ M = \left(\begin{smallmatrix} a & -\delta b \\ b & a \end{smallmatrix}\right) | Det(M) = 1 \right\} = \left\{ \frac{1}{2} \left(\begin{smallmatrix} t+\frac{1}{t} & \sqrt{-\delta}(t-\frac{1}{t}) \\ \frac{1}{\sqrt{-\delta}}(t-\frac{1}{t}) & t+\frac{1}{t} \end{smallmatrix} \right) \right\}.$$

Remark. The field in which a, b, t lie in the above depend on the ring in which you are trying to take points. For the K points, a, b would be in K but t would be in F.
The map between the two interpretations has $t = a + b\sqrt{-\delta}$, t in particular then generates the character module of $R^{(1)}_{F/K}(\mathbb{G}_m)$.

We will now explicitly diagonalize this torus over F. The above representation comes from the action of F on F as a K vector space with basis $\{1, \sqrt{-\delta}\}$. To diagonalize we need to find the eigenvectors of the action on $F \otimes_K F$. Indeed we get that $M_t \in R^{(1)}_{F/K}(\mathbb{G}_m)$ acts as t on the vector $(\sqrt{-\delta}, 1)$ and as $\frac{1}{t}$ on $(-\sqrt{-\delta}, 1)$. So then, if we take $\{(\sqrt{-\delta}, 1), (-\sqrt{-\delta}, 1)\}$ for a basis of $F \otimes_K F$ we get:

$$R^{(1)}_{F/K}(\mathbb{G}_m)_F \simeq \left\{ \frac{1}{2} \left(\begin{smallmatrix} t & 0 \\ 0 & \frac{1}{t} \end{smallmatrix} \right) \right\}.$$

We now wish to perform the further restriction down to $\mathbb{Q}$. If we then take a basis of $K/\mathbb{Q}$ $\{1, \sqrt{D}\}$, then perform the restriction of scalars we have:

$$t = \frac{r}{2} \begin{pmatrix} s + \frac{1}{s} & \sqrt{D}(s - \frac{1}{s}) \\ \frac{1}{\sqrt{D}}(s - \frac{1}{s}) & s + \frac{1}{s} \end{pmatrix}$$

$$\frac{1}{t} = \frac{1}{2r} \begin{pmatrix} s + \frac{1}{s} & \sqrt{D}(\frac{1}{s} - s) \\ \frac{-1}{\sqrt{D}}(s - \frac{1}{s}) & s + \frac{1}{s} \end{pmatrix}$$

$$\sqrt{-\delta} = \begin{pmatrix} \sqrt{-\delta} + \sqrt{-\delta'} & \sqrt{D}(\sqrt{-\delta} - \sqrt{-\delta'}) \\ \frac{1}{\sqrt{D}}(\sqrt{-\delta} - \sqrt{-\delta'}) & \sqrt{-\delta} + \sqrt{-\delta'} \end{pmatrix}.$$

We then get that if we had taken as a basis for $F/\mathbb{Q}$ the elements $\{1, \sqrt{D}, \sqrt{-\delta}, \sqrt{-\delta D}\}$ we would have $F^{(1)}$ is:

$$\frac{1}{4} \begin{pmatrix} rs + \frac{r}{s} + \frac{s}{r} + \frac{1}{sr} & \sqrt{D}(rs - \frac{r}{s} - \frac{s}{r} + \frac{1}{sr}) & \sqrt{-\delta}(rs - \frac{1}{sr}) + \sqrt{-\delta'}(\frac{r}{s} - \frac{s}{r}) & \sqrt{-\delta D}(rs - \frac{1}{sr}) + \sqrt{-\delta' D}(-\frac{r}{s} + \frac{s}{r}) \\ \frac{1}{\sqrt{D}}(rs - \frac{r}{s} - \frac{s}{r} + \frac{1}{sr}) & rs + \frac{r}{s} + \frac{s}{r} + \frac{1}{sr} & \frac{\sqrt{-\delta}}{\sqrt{D}}(rs - \frac{1}{sr}) + \frac{\sqrt{-\delta'}}{\sqrt{D}}(-\frac{r}{s} + \frac{s}{r}) & \sqrt{-\delta}(rs - \frac{1}{sr}) + \sqrt{-\delta'}(\frac{r}{s} - \frac{s}{r}) \\ \frac{1}{\sqrt{-\delta}}(rs - \frac{1}{sr}) + \frac{1}{\sqrt{-\delta'}}(\frac{r}{s} - \frac{s}{r}) & \frac{\sqrt{D}}{\sqrt{-\delta}}(rs - \frac{1}{sr}) + \frac{\sqrt{D}}{\sqrt{-\delta'}}(-\frac{r}{s} + \frac{s}{r}) & rs + \frac{r}{s} + \frac{s}{r} + \frac{1}{sr} & \sqrt{D}(rs - \frac{r}{s} - \frac{s}{r} + \frac{1}{sr}) \\ \frac{1}{\sqrt{-\delta D}}(rs - \frac{1}{sr}) + \frac{1}{\sqrt{-\delta' D}}(-\frac{r}{s} + \frac{s}{r}) & \frac{1}{\sqrt{-\delta}}(rs - \frac{1}{sr}) + \frac{1}{\sqrt{-\delta'}}(+\frac{r}{s} - \frac{s}{r}) & \frac{1}{\sqrt{D}}(rs - \frac{r}{s} - \frac{s}{r} + \frac{1}{sr}) & rs + \frac{r}{s} + \frac{s}{r} + \frac{1}{sr} \end{pmatrix}.$$

Alternatively, we might prefer to perform the restriction straight from F down to $\mathbb{Q}$. Consider the element $w = w_1 + w_2\sqrt{D} + w_3\sqrt{-\delta} + w_4\sqrt{-\delta D} \in F$ with $w\overline{w} = 1$. Then w gives us an element

$t_w \in F^{(1)}$. Firstly in $R^{(1)}_{F/K}(\mathbb{G}_m)$ we get:

$$t_w = \begin{pmatrix} w_1 + w_2\sqrt{D} & -\delta(w_3 + w_4\sqrt{D}) \\ w_3 + w_4\sqrt{D} & w_1 + w_2\sqrt{D} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} w + \frac{1}{w} & \sqrt{-\delta}(w - \frac{1}{w}) \\ \frac{1}{\sqrt{-\delta}}(w - \frac{1}{w}) & w + \frac{1}{w} \end{pmatrix}$$

To perform the restriction down to $\mathbb{Q}$ is to do it componentwise, this then gives:

$$t_w = \begin{pmatrix} w_1 & Dw_2 & -\delta_1 w_3 - D\delta_2 w_4 & -D(\delta_1 w_4 + \delta_2 w_3) \\ w_2 & w_1 & -\delta_1 w_4 - \delta_2 w_3 & -\delta_1 w_3 - D\delta_2 w_4 \\ w_3 & Dw_4 & w_1 & Dw_2 \\ w_4 & w_3 & w_2 & w_1 \end{pmatrix}.$$

To compare this to the previous version, set:

$$\begin{aligned} r_w^2 &= "N_{K/Q}(w)" = (w_1 + w_3\sqrt{-\delta} + w_2\sqrt{D} + w_4\sqrt{-\delta D})(w_1 + w_3\sqrt{-\delta'} - w_2\sqrt{D} - w_4\sqrt{-\delta' D}) \\ &= (w_1 + w_3\sqrt{-\delta})^2 - D(+w_2 + w_4\sqrt{-\delta})^2 \\ s_w &= w/r_w, \\ w' &= (w_1 + w_3\sqrt{-\delta'} - w_2\sqrt{D} - w_4\sqrt{-\delta' D}) \end{aligned}$$

then we will have $1/w' = \overline{w'}$. We see that:

$$\begin{aligned} r_w s_w + \frac{r_w}{s_w} + \frac{s_w}{r_w} + \frac{1}{s_w r_w} &= \frac{r_w w}{r_w} + \frac{r_w^2}{w} + \frac{w}{r_w^2} + \frac{r_w}{r_w w} \\ &= w + ww'/w + w/ww' + 1/w \\ &= w + w' + 1/w' + 1/w \\ &= 2w_1 + 2w_2\sqrt{D} + w' + \overline{w'} \\ &= 4w_1. \end{aligned}$$

One can check that the other components also agree. In particular this tells you how to interpret the characters r, s of our torus.

