Non-split Semisimple Groups admitting Integral Models

Yi Shan

October 6, 2021

Abstract

When we study automorphic representations of a reductive $\mathbb{Q}$-group G, sometimes we need G to be the generic fiber of some reductive $\mathbb{Z}$-group scheme. If this holds, we say that G admits a $\mathbb{Z}$-model. In [DG70], the theory of Chevalley groups tells us any split connected reductive $\mathbb{Q}$-group has a unique $\mathbb{Z}$-model up to $\mathbb{Z}$-group isomorphism. For semisimple groups there are also some non-split examples. However, not all non-split semisimple $\mathbb{Q}$-groups have $\mathbb{Z}$-models. In his famous survey paper [Gro96], Gross states two necessary and sufficient conditions for semisimple groups to admit $\mathbb{Z}$-models, which are proved by Harder, and enumerates all the possibilities via the mass formula in some cases.

In this thesis, we are going to give detailed proofs of these conditions (Proposition 1.5,1.7) and the mass formula (Theorem 2.4), and then follow Gross's route to construct $\mathbb{Z}$-models for these non-split $\mathbb{Q}$-groups, especially for anisotropic groups of exceptional types G_2, F_4.

1 Models of Non-split Groups

In this section, we will state and prove these necessary and sufficient conditions for semisimple groups to admit $\mathbb{Z}$-models. Before that, we give a quick review on linear algebraic groups and Galois cohomology. Our main reference for the theory of linear algebraic groups is Milne's book [Mil17].

1.1 Algebraic Groups

Let k be a commutative ring. In this section, we denote commutative k-algebras by k-algebras for short. As we know, a k-scheme X can be viewed as a covariant functor from the category of k-algebras to the category of sets:

$$R \mapsto \mathrm{Hom}_{\mathrm{Spec}\, k}(\mathrm{Spec}\, R, X).$$

We can define group schemes in a similar way:

Definition 1.1. An *affine group scheme* G over k is a covariant functor from the category of k-algebras to the category of groups which is representable by a k-algebra. We can call it an affine k-group for short.

Remark 1.1. Yoneda's lemma tells us the k-algebra representing an affine group scheme is unique up to a unique k-algebra isomorphism. We choose one k-algebra in this isomorphism class and denote it by $\mathscr{O}(G)$.

This definition can also be described in the following way: an affine k-scheme G is said to be an affine group scheme if there exist morphisms of k-schemes $m : G \times_{\operatorname{Spec}(k)} G \to G$, $e : \operatorname{Spec}(k) \to G$ and $i : G \to G$ such that the following diagrams commute:

$$\begin{tikzcd} G \times_{\operatorname{Spec} k} G \times_{\operatorname{Spec} k} G \arrow[r, "\mathrm{id}\times m"] \arrow[d, "m\times \mathrm{id}"'] & G \times_{\operatorname{Spec} k} G \arrow[d, "m"] \\ G \times_{\operatorname{Spec} k} G \arrow[r, "m"] & G \end{tikzcd}$$

$$\begin{tikzcd} \operatorname{Spec} k \times_{\operatorname{Spec} k} G \arrow[r, "e\times \mathrm{id}"] \arrow[dr, "\simeq"] & G \times_{\operatorname{Spec} k} G \arrow[d, "m"] & G \times_{\operatorname{Spec} k} \operatorname{Spec} k \arrow[l, "\mathrm{id}\times e"'] \arrow[dl, "\simeq"'] \\ & G & \end{tikzcd}$$

$$\begin{tikzcd} G \arrow[r, "(i\times \mathrm{id})\circ\Delta"] \arrow[d] & G \times_{\operatorname{Spec} k} G \arrow[d, "m"] & G \arrow[l, "(\mathrm{id}\times i)\circ\Delta"'] \arrow[d] \\ \operatorname{Spec} k \arrow[r, "e"] & G & \operatorname{Spec} k \arrow[l, "e"'] \end{tikzcd},$$

where $\Delta : G \to G \times_{\operatorname{Spec} k} G$ is the diagonal embedding in the last diagram. Given such a G and any k-algebra R, the set $\operatorname{Hom}_{\operatorname{Spec} k}(\operatorname{Spec} R, G)$ has a group structure via the morphism $m : G \times_{\operatorname{Spec} k} G \to G$. So we can view this scheme as a functor whose target is the category of groups. Given a group functor G as defined in Definition 1.1, we can take $\operatorname{Spec} \mathscr{O}(G)$ and construct the morphisms m, e, i by Yoneda's lemma, thus these two definitions are actually equivalent. We will switch between these two definitions.

Remark 1.2. There is another definition of affine group schemes via *Hopf algebras*, but we will only use it in the proof of Proposition 1.5. For an affine group scheme $G = \operatorname{Spec}(\mathscr{O}(G))$, the existence of morphisms m, e, i above gives $\mathscr{O}(G)$ a commutative Hopf k-algebra structure. For the definition of Hopf algebras, see [Mil17, Chapter 3]. Conversely, the spectrum of a commutative Hopf algebra over k is an affine group scheme.

We also have the notion of subgroups:

Definition 1.2. A *k-subgroup* scheme of an affine k-group scheme G is a k-subscheme H satisfying that $H(R)$ is an (abstract) subgroup of $G(R)$ for each k-algebra R. Moreover, it is called a *closed subgroup* scheme if H is a closed subscheme of G.

After introducing the objects, we define the morphisms in this category of affine k-group schemes.

Definition 1.3. A *homomorphism* $\varphi : G \to H$ of affine group schemes is a natural transformation between two group functors. Equivalently, it is a morphism between affine schemes G and H such that $\varphi \circ m_G = m_H \circ (\varphi \times \varphi)$, where m_G, m_H are the multiplication morphisms of G, H respectively. A homomorphism of affine group schemes admitting a two-sided inverse is called an *isomorphism*.

Example 1.1. The *additive group* $\mathbb{G}_a$ is the functor assigning to each k-algebra R its additive group:

$$\mathbb{G}_a(R) = (R, +).$$

It is represented by the polynomial algebra $k[T]$:

$$\mathrm{Hom}_{\mathrm{Spec}\, k}(\mathrm{Spec}\, R, \mathrm{Spec}\, k[T]) = \mathrm{Hom}_k(k[T], R) \simeq (R, +).$$

Example 1.2. The *multiplicative group* $\mathbb{G}_m$ is the functor assigning to each k-algebra R its multiplicative group:

$$\mathbb{G}_m(R) = (R^\times, \cdot).$$

It is represented by $k[T, T^{-1}]$:

$$\mathrm{Hom}_{\mathrm{Spec}\, k}(\mathrm{Spec}\, R, \mathrm{Spec}\, k[T, T^{-1}]) = \mathrm{Hom}_k(k[T, T^{-1}], R) \simeq (R^\times, \cdot).$$

Example 1.3. Another basic example is the *general linear group* GL_n. This is the affine group scheme assigning to each k-algebra R the group of invertible $n \times n$ matrix with coefficients in R. It is represented by $k[T_{ij}, 1 \leq i, j \leq n][S]/(\det(T_{ij}) \cdot S - 1)$. When $n = 1$, we have $\mathrm{GL}_1 \simeq \mathbb{G}_m$. We can also give a coordinate-free definition: if V is a free k-module of rank n, GL_V is the group assigning to each R the group consisting of R-automorphisms of $V \otimes_k R$.

When dealing with group schemes, we often need to change the base ring:

Definition 1.4. Let $k \to k'$ be a homomorphism of rings and G be an affine group scheme over k. The *base change* of G to k' is defined as a group functor that maps each k'-algebra R' to $G(R')$ by viewing R' as a k-algebra. This affine group k'-scheme is represented by $\mathscr{O}(G) \otimes_k k'$ and denoted by $G_{k'}$. Sometimes we also denote this group by $G \otimes_k k'$.

Definition 1.5. Let $k \to k'$ be a homomorphism of rings and G be an affine group scheme over k'. The *Weil restriction* of G to k is defined as a group functor that maps each k-algebra R to $G(k' \otimes_k R)$. This functor is denoted by $\mathrm{Res}_{k'/k} G$ and when k'/k is a finite extension of fields, it is representable and becomes an affine group k-scheme [BLR90, Theorem 7.6.4].

In this thesis, all the affine group schemes we will meet satisfy some finiteness condition:

Definition 1.6. An affine *algebraic* group over k is an affine k-group scheme G such that $\mathscr{O}(G)$ is an algebra of finite type over k.

From now on, we assume that k is a field and fix a separable closure k^{sep} in an algebraic closure $\overline{k}$ of k.

Instead of defining normal subgroups directly, we first state a proposition which shows the existence and uniqueness of *normalizers*.

Proposition 1.1. *[Mil17, Proposition 1.83] Let H be an algebraic subgroup of G. There is a unique algebraic subgroup $N = N_G(H)$ of G such that for any k-algebra R,*

$$N(R) = \{g \in G(R) | gH_R g^{-1} = H_R\}.$$

This subgroup is called the normalizer *of H in G.*

Remark 1.3. Similarly we have a unique subgroup $C = C_G(H)$ which is called the *centralizer* of H in G: for any k-algebra R, $C(R)$ consists of elements in $G(R)$ that centralize $H(R')$ in $G(R')$ for all R-algebras R' [Mil17, Proposition 1.92]. The centralizer of G in G is called the *center* of G, usually denoted by $Z(G)$.

Remark 1.4. If H is a closed subgroup of G, then the normalizer $N_G(H)$ and the centralizer $C_G(H)$ are also closed.

Definition 1.7. A subgroup H of G is *normal* if $H = N_G(H)$.

Now we define injections and surjections for affine algebraic groups over k.

Definition 1.8. A homomorphism $\varphi : H \to G$ between two affine algebraic groups over k is a *monomorphism* (resp. *epimorphism*) if the corresponding k-algebra homomorphism $\varphi^* : \mathscr{O}(G) \to \mathscr{O}(H)$ is surjective (resp. injective).

Remark 1.5. It can be verified that $H \to G$ is a monomorphism if and only if $H(R) \to G(R)$ is injective for all k-algebras R. However, for an epimorphism $H \to G$, $H(R) \to G(R)$ need not to be surjective for some given k-algebra R.

Remark 1.6. It is not easy to define the quotient of an affine algebraic group by its subgroups. However, [Mil17, Theorem 5.14] says that each normal algebraic subgroup N of an affine algebraic group G arises as the kernel of an epimorphism $G \to Q$. So we can view the algebraic group Q as the *quotient group* G/H.

Since here we assume that k is a field, by [Mil17, Corollary 3.35] we have: a monomorphism $\varphi : G \to H$ of affine algebraic k-groups must be a closed embedding of schemes. Hence any subgroup of an affine algebraic group over a field k is automatically a closed subgroup.

An affine algebraic group G is said to be *linear* if there is a homomorphism ρ from G to some general linear group GL_V which is also a closed immersion of k-schemes. We call (ρ, V) a faithful representation of G.

Theorem 1.1. *[Mil17, Corollary 4.10] An affine algebraic group is isomorphic to a closed subgroup of some* GL_n *over* k*.*

Remark 1.7. This theorem tells us an affine algebraic group over a field k must be linear. So we also call it a *linear algebraic group*. In the following text, we often call such G by an *algebraic group* for short.

Another nice property of algebraic groups is that they are often smooth:

Theorem 1.2. *An algebraic group* G *over* k *is smooth if* $\mathrm{char}(k) = 0$ *or if* G *is geometrically reduced.*

Proof. [Liu06, Lemma 4.2.21] shows that any geometrically reduced algebraic variety over k contains a smooth closed point. So if G is geometrically reduced, it must be smooth at some point, then by translations G is smooth everywhere.

If $\mathrm{char}(k) = 0$, this is known as Cartier's theorem, see [Mil17, Theorem 3.23]. $\square$

An algebraic group is called *connected* if its underlying topological space is connected. For an algebraic group G, the connected component of G containing the identity element e is called the *neutral component* of G, denoted by G°. [Mil17, Proposition 1.34] and [Mil17, Proposition 2.37] tell us that G° is a normal algebraic subgroup of G.

Definition 1.9. Let k be an algebraically closed field. A matrix $x \in M_n(k)$ is *semisimple* if it is conjugate to some diagonal matrix, it is *nilpotent* if $x^m = 0$ for some m, and it is *unipotent* if $x - I_n$ is nilpotent. For an algebraic group G, we say that $x \in G(k)$ is *semisimple* (resp. *unipotent*), if for any faithful representation $r : G \to \mathrm{GL}_V$ the image $r(x)$ is so.

If $x \in G(\overline{k})$ satisfies the property that $r(x)$ is semisimple (resp. unipotent) for some r, then it is so for any faithful representation r (see [Hum75, Theorem 15.3]). Similar with what we know in linear algebra, we have the *Jordan decomposition*. This was made a fundamental tool by Chevalley, so sometimes it is called a *Jordan-Chevalley decomposition*.

Theorem 1.3. *[Mil17, Theorem 9.18] Let G be an algebraic group over an algebraically closed field k. Given $x \in G(k)$, there exists a unique decomposition $x = x_s x_u = x_u x_s$ such that x_s is semisimple and x_u is unipotent.*

Jordan decomposition leads us to some notions of algebraic groups. An algebraic group over an arbitrary field k is *unipotent* if every representation of G has a fixed vector. If G is also smooth, then G is unipotent if and only if $G(\overline{k})$ consists of unipotent elements [Mil17, Corollary 14.12].

The *derived subgroup* $G^{\mathrm{der}} = \mathcal{D}G$ of an algebraic group G is the intersection of all normal subgroups $N \leq G$ such that G/N is commutative. If G is connected then G^{der} is connected [Mil17, Corollary 6.19]. We have

$$G^{\mathrm{der}}(\overline{k}) = \langle xyx^{-1}y^{-1} : x, y \in G(\overline{k}) \rangle.$$

We can inductively define $\mathcal{D}^n G = \mathcal{D}(\mathcal{D}^{n-1}G)$, then G is *solvable* if $\mathcal{D}^n(G)$ is trivial for some sufficiently large n. A unipotent group is always solvable.

Definition 1.10. Let G be a smooth algebraic group over k. The *unipotent radical* $R_u(G)$ is the maximal connected unipotent normal subgroup of G. The *(solvable) radical* $R(G)$ is the maximal connected normal solvable subgroup of G. The existences of $R_u(G)$ and $R(G)$ are guaranteed by [Mil17, Proposition 6.42].

A smooth connected algebraic group G is said to be *reductive* if $R_u(G_{\overline{k}}) = 1$ and *semisimple* if $R(G_{\overline{k}}) = 1$.

Remark 1.8. A unipotent group is solvable, so $R_u(G)$ is contained in $R(G)$. This implies that any semisimple group is reductive.

The classification of semisimple groups over an algebraically closed field is related to their root systems. Before stating this correspondence, we first introduce the theory of tori.

Definition 1.11. A *torus* is an algebraic k-group T such that $T_{\overline{k}} \simeq \mathbb{G}_{m,\overline{k}}^n$ for some n. Here $\mathbb{G}_{m,\overline{k}}$ means the multiplicative group over $\overline{k}$. The integer n is called the *rank* of T.

The *character* group of T is $X^*(T) = \mathrm{Hom}(T, \mathbb{G}_{m,k})$, and the *cocharacter* group is $X_*(T) = \mathrm{Hom}(\mathbb{G}_{m,k}, T)$. For a k-algebra k', we often write $X^*(G)_{k'} := X^*(G_{k'})$.

If $T \simeq \mathbb{G}_{m,k}^n$ over k, this torus T is said to be *split*. T is called *anisotropic* if $X^*(T)_k$ is trivial.

Remark 1.9. If T is a torus over k, then T splits over some finite separable extension L/k, in other words $T_L \simeq \mathbb{G}_{m,L}^n$ [Con14, Lemma B.15].

A torus T contained in G is called *maximal* if $T_{\overline{k}}$ is maximal among all the tori contained in $G_{\overline{k}}$. A k-group G is said to be *split* if it has a maximal torus that is split over k.

In 1955, Borel proved the following theorem, which is an analogue of Cartan's theorem in Lie group theory.

Theorem 1.4. *Every connected algebraic group has a maximal torus, and all the maximal tori in $G_{\overline{k}}$ are conjugate under $G(\overline{k})$.*

Proof. The first assertion is due to [Mil17, Corollary 17.83], the second one is [Mil17, Theorem 17.87]. □

By the second assertion of Theorem 1.4, different maximal tori of G have the same rank, which is called the rank of G.

For the remainder of this section, G is a reductive group over a field k and T is a torus contained in G. Let $N_G(T), Z_G(T)$ be the normalizer and centralizer of T in G respectively. A torus T is maximal if and only if $Z_G(T) = T$ [Mil17, Corollary 17.84].

Definition 1.12. The *Weyl group* of T in G is $W(G,T) = N_G(T)/Z_G(T)$.

