NON-SPLIT REDUCTIVE GROUPS OVER Z

Brian Conrad

Abstract. — We study the following phenomenon: some *non-split* connected semisimple $\mathbf{Q}$-groups G admit flat affine $\mathbf{Z}$-group models $\mathscr{G}$ with "everywhere good reduction" (i.e., $\mathscr{G}_{\mathbf{F}_p}$ is a connected semisimple $\mathbf{F}_p$-group for every prime p). Moreover, considering such $\mathscr{G}$ up to $\mathbf{Z}$-group isomorphism, there can be more than one such $\mathscr{G}$ for a given G. This is seen classically for types B and D by using positive-definite quadratic lattices.

The study of such $\mathbf{Z}$-groups provides concrete applications of many facets of the theory of reductive groups over rings (scheme of Borel subgroups, automorphism scheme, relative non-abelian cohomology, etc.), and it highlights the role of number theory (class field theory, mass formulas, strong approximation, point-counting over finite fields, etc.) in analyzing the possibilities. In part, this is an expository account of [**G96**].

Résumé. — Nous étudions le phénomène suivant : certains $\mathbf{Q}$-groupes G semi-simples connexes *non déployés* admettent comme modèles des $\mathbf{Z}$-groupes $\mathscr{G}$ affines et plats avec "partout bonne réduction" (c'est à dire, $\mathscr{G}_{\mathbf{F}_p}$ est un $\mathbf{F}_p$-groupe $\mathbf{Q}$-groupes G pour chaque premier p). En outre, considérant de tels $\mathscr{G}$ à $\mathbf{Z}$-groupe isomorphisme près, il y a au plus un tel $\mathscr{G}$ pour un G donné. Ceci est vu classiquement pour les types B et D en utilisant des réseaux quadratiques définis positifs.

L'étude de ces $\mathbf{Z}$-groupes donne lieu à des applications concrètes d'aspects multiples, de la théorie des groupes réductifs sur des anneaux (schémas de sous-groupes de Borel, schémas d'automorphismes, cohomologie relative non abélienne, etc.), et met en évidence le rôle de la théorie des nombres (théorie du corps de classes, formules de masse, approximation forte, comptage de points sur les corps finis, etc.) dans l'analyse des possibilités. En partie, ceci est un article d'exposition sur [**G96**].

Contents

1. Chevalley groups and Z-models

A *Chevalley group* is a reductive **Z**-group scheme (i.e., a smooth affine group scheme $G \to \mathrm{Spec}(\mathbf{Z})$ with connected reductive fibers) that admits a fiberwise maximal **Z**-torus $T \subset G$. For example, the classical groups SL_n, GL_n, PGL_n, Sp_{2n}, and SO_n over **Z** are all Chevalley groups. (The characteristic-free definition of SO_n requires some care when n is even; see [**Co2**, C.2.9].) Many authors require Chevalley groups to have semisimple fibers, but this is a matter of convention.

A more traditional viewpoint on Chevalley groups is obtained via the notion of **Z**-*model* of a connected reductive **Q**-group. In general, if K is the fraction field of a domain R then an R-*model* of a connected reductive K-group G is a pair $(\mathscr{G}, \theta)$ consisting of a reductive R-group scheme $\mathscr{G}$ and an isomorphism of K-groups $\theta : \mathscr{G}_K \simeq G$. The notion of isomorphism between models of G is defined in an evident manner. (Our notion of "model" is more restrictive than in other circumstances, where one allows any flat and finitely presented – or perhaps even smooth – affine group with a specified generic fiber.)

Lemma 1.1. — *The generic fiber of any Chevalley group is split.*

Proof. — It suffices to show that any **Z**-torus is necessarily split. By [**SGA3**, X, 1.2, 5.16] (or [**Co2**, Cor. B.3.6]), the category of tori over a connected normal noetherian scheme S is anti-equivalent to the category of finite free **Z**-modules equipped with a continuous action of $\pi_1(S)$. (When $S = \mathrm{Spec}(k)$ for a field k, this recovers the familiar "character lattice" construction for k-tori.) An S-torus is split when the associated $\pi_1(S)$-action is trivial.

For any Dedekind domain A, the connected finite étale covers of Spec(A) correspond to the finite extensions of Dedekind domains $A \hookrightarrow A'$ with unit discriminant. Thus, by Minkowski's theorem that every number field $\mathrm{K} \neq \mathbf{Q}$ has a ramified prime, $\mathrm{Spec}(\mathbf{Z})$ has no nontrivial connected finite étale covers. Hence, $\pi_1(\mathrm{Spec}(\mathbf{Z})) = 1$, so all $\mathbf{Z}$-tori are split. □

Every Chevalley group $\mathscr{G}$ is a $\mathbf{Z}$-model of its split connected reductive generic fiber over $\mathbf{Q}$, and the Existence and Isomorphisms Theorems over $\mathbf{Z}$ provide a converse that is one of the main theorems of [**SGA3**]:

***Theorem 1.2* (Chevalley, Demazure).** — *Let* R *be a domain with fraction field* K*. Every split connected reductive* K*-group* G *admits an* R*-model of the form* $\mathbf{G}_{\mathrm{R}}$ *for a Chevalley group* $\mathbf{G}$ *over* $\mathbf{Z}$*, and* $\mathbf{G}$ *is uniquely determined up to* $\mathbf{Z}$*-group isomorphism.*

The existence of $\mathbf{G}$ for each G was first proved for $\mathrm{K} = \mathbf{Q}$ as the main result in [**Chev61**], though the language of reductive group schemes over $\mathbf{Z}$ was not available at that time. The approach used by Demazure in [**SGA3**, XXV] is to abstractly build a "split" $\mathbf{Z}$-group $\mathbf{G}$ whose associated root datum may be specified in advance. The Isomorphism Theorem for split connected reductive groups over K then ensures that one gets all such K-groups as generic fibers of the $\mathbf{G}_{\mathrm{R}}$'s by varying over all possibilities for the root datum. Chevalley groups are the *only* $\mathbf{Z}$-models in the split case over $\mathbf{Q}$, so we get a characterization of Chevalley groups without any mention of maximal tori over rings. More generally:

Proposition 1.3. — *If* R *is a principal ideal domain and* G *is a split connected reductive group over* $\mathrm{K} = \mathrm{Frac}(\mathrm{R})$ *then any* R*-model of* G *is* $\mathbf{G}_{\mathrm{R}}$ *for a Chevalley group* $\mathbf{G}$ *over* $\mathbf{Z}$*.*

The hypothesis on R is optimal: if R is Dedekind with fraction field K and I is a nonzero ideal in R whose class in Pic(R) is not a square then $\mathrm{SL}(\mathrm{R} \oplus \mathrm{I})$ is a *non-trivial* Zariski-form of $\mathrm{SL}_{2,\mathrm{R}}$ (see [**Co2**, Exer. 7.4.10]). We postpone the proof of Proposition 1.3 until § 3, as it requires cohomological notions introduced there.

The preceding discussion is summarized by:

Theorem 1.4. — *Passage to the* $\mathbf{Q}$*-fiber defines a bijection from the set of* $\mathbf{Z}$*-isomorphism classes of Chevalley groups onto the set of isomorphism classes of split connected reductive* $\mathbf{Q}$*-groups, with each set classified by root data* (*up to isomorphism*)*. Moreover, the* only $\mathbf{Z}$*-models of such* $\mathbf{Q}$*-groups are those provided by Chevalley groups.*

Work of Chevalley ([**BIBLE**], [**Chev61**]) and Demazure–Grothendieck [**SGA3**] provides a satisfactory understanding of this remarkable theorem.

(For any scheme $\mathrm{S} \neq \varnothing$, [**SGA3**, XXII, 1.13] provides a definition of *Chevalley* S-*group* avoiding the crutch of the theory over $\mathbf{Z}$. This involves additional conditions that are automatic for $\mathrm{S} = \mathrm{Spec}(\mathbf{Z})$.)

Informally, the connected semisimple $\mathbf{Q}$-groups arising as generic fibers of non-Chevalley semisimple $\mathbf{Z}$-groups are those with "good reduction" at all primes but non-split over $\mathbf{R}$ (see Propositions 3.12 and 4.10). The theory surrounding such $\mathbf{Z}$-groups was the topic of [**G96**], where the possibilities for the $\mathbf{Q}$-fiber were classified (under an absolutely simple hypothesis) and some explicit $\mathbf{Z}$-models were given for exceptional types, generalizing examples arising from quadratic lattices.

Overview. In § 2 we discuss special orthogonal groups in the scheme-theoretic framework, highlighting the base scheme $\mathrm{Spec}(\mathbf{Z})$ and some classical examples of semisimple $\mathbf{Z}$-groups with non-split generic fiber arising from quadratic lattices. In § 3 we discuss general cohomological formalism for working with smooth (or more generally, fppf) affine groups over rings, extending the more widely-known formalism over fields as in [**S97**, III].

In § 4 we describe the possibilities for the generic fibers of reductive $\mathbf{Z}$-groups, with an emphasis on the case of semisimple $\mathbf{Z}$-groups whose fibers are absolutely simple and simply connected, and we show that this case accounts for the rest via direct products and central isogenies. In § 5 we introduce Coxeter's order in Cayley's definite octonion algebra over $\mathbf{Q}$, and we use it in § 6 to describe some non-split examples over $\mathbf{Z}$. In § 7 we explain (following [**G96**]) how to use mass formulas to prove in some cases that the list of $\mathbf{Z}$-models found in § 6 for certain $\mathbf{Q}$-groups is exhaustive.

In Appendix A we use the cohomological formalism of semisimple $\mathbf{Z}$-groups to prove that an indefinite non-degenerate quadratic lattice over $\mathbf{Z}$ is determined up to isomorphism by its signature (in odd rank these are not unimodular lattices), and in Appendix B we discuss generalities concerning octonion algebras over commutative rings, with an emphasis on the special case of Dedekind domains. Finally, in Appendix C we discuss an explicit construction of the simply connected Chevalley group of type E_6.

Justification of the construction of simply connected Chevalley groups over $\mathbf{Z}$ of types F_4 and E_6 via Jordan algebras (in § 6 and Appendix C) uses concrete linear algebra and Lie algebra computations over $\mathbf{Z}$ via Mathematica code written by Jiu-Kang Yu (see [**Yu**]); for E_6 this is only needed with local problems at $p = 2, 3$. Reliance on the computer can probably be replaced with theoretical arguments by justifying the applicability of results in [**Sp**, Ch. 14], [**Loos**, § 6], [**A**, § 5], and [**BLG**, § 3] to our circumstances, but it seems less time-consuming to use the computer.

Terminology. A connected semisimple group G over a field k is *absolutely simple* if $\mathrm{G} \neq 1$ and $\mathrm{G}_{\overline{k}}$ has no nontrivial smooth connected proper normal subgroup. This is equivalent to irreducibility of the root system of $\mathrm{G}_{\overline{k}}$. In the literature there is a plethora of terminology for this concept: *absolutely almost simple*, *absolutely quasi-simple*, etc. (see [**G96**, § 1, p. 264]).

Acknowledgements. This work was partially supported by NSF grant DMS-0917686. I am grateful to Wee Teck Gan and Gopal Prasad for their advice, Benedict Gross for illuminating discussions and his inspiring work upon which these notes are based, Jiu-Kang Yu for generously sharing his expertise with group scheme computations on the computer, and the referees for providing useful feedback. Most of all, I am indebted to Patrick Polo for his extensive and insightful suggestions and corrections that vastly improved the content and exposition (and fixed gaps in an earlier treatment).

2. Quadratic spaces and quadratic lattices

A *quadratic space* over a ring R is a pair (M, q) consisting of a locally free R-module M of finite rank $n > 0$ equipped with an R-valued *quadratic form* on M: a map

$$q : \mathrm{M} \to \mathrm{R}$$

such that (i) $q(cx) = c^2 q(x)$ for all $x \in \mathrm{M}$, $c \in \mathrm{R}$ and (ii) the symmetric

$$\mathrm{B}_q : \mathrm{M} \times \mathrm{M} \to \mathrm{R}$$

defined by $(x, y) \mapsto q(x+y) - q(x) - q(y)$ is R-bilinear. (For our purposes, the quadratic spaces of most interest will be over fields and Dedekind domains.)

For a quadratic space (M, q) over R such that M admits an R-basis $\{e_1, \ldots, e_n\}$,

$$\mathrm{disc}(q) := \det(\mathrm{B}_q(e_i, e_j)) \in \mathrm{R} \tag{2.1}$$

changes by $(\mathrm{R}^\times)^2$-scaling when we change the basis. For $\mathrm{R} = \mathbf{Z}$, this is a well-defined element of $\mathbf{Z}$ called the *discriminant* of (M, q). (For general R, the ideal $\mathrm{disc}(q)$ generates in R is independent of $\{e_i\}$ and thus globalizes to a locally principal ideal of R when M is not assumed to be free. If $\mathrm{R} = \mathbf{Z}$ then this ideal provides less information than the discriminant in $\mathbf{Z}$.)

A *quadratic lattice* is a quadratic space (M, q) over $\mathbf{Z}$ such that $\mathrm{disc}(q) \neq 0$. For such pairs, $(\mathrm{M}_{\mathbf{R}}, q_{\mathbf{R}})$ is a non-degenerate quadratic space over $\mathbf{R}$ and so has a *signature* (r, s) with $s = n - r$.

Example 2.1. — Let V be a finite-dimensional inner product space over $\mathbf{R}$, and $\mathrm{L} \subset \mathrm{V}$ a lattice such that $q(x) := \langle x, x \rangle \in \mathbf{Z}$ for all $x \in \mathrm{L}$. Then (L, q) is a quadratic lattice. Note that $\mathrm{B}_q(x, y) = 2\langle x, y \rangle \in 2\mathbf{Z}$ for all $x, y \in \mathrm{L}$.

Remark 2.2. — In the literature, one sometimes finds another convention for (2.1), multiplying against $(-1)^{n(n-1)/2}$ where n is the rank of the underlying module. (The definition without the sign is then called the *determinant* of the quadratic space.) This sign coincides with that of $\mathrm{disc}(q_n)$ for $(\mathbf{Z}^n, q_n)$ as in (2.2) below.

The "signed discriminant" is the convention in the book of Husemöller–Milnor [**HM**, III, § 5], whereas the books of Serre [**S73**, IV, 1.1] and Knus [**Knus**, I, (3.1.1); IV, (3.1.2), (3.1.3)] do not insert the sign. We follow [**S73**] by not inserting a sign in the definition of $\mathrm{disc}(q)$.

The *orthogonal group* of a quadratic lattice (M, q) is the affine $\mathbf{Z}$-group

$$\mathrm{O}(q) = \{g \in \mathrm{GL}(\mathrm{M}) \,|\, q \circ g = q\}.$$

This can fail to be $\mathbf{Z}$-flat for fiber-jumping reasons, even when q is $\mathbf{Z}$-primitive. For example, if $q = x^2 + y^2 + pz^2$ for an odd prime p then $\mathrm{O}(q)_{\mathbf{Q}}$ has dimension 3 whereas $\mathrm{O}(q)_{\mathbf{F}_p}$ has dimension 4 and $\mathrm{O}(q)_{\mathbf{F}_2}$ has dimension 6. (In this case, $\mathrm{disc}(q) = 8p^2$.) A nicer situation is that of the standard split quadratic form q_n on $\mathbf{Z}^n$ given by

$$q_{2m} = x_1x_2 + x_3x_4 + \cdots + x_{2m-1}x_{2m}, \quad q_{2m+1} = x_0^2 + q_{2m}. \tag{2.2}$$

This satisfies $\mathrm{disc}(q_{2m}) = (-1)^m$ and $\mathrm{disc}(q_{2m+1}) = 2(-1)^m$, so $\mathrm{disc}(q_n)$ has sign $(-1)^{n(n-1)/2}$ for all n.