We now wish to diagonalize this torus, to do this, we need to work over N since it is over this field that the torus splits. If we choose instead the basis of $K \otimes_{\mathbb{Q}} K$ of $\{(\sqrt{D}, 1), (-\sqrt{D}, 1)\}$ The t's would become:

$$t = r\begin{pmatrix} s & 0 \\ 0 & \frac{1}{s} \end{pmatrix}, \frac{1}{t} = \frac{1}{r}\begin{pmatrix} \frac{1}{s} & 0 \\ 0 & s \end{pmatrix}.$$

So, if we choose as a basis of $F \otimes_{\mathbb{Q}} N$ the elements:

$$\begin{aligned} \{v_1 &= (\sqrt{-\delta D}, \sqrt{-\delta}, \sqrt{D}, 1), & v_2 &= (\sqrt{-\delta' D}, -\sqrt{-\delta'}, \sqrt{D}, -1), \\ v_3 &= (\sqrt{-\delta D}, \sqrt{-\delta}, -\sqrt{D}, -1), & v_4 &= (\sqrt{-\delta' D}, -\sqrt{-\delta'}, -\sqrt{D}, 1)\}. \end{aligned}$$

Then we have:

$$F^{(1)}{}_N \simeq \left\{ \begin{pmatrix} rs & 0 & 0 & 0 \\ 0 & \frac{r}{s} & 0 & 0 \\ 0 & 0 & \frac{1}{rs} & 0 \\ 0 & 0 & 0 & \frac{s}{r} \end{pmatrix} \right\} = \left\{ \begin{pmatrix} w & 0 & 0 & 0 \\ 0 & w' & 0 & 0 \\ 0 & 0 & \overline{w} & 0 \\ 0 & 0 & 0 & \overline{w'} \end{pmatrix} \right\}.$$

We are now in a position to say something about which orthogonal groups such a torus can lie in. In particular, if $F_N^{(1)} \subset O_q$, then having extended scalars to N and performed the change of basis as above we get we must have:

$$q(x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4) = ax_1x_3 + bx_2x_4.$$

For example the map $Tr_{F/\mathbb{Q}} \circ N_{F/K}$ gives a quadratic form on F (as a $\mathbb{Q}$-vector space) which is preserved by $F^{(1)}$ under the regular representation. We now compute what this quadratic form looks like in terms of this other basis. (the "" in the formulas indicate that the operator has been linearly extended and is not literally the trace or norm map).

$$\begin{aligned}
&"Tr_{F/\mathbb{Q}} \circ N_{F/K}"(x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4)\\
&\quad =2(\sqrt{-\delta D}(x_1 + x_3) + \sqrt{-\delta' D}(x_2 + x_4))^2 + D(\sqrt{-\delta}(x_1 + x_3) - \sqrt{-\delta'}(x_2 + x_4))^2\\
&\qquad + \delta_1((\sqrt{D}(x_1 + x_2 - x_3 - x_4))^2 + D(x_1 - x_2 - x_3 + x_4)^2)\\
&\qquad + \delta_2(2D\sqrt{D}(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 - x_3 + x_4))\\
&\quad =2D(-\delta(x_1 + x_3)^2 + 2\sqrt{\delta\delta'}(x_1 + x_3)(x_2 + x_4) - \delta'(x_2 + x_4)^2\\
&\qquad - \delta(x_1 + x_3)^2 - 2\sqrt{\delta\delta'}(x_1 + x_3)(x_2 + x_4) - \delta'(x_2 + x_4)^2)\\
&\qquad + \delta_1(D(x_1 + x_2 - x_3 - x_4)^2 + D(x_1 - x_2 - x_3 + x_4)^2)\\
&\qquad + 2\delta_2 D\sqrt{D}(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 - x_3 + x_4)\\
&\quad = - 4\delta_1 D((x_1 + x_3)^2 + (x_2 + x_4)^2) - 4\delta_2 D\sqrt{D}((x_1 + x_3)^2 - (x_2 + x_4)^2)\\
&\qquad + 2\delta_1 D((x_1 + x_2 - x_3 - x_4)^2 + (x_1 - x_2 - x_3 + x_4)^2)\\
&\qquad + 4\delta_2 D\sqrt{D}(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 - x_3 + x_4)\\
&\quad =2\delta_1 D(-8x_1x_3 - 8x_2x_4) + 4\delta_2 D\sqrt{D}(-4x_1x_3 - 4x_2x_4)\\
&\quad = - 16D\delta(x_1x_3 + x_2x_4).
\end{aligned}$$

Which we note, is of the allowable form.

We will now try to "undo" the above computation and express the candidate quadratic form:

$$q(x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4) = ax_1x_3 + bx_2x_4$$

from above in terms of the usual rational basis $e_1 = (1, 0, 0, 0), \ldots, e_4 = (0, 0, 0, 1)$. We have that:

$$e_1 = \frac{1}{4}\left(\frac{1}{\sqrt{-\delta D}}(v_1 + v_3) + \frac{1}{\sqrt{-\delta' D}}(v_2 + v_4)\right) \qquad e_2 = \frac{1}{4}\left(\frac{1}{\sqrt{-\delta}}(v_1 + v_3) - \frac{1}{\sqrt{-\delta'}}(v_2 + v_4)\right)$$

$$e_3 = \frac{1}{4\sqrt{D}}(v_1 - v_3 + v_2 - v_4) \qquad e_4 = \frac{1}{4}(v_1 - v_3 - v_2 + v_4)$$

and so we can compute that:

$$q(e_1) = \left(\frac{-1}{16D}\right)\left(\frac{a}{\delta} + \frac{b}{\delta'}\right) \qquad q(e_2) = \left(\frac{-1}{16}\right)\left(\frac{a}{\delta} + \frac{b}{\delta'}\right)$$
$$q(e_3) = \left(\frac{-1}{16D}\right)(a+b) \qquad q(e_4) = \left(\frac{-1}{16}\right)(a+b)$$
$$q(e_1+e_3) = \left(\frac{-1}{16D}\right)\left(\frac{1+\delta}{\delta}a + \frac{1+\delta'}{\delta'}b\right) \qquad q(e_1+e_2) = \left(\frac{-1}{16D}\right)\left(\frac{(1+\sqrt{D})^2}{\delta}a + \frac{(1-\sqrt{D})^2}{\delta'}b\right)$$
$$q(e_1+e_4) = \left(\frac{-1}{16D}\right)\left(\frac{1+\delta D}{\delta}a + \frac{1+\delta' D}{\delta'}b\right) \quad q(e_2+e_3) = \left(\frac{-1}{16D}\right)\left(\frac{D+\delta}{\delta}a + \frac{D+\delta'}{\delta'}b\right)$$
$$q(e_2+e_4) = \left(\frac{-1}{16}\right)\left(\frac{1+\delta}{\delta}a + \frac{1+\delta'}{\delta'}b\right) \qquad q(e_3+e_4) = \left(\frac{-1}{16D}\right)\left((1+\sqrt{D})^2 a + (1-\sqrt{D})^2 b\right)$$