Given a split reductive group G and a split maximal torus T, for any linear representation $r : G \to \mathrm{GL}_V$ we can decompose V as:

$$V = \bigoplus_{\alpha \in X^*(T)} V_\alpha,$$

where $V_\alpha = \{v \in V \mid r(t).v = \alpha(t)v\}$ is called the *weight space* [Mil17, Theorem 4.25].

Now we consider a special representation of G: let

$$\mathfrak{g} := \ker(G(k[t]/t^2) \to G(k))$$

be the *Lie algebra* of G. For each k-algebra R, the action of $G(R)$ on $G(R[t]/t^2)$ via conjugation induces a representation:

$$\mathrm{Ad} : G \to \mathrm{GL}_{\mathfrak{g}},$$

which is called the *adjoint representation.*

Definition 1.13. A nonzero $\alpha \in X^*(T)$ such that the weight space of α in $\mathfrak{g}$ is nonzero is called a *root* of T in G. We denote the set of all such roots by $\Phi(G,T)$.

We have a decomposition

$$\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi(G,T)} \mathfrak{g}_\alpha,$$

where $\mathfrak{t}$ is the Lie algebra of T. Due to [Mil17, Theorem 21.11(b)], each root space $\mathfrak{g}_\alpha$ has dimension 1.

Let V be a finite-dimensional $\mathbb{R}$-vector space and $\alpha \in V$ a nonzero vector. A *symmetry about a vector* α is an automorphism s of V such that s maps α to $-\alpha$ and the set H of elements of V fixed by s is a hyperplane of V.

Lemma 1.1. *Let α be a nonzero vector of V and let Φ be a finite subset of V which spans V. There is at most one symmetry about α which leaves Φ invariant.*

Proof. Let s and s' be two such symmetries and let u be their product, then u maps α to α and induces the identity on $V/\mathbb{R}\alpha$. This implies that the eigenvalues of u are all equal to 1. Since Φ is finite, there is an integer $n \geq 1$ such that u^n acts as the identity on Φ. Hence $u^n = id$ since Φ spans V, thus u is diagonalizable and therefore $u = \mathrm{id}_V$. Because any symmetry about α has order 2, we have $s = s'$. $\square$

Definition 1.14. Let V be a finite dimensional $\mathbb{R}$-vector space and Φ a finite subset of V. (Φ, V) is a *root system* if it satisfies:

(1) $0 \notin \Phi$, and Φ spans V;

(2) For each $\alpha \in \Phi$, there is a symmetry s_α about α such that $s_\alpha(\Phi) = \Phi$ (this symmetry is unique by Lemma 1.1);

(3) For each $\alpha, \beta \in \Phi$, $s_\alpha(\beta) - \beta \in \mathbb{Z}\alpha$.

$\dim_{\mathbb{R}} V$ is called the rank of this root system. A root system is said to be *reduced* if for each root $\alpha \in \Phi$, $\Phi \cap \mathbb{Z}\alpha = \{\pm\alpha\}$.

The *Weyl group* W of a root system (Φ, V) is the subgroup of $\mathrm{GL}_V(\mathbb{R})$ generated by all the symmetries s_α.

Remark 1.10. We can choose a positive-definite symmetric W-invariant bilinear form $(,)$ on V. For any two roots $\alpha, \beta \in \Phi$, we have the Cartan integer $\langle \alpha, \beta \rangle = \frac{2(\alpha,\beta)}{(\beta,\beta)}$. Two root systems $(\Phi_1, V_1), (\Phi_2, V_2)$ are isomorphic if there is a linear isomorphism $\varphi : V_1 \simeq V_2$ such that $\varphi(\Phi_1) = \Phi_2$ and φ preserves the Cartan integers.

For a reduced root system (Φ, V), we have the notion of base:

Definition 1.15. A subset $\Delta = \{\alpha_1, \cdots, \alpha_l\} \subset \Phi$ is a *basis* of the root system Φ if it is a $\mathbb{R}$-basis of the vector space V and each $\alpha \in \Phi$ can be uniquely expressed as

$$\sum_i^l \lambda_i \alpha_i,$$

where the λ_i's are all integers having the same sign. We define the set of positive roots to be

$$\Phi^+ = \big(\sum_{i=1}^l \mathbb{Z}_{\geq 0}\alpha_i\big) \cap \Phi$$

and Φ^- to be its complement in Φ, or equivalently $\Phi^- = -\Phi^+$.

For a split reductive group G and a split maximal torus $T \leq G$, we can define:

$$\Phi = \Phi(G,T), V = \mathrm{Span}_{\mathbb{R}}(\Phi(G,T)) \subset X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}.$$

Actually we obtain a root system:

Proposition 1.2. *[Hum75, Theorem 27.1] The (Φ, V) defined above is a reduced root system, the rank is equal to the rank of G, and two notions of Weyl group coincide:*

$$W(\Phi, V) \simeq W(G, T)(k).$$

Under this correspondence, the choice of a basis of (Φ, V) corresponds to the choice of a *Borel subgroup* of G containing T.

Definition 1.16. Let G be a reductive group over a field k. A closed subgroup $B \leq G$ is called a *Borel subgroup* if $B_{\overline{k}}$ is a maximal smooth connected solvable subgroup of $G_{\overline{k}}$. G is *quasi-split* if it contains a Borel subgroup.

Then the correspondence can be described as:

Theorem 1.5. *Let G be a quasi-split reductive group and $T \leq G$ a maximal split torus. Then there is a bijection between the set of bases $\Delta \subseteq \Phi(G, T)$ and the set of Borel subgroups containing $Z_G(T)$.*

Proof. See [Bor91, Proposition 21.9]. Notice that in [Bor91], he uses *minimal parabolic groups* in order to deal with the case where Borel k-subgroups do not exist, but here we assume that G is quasi-split, thus minimal parabolic subgroups are just Borel subgroups. ☐

The classification of semisimple algebraic groups over an algebraically closed field is proved by Chevalley:

Theorem 1.6. *[Hum75, Theorem 32.1] An epimorphism $G \to G'$ whose kernel is finite is called an* isogeny*. Semisimple algebraic groups over $\overline{k}$ are classified up to isogeny by the isomorphism classes of their associated reduced root systems.*

Definition 1.17. Let G be a semisimple group over k. G is *simply-connected* if any central isogeny $H \to G$ is an isomorphism.

Combine this definition with Theorem 1.6, we obtain that there is a bijection between the isomorphism classes of simply-connected semisimple algebraic $\overline{k}$-groups and isomorphism classes of reduced root systems.

Definition 1.18. Let G be an algebraic group over a field k. If it is semisimple and non-commutative, and every proper normal algebraic subgroup of G is finite, then we say G is *almost-simple.*

We can decompose any simply-connected semisimple algebraic group into a direct product of almost-simple groups:

Theorem 1.7. *[Mil17, Theorem 24.3] Let G be a simply-connected semisimple algebraic group over a field k, then there exist almost-simple algebraic groups $G_i, 1 \leq i \leq r$ such that*

$$G \simeq G_1 \times \cdots \times G_r.$$

Therefore, to understand all simply-connected semisimple algebraic groups over k, it suffices to understand the simply-connected almost-simple groups. So we can reduce the problem to simply-connected almost-simple algebraic groups in Section 1.3. By [Mil17, Proposition 24.1], the associated root system of an almost-simple group is indecomposable, and must be of one of these types:

$$A_n(n \geq 1), B_n(n \geq 2), C_n(n \geq 3), D_n(n \geq 4), E_6, E_7, E_8, F_4, G_2,$$

here the subscript equals to the rank of this group.

In the end of this section, we give the definition of *hyperspecial* subgroups, which was originally given by Tits.

Let G be a reductive group over a nonarchimedean local field F and $\mathscr{O}$ be the ring of integers of F. The F-points $G(F)$ is actually a topological group.

We first define this topology for $G = \mathrm{GL}_n$: if ϖ is a uniformizer for $\mathscr{O}$, then

$$\{I_n + \varpi^k M_n(\mathscr{O}) \mid k \geq 1\}$$

forms a neighborhood base of the identity element in $\mathrm{GL}_n(F)$. This topology is the same with the subspace topology induced by $\mathrm{GL}_n(F) \subset M_n(F)$.

In order to define a topology on $G(F)$, we choose an embedding $G \hookrightarrow \mathrm{GL}_n$ and give $G(F)$ the subspace topology induced from $\mathrm{GL}_n(F)$.

Remark 1.11. Weil and Grothendieck both gave approaches to topologizing the points of schemes of finite type over a topological ring (for example, a local field or the adèle ring of a global field). This can be seen in [Con12]. Their results tell us the topology we give on $G(F)$ is independent of the choice of the embedding $G \hookrightarrow \mathrm{GL}_n$.

Definition 1.19. Let G be a reductive group over a nonarchimedean local field F. Let $\mathscr{O}$ be the ring of integers of F and k the residue field. A subgroup K of $G(F)$ is called *hyperspecial* if there exists a smooth group scheme Γ over $\mathscr{O}$ such that $\Gamma_F = G$, the special fiber Γ_k is a connected reductive group, and $\Gamma(\mathscr{O}) = K$.

In [Mac17, Section 1.2] we can see that G is unramified, which means it is quasi-split and splits over a finite unramified extension of F, if and only if $G(F)$ admits hyperspecial subgroups. Moreover a hyperspecial subgroup is also a maximal compact subgroup of the topological group $G(F)$.

1.2 Galois Cohomology

At first, we give the definition of non-abelian continuous cohomology of groups:

Definition 1.20. Let G be a topological group and A be a topological group with a continuous G-action. We denote the action by $ga := g(a), g \in G, a \in A$.

(1)The 0th cohomology group is $H^0(G, A) = {}^G A := \{a \in A | ga = a, \forall g \in G\}$;

(2)A 1-*cocycle* is a continuous map $G \to A, s \mapsto a_s$ such that

$$\forall s, t \in G, a_{st} = a_s s(a_t).$$

We denote the set of 1-cocycles by $Z^1(G, A)$. Two 1-cocycles $(s \mapsto a_s), (s \mapsto b_s)$ are said to be *cohomologous*, if there exists a $c \in A$ such that

$$\forall s \in G, b_s = c^{-1} a_s s(c).$$

This defines an equivalence relation between 1-cocycles, then we define the 1st cohomology set $H^1(G, A)$ to be the set of equivalence classes of 1-cocycles. This is a pointed set with the distinguished point being $s \mapsto 1$.

Theorem 1.8. *Let G be a topological group and A, B, C three topological groups with continuous G-actions. An G-equivariant exact sequence*

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

gives rise to an exact sequence of pointed sets:

$$1 \longrightarrow {}^G A \longrightarrow {}^G B \longrightarrow {}^G C \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C)$$

Remark 1.12. This is a part of the famous *long exact sequence theorem.* Moreover, when A is contained in the center of B, this exact sequence can be extended by adding $\to H^2(G, A)$ to the rightest side. We will use $H^2(G, A)$ in the proof of Proposition 1.7. Notice that we did not define $H^2(G, A)$ in Definition 1.20, but what we only need to know is that

$$H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mu_n) \simeq \mathrm{Br}(\mathbb{Q})[n],$$

where μ_n is the group of nth roots of unity and $\mathrm{Br}(\mathbb{Q})[n]$ is the n-torsion subgroup of the Brauer group over $\mathbb{Q}$. See [Ser94, Chapter 5] for a detailed treatment of this.

We apply Definition 1.20 to the following case: take $G = \mathrm{Gal}(L/k)$ to be a Galois group with profinite topology, and take A to be a discrete topological group with a continuous G-action. In this case, when defining a 1-cocycle, the condition that the map is continuous is equivalent to that it factors through a finite extension of k.

Now we use Galois cohomology to classify the so-called k-forms of an algebraic group.

Definition 1.21. Let G_0 be an algebraic group over a field k. If G is an algebraic group over k and its base change G_L is isomorphic with $G_{0,L}$ for some field extension L of k, we call G a *L/k-form* of G_0. A $\overline{k}/k$-form of G_0 is called a *k-form* of G_0.

Now we assume that L is a Galois extension of k. Let $\mathcal{S}(L/k, G_0)$ be the set of L/k-forms of G_0. Two L/k-forms G, G' are said to be equivalent if they are isomorphic over k. Denote the equivalence class containing G by $[G]$. Let $\mathscr{S}(L/k, G_0)$ be the set of equivalence classes of L/k-forms of G_0.

For $s \in \mathrm{Gal}(L/k)$ and an isomorphism $f : G_1 \to G_2$ of algebraic groups over L, we can define an action:

$$s.f(g) = s(f(s^{-1}(g))), \forall g \in G_1.$$

In particular, $f \mapsto s.f$ gives a Galois action on $\mathrm{Aut}_L(G_{0,L})$. Thus we can apply Definition 1.20 to this action and obtain $H^1(\mathrm{Gal}(L/k), \mathrm{Aut}_L(G_{0,L}))$. Now we want to give an explicit description of this cohomology set.

Given a L/k-form G of G_0, by definition we have an isomorphism $f : G_{0,L} \to G_L$ over L. Define a continuous map:

$$a : \mathrm{Gal}(L/k) \to \mathrm{Aut}_L(G_{0,L}), s \mapsto a_s = f^{-1} \circ s.f$$

Proposition 1.3. *The map a defined above is a 1-cocycle in $Z^1(\mathrm{Gal}(L/k), \mathrm{Aut}_L(G_{0,L}))$. Moreover, the 1-cocycles defined by two L/k-forms G, G' are cohomologous if and only if $[G] = [G']$.*

Proof. For $s, t \in \mathrm{Gal}(L/k)$,

$$\begin{aligned} a_{st} &= f^{-1} \circ (st).f = f^{-1} \circ s.f \circ s.(f^{-1}) \circ (st).f \\ &= (f^{-1} \circ s.f) \circ s.(f^{-1} \circ t.f) \\ &= a_s \circ s(a_t), \end{aligned}$$

so $s \mapsto a_s$ is a 1-cocycle.

If $[G] = [G'] \in \mathscr{S}(L/k, G_0)$, then we have two isomorphisms over L:

$$f : G_{0,L} \to G_L, \quad f' : G_{0,L} \to G'_L \tag{1}$$

and an isomorphism $h : G' \to G$ over k.

Two 1-cocycles defined via f, f' are $s \mapsto a_s = f^{-1} \circ s.f, s \mapsto b_s = f'^{-1} \circ s.f'$. Let $c = f^{-1} \circ h_L \circ f' \in \mathrm{Aut}_L(G_0, L)$, then

$$\begin{aligned} c^{-1} \circ a_s \circ s(c) &= (f^{-1} \circ h_L \circ f')^{-1} \circ (f^{-1} \circ s.f)s.(f^{-1} \circ h_L \circ f') \\ &= (f'^{-1} \circ h_L^{-1} \circ f) \circ (f^{-1} \circ s.f) \circ ((s.f^{-1}) \circ (s.h) \circ (s.f')) \\ &= f'^{-1} \circ s.f' = b_s, \end{aligned}$$

thus the two 1-cocyles are cohomologous.

Conversely, given $[G], [G'] \in \mathscr{S}(L/k, G_0)$ with isomorphisms f, f' in (1) such that their associated 1-cocycles $a \mapsto a_s$ and $s \mapsto b_s$ are cohomologous. There exists an automorphism $c \in \mathrm{Aut}_L(G_{0,L})$ such that $b_s = c^{-1} \circ a_s \circ s(c)$ for any $s \in \mathrm{Gal}(L/k)$. This shows that

$$c^{-1} \circ f^{-1} \circ (s.f) \circ (s.c) = f'^{-1} \circ s.f',$$

which tells us $s.(f \circ c \circ f'^{-1}) = f \circ c \circ f'^{-1}$ for any element $s \in \mathrm{Gal}(L/k)$. Hence $f \circ c \circ f'^{-1}$ is an isomorphism defined over the base field k, thus $[G] = [G']$. $\square$

Corollary 1.1. *The map*

$$\begin{aligned} \theta : \mathscr{S}(L/k, G_0) &\to H^1(\mathrm{Gal}(L/k), \mathrm{Aut}_L(G_0)) \\ [G] &\mapsto [(s \mapsto a_s)] \end{aligned}$$

is a bijection.

Proof. The surjectivity can be seen in [Ser94, Proposition III.5]. The proof depends on the fact that an algebraic group is quasi-projective and we can define its quotient groups. The main idea of the proof is twisting the Galois action on G_0 with the given 1-cocycle. $\square$

When we take L to be the algebraic closure $\overline{k}$ of k, we write the set $H^1(\mathrm{Gal}(\overline{k}/k), A)$ as $H^1(k, A)$ for short.

Now we let G_0 be a simply-connected almost-simple algebraic group over k. The conjugation by elements of $G_0(\overline{k})$ gives rise to a subgroup $\mathrm{Inn}(G_0)$ of $\mathrm{Aut}_{\overline{k}}(G_{0,\overline{k}})$, which is called the *inner automorphism group.* Obviously, we have an isomorphism $\mathrm{Inn}(G_0) \simeq (G_0/Z(G_0))(\overline{k})$. Fix a maximal $\overline{k}$-torus $T_0 \leq G_{0,\overline{k}}$ and a Borel $\overline{k}$-subgroup B_0 containing T_0, then we obtain a root system $\Phi(G_{0,\overline{k}}, T_0)$ with a choice of base Δ_0. A well-known fact [Mil17, Appendix C.g] is that the isomorphism classes of reduced root systems can be classified by Dynkin diagrams. We denote the Dynkin diagram associated to $\Phi(G_{0,\overline{k}}, T_0)$ by Σ_0.