The $\mathbf{Z}$-group $\mathrm{O}_n := \mathrm{O}(q_n)$ is smooth for even n [**Co2**, C.1.5] whereas for $n = 2m+1$ it is $\mathbf{Z}$-flat and equal to $\mu_2 \times \mathrm{SO}_{2m+1}$ where

$$\mathrm{SO}_{2m+1} := \mathrm{O}_{2m+1} \cap \mathrm{SL}_{2m+1} \tag{2.3}$$

is $\mathbf{Z}$-smooth [**Co2**, C.2.9–C.2.11].

A useful variant of the notion of a quadratic lattice is:

Definition 2.3. — A *unimodular lattice* is a pair $(\mathrm{M}', \mathrm{B}')$ where M' is a nonzero finite free $\mathbf{Z}$-module and $\mathrm{B}' : \mathrm{M}' \times \mathrm{M}' \to \mathbf{Z}$ is a symmetric bilinear form such that $\mathrm{disc}(\mathrm{B}') := \det(\mathrm{B}'(e_i, e_j))$ equals ± 1 for some (equivalently, any) $\mathbf{Z}$-basis $\{e_i\}$ of M'.

Associated to such an $(\mathrm{M}', \mathrm{B}')$ is the quadratic lattice $(\mathrm{M}', \mathrm{Q}_{\mathrm{B}'})$ with $\mathrm{Q}_{\mathrm{B}'}(x) = \mathrm{B}'(x, x)$. If $(\mathrm{M}', \mathrm{B}') = (\mathrm{M}, \mathrm{B}_q)$ for a quadratic lattice (M, q) then $\mathrm{Q}_{\mathrm{B}'} = 2q$ is valued in $2\mathbf{Z}$, so unimodular lattices $(\mathrm{M}', \mathrm{B}')$ of rank n that are *even* in the sense that $\mathrm{Q}_{\mathrm{B}'}$ is valued in $2\mathbf{Z}$ (called "type II" in [**S73**, Ch. V]) are equivalent to quadratic lattices (M, q) of rank n such that $\mathrm{disc}(q) = \pm 1$. If $\mathrm{Q}_{\mathrm{B}'}(\mathrm{M}') \not\subset 2\mathbf{Z}$ then we say $(\mathrm{M}', \mathrm{B}')$ is *odd*.

Example 2.4. — The lattice $\mathrm{M}' = \mathbf{Z}^n$ equipped with $\mathrm{B}'(\vec{x}, \vec{y}) = \sum_{i=1}^n x_iy_i$ is a unimodular lattice for any n. This is never even.

Examples of even unimodular lattices include the hyperbolic plane H over $\mathbf{Z}$ (arising from the quadratic form $q_2(x,y) = xy$ on $\mathbf{Z}^2$) and the positive-definite or negative-definite versions of the E_8 root lattice inside $\mathbf{Z}^8$ [**S73**, Ch. V, 1.4.3].

Any unimodular lattice $(\mathrm{M}', \mathrm{B}')$ with odd rank must satisfy $\mathrm{Q}_{\mathrm{B}'}(\mathrm{M}') \not\subset 2\mathbf{Z}$; i.e., it is "type I" in the terminology of [**S73**, Ch. V]. Indeed, otherwise the non-degenerate B' mod 2 on M/2M would be alternating, hence a symplectic form over $\mathbf{F}_2$, and symplectic spaces over a field always have even dimension.

In many characteristic-free references on quadratic forms (e.g., [**Chev97**], [**SV**]), a quadratic space (V, q) over a field k is called "non-degenerate" when $\mathrm{B}_q : \mathrm{V} \times \mathrm{V} \to k$ is a perfect pairing. This has the effect of ruling out odd-dimensional V when $\mathrm{char}(k) = 2$, since B_q is alternating in characteristic 2 and a symplectic space is always even-dimensional. A systematic approach to semisimple group schemes over $\mathbf{Z}$ must incorporate all special orthogonal groups in a characteristic-free manner, and to that end we will find it convenient to use a broader notion of non-degeneracy that allows odd-dimensional examples in characteristic 2:

Definition 2.5. — A quadratic space (M, q) over a commutative ring R is *non-degenerate* if q is fiberwise nonzero over Spec(R) and the R-flat zero scheme $(q = 0) \subset \mathbf{P}(\mathrm{M}^*)$ is R-smooth.

If R is a field then our notion of non-degeneracy is equivalent to perfectness of B_q except in odd dimension in characteristic 2, for which it is the condition that the defect space

$$\mathrm{M}^{\perp} := \{m \in \mathrm{M} \,|\, \mathrm{B}_q(m, \cdot) = 0\}$$

is 1-dimensional (the smallest possibility in odd-rank cases in characteristic 2); the steps of the proof of this equivalence are given in [**Co2**, Exer. 1.6.10]. For $\mathrm{R} = \mathbf{Z}$, the condition of fiberwise non-vanishing for q over Spec(R) is classically called *primitivity* for q. In general, the R-smoothness of $(q = 0)$ may be checked fiberwise due to its R-flatness. If R is a domain with fraction field K and $\mathrm{R} \neq \mathrm{K}$ then non-degeneracy for a quadratic space (M, q) over R is much stronger than non-degeneracy for $(\mathrm{M}_{\mathrm{K}}, q_{\mathrm{K}})$.

To make non-degeneracy explicit for $\mathrm{R} = \mathbf{Z}$, we shall consider the cases of even and odd rank separately. Consider an even integer $n > 0$. It is easy to check that the following are equivalent for (M, q) with M of rank n:

– $\mathrm{disc}(q) \in \mathbf{Z}^{\times} = \{\pm 1\}$,

– B_q is perfect over $\mathbf{Z}$,

– q is $\mathbf{Z}$-primitive with $\mathbf{Z}$-smooth projective zero scheme $(q = 0) \subset \mathbf{P}(\mathrm{M}^*)$.

These correspond to the rank-n even unimodular lattices studied in [**S73**, Ch. V]. They exist with signature (r, s) whenever $r - s \equiv 0 \bmod 8$ (in which case $n = r + s$ is certainly even):

Example 2.6. — If $r = s + 8k$ with $k \geqslant 0$ then $n = 2s + 8k$ and we can take (M, q) to be the orthogonal direct sum $\mathrm{H}^{\oplus s} \oplus \mathrm{E}_8^{\oplus k}$. If instead $r = s - 8k$ with $k > 0$ then $n = 2r + 8k$ and we can take (M, q) to be the orthogonal direct sum of r copies of H and k copies of the negative-definite version of E_8.

The condition $r - s \equiv 0 \bmod 8$ is not only sufficient for the existence of an even-rank (M, q) of signature (r, s) with $\mathrm{disc}(q) = \pm 1$, but it is also necessary. Indeed, evenness of the rank reduces this to the same necessity for even unimodular lattices, which holds for any rank [**S73**, Ch. V, 2.1, Cor. 1 to Thm. 2].

For odd $n = 2m + 1$ the discriminant $\mathrm{disc}(q)$ is always even. Indeed, $\mathrm{B}_q \bmod 2$ is always an alternating form over $\mathbf{F}_2$ and hence would be symplectic if $\mathrm{disc}(q)$ is odd, yet symplectic spaces over fields always have even dimension. Thus, a better measure of non-degeneracy over $\mathbf{Z}$ for odd n is provided by the *half-discriminant* $\mathrm{disc}'(q) = \mathrm{disc}(q)/2$. More specifically, if $n = 2m + 1 \geqslant 1$ then by [**Co2**, C.1.4(3)] the two conditions

– $\mathrm{disc}'(q) \in \mathbf{Z}^\times = \{\pm 1\}$,

– q is $\mathbf{Z}$-primitive with $\mathbf{Z}$-smooth projective zero scheme $(q = 0) \subset \mathbf{P}(\mathrm{M}^*)$ are equivalent and in such cases $\mathrm{B}_q \bmod 2$ on $\mathrm{M}/2\mathrm{M}$ has a 1-dimensional defect space $(\mathrm{M}/2\mathrm{M})^\perp$. (For the rank-1 case $(\mathbf{Z}, \pm x^2)$, the projective space $\mathbf{P}(\mathrm{M}^*)$ is $\mathrm{Spec}(\mathbf{Z})$ and the zero scheme $(q = 0)$ in there is empty.)

Example 2.7. — Odd-rank quadratic lattices (M, q) with half-discriminant ± 1 exist with signature (r, s) whenever $r - s \equiv \pm 1 \bmod 8$. For example, if $r = s + 8k - 1$ with $k > 0$ then we can take (M, q) to be an orthogonal direct sum $\mathrm{H}^{\oplus s} \oplus \mathrm{E}_8^{\oplus (k-1)} \oplus \mathrm{E}_7$. If instead $r = s + 8k + 1$ with $k \geqslant 0$ then we use $\mathrm{H}^{\oplus s} \oplus \mathrm{E}_8^{\oplus k} \oplus (x^2)$.

In the indefinite case, any (M, q) that is non-degenerate over $\mathbf{Z}$ is determined up to $\mathbf{Z}$-isomorphism by its rank and signature. The proof for M of even rank reduces to the analogue for unimodular lattices, which is [**S73**, Ch. V, 2.2, Thm. 6] (for any rank). (In the special case $r = s$, which is to say signature $(n/2, n/2)$ with n even, it follows that the only example is a direct sum of $n/2$ hyperbolic planes over $\mathbf{Z}$.) The proof for M of odd rank is harder because it does not reduce to the analogue for unimodular lattices, so we give a proof in Appendix A using special orthogonal group schemes (to be defined shortly) and cohomological techniques with semisimple $\mathbf{Z}$-groups (see § 3).

In the definite case the situation is completely different. In addition to Examples 2.6 and 2.7 with rank $n \equiv 0, \pm 1 \bmod 8$, the number of additional examples grows in abundance as $n \to \infty$. A weighted enumeration of the definite examples of a given rank $n \equiv 0, \pm 1 \bmod 8$ is provided by the Minkowski–Siegel mass formula (see [**S73**, Ch. V, 2.3], [**CS**, § 4], and the references therein).

We have seen that the possibilities for the signature of an even-rank quadratic lattice that is non-degenerate over **Z** are precisely those (r,s) with $r,s \geqslant 0$ such that $r-s \equiv 0 \bmod 8$, and that in odd rank the pairs satisfying $r-s \equiv \pm 1 \bmod 8$ do occur. To show that no other signatures occur for odd rank, we need to digress and explain a general procedure that associates *unimodular* lattices of *odd* rank n to rank-n quadratic lattices that are non-degenerate over **Z**. The construction and study of such unimodular lattices is informed by properties of special orthogonal group schemes over **Z** attached to quadatic lattices, so we first review how such group schemes are defined.

Definition 2.8. — The *special orthogonal group* $\mathrm{SO}(q)$ of a quadratic lattice (M,q) is the schematic closure inside $\mathrm{O}(q)$ (or equivalently, inside $\mathrm{GL}(\mathrm{M})$) of the smooth closed subgroup $\mathrm{SO}(q_{\mathbf{Q}}) \subset \mathrm{O}(q_{\mathbf{Q}}) = \mathrm{O}(q)_{\mathbf{Q}}$.

Since **Z** is Dedekind, this is a **Z**-flat closed subscheme of $\mathrm{O}(q)$ that is moreover a subgroup scheme. To prove that $\mathrm{SO}(q)$ has good properties when (M,q) is non-degenerate over **Z**, one uses another procedure in such cases to produce a **Z**-smooth closed subgroup of $\mathrm{O}(q)$ with generic fiber $\mathrm{SO}(q_{\mathbf{Q}})$; such a closed subgroup must equal the flat closure $\mathrm{SO}(q)$ as just defined. (For example, if $q = q_{2m+1}$ then $\mathrm{SO}(q_{2m+1})$ as defined by Zariski closure over **Z** must coincide with the **Z**-smooth SO_{2m+1} as defined in (2.3).) Such alternative procedures underlie the proofs of the results invoked in the next two examples.

Example 2.9. — Let (M,q) be non-degenerate over **Z** with rank $n = 2m \geqslant 4$. The **Z**-group $\mathrm{O}(q)$ is **Z**-smooth [**Co2**, C.1.5] and $\mathrm{SO}(q)$ is a semisimple **Z**-group of type D_m that coincides with $\mathrm{O}(q) \cap \mathrm{SL}(\mathrm{M})$ over $\mathbf{Z}[1/2]$ [**Co2**, C.2.9, C.3.9, C.3.2]. We denote $\mathrm{SO}(q_{2m})$ as SO_{2m}.

In contrast, the **Z**-group $\mathrm{O}(q) \cap \mathrm{SL}(\mathrm{M})$ is not flat at 2 [**Co2**, C.3.4]. Moreover, the **Z**-group $\mathrm{SO}(q) = \mathrm{SO}(-q)$ is a Chevalley group when $r = s$ (this applies to $q = q_{2m}$), but otherwise its **Q**-fiber is not split since even its **R**-fiber is not split (as $\pm q_{\mathbf{R}}$ are non-split for signature reasons and the homothety class of a non-degenerate quadratic space over a field is determined by the isomorphism class of its special orthogonal group [**Co2**, C.3.13, C.3.15]). Thus, distinct integers $r,s \geqslant 0$ in the same congruence class modulo 8 with $n = r+s \geqslant 4$ provide **Z**-models of non-split connected semisimple **Q**-groups of type $\mathrm{D}_{n/2}$.

Example 2.10. — If (M,q) is non-degenerate over **Z** with odd rank $n = 2m+1 \geqslant 3$ then $\mathrm{SO}(q)$ is a semisimple **Z**-group of type B_m (in particular, it is **Z**-smooth with connected semisimple fibers); see [**Co2**, C.2.9, C.3.9].