And then evaluating the bilinear pairing yields:

$$(e_1,e_2) = \left(\frac{-1}{16D}\right)\left(\left(\frac{(1+\sqrt{D})^2}{\delta}a + \frac{(1-\sqrt{D})^2}{\delta'}b\right) - \left(\frac{a}{\delta}+\frac{b}{\delta'}\right) - D(\frac{a}{\delta}+\frac{b}{\delta'})\right) = \frac{-1}{8\sqrt{D}}\left(\frac{a}{\delta}-\frac{b}{\delta'}\right)$$
$$(e_1,e_3) = \left(\frac{-1}{16D}\right)\left(\left(\frac{1+\delta}{\delta}a + \frac{1+\delta'}{\delta'}b\right) - \left(\frac{a}{\delta}+\frac{b}{\delta'}\right) - (a+b)\right) = 0$$
$$(e_1,e_4) = \left(\frac{-1}{16D}\right)\left(\left(\frac{1+\delta D}{\delta}a + \frac{1+\delta' D}{\delta'}b\right) - \left(\frac{a}{\delta}+\frac{b}{\delta'}\right) - D(a+b)\right) = 0$$
$$(e_2,e_3) = \left(\frac{-1}{16D}\right)\left(\left(\frac{D+\delta}{\delta}a + \frac{D+\delta'}{\delta'}b\right) - D\left(\frac{a}{\delta}+\frac{b}{\delta'}\right) - (a+b)\right) = 0$$
$$(e_2,e_4) = \left(\frac{-1}{16}\right)\left(\left(\frac{1+\delta}{\delta}a + \frac{1+\delta'}{\delta'}b\right) - \left(\frac{a}{\delta}+\frac{b}{\delta'}\right) - (a+b)\right) = 0$$
$$(e_3,e_4) = \left(\frac{-1}{16D}\right)\left(\left((1+\sqrt{D})^2 a + (1-\sqrt{D})^2 b\right) - (a+b) - D(a+b)\right) = \frac{-1}{8\sqrt{D}}(a-b).$$

In particular we then have:

$$q(y_1e_1+\cdots+y_4e_4) = \frac{-1}{16D}\Big[\left(\frac{a}{\delta}+\frac{b}{\delta'}\right)y_1^2 + D\left(\frac{a}{\delta}+\frac{b}{\delta'}\right)y_2^2 + (a+b)y_3^3 + D(a+b)y_4^2 + 2\left(\frac{a}{\delta}-\frac{b}{\delta'}\right)\sqrt{D}y_1y_2 + 2\sqrt{D}(a-b)y_3y_4\Big].$$

Rescaling a, b allows us to write:

$$q(y_1e_1+\cdots+y_4e_4) = (a+b)y_1^2 + 2\sqrt{D}(a-b)y_1y_2 + D(a+b)y_2^2 + (a\delta+b\delta')y_3^3 + 2\sqrt{D}(a\delta-b\delta')y_3y_4 + D(a\delta+b\delta')y_4^2.$$

But we are interested in forms with rational coefficients and the requirement for this is that $(a+b), \sqrt{D}(a-b) \in \mathbb{Q}$. But then this implies that we get $a = b + r\sqrt{D}$ and thus $2b + r\sqrt{D} \in \mathbb{Q}$. We conclude that $b = s - \frac{r}{2}\sqrt{D}$ and $a = s + \frac{r}{2}\sqrt{D}$ for $s, r \in \mathbb{Q}$. In particular we have $b = a'$ and so we can rewrite this as:

$$q(y_1e_1+\cdots+y_4e_4) = (a+a')y_1^2 + 2\sqrt{D}(a-a')y_1y_2 + D(a+a')y_2^2 + (a\delta+a'\delta')y_3^3 + 2\sqrt{D}(a\delta-a'\delta')y_3y_4 + D(a\delta+a'\delta')y_4^2.$$

The requirement that $(a\delta + a'\delta'), \sqrt{D}(a\delta - a'\delta') \in \mathbb{Q}$ is then automatic.

We notice that this is up to a multiple of 2 the form $Tr_{F/\mathbb{Q}}(ax\overline{x})$. In particular, we have shown that, for $F^{(1)}$ acting via the regular representation, these trace forms are the only quadratic forms that $F^{(1)}$ can preserve.

The Forms $Tr_{F/\mathbb{Q}}(\lambda N_{F/K}(x))$

We have previously worked out the invariants of these forms for the more general case, We will do it here more explicitly for the specific case we are looking at.

Choosing basis F/Q of the form $a_1, a_2, a_3\sqrt{-\delta}, a_4\sqrt{-\delta}$ with $a_i \in K$ decomposes the form as:

$$Tr_{F/\mathbb{Q}}(\lambda N_{F/K}(x) \sim 2Tr_{K/\mathbb{Q}}(\lambda x^2) \oplus 2Tr_{K/\mathbb{Q}}(-\lambda\delta y^2).$$

Provided $Tr_{K/\mathbb{Q}}(\alpha) \neq 0$ we can use the basis $1, \alpha'\sqrt{D}$ to express the form $Tr_{K/\mathbb{Q}}(\alpha y^2)$ as:

$$Tr_{K/\mathbb{Q}}(\alpha(y_1 + y_2\alpha'\sqrt{D})^2) = Tr_{K/\mathbb{Q}}(\alpha)y_1^2 + N_{K/\mathbb{Q}}(\alpha)DTr_{K/\mathbb{Q}}(\alpha)y_2^2.$$

If $Tr_{K/\mathbb{Q}}(\alpha) = 0$ then the basis $1 + \sqrt{D}, 1 - \sqrt{D}$ gives us:

$$Tr_{K/\mathbb{Q}}(\alpha(y_1(1 + \sqrt{D}) + y_2(1 - \sqrt{D}))^2) = 2Tr_{K/\mathbb{Q}}(\alpha\sqrt{D})y_1^2 - 2Tr_{K/\mathbb{Q}}(\alpha\sqrt{D})y_2^2.$$

We consider first the cases where $Tr_{K/\mathbb{Q}}(\alpha) = 0$, in particular in the case $\lambda = \frac{1}{\sqrt{D}}$ we get:

$$Tr_{K/\mathbb{Q}}(\lambda x^2) = 2x_1^2 - 2x_2^2.$$

And thus we have:

$$\begin{aligned} Tr_{K/\mathbb{Q}}(-\lambda\delta y^2) &= Tr_{K/\mathbb{Q}}(\frac{-\delta}{\sqrt{D}})y_1^2 + N_{K/\mathbb{Q}}(\frac{-\delta}{\sqrt{D}})DTr_{K/\mathbb{Q}}(\frac{-\delta}{\sqrt{D}})y_2^2 \\ &= (-2\delta_2)y_1^2 - (\delta_1^2 - D\delta_2^2)(-2\delta_2)y_2^2. \end{aligned}$$

And so we get:

$$\begin{aligned} Tr_{F/\mathbb{Q}}(\lambda N_{F/K}(x)) &\sim 4x_1^2 - 4x_2^2 + 2(-2\delta_2)y_1^2 - 2(\delta_1^2 - D\delta_2^2)(-2\delta_2)y_2^2 \\ &\sim x_1^2 - x_2^2 - \delta_2 y_1^2 + N_{K/\mathbb{Q}}(\delta)\delta_2 y_2^2 \end{aligned}$$

This quadratic form has discriminant $N_{K/\mathbb{Q}}(\delta)$, Witt invariants $(-1,-1)_p(\delta_2, N(\delta))_p$ and signature (2,2). If we had taken $\lambda = \frac{\delta_2}{\sqrt{D}}$ we would have had Witt invariants $(-1,-1)_p$.

If we instead consider the case $\lambda = \sqrt{D}\delta'$ we get the same thing essentially. Up to scaling by $\mathbb{Q}$ this covers all cases where one of the $Tr_{K/\mathbb{Q}}(\alpha) = 0$.

For all other choices for λ we have $Tr_{K/\mathbb{Q}}(\alpha) \neq 0$ for both $\alpha = \lambda, -\lambda\delta$. Up to rescaling over $\mathbb{Q}$ we may assume $Tr_{K/\mathbb{Q}}(\lambda) = 1$ and thus we get:

$$\begin{aligned} Tr_{K/\mathbb{Q}}(\lambda N_{F/K}(x)) \sim Tr_{K/\mathbb{Q}}(\lambda)x_1^2 + N_{K/\mathbb{Q}}(\lambda)DTr_{K/\mathbb{Q}}(\lambda)x_2^2 + Tr_{K/\mathbb{Q}}(-\lambda\delta)y_1^2 \\ + N_{K/\mathbb{Q}}(-\lambda\delta)DTr_{K/\mathbb{Q}}(-\lambda\delta)y_2^2. \end{aligned}$$

This quadratic form has discriminant $N_{K/\mathbb{Q}}(\delta)$ and Witt invariants:

$$(D,D)(D, N_{K/\mathbb{Q}}(\delta))(N_{K/\mathbb{Q}}(\delta), N_{K/\mathbb{Q}}(\lambda))(N_{K/\mathbb{Q}}(\lambda), N_{K/\mathbb{Q}}(\lambda))(-Tr_{K/\mathbb{Q}}(\lambda\delta), -N_{K/\mathbb{Q}}(\lambda\delta)D),$$

the signature is twice the number of positive/negative embeddings of λ.