Definition 1.22. A *pinning* of $G_{0,\overline{k}}$ is a tuple $(B, T, \{X_\alpha\}_{\alpha\in\Delta})$, where T is a maximal $\overline{k}$-torus in $G_{0,\overline{k}}$, B is a Borel $\overline{k}$-subgroup containing T, Δ is the set of simple roots associated to B, and X_α is a nonzero element in the root space $\mathfrak{g}_{0,\alpha}$ for each simple root $\alpha \in \Delta$.

The group of automorphisms of $G_{0,\overline{k}}$ preserving B,T and the set $\{X_\alpha\}_{\alpha\in\Delta}$ is isomorphic to the automorphism group of the Dynkin diagram Σ_0 [Mil17, Proposition 23.45].

Proposition 1.4. *There is a split exact sequence*

$$1 \longrightarrow \mathrm{Inn}(G_0) \longrightarrow \mathrm{Aut}_{\overline{k}}(G_{0,\overline{k}}) \longrightarrow \mathrm{Aut}(\Sigma_0) \longrightarrow 1. \tag{2}$$

Proof. Denote the second arrow in the sequence by a and the third one by b. Obviously a is injective.

For any $\phi \in \mathrm{Aut}_{\overline{k}}(G_{0,\overline{k}})$, there exists some $g \in G_0(\overline{k})$ such that $\phi \circ \mathrm{Ad}(g)$ preserves both B and T. Thus $\phi \circ \mathrm{Ad}(g)$ defines an automorphism of the root system $\Phi(G_0, T)$. Replacing g by tg for some $t \in T(\overline{k})$, we may assume that $\phi \circ \mathrm{Ad}(g)$ also preserves the basis Δ of the root system. In this way we obtain the map b. It is surjective and we can check that $\mathrm{Im}(a) = \mathrm{Ker}(b)$.

As explained above, the subgroup preserving a pinning gives us a splitting of this short exact sequence. $\square$

With this split short exact sequence in mind, we can define inner forms and pure inner forms of G_0:

Definition 1.23. A k-form G of G_0 is called an *inner form* if $\theta([G])$ lies in the image of the map $H^1(k, \mathrm{Inn}(G_0)) \to H^1(k, \mathrm{Aut}_{\overline{k}}(G_{0,\overline{k}}))$. Moreover, it is called a *pure inner form*, if the cohomology class $\theta([G])$ lies in the image of

$$H^1(k, G_0(\overline{k})) \longrightarrow H^1(k, (G_0/Z(G_0))(\overline{k})) \simeq H^1(k, \mathrm{Inn}(G_0)) \longrightarrow H^1(k, \mathrm{Aut}_{\overline{k}}(G_{0,\overline{k}})).$$

1.3 Non-split Groups with Models

If G is a connected reductive $\mathbb{Q}$-group, we call $\mathscr{G}$ a $\mathbb{Z}$*-model* of G if $\mathscr{G}$ is a reductive $\mathbb{Z}$-group scheme with the generic fiber $\mathscr{G}_{\mathbb{Q}} \simeq G$. Here a *reductive $\mathbb{Z}$-group scheme* means a smooth affine group scheme $\mathscr{G}$ of finite type over $\mathbb{Z}$ whose fiber $\mathscr{G} \otimes \mathbb{Z}/p\mathbb{Z}$ is a reductive algebraic group for each finite prime p.

A *Chevalley group* is a reductive $\mathbb{Z}$-group scheme which has a fiberwise maximal $\mathbb{Z}$-torus. Any Chevalley group $\mathscr{G}$ is a $\mathbb{Z}$-model of its generic fiber $G = \mathscr{G}_{\mathbb{Q}}$. The generic fiber of a Chevalley group is split. Conversely, in [DG70] we have:

Theorem 1.9. *Every split connected reductive $\mathbb{Q}$-group G has a Chevalley group as a $\mathbb{Z}$-model, and this group is unique up to $\mathbb{Z}$-group isomorphism.*

In this section, we consider another class of $\mathbb{Q}$-groups arising as generic fibers of non-Chevalley $\mathbb{Z}$-groups. Now as we mentioned in Section 1.1, we can assume that G is a simply-connected almost-simple algebraic group over $\mathbb{Q}$. Not all such $\mathbb{Q}$-groups admit $\mathbb{Z}$-models, but the following proposition proved by Harder gives us a necessary and sufficient condition:

Proposition 1.5. *If G admits a $\mathbb{Z}$-model $\mathscr{G}$, then G is split over $\mathbb{Q}_p$ for all primes p. Moreover, $\mathscr{G}(\mathbb{Z}_p)$ is a hyperspecial maximal compact subgroup of the locally compact group $G(\mathbb{Q}_p)$.*

Conversely, if G is split over $\mathbb{Q}_p$ for all primes p, then G has a $\mathbb{Z}$-model.

Proof. If $\mathscr{G}$ is a $\mathbb{Z}$-model of G, by definition $\mathscr{G}(\mathbb{Z}_p)$ is a hyperspecial subgroup of $G(\mathbb{Q}_p)$. By the ressult we stated in the end of Section 1.1, the existence of such a hyperspecial subgroup implies that G is unramified.

Fix a maximal torus T of G, and let Σ be the Dynkin diagram corresponding to $(G_{\overline{\mathbb{Q}}}, T_{\overline{\mathbb{Q}}})$. By Proposition 1.4, we have a morphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\overline{\mathbb{Q}}}(G_{\overline{\mathbb{Q}}}) \to \mathrm{Aut}(\Sigma)$, thus we have a Galois action on Σ. The kernel of this morphism has finite index in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ because $\mathrm{Aut}(\Sigma)$ is a finite group, thus there exists a finite field extension L of $\mathbb{Q}$ such that $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ equals to this kernel. This means we have an injection $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(\Sigma)$.

Suppose that $L \neq \mathbb{Q}$, then by Minkowski's theorem some rational prime p is ramified in L. Choose one place of L over p, denoted by v, then the completion L_v is ramified over $\mathbb{Q}_p$. In this way we obtain an injection $\mathrm{Gal}(L_v/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(\Sigma)$. However, since G is unramified, it is split over a finite unramified extension of $\mathbb{Q}_p$. This tells us the action of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ on Σ must factor through a finite unramified extension over $\mathbb{Q}_p$, which is a contradiction to the injection $\mathrm{Gal}(L_v/\mathbb{Q}_p) \hookrightarrow \mathrm{Aut}(\Sigma)$. Hence $L = \mathbb{Q}$ and as a consequece the action of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ on Σ is trivial for each p. Since the base change $G_{\mathbb{Q}_p}$ is quasi-split for each p, the Galois action on Σ is trivial implies that $G_{\mathbb{Q}_p}$ is split over $\mathbb{Q}_p$.

Conversely, assume that G is split over $\mathbb{Q}_p$ for all primes p. Embed G into the general linear group GL_V for some finite-dimensional $\mathbb{Q}$-vector space V and take a lattice L in V, then we can construct an affine group scheme $H = \mathrm{GL}_L \cap G$. By [Tit79, Proposition 3.9], $H_{\mathbb{Q}} \simeq G$ and H has reductive fibers for almost all primes except a finite subset S, which is the set of primes where H has "bad reduction". So H is a model of G over $\mathbb{Z}_S = \mathbb{Z}[1/N]$, where $N = \prod_{p \in S} p$.

For any prime $p \in S$, since G is split over $\mathbb{Q}_p$, we have a hyperspecial maximal compact subgroup K_p of $G(\mathbb{Q}_p)$. Let $\mathscr{G}_p$ be a reductive group scheme over $\mathbb{Z}_p$ with $\mathscr{G}_p(\mathbb{Z}_p) = K_p$ and $\mathscr{G}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq G_{\mathbb{Q}_p}$. Denote $\mathbb{Z}[1/p]$ by $\mathbb{Z}_{(p)}$, which can be viewed as a subring of $\mathbb{Z}_p$, then we have an isomorphism between affine group schemes:

$$\tau_p : G \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq G_{\mathbb{Q}_p} \simeq \mathscr{G}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Apply Proposition 1.6 below to $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$ and the triple $(G, \mathscr{G}_p, \tau_p)$, then there exists a unique model $\mathscr{G}_{(p)}$ for G over $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ such that the base change of $\mathscr{G}_{(p)}$ to $\mathbb{Z}_p$ is isomorphic to $\mathscr{G}_p$.

Since $\mathscr{O}(H) \otimes_{\mathbb{Z}_S} \mathbb{Q} \simeq \mathscr{O}(G), \mathscr{O}(\mathscr{G}_{(p)}) \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q} \simeq \mathscr{O}(G), p \in S$, we can view $\mathscr{O}(H), \mathscr{O}(\mathscr{G}_{(p)})$ as subrings of $\mathscr{O}(G)$. Now we define a Hopf algebra of finite type over $\mathbb{Z}$:

$$\mathscr{O} = \mathscr{O}(H) \cap \bigcap_{p \in S} \mathscr{O}(\mathscr{G}_{(p)}) \subset \mathscr{O}(G).$$

It is obvious that $\mathscr{O} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathscr{O}(G)$, then we are going to show that

$$\mathscr{O} \otimes_{\mathbb{Z}} \mathbb{Z}_S = \mathscr{O}(H), \mathscr{O} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} = \mathscr{O}(\mathscr{G}_{(p)}), \forall p \in S.$$

For any element $x \in \mathscr{O}(H) \subset \mathscr{O}(G)$ and any $p \in S$, x can be written as a polynomial of elements in $\mathscr{O}(\mathscr{G}_{(p)})$ with coefficients in $\mathbb{Q}$. Since any prime other than p is invertible in $\mathbb{Z}_{(p)}$, there exists some positive integer n_p such that $p^{n_p}x$ is an element in $\mathscr{O}(\mathscr{G}_{(p)})$. If we take $n_0 = \max_{p \in S}\{n_p\}$, then $N^{n_0}x \in \mathscr{O}$, thus $x = \frac{1}{N^{n_0}} \cdot (N^{n_0}x) \in \mathscr{O} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. So we obtain the desired identity $\mathscr{O} \otimes_{\mathbb{Z}} \mathbb{Z}_S = \mathscr{O}(H)$. By the same argument, $\mathscr{O} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} = \mathscr{O}(\mathscr{G}_{(p)})$ for each $p \in S$.

Now we let $\mathscr{G}$ be the affine $\mathbb{Z}$-group scheme $\mathrm{Spec}(\mathscr{O})$ defined by this Hopf algebra, then it is a model for G over $\mathbb{Z}$. □

Proposition 1.6. *[BLR90, Chapter 6, Proposition D.4] Let $R \subset R'$ be a pair of discrete valuation rings with same uniformizing element π and with the same residue field and denote their fields of fractions by K and K'. The functor which associates to each R-scheme X the triple (X_K, X', τ) consists of the K-scheme $X_K = X \otimes_R K$, the R'-scheme $X' = X \otimes_R R'$, and the canonical isomorphism $\tau : X_K \otimes_K K' \simeq X' \otimes_{R'} K'$ is fully faithful. Its essential image consists of all triples (X_K, X', τ) which admit a quasi-affine open covering.*

Now we are going to give a cohomological interpretation of this sufficient and necessary condition and use this to enumerate the groups over $\mathbb{Q}$ which have $\mathbb{Z}$-models.

Let G_0 be a *split form* of G, which means G_0 is a simply-connected semisimple algebraic group that is split over $\mathbb{Q}$ and $G_0 \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \simeq G \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$. The group G is also a $\mathbb{Q}$-form of G_0 by definition. As we stated in Section 1.2, such a $\mathbb{Q}$-form G determines a cohomology class $c(G)$ in $H^1(\mathbb{Q}, \mathrm{Aut}_{\overline{\mathbb{Q}}}(G_{0,\overline{Q}}))$.

Proposition 1.7. *Let G be a almost-simple simply-connected algebraic group over $\mathbb{Q}$, and G_0 be a split form of G. The followings are equivalent:*

(1) G admits a $\mathbb{Z}$-model.

(2) G is a pure inner form of G_0.

Proof. (1) $\Rightarrow$ (2): If G admits a model over $\mathbb{Z}$, we have already seen that the Galois action on its Dynkin diagram Σ is trivial in the proof of Proposition 1.5. Consider the long exact sequence associated to the short exact sequence in Proposition 1.4:

$$H^1(\mathbb{Q}, \mathrm{Inn}(G_{0,\overline{\mathbb{Q}}})) \longrightarrow H^1(\mathbb{Q}, \mathrm{Aut}_{\overline{\mathbb{Q}}}(G_{0,\overline{\mathbb{Q}}})) \longrightarrow H^1(\mathbb{Q}, \mathrm{Aut}(\Sigma)).$$

Since $c(G)$ is sent to the trivial element in $H^1(\mathbb{Q}, \mathrm{Aut}(\Sigma))$, it arises from an element in $H^1(\mathbb{Q}, \mathrm{Inn}(G_{0,\overline{\mathbb{Q}}}))$, thus G is an inner form of G_0. We can view $c(G)$ as the image of some cohomology class c' contained in $H^1(\mathbb{Q}, (G_0/Z(G_0))(\overline{\mathbb{Q}}))$. Since G is split over any $\mathbb{Q}_p$, the local restrictions $c'|_{\mathbb{Q}_p} \in H^1(\mathbb{Q}_p, (G_0/Z(G_0))(\overline{\mathbb{Q}_p}))$ are all trivial.

The Hasse principle for semisimple groups [PR94, Section 6.5] says that the map

$$H^1(\mathbb{Q}, (G_0/Z(G_0))(\overline{\mathbb{Q}})) \longrightarrow \prod_v H^1(\mathbb{Q}_v, (G_0/Z(G_0))(\overline{\mathbb{Q}_v}))$$

is injective, so c' is determined by its restriction c'_∞ in $H^1(\mathbb{R}, G_0/Z(G_0)(\mathbb{C}))$. By the theorem of long exact sequence, we obtain an exact sequence:

$$H^1(\mathbb{Q}, Z(G_0)(\overline{\mathbb{Q}})) \longrightarrow H^1(\mathbb{Q}, G_0(\overline{\mathbb{Q}})) \longrightarrow H^1(\mathbb{Q}, (G_0/Z(G_0))(\overline{\mathbb{Q}})) \xrightarrow{\delta} H^2(\mathbb{Q}, Z(G_0)(\overline{\mathbb{Q}})),$$

similarly for each $\mathbb{Q}_v$. The class $\delta(c')$ restricts to $(\delta_\infty(c'_\infty), 0, \ldots, 0) \in \bigoplus_v H^2(\mathbb{Q}_v, Z(G_0)(\overline{\mathbb{Q}_v}))$.

As the center of a split simply-connected semisimple group, by [Bum04, Theorem 26.3] $Z(G_0)$ is the Cartier dual of the fundamental group $X^*(T)/\mathbb{Z}\Phi$ of the root system $\Phi(G_0, T)$, so it must be isomorphic to $\mu_n (n \geq 1)$ or $\mu_2 \times \mu_2$. Thus $H^2(\mathbb{Q}, Z(G_0)(\overline{\mathbb{Q}}))$ is isomorphic to either the Brauer group $\mathrm{Br}(\mathbb{Q})[n]$ or $\mathrm{Br}(\mathbb{Q})[2] \times \mathrm{Br}(\mathbb{Q})[2]$, and can be viewed as a subgroup of $\mathrm{Br}(\mathbb{Q}/\mathbb{Z})$. The global class field theory [Wei95, Chapter XIII, Theorem 4] tells us, the image of an element of $\mathrm{Br}(\mathbb{Q}/\mathbb{Z})$ in $\prod_v \mathrm{Br}(\mathbb{Q}_v/\mathbb{Z}_v)$ vanishes at almost every place and their sum is 0 in $\mathrm{Br}(\mathbb{Q}/\mathbb{Z})$. Apply this to our case here, $\delta_\infty(c'_\infty)$ must be trivial too, thus c' is in the image of the cohomology set $H^1(\mathbb{Q}, G_0(\overline{\mathbb{Q}}))$.