Now we are in position to construct unimodular lattices of odd rank n from quadratic lattices (M,q) of odd rank n that are non-degenerate over **Z** (i.e., $\mathrm{disc}(q) = \pm 2$). The first step is:

Lemma 2.11. — *There is an* $\mathbf{F}_2$*-isomorphism* $q_{\mathbf{F}_2} \simeq q_n$ *as quadratic spaces.*

Proof. — The condition $\mathrm{disc}(q) = \pm 2$ ensures that the *odd*-dimensional quadratic space $\mathrm{M}/2\mathrm{M}$ over $\mathbf{F}_2$ is non-degenerate in the sense that its defect space has the minimal possible dimension (namely, 1). By [**SGA7**, XII, Prop. 1.2] the quadratic spaces $(\mathrm{M}, q)_{\mathbf{F}_2}$ and $(\mathbf{F}_2^n, q_n)$ are isomorphic over $\overline{\mathbf{F}}_2$, so the isomorphism class of $(\mathrm{M}, q)_{\mathbf{F}_2}$ is classified by a Galois cohomology class in $\mathrm{H}^1(\mathbf{F}_2, \mathrm{O}_n(\overline{\mathbf{F}}_2))$. But $\mathrm{O}_n = \mu_2 \times \mathrm{SO}_n$ since n is odd, and SO_n is smooth and connected, so $\mathrm{H}^1(\mathbf{F}_2, \mathrm{O}_n(\overline{\mathbf{F}}_2)) = \mathrm{H}^1(\mathbf{F}_2, \mathrm{SO}_n) = 1$ by a vanishing theorem of Lang [**Bor**, 16.5(i)]. Hence, $q_{\mathbf{F}_2} \simeq q_n$ as desired. □

Remark 2.12. — The existence of an $\mathbf{F}_2$-isomorphism $q_{\mathbf{F}_2} \simeq q_n$ for odd n, as proved above, can be strengthened: $q_{\mathbf{Z}_2} \simeq \pm q_n$ over $\mathbf{Z}_2$. (This will be useful later.) To prove this, we may and do replace q with $-q$ if necessary so that $\mathrm{disc}(q) = 2(-1)^{n(n-1)/2} = \mathrm{disc}(q_n)$. By [**SGA7**, XII, Prop. 1.2], q and q_n become isomorphic fppf-locally over $\mathbf{Z}_2$, so the affine finite type Isom-scheme $\mathrm{I} = \mathrm{Isom}(q, q_n)$ over $\mathbf{Z}_2$ is an O_n-torsor for the fppf topology. Since $\mathrm{SO}_n \to \mathrm{Spec}(\mathbf{Z})$ is smooth with connected fibers, $\mathrm{H}^1(\mathbf{Z}_2, \mathrm{SO}_n) = 1$ (as we will explain more generally in Proposition 3.10). But $\mathrm{O}_n = \mu_2 \times \mathrm{SO}_n$ because n is odd, so the isomorphism class of I is classified by an fppf μ_2-torsor.

This μ_2-torsor is classified by an element in the fppf cohomology group $\mathrm{H}^1(\mathbf{Z}_2, \mu_2)$, and that group in turn is identified with $\mathbf{Z}_2^\times/(\mathbf{Z}_2^\times)^2$ via the 2-power fppf Kummer sequence

$$1 \to \mu_2 \to \mathbf{G}_\mathrm{m} \xrightarrow{t^2} \mathbf{G}_\mathrm{m} \to 1$$

over $\mathbf{Z}_2$. If $a \in \mathbf{Z}_2^\times$ represents the Kummer class of I then upon passing from the fppf O_n-torsor I back to the quadratic space q via descent theory yields a $\mathbf{Z}_2$-isomorphism

$$\varphi : (\mathrm{M}, q)_{\mathbf{Z}_2} \simeq (\mathbf{Z}_2^n, a x_0^2 + x_1 x_2 + \cdots + x_{n-2} x_{n-1}).$$

The discriminants of the two sides in $\mathbf{Q}_2^\times/(\mathbf{Z}_2^\times)^2$ are $2(-1)^{n(n-1)/2}$ and $2a(-1)^{n(n-1)/2}$ respectively, so $a \in (\mathbf{Z}_2^\times)^2$. Hence, $q_{\mathbf{Z}_2} \simeq q_n$ as desired.

By inspection of $(q_n)_{\mathbf{F}_2}$ with $n = 2m+1$, it follows from Lemma 2.11 that the maximal isotropic subspaces $\mathrm{V} \subset \mathrm{M}/2\mathrm{M}$ have codimension m. Clearly B_q is $2\mathbf{Z}$-valued on the preimage M' of such a V in M. Upon choosing V to obtain such an M', the symmetric bilinear form $\mathrm{B}' = (1/2)\mathrm{B}_q|_{\mathrm{M}' \times \mathrm{M}'}$ is $\mathbf{Z}$-valued with $\mathrm{disc}(\mathrm{B}') = 2^{-n}[\mathrm{M} : \mathrm{M}']^2 \mathrm{disc}(q) = \pm 1$, so $(\mathrm{M}', \mathrm{B}')$ is unimodular. Note that $\mathrm{Q}_{\mathrm{B}'} = q|_{\mathrm{M}'}$, and $(\mathrm{M}', \mathrm{B}')$ has the same signature as (M, q). The unimodular lattices $(\mathrm{M}', \mathrm{B}')$ built in this way are always odd ("type I" in the terminology of [**S73**, Ch. V]), since their rank n is odd; see Example 2.4.

For odd rank $n \geqslant 3$ there is more than one choice of $\mathrm{V} \subset \mathrm{M}/2\mathrm{M}$, and as we vary V the sublattices $\mathrm{M}' \subseteq \mathrm{M}$ will vary too. However, the isomorphism class of $(\mathrm{M}', \mathrm{B}')$ does not vary in the indefinite case, since these unimodular lattices all have the same signature and in the indefinite case a unimodular lattice (of any rank) is determined up to isomorphism by its signature [**S73**, Ch. V, 2.2, Thm. 6]. The abstract isomorphisms among all $(\mathrm{M}', \mathrm{B}')$'s in the indefinite odd-rank case can be made more concrete by using the strong approximation theorem for indefinite spin groups to prove:

Proposition 2.13. — *If* (M, q) *is indefinite and non-degenerate over* $\mathbf{Z}$ *with odd rank* $n \geqslant 3$ *then the group* $\mathrm{SO}(q)(\mathbf{Z})$ *acts transitively on the set of all such lattices* $\mathrm{M}' \subseteq \mathrm{M}$.

Proof. — Since $n \geqslant 3$, $\mathrm{SO}(q)$ is a semisimple $\mathbf{Z}$-group with absolutely simple fibers. We first claim that the group $\mathrm{SO}(q)(\mathbf{F}_2) = \mathrm{O}(q)(\mathbf{F}_2)$ acts transitively on the set of maximal isotropic subspaces $\mathrm{V} \subset \mathrm{M}/2\mathrm{M}$.

Letting W be the quotient of M/2M by the defect line $(\mathrm{M}/2\mathrm{M})^{\perp}$, the bilinear form B_q mod 2 induces a symplectic form $\overline{\mathrm{B}}_q$ on W. The maximal isotropic subspaces of M/2M with respect to B_q mod 2 contain the defect line, so the set of such subspaces corresponds bijectively to the set of maximal isotropic subspaces of W (relative to $\overline{\mathrm{B}}_q$). It is elementary that the automorphism group of a symplectic space over a field acts transitively on the set of maximal isotropic subspaces, so $\mathrm{Sp}(\overline{\mathrm{B}}_q)(\mathbf{F}_2)$ acts transitively on the set of maximal isotropic subspaces of W. To conclude the same for the action of $\mathrm{SO}(q)(\mathbf{F}_2)$ on the set of maximal isotropic subspaces of M/2M, it suffices to show that the natural isogeny $f : \mathrm{SO}(q)_{\mathbf{F}_2} \to \mathrm{Sp}(\overline{\mathrm{B}}_q)$ (see [**Co2**, C.3.6]) induces a bijection on $\mathbf{F}_2$-points.

Isogenous smooth connected affine groups over a finite field have the same number of rational points [**Bor**, 16.8], and $\ker f$ is infinitesimal (it is α_2^{n-1} since $q_{\mathbf{F}_2} \simeq q_n$; see [**Co2**, C.3.6]). Thus, f is bijective on $\mathbf{F}_2$-points.

In view of the transitivity of the $\mathrm{SO}(q)(\mathbf{F}_2)$-action, it suffices to show that $\mathrm{SO}(q)(\mathbf{Z}) \to \mathrm{SO}(q)(\mathbf{F}_2)$ is *surjective.* The verification of this surjectivity property is a job for the strong approximation theorem, except that strong approximation applies to simply connected groups whereas $\mathrm{SO}(q)$ is not simply connected. But $\mathrm{Spin}(q)_{\mathbf{F}_2} \to \mathrm{SO}(q)_{\mathbf{F}_2}$ is an isogeny with infinitesimal kernel over a finite field, so the map on rational points is bijective. Hence, it suffices to show that $\mathrm{Spin}(q)(\mathbf{Z}) \to \mathrm{Spin}(q)(\mathbf{F}_2)$ is surjective.

The indefiniteness of $q_{\mathbf{R}}$ implies that $\mathrm{SO}(q)_{\mathbf{R}}$ is $\mathbf{R}$-isotropic, so $\mathrm{Spin}(q)_{\mathbf{R}}$ is $\mathbf{R}$-isotropic. Hence, the strong approximation theorem for absolutely simple and simply connected $\mathbf{Q}$-groups (see [**Pras**] and references therein) is applicable to $\mathrm{Spin}(q)_{\mathbf{Q}}$ and the archimedean place of $\mathbf{Q}$. This says that $\mathrm{Spin}(q)(\mathbf{Q}) \cdot \mathrm{Spin}(q)(\mathbf{R})$ is dense in $\mathrm{Spin}(q)(\mathbf{A}_{\mathbf{Q}})$, so for the open subring $\widehat{\mathbf{Z}}$ inside the ring of finite adeles of $\mathbf{Q}$ we conclude that the intersection

$$\mathrm{Spin}(q)(\mathbf{Q}) \cap \mathrm{Spin}(q)(\widehat{\mathbf{Z}}) = \mathrm{Spin}(q)(\mathbf{Z})$$

is dense in $\mathrm{Spin}(q)(\widehat{\mathbf{Z}})$. But $\mathrm{Spin}(q)(\widehat{\mathbf{Z}}) \to \mathrm{Spin}(q)(\mathbf{Z}/d\mathbf{Z})$ is surjective with open kernel for all $d > 0$ since $\mathrm{Spin}(q)$ is $\mathbf{Z}$-smooth, so any dense subset of $\mathrm{Spin}(q)(\widehat{\mathbf{Z}})$ maps onto $\mathrm{Spin}(q)(\mathbf{Z}/d\mathbf{Z})$. In particular, $\mathrm{Spin}(q)(\mathbf{Z}) \to \mathrm{Spin}(q)(\mathbf{Z}/d\mathbf{Z})$ is surjective. Setting $d = 2$ gives the desired surjectivity from $\mathbf{Z}$-points onto $\mathbf{F}_2$-points. □

Now we may resume our discussion of the possibilities for the signature (r, s) of a quadratic lattice (M, q) of odd rank $n = 2m + 1$ with $\mathrm{disc}(q) = \pm 2$, showing that the sufficient condition $r - s \equiv \pm 1 \bmod 8$ from Example 2.7 is necessary.

By passing to $(\mathrm{M}, -q)$ if necessary so that $\mathrm{disc}(q) = \mathrm{disc}(q_n)$, we claim that $r - s \equiv 1 \bmod 8$. To prove this, consider a unimodular lattice $(\mathrm{M}', \mathrm{B}')$ associated to (M, q) via a choice of maximal isotropic subspace V in M/2M as in the discussion preceding Proposition 2.13. Let $\overline{\mathrm{B}}' = \mathrm{B}' \bmod 2$ on $\mathrm{M}'/2\mathrm{M}'$. By [**S73**, Ch. V, § 2.1, Thm. 2], $r - s \equiv \mathrm{Q}_{\mathrm{B}'}(\mathbf{m}'_0) \bmod 8$ where $\mathbf{m}'_0 \in \mathrm{M}'$ lifts the unique $\overline{\mathbf{m}}'_0 \in \mathrm{M}'/2\mathrm{M}'$ such that $\overline{\mathrm{B}}'(\overline{\mathbf{m}}'_0, \cdot) = \mathrm{Q}_{\mathrm{B}'} \bmod 2$ on $\mathrm{M}'/2\mathrm{M}'$. Thus, we seek to prove $\mathrm{Q}_{\mathrm{B}'}(\mathbf{m}'_0) \equiv 1 \bmod 8$.

As we saw in Remark 2.12, there is a $\mathbf{Z}_2$-isomorphism $\varphi : q_{\mathbf{Z}_2} \simeq q_n$. The map $\mathrm{O}_n(\mathbf{Z}_2) \to \mathrm{O}_n(\mathbf{F}_2) = \mathrm{SO}_n(\mathbf{F}_2)$ is surjective since SO_n is $\mathbf{Z}_2$-smooth, and $\mathrm{O}_n(\mathbf{F}_2)$ acts transitively on the set of maximal isotropic subspaces (as we saw in the proof of Proposition 2.13), so φ may be chosen such that $\varphi \bmod 2$ carries V onto any desired maximal isotropic subspace. Hence, we can choose V to correspond to the span of the standard basis vectors $\overline{e}_1, \overline{e}_3, \dots, \overline{e}_{n-2}$ in $\oplus_{j=0}^{n-1} \mathbf{F}_2 \overline{e}_j$, so $\overline{\mathbf{m}}'_0 = \overline{e}_0$. We may therefore choose $\mathbf{m}'_0$ to lift $e_0 \bmod 8$ via the mod-8 reduction of the $\mathbf{Z}_2$-isomorphism φ, so $\mathrm{Q}_{\mathrm{B}'}(\mathbf{m}'_0) \equiv q_n(e_0) \bmod 8$. But $q_n(e_0) = 1$, so necessity of the signature condition for odd n is proved.

Example 2.14. — Consider (M, q) with odd rank $n = 2m + 1 \geqslant 3$ such that $\mathrm{disc}(q) = \pm 2$. Let (r, s) be the signature of $q_{\mathbf{R}}$.

Assume $r = s \pm 1$, so we are in the indefinite case since $r + s = n \geqslant 3$. By uniqueness for a given indefinite signature (see Theorem A.1). (M, q) is an orthogonal direct sum of $(\mathbf{Z}, \pm x^2)$ and m hyperbolic planes over $\mathbf{Z}$. Thus, in such cases the semisimple $\mathbf{Z}$-group $\mathrm{SO}(q) = \mathrm{SO}(-q)$ is a Chevalley group (this applies to $q = q_{2m+1}$).

Suppose $|r - s| > 1$, so the $\mathbf{Q}$-fiber of $\mathrm{SO}(q)$ is not split (as even the $\mathbf{R}$-fiber is not split, since $\pm q_{\mathbf{R}}$ is non-split due to signature reasons and hence we can argue as in Example 2.9). Thus, for $n = r + s \geqslant 3$ with integers $r, s \geqslant 0$ satisfying $r - s \equiv \pm 1 \bmod 8$ and $r - s \neq \pm 1$, we obtain $\mathbf{Z}$-models of non-split connected semisimple $\mathbf{Q}$-groups of type $\mathrm{B}_{(n-1)/2}$.

Summary. For a quadratic lattice (M, q) that is non-degenerate over $\mathbf{Z}$ (i.e., $\mathrm{disc}(q) = \pm 1$ for even rank, and $\mathrm{disc}(q) = \pm 2$ for odd rank), $\mathrm{SO}(q)$ is a semisimple $\mathbf{Z}$-group. If the signature (r, s) satisfies $|r - s| > 1$ then $\mathrm{SO}(q)_{\mathbf{Q}}$ is *non-split*; such (M, q) exist if and only if $r - s \equiv 0, \pm 1 \bmod 8$. Later we will see other examples of **Z**-models of non-split semisimple **Q**-groups.