The Hilbert Modular Surface

Consider a totally real quadratic field $H/\mathbb{Q}$, we have seen that the Hilbert modular space for H comes from the quadratic form $q_H(a,b,h) = ab - hh'$. With the choice of basis $(1,1,0)$, $(1,-1,0)$, $(0,0,1)$, $(0,0,\sqrt{d})$ this quadratic form is equivalent to $q_H = [1,-1,-1,d]$, has discriminant d, Witt invariants $(-1,-1)_p$ for each prime p and has signature (2,2).

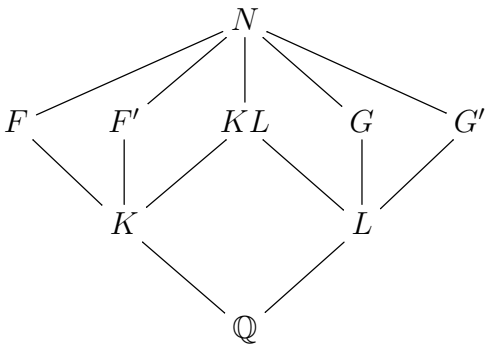
So what we have now, is that we have algebraic tori $F^{(1)}$ which will be contained in the orthogonal group associated to the Hilbert modular space $\mathbb{H}_{\mathbb{Q}(\sqrt{N_{K/\mathbb{Q}}(\delta)})}$. Through the association of points of the space and abelian varieties we will then have that $F^{(1)}$ will stabilize some point on $\mathbb{H}_{\mathbb{Q}(\sqrt{N(\delta)})}$ and thus will map to the endomorphism group of the associated abelian variety. However, the general theory tells us that the abelian varieties associated to $\mathbb{H}_{\mathbb{Q}(\sqrt{N(\delta)})}$ should if anything have CM through fields over $\mathbb{Q}(\sqrt{N_{K/\mathbb{Q}}(\delta)})$ and not over K.

We are thus driven to the questions:

- When can $N_{K/\mathbb{Q}}(\delta) = d$?
  The answer is if and only if $(d,D)_p = 1$ for all primes. This is a local class field theory question.
- How does an abelian variety seem to end up with CM by two seemingly unassociated fields?
  The answer (in part) is in the next sections and amounts to showing how the fields are associated, and which field the abelian variety will actually have CM by.

Field towers

We make the following definitions (which are compatible with previous notation)
$K = \mathbb{Q}(\sqrt{D})$
$F = \mathbb{Q}(\sqrt{D},\sqrt{-\delta})$ $F' = \mathbb{Q}(\sqrt{D},\sqrt{-\delta'})$
$L = \mathbb{Q}(\sqrt{\delta\delta'})$
$G = \mathbb{Q}(\sqrt{\delta\delta'},\sqrt{-\delta}+\sqrt{-\delta}')$ $G' = \mathbb{Q}(\sqrt{\delta\delta'},\sqrt{-\delta}-\sqrt{-\delta}')$
$N = FF' = GG' = \mathbb{Q}(\sqrt{D},\sqrt{-\delta},\sqrt{-\delta'})$
We then have the following diagram:



Which is possibly incomplete and may have some redundancy.

Note that we have: $\sqrt{-\delta}+\sqrt{-\delta'} = \sqrt{-2(\delta_1 - \sqrt{\delta\delta'})}$, $\sqrt{-\delta}-\sqrt{-\delta'} = \sqrt{-2(\delta_1+\sqrt{\delta\delta'})}$ and $(-2(\delta_1-\sqrt{\delta\delta'}))(-2(\delta_1+\sqrt{\delta\delta'})) = 4(\delta_1^2 - (\delta_1^2 - D\delta_2^2)) = 4D\delta_2^2$. Consequently we have that G, G' are quadratic imaginary (over L) when δ is not in $\mathbb{Q}$.

We have 3 cases to consider:

F cyclic Galois

We immediately have $N = F = F'$. Since KL is totally real this implies $KL \subset K$ which implies $L \subset K$. We note that in the case of cyclic Galois $L \not\subseteq \mathbb{Q}$ since if it were, then at least

one of G, G' would be an imaginary quadratic extension of $\mathbb{Q}$ contained in F, but F being cyclic Galois CM, means this does not happen.

Therefor we have in this case that: $N = F = F' = G = G'$ and $K = KL = L$ in particular $D = \delta\delta'$ mod squares.

Conversely, one has that if $D = \delta\delta'$ mod squares so that $K = KL = L$, one gets then that: $N = F = F' = G = G'$ and so F is at least Galois. ($F = G = G'$ follows from δ not being in $\mathbb{Q}$ and from the remarks above).

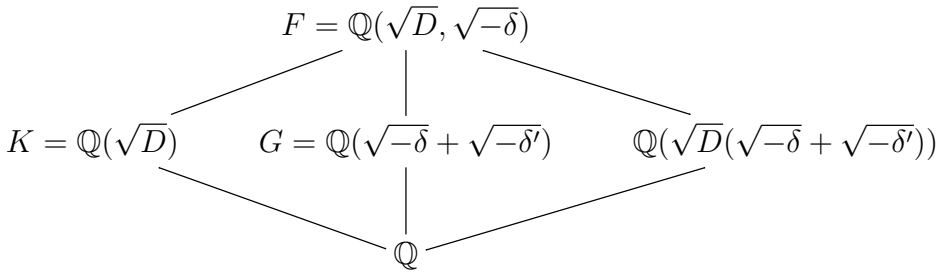
Now we know there is an element of $\mathrm{Gal}(K/\mathbb{Q})$ which takes $\delta \mapsto \delta'$. It must have two extensions to an element of $\mathrm{Gal}(F/\mathbb{Q})$ and each extension must act on $\sqrt{-\delta}, \sqrt{-\delta'}$ in one of the following ways:

- $\sqrt{-\delta} \mapsto \sqrt{-\delta}$ would imply $\delta \mapsto \delta$ so not allowed as an extension
- $\sqrt{-\delta} \mapsto -\sqrt{-\delta}$ would imply $\delta \mapsto \delta$ so not allowed as an extension
- $\sqrt{-\delta} \mapsto \sqrt{-\delta'}$ here we have the subcases:
  - $:\sqrt{-\delta'} \mapsto \pm\sqrt{-\delta'}$ would imply $\delta' \mapsto \delta'$ so not allowed as an extension
  - $:\sqrt{-\delta'} \mapsto \sqrt{-\delta}$ For such an automorphism G is in its fixed field, but $G = F$.
  - $:\sqrt{-\delta'} \mapsto -\sqrt{-\delta}$ such an element has order 4 so the Galois group is C_4.
- $\sqrt{-\delta} \mapsto -\sqrt{-\delta'}$ here we have the subcases:
  - $:\sqrt{-\delta'} \mapsto \pm\sqrt{-\delta'}$ would imply $\delta' \mapsto \delta'$ so not allowed as an extension
  - $:\sqrt{-\delta'} \mapsto \sqrt{-\delta}$ such an element has order 4 so the Galois group is C_4.
  - $:\sqrt{-\delta'} \mapsto -\sqrt{-\delta}$ For such an automorphism G' is in its fixed field, but $G' = F$

In particular we see that for all valid cases, F is a cyclic Galois extension.

F is bi-quadratic

We again have $N = F = F'$ but by the above work in the cyclic case we know that $L \neq K$, but $L \subset G \subset N = F$ is totally real, so we conclude $L = \mathbb{Q}$. We then have that at least one of G, G' is quadratic imaginary over $\mathbb{Q}$, without loss of generality suppose it is G (this amounts to fixing an embedding of everything in $\mathbb{C}$ and supposing that $\sqrt{-\delta}, \sqrt{-\delta'}$ where both taken to be the square roots in the upper half plane, we might as well have made this assumption earlier). We then arrive at the following diagram of fields:



Note that when δ is not in $\mathbb{Q}$ then $\mathbb{Q}(\sqrt{D}(\sqrt{-\delta} + \sqrt{-\delta'})) = G'$.