(2) $\Rightarrow$ (1): If G is a pure inner form, then $G_{\mathbb{Q}_p}$ is obtained by a cohomology class in the set $H^1(\mathbb{Q}_p, G_0(\overline{\mathbb{Q}_p}))$, which is trivial by [PR94, Theorem 6.4] as G_0 is simply-connected, thus G is split over each nonarchimedean local field $\mathbb{Q}_p$. By Proposition 1.5, G admits a $\mathbb{Z}$-model. $\square$

Remark 1.13. From the proof we can see that G is a pure inner form is equivalent to that $c_p(G)$ is trivial for any finite prime p and $c_\infty(G)$ is in the image of

$$H^1(\mathbb{R}, G_0(\mathbb{C})) \longrightarrow H^1(\mathbb{R}, \mathrm{Aut}_{\mathbb{C}}(G_{0,\mathbb{C}})).$$

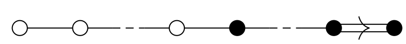
From Remark 1.13, we may wonder if we can classify such G by real forms. Actually, in [CG12] Conrad proves the following proposition:

Proposition 1.8. *[CG12, Proposition 4.10] Each almost-simple simply-connected $\mathbb{Q}$-group G admitting a $\mathbb{Z}$-model is determined by $G_{\mathbb{R}}$ up to $\mathbb{Q}$-isomorphism.*

By this proposition, the image of $H^1(\mathbb{R}, G_0(\mathbb{C}))$ in $H^1(\mathbb{R}, \mathrm{Aut}_{\mathbb{C}}(G_{0,\mathbb{C}}))$ parametrizes these $G_{\mathbb{R}}$. A table of different $|H^1(\mathbb{R}, G_0)|$ can be found on `www.liegroups.org/tables/galois/`.

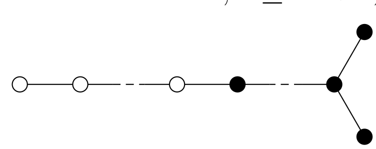
We can list these possibilities of $G_{\mathbb{R}}$ by giving the real Satake diagram of the non-split groups $G(\mathbb{R})$:

$B_n, n \geq 3$



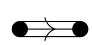
k white vertices, $0 \leq k < n, k \equiv n, n+1 \bmod 4$

$D_n, n \geq 4$

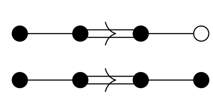


k white vertices, $0 \leq k < n, k \equiv n \bmod 4$

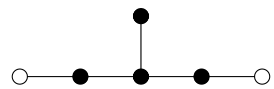
G_2



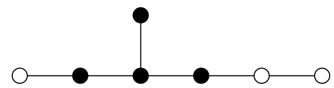
F_4



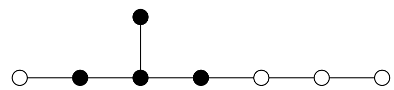
E_6

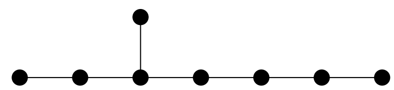


E_7



E_8





Here a real Satake diagram is obtained in the following way: given a group $G_{\mathbb{R}}$ over $\mathbb{R}$, then we choose a maximal $\mathbb{R}$-split torus S in $G_{\mathbb{R}}$ and a maximal torus T containing S, which means $T_{\mathbb{C}}$ is maximal among tori of $G_{\mathbb{C}}$. Choose a Borel $\mathbb{C}$-subgroup of $G_{\mathbb{C}}$ containing $T_{\mathbb{C}}$, then we get a basis Δ of the root system and can draw the Dynkin diagram Σ. For each $\alpha \in \Delta$, if it is trivial on S when we view it as a character of T, then we blacken the point in Σ corresponding to α. If two simple roots α, β are conjugate under the non-trivial element in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, then we connect these two points in Σ. This new diagram we obtain is called the real Satake diagram associated to $G_{\mathbb{R}}$.

In particular, the anisotropic groups correspond to the Satake digrams whose points are all blackened. These groups are:

$B_{(d-1)/2}$: $\mathrm{Spin}(\mathbb{Q}^d, \frac{1}{2}\sum_{i=1}^{d} x_i^2), d \equiv \pm 1 \bmod 8$;

$D_{d/2}$: $\mathrm{Spin}(\mathbb{Q}^d, \frac{1}{2}\sum_{i=1}^{d} x_i^2), d \equiv 0 \bmod 8$;

G_2 : The automorphism group of Cayley's definite octonion;

F_4 : The automorphism group of the 27-dimensional exceptional Jordan algebra;

E_8 : The isometry group of the 128-dimensional "octonionic projective plane".

Later we will explain these groups except E_8.

2 The Mass Formula

A simply-connected almost-simple group G admitting a $\mathbb{Z}$-model may admit more than one $\mathbb{Z}$-model $\mathscr{G}$. The mass formula can help us enumerate all such $\mathscr{G}$ in some cases. Before we state this, we introduce some notions that will appear in the formula and some theorems we are going to use.

2.1 Invariants of the Weyl Group

In this section, we assume that k is a field of characteristic 0.

Definition 2.1. Let V be a finite dimensional vector space over k. We define the *ith tensor power* of V to be the tensor product of V with itself i times: $T^kV = V^{\otimes i}$. By convention, $T^0V = k$. The *tensor algebra* of V is

$$T(V) := \bigoplus_{i=0}^{\infty} T^iV = \bigoplus_{i=0}^{\infty} V^{\otimes i}.$$

The multiplication in $T(V)$ is determined by the canonical isomorphism given by the tensor product:

$$T^iV \otimes T^jV \simeq T^{i+j}V.$$

Definition 2.2. Let V be a finite dimensional vector space over k. Let I be the two-sided ideal of $T(V)$ generated by the elements $x \otimes y - y \otimes x$, where $x, y \in V$. The *symmetric algebra* of V is defined to be the quotient algebra:

$$S(V) := T(V)/I.$$

Remark 2.1. $T(V)$ is a graded k-algebra, whose degree i part is T^iV. This also induces a graded algebra structure on $S(V)$, where the degree i part S^iV is the image of T^iV under the quotient morphism.

Let $G \subset \mathrm{GL}_V(k)$ be a finite subgroup. This group also acts on $T(V)$ and preserves the ideal I, so it induces an action on $S(V)$. The space $S(V)^G$ consisting of elements invariant under G is called the *ring of invariants* of G.

Most rings of invariants are not polynomial rings, but for a group generated by pseudo-reflections, it is always a polynomial ring [Bou07, Theorem V.5.4]. Here a *pseudo-reflection* means a linear automorphism of finite order whose fixed subspace is a hyperplane.

Notice that $S(V)^G$ admits a natural structure of graded algebra, thus we can define a Poincaré series associated to it.

Definition 2.3. Let $M = \oplus_{i\geq 0} M_i$ be a graded k-vector space and $\dim_k M_i < \infty$ for each i. The *Poincaré series* of M is defined as

$$P_t(M) = \sum_{i\geq 0} (\dim_k M_i) t^i.$$

Theorem 2.1. *(Molien) If G is a finite subgroup of $\mathrm{GL}_V(k)$, then the Poincaré series of the graded algebra $S(V)^G$ equals to*

$$\frac{1}{|G|} \sum_{g\in G} \frac{1}{\det(1-tg)}.$$

Proof. Consider the action of an element $g \in G$ on $U = \bigoplus_{i\geq 0} t^i S^i V$. By diagonalizing g as a diagonal matrix $\mathrm{diag}(x_1, \cdots, x_n)$, the trace of g on U is

$$\sum_{i=0}^{\infty} \Big(\sum_{1\leqslant j_1,\cdots,j_n\leqslant n} x_{j_1} \cdots x_{j_n} \Big) t^i = \prod_{j=1}^{n} \frac{1}{1-x_j t} = \frac{1}{\det(1-tg)}.$$

The dimension of the invariant space of a representation is the average of traces of all the elements in G, so

$$P_t(S(V)^G) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(1-tg)}.$$

$\square$

If the ring of invariants of G is a polynomial ring with n generators of degrees $d_1, \cdots, d_n$, we have

$$\prod_{i=1}^{n}\frac{1}{1-t^{d_i}} = P_t(S(V)^G) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(1-tg)}.$$

Multiplying both sides by $(1-t)^n$ for $n = \dim V$,

$$\prod_{i=1}^{n}\frac{1}{1+t+\cdots+t^{d_i}} = \frac{1}{|G|}\sum_{g\in G}\frac{(1-t)^n}{\det(1-tg)}.$$

If we take $t = 1$ at both sides, we can see:

$$\prod_{i=1}^{n} d_i = |G|.$$

If we take the derivative of both sides at 1, we obtain that the sum of all $d_i - 1$ equals to half of the number of non-trivial pseudo-reflections in G.

Now we consider the case of Weyl groups. Let G be a reductive group over $\mathbb{C}$ and T be a maximal torus in G, Φ be the set of roots associated to (G, T). The Weyl group W acts on the vector space $V = X^*(T)\otimes_{\mathbb{Z}}\mathbb{R}$. The ring of invariants $S(V)^W$ is a polynomial ring of r variables $f_1, \cdots, f_r$, where r is the rank of G. Let d_i be the degree of f_i, and since there exists an invariant $\sum_{\alpha\in\Phi}\alpha\otimes\alpha$ of degree 2, we may assume $d_1 = 2$. By the results above we have

$$\prod_{i=1}^{r} d_i = |W|, \qquad \sum_{i=1}^{r}(d_i - 1) = |\Phi|/2.$$

Hence $\dim G = |\Phi| + \dim T = \sum_{i=1}^{r}(2d_i - 1)$.

2.2 Weak and Strong Approximations

In this section let F be a number field. For each place v of F, let $\mathcal{O}_v$ be the valuation ring of the local field F_v. Let $\mathbb{A}_F$ be its adèle ring. For a finite set S of places, let $F_S = \prod_{v\in S} F_v$ and $\mathbb{A}_F^S = \prod'_{v\notin S} F_v$ be the restricted product of local fields outside S. For the details on the theory of adèles, our main reference is [Wei95, Chapter IV].

Definition 2.4. Let S be a nonempty finite set of places of F. An affine scheme X satisfies *weak approximation with respect to* S if the image of the embedding $X(F) \to X(F_S)$ is dense. It satisfies *strong approximation with respect to* S if $X(F)$ is dense in $X(\mathbb{A}_F^S)$.

Example 2.1. [PR94, Section 1.2] A basic example in algebraic number theory is that the addition group $\mathbb{G}_a$ satisfies both weak and strong approximations for any nonempty S.

Although it is hard to study whether or not weak (resp. strong) approximation holds for an arbitrary affine scheme, under some suitable restrictions weak (resp. strong) approximation holds for algebraic groups. Our main reference is [PR94, Chapter 7].

Theorem 2.2. *[PR94, Theorem 7.8] A simply-connected semisimple group G over a number field F admits weak approximation with respect to any nonempty finite set S of places of F.*

Theorem 2.3. *[PR94, Theorem 7.12] Let G be a simply-connected geometrically almost simple algebraic group over a number field F and S be a finite set of places of F. If $G(F_S)$ is noncompact, then G satisfies strong approximation with respect to S.*

2.3 The Mass Formula and its Proof

Now we fix a $\mathbb{Z}$-model $\mathscr{G}$ of G, where G is either split over $\mathbb{Q}$ or has real Satake diagram given in Section 1.3. Now we want to classify other $\mathbb{Z}$-models of G up to conjugacy by $G(\mathbb{Q})$. In this section we let $\widehat{\mathbb{Z}}$ be the product space $\prod_p \mathbb{Z}_p$ and $\widehat{\mathbb{Q}} = \widehat{\mathbb{Z}} \otimes \mathbb{Q}$ be the ring of finite adèle.

Definition 2.5. For another $\mathbb{Z}$-model $\mathscr{G}'$, we say $\mathscr{G}$ and $\mathscr{G}'$ are in the same *genus* if $\mathscr{G}(\widehat{\mathbb{Z}})$ and $\mathscr{G}'(\widehat{\mathbb{Z}})$ are conjugate in $G(\widehat{\mathbb{Q}})$.

This condition is equivalent to that $\mathscr{G}(\mathbb{Z}_p)$ and $\mathscr{G}'(\mathbb{Z}_p)$ are conjugate in $G(\mathbb{Q}_p)$ for each finite prime p. From the definition of $\widehat{\mathbb{Z}}$, we can see $\mathscr{G}(\mathbb{Z}_p) = \mathscr{G}'(\mathbb{Z}_p)$ for almost all p. For any $\mathbb{Z}$-model $\mathscr{G}'$ in the genus containing $\mathscr{G}$, there exists an element $\sigma \in G(\widehat{\mathbb{Q}})/\mathscr{G}(\widehat{\mathbb{Z}})$ such that $\mathscr{G}'(\widehat{\mathbb{Z}}) = \sigma\mathscr{G}(\widehat{\mathbb{Z}})\sigma^{-1}$. So the $\mathbb{Z}$-group scheme $\mathscr{G}'$ is determined by $\mathscr{G}'(\mathbb{Z}) = \sigma\mathscr{G}(\widehat{\mathbb{Z}})\sigma^{-1} \cap G(\mathbb{Q})$, and we denote it by $\mathscr{G}_\sigma$. Hence the set of conjugacy classes of $\mathbb{Z}$-models in the same genus with $\mathscr{G}$ is in bijection with the double cosets

$$G(\mathbb{Q})\backslash G(\widehat{\mathbb{Q}})/\mathscr{G}(\widehat{\mathbb{Z}}).$$

Proposition 2.1. *(1) If $G(\mathbb{R})$ is not compact, then $G(\widehat{\mathbb{Q}}) = G(\mathbb{Q}) \cdot \mathscr{G}(\widehat{\mathbb{Z}})$. There is a unique model $\mathscr{G}$ in this genus up to $G(\mathbb{Q})$-conjugation. The group $\Gamma = \mathscr{G}(\mathbb{Z})$ is a discrete subgroup of $G(\mathbb{R})$ and the right $G(\mathbb{R})$-invariant Radon measure on $\Gamma\backslash G(\mathbb{R})$ induced by the Haar measure on $G(\mathbb{R})$ is finite.*

(2) If $G(\mathbb{R})$ is compact, then $G(\mathbb{Q})\backslash G(\widehat{\mathbb{Q}})/\mathscr{G}(\widehat{\mathbb{Z}})$ is finite and of cardinality $n =: n(G)$. For each $\mathscr{G}_\sigma$, the group $\Gamma_\sigma = \mathscr{G}_\sigma(\mathbb{Z})$ is a finite subgroup of $G(\mathbb{R})$.

Proof. (1) Since G is simply-connected and $G(\mathbb{R})$ is not compact, by the strong approximation theorem Theorem 2.3, the image of $G(\mathbb{Q})$ in $G(\widehat{\mathbb{Q}})$ is dense. Notice that $\mathscr{G}(\widehat{\mathbb{Z}})$ is an open neighborhood of the identity in $G(\widehat{\mathbb{Q}})$. For any $x \in G(\widehat{\mathbb{Q}})$ its neighborhood $x \cdot \mathscr{G}(\widehat{\mathbb{Z}})$ must contain an element of $G(\mathbb{Q})$, thus $x \in G(\mathbb{Q}) \cdot \mathscr{G}(\widehat{\mathbb{Z}})$, which implies that $G(\widehat{\mathbb{Q}}) = G(\mathbb{Q}) \cdot \mathscr{G}(\widehat{\mathbb{Z}})$. So there is only one $\mathbb{Z}$-model in the genus of $\mathscr{G}$ up to $G(\mathbb{Q})$-conjugation. Obviously, $\Gamma = \mathscr{G}(\mathbb{Z})$ is a discrete subgroup of the locally compact group $G(\mathbb{R})$. So the quotient map $G(\mathbb{R}) \to \Gamma\backslash G(\mathbb{R})$ is a covering map and we can naturally define a right $G(\mathbb{R})$-invariant Radon measure on $\Gamma\backslash G(\mathbb{R})$. The Borel-Harish-Chandra theorem [BH62, Theorem 7.8] tells us this measure is finite.

(2) By Borel's famous result [Bor63], the double quotient $G(\mathbb{Q})\backslash G(\widehat{\mathbb{Q}})/\mathscr{G}(\widehat{\mathbb{Z}})$ is finite. Since the group of real points $G(\mathbb{R})$ is compact, each discrete subgroup Γ_σ must be a finite group. $\square$

The group $\Gamma = \mathscr{G}(\mathbb{Z})$ in Proposition 2.1(1) is an *arithmetic group*:

Definition 2.6. Let $G \leq \mathrm{GL}_n$ be a linear algebraic group over $\mathbb{Q}$. A subgroup $\Gamma \leq G(\mathbb{Q})$ is *arithmetic* if it is commensurable with $\Lambda = G(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$, which means that both $\Gamma/(\Gamma \cap \Lambda)$ and $\Lambda/(\Gamma \cap \Lambda)$ are finite sets.

Remark 2.2. This definition is independent of the choice of representation $G \hookrightarrow \mathrm{GL}_n$.

Definition 2.7. Let G be a semisimple algebraic group over $\mathbb{R}$ and Γ be an arithmetic subgroup of $G(\mathbb{R})$ with finite cohomological dimension (see [Ser94, Section I.3] for details on the theory of cohomology), K be a maximal compact subgroup of $G(\mathbb{R})$. If Γ is torsion-free, then define its *Euler-Poincaré characteristic* to be

$$\chi(\Gamma) = \sum (-1)^i \dim H^i(\Gamma, \mathbb{R}).$$

For general Γ, we take a torsion-free subgroup Γ_0 of Γ with finite index, and define

$$\chi(\Gamma) = \frac{1}{[\Gamma : \Gamma_0]} \chi(\Gamma_0).$$

This definition doesn't depends on the choice of Γ_0.