(In Proposition 4.4 we will show that for any quadratic lattice (M, q) that is non-degenerate over **Z**, the **Z**-isomorphism class of $\mathrm{SO}(q)$ determines the isomorphism class of (M, q) up to negating q. Furthermore, a semisimple **Z**-group whose generic fiber is a **Q**-form of SO_n for $n \geqslant 3$ *must* be $\mathrm{SO}(q)$ for such an (M, q), as we will explain in Remark 4.11.)

3. Cohomological formalism and Z-groups

Non-abelian Galois cohomology is a useful formalism for understanding the structure of and possibilities for connected semisimple groups over interesting fields (see [**S97**, III]). We need to apply a version of this over rings when studying semisimple **Z**-groups.

We begin our discussion by summarizing some general non-abelian cohomological constructions and terminology for reductive group schemes over any non-empty scheme S. This requires working systematically with the étale topology on S, and it differs significantly from the case of fields in that *finite* étale covers of S are generally not cofinal among all étale covers, even if S is the spectrum of a Dedekind domain (e.g., consider Zariski refinements of finite étale covers). The cases of most interest to us are $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$ where A is a field or principal ideal domain (such as a number field, local field, or **Z**). Some additional details on this formalism are provided in [**SGA3**, XXIV] and [**Co2**, 7.1.4, 7.1.9].

Let G_0 be a reductive S-group, and $\mathrm{Z}_{\mathrm{G}_0}$ its scheme-theoretic center. There is a smooth separated S-group $\mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}}$ representing the automorphism functor of G_0 (on the category of S-schemes). The conjugation action of G_0 on itself factors through an action of the semisimple S-group $\mathrm{G}_0^{\mathrm{ad}} := \mathrm{G}_0/\mathrm{Z}_{\mathrm{G}_0}$ on G_0 that identifies $\mathrm{G}_0^{\mathrm{ad}}$ as an open and closed subgroup scheme of $\mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}_0}$. The quotient sheaf $\mathrm{Out}_{\mathrm{G}_0/\mathrm{S}} := \mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}}/\mathrm{G}_0^{\mathrm{ad}}$ for the étale topology on S is represented by a separated étale S-group that is locally constant for the étale topology on S. The diagram of S-groups

$$1 \to \mathrm{G}_0^{\mathrm{ad}} \to \mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}} \to \mathrm{Out}_{\mathrm{G}_0/\mathrm{S}} \to 1 \tag{3.1}$$

is short exact for the étale topology on S-schemes. If S is noetherian, normal, and connected (e.g., $\mathrm{Spec}(k)$ for a field k, or $\mathrm{Spec}(\mathbf{Z})$) then considering closures of points in the generic fiber shows $\mathrm{Out}_{\mathrm{G}_0/\mathrm{S}}$ has S-finite connected components (see [**SGA3**, X, 5.14] or the proof of [**Co2**, 7.1.9]).

Example 3.1. — Suppose G_0 is split, so we may choose a split (fiberwise) maximal S-torus $\mathrm{T}_0 \subset \mathrm{G}_0$ whose $\mathbf{G}_{\mathrm{m}}$-dual is identified as a constant étale sheaf M_{S} for a finite free **Z**-module M such that the nontrivial T_0-weights on

$\mathfrak{g}_0$ arise from the $\mathbf{Z}$-dual $\mathrm{M}^\vee \subset \mathrm{Hom}_{\mathrm{S}}(\mathrm{T}_0, \mathbf{G}_{\mathrm{m}})$ and the root line bundles $\mathfrak{g}_a$ ($a \in \Phi(\mathrm{G}_0, \mathrm{T}_0) \subset \mathrm{M}^\vee - \{0\}$) are trivial. Let $\mathrm{B}_0 \supset \mathrm{T}_0$ be the Borel S-subgroup $\mathrm{P}_{\mathrm{G}_0}(\lambda)$ for a cocharacter $\lambda \in \mathrm{M} \subset \mathrm{Hom}_{\mathrm{S}}(\mathbf{G}_{\mathrm{m}}, \mathrm{T}_0)$ not annihilated by any $a \in \Phi(\mathrm{G}_0, \mathrm{T}_0)$ [**Co2**, 5.2.2].

Let (R, Δ) denote the associated based root datum. Choose a pinning (i.e., a trivialization of the line bundle $\mathfrak{g}_a$ for each $a \in \Delta$). The subgroup functor of $\mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}}$ consisting of "pinned automorphisms" (i.e., those that respect $(\mathrm{T}_0, \mathrm{B}_0)$ and the pinning) maps isomorphically onto $\mathrm{Out}_{\mathrm{G}_0/\mathrm{S}}$ and is identified with the constant S-group $\mathrm{Aut}(\mathrm{R}, \Delta)_{\mathrm{S}}$ associated to the automorphism group of the based root datum. Hence, (3.1) splits as a semi-direct product, giving an isomorphism

$$\mathrm{G}_0^{\mathrm{ad}} \rtimes \mathrm{Aut}(\mathrm{R}, \Delta)_{\mathrm{S}} \simeq \mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}} \tag{3.2}$$

depending on $(\mathrm{T}_0, \mathrm{B}_0)$ and the pinning. (See [**SGA3**, XXIV, 1.3(iii)] or [**Co2**, 7.1.9(3)] for details.)

Example 3.2. — Suppose $\mathrm{S} = \mathrm{Spec}(k)$ for a field k, so the étale k-group $\mathrm{Out}_{\mathrm{G}_0/k}$ corresponds to a continuous action of $\mathrm{Gal}(k_s/k)$ on the discrete group $\mathrm{Out}_{\mathrm{G}_0/k}(k_s) = \mathrm{Aut}(\mathrm{R}, \Delta)$, where (R, Δ) is the based root datum associated to $(\mathrm{G}_0)_{k_s}$. For a theoretical understanding of how the Galois group acts on (R, Δ) without a split hypothesis on G_0, it is best to work with the *canonical based root datum* associated to G_0 as in [**Co2**, 7.1.2]. A more concrete description is provided by the formalism of the "$*$-action" as explained in [**T1**, § 2.3].

Consider $\mathrm{S} = \mathrm{Spec}(\mathbf{Z})$. Since $\mathbf{Z}$ is noetherian and normal, the connected components of $\mathrm{Out}_{\mathrm{G}_0/\mathbf{Z}}$ are finite étale over $\mathrm{Spec}(\mathbf{Z})$. But $\pi_1(\mathrm{Spec}(\mathbf{Z})) = 1$, as we noted in the proof of Lemma 1.1, so $\mathrm{Out}_{\mathrm{G}_0/\mathbf{Z}}$ must be a *constant* $\mathbf{Z}$-group (even if G_0 is not split). Likewise, the schematic center $\mathrm{Z}_{\mathrm{G}_0}$ is a $\mathbf{Z}$-group of multiplicative type [**Co2**, 3.3.4], so since $\mathbf{Z}$ is a noetherian normal domain with trivial étale fundamental group it follows that $\mathrm{Z}_{\mathrm{G}_0}$ is $\mathbf{G}_{\mathrm{m}}$-dual to the *constant* sheaf on $(\mathrm{Spec}(\mathbf{Z}))_{\text{ét}}$ associated to a finitely generated abelian group [**Co2**, B.3.6] (even if G_0 is not split).

Example 3.3. — Let (M, q) be a quadratic lattice with rank $n \geqslant 3$, and assume it is non-degenerate over $\mathbf{Z}$. Let $\mathrm{GO}(q)$ denote the orthogonal similitude group scheme; i.e., points of $\mathrm{GL}(\mathrm{M})$ that preserve q up to a unit scaling factor. (Define $\mathrm{GO}_n := \mathrm{GO}(q_n)$.) This is a smooth $\mathbf{Z}$-group [**Co2**, C.3.11]. Since $\mathrm{GO}(q)$ is generated by $\mathrm{O}(q)$ and the central $\mathbf{G}_{\mathrm{m}}$, clearly $\mathrm{SO}(q)$ is normal inside $\mathrm{GO}(q)$. The resulting conjugation action of $\mathrm{GO}(q)$ on $\mathrm{SO}(q)$ makes the central subgroup $\mathbf{G}_{\mathrm{m}}$ act trivially and so defines a $\mathbf{Z}$-homomorphism

$$\mathrm{PGO}(q) := \mathrm{GO}(q)/\mathbf{G}_{\mathrm{m}} \to \mathrm{Aut}_{\mathrm{SO}(q)/\mathbf{Z}}.$$

(Define $\mathrm{PGO}_n := \mathrm{PGO}(q_n)$.) This is an isomorphism [**Co2**, Lemma C.3.12].

The adjoint quotient $\mathrm{SO}(q)^{\mathrm{ad}}$ is identified as a subgroup of $\mathrm{PGO}(q)$ in the evident manner. For even n (allowing $n = 8$) the quotient group $\mathrm{Out}_{\mathrm{SO}(q)/\mathbf{Z}}$ is the constant group $\mathrm{O}(q)/\mathrm{SO}(q) = \mathbf{Z}/2\mathbf{Z}$ and for odd n we have $\mathrm{Out}_{\mathrm{SO}(q)/\mathbf{Z}} = 1$ (see [**Co2**, C.3.11]).

The set of isomorphism classes of reductive S-groups G that are isomorphic to G_0 étale-locally on S is in bijection with the pointed Čech cohomology set

$$\mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}}) = \varinjlim_{\mathrm{S}'/\mathrm{S}} \mathrm{H}^1(\mathrm{S}'/\mathrm{S}, \mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}})$$

where S' varies through a cofinal set of étale covers of S and $\mathrm{H}^1(\mathrm{S}'/\mathrm{S}, \cdot)$ is defined in terms of Čech 1-cocycles relative to $\mathrm{S}' \to \mathrm{S}$ (see [**SGA3**, XXIV, 1.18], [**Ha**, 1.3], or [**Co2**, (7.1.1)]). The isomorphism class of G thereby corresponds to an element

$$c(\mathrm{G}) \in \mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}})$$

that is functorial with respect to base change on S. We write

$$d(\mathrm{G}) \in \mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{Out}_{\mathrm{G}_0/\mathrm{S}})$$

to denote its image via $\mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}} \to \mathrm{Out}_{\mathrm{G}_0/\mathrm{S}}$.

Example 3.4. — Assume $\mathrm{S} = \mathrm{Spec}(k)$ for a field k, so $\mathrm{H}^1(k, \mathrm{Aut}_{\mathrm{G}_0/k})$ can be identified with the Galois cohomology set $\mathrm{H}^1(\mathrm{Gal}(k_s/k), \mathrm{Aut}((\mathrm{G}_0)_{k_s}))$. An explicit 1-cocycle representing the class $c(\mathrm{G})$ is given by the procedure in the proof of [**Co2**, 7.1.1] (or see [**S97**, III, § 1.1–1.3]). If G_0 is semisimple then $d(\mathrm{G})$ is represented by the conjugacy class of the continuous homomorphism $\mathrm{Gal}(k_s/k) \to \mathrm{Aut}(\mathrm{R}, \Delta) \subset \mathrm{Aut}(\mathrm{Dyn}((\mathrm{G}_0)_{k_s})$ given by the "$*$-action" [**T1**, § 2.3] of the Galois group on the Dynkin diagram of $(\mathrm{G}_0)_{k_s}$.

Example 3.5. — Let $\mathrm{G} \to \mathrm{S}$ be an affine group scheme. The set of isomorphism classes of right G-torsors $\mathrm{E} \to \mathrm{S}$ satisfying $\mathrm{E}(\mathrm{S}') \neq \varnothing$ for an étale surjection $\mathrm{S}' \to \mathrm{S}$ is $\mathrm{H}^1(\mathrm{S}'/\mathrm{S}, \mathrm{G})$. This identification uses that G is S-affine to ensure that the descent datum encoded by an element of the set $\mathrm{Z}^1(\mathrm{S}'/\mathrm{S}, \mathrm{G})$ of Čech 1-cocycles relative to S'/S is effective. Passing to the limit over étale covers, $\mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{G})$ is the set of isomorphism classes of G-torsors $\mathrm{E} \to \mathrm{S}$ for the étale topology. The same formalism carries over using the fppf topology.

For *smooth* S-affine G, the natural map of sets $\mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{G}) \to \mathrm{H}^1(\mathrm{S}_{\text{fppf}}, \mathrm{G})$ is bijective. This amounts to the assertion that any fppf right G-torsor $\mathrm{E} \to \mathrm{S}$ admits sections étale-locally on S. To prove this assertion, note that by fppf descent for the property of smoothness, $\mathrm{E} \to \mathrm{S}$ inherits smoothness from $\mathrm{G} \to \mathrm{S}$. Smooth surjections of schemes always admit sections étale-locally on the base [**EGA**, IV_4, 17.16.3(2)], so E is indeed a torsor for the étale topology when G is smooth.

Example 3.6. — To bring the previous example down to earth, $\mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{O}_{2m})$ is identified functorially in S with the set of isomorphism classes of pairs (V, q) where V is a rank-$2m$ vector bundle on S and $q : \mathrm{V} \to \mathscr{O}_{\mathrm{S}}$ is a (fiberwise) non-degenerate quadratic form. This identification assigns to each (V, q) the Isom-scheme $\mathrm{Isom}((\mathscr{O}_{\mathrm{S}}^{\oplus 2m}, q_{2m}), (\mathrm{V}, q))$ that is a right O_{2m}-torsor via precomposition with the O_{2m}-action on $\mathscr{O}_{\mathrm{S}}^{\oplus 2m}$. For $\mathrm{O}_{2m+1} = \mu_2 \times \mathrm{SO}_{2m+1}$ we have an analogous result for (V, q) of rank $2m+1$, but we must use the fppf topology if 2 is not a unit on S (as μ_2 is not S-smooth in such cases).

Consider the special case $\mathrm{S} = \mathrm{Spec}(\mathrm{R})$ for a principal ideal domain R with fraction field K. Let $n > 0$ be an integer, and assume either n is odd or $\mathrm{char}(\mathrm{K}) \neq 2$. Let (M, q) be a fiberwise non-degenerate quadratic space over R of rank $n > 0$, so $\mathrm{O}(q_{\mathrm{K}})/\mathrm{SO}(q_{\mathrm{K}}) = \mu_2$ (using that $\mathrm{char}(\mathrm{K}) \neq 2$ if n is even; see [**Co2**, Rem. C.2.11]). We have a well-defined element $\mathrm{disc}(q) \in (\mathrm{R} - \{0\})/(\mathrm{R}^\times)^2 \subset \mathrm{K}^\times/(\mathrm{K}^\times)^2$.

The canonical map $\mathrm{O}(q_{\mathrm{K}}) \to \mu_2$ induces $f : \mathrm{H}^1(\mathrm{R}, \mathrm{O}(q)) \to \mathrm{H}^1(\mathrm{K}, \mu_2) = \mathrm{K}^\times/(\mathrm{K}^\times)^2$ that lands inside $\mathrm{R}^\times/(\mathrm{R}^\times)^2$ and is made explicit as follows: for any fiberwise non-degenerate (M', q') of rank n, the isomorphism class of the right $\mathrm{O}(q)$-torsor $\mathrm{Isom}(q, q')$ is carried by f to the class of the ratio $\mathrm{disc}(q')/\mathrm{disc}(q)$. As a special case, the natural map $\mathrm{H}^1(\mathrm{R}, \mathrm{O}_n) \to \mathrm{R}^\times/(\mathrm{R}^\times)^2$ carries the class of (M', q') to the class of $\mathrm{disc}(q')/\mathrm{disc}(q_n)$, and the presence of $\mathrm{disc}(q_n)$ here cannot be ignored since it is generally not in $(\mathrm{R}^\times)^2$.