F is not Galois

Then nothing in the original diagram collapses, we should note that we do in fact have: $F \simeq F'$ and $G \simeq G'$ coming from Galois automorphisms of N, moreover the map taking $G' \to G$ can be taken to be the Galois element σ whose fixed field is F. We have that for an element $f \in F$, $N_{N/G}(F) = ff'$, $N_{N/G'}(F) = f\overline{f'} = \sigma(ff')$.

Moreover we should generally expect to have the maps of complex norm 1 elements:

$$\pm 1 \longrightarrow F^{(1)} \times F'^{(1)} \xrightarrow{(f_1,f_2)\mapsto f_1 f_2} N^{(1)}$$

$$\pm 1 \longrightarrow N^{(1)} \xrightarrow{N_{N/F}\times N_{N/F'}} F^{(1)} \times F'^{(1)}$$

$$\pm 1 \longrightarrow F^{(1)} \xrightarrow{N_{N/G}\times N_{N/G'}} G^{(1)} \times G'^{(1)}$$

However in the last map, the images are of the form $(ff', \sigma(ff'))$ and so we lose no information by further projecting to $G^{(1)}$. In particular we have maps:

$$\pm 1 \longrightarrow F^{(1)} \xrightarrow{\alpha: f\mapsto ff'} G^{(1)}$$

$$\pm 1 \longrightarrow G^{(1)} \xrightarrow{\beta: g\mapsto g\sigma(g)} F^{(1)}$$

Moreover, the composition $\beta \circ \alpha : f \mapsto f^2$ and $\alpha \circ \beta : g \mapsto g^2$. And so what we see is that $F^{(1)} \sim G^{(1)}$ that is they are isogenous.

How $G^{(1)}$ acts on $\mathbb{H} \times \mathbb{H}$

We usually interpret the action of $\mathrm{SL}_2(L)$ on the Hilbert modular space for G as $M \circ (h_1, h_2) = (M \circ h_1, M' \circ h_2)$. Viewing the Hilbert modular surface as the space associated to the orthogonal group. That is:

$$V := \left\{ \left(\begin{smallmatrix} a & v' \\ v & b \end{smallmatrix}\right) | a, b \in \mathbb{Q}, v \in F \right\}$$

together with the quadratic form given by $-\det\left(\left(\begin{smallmatrix} a & v' \\ v & b \end{smallmatrix}\right)\right)$ the action is given by:

$$M \circ \begin{pmatrix} a & v' \\ v & b \end{pmatrix} = M \begin{pmatrix} a & v' \\ v & b \end{pmatrix} {}^t M'.$$

Now, the usual way to embed $G^{(1)} \hookrightarrow \mathrm{SL}_2(L)$ is via the restriction of scalars map:

$$G^{(1)} = \left\{ \begin{pmatrix} x & -2(\delta_1 - \sqrt{\delta\delta'})y \\ y & x \end{pmatrix} \right\}.$$

With the notation $v = v_1 + v_2\sqrt{\delta\delta'}$, $\Delta = 2(\delta_1 - \sqrt{\delta\delta'})$, $\Delta' = 2(\delta_1 + \sqrt{\delta\delta'})$ (note that $'$ refers to the conjugate in the appropriate field, which is not always the same field). We then have that an element $g \leftrightarrow x + y(\sqrt{-\delta} + \sqrt{-\delta'}) = x + y\sqrt{-\Delta}$ acts on the quadratic space V as

$$\begin{aligned} g \circ \begin{pmatrix} a & v' \\ v & b \end{pmatrix} &= \begin{pmatrix} x & -2(\delta_1 - \sqrt{\delta\delta'})y \\ y & x \end{pmatrix} \begin{pmatrix} a & v' \\ v & b \end{pmatrix} \begin{pmatrix} x' & y' \\ -2(\delta_1 + \sqrt{\delta\delta'})y' & x' \end{pmatrix} \\ &= \begin{pmatrix} xa - \Delta yv & xv' - \Delta yb \\ ya + xv & yv' + xb \end{pmatrix} \begin{pmatrix} x' & y' \\ -\Delta' y' & x' \end{pmatrix} \\ &= \begin{pmatrix} xx'a - \Delta x'yv - \Delta' xy'v' + \Delta\Delta' yy'b & xy'a - \Delta yy'v - \Delta x'yb + xx'v' \\ xx'v + x'ya - yy'\Delta'v' - xy'b\Delta' & yy'a + xy'v + x'yv' + xx'b \end{pmatrix}. \end{aligned}$$

Reinterpreting this into column vectors we get that g acts as:

$$\begin{pmatrix} xx' & \Delta\Delta' yy' & -(\Delta x'y + \Delta' xy') & -(\Delta x'y - \Delta' xy')\sqrt{\delta\delta'} \\ yy' & xx' & xy' + x'y & (xy' - x'y)\sqrt{\delta\delta'} \\ \frac{1}{2}(xy' + x'y) & \frac{-1}{2}(\Delta x'y + \Delta' xy') & (xx' + \frac{1}{2}yy'(\Delta + \Delta')) & \frac{1}{2}yy'(\Delta - \Delta')\sqrt{\delta\delta'} \\ \frac{1}{2\sqrt{\delta\delta'}}(x'y - xy') & \frac{1}{2\sqrt{\delta\delta'}}(\Delta x'y - \Delta' xy') & \frac{1}{2\sqrt{\delta\delta'}}yy'(\Delta - \Delta') & (xx' + \frac{1}{2}yy'(\Delta + \Delta')) \end{pmatrix} \begin{pmatrix} a \\ b \\ v_1 \\ v_2 \end{pmatrix}$$

We had embedded $F^{(1)} \hookrightarrow O_V$ via its regular representation. Decomposing the $\mathbb{Q}$ vector space $F \simeq K_1 + K_2\sqrt{-\delta}$ the mapping $F \to V$ took the form $K_1 \to \mathbb{Q} \oplus \mathbb{Q}$, $K_2 \to L$. Taking as a basis for F the elements $\{\frac{1}{4\delta_2}, \frac{\sqrt{D}}{2}, \frac{\sqrt{-\delta}}{2\delta_2}, \frac{(\delta_1 - \delta_2\sqrt{D})\sqrt{-\delta}}{2\delta_2}\}$ Then the quadratic form $q_{\frac{\delta_2}{\sqrt{D}}} = Tr_{F/\mathbb{Q}}((\delta_2/\sqrt{D})x\overline{x})$ takes the form:

$$q(v_1, v_2, v_3, v_4) = v_1 v_2 + v_3^2 - N_{K/\mathbb{Q}}(\delta)v_4^2$$

An element in $F^{(1)}$ ($t_f \leftrightarrow f_1 + f_2\sqrt{D} + f_3\sqrt{-\delta} + f_4\sqrt{-\delta D}$) then acts on this as:

$$t_f \circ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} f_1 & 2D\delta_2 f_2 & -2(\delta_1 f_3 + D\delta_2 f_4) & -2\delta\delta' f_3 \\ \frac{1}{2\delta_2}f_2 & f_1 & -f_3 - \frac{\delta_1}{\delta_2}f_4 & -\frac{\delta\delta'}{\delta_2}f_4 \\ \frac{1}{2}(f_3 + \delta_1 f_4) & \delta_1 f_3 + D\delta_2 f_4 & f_1 + \frac{\delta_1}{\delta_2}f_3 & \frac{\delta_1^2}{\delta_2} - D\delta_2 \\ -\frac{1}{2}f_4 & -f_3 & \frac{-1}{\delta_2}f_3 & f_1 - \frac{\delta_1}{\delta_2}f_3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

Consider the norm map $G^{(1)} \overset{N_{N/F}}{\longrightarrow} F^{(1)}$, it takes

$$x + y\sqrt{-\Delta} \mapsto (x + y(\sqrt{-\delta} + \sqrt{-\delta'}))(x' + y'(\sqrt{-\delta} - \sqrt{-\delta'}))$$

This is:

$$\begin{aligned} &= xx' + xy'(\sqrt{-\delta} - \sqrt{-\delta'}) + x'y(\sqrt{-\delta} + \sqrt{-\delta'}) + 2yy'\delta_2\sqrt{D} \\ &= xx' + (xy' + x'y)\sqrt{-\delta} + (x'y - xy')\frac{\Delta - \Delta'}{4\delta}\sqrt{-\delta} + 2yy'\delta_2\sqrt{D} \\ &= xx' + (2yy'\delta_2)\sqrt{D} + (xy'(1 - \delta_1\frac{\Delta - \Delta'}{4\delta\delta'}) + x'y(1 + \delta_1\frac{\Delta - \Delta'}{4\delta\delta'}))\sqrt{-\delta} \\ &\quad + (x'y - xy')\frac{\Delta - \Delta'}{4\delta\delta'}\delta_2\sqrt{-\delta D} \end{aligned}$$

In particular, one can now check that under the given choices of basis that the actions agree, that is we have $g \circ (a, b, v_1, v_2) \simeq N_{N/F}(g) \circ (x_1, x_2, x_3, x_4)$.