Under our settings in the beginning of this section, if $G(\mathbb{R})$ is compact, the discrete group $\Gamma_\sigma = \mathscr{G}_\sigma(\mathbb{Z})$ is a finite subgroup for any σ, so the Euler-Poincaré characteristic $\chi(\Gamma_\sigma)$ is simply $1/|\Gamma_\sigma|$. Now we want to have a formula for $\chi(\Gamma)$ when $G(\mathbb{R})$ is not compact, and a relation between different $\chi(\Gamma_\sigma) = 1/|\Gamma_\sigma|$ when $G(\mathbb{R})$ is compact.

Theorem 2.4. *(1) If $G(\mathbb{R})$ is not compact, let $K(\mathbb{R})$ be a maximal compact subgroup and W, W_c be the Weyl group and the compact Weyl group (the Weyl group of K over $\mathbb{C}$) respectively. Then the Euler-Poincaré characteristic of $\Gamma = \mathscr{G}(\mathbb{Z})$ is*

$$\chi(\Gamma) = \frac{|W|}{|W_c|} \cdot \prod_{i=1}^{r} \frac{1}{2} \zeta(1 - d_i),$$

where $d_1, \cdots, d_r$ are the degrees of the invariants for the representation of W as in Section 2.1 and $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ is the Riemman zeta function.

(2)If $G(\mathbb{R})$ is compact, then we have the mass formula*:*

$$\sum_\sigma \frac{1}{|\Gamma_\sigma|} = \prod_{i=1}^{r} \frac{1}{2} \zeta(1 - d_i), \tag{3}$$

where the sum is taken over the representatives of the double coset space $G(\mathbb{Q})\backslash G(\widehat{\mathbb{Q}})/\mathscr{G}(\widehat{\mathbb{Z}})$ and $\Gamma_\sigma = \mathscr{G}_\sigma(\mathbb{Z})$.

Proof. (1) For any finite prime p we fix the Haar measure μ_p on $\mathbb{Q}_p$ such that $\mu_p(\mathbb{Z}_p) = 1$, and for the infinite place ∞ we fix the original Lebesgue measure on $\mathbb{R}$. Take ω to be a generator of the module of top forms $\Gamma(\mathscr{G}, \Omega^n_{\mathscr{G}/\operatorname{Spec}(\mathbb{Z})})$, which is defined up to sign. For each place v, let $|\omega|_v$ be the Haar measure on $G(\mathbb{Q}_v)$ induced by $|\omega|$, and $|\omega|_f$ be the product of all the $|\omega|_p$ for finite primes p.

When $\mathscr{G}$ is a Chevalley group (equivalently, G is split), this formula was proved by Harder by his Gauss-Bonnet formula in [Har71]. We will not copy his long proof here but instead show that his argument can be generalized to non-split $\mathbb{Q}$-groups admitting $\mathbb{Z}$-models.

The key global result used in Harder's argument is

$$\int_{\mathscr{G}(\mathbb{Z})\backslash G(\mathbb{R})} |\omega|_\infty = \prod_{i=1}^{r} \zeta(d_i),$$

which is proved for Chevalley group $\mathscr{G}$ by Langlands in [Lan96].

Before generalizing this result, we consider the integration of $|\omega|_p$ over the compact subgroup $\mathscr{G}(\mathbb{Z}_p)$ for a finite place p. Let φ be the reduction map $\mathscr{G}(\mathbb{Z}_p) \to \mathscr{G}(\mathbb{Z}/p\mathbb{Z})$. By a generization of Hensel's lemma [Wei82, Lemma 2.2.4], for each point $\overline{x} \in \mathscr{G}(\mathbb{Z}/p\mathbb{Z})$, its fiber $\varphi^{-1}(\overline{x})$ is non-empty, and by taking local coordinates we get a $\mathbb{Q}_p$-analytic isomorphism $\varphi^{-1}(\overline{x}) \simeq (p\mathbb{Z}_p)^n$, where $n = \dim G$. For some local coordinates near a point $x \in G(\mathbb{Q}_p)$, we can write the top form ω in the form $f(T)\mathrm{d}T_1 \wedge \cdots \wedge \mathrm{d}T_n$. By our choice of ω, $f(x)$ is a unit in $\mathbb{Z}_p$ for each point $x \in \mathscr{G}(\mathbb{Z}_p)$ lying in this coordinate chart. Combining these together,we have

$$\int_{\mathscr{G}(\mathbb{Z}_p)} |\omega|_p = |\mathscr{G}(\mathbb{Z}/p\mathbb{Z})| \cdot \int_{(p\mathbb{Z}_p)^n} 1 \cdot \mathrm{d}x_1 \cdots \mathrm{d}x_n = |\mathscr{G}(\mathbb{Z}/p\mathbb{Z})|/p^n. \tag{4}$$

For more details on p-adic integrations, see [Pop11, Chapter 3].

As a split reductive group over the finite field $\mathbb{Z}/p\mathbb{Z}$, consider the Bruhat decomposition of $\mathscr{G}_{\mathbb{Z}/p\mathbb{Z}}$:

$$\mathscr{G}_{\mathbb{Z}/p\mathbb{Z}} = \bigsqcup_{w \in W} BwB,$$

where B is a Borel subgroup and w runs over a set of representatives of the Weyl group. By [Con20, Proposition 5.2.10], if an element $w \in W$ sends $n(w)$ positive roots to negative roots, then

$$|(BwB)(\mathbb{Z}/p\mathbb{Z})| = (p-1)^r p^{m+n(w)},$$

where $m = \frac{n-r}{2}$ is the number of positive roots. Notice that here the rank r of $\mathscr{G}_{\mathbb{Z}/p\mathbb{Z}}$ coincides with the rank of G because $\mathscr{G}$ is split over $\mathbb{Q}_p$ according to Proposition 1.5. Hence, we obtain the order of the finite group $\mathscr{G}(\mathbb{Z}/p\mathbb{Z})$:

$$|\mathscr{G}(\mathbb{Z}/p\mathbb{Z})| = (p-1)^r p^m \sum_{w \in W} p^{n(w)}.$$

By a result of Chevalley-Solomon [Sol63],

$$\sum_{w \in W} p^{n(w)} = \prod_{i=1}^{r} (1 + p + \cdots + p^{d_i - 1}),$$

we get an explicit formula:

$$|\mathscr{G}(\mathbb{Z}/p\mathbb{Z})| = (p-1)^r p^m \prod_{i=1}^{r}(1+p+\cdots+p^{d_i-1}) = p^{\frac{n-r}{2}} \prod_{i=1}^{r}(p^{d_i}-1), \tag{5}$$

and we can compute the integration over $\mathscr{G}(\widehat{\mathbb{Z}})$ by multiplying the local integrals (4) together:

$$\begin{aligned}\int_{\mathscr{G}(\widehat{\mathbb{Z}})} |\omega|_f = \prod_p \int_{\mathscr{G}(\mathbb{Z}_p)} |\omega|_p &= \prod_p p^{\frac{-n-r}{2}} \prod_{i=1}^{r}(p^{d_i}-1) \\ &= \prod_p \prod_{i=1}^{r}(1-p^{-d_i}) = \prod_{i=1}^{r}\zeta(d_i)^{-1}.\end{aligned}$$

Now we can observe that Langlands' result is equivalent to the claim that the *Tamagawa number*

$$\tau(G) := \int_{G(\mathbb{Q})\backslash G(\mathbb{A})} |\omega|$$

is equal to 1, where $\mathbb{A} = \mathbb{R}\times\widehat{\mathbb{Q}}$ is the adèle of $\mathbb{Q}$. This is because we have a homeomorphism

$$\begin{aligned}G(\mathbb{Q})\backslash G(\mathbb{A}) &= G(\mathbb{Q})\backslash\Big(G(\mathbb{R})\times G(\widehat{\mathbb{Q}})\Big) \\ &= G(\mathbb{Q})\backslash\Big(G(\mathbb{Q})\times\big(G(\mathbb{Q})\cdot\mathscr{G}(\widehat{\mathbb{Z}})\big)\Big) \\ &\simeq \Big(\big(\mathscr{G}(\widehat{\mathbb{Z}})\cap G(\mathbb{Q})\big)\backslash G(\mathbb{R})\Big)\times\mathscr{G}(\widehat{\mathbb{Z}}) \\ &= \Big(\mathscr{G}(\mathbb{Z})\backslash G(\mathbb{R})\Big)\times\mathscr{G}(\widehat{\mathbb{Z}})\end{aligned}$$

The claim that $\tau(G)=1$ for any simply-connected groups over $\mathbb{Q}$ was conjectured by Weil. We have already said that it was proved by Langlands for split groups, and for quasi-split groups without factors of E_8 type, it was proved by Kottwitz in [Kot88], and for groups of E_8 type the proof was completed by Chernousov in [Che89]. Hence Harder's argument can be generalized to the case of non-split simply-connected group G with a $\mathbb{Z}$-model $\mathscr{G}$, because in this case G is quasi-split.

(2) From the proof of (1), we have

$$\int_{G(\mathbb{Q})\backslash\mathscr{G}(\mathbb{A})} |\omega| = 1, \qquad \int_{\mathscr{G}(\widehat{\mathbb{Z}})} |\omega|_f = \prod_{i=1}^{r}\zeta(d_i)^{-1}.$$

When $G(\mathbb{R})$ is compact, we have

$$G(\mathbb{A}) = \bigsqcup_{\sigma} G(\mathbb{Q})\cdot\Big(G(\mathbb{R})\sigma\mathscr{G}(\widehat{\mathbb{Z}})\Big),$$

where σ runs over a representative set of the double quotient $G(\mathbb{Q})\backslash G(\widehat{\mathbb{Q}})/\mathscr{G}(\widehat{\mathbb{Z}})$, which is finite by Proposition 2.1(2). So we have a homeomorphism:

$$G(\mathbb{Q})\backslash G(\mathbb{A}) \simeq \bigsqcup_{\sigma}\Gamma_\sigma\backslash\Big(G(\mathbb{R})\times\mathscr{G}(\widehat{\mathbb{Z}})\Big).$$

Since Γ_σ is finite for each σ, we have:

$$1 = \int_{G(\mathbb{Q})\backslash \mathscr{G}(\mathbb{A})} |\omega| = \sum_\sigma \frac{1}{|\Gamma_\sigma|} \int_{G(\mathbb{R})\times \mathscr{G}(\widehat{\mathbb{Z}})} |\omega|.$$

Thus the left hand side of the mass formula (3) is

$$\sum_\sigma \frac{1}{|\Gamma_\sigma|} = \prod_{i=1}^r \zeta(d_i)\cdot (\int_{G(\mathbb{R})} |\omega|_\infty)^{-1}.$$

We have a formula in [Mac80] for the volume of the compact Lie group $G(\mathbb{R})$, which is an exercise in [Bou07]:

$$\int_{G(\mathbb{R})} |\omega|_\infty = \prod_{i=1}^r \frac{(2\pi\sqrt{-1})^{d_i}}{(d_i-1)!}.$$

Hence

$$\sum_\sigma \frac{1}{|\Gamma_\sigma|} = \prod_{i=1}^r \zeta(d_i)\frac{(d_i-1)!}{(2\pi\sqrt{-1})^{d_i}} = \prod_{i=1}^r \frac{1}{2}\zeta(1-d_i),$$

by the functional equation of Riemann ζ function:

$$\pi^{-\frac{s}{2}}\Gamma\big(\frac{s}{2}\big)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\big(\frac{1-s}{2}\big)\zeta(1-s).$$

□

This formula can be generalized to any number field, here we give the mass formula for totally real field:

Theorem 2.5. *Let F be a totally real number field. Let G be a simply-connected almost-simple semisimple algebraic group over F such that $G(F\otimes_{\mathbb{Q}}\mathbb{R})$ is compact and G admits an $\mathcal{O}_F$-model $\mathscr{G}$ which is the base change of a $\mathbb{Z}$-group scheme $\mathscr{G}_0$. Then the double quotient $G(F)\backslash G(\mathbb{A}_F^\infty)/\mathscr{G}(\widehat{\mathcal{O}_F})$ is finite. For each element σ in this double quotient, the group $\Gamma_\sigma = \sigma\mathscr{G}(\widehat{\mathcal{O}_F})\sigma^{-1}\cap G(F)$ is a finite group. We have the mass formula:*

$$\sum_{\sigma\in G(F)\backslash G(\mathbb{A}_F^\infty)/\mathscr{G}(\widehat{\mathcal{O}_F})} \frac{1}{|\Gamma_\sigma|} = \prod_{i=1}^r \frac{1}{2^{[F:\mathbb{Q}]}}\zeta_F(1-d_i),$$

where $d_1,\cdots,d_r$ are the degrees of the invariants and $\zeta_F(s) = \sum_{\mathfrak{a}\subset\mathcal{O}_F} \frac{1}{\mathrm{N}\mathfrak{a}^s}$ is the Dedekind zeta function.

Proof. The proof is similar with that of Theorem 2.4. Since $\mathscr{G}$ is the base change of a $\mathbb{Z}$-group scheme $\mathscr{G}_0$, we can take a generator in $\Gamma(\mathscr{G}_0, \Omega^n_{\mathscr{G}_0,\mathrm{Spec}(\mathbb{Z})})\otimes_{\mathbb{Z}}\mathscr{O}_F$ and define the measures $|\omega|_v$ similarly.

In this case, the Tamagawa number is

$$\tau_F(G) = |\mathrm{disc}(F)|^{-\frac{\dim G}{2}} \int_{G(F)\backslash G(\mathbb{A}_F)} |\omega|,$$

here we just state this identity in order to avoid the definition of Tamagawa measure. We still have $\tau_F(G) = 1$ for a number field F.

Borel's result also holds for number fields: the double quotient $G(F)\backslash G(\mathbb{A}_F^\infty)/\mathscr{G}(\widehat{\mathcal{O}_F})$ is finite. This can be proved by applying Proposition 2.1(2) to the $\mathbb{Q}$-group $\mathrm{Res}_{F/\mathbb{Q}}G$. Hence we have the similar homeomorphism:

$$G(F)\backslash G(\mathbb{A}_F) \simeq \bigsqcup_{\sigma} \Gamma_\sigma\backslash\Big(G(F\otimes_{\mathbb{Q}}\mathbb{R}) \times \mathscr{G}(\widehat{\mathcal{O}_F})\Big),$$

where σ runs over a representative set of the double quotient. Hence

$$1 = |\mathrm{disc}(F)|^{-\frac{\dim G}{2}} \cdot \Big(\sum_{\sigma} \frac{1}{|\Gamma_\sigma|}\big(\int_{G(\mathbb{R})} |\omega|_\infty\big)^{[F:\mathbb{Q}]}\Big) \cdot \prod_{v\,finite} \int_{G(\mathcal{O}_{F_v})} |\omega|_v.$$

For each finite place v, we have:

$$\int_{G(\mathcal{O}_{F_v})} |\omega|_v = |\mathscr{G}(\mathcal{O}_{F_v}/\varpi_{F_v}\mathcal{O}_{F_v})| \cdot q_v^{-\dim G} = \prod_{i=1}^{r}(1-q_v^{-d_i}),$$

where ϖ_{F_v} is a uniformizer of $\mathscr{O}_{F_v}$ and q_v is the order of residue field $\mathscr{O}_{F_v}/\varpi_{F_v}\mathscr{O}_{F_v}$. For the integral over $G(\mathbb{R})$, we still has the formula:

$$\int_{G(\mathbb{R})} |\omega|_\infty = \prod_{i=1}^{r} \frac{(2\pi\sqrt{-1})^{d_i}}{(d_i-1)!}.$$

Combine these together, we obtain that:

$$\begin{aligned}
\sum_{\sigma} \frac{1}{|\Gamma_\sigma|} &= |\mathrm{disc}(F)|^{\frac{\dim G}{2}} \cdot \big(\prod_{i=1}^{r} \frac{(d_i-1)!}{(2\pi\sqrt{-1})^{d_i}} \cdot \big)^{[F:\mathbb{Q}]} \prod_{v\,finite}\prod_{i=1}^{r}(1-q_v^{-d_i})^{-1} \\
&= |\mathrm{disc}_F|^{\frac{\dim G}{2}} \cdot \big(\prod_{i=1}^{r} \frac{(d_i-1)!}{(2\pi\sqrt{-1})^{d_i}}\big)^{[F:\mathbb{Q}]} \cdot \prod_{i=1}^{r} \zeta_F(d_i) \\
&= \prod_{i=1}^{r} \frac{1}{2^{[F:\mathbb{Q}]}} \zeta_F(1-d_i),
\end{aligned}$$

where the last step is by the functional equation for Dedekind zeta functions. $\square$

3 Constructions of Models

Now we start to give an explicit construction of models of anisotropic groups listed in the end of Section 1.3 except E_8.