Returning to the setting above Example 3.4, the S-group G is called a *pure inner form* of G_0 if $c(\mathrm{G})$ is in the image of $\mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{G}_0)$. Under the weaker hypothesis that $c(\mathrm{G})$ is in the image of $\mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{G}_0^{\mathrm{ad}})$, we say that G is an *inner form* of G_0.

Example 3.7. — Assume $\mathrm{S} = \mathrm{Spec}(k)$ for a field k. The "pure inner form" condition means that G is constructed from G_0 by modifying the canonical k_s/k-descent datum on $(\mathrm{G}_0)_{k_s}$ via 1-cocycles in $\mathrm{Z}^1(k_s/k, \mathrm{Aut}_{\mathrm{G}_0/k})$ arising from 1-cocycles valued in $\mathrm{G}_0(k_s)$. The "inner form" condition means that we can instead get G by using a 1-cocycle valued in $\mathrm{G}_0^{\mathrm{ad}}(k_s)$.

A 1-cocycle of the latter type lifts to a 1-cochain valued in $\mathrm{G}_0(k_s)$ if k is perfect or if $\mathrm{Z}_{\mathrm{G}_0}$ is smooth (equivalently, $\mathrm{char}(k)$ does not divide the order of the torsion part of the geometric character group of $\mathrm{Z}_{\mathrm{G}_0}$), but it generally does not lift to a 1-*cocycle* valued in $\mathrm{G}_0(k_s)$.

Computations with Čech 1-cocycles show (as in [**Co1**, Prop. B.3.2] over fields, via a method also applicable over schemes) that the exact sequence (3.1) gives an exact sequence of pointed sets

$$\mathrm{Aut}(\mathrm{G}_0)\backslash\mathrm{Out}_{\mathrm{G}_0/\mathrm{S}}(\mathrm{S}) \to \mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{G}_0^{\mathrm{ad}}) \to \mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}}) \to \mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{Out}_{\mathrm{G}_0/\mathrm{S}})$$

in which the final map carries $c(\mathrm{G})$ to $d(\mathrm{G})$. Thus, $d(\mathrm{G}) = 1$ if and only if G is an inner form of G_0. Also, if G_0 is split then the semidirect product structure in Example 3.1 shows that $\mathrm{Aut}(\mathrm{G}_0) \to \mathrm{Out}_{\mathrm{G}_0/\mathrm{S}}(\mathrm{S})$ is surjective, so the map

$$\mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{G}_0^{\mathrm{ad}}) \to \mathrm{H}^1(\mathrm{S}_{\text{ét}}, \mathrm{Aut}_{\mathrm{G}_0/\mathrm{S}})$$

between pointed sets has trivial kernel in such cases. However, in those cases this map can fail to be injective, even over fields:

Example 3.8. — Consider $\mathrm{G}_0 = \mathrm{SL}_n$ over a field k, with $n > 1$. The map $\mathrm{G}_0^{\mathrm{ad}} \to \mathrm{Aut}_{\mathrm{G}_0/k}$ is the natural map $\mathrm{PGL}_n \to \mathrm{Aut}_{\mathrm{SL}_n/k}$ defined by the conjugation action of $\mathrm{PGL}_n = \mathrm{GL}_n/\mathbf{G}_{\mathrm{m}}$ on SL_n. The induced map on H^1's carries the Brauer class of a rank-n^2 central simple algebra A over k to the isomorphism class of the k-group $\mathrm{SL}_1(\mathrm{A})$ of units of A with reduced norm 1.

If A is a division algebra whose Brauer class is not of order dividing 2 then the opposite algebra $\mathrm{A}^{\mathrm{opp}}$ defines a different Brauer class from that of A but their associated k-groups $\mathrm{SL}_1(\mathrm{A}^{\mathrm{opp}}) = \mathrm{SL}_1(\mathrm{A})^{\mathrm{opp}}$ and $\mathrm{SL}_1(\mathrm{A})$ are k-isomorphic (via inversion). Thus, we get counterexamples to injectivity when k admits central division algebras A of rank n^2 whose class in $\mathrm{Br}(k)$ is not killed by 2. It is a consequence of class field theory that such division algebras exist over any global or non-archimedean local field when $n > 2$ ([**AT**, X, Cor. to Thm. 6], [**S79**, XIII, § 3, Cor. 3]).

For any semisimple group scheme $\mathrm{G} \to \mathrm{S}$, there is a unique central isogeny $\widetilde{\mathrm{G}} \to \mathrm{G}$ where $\widetilde{\mathrm{G}}$ is a semisimple S-group with simply connected fibers (see [**Ha**, § 1.2] or [**Co2**, Exer. 6.5.2]). The canonicity of this central cover identifies $\mathrm{Aut}_{\mathrm{G}/\mathrm{S}}$ with a closed and open S-subgroup of $\mathrm{Aut}_{\widetilde{\mathrm{G}}/\mathrm{S}}$. In the split case, the resulting equality $(\widetilde{\mathrm{G}})^{\mathrm{ad}} = \mathrm{G}^{\mathrm{ad}}$ thereby yields an inclusion between the constant outer automorphism schemes of G and $\widetilde{\mathrm{G}}$, corresponding to the natural injective homomorphism from the automorphism group of a semisimple root datum into the automorphism group of the associated root system.

We now specialize the preceding considerations to the special case $\mathrm{S} = \mathrm{Spec}(\mathbf{Z})$. Let $\mathscr{G}_0$ be a reductive **Z**-group. The **Z**-group $\mathrm{Out}_{\mathscr{G}_0/\mathbf{Z}}$ is constant by Example 3.2, and it is not **Z**-finite when $\mathrm{Z}_{\mathrm{G}_0}$ has fiber dimension > 1. The pointed set $\mathrm{H}^1(\mathbf{Z}, \mathrm{Out}_{\mathscr{G}_0/\mathbf{Z}})$ is therefore trivial due to the vanishing of $\pi_1(\mathrm{Spec}(\mathbf{Z}))$ and:

Proposition 3.9. — *If* S *is a connected normal noetherian scheme and* Γ *is a group then* $\mathrm{H}^1(\mathrm{S}_{\text{ét}}, \Gamma_{\mathrm{S}})$ *is identified with the set of conjugacy classes of continuous homomorphisms from* $\pi_1(\mathrm{S})$ *into the discrete group* Γ.

Proof. — By the formalism of étale fundamental groups and étale sheaf theory, conjugacy classes of continuous homomorphisms $\pi_1(\mathrm{S}) \to \Gamma$ correspond to isomorphism classes of Γ-torsors for the étale topology on S that are split by a *finite* étale cover. The set $\mathrm{H}^1(\mathrm{S}_{\text{ét}}, \Gamma_{\mathrm{S}})$ classifies the set of isomorphism classes of Γ_{S}-torsor sheaves $\mathscr{F}$ on $\mathrm{S}_{\text{ét}}$. Thus, it suffices to show that every such $\mathscr{F}$ is represented by an étale S-scheme $\mathrm{E} \to \mathrm{S}$ that is a disjoint union of *finite* étale S-schemes (so $\mathrm{E}(\mathrm{S}') \neq \varnothing$ for some finite étale cover $\mathrm{S}' \to \mathrm{S}$).

We may choose an étale cover $\mathrm{S}' \to \mathrm{S}$ of finite type such that $\mathscr{F}(\mathrm{S}')$ is non-empty. The torsor property gives that $\mathscr{F}_{\mathrm{S}'}$ is represented by the constant S'-scheme $\Gamma_{\mathrm{S}'}$, so $\mathscr{F}$ is an étale descent over $\mathrm{S}_{\text{ét}}$ of the functor on $\mathrm{S}'_{\text{ét}}$ represented by $\Gamma_{\mathrm{S}'}$. Such a descent is necessarily an algebraic space E étale over S, and this algebraic space is S-separated since $\Gamma_{\mathrm{S}'}$ is S'-separated.

The locally noetherian algebraic space E can be covered by quasi-compact open subspaces, each of which is necessarily quasi-finite and separated over the scheme S and hence is a scheme [**Knut**, II, 6.15]. Thus, E is a scheme étale over S. Since $\mathrm{E} \to \mathrm{S}$ becomes constant over an étale cover of the normal noetherian S, the connected components of E are finite étale over S by [**SGA3**, X, 5.14] (or see the proof of [**Co2**, 7.1.9]). □

For general reductive **Z**-groups $\mathscr{G}_0$, we have just shown that the map $\mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0^{\mathrm{ad}}) \to \mathrm{H}^1(\mathbf{Z}, \mathrm{Aut}_{\mathscr{G}_0/\mathbf{Z}})$ is surjective. Before we discuss the consequences of this, we digress to prove Proposition 1.3, as the necessary tools are now in place.

Proof. — (of Proposition 1.3) Let $\mathscr{G}_0$ be the Chevalley group over **Z** with **Q**-fiber G_0 having the same root datum as G, so $(\mathrm{G}_0)_{\mathrm{K}} \simeq \mathrm{G}$, and let $\mathscr{G}$ be an R-model of G. Since $\mathscr{G}_0$ contains a split fiberwise maximal **Z**-torus $\mathscr{T}_0$, it contains a Borel **Z**-subgroup $\mathscr{B}_0$ (by the same dynamic procedure with a sufficiently generic cocharacter λ as at the start of Example 3.1).

The Borel K-subgroup $\mathrm{B} = (\mathscr{B}_0)_{\mathrm{K}} \subset (\mathscr{G}_0)_{\mathrm{K}} = \mathrm{G} = \mathscr{G}_{\mathrm{K}}$ gives rise to a K-point on the scheme $\mathrm{Bor}_{\mathscr{G}/\mathrm{R}}$ of Borel subgroups of $\mathscr{G}$. By the valuative criterion for properness, this K-point extends to an R-point since $\mathrm{Bor}_{\mathscr{G}/\mathrm{R}}$ is R-proper and R is Dedekind. Thus, $\mathrm{B} = \mathscr{B}_{\mathrm{K}}$ for a Borel R-subgroup $\mathscr{B} \subset \mathscr{G}$.

Consider the Isom-functor

$$\mathscr{I} := \mathrm{Isom}((\mathscr{G}_0, \mathscr{B}_0)_{\mathrm{R}}, (\mathscr{G}, \mathscr{B}))$$

that assigns to any R-scheme Y the set of Y-group isomorphisms $(\mathscr{G}_0)_{\mathrm{Y}} \simeq \mathscr{G}_{\mathrm{Y}}$ carrying $(\mathscr{B}_0)_{\mathrm{Y}}$ onto $\mathscr{B}_{\mathrm{Y}}$. This functor is a sheaf for the étale topology. We want to show that $\mathscr{I}$ has an R-point, as then $\mathscr{G} \simeq (\mathscr{G}_0)_{\mathrm{R}}$, concluding the proof.

Note that $\mathscr{I}$ has a natural right action by the group functor $\mathscr{A} := \mathrm{Aut}_{(\mathscr{G}_0, \mathscr{B}_0)_{\mathrm{R}}/\mathrm{R}}$ that is a sheaf on the étale site of Spec(R). This action makes $\mathscr{I}$ an $\mathscr{A}$-torsor for the étale topology because any reductive group scheme splits étale-locally on the base and any two Borel subgroups of a reductive group scheme become conjugate étale-locally on the base. Thus, it suffices to show that the class of $\mathscr{I}$ in the pointed set $\mathrm{H}^1(\mathrm{R}, \mathscr{A})$ of isomorphism classes of right $\mathscr{A}$-torsor sheaves on $(\mathrm{Spec}(\mathrm{R}))_{\text{ét}}$ is trivial.

Let Θ denote the automorphism group of the based root datum associated to the split $\mathbf{Z}$-group $(\mathscr{G}_0, \mathscr{B}_0, \mathscr{T}_0)$, or equivalently to the split K-group G. Using the semi-direct product structure (3.2) in Example 3.1 applied to $\mathscr{G}_0$, the automorphism functor $\mathscr{A}$ over $(\mathrm{Spec}(\mathrm{R}))_{\text{ét}}$ is an extension of the constant R-group Θ_{R} by the R-pullback of the Borel subgroup $\mathscr{B}_0^{\mathrm{ad}} := \mathscr{B}_0/\mathrm{Z}_{\mathscr{G}_0} \subset \mathscr{G}_0^{\mathrm{ad}}$ since a Borel subgroup of a reductive group scheme is its own normalizer scheme [**Co2**, Cor. 5.2.8]. Consider the resulting exact sequence of pointed sets

$$\mathrm{H}^1(\mathrm{R}, (\mathscr{B}_0^{\mathrm{ad}})_{\mathrm{R}}) \to \mathrm{H}^1(\mathrm{R}, \mathscr{A}) \to \mathrm{H}^1(\mathrm{R}, \Theta_{\mathrm{R}}).$$

The class of $\mathscr{I}$ in the middle term is trivial over K since $\mathscr{I}(\mathrm{K})$ is non-empty by design of $\mathscr{B}$. The image of this class in $\mathrm{H}^1(\mathrm{R}, \Theta_{\mathrm{R}})$ has trivial restriction over K and hence is trivial, due to Proposition 3.9 (since $\pi_1(\mathrm{Spec}(\mathrm{K})) \to \pi_1(\mathrm{Spec}(\mathrm{R}))$ is surjective, as R is a normal noetherian domain). Hence, we just have to prove the vanishing of $\mathrm{H}^1(\mathrm{R}, (\mathscr{B}_0^{\mathrm{ad}})_{\mathrm{R}})$. By choosing a composition series of $\mathscr{B}_0^{\mathrm{ad}}$ over $\mathbf{Z}$ with successive quotients $\mathbf{G}_{\mathrm{a}}$ and $\mathbf{G}_{\mathrm{m}}$ (see [**Co2**, Prop. 5.1.16]) this reduces to the vanishing of Pic(R) □

Returning to the study of a general reductive $\mathbf{Z}$-group $\mathscr{G}_0$ (not necessarily a Chevalley group) with generic fiber denoted G_0, classes in $\mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0^{\mathrm{ad}})$ satisfy a strong local triviality property upon restricting them to $\mathbf{Z}_p$:

Proposition 3.10. — *Let* R *be a complete discrete valuation ring with finite residue field* $\mathbf{F}$. *For any smooth affine* R*-group* $\mathscr{H}$ *with connected fibers, the set* $\mathrm{H}^1(\mathrm{R}, \mathscr{H})$ *is trivial.*