What the above means?

It means essentially that all is as we expected. We can embed the torus $F^{(1)}$ into the orthogonal group and the torus $G^{(1)}$ into the spin group for the quadratic space associated to the Hilbert modular variety. The map from the spin group to the orthogonal group ends up taking $G^{(1)} \to F^{(1)}$ and moreover does so via the isogeny we knew existed already. It turns out that in the natural way to attach abelian varieties to points of the Hilbert modular space (see for example [Gor02]) it will be the tori in the spin group that end up acting on them.

What it says about abelian varieties with CM is the following: In the cyclic Galois case we have in fact no surprises, we end up with CM by a field that is in fact an extension of a field that should be associated to the Hilbert modular space. In the bi-quadratic case, the Hilbert modular space we thought we had turned out not to really be one (the totally real field was $\mathbb{Q}$). Though

of course one can in fact carry out some constructions here and see that what you would have is F acting on a product of 2 elliptic curves via the 2 complex subfields. In the non-Galois case we saw that our torus is isogenous to one coming from a CM field of a field associated to the Hilbert modular surface, we saw moreover how the actions are related.

4.4 The General Case - Concretely

The above constructions illustrated some of things we might try to do in a more general setting with the algebraic torus coming from the complex norm 1 elements of a higher degree CM-field, and moreover give us some hints at things we would like to be true.

In particular we can prove the following theorem:

Theorem 4.4.1. *Let F be a CM-field and let $F^{(1)}$ be the algebraic torus of norm 1 elements of F. If $F^{(1)}$ acts via the regular representation, (that is on F as a $\mathbb{Q}$ vector space via multiplication) then the only quadratic forms $F^{(1)}$ can preserve are the forms $Tr_{F/\mathbb{Q}}(\lambda x\overline{x})$ where $\lambda \in F \cap \mathbb{R}$.*

Proof. Fix a normal closure N of F.

Fix a $\mathbb{Q}$ basis $\{\gamma_1, \ldots, \gamma_n\}$ of F such that $Tr_{F/\mathbb{Q}}(\gamma_i\gamma_j) = 0$ for $i \neq j$. This is possible over any field and amounts to diagonalizing the trace form on F. Note that these conditions imply also that $Tr_{F/\mathbb{Q}}(\gamma_i^2) \neq 0$.

Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of F into N.

Consider the basis of $N \otimes_{\mathbb{Q}} F$ given by $\{v_l := \sum_i \frac{\sigma_l(\gamma_i)}{Tr_{F/\mathbb{Q}}(\gamma_i^2)} \otimes \gamma_i\}_{l=1..n}$.

Using that $Tr_{F/\mathbb{Q}}(\gamma_i\gamma_j) = 0$ we get: $\gamma_j\gamma_i = \sum_k \frac{Tr_{F/\mathbb{Q}}(\gamma_j\gamma_i\gamma_k)}{Tr_{F/\mathbb{Q}}(\gamma_k^2)}\gamma_k$.

Observe that:

$$\begin{aligned}
\gamma_j \circ \sum_i \frac{\sigma_l(\gamma_i)}{Tr_{F/\mathbb{Q}}(\gamma_i^2)} \otimes \gamma_i =& \sum_i \frac{\sigma_k(\gamma_i)}{Tr_{F/\mathbb{Q}}(\gamma_i^2)} \otimes \gamma_j\gamma_i \\
=& \sum_i \frac{\sigma_l(\gamma_i)}{Tr_{F/\mathbb{Q}}(\gamma_i^2)} \otimes \sum_k \frac{Tr_{F/\mathbb{Q}}(\gamma_j\gamma_i\gamma_k)}{Tr_{F/\mathbb{Q}}(\gamma_k^2)}\gamma_k \\
=& \sum_k \sum_i \frac{Tr_{F/\mathbb{Q}}(\gamma_j\gamma_i\gamma_k)}{Tr_{F/\mathbb{Q}}(\gamma_k^2)} \frac{\sigma_l(\gamma_i)}{Tr_{F/\mathbb{Q}}(\gamma_i^2)} \otimes \gamma_k \\
=& \sum_k \frac{\sigma_l(\sum_i \frac{Tr_{F/\mathbb{Q}}(\gamma_j\gamma_i\gamma_k)}{Tr_{F/\mathbb{Q}}(\gamma_i^2)}\gamma_i)}{Tr_{F/\mathbb{Q}}(\gamma_k^2)} \otimes \gamma_k \\
=& \sum_k \frac{\sigma_l(\gamma_j\gamma_k)}{Tr_{F/\mathbb{Q}}(\gamma_k^2)} \otimes \gamma_k \\
=& \sigma_l(\gamma_j) * \sum_k \frac{\sigma_l(\gamma_k)}{Tr_{F/\mathbb{Q}}(\gamma_k^2)} \otimes \gamma_k.
\end{aligned}$$

That is to say that, $f \in F$ acts on the l^{th} basis vector via multiplication in N by $\sigma_l(f)$.

Since the embeddings are distinct, this shows us (a-posteriori) that our purported basis actually is one, since they give us a basis for n distinct eigenspaces. Moreover we have thus diagonalized the action of $F^{(1)}$.

Supposing that $\overline{\sigma_l} = \sigma_{l+n/2}$ for $l < n/2$ we then conclude that any quadratic form preserved by this action of $F^{(1)}$ must take the form $Q(\sum_{i=1}^{n} x_i v_i) = \sum_{i=1}^{n/2} a_i x_i x_{i+n/2}$.

We now wish to undo the diagonalization of the form and express the form back into the basis: $e_l = 1 \otimes \gamma_l$. We have that:

$$\begin{aligned}\sum_{j=1}^{n}\sigma_j(\gamma_l)v_j =&\sum_{j=1}^{n}\sigma_j(\gamma_l)\sum_{i=1}^{n}\frac{\sigma_j(\gamma_i)}{Tr_{F/\mathbb{Q}}(\gamma_i^2)}\otimes\gamma_i\\ =&\sum_{i=1}^{n}\frac{\sum_{j=1}^{n}\sigma_j(\gamma_l\gamma_i)}{Tr_{F/\mathbb{Q}}(\gamma_i^2)}\otimes\gamma_i\\ =&1\otimes\gamma_l\\ =&e_l.\end{aligned}$$

We note that Q will be a rational quadratic form, if and only if $Q(e_l), Q(e_i+e_j)-Q(e_i)-Q(e_j) \in \mathbb{Q}$ for all i, j, l. We compute that:

$$Q(e_l) = \frac{1}{2}\sum_{k=1}^{n}a_k\sigma_k(\gamma_l\overline{\gamma_l})$$

and

$$Q(e_i+e_j)-Q(e_i)-Q(e_j) = \frac{1}{2}\sum_{k=1}^{n}a_k\sigma_k(\gamma_i\overline{\gamma_j}+\gamma_j\overline{\gamma_i}) = \sum_{k=1}^{n}a_k\sigma_k(\gamma_i\overline{\gamma_j}).$$

Where we have taken $a_{k+n/2} = a_k$. By taking linear combinations of these conditions, we can conclude we have the requirement that:

$$\Gamma(f) = \sum_{k=1}^{n}a_k\sigma_k(f) \in \mathbb{Q}\ \forall f \in F$$

We thus have that $\Gamma \in \mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{Q})$ but the trace pairing on F is perfect and thus induces an isomorphism from F to the vector space dual of F. Thus we have that $\Gamma(f) = \sum_{k=1}^{n}\sigma_k(A)\sigma_k(f)$ for some A in F.