3.1 Constructions of Models: Classical Groups

In this section, we will construct $\mathbb{Z}$-models for anisotropic classical groups of type $B_n(n \geq 3)$ and $D_n(n \geq 4)$. A simply-connected simple group of type B_n, D_n is isomorphic to the *spin groups* of a quadratic form, which is the double cover of the *special orthogonal group*.

Definition 3.1. Let (V, q) be a quadratic space over a field k of characteristic 0. For each k-algebra R, (V, q) can be extended to a quadratic space $(V \otimes_k R, q \otimes R)$ over R. The *special orthogonal group* $\mathrm{SO}(V, q)$ of (V, q) is a k-group scheme assigning each k-algebra R the group consisting of isometries of $(V \otimes_k R, q \otimes R)$ with determinant 1. The *spin group* $\mathrm{Spin}(V, q)$ is the double cover of $\mathrm{SO}(V, q)$, which means there is a short exact sequence of k-group schemes:

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(V, q) \longrightarrow \mathrm{SO}(V, q) \longrightarrow 1,$$

where μ_2 is the group of square roots of 1.

Remark 3.1. These groups can also be defined over a commutative ring k via *Clifford algebras* and the short exact sequence still holds. For the details, see [Mil17, Chapter 24].

Since the maximal real torus of the spin group of a positive-definite quadratic form is trivial, from the table in the end of Section 1.3 we should consider groups of the form $G = \mathrm{Spin}(V, q)$, where V is a vector space over $\mathbb{Q}$ of dimension $d \equiv 0, \pm 1 (\mathrm{mod} 8)$ and $q = \frac{1}{2} \sum\limits_{i=1}^{d} x_i^2$ is a quadratic form on V. Let $B_q(x, y) = \sum\limits_{i=1}^{d} x_i y_i$ be the associated symmetric bilinar form.

For an integral lattice $L \subset V$, which means the lattice L satisfies $B_q(L, L) \subset \mathbb{Z}$, we can define the determinant of L to be

$$\det L = \det(B_q(e_i, e_j))_{1 \leq i,j \leq d},$$

where $\{e_1, \cdots, e_d\}$ is any $\mathbb{Z}$-basis of L. An integral lattice is called *even* if $q(L) \subset \mathbb{Z}$. When $d \equiv 0 \bmod 8$, we consider even lattices L with $\det L = 1$, which are called *unimodular* lattices; when $d \equiv \pm 1 \bmod 8$, we consider even L with $\det L = 2$. Then we have a $\mathbb{Z}$-group scheme $\mathscr{G} = \mathrm{Spin}(L, q)$. It is smooth by the Jacobian criterion and it has reductive fiber at each prime p since L is a non-degenerate quadratic space modulo p (when $p = 2$, see [Bor91, Section 23]). Hence $\mathscr{G} = \mathrm{Spin}(L, q)$ is a $\mathbb{Z}$-model of $G = \mathrm{Spin}(V, q)$.

In general, the classification of $\mathbb{Z}$-models of these $\mathrm{Spin}(V, q)$ is related to the classification of unimodular lattices (see [CL19]). When $\dim V = 8, 16, 24$, there are $1, 2, 24$ isometry classes of even unimodular lattices respectively. For higher dimensions, there are a huge number of isometry classes.

Example 3.1. When $d = 8$, there is only one even unimodular lattice up to isomorphism:

$$E_8 = \left\{ x = (x_i)_{1 \leq i \leq 8} \,\middle|\, 2x_i \in \mathbb{Z}, x_i - x_j \in \mathbb{Z}, \sum_{i=1}^{8} x_i \in 2\mathbb{Z} \right\}.$$

Then $\mathrm{Spin}(E_8, q)$ is the unique $\mathbb{Z}$-model of the non-spit anisotropic group $G = \mathrm{Spin}(\mathbb{Q}^8, q)$ of type D_4 in its genus. We can also prove this via the mass formula Theorem 2.4. The degrees of the invariants for the Weyl group of root system D_4 are $2, 4, 4, 6$ (the degrees for different root systems can be found in [Bou07, Chapitre VI.4]). The mass of G is

$$\frac{1}{16}\zeta(-1)\zeta(-3)\zeta(-3)\zeta(-5) = \frac{1}{2^{14} \cdot 3^5 \cdot 5^2 \cdot 7}.$$

The isometry group of E_8 lattice is isomorphic to the Weyl group of root system E_8, hence by the result we stated in Section 2.1,

$$|\mathrm{Spin}(E_8, q)(\mathbb{Z})| = |\mathrm{O}(E_8, q)(\mathbb{Z})| = |W(E_8)| = \prod_{i=1}^{r} d_i = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7,$$

which implies that $\mathrm{Spin}(E_8, q)$ is the unique $\mathbb{Z}$-model in this genus.

We can also use computers to compute the isometry group of a lattice by the Plesken-Souvignier algorithm [PS97], via the function **qfauto** in [GP]. This leads to the same result above.

Example 3.2. Let E_7 be the orthogonal complement of $e_7 + e_8$ in E_8. It is the unique even lattice of rank 7 and determinant 2. Let $A_1 \subset \mathbb{R}^2$ be the lattice of integral points in the hyperplane $x_1 + x_2 = 0$. The unique even lattice of rank 9 and determinant 2 is $E_8 \oplus A_1$. Thus $\mathrm{Spin}(E_7, q)$ and $\mathrm{Spin}(E_8 \oplus A_1, q)$ are the $\mathbb{Z}$-models of non-split anisotropic groups G of type B_3, B_4 respectively. We can show that they are the unique $\mathbb{Z}$-model in their genera respectively by the same method in Example 3.1.

Example 3.3. When $d = 16$ there are two isometry classes of even unimodular lattices: $E_8 \oplus E_8$ and

$$D_{16}^{+} = \left\{ x = (x_i)_{1 \le i \le 16} \;\middle|\; 2x_i \in \mathbb{Z}, x_i - x_j \in \mathbb{Z}, \sum_{i=1}^{16} x_i \in 2\mathbb{Z} \right\},$$

so we obtain two $\mathbb{Z}$-models for $G = \mathrm{Spin}(\mathbb{Q}^{16}, q)$. Again with the help of [GP]:

$$\begin{aligned} |\mathrm{Spin}(E_8 \oplus E_8, q)| &= 2^{29} \cdot 3^{10} \cdot 5^4 \cdot 7^2, \\ |\mathrm{Spin}(D_{16}^{+}, q)| &= 2^{30} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13. \end{aligned}$$

We have

$$\frac{1}{|\mathrm{Spin}(E_8 \oplus E_8, q)|} + \frac{1}{|\mathrm{Spin}(D_{16}, q)|} = \frac{691}{2^{30} \cdot 3^6 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13}.$$

Notice that the righthand side is equal to the mass

$$\frac{1}{2^8}\zeta(-1)\zeta(-3)\zeta(-5)\zeta(-7)\zeta(-7)\zeta(-9)\zeta(-11)\zeta(-13),$$

thus these two groups are all the $\mathbb{Z}$-models of G in this genus.

3.2 Octonion Algebras

In this section, we will introduce Coxeter's integral order $\mathscr{R}$ lying in Cayley's definite octonions $\mathbb{O}$, which is used to construct $\mathbb{Z}$-models for exceptional groups. At first, we give the general definition of an octonion algebra.

Definition 3.2. An *octonion algebra* C over a commutative ring k is a non-associative k-algebra which is a free k-module of rank 8 and admits a non-degenerate quadratic form N on C satisfying:

$$\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y), \forall x, y \in C.$$

The quadratic form N is referred as the *norm* of the octonion algebra C, and the associated bilinear form $\langle x, y\rangle = \mathrm{N}(x+y) - \mathrm{N}(x) - \mathrm{N}(y)$ is called the inner product.

Remark 3.2. In general, C should be defined as a *projective* k-module. However, in this thesis k is either a field or a principal ideal domain like $\mathbb{Z}$ or $\mathbb{Z}_p$, so we just let C be a free k-module.

The octonion algebra used to construct split groups is the split octonion algebra:

Definition 3.3. As a vector space the *split* octonion algebra over a field k is the space of vector matrices

$$\begin{pmatrix} \xi & x \\ y & \eta \end{pmatrix} \qquad (\xi, \eta \in k, x, y \in k^3).$$

On k^3 we have a non-degenerate bilinear form $\langle x, y\rangle = \sum_{i=1}^{3} x_i y_i$ and an exterior product defined by

$$\langle x \wedge y, z\rangle = \det(x, y, z).$$

The addition of vector matrices is entrywise, and the multiplication is defined by

$$\begin{pmatrix} \xi & x \\ y & \eta \end{pmatrix}\begin{pmatrix} \xi' & x' \\ y' & \eta' \end{pmatrix} = \begin{pmatrix} \xi\xi' + \langle x, y'\rangle & \xi x' + \eta' x + y \wedge y' \\ \eta y' + \xi' y + x \wedge x' & \eta\eta' + \langle y, x'\rangle \end{pmatrix}.$$

The quadratic form N is defined by $\mathrm{N}(\begin{pmatrix} \xi & x \\ y & \eta \end{pmatrix}) = \xi\eta - \langle x, y\rangle$.

The automorphism group of a split octonion algebra over k is a connected split simple algebraic k-group of type G_2 [Spr00, Theorem 2.3.5]. To define an anisotropic group, we need an octonion algebra over $\mathbb{Q}$ whose quadratic form is positive-definite:

Definition 3.4. As a $\mathbb{Q}$-vector space, *Cayley's definite octonion algebra* $\mathbb{O}$ has the form

$$\mathbb{O} = \mathbb{Q} \oplus \mathbb{Q}e_1 \oplus \cdots \oplus \mathbb{Q}e_7.$$

The multiplication law is determined by:

- $e_i^2 = -1$ for $1 \leq i \leq 7$;

- for any $i \bmod 7$, the subalgebra $\mathbb{Q} \oplus \mathbb{Q}e_i \oplus \mathbb{Q}e_{i+1} \oplus \mathbb{Q}e_{i+3}$ is isomorphic to Hamilton's rational quaternion algebra $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$, whose multiplication structure is given by $i^2 = j^2 = -1, ij = -ji = k$;
- If three elements e_r, e_s, e_t don not lie in one of the 7 quaternion algebras described above, then the multiplication is anti-associative: $(e_r \cdot e_s) \cdot e_k = -e_r \cdot (e_s \cdot e_t)$.

There is an anti-involution of algebra $x \mapsto \overline{x}$ called conjugation on $\mathbb{O}$, which is defined by $\overline{1} = 1$ and $\overline{e_i} = -e_i$ for each i. The trace and norm on $\mathbb{O}$ are:

$$\mathrm{Tr}(x) = x + \overline{x}, \quad \mathrm{N}(x) = x \cdot \overline{x} = \overline{x} \cdot x.$$

The norm N is a positive-definite quadratic form and the associated symmetric bilinear form is

$$\langle x, y \rangle = (x + y) \cdot \overline{x + y} - x \cdot \overline{x} - y \cdot \overline{y} = \mathrm{Tr}(x \cdot \overline{y}).$$

Theorem 3.1. *The $\mathbb{Q}$-group scheme $G = \mathrm{Aut}_{\mathbb{O}/\mathbb{Q}}$, which associates to each $\mathbb{Q}$-algebra R the automorphism group of the octonion algebra $\mathbb{O} \otimes_{\mathbb{Q}} R$, is a 14-dimensional connected semisimple group of type G_2 over $\mathbb{Q}$. It is $\mathbb{R}$-anisotropic and split over $\mathbb{Q}_p$ for all primes p.*

Proof. The proof of the first assertion can be found in [Spr00, Section 2.3]. The norm N is a positive-definite quadratic form, so $G = \mathrm{Aut}_{\mathbb{O}/\mathbb{Q}}$ is a closed subgroup of the isometry group $\mathrm{O}(\mathbb{O}, N)$ of $\mathbb{O}$ and must be also $\mathbb{R}$-anisotropic. For each prime p, $\mathbb{O}_{\mathbb{Q}_p} = \mathbb{O} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is an octonion algebra over $\mathbb{Q}_p$. A well-known fact [Ser93, Theorem IV.6] is that for any quadratic form over $\mathbb{Q}_p$ in more than 4 variables represents 0 non-trivially, thus $\mathbb{O}_{\mathbb{Q}_p}$ must be a split octonion and then G is $\mathbb{Q}_p$-split for each p. □

To construct the $\mathbb{Z}$-model of $\mathscr{G}$, we need an *order* in $\mathbb{O}$, which means a $\mathbb{Z}$-lattice in $\mathbb{O}$ containing the identity 1 and stable under multiplication. Now we are going to choose a specific maximal order in $\mathbb{O}$.

Definition 3.5. *Coxeter's integral order $\mathscr{R}$* in $\mathbb{O}$ is the lattice spanned by $\mathbb{Z} \oplus \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_7$ and

$$\begin{aligned} h_1 &= (1 + e_1 + e_2 + e_4)/2, \\ h_2 &= (1 + e_1 + e_3 + e_7)/2, \\ h_3 &= (1 + e_1 + e_5 + e_6)/2, \\ h_4 &= (e_1 + e_2 + e_3 + e_5)/2. \end{aligned}$$

Remark 3.3. In [CS03, Section 9.2] we can see that any maximal order in $\mathbb{O}$ is isomorphic to $\mathscr{R}$.

If we view $(\mathscr{R}, N|_{\mathscr{R}})$ as a lattice with a definite quadratic form, it is even unimodular. Actually, as an even unimodular lattice $\mathscr{R}$ is isomorphic to the lattice E_8, which was defined in Example 3.1.

3.3 The Exceptional Jordan Algebra

Consider the 27-dimensional $\mathbb{Q}$-vector space V of 3×3 Hermitian matrices over $\mathbb{O}$:

$$A = \begin{pmatrix} a & z & \overline{y} \\ \overline{z} & b & x \\ y & \overline{x} & c \end{pmatrix},$$

where $a, b, c \in \mathbb{Q}, x, y, z \in \mathbb{O}$. On this vector space V, we have a multiplicative structure which is commutative but not associative:

$$A \circ A' = \frac{1}{2}(AA' + A'A).$$

This algebra V has a 2-sided identity $e = \mathrm{diag}(1,1,1)$ and is often referred as the *exceptional Jordan algebra*.

We can also equip this algebra with a non-degenerate positive-definite quadratic form:

$$Q(A) = \mathrm{Tr}(A \circ A)/2 = \frac{1}{2}(a^2 + b^2 + c^2) + \mathrm{N}(x) + \mathrm{N}(y) + \mathrm{N}(z),$$

and the associated bilinear form is $B_Q(A, B) = \mathrm{Tr}(A \circ B)$.

The determinant of the matrix

$$\det(A) = abc + \mathrm{Tr}(xyz) - a \cdot \mathrm{N}(x) - b \cdot \mathrm{N}(y) - c \cdot \mathrm{N}(z)$$

is a cubic form on V.

The $\mathbb{Q}$-group $H = \mathrm{Aut}_{(V,\det)/\mathbb{Q}}$, which assigns to each $\mathbb{Q}$-algebra R the group of linear automorphisms of $V \otimes_{\mathbb{Q}} R$ preserving the cubic form $\det \otimes_{\mathbb{Q}} R$, is a non-split simply-connected $\mathbb{Q}$-group of type E_6 [Spr00, Theorem 7.3.2]. The $\mathbb{Q}$-group $\mathrm{Aut}_{(V,\circ)/\mathbb{Q}}$ consisting of automorphisms preserving the multiplicative structure is a connected semisimple $\mathbb{Q}$-group of type F_4 [Spr00, Theorem 7.2.1]. Since H is contained in the isometry group of a positive-definite quadratic form, $H(\mathbb{R})$ is a compact group.

We have an alternative description of $\mathrm{Aut}_{(V,\circ)/\mathbb{Q}}$ which will be used in the next section. Actually, $\mathrm{Aut}_{(V,\circ)/\mathbb{Q}}$ coincides with the group $\mathrm{Aut}_{(V,\det,e)/\mathbb{Q}}$ consisting of automorphisms preserving the cubic form det and the identity element e.

Lemma 3.1. *As subgroups of* GL_V, $\mathrm{Aut}_{(V,\circ)/\mathbb{Q}} = \mathrm{Aut}_{(V,\det,e)/\mathbb{Q}}$.

Proof. To prove this lemma, it suffices to show that for any $\mathbb{Q}$-algebra R, $\mathrm{Aut}_{(V,\circ)/\mathbb{Q}}(R) = \mathrm{Aut}_{(V,\det,e)/\mathbb{Q}}(R)$.