Proof. — By Example 3.5, it suffices to show that if $\mathrm{E} \to \mathrm{Spec}(\mathrm{R})$ is an $\mathscr{H}$-torsor for the étale topology then E(R) is non-empty. By descent theory, $\mathrm{E} \to \mathrm{Spec}(\mathrm{R})$ is a smooth surjection since $\mathscr{H}$ is a smooth R-group. Since the special fiber $\mathrm{E}_{\mathbf{F}}$ over $\mathbf{F}$ is an $\mathscr{H}_{\mathbf{F}}$-torsor, by Lang's theorem for homogeneous spaces under smooth connected groups over finite fields [**Bor**, 16.5(i)] (or see [**DGa**, III, § 5, 7.5] with smoothness relaxed to finite type) it follows that $\mathrm{E}(\mathbf{F})$ is non-empty. But Zariski-locally on the source, any smooth map factors through an étale map to an affine space, so Hensel's Lemma implies that any rational point in the special fiber of a smooth scheme over R lifts to an R-point; see [**EGA**, IV_4, 18.5.17]. □

Corollary 3.11. — *Let* $\mathscr{H}$ *be a smooth affine* $\mathbf{Z}$*-group with connected fibers. Any class in the image of* $\mathrm{H}^1(\mathbf{Z}, \mathscr{H}) \to \mathrm{H}^1(\mathbf{Q}, \mathscr{H}_{\mathbf{Q}})$ *has trivial image in* $\mathrm{H}^1(\mathbf{Q}_p, \mathscr{H}_{\mathbf{Q}_p})$ *for every prime p.*

Proof. — Apply base-change functoriality of Čech cohomology with respect to the compositions $\mathbf{Z} \to \mathbf{Z}_p \to \mathbf{Q}_p$ and $\mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}_p$ and use Proposition 3.10 with $\mathrm{R} = \mathbf{Z}_p$. □

We have shown that every class in $\mathrm{H}^1(\mathbf{Z}, \mathrm{Aut}_{\mathscr{G}_0/\mathbf{Z}})$ arises from $\mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0^{\mathrm{ad}})$, so applying Proposition 3.10 and Corollary 3.11 to $\mathscr{G}_0^{\mathrm{ad}}$ gives that the restriction

$$\mathrm{H}^1(\mathbf{Z}, \mathrm{Aut}_{\mathscr{G}_0/\mathbf{Z}}) \to \mathrm{H}^1(\mathbf{Q}_p, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{Q}_p}) \tag{3.3}$$

is trivial for all primes p. Thus, *every* $\mathbf{Z}$-form of $\mathscr{G}_0$ has $\mathbf{Q}_p$-fiber isomorphic to $(\mathrm{G}_0)_{\mathbf{Q}_p}$ for all p. But there is a Chevalley group that is a $\mathbf{Z}$-form of $\mathscr{G}_0$, so by Lemma 1.1 we see that $(\mathrm{G}_0)_{\mathbf{Q}_p}$ is *split* for all p.

We finish our preliminary discussion of $\mathbf{Z}$-models with a useful description of simply connected semisimple $\mathbf{Z}$-groups.

Proposition 3.12. — *Any simply connected semisimple $\mathbf{Z}$-group is a direct product $\prod \mathscr{G}_i$ where each $\mathscr{G}_i$ is a simply connected semisimple $\mathbf{Z}$-group with absolutely simple fibers.*

Proof. — By [**Co2**, 6.4.4], any fiberwise nontrivial simply connected semisimple group over a non-empty scheme S is a Weil restriction $\mathrm{R}_{\mathrm{S}'/\mathrm{S}}(\mathrm{H})$ for a finite étale cover $\mathrm{S}' \to \mathrm{S}$ and a simply connected semisimple S'-group H whose fibers $\mathrm{H}_{s'}$ are absolutely simple. In the case $\mathrm{S} = \mathrm{Spec}(\mathbf{Z})$, necessarily S' is a disjoint union of copies of $\mathrm{Spec}(\mathbf{Z})$ (by Minkowski's theorem). For any scheme S and disjoint union $\mathrm{S}' = \coprod \mathrm{S}_i$ of finitely many copies S_i of S, any S'-scheme X' has the form $\mathrm{X}' = \coprod \mathrm{X}_i$ for an S_i-scheme X_i. It is easy to check via the functorial characterization of Weil restriction that as functors on S-schemes, $\mathrm{R}_{\mathrm{S}'/\mathrm{S}}(\mathrm{X}') = \prod \mathrm{X}_i$. □

4. The generic fiber

Consider a connected reductive $\mathbf{Q}$-group G admitting a $\mathbf{Z}$-model $\mathscr{G}$ (understood to be reductive). We shall prove that $\mathscr{G}$ is split over $\mathbf{Z}_p$ for all primes p (improving on the observation after Corollary 3.11 that $\mathscr{G}_{\mathbf{Q}_p}$ is split for all p). We will also show that G is a pure inner form of a split group over $\mathbf{Q}$ (see Lemma 4.7), and by a more sophisticated version of the same arguments we will even prove that $\mathscr{G}$ is a pure inner form of a Chevalley group over $\mathbf{Z}$ (see Remark 4.8).

Let $\mathscr{G}_0$ be the split form of $\mathscr{G}$ over $\mathbf{Z}$ (i.e., the Chevalley group with the same root datum as $\mathrm{G}_{\overline{\mathbf{Q}}}$), and let $\mathrm{G}_0 = (\mathscr{G}_0)_{\mathbf{Q}}$, so G_0 is the split form of G over $\mathbf{Q}$. Let $c(\mathrm{G}) \in \mathrm{H}^1(\mathbf{Q}, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{Q}})$ and $d(\mathrm{G}) \in \mathrm{H}^1(\mathbf{Q}, \mathrm{Out}_{\mathrm{G}_0/\mathbf{Q}})$ be the associated cohomology classes as above Example 3.4. Define $c(\mathscr{G})$ and $d(\mathscr{G})$ over $\mathbf{Z}$ similarly.

Lemma 4.1. — *The class $d(\mathrm{G})$ is trivial; i.e., G is an inner form of G_0.*

Proof. — We have already given a proof of this result using the cohomological formalism over $\mathbf{Z}$: by Proposition 3.9 we have $\mathrm{H}^1(\mathbf{Z}, \mathrm{Out}_{\mathscr{G}_0/\mathbf{Z}}) = 1$, so

$d(\mathscr{G}) = 1$ and hence $d(\mathrm{G}) = 1$. But that argument rests on the entire appartus of the automorphism scheme over rings, rather than just over fields (where it is more classical). So we now give another proof via Galois-theoretic considerations over fields (also using the theory of reductive group schemes over discrete valuation rings). The arithmetic content will remain exactly the same: Minkowski's theorem that every number field $\mathrm{K} \neq \mathbf{Q}$ is ramified at some prime.

Note that $d(\mathrm{G})$ is a conjugacy class of homomorphisms from $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ into $\mathrm{Aut}(\mathrm{R}, \Delta)$. If $\mathrm{K}/\mathbf{Q}$ is the finite Galois extension cut out by this conjugacy class, we want to show $\mathrm{K} = \mathbf{Q}$. By Minkowski's theorem, if $\mathrm{K} \neq \mathbf{Q}$ then some rational prime is ramified in K and hence the local class $d_p(\mathrm{G}) := d(\mathrm{G})|_{\mathbf{Q}_p} = d(\mathrm{G}_{\mathbf{Q}_p}) \in \mathrm{H}^1(\mathbf{Q}_p, \mathrm{Aut}(\mathrm{R}, \Delta))$ at such a prime p is ramified (i.e., nontrivial on the inertia group at p). Thus, to prove $\mathrm{K} = \mathbf{Q}$ it suffices to show that $d(\mathrm{G})$ is unramified for all p. But $\mathscr{G}$ is reductive over $\mathbf{Z}$, so it is reductive over the completion $\mathbf{Z}_p$, and a reductive group over $\mathbf{Z}_p$ splits over a finite unramified extension [**SGA3**, XIX, 6.1] (or see [**Co2**, 5.2.14]). Hence, G splits over a finite unramified extension of $\mathbf{Q}_p$, so $d_p(\mathrm{G})$ is unramified for all p. □

We have already seen that $\mathrm{G}_{\mathbf{Q}_p}$ is split for all primes p. This property, which makes no reference to reductive groups over rings, forces G to be an inner form of G_0. Indeed, this is a consequence of a more general result over any global field (where Minkowski's theorem on extensions unramified at finite places is not available):

Proposition 4.2. — *Let k be a global field. Any connected reductive k-group* H *that splits at all finite places must be an inner form of the split k-group* H_0 *of the same type.*

Proof. — We have to prove triviality of the class $d(\mathrm{H}) \in \mathrm{H}^1(k, \mathrm{Aut}(\mathrm{R}, \Delta))$, where (R, Δ) is the based root datum of H_0. The task is to show that a continuous homomorphism from $\mathrm{Gal}(k_s/k)$ into a discrete group is trivial if it is trivial at all finite places (i.e., trivial on all decomposition groups at finite places). The image of such a homomorphism is a finite Galois group $\mathrm{Gal}(k'/k)$, so it suffices to show that any such Galois group is generated by its decomposition groups at the finite places.

The subgroup of $\mathrm{Gal}(k'/k)$ generated by such decomposition groups is normal and thereby corresponds to a finite Galois subextension K/k for which all decomposition groups are trivial. In other words, all finite places of k are totally split in K, which forces $[\mathrm{K} : k] = 1$ by the Chebotarev Density Theorem. □

By [**Co2**, 5.3.1, 5.3.3], there is a natural central isogeny $\mathscr{T} \times \mathscr{G}' \to \mathscr{G}$ over $\mathbf{Z}$, where $\mathscr{G}'$ is a semisimple normal $\mathbf{Z}$-subgroup of $\mathscr{G}$ (the derived group) and

$\mathscr{T}$ is the maximal central $\mathbf{Z}$-torus in $\mathscr{G}$. All $\mathbf{Z}$-tori are split, as we explained in the proof of Lemma 1.1. Thus, to classify the possibilities for $\mathscr{G}$ over $\mathbf{Z}$, or even for its generic fiber G over $\mathbf{Q}$, it is reasonable to concentrate on the semisimple case, which we now do.

Any semisimple group over a scheme S is a central quotient of a simply connected semisimple S-group that is unique up to unique isomorphism; this follows via étale descent from the split case, which in turn is deduced from the Existence and Isomorphism Theorems (see [**Co2**, Ex. 6.5.2]). Note also that a semisimple $\mathbf{Z}$-group is a pure inner form of a Chevalley group if its simply connected central cover is. Thus, for our purposes (especially to describe the generic fibers of semisimple $\mathbf{Z}$-groups) there is no loss of generality in focusing on the simply connected case.

In view of Proposition 3.12 (which breaks down completely over integer rings of number fields other than $\mathbf{Q}$), we also lose no generality by restricting attention to describing the connected semisimple $\mathbf{Q}$-groups G that are *absolutely simple*, simply connected, and admit a $\mathbf{Z}$-model. These $\mathbf{Q}$-groups can be characterized without reference to $\mathbf{Z}$-models, as follows. We have shown that any such G is split over $\mathbf{Q}_p$ for all rational primes p, and the converse holds by applying the following with $\mathrm{R} = \mathbf{Z}$:

Lemma 4.3. — *Let* R *be a Dedekind domain with fraction field* K*, and* H *a connected reductive* K*-group that is split over the fraction field* $\mathrm{K}_{\mathfrak{m}}^{\wedge}$ *of the completion* $\mathrm{R}_{\mathfrak{m}}^{\wedge}$ *at every maximal ideal* $\mathfrak{m}$ *of* R*. There exists a reductive* R*-group* $\mathscr{H}$ *such that* $\mathrm{H} \simeq \mathscr{H}_{\mathrm{K}}$.

Proof. — By direct limit arguments (viewing K as a direct limit of its finitely generated R-subalgebras $\mathrm{R}[1/r]$), we can extend H to a smooth affine group with connected fibers over $\mathrm{Spec}(\mathrm{R}[1/r])$ for some nonzero $r \in \mathrm{R}$. Since the generic fiber H is reductive, by openness of the locus of reductive fibers (see [**SGA3**, XIX, 2.5(i)] or [**Co2**, 3.1.9(1), 3.1.12]) this group has reductive restriction over some dense open locus $\mathrm{Spec}(\mathrm{R}[1/r']) \subset \mathrm{Spec}(\mathrm{R}[1/r])$ (with a nonzero $r' \in (r)$). For each maximal ideal $\mathfrak{m}$ dividing (r'), a split $\mathrm{R}_{\mathfrak{m}}^{\wedge}$-model of the split $\mathrm{K}_{\mathfrak{m}}^{\wedge}$-fiber specifies an $\mathrm{R}_{\mathfrak{m}}$-model for H [**BLR**, 6.2/D.4(b)]. These finitely many local models glue to the $\mathrm{R}[1/r']$-model to define a reductive group over R with generic fiber H (cf. the proof of [**BLR**, 1.4/1]). □

To summarize, for the purpose of describing generic fibers of reductive $\mathbf{Z}$-groups the essential task is to describe all connected semisimple $\mathbf{Q}$-groups G that are absolutely simple, simply connected, and split over $\mathbf{Q}_p$ for all p. (In § 6 we will address the construction of explicit $\mathbf{Z}$-models.) This makes no reference to group schemes over rings other than fields.

In the setting of Lemma 4.3 with $\mathrm{R} = \mathbf{Z}$, it is natural to wonder if the $\mathbf{Z}$-group $\mathscr{H}$ is determined up to isomorphism by the $\mathbf{Q}$-isomorphism class of

H. When $\mathrm{H}_{\mathbf{R}}$ is $\mathbf{R}$-anisotropic (or equivalently, when $\mathrm{H}(\mathbf{R})$ is compact), there can exist several such $\mathscr{H}$ that are not isomorphic as $\mathbf{Z}$-groups. This is classical for special orthogonal groups in the definite case. Before we discuss that, it is convenient to record the ambiguity in passing from a non-degenerate quadratic lattice to its special orthogonal group.

Proposition 4.4. — *Let* (M, q) *be a quadratic lattice that is non-degenerate over* $\mathbf{Z}$*. The isomorphism class of the* $\mathbf{Z}$*-group* $\mathrm{SO}(q)$ *determines the isomorphism class of* (M, q) *up to replacing* q *with* $-q$

Proof. — Let $n \geqslant 1$ be the rank of M. The cases $n \leqslant 2$ are elementary (necessarily $q \simeq \pm q_n$), and the cases $n \geqslant 3$ are a consequence of [**Co2**, C.3.13] since $\mathrm{Pic}(\mathrm{Spec}(\mathbf{Z})) = 1$ and $\mathbf{Z}^{\times} = \{\pm 1\}$. □

Since (M, q) is determined by its signature in the indefinite case, as we discussed in § 2, Proposition 4.4 implies that for integers $r, s > 0$ with $r - s \equiv 0, \pm 1 \bmod 8$ and $n := r+s \geqslant 3$ there is *exactly one* $\mathbf{Z}$-form of SO_n with positive $\mathbf{R}$-rank $\min(r, s)$. In the $\mathbf{R}$-anisotropic case this uniqueness breaks down in a very interesting way: there is an abundance of $\mathbf{Z}$-forms (up to isomorphism) but their $\mathbf{Q}$-fibers are all the same, as we now explain. (See Proposition 4.10 for a generalization.)