We therefore have $\sum_{k=1}^{n}(a_k - \sigma_k(A))\sigma_k(f) = 0$ for all $f \in F$. But then by linear independence of the embeddings of F we conclude $a_k = \sigma_k(A)$. ($a_{k+n/2} = a_k$ implies then A is in the totally real subfield of F).

But then the quadratic form Q is just up to integer multiples the form $Tr_{F/\mathbb{Q}}(Ax\overline{x})$. □

We also have the following results:

Theorem 4.4.2. *Let $F^{(1)}$ be the torus of complex norm 1 elements for the CM-field $F/\mathbb{Q}$. Let $\rho : F^{(1)} \to \mathrm{O}_q$ be any faithful rational representation of $F^{(1)}$ into the orthogonal group for a space (V, q). Then there exists a faithful rational representation $\rho' : T = R_{F/\mathbb{Q}}(\mathbb{G}_m) \to \mathrm{GL}(V)$ such that $\rho = \rho'|_{F^{(1)}}$.*

Proof. When we diagonalize $F^{(1)}$ over $\overline{F}$ the condition for faithfulness implies that $F^{(1)}$ will act by a spanning set of characters for its character module. The orthogonality condition implies that it must also act via the complex conjugates (that is the inverses in $X(F^{(1)})$ of these characters). The natural map $X(T) \to X(F^{(1)})$ is a $2-1$ map however fixing a CM-type we can choose a mapping from the characters that act on V onto a spanning set of characters for $X(T)$ by simply having the 2 conjugate characters that appear map to the different embeddings.

That is to say $X(F^{(1)})$ is generated by the set of embeddings $F \hookrightarrow \overline{F}$ with relation $\overline{\chi} = \chi^{-1}$. $X(T')$ is generated by all embeddings $F \hookrightarrow \overline{F}$. By taking the inverses that appear to the conjugate of where we send the character, we get our mapping.

Doing this then gives us a faithful (not necessarily rational) representation $\rho' T' \to \mathrm{GL}(V \otimes \overline{F})$. However, we know that in diagonalizing $F^{(1)}$ to ${F^{(1)}}'$ that it is a form of the split torus ${F^{(1)}}'$ via a co-cycle $\xi_\sigma \in H^1(\mathrm{Gal}(\overline{F}/\mathbb{Q}), N_{\mathrm{GL}_n}({F^{(1)}}'))$ (this follows by rationality). In order to see that ρ' maps T onto a rational torus we need that the same co-cycle ξ_σ is in $H^1(\mathrm{Gal}(\overline{F}/\mathbb{Q}), N_{\mathrm{GL}_n}(T'))$.

Indeed ${F^{(1)}}'$ looks like blocks of the form (a) : $\begin{pmatrix} \chi(t) & 0 \\ 0 & \chi(t)^{-1} \end{pmatrix}$ and T' looks like blocks of the form (b) : $\begin{pmatrix} \chi(t) & 0 \\ 0 & \overline{\chi}(t) \end{pmatrix}$. By additive linear independence of multiplicative characters we know that $\left(\sum_{i=1}^{n} a_i \chi_i\right)\left(\sum_{i=1}^{m} b_i \chi_i'\right) \neq id$ unless $n = m = 1$ and $\chi_1' = \chi_1^{-1}$. Moreover $\sum_{i=1}^{n} a_i \chi_i \neq 0$ unless $a_i = 0$. From this it follows that the only sorts of conjugation that can preserve these block matrices are those that permute blocks or preserve them blockwise. Consequently, since the question of rationality comes down to a question about the normalizers of these tori, we need to only to show that normalizing all matrices of type (a) implies you normalize all matrices of type (b). This is an easy check. □

Theorem 4.4.3. *Let F be a CM-field and let $F^{(1)}$ be the algebraic torus of norm 1 elements of F. Suppose $F^{(1)}$ is contained in some rational orthogonal group O and acts via the regular representation. Let $[Z] \in \kappa$ be a fixed point of $F^{(1)}$. Then the point $[Z]$ as an element of the complex space κ (under the given realization) is defined over F' some Galois conjugate of F.*

Proof. The idea of the argument is to diagonalize slightly less than we did previously, so that we can work with the positive definite conditions that define κ.

Suppose that $F = K(\sqrt{-\delta})$ where K is the totally real subfield of F and $\delta \in K$ is totally positive. As we have done before fix a normal closure N of F and an embedding of N into $\mathbb{C}$. Fix a $\mathbb{Q}$ basis $\{\gamma_1, \ldots, \gamma_n\}$ of F such that $Tr_{F/\mathbb{Q}}(\gamma_i \gamma_j) = 0$ for $i \neq j$. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of F into N, supposing moreover that $\overline{\sigma_i} = \sigma_{i+n/2}$ for $i > n/2$.

We have the basis of $N \otimes_{\mathbb{Q}} F$ given by $\{v_l := \sum_i \frac{\sigma_l(\gamma_i)}{Tr_{F/\mathbb{Q}}(\gamma_i^2)} \otimes \gamma_i\}_{l=1..n}$. For notational convenience arrange so that $v_{\overline{l}} = v_{l+n/2}$ for $l < n/2$.

Consider now the new basis for $N \otimes_{\mathbb{Q}} F$ given by $\{x_l = \frac{1}{2}(v_l + v_{\overline{l}}), x_l' = \sigma_l(\frac{1}{2\sqrt{-\delta}})(v_l - v_{\overline{l}})\}_{l=1..n/2}$. Note that x_l, x_l' are both fixed by complex conjugation and are hence in $\mathbb{R}$. Since we understand the action of F on v_l we can understand the action of F on the vector subspaces generated by x_l, x_l' for each l. In particular these are fixed and we can compute that for $f \in F$:

$$f \circ x_l = \frac{1}{2}(\sigma_l(f) + \sigma_{\overline{l}}(f))x_l + \frac{\sqrt{-\delta}}{2}(\sigma_l(f) - \sigma_{\overline{l}}(f))x_l'$$
$$f \circ x_l' = \frac{1}{2\sqrt{-\delta}}(\sigma_l(f) - \sigma_{\overline{l}}(f))x_l + \frac{1}{2}(\sigma_l(f) + \sigma_{\overline{l}}(f))x_l'.$$

So then the action of $F^{(1)}$ on $(N \cap \mathbb{R}) \otimes_{\mathbb{Q}} F$ decomposes into blocks of the form:

$$\frac{1}{2}\begin{pmatrix} \sigma_l(f) + \sigma_{\overline{l}}(f) & \sqrt{-\delta}(\sigma_l(f) - \sigma_{\overline{l}}(f)) \\ \frac{1}{\sqrt{-\delta}}(\sigma_l(f) - \sigma_{\overline{l}}(f)) & \sigma_l(f) + \sigma_{\overline{l}}(f) \end{pmatrix} = \begin{pmatrix} a & \sigma_l(-\delta)b \\ b & a \end{pmatrix} \mid a^2 + \delta b^2 = 1.$$

In particular we can see that any quadratic form this block can preserve must look like:

$$Q(y_l x_l + y_l' x_l') = a_l(y_l^2 + \delta y_l'^2).$$

In particular, each plane spanned by a pair x_l, x_l' is definite. Since the signature of our original form was $(2, n-2)$ and we have diagonalized over a subfield of $\mathbb{R}$ and hence not changed signature precisely one of the $a_l > 0$ and it corresponds to the choice of embeddings $\sigma_l, \sigma_{\bar{l}}$ where the λ that defined the form was positive.