Before proving the lemma, we define the Freudenthal multiplication on $V \otimes_{\mathbb{Q}} R$:

$$A \times B = A \circ B + \frac{1}{2}[(\mathrm{Tr}(A)\mathrm{Tr}(B) - B_Q(A, B))e - \mathrm{Tr}(B)A - \mathrm{Tr}(A)B]$$

and a symmetric trilinear form:

$$(A, B, C) = B_Q(A, B \times C).$$

The relations between this trilinear form and the cubic form det can be easily checked:

$$\begin{aligned}\det(A) =& \frac{1}{3}(A,A,A)\\ (A,B,C) =& \frac{1}{2}[\det(A+B+C)-\det(A+B)-\det(B+C)-\det(C+A)\\ &+\det(A)+\det(B)+\det(C)]\end{aligned}$$

If $\alpha \in \mathrm{Aut}_{(V,\circ)/\mathbb{Q}}(R)$, then it is obvious that α fixes the identity element e. From the definition of $A \times B$ and (A,B,C), we can see that α also preserves this trilinear form, thus

$$\det(\alpha A) = \frac{1}{3}(\alpha A, \alpha A, \alpha A) = \frac{1}{3}(A,A,A) = \det(A).$$

Conversely, if $\alpha \in \mathrm{Aut}_{(V,\det,e)/\mathbb{Q}}(R)$, it also preserves the trilinear form (A,B,C). It can be easily verified that:

$$B_Q(A,B) = (A,e,e)(B,e,e) - 2(A,B,e),$$

so α preserves the inner product. In particular, $\mathrm{Tr}(\alpha A) = B_Q(\alpha A, e) = B_Q(A,e) = \mathrm{Tr}(A)$. Fix A, B, for any $C \in V \otimes_{\mathbb{Q}} R$, we have:

$$\begin{aligned}B_Q(C, A\times B) &= (C,A,B) = (\alpha C, \alpha A, \alpha B)\\ &= B_Q(\alpha C, \alpha A \times \alpha B) = B_Q(C, \alpha^{-1}(\alpha A \times \alpha B)),\end{aligned}$$

which shows that $\alpha(A\times B) = \alpha A \times \alpha B$. From the definition of the Freudenthal multiplication, we get

$$\begin{aligned}(C, A\times B) =& B_Q(C, A\circ B) + \frac{1}{2}(\mathrm{Tr}(A)\mathrm{Tr}(B) - B_Q(A,B))\mathrm{Tr}(C)\\ &- \frac{1}{2}(\mathrm{Tr}(B)B_Q(C,A) - \mathrm{Tr}(A)B_Q(C,B)).\end{aligned}$$

Hence $B_Q(\alpha C, \alpha A \circ \alpha B) = B_Q(C, A\circ B)$, which tells us α lies in $\mathrm{Aut}_{(V,\circ)/\mathbb{Q}}(R)$. □

Remark 3.4. From the proof we can see that for any commutative algebra k whose characteristic not equal to $2, 3$, a k-linear isomorphism of V preserves the multiplication $\circ$ if and only if it preserves the cubic form det and fixes the identity element e.

By this lemma, we can view the group of type F_4 as $\mathrm{Aut}_{(V,\det,e)/\mathbb{Q}}$.

If we replace the conditions on a,b,c,x,y,z in the definition of V by $a,b,c \in \mathbb{Z}, x,y,z \in \mathscr{R}$, then we get an order $J \subseteq V$. If we view $(J, Q|_J)$ as a lattice with a positive-definite quadratic form, it is unimodular and isomorphic to $\mathbb{Z}^{\oplus 3} \oplus E_8^{\oplus 3}$.

3.4 Construction of Models: Exceptional Groups

In this section we will construct non-split $\mathbb{Z}$-models for anisotropic groups with root systems of exceptional types G_2 and F_4.

The automorphism scheme $G = \mathrm{Aut}_{\mathbb{O}/\mathbb{Q}}$ of Cayley's definite octonion $\mathbb{O}$ is a connected anisotropic semisimple group over $\mathbb{Q}$ of type G_2. By [CG12, Theorem B.14] the $\mathbb{Z}$-group scheme $\mathscr{G} = \mathrm{Aut}_{\mathscr{R}/\mathbb{Z}}$ is a $\mathbb{Z}$-model of G. We want to see whether there is any other such $\mathbb{Z}$-model in this genus, just like what we did in Example 3.1. In order to use the mass formula, we need to determine the order of $\mathscr{G}(\mathbb{Z})$. We are going to show that $\mathscr{G}(\mathbb{Z})$ is isomorphic to $\mathscr{G}(\mathbb{Z}/2\mathbb{Z})$ and then use the formula (5) we obtained in the proof of Theorem 2.4:

$$|\mathscr{G}(\mathbb{Z}/p\mathbb{Z})| = p^{\frac{n-r}{2}} \prod_{i=1}^{r} (p^{d_i} - 1).$$

Lemma 3.2. *Any non-trivial torsion element in the kernel of the reduction map*

$$\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/2\mathbb{Z}), X \mapsto X \bmod M_n(2\mathbb{Z})$$

must have order 2.

Proof. For an element $X \in \mathrm{GL}_n(\mathbb{Z})$, define

$$d(X) := \sup\{m \mid X - I_n \in M_n(2^m\mathbb{Z})\}.$$

From the definition, X is contained in the torsion of the reduction map if and only if $d(X) > 0$, and $d(X) = \infty$ means $X = I_n$.

Now we assume that $0 < d = d(X) < \infty$ and $X = I_n + 2^d Y$, where $Y \in M_n(\mathbb{Z}) \backslash M_n(2\mathbb{Z})$. For any $r > 1$, we have $X^r = I_n + 2^d(rY + Z)$ with

$$Z = \sum_{i=2}^{r} \binom{r}{i} 2^{d(i-1)} Y^i \in M_n(2\mathbb{Z}).$$

If r is odd, then $rY + Z \notin M_n(2\mathbb{Z})$, thus $rY + Z \neq 0$ and X^r can not be the identity matrix. Hence if X is a non-trivial torsion element, its order must be 2^m for some $m \geq 1$.

We claim that for $X \in \mathrm{GL}_n(\mathbb{Z})$ with $d = d(X) > 0$, it satisfies $d(X^2) \geq \min\{1 + d, 2d\}$ and $d(X^2) = 1 + d$ if $d > 1$. Indeed if we write $X = I_n + 2^d Y$, then

$$X^2 = I_n + 2^{d+1} Y + 2^{2d} Y^2,$$

and the claim follows immediately.

Now we assume that X has order $2^i, i \geq 1$. Since $d\big((X^{2^{i-1}})^2\big) = \infty$, by the claim above we know $d(X^{2^{i-1}}) \leq 1$. Hence $1 \geq d(X^{2^{i-1}}) \geq 2d(X^{2^{i-2}}) \geq \cdots \geq 2^{i-1} d(X) \geq 2^{i-1}$, which implies that the order of X can only be 2. $\square$

Proposition 3.1. *The finite group $\mathscr{G}(\mathbb{Z})$ is isomorphic to $\mathscr{G}(\mathbb{Z}/2\mathbb{Z})$.*

Proof. Fix a $\mathbb{Z}$-basis of $\mathscr{R}$, we can write an element in $\mathscr{G}(\mathbb{Z})$ or $\mathscr{G}(\mathbb{Z}/2\mathbb{Z})$ as a 8×8 matrix and obtain the following commutative diagram:

$$\begin{array}{ccc} \mathscr{G}(\mathbb{Z}) & \longrightarrow & \mathrm{GL}_8(\mathbb{Z}) \\ \downarrow & & \downarrow \\ \mathscr{G}(\mathbb{Z}/2\mathbb{Z}) & \longrightarrow & \mathrm{GL}_8(\mathbb{Z}/2\mathbb{Z}) \end{array}.$$

Suppose that g is a non-trivial element in the kernel of the reduction map $\mathscr{G}(\mathbb{Z}) \to \mathscr{G}(\mathbb{Z}/2\mathbb{Z})$, then when we view it as an element in $\mathrm{GL}_8(\mathbb{Z})$ it also lies in the kernel of the reduction map $\mathrm{GL}_8(\mathbb{Z}) \to \mathrm{GL}_8(\mathbb{Z}/2\mathbb{Z})$. Since $\mathscr{G}(\mathbb{Z})$ is a finite group, g is a torsion element. By Lemma 3.2, g has order 2. If we write $g = \mathrm{id}_{\mathscr{R}} - 2P$, where P is an integral matrix, then we have $P^2 = P$. By an easy exercise in linear algebra, we know that P is the matrix of a projection operator. Hence P can be diagnalized to a diagnal matrix of the form $\mathrm{diag}(1, 1, \cdots, 1, 0, \cdots, 0)$, thus we have an orthogonal decomposition $\mathscr{R} = M \oplus N$ of $\mathscr{R}$ such that $g|_M = \mathrm{id}_M$ and $g|_N = -\mathrm{id}_N$. This also gives rise to a decomposition of the root system of lattice $\mathscr{R}$. However as a lattice $\mathscr{R} \simeq E_8$ its root system is irreducible of type E_8, thus $M = 0$ or $N = 0$. Since g is non-trivial, the only possibility is $M = 0$ and $g = -\mathrm{id}_{\mathscr{R}}$, but this is not an automorphism of the octonion algebra! So $\mathscr{G}(\mathbb{Z}) \to \mathscr{G}(\mathbb{Z}/2\mathbb{Z})$ is an injection.

Now we have

$$|\mathscr{G}(\mathbb{Z})| \leq |\mathscr{G}(\mathbb{Z}/2\mathbb{Z})| = 2^{\frac{14-2}{2}}(2^2 - 1)(2^6 - 1) = 2^6 \cdot 3^3 \cdot 7.$$

By Theorem 2.4 the mass of group G is:

$$\frac{1}{2^2}\zeta(-1)\zeta(-5) = \frac{1}{2^6 \cdot 3^3 \cdot 7} \leq \frac{1}{|\mathscr{G}(\mathbb{Z})|},$$

which shows that the right hand side of the mass formula has only one term $\frac{1}{|\mathscr{G}(\mathbb{Z})|}$. Hence the orders of $\mathscr{G}(\mathbb{Z})$ and $\mathscr{G}(\mathbb{Z}/2\mathbb{Z})$ are the same, thus they are isomorphic. □

As an immediate result of the proof:

Corollary 3.1. *The group scheme $\mathscr{G} = \mathrm{Aut}_{\mathscr{R}/\mathbb{Z}}$ is the unique $\mathbb{Z}$-model in this genus.*

Before turning to groups of type F_4, we state a result about type E_6. We have already known that the group $H = \mathrm{Aut}_{(V,\det)/\mathbb{Q}}$ is a non-split simply-connected $\mathbb{Q}$-group of type E_6.

Theorem 3.2. *[CG12, Proposition 6.5] The $\mathbb{Z}$-group $\mathscr{H} = \mathrm{Aut}_{(J,\det)/\mathbb{Z}}$ is a $\mathbb{Z}$-model for $H = \mathrm{Aut}_{(V,\det)/\mathbb{Q}}$.*

If we choose any positive-definite $E \in J$ such that $\det E = 1$, which is called a *polarization*, then we can construct a $\mathbb{Z}$-subgroup scheme $\mathscr{H}_E = \mathrm{Aut}_{(J,\det,E)/\mathbb{Z}} \subset \mathscr{H}$ similarly.

Theorem 3.3. *[CG12, Proposition 6.6] For any choice of polarization $E \in J$, the $\mathbb{Z}$-group scheme $\mathscr{H}_E = \mathrm{Aut}_{(J,\det,E)/\mathbb{Z}}$ is semisimple of type F_4.*

When E is the identity matrix $e := \mathrm{diag}(1, 1, 1)$, the $\mathbb{Z}$-group $\mathscr{H}_e$ is a $\mathbb{Z}$-model of the group $\mathrm{Aut}_{(V,\det,e)/\mathbb{Q}} = \mathrm{Aut}_{(V,\circ)/\mathbb{Q}}$. By Theorem 3.3 $\mathscr{H}_{e'}$ is also a $\mathbb{Z}$-model of $\mathrm{Aut}_{(V,\circ),\mathbb{Q}}$ in this genus, where

$$e' = \begin{pmatrix} 2 & \beta & \overline{\beta} \\ \overline{\beta} & 2 & \beta \\ \beta & \overline{\beta} & 2 \end{pmatrix}$$

and $\beta = \frac{1}{2}(-1 + e_1 + e_2 + \cdots + e_7) \in J$. Now we want to show that they are exactly the two different $\mathbb{Z}$-models of $\mathrm{Aut}_{(V,\circ)/\mathbb{Q}}$, so taking other positive-definite E will give rise to one of these two $\mathbb{Z}$-groups above. In order to use the mass formula, we need to compute the orders of $\mathscr{H}_e(\mathbb{Z})$ and $\mathscr{H}_{e'}(\mathbb{Z})$.

In Gross's paper [Gro96], he says that $\mathscr{H}_e(\mathbb{Z})$ is isomorphic to $2^2.\mathrm{O}_8^+(2).S_3$. He cites this result from [Con85] and Conway does not give it a proof, so we are going to compute $|\mathscr{H}_e(\mathbb{Z})|$ without using this isomorphism.

Denote the subset of J consisting of diagonal matrices by D, and the subset of elements whose diagnal entries are all zero by E, then D is a lattice isomorphic to $\mathbb{Z}^{\oplus 3}$ and E is 3 copies of $\mathscr{R}$, thus $E \simeq E_8^{\oplus 3}$. Any element σ in $\mathscr{H}_e(\mathbb{Z})$ is an isometry of the orthogonal complement of e in J, which is isomorphic to $A_2 \oplus E_8^{\oplus 3}$ as an even unimodular lattice. We have

$$\mathrm{O}(A_2 \oplus E_8^{\oplus 3}) \simeq \mathrm{O}(A_2) \oplus (\mathrm{O}(E_8) \wr S_3),$$

where S_3 is the permutation group of three elements and $\wr$ means the wreath product, so $\sigma(D) \subset D$ and $\sigma(E) \subset E$. Let $\mathscr{D}$ be the kernel of the projection $\mathscr{H}_e(\mathbb{Z}) \to \mathrm{O}(D), \sigma \mapsto \sigma|_D$. This is a normal subgroup of $\mathscr{H}_e(\mathbb{Z})$ by definition.

We can also identify the permutation group S_3 as a subgroup of $\mathscr{H}_e(\mathbb{Z})$ by:

$$\sigma.\begin{pmatrix} a_1 & x_3 & \overline{x_2} \\ \overline{x_3} & a_2 & x_1 \\ x_2 & \overline{x_1} & a_3 \end{pmatrix} = \begin{pmatrix} a_{\sigma^{-1}(1)} & x^*_{\sigma^{-1}(3)} & \overline{x^*_{\sigma^{-1}(2)}} \\ \overline{x^*_{\sigma^{-1}(3)}} & a_{\sigma^{-1}(2)} & x^*_{\sigma^{-1}(1)} \\ x^*_{\sigma^{-1}(2)} & \overline{x^*_{\sigma^{-1}(1)}} & a_{\sigma^{-1}(3)} \end{pmatrix},$$

here $x^* = x$ if σ is a even permutation and $x^* = \overline{x}$ if σ is odd. Indeed, $\sigma \in S_3$ preserves e and

$$\begin{aligned}\det(\sigma.\begin{pmatrix} a_1 & x_3 & \overline{x_2} \\ \overline{x_3} & a_2 & x_1 \\ x_2 & \overline{x_1} & a_3 \end{pmatrix}) &= \prod_{i=1}^{3} a_{\sigma^{-1}(i)} + \mathrm{Tr}(x^*_{\sigma^{-1}(1)}x^*_{\sigma^{-1}(2)}x^*_{\sigma^{-1}(3)}) - \sum_{i=1}^{3} a_{\sigma^{-1}(i)} \cdot \mathrm{N}(x^*_{\sigma^{-1}(i)}) \\ &= a_1a_2a_3 + \mathrm{Tr}(x^*_{\sigma^{-1}(1)}x^*_{\sigma^{-1}(2)}x^*_{\sigma^{-1}(3)}) - \sum_{i=1}^{3} a_i \cdot \mathrm{N}(x_i).\end{aligned}$$

It can be checked easily from the definition that for $x, y, z \in \mathscr{R}$ we have

$$\mathrm{Tr}(xyz) = \mathrm{Tr}(yzx) = \mathrm{Tr}(zxy), \mathrm{Tr}(xy) = \mathrm{Tr}(\overline{y} \cdot \overline{x}),$$

which implies that

$$\mathrm{Tr}(x^*_{\sigma^{-1}(1)}x^*_{\sigma^{-1}(2)}x^*_{\sigma^{-1}(3)}) = \mathrm{Tr}(x_1x_2x_3),$$

thus σ also preserves the cubic form det.

Theorem 3.4. *The finite group $\mathscr{H}_e(\mathbb{Z})$ is isomorphic to the inner semidirect product:*

$$\mathscr{D} \rtimes S_3.$$

Moreover, $\mathscr{D}$ is isomorphic to the group of isotopies*:*

$$\{(\alpha, \beta, \gamma) \in \mathrm{O}(\mathscr{R})^3 | \alpha(x)\beta(y) = \overline{\gamma(\overline{xy})}, \forall x, y \in \mathscr{R}\}.$$

Proof. Let σ be an element of $\mathscr{H}_e(\mathbb{Z})$. If we write the element of J in the form:

$$\begin{pmatrix} a & z & \overline{y} \\ \overline{z} & b & x \\ y & \overline{x} & c \end{pmatrix},$$

then the restriction of σ on D must be an element permuting a, b, c. So we can multiply σ by some element μ in $S_3 \leq \mathscr{H}_e(\mathbb{Z})$ so that $\sigma\mu \in \mathscr{D}$. Since $\mathscr{D}$ is a normal subgroup of $\mathscr{H}_e(\mathbb{Z})$ and $\mathscr{D} \cap S_3 = \{1\}$, we obtain the desired isomorphism $\mathscr{H}_e(\mathbb{Z}) \simeq \mathscr{D} \rtimes S_3$.