Consider *definite* quadratic lattices (M, q) of rank $n \geqslant 3$; assume n is as required for the existence of such quadratic spaces. The Minkowski–Siegel mass formula ensures the existence of many non-isomorphic pairs (M, q) for large n. Hence, accounting for the sign ambiguity in the dependence of (M, q) on $\mathrm{SO}(q)$ as in Proposition 4.4, there are at least half as many isomorphism classes among the $\mathbf{Z}$-groups as there are among the quadratic lattices (M, q). Thus, for large n the mass formula provides many pairwise non-isomorphic $\mathbf{Z}$-groups $\mathrm{SO}(q)$ whose $\mathbf{Q}$-fibers are $\mathbf{R}$-anisotropic $\mathbf{Q}$-forms of SO_n.

Proposition 4.5. — *All such lattices* (M, q) *are isomorphic to each other over* $\mathbf{Q}$*, up to negating* q*. In particular, the* $\mathbf{Q}$*-fibers* $\mathrm{SO}(q)_{\mathbf{Q}}$ *coincide up to* $\mathbf{Q}$*-isomorphism.*

Proof. — Negate q if necessary so that $\mathrm{disc}(q) = \mathrm{disc}(q_n)$ (with sign $(-1)^{n(n-1)/2}$). Choose a prime p. We will first show that the isomorphism class of $(\mathrm{M}, q)_{\mathbf{Q}_p}$ is the same for all such (M, q)'s. This class is in the image of $\mathrm{H}^1(\mathbf{Z}_p, \mathrm{O}_n) \to \mathrm{H}^1(\mathbf{Q}_p, \mathrm{O}_n)$, using fppf cohomology (which coincides with the corresponding étale cohomology by Example 3.5 except for odd n over $\mathbf{Z}_p$ when $p = 2$, as in such cases the $\mathbf{Z}_p$-group $\mathrm{O}_n = \mu_2 \times \mathrm{SO}_n$ is flat but not smooth).

For odd n we have $\mathrm{O}_n = \mu_2 \times \mathrm{SO}_n$, and $\mathrm{H}^1(\mathbf{Z}_p, \mathrm{SO}_n) = 1$ by Proposition 3.10. But $\mathrm{H}^1(\mathbf{Z}_p, \mu_2) \to \mathrm{H}^1(\mathbf{Q}_p, \mu_2)$ is the map $\mathbf{Z}_p^{\times}/(\mathbf{Z}_p^{\times})^2 \to \mathbf{Q}_p^{\times}/(\mathbf{Q}_p^{\times})^2$ that is injective, so for odd n the isomorphism class of $(\mathrm{M}, q)_{\mathbf{Q}_p}$ is determined by its image under the natural map

$$\mathrm{H}^1(\mathbf{Q}_p, \mathrm{O}_n) \to \mathrm{H}^1(\mathbf{Q}_p, \mu_2) = \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2.$$

As in Example 3.6, this map carries the class of $(\mathrm{M}, q)_{\mathbf{Q}_p}$ to the class of $\mathrm{disc}(q)/\mathrm{disc}(q_n) = 1$, so for odd n the isomorphism class of $(\mathrm{M}, q)_{\mathbf{Q}_p}$ is the same for all (M, q) under consideration.

Suppose instead that n is even, so the $\mathbf{Z}_p$-group O_n is an extension of $\mathbf{Z}/2\mathbf{Z}$ by SO_n. The diagram of pointed sets

$$\mathrm{H}^1(\mathbf{Z}_p, \mathrm{SO}_n) \to \mathrm{H}^1(\mathbf{Z}_p, \mathrm{O}_n) \to \mathrm{H}^1(\mathbf{Z}_p, \mathbf{Z}/2\mathbf{Z})$$

is exact, so in view of the vanishing of $\mathrm{H}^1(\mathbf{Z}_p, \mathrm{SO}_n)$ it suffices to show that the class of $(\mathrm{M}, q)_{\mathbf{Z}_p}$ has trivial image in $\mathrm{H}^1(\mathbf{Z}_p, \mathbf{Z}/2\mathbf{Z})$. The restriction map $\mathrm{H}^1(\mathbf{Z}_p, \mathbf{Z}/2\mathbf{Z}) \to \mathrm{H}^1(\mathbf{Q}_p, \mathbf{Z}/2\mathbf{Z}) = \mathrm{H}^1(\mathbf{Q}_p, \mu_2)$ is injective (as it is "$\mathbf{Z}/2\mathbf{Z}$-dual" to the surjection of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ onto its maximal unramified quotient), so we just have to compute the image of the class of $(\mathrm{M}, q)_{\mathbf{Q}_p}$ under the map $\mathrm{H}^1(\mathbf{Q}_p, \mathrm{O}_n) \to \mathrm{H}^1(\mathbf{Q}_p, \mu_2)$. This image is $\mathrm{disc}(q)/\mathrm{disc}(q_n) = 1$, as for odd n.

We have shown that for each prime p, the isomorphism class of $(\mathrm{M}, q)_{\mathbf{Q}_p}$ is the same for all (M, q)'s. The isomorphism class of $(\mathrm{M}, q)_{\mathbf{R}}$ is the unique *definite* one of rank n with discriminant having the same sign as $\mathrm{disc}(q_n)$. By the Hasse–Minkowski theorem, it follows that the isomorphism class of $(\mathrm{M}, q)_{\mathbf{Q}}$ is the same for all such (M, q) with a given rank $n \geqslant 3$, so the $\mathbf{Z}$-groups $\mathrm{SO}(q)$ all have the same $\mathbf{Q}$-fiber. □

Remark 4.6. — For some exceptional types (F_4 and E_8, each of which has trivial fundamental group), in § 6 and § 7 we will find that there are non-isomorphic $\mathbf{Z}$-forms that are anisotropic over $\mathbf{R}$ (and so have isomorphic $\mathbf{Q}$-fibers, by Proposition 4.10 below).

Let G be a connected semisimple $\mathbf{Q}$-group that is absolutely simple, simply connected, and split over $\mathbf{Q}_p$ for every p. Let G_0 be the split form of G over $\mathbf{Q}$, so G is an inner form of G_0 by Proposition 4.2. That is, $c(\mathrm{G})$ is the image under $\mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0^{\mathrm{ad}}) \to \mathrm{H}^1(\mathbf{Q}, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{Q}})$ of a class $c' \in \mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0^{\mathrm{ad}})$.

We can do better: such a c' can be chosen such that $c'|_{\mathbf{Q}_p}$ is trivial for all p. Indeed, we know that G admits a $\mathbf{Z}$-model $\mathscr{G}$, and $d(\mathscr{G}) = 1$ by Proposition 3.9, so $c(\mathscr{G})$ arises from a class $\xi \in \mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0^{\mathrm{ad}})$. It follows from Proposition 3.10 that $\xi|_{\mathbf{Z}_p} = 1$ for all p, so $c(\mathscr{G}_{\mathbf{Z}_p}) = 1$ for all p, which is to say that $\mathscr{G}_{\mathbf{Z}_p}$ is split for all p. Moreover, by Corollary 3.11, the class $c' := \xi_{\mathbf{Q}}$ has trivial restriction over every $\mathbf{Q}_p$, so c' is of the desired type. Such a c' that is trivial over every $\mathbf{Q}_p$ will be shown to arise from $\mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0)$ in the proof of:

Lemma 4.7. — *The* $\mathbf{Q}$*-group* G *is a pure inner form of the split group* G_0.

Proof. — The Hasse principle for adjoint semisimple groups [**PR**, § 6.5, Thm. 6.22] says that the map of sets

$$\mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0^{\mathrm{ad}}) \to \prod_v \mathrm{H}^1(\mathbf{Q}_v, \mathrm{G}_0^{\mathrm{ad}})$$

is injective, so the class $c' \in \mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0^{\mathrm{ad}})$ is determined by its restriction c'_∞ in $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0^{\mathrm{ad}})$ (since the local classes $c'_p = c'|_{\mathbf{Q}_p}$ are trivial by hypothesis). In particular, c'_∞ determines the **Q**-isomorphism class of G (as this isomorphism class is the image of c' in $\mathrm{H}^1(\mathbf{Q}, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{Q}})$). For example, if $c'_\infty = 1$ then $\mathrm{G} \simeq \mathrm{G}_0$ as **Q**-groups.

Let $\mathrm{Z} := \mathrm{Z}_{\mathrm{G}_0}$ be the center of G_0, giving an exact sequence of pointed sets

$$\mathrm{H}^1(\mathbf{Q}, \mathrm{Z}) \longrightarrow \mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0) \longrightarrow \mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0^{\mathrm{ad}}) \xrightarrow{\delta} \mathrm{H}^2(\mathbf{Q}, \mathrm{Z}).$$

The center of a split simply connected semisimple group is Cartier dual to the fundamental group of the root system, so the **Q**-group Z is isomorphic to μ_n for some $n \geqslant 1$ or $\mu_2 \times \mu_2$ (by inspection of the classification of irreducible root systems). Since $\mathrm{H}^2(k, \mu_d) = \mathrm{Br}(k)[d]$ for any field k and integer $d > 0$, $\mathrm{H}^2(\mathbf{Q}, \mathrm{Z})$ is equal to $\mathrm{Br}(\mathbf{Q})[n]$ or $\mathrm{Br}(\mathbf{Q})[2] \times \mathrm{Br}(\mathbf{Q})[2]$. Local restriction at each place v of **Q** carries $\delta(c')$ to $\delta_v(c'_v) \in \mathrm{H}^2(\mathbf{Q}_v, \mathrm{Z})$ for $c'_v := c'|_{\mathbf{Q}_v}$.

By global class field theory, any Brauer class over a global field has local invariants in **Q**/**Z** that vanish at all but finitely many places and sum to 0, so a global class that is locally trivial away from one place is globally trivial. Thus, since $\delta_p(c'_p) = 1$ for all primes p, we conclude that $\delta(c') = 1$, so the class c' (whose archimedean component c'_∞ determines the isomorphism class of the group G over **Q**) is in the image of $\mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0)$. This says that G is a pure inner form of G_0 over **Q**. □

Remark 4.8. — A variant of the preceding proof gives more: any **Z**-model $\mathscr{G}$ of G is a pure inner form of the split form over **Z**. That is, if $\mathscr{G}_0$ is the split simply connected **Z**-group of the same type as G then we claim that the class of $\mathscr{G}$ in $\mathrm{H}^1(\mathbf{Z}, \mathrm{Aut}_{\mathscr{G}_0/\mathbf{Z}})$ arises from $\mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0)$. We have already seen that the class of $\mathscr{G}$ arises from $\mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0^{\mathrm{ad}})$ (this is the vanishing of $d(\mathscr{G})$), so it suffices to show that the map $\mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0) \to \mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0^{\mathrm{ad}})$ is surjective.

The central extension

$$1 \to \mathrm{Z}_{\mathscr{G}_0} \to \mathscr{G}_0 \to \mathscr{G}_0^{\mathrm{ad}} \to 1$$

is a short exact sequence for the fppf topology over Spec(**Z**), and degree-1 Čech-cohomology with coefficients in a smooth affine group is the same for the étale and fppf topologies (as we noted in Example 3.5). The **Z**-group $\mathrm{Z}_{\mathscr{G}_0}$ is Cartier dual to the finite abelian fundamental group of the root system [**Co2**, Ex. 5.1.7]. Explicitly, by inspection of the classification of irreducible root systems, it is either μ_n for some $n \geqslant 1$ or $\mu_2 \times \mu_2$. As is explained in the proof of Theorem A.1, there is a connecting map of pointed sets $\delta : \mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0^{\mathrm{ad}}) \to \mathrm{H}^2(\mathbf{Z}, \mathrm{Z}_{\mathscr{G}_0})$ whose kernel is the image of $\mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0)$. Hence, it suffices to show that $\mathrm{H}^2(\mathbf{Z}, \mu_d) = 1$ for any integer $d > 0$, which is Lemma A.4.

Let G_0 be a connected semisimple $\mathbf{Q}$-group that is split, simple, and simply connected. The map $\mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0) \to \mathrm{H}^1(\mathbf{R}, \mathrm{G}_0)$ is bijective: surjectivity holds for any connected linear algebraic group over $\mathbf{Q}$ [**PR**, § 6.5, Prop. 6.17], and the vanishing of $\mathrm{H}^1(\mathbf{Q}_p, \mathrm{G}_0)$ for all p (theorem of Kneser–Bruhat–Tits: [**PR**, § 6.1, Thm. 6.4], [**BT**, Thm. 4.7(ii)]) reduces the injectivity to the Hasse principle for simply connected semisimple groups [**PR**, § 6.1, Thm. 6.6]. The pointed set $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0)$ is finite, and (especially for the exceptional types) can be computed using methods of Serre [**S97**, III, § 4.5] and Borovoi [**Brv**].

For a class $c_\infty \in \mathrm{H}^1(\mathbf{R}, \mathrm{G}_0)$, the image in $\mathrm{H}^1(\mathbf{Q}, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{Q}})$ of the associated $c \in \mathrm{H}^1(\mathbf{Q}, \mathrm{G}_0)$ classifies a $\mathbf{Q}$-form G of G_0 split at all finite places. (If $c_\infty = 1$ then $c = 1$ and the corresponding G is G_0.) Such a G admits a $\mathbf{Z}$-model, by Lemma 4.3, and we have seen that *every* $\mathbf{Q}$-form of G_0 admitting a $\mathbf{Z}$-model must arise in this way for some c_∞. Thus, the $\mathbf{R}$-groups that arise from $\mathbf{Q}$-forms of G_0 admitting a $\mathbf{Z}$-model are classified by the image of $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0) \to \mathrm{H}^1(\mathbf{R}, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{R}})$.

We claim that every such G as a $\mathbf{Q}$-group is determined *up to* $\mathbf{Q}$-*isomorphism* by the $\mathbf{R}$-group $\mathrm{G}_{\mathbf{R}}$. To prove this, it is sufficient (but not necessary) to show that $\mathrm{G}_{\mathbf{R}}$ determines the class $c_\infty \in \mathrm{H}^1(\mathbf{R}, \mathrm{G}_0)$ with which we began, so we first show:

Lemma 4.9. — *The natural map of sets* $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0) \to \mathrm{H}^1(\mathbf{R}, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{R}})$ *is injective except possibly for types* B_n *with* $n \geqslant 3$ *and* D_n *with* $n \geqslant 4$.

Proof. — For types A and C there is nothing to do since for any field k (such as $k = \mathbf{R}$) we have $\mathrm{H}^1(k, \mathrm{SL}_n) = 1$ by [**S79**, X, § 1] and $\mathrm{H}^1(k, \mathrm{Sp}_{2n}) = 1$ by [**S97**, III, 1.2, Prop. 3]. For types E_8, F_4, and G_2 the map of H^1's is bijective since $\mathrm{G}_0 \to \mathrm{Aut}_{\mathrm{G}_0/\mathbf{R}}$ is an isomorphism by (3.2).

It remains to treat types E_6 and E_7. In both cases, computations with the methods of Borovoi [**Brv**] yield that $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0)$ has size 2. Thus, it suffices to show that in each case the map of pointed sets $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0) \to \mathrm{H}^1(\mathbf{R}, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{R}})$ has trivial kernel. The map $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0^{\mathrm{ad}}) \to \mathrm{H}^1(\mathbf{R}, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{R}})$ has trivial kernel since $\mathrm{Aut}_{\mathrm{G}/k}(k) \to \mathrm{Out}_{\mathrm{G}/k}(k)$ is surjective for any split connected reductive group G over any field k (using pinned automorphisms; see (3.2)). Thus, it is equivalent to show that $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0) \to \mathrm{H}^1(\mathbf{R}, \mathrm{G}_0^{\mathrm{ad}})$ has trivial kernel. In other words, we need to show that the connecting map $\delta : \mathrm{G}_0^{\mathrm{ad}}(\mathbf{R}) \to \mathrm{H}^1(\mathbf{R}, \mathrm{Z}_{\mathrm{G}_0})$ is surjective.

For type E_6 we have $\mathrm{Z}_{\mathrm{G}_0} = \mu_3$, so $\mathrm{H}^1(\mathbf{R}, \mathrm{Z}_{\mathrm{G}_0}) = 1$. This settles the case of E_6. For type E_7 we have $\mathrm{Z}_{\mathrm{G}_0} = \mu_2$, so $\mathrm{H}^1(\mathbf{R}, \mu_2)$ has order 2. Hence, it is equivalent to show that δ is nontrivial, which in turn is equivalent to the map $\mathrm{G}_0(\mathbf{R}) \to \mathrm{G}_0^{\mathrm{ad}}(\mathbf{R})$ not being surjective. But $\mathrm{G}_0(\mathbf{R})$ is connected (because it is generated by subgroups of the form $\mathrm{SL}_2(\mathbf{R})$, as for any split simply connected semisimple $\mathbf{R}$-group, or alternatively because of Cartan's general theorem that the space of $\mathbf{R}$-points of a simply connected semisimple $\mathbf{R}$-group is connected), so it suffices to show that the topological space of $\mathbf{R}$-points of the adjoint split $\mathbf{R}$-group of type E_7 is disconnected. More generally, for any split connected semisimple $\mathbf{R}$-group G_0 with split maximal $\mathbf{R}$-torus T_0 and simply connected central cover $\widetilde{\mathrm{G}}_0$ in which T_0 has split maximal $\mathbf{R}$-torus preimage $\widetilde{\mathrm{T}}_0$, $\pi_0(\mathrm{G}_0(\mathbf{R})) = \mathrm{coker}(\widetilde{\mathrm{T}}_0(\mathbf{R}) \to \mathrm{T}_0(\mathbf{R})) = \mathrm{H}^1(\mathrm{R}, \mu)$ where μ denotes $\ker(\widetilde{\mathrm{G}}_0 \to \mathrm{G}_0)$. For G is adjoint of type E_7 we have $\mu = \mu_2$, so $\#\pi_0(\mathrm{G}_0(\mathbf{R})) = 2$ in such cases. □

Proposition 4.10. — *Let* G *be a connected semisimple* $\mathbf{Q}$*-group that is absolutely simple and simply connected. If* G *admits a* $\mathbf{Z}$*-model then* G *is determined up to isomorphism by* $\mathrm{G}_{\mathbf{R}}$*, and the* $\mathbf{R}$*-groups arising in this way correspond to the image of* $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0) \to \mathrm{H}^1(\mathbf{R}, \mathrm{Aut}_{\mathrm{G}_0/\mathbf{R}})$ *for the split simple simply connected semisimple* $\mathbf{R}$*-group* G_0 *that is a form of* $\mathrm{G}_{\mathbf{R}}$*.*

In particular, for any reduced and irreducible root system Φ*, there is at most one connected semisimple* $\mathbf{Q}$*-group* $\mathrm{G} = \mathrm{G}_\Phi$ *that is absolutely simple and simply connected such that* $\mathrm{G}_{\overline{\mathbf{Q}}}$ *has root system* Φ *and* $\mathrm{G}_{\mathbf{R}}$ *is anisotropic* (*equivalenty,* $\mathrm{G}(\mathbf{R})$ *is compact*)*. The split* $\mathbf{Q}$*-form of* G_Φ *is the only one that admits a* $\mathbf{Z}$*-model and has split* $\mathbf{R}$*-fiber with root system* Φ*.*

Proof. — As we saw via (3.3), the existence of a $\mathbf{Z}$-model implies that $\mathrm{G}_{\mathbf{Q}_p}$ is split for all p. The uniqueness of G over $\mathbf{Q}$ with a given Killing–Cartan type for which $\mathrm{G}_{\mathbf{R}}$ either anisotropic or split follows from the rest because anisotropic and split forms over $\mathbf{R}$ are unique. Hence, by Lemma 4.9 and the discussion preceding it, we just need to prove that G is determined by $\mathrm{G}_{\mathbf{R}}$ for types B_n with $n \geqslant 3$ and D_n with $n \geqslant 4$. Such a G is a form of $\mathrm{Spin}_{\mathrm{N}}$ for some $\mathrm{N} \geqslant 7$. (The argument below will work for any $\mathrm{N} \geqslant 3$.)

Since the $\mathbf{Q}$-form G of $\mathrm{Spin}_{\mathrm{N}}$ is a pure inner form by Lemma 4.7, the map

$$h : \mathrm{H}^1(\mathbf{Q}, \mathrm{Spin}_{\mathrm{N}}) \to \mathrm{H}^1(\mathbf{Q}, \mathrm{Aut}_{\mathrm{Spin}_{\mathrm{N}}/\mathbf{Q}})$$

carries the class of some $\mathrm{Spin}_{\mathrm{N}}$-valued 1-cocycle c to the isomorphism class of the $\mathbf{Q}$-form G. The associated SO_{N}-valued 1-cocycle $\overline{c}$ can be used to twist the quadratic space $(\mathbf{Q}^{\mathrm{N}}, q_{\mathrm{N}})$ into a non-degenerate quadratic space (W, q) over $\mathbf{Q}$ of dimension N, and h carries the class of c to the class of $\mathrm{Spin}(q)$. Hence, $\mathrm{G} = \mathrm{Spin}(q)$ for some (W, q). (Note that the $\mathbf{Q}^\times$-multiples of q need *not* arise via this twisting process, though such multiples give rise to the same spin group over $\mathbf{Q}$.)

The class $\xi \in \mathrm{H}^1(\mathbf{Q}, \mathrm{O}_\mathrm{N})$ of (W, q) is carried by

$$\mathrm{H}^1(\mathbf{Q}, \mathrm{O}_\mathrm{N}) \to \mathrm{H}^1(\mathbf{Q}, \mu_2) = \mathbf{Q}^\times/(\mathbf{Q}^\times)^2$$

to $\mathrm{disc}(q)/\mathrm{disc}(q_\mathrm{N})$ and is in the image of $\mathrm{H}^1(\mathbf{Q}, \mathrm{Spin}_\mathrm{N})$ by design, so it comes from $\mathrm{H}^1(\mathbf{Q}, \mathrm{SO}_\mathrm{N})$ and hence $\mathrm{disc}(q) = \mathrm{disc}(q_\mathrm{N})$ in $\mathbf{Q}^\times/(\mathbf{Q}^\times)^2$. Likewise, since

$$\delta : \mathrm{H}^1(\mathbf{Q}, \mathrm{SO}_\mathrm{N}) \to \mathrm{H}^2(\mathbf{Q}, \mu_2) = \mathrm{Br}(\mathbf{Q})[2]$$

kills the image of $\mathrm{H}^1(\mathbf{Q}, \mathrm{Spin}_\mathrm{N})$, the Hasse-Witt invariants for (W, q) at all places are trivial.

The only local invariant of (W, q) in the Hasse–Minkowski theorem that has not been uniquely determined is the signature (r, s). The $\mathbf{R}$-group $\mathrm{G}_\mathbf{R}$ determines (r, s) up to possibly swapping r and s: $\min(r, s)$ is the $\mathbf{R}$-rank of $\mathrm{G}_\mathbf{R} = \mathrm{Spin}(q_\mathbf{R})$ (as we may compute via the isogenous quotient $\mathrm{SO}(q_\mathbf{R})$), and $\max(r, s) = \mathrm{N} - \min(r, s)$.

The sign $(-1)^s$ of $\mathrm{disc}(q)$ is the same as that of $\mathrm{disc}(q_\mathrm{N})$, so the parity of s is uniquely determined. This eliminates any swapping ambiguity for odd $\mathrm{N} = r + s$ since r and s have opposite parity in such cases. Thus, for odd N the group $\mathrm{G}_\mathbf{R}$ determines the $\mathbf{Q}$-isomorphism class of (W, q) and hence of $\mathrm{G} = \mathrm{Spin}(q)$.

Suppose N is even, so the quadratic space $(\mathrm{W}, -q)$ has the same discriminant and the same local Hasse–Witt invariants as (W, q) since $(\mathbf{Q}^{2n}, q_{2n}) \simeq (\mathbf{Q}^{2n}, -q_{2n})$ (by negating the standard basis vectors e_j of $\mathbf{Q}^{2n}$ for j of a fixed parity). But $(\mathrm{W}, -q)$ realizes the swapped signature, so by the Hasse–Minkowski theorem the only possibilities for G realizing a given $\mathrm{G}_\mathbf{R}$ are $\mathrm{Spin}(q)$ and $\mathrm{Spin}(-q)$. These $\mathbf{Q}$-groups are isomorphic, so we are done. □

Remark 4.11. — For any integer $\mathrm{N} \geqslant 3$, the pure inner forms of Spin_N over $\mathbf{Z}$ are the $\mathbf{Z}$-groups $\mathrm{Spin}(q)$ for (fiberwise) non-degenerate quadratic lattices (M, q) with rank N. Indeed, by Remark 4.8 every such $\mathrm{Spin}(q)$ is a pure inner form of the Chevalley group Spin_N with the same $\overline{\mathbf{Q}}$-fiber, and conversely a twisting argument as done with the map h in the preceding proof shows that every pure inner form of Spin_N is given by $\mathrm{Spin}(q)$ for some (M, q). By similar reasoning, the $\mathbf{Z}$-groups $\mathrm{SO}(q)$ for such quadratic lattices (M, q) exhaust the set of isomorphism classes of semisimple $\mathbf{Z}$-groups with $\mathbf{Q}$-fiber a form of SO_N, for any $\mathrm{N} \geqslant 3$.

Proposition 4.4 shows that the $\mathbf{Z}$-group $\mathrm{SO}(q)$ determines the isomorphism class of (M, q) up to negating q, and we claim that the same holds for $\mathrm{Spin}(q)$. That is, if (M', q') is another such quadratic lattice of rank N with $\mathrm{Spin}(q') \simeq \mathrm{Spin}(q)$ over $\mathbf{Z}$ then necessarily $q' \simeq \pm q$. To prove this, it is sufficient that such an isomorphism between the spin groups over $\mathbf{Z}$ descends to an isomorphism between the special orthogonal group quotients.

Since $\mathrm{Spin}(q')$ and $\mathrm{Spin}(q)$ are separately étale-locally isomorphic to Spin_N in such a way that their special orthogonal group quotients are carried to the same quotient SO_{N}, it is sufficient that the kernel of the central isogeny $\mathrm{Spin}_{\mathrm{N}} \to \mathrm{SO}_{\mathrm{N}}$ is stable under $\mathrm{Aut}_{\mathrm{Spin}_{\mathrm{N}}/\mathbf{Z}}$, or equivalently is stable under the action of $\mathrm{Out}_{\mathrm{Spin}_{\mathrm{N}}/\mathbf{Z}}$. This outer automorphism group is the constant group associated to the diagram automorphisms, so case-checking of the B and D root systems shows that such stability holds except when $\mathrm{N} = 8$ (triality).

In the case $\mathrm{N} = 8$, the possible signatures over $\mathbf{R}$ are the indefinite (4,4) and the definite (8,0) and (0,8). The $\mathbf{R}$-rank of $\mathrm{Spin}(q)$ determines the signature up to negating q, so in the indefinite cases we are done because the signature determines the isomorphism class in such cases (as discussed in § 2; also see Theorem A.1). In the definite cases, the Minkowski–Siegel mass formula for positive-definite even unimodular lattices shows that the only examples in rank 8 are the quadratic spaces of discriminant ±1 arising from the even unimodular E_8 root lattice and its negative-definite analogue.

We now describe the groups $\mathrm{G}_{\mathbf{R}}$ for G as in Proposition 4.10 (also see [**G96**, Table 1.3]). First we treat the classical types. As explained in the proof of Lemma 4.9, for types A and C necessarily $\mathrm{G}_{\mathbf{R}}$ is split. For types B and D, the $\mathbf{R}$-groups that arise from absolutely simple and simply connected semisimple $\mathbf{Q}$-groups admitting a $\mathbf{Z}$-model are $\mathrm{Spin}(r, s)$ with $r - s \equiv \pm 1 \bmod 8$ for type B and $r - s \equiv 0 \bmod 8$ for type D. These congruences can be found in two ways. One way is by using Remark 4.11 and the determination of the signatures of non-degenerate quadratic spaces over $\mathbf{Z}$ as discussed in § 2. Another way is to describe $\mathrm{H}^1(\mathbf{R}, \mathrm{Spin}_n)$ using the methods of Serre and Borovoi and then compute the image of the map $\mathrm{H}^1(\mathbf{R}, \mathrm{Spin}_n) \to \mathrm{H}^1(\mathbf{R}, \mathrm{Aut}_{\mathrm{Spin}_n/\mathbf{R}})$.

Now we turn to the exceptional types. For G_2 one gets both real forms (of ranks 0, 2), and for F_4 one gets all three real forms (of ranks 0, 1, 4). For E_6 one gets precisely the real inner forms (of ranks 2, 6), and for E_7 one gets real forms of ranks 3, 7 but not those of ranks 0, 4. Finally, for E_8 one gets every real form (of ranks 0, 4, 8).

Remark 4.12. — The $\mathbf{R}$-forms described above are the $\mathbf{R}$-groups arising from absolutely simple and simply connected semisimple $\mathbf{Q}$-groups G that admit a (reductive) $\mathbf{Z}$-model. Such G may arise as the generic fiber of several semisimple $\mathbf{Z}$-groups that are pairwise non-isomorphic over $\mathbf{Z}$. For example, in types B and D this happens with definite quadratic lattices (M, q) that are non-degenerate over $\mathbf{Z}$, due to Proposition 4.4. We shall see additional examples in § 6 for type F_4 (and many for type E_8 in § 7 by more indirect means).

By Proposition 4.10, $\mathrm{H}^1(\mathbf{R}, \mathrm{G}_0)$ parameterizes the set of isomorphism classes of $\mathbf{Q}$-fibers of simply connected semisimple groups over $\mathbf{Z}$ with absolutely simple fibers. The proof ultimately rested on the triviality of the fundamental group $\pi_1(\mathrm{S})$ and the Brauer group $\mathrm{H}^2(\mathrm{S}, \mathbf{G}_m)$ for $\mathrm{S} = \mathrm{Spec}(\mathbf{Z})$. (The triviality of $\mathrm{Br}(\mathbf{Z})$ expresses the fact that a Brauer class for $\mathbf{Q}$ that is split at all finite places is globally split.) These groups need not be trivial for $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$ when A is the ring of integers in a general number field K, and that makes the description of the generic fibers of semisimple groups over such A much more involved when $\mathrm{K} \neq \mathbf{Q}$ (and it seems hopeless to give a general answer; in [**Ha**] the case of split generic fiber over Dedekind domains is studied).

5. Coxeter's integral octonions

To build non-split semisimple $\mathbf{Z}$-groups going beyond § 2, we shall use one remarkable structure: Coxeter's