From the above computation we see that, in the Grassmannian model $\mathrm{Gr}(V)$ the positive definite plane stabilized by $F^{(1)}$ is precisely the plane generated by x_l, x_l', Since F is quadratic over the field generated by the coordinates of these vectors we conclude that the field of definition for this point in $\mathrm{Gr}(V)$ is the totally real subfield K of F.

We now wish to compute the image of this point in κ. To do this we need to change the basis for the plane such that $Q(x_l) = Q(x_l')$, to do this we must work in the field $(N \cap \mathbb{R})(\sqrt{\sigma_l(\delta)})$ and replace x_l' by $\frac{1}{\sqrt{\sigma_l(\delta)}} x_l'$. We then have that the point $Z \in \kappa \in P(V(\mathbb{C}))$ corresponding to the plane is given by the point:

$$[Z] = x_l + i x_l' = \frac{1}{2}(v_l + v_{\bar{l}}) - \frac{1}{2\sigma_l(\delta)}(v_l - v_{\bar{l}}).$$

Writing this in projective coordinates in terms of the basis γ_i for V we get:

$$[Z] = [\ldots, \frac{1}{2}\left(\sigma_l((\delta-1)\gamma_i) + \sigma_{\bar{l}}((\delta+1)\gamma_i)\right), \ldots] = [\ldots, \sigma_l((\delta-1)\gamma_i + (\delta+1)\overline{\gamma_i}), \ldots].$$

The coordinates of this point all clearly lie in $\sigma_l(F)$ and hence the point can be defined over this field. □

Remark. It should be noted the field of definition of points in κ viewed as a complex space under the realization we have does not necessarily relate directly to the field of definition in some algebraic model for the quotients of κ. The above result is analogous (and in fact in the special case amounts) to saying that the special points in the usual upper half plane are quadratic imaginary points. This however does not tell us much about the field of definition for the algebraic objects these might classify. In particular in the usual case of the upper half plane the objects (in this case elliptic curves) associated to the CM-points are defined over the Hilbert class field of the quadratic imaginary field.

CHAPTER 5
Summary and Further Questions

What We Have Seen

We have in the proceeding determined a general classification of both which tori might embed into a given orthogonal group as well as into which orthogonal groups a given torus might embed. In particular the former can be classified by:

$$\mathrm{Ker}\left[H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(T) \cap N_{\mathrm{GL}_n}(O)) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(O))\right]$$

and the latter by:

$$\mathrm{Ker}\left[(H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(T) \cap N_{\mathrm{GL}_n}(O)) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(T))\right].$$

Through more concrete study of the case of tori coming from regular representations of CM-fields we have shown that we can describe the required correspondence between invariants of an orthogonal groups and the field. This suggests that we might wish to consider rather than which isomorphism classes of tori can embed but rather which isomorphism classes together with a representation into GL_n might embed. We have shown that this classification amounts to looking at:

$$\mathrm{Ker}\left[H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(T) \cap N_{\mathrm{GL}_n}(O)) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), N_{\mathrm{GL}_n}(T))\right].$$

The problem of determining which of these correspond to special points, that is which ones have compact sets of real points, was determined entirely by the isomorphism class and allowed us to associate a minimal CM-algebra into which its $\mathbb{Q}$-rational points would embed.

What We Still Do Not Know

There remain of course a number of unanswered questions. We still have not given a complete classification for tori with compact sets of real points, though we know they are subtori of $R_{K/\mathbb{Q}}(R^{(1)}_{F/K}(\mathbb{G}_m))^l$ we do not know if they all are precisely of this form (though we should not really expect this).

We do not know that all rational faithful algebraic representations of $R_{K/\mathbb{Q}}(R^{(1)}_{F/K}(\mathbb{G}_m))$ are sufficiently like the regular representation so that we understand the quadratic forms they may preserve. For example if we knew that for any such representation ρ that $\mathrm{im}(\rho) \subset \mathrm{GL}_n$ was rationally conjugate to the image of the regular representation this would be enough. (This statement is true for any such ρ that I have been able to construct). We know that the images of any (maximal) representations into orthogonal groups are conjugate over $\mathrm{GL}_n(\overline{k})$. One could conjecture that if T_1, T_2 are conjugate and rationally isomorphic then they are rationally conjugate. This statement is true for split tori, it is unclear that it would be true in general. We moreover do not know the analogous result about the rational faithful algebraic representations for tori coming from CM-algebras and as such our understanding in this case is also limited.

We also don't have a method that, given some quadratic form q actually finds a totally real field K with elements δ, λ such that $q = q_{K(\sqrt{-\delta}),\lambda}$. Moreover, we don't actually know that such a K is even guaranteed to exist. Consequently, we don't know that a given orthogonal symmetric

space is guaranteed to have any special points which are associated to CM-fields. (They will always have CM-points associated to CM-algebras).

It is hoped that further work in these areas could complete the presented results.

REFERENCES

[BF01] J. H. Bruinier and E. Freitag, *Local Borcherds products*, Ann. Inst. Fourier (Grenoble) **51** (2001), no. 1, 1–26. MR 1821065 (2002k:11067)

[Bor91] A. Borel, *Linear algebraic groups*, 2nd ed., Springer-Verlag, 1991.

[Bor95] Richard E. Borcherds, *Automorphic forms on* $\mathrm{O}_{s+2,2}(\mathbf{R})$ *and infinite products*, Invent. Math. **120** (1995), no. 1, 161–213. MR 1323986 (96j:11067)

[Bru02] Jan H. Bruinier, *Borcherds products on O(2, l) and Chern classes of Heegner divisors*, Lecture Notes in Mathematics, vol. 1780, Springer-Verlag, Berlin, 2002. MR 1903920 (2003h:11052)

[Bru04] Jan Hendrik Bruinier, *Infinite products in number theory and geometry*, Jahresber. Deutsch. Math.-Verein. **106** (2004), no. 4, 151–184. MR 2068524 (2005m:11085)

[Bru08] ———, *Hilbert modular forms and their applications*, The 1-2-3 of modular forms, Universitext, Springer, Berlin, 2008, pp. 105–179. MR 2447162 (2009g:11057)

[DM74] J. W. Davies and A. O. Morris, *The Schur multiplier of the generalized symmetric group*, J. London Math. Soc. (2) **8** (1974), 615–620. MR 0347987 (50 #485)

[FH91] William Fulton and Joe Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991, A first course, Readings in Mathematics. MR 1153249 (93a:20069)

[Fre90] Eberhard Freitag, *Hilbert modular forms*, Springer-Verlag, Berlin, 1990. MR 1050763 (91c:11025)

[GMS03] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003. MR 1999383 (2004f:11034)

[Gor02] Eyal Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Series, vol. 14, American Mathematical Society, Providence, RI, 2002, With the assistance of Marc-Hubert Nicole. MR 1863355 (2003c:11038)

[Hel01] Sigurdur Helgason, *Differential geometry, Lie groups, and symmetric spaces*, Graduate Studies in Mathematics, vol. 34, American Mathematical Society, Providence, RI, 2001, Corrected reprint of the 1978 original. MR 1834454 (2002b:53081)

[Hun80] Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York, 1980, Reprint of the 1974 original. MR 600654 (82a:00006)

[Mil05] J. S. Milne, *Introduction to Shimura varieties*, Harmonic analysis, the trace formula, and Shimura varieties, Clay Math. Proc., vol. 4, Amer. Math. Soc., Providence, RI, 2005, pp. 265–378. MR 2192012 (2006m:11087)

[PR94] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and applied mathematics (Academic Press), vol. 139, Boston : Academic Press, 1994.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, New York, 1973, Translated from French. MR 0344216 (49 #8956)

[Ser79] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)

[Ser84] ———, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. **59** (1984), no. 4, 651–676. MR 780081 (86k:11067)

[Ser02] ———, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author. MR 1867431 (2002i:12004)

[Spr98] T.A. Springer, *Linear algebraic groups*, Progress in mathematics (Boston, Mass.), vol. 9, Boston : Birkhauser, 1998.

[Wei99] S. Weinberg, *Quantum theory of fields, vol. 1*, Cambridge University Press: Cambridge, UK, 1999.