Now we are going to show that $\mathscr{D}$ is isomorphic to the group of isotopies. Assume that $\sigma \in \mathscr{D}$ is of the form:

$$\sigma(\begin{pmatrix} a & z & \overline{y} \\ \overline{z} & b & x \\ y & \overline{x} & c \end{pmatrix}) = \begin{pmatrix} a & \gamma(\tilde{z}) & \overline{\beta(\tilde{y})} \\ \overline{\gamma(\tilde{z})} & b & \alpha(\tilde{x}) \\ \beta(\tilde{y}) & \overline{\alpha(\tilde{x})} & c \end{pmatrix},$$

for some isometries $\alpha, \beta, \gamma \in \mathrm{O}(\mathscr{R})$ and $\{\tilde{x}, \tilde{y}, \tilde{z}\}$ is a permutation of $\{x, y, z\}$. The fact that σ preserves the cubic form det implies that

$$\begin{aligned} &abc + \mathrm{Tr}(xyz) - a \cdot \mathrm{N}(x) - b \cdot \mathrm{N}(y) - c \cdot \mathrm{N}(z) \\ =&abc + \mathrm{Tr}(\alpha(\tilde{x})\beta(\tilde{y})\gamma(\tilde{z})) - a \cdot \mathrm{N}(\alpha(\tilde{x})) - b \cdot \mathrm{N}(\beta(\tilde{y})) - c \cdot \mathrm{N}(\gamma(\tilde{z})) \\ =&abc + \mathrm{Tr}(\alpha(\tilde{x})\beta(\tilde{y})\gamma(\tilde{z})) - a \cdot \mathrm{N}(\tilde{x}) - b \cdot \mathrm{N}(\tilde{y}) - c \cdot \mathrm{N}(\tilde{z}) \end{aligned}$$

for all $a, b, c \in \mathbb{Z}, x, y, z \in \mathscr{R}$, thus $\tilde{x} = x, \tilde{y} = y, \tilde{z} = z, \mathrm{Tr}(xyz) = \mathrm{Tr}(\alpha(x)\beta(y)\gamma(z))$. We have:

$$\begin{aligned} &\alpha(x)\beta(y) = \overline{\gamma(\overline{xy})}, \forall x, y \in \mathscr{R} \\ \Leftrightarrow &\langle \alpha(x)\beta(y), \overline{\gamma(z)} \rangle = \langle \overline{\gamma(\overline{xy})}, \overline{\gamma(z)} \rangle = \langle \overline{xy}, z \rangle = \langle xy, \overline{z} \rangle, \forall x, y, z \in \mathscr{R} \\ \Leftrightarrow &\mathrm{Tr}(\alpha(x)\beta(y)\gamma(z)) = \mathrm{Tr}(xyz). \end{aligned}$$

Hence $\mathscr{D}$ is isomorphic to the group of isotopies. $\square$

Proposition 3.2. *The group of isotopies is a double cover of the special orthogonal group* $\mathrm{SO}(\mathscr{R})$.

Proof. Let p be the morphism from the group of isotopies to $\mathrm{O}(\mathscr{R})$ mapping (α, β, γ) to γ. [Yok09, Lemma 1.14.4] shows that the image of p lies in $\mathrm{SO}(\mathscr{R})$. It is easy to verify that the kernel of p is $\{(1, 1, 1), (1, -1, -1)\}$. The rest of the proof is the surjectivity of p.

For an element $a \in \mathbb{O}$, let L_a, R_a be the left and right multiplication by a and $B_a = L_a \circ R_a = R_a \circ L_a$. The triple $(L_a, R_a, B_{\overline{a}})$ satisfies

$$L_a(x)R_a(y) = (ax)(ya) = a(xy)a = \overline{B_{\overline{a}}(\overline{xy})},$$

so it is an isotopy. Let ref(a) be the reflection $x \mapsto x - 2\frac{\langle x,a \rangle}{\langle a,a \rangle}a$. We have two identities:

$$\mathrm{ref}(a) \circ \mathrm{ref}(1) = \frac{1}{\mathrm{N}(a)} B_a, \mathrm{ref}(1) \circ \mathrm{ref}(a) = \frac{1}{\mathrm{N}(a)} B_{\overline{a}}.$$

For any $\gamma \in \mathrm{SO}(\mathscr{R})$, it can be decomposed as the composition of an even number of reflections:

$$\gamma = \mathrm{ref}(a_1) \circ \cdots \circ \mathrm{ref}(a_{2n}).$$

Write $\mathrm{ref}(a) \circ \mathrm{ref}(b)$ as $(\mathrm{ref}(a) \circ 1) \circ (\mathrm{ref}(1) \circ \mathrm{ref}(b))$, then we can rewrite γ as

$$\gamma = \frac{1}{\prod_{i=1}^{2n} \mathrm{N}(c_i)} B_{\overline{c_1}} \circ \cdots \circ B_{\overline{c_{2n}}}.$$

Define:

$$\alpha = \frac{1}{\prod_{i=1}^{2n} \mathrm{N}(c_i)} L_{c_1} \circ \cdots \circ L_{c_{2n}},$$
$$\beta = \frac{1}{\prod_{i=1}^{2n} \mathrm{N}(c_i)} R_{c_1} \circ \cdots \circ R_{c_{2n}},$$

and it can be easily checked that (α, β, γ) is an orthogonal isotopy. □

Remark 3.5. Actually we have already proved the isomorphism used by Gross, because in [Con85] $2^2.\mathrm{O}_8^+$ is constructed as the group of isotopies of $\mathscr{R}$.

By these results we can compute the order of $\mathscr{H}_e(\mathbb{Z})$:

$$|\mathscr{H}_e(\mathbb{Z})| = 2 \cdot |S_3| \cdot |\mathrm{SO}(E_8)| = 2^{15} \cdot 3^6 \cdot 5^2 \cdot 7.$$

Now we start to deal with another finite group $\mathscr{H}_{e'}(\mathbb{Z})$. In [EG96], Gross and Elkies also cite a result from [Con85] which says $\mathscr{H}_{e'}(\mathbb{Z})$ is isomorphic to the twisted group ${}^3D_4(2).3$. I failed to find the proof of this result, so here we are going to use another method to compute the order of this group.

Proposition 3.3. *The order of $\mathscr{H}_{e'}(\mathbb{Z})$ is $2^{12} \cdot 3^5 \cdot 7^2 \cdot 13$.*

Proof. With the choice of polarization e', we can define a bilinear form on J:

$$\langle A, B \rangle = (A, e', e')(B, e', e') - 2(A, B, e'),$$

where the trilinear form is defined as in the proof of Lemma 3.1. This bilinear form is integral and positive-definite on J by [EG96, Proposition 7.2]. Any element in $\mathscr{H}_{e'}(\mathbb{Z})$ also preserves this bilinear form, thus this group is a subgroup of the isometry group of $(J, \langle\, , \rangle)$. We denote this isometry group by $\mathrm{O}'(J)$.

With the help of the Plesken-Souvignier algorithm and [GP], we obtain the order of $\mathrm{O}'(J)$:

$$|\mathrm{O}'(J)| = 2^{13} \cdot 3^5 \cdot 7^2 \cdot 13.$$

Notice that in this case $\mathrm{O}'(J)$ contains an involution $A \mapsto -A$, which did not happen when we choose e to be the polarization. This involution does not fix e', thus

$$|\mathscr{H}_{e'}(\mathbb{Z})| \leq 2^{12} \cdot 3^5 \cdot 7^2 \cdot 13.$$

The mass of F_4 is

$$\frac{1}{2^4}\zeta(-1)\zeta(-5)\zeta(-7)\zeta(-11) = \frac{691}{2^{15} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 13} = \frac{1}{2^{15} \cdot 3^6 \cdot 5^2 \cdot 7} + \frac{1}{2^{12} \cdot 3^5 \cdot 7^2 \cdot 13},$$

which is not more than $\frac{1}{|\mathscr{H}_e(\mathbb{Z})|} + \frac{1}{|\mathscr{H}_{e'}(\mathbb{Z})|}$. This implies that the order of $\mathscr{H}_{e'}(\mathbb{Z})$ must be equal to $2^{12} \cdot 3^5 \cdot 7^2 \cdot 13$. □

Remark 3.6. The proof of this proposition tells us any isometry in $\mathrm{O}'(J)$ fixing e' automatically preserves the cubic form det.

As an immediate corollary:

Corollary 3.2. *$\mathscr{H}_e$ and $\mathscr{H}_{e'}$ are exactly the two different $\mathbb{Z}$-models of $\mathrm{Aut}_{(V,\circ)/\mathbb{Q}}$ in the genus.*

Remark 3.7. We can also use this method to construct the $\mathbb{R}$-rank 1 $\mathbb{Q}$-group of type F_4. If we choose

$$E_0 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix},$$

then the group $\mathscr{H}_{E_0}$ is still semisimple of type F_4 but the real point $\mathscr{H}_{E_0}(\mathbb{R})$ has rank 1, thus $\mathscr{H}_{E_0,\mathbb{Q}}$ is the another non-split $\mathbb{Q}$-group mentioned in Section 1.3.

Another exceptional type admitting anisotropic $\mathbb{Z}$-models is E_8. Unlike G_2, F_4, the number of $\mathbb{Z}$-models is still unknown. We can use Theorem 2.4 to compute the mass of E_8:

$$\frac{1}{2^8}\zeta(-1)\zeta(-7)\zeta(-11)\zeta(-13)\zeta(-17)\zeta(-19)\zeta(-23)\zeta(-29) \approx 13934.5.$$

So we have the inequality:

$$|\{\text{models of}\, E_8\}| \geq \sum_{\sigma} \frac{1}{|\mathscr{G}_\sigma(\mathbb{Z})|} \approx 13934.5,$$

which tells us there are at least 13935 different $\mathbb{Z}$-models of the anisotropic group E_8 in a given genus. Gross uses adjoint representations to construct two such models in [Gro96].

References

[BH62] A. Borel and Harish-Chandra. “Arithmetic Subgroups of Algebraic Groups”. In: *Annals of Mathematics* 75.3 (1962), pp. 485–535. ISSN: 0003486X. URL: `http://www.jstor.org/stable/1970210`.

[BLR90] S. Bosch, W. Lutkebohmert, and M. Raynaud. *Néron Models*. Springer, 1990.

[Bor63] Armand Borel. “Some finiteness properties of adele groups over number fields”. en. In: *Publications Mathématiques de l'IHÉS* 16 (1963), pp. 5–30. URL: `www.numdam.org/item/PMIHES_1963__16__5_0/`.

[Bor91] A. Borel. *Linear Algebraic Groups*. Springer-Verlag New York, 1991.

[Bou07] N. Bourbaki. *Groupes et algèbres de Lie, Chapitres 4 à 6*. Berlin: Springer, 2007.

[Bum04] D. Bump. *Lie groups*. Graduate texts in mathematics. New York: Springer, 2004. ISBN: 0-387-21154-3.

[CG12] Brian Conrad and Benedict Gross. “Non-split reductive groups over Z”. In: *Autour des schémas en groupes. Vol. II, Panor. Synthèses* 46 (May 2012).

[Che89] V. I. Chernousov. “On the Hasse principle for groups of type E_8”. English. In: *Sov. Math., Dokl.* 39.3 (1989), pp. 592–596. ISSN: 0197-6788.

[CL19] Gaëtan Chenevier and Jean Lannes. *Automorphic Forms and Even Unimodular Lattices*. Vol. 69. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer Verlag, 2019, 428 p. URL: `https://hal.archives-ouvertes.fr/hal-02113226`.

[Con12] B. Conrad. “Weil and Grothendieck approaches to adelic points”. In: (2012). URL: `http://math.stanford.edu/~conrad/papers/adelictop.pdf`.

[Con14] Brian Conrad. *Reductive group schemes*. Soc.Math.France,Paris, 2014.

[Con20] B. Conrad. “Reductive Groups Over Fields”. In: (2020). URL: `https://www.ams.org/open-math-notes/files/course-material/OMN-201701-110663-1-Course_notes-v5.pdf`.

[Con85] J.H. Conway. *Atlas of finite groups : maximal subgroups and ordinary characters for simple groups*. Oxford University Press Oxford, New York, 1985.

[CS03] J.H. Conway and D.A. Smith. *On Quaternions and Octonions*. 2003. DOI: `https://doi.org/10.1201/9781439864180`.

[DG70] M. Demazure and A. Grothendieck. *Schémas en Groupes I,II,III*. Lecture Notes in Math 151,152,153. Springer-Verlag, New York, 1970.

[EG96] Noam D. Elkies and Benedict H. Gross. “The exceptional cone and the Leech lattice”. In: *International Mathematics Research Notices* 1996.14 (July 1996), pp. 665–698. ISSN: 1073-7928. DOI: `10.1155/S1073792896000426`. eprint: `https://academic.oup.com/imrn/article-pdf/1996/14/665/6768537/1996-14-665.pdf`. URL: `https://doi.org/10.1155/S1073792896000426`.

[GP] GP. *PARI/GP version* `2.13.0`. available from `http://pari.math.u-bordeaux.fr/`. The PARI Group. Univ. Bordeaux.

[Gro96] B. Gross. “Groups over Z”. In: *Invent.math.124* (1996).

[Har71] G. Harder. “A Gauss-Bonnet formula for discrete arithmetically defined groups”. en. In: *Annales scientifiques de l’École Normale Supérieure* Ser. 4, 4.3 (1971), pp. 409–455. DOI: `10.24033/asens.1217`. URL: `www.numdam.org/item/ASENS_1971_4_4_3_409_0/`.

[Hum75] James E. Humphreys. *Linear algebraic groups*. Graduate texts in mathematics. New York Berlin Heidelberg: Springer-Verlag, 1975. ISBN: 0-387-90108-6.

[Kot88] Robert E. Kottwitz. “Tamagawa Numbers”. In: *Annals of Mathematics* 127.3 (1988), pp. 629–646. ISSN: 0003486X. URL: `http://www.jstor.org/stable/2007007`.

[Lan96] R. Langlands. “The Volume of the Fundamental Domain for Some Arithmetical Subgroups of Chevalley Groups”. In: *Proc.Sym.Math.AMS* 9 (1996), pp. 143–148.

[Liu06] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2006, p. 576.

[Mac17] Marco Maculan. “Maximality of hyperspecial compact subgroups avoiding Bruhat–Tits theory”. en. In: *Annales de l’Institut Fourier* 67.1 (2017), pp. 1–21. DOI: 10.5802/aif.3075. URL: www.numdam.org/item/AIF_2017__67_1_1_0/.

[Mac80] I.G. Macdonald. “The Volume of a Compact Lie Group.” In: *Inventiones mathematicae* 56 (1980), pp. 93–96. URL: http://eudml.org/doc/142687.

[Mil17] J. S. Milne. *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field*. Cambridge University Press, 2017. DOI: 10.1017/9781316711736.

[Pop11] M. Popa. “Modern aspects of the cohomological study of varieties”. In: (2011). URL: http://people.math.harvard.edu/~mpopa/571/index.html.

[PR94] V. Platonov and A. Rapinchuk. *Algebraic groups and number theory*. Academic Press, New York, 1994.

[PS97] W Plesken and B Souvignier. “Computing Isometries of Lattices”. In: *Journal of Symbolic Computation* 24.3 (1997), pp. 327–334. ISSN: 0747-7171. DOI: https://doi.org/10.1006/jsco.1996.0130. URL: https://www.sciencedirect.com/science/article/pii/S0747717196901303.

[Ser93] Jean-Pierre Serre. *A course in arithmetic*. Springer, 1993.

[Ser94] J.-P. Serre. *Cohomologie Galoisienne*. Springer, 1994.

[Sol63] L. Solomon. “Invariants of finite reflection groups”. In: 22 (1963), pp. 57–64.

[Spr00] A. Springer. *Octonions, Jordan Algebras and Exceptional Groups*. Springer, Berlin, Heidelberg, 2000.

[Tit79] J. Tits. “Reductive groups over local fields”. In: *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*. Proc. Sympos. Pure Math., XXXIII. Amer. Math. Soc., Providence, R.I., 1979, pp. 29–69.

[Wei82] A. Weil. *Adeles and Algebraic Groups*. Birkhäuser Boston, 1982.

[Wei95] A. Weil. *Basic Number Theory*. Springer-Verlag Berlin Heidelberg, 1995.

[Yok09] Ichiro Yokota. “Exceptional Lie groups”. In: *arXiv: Differential Geometry* (2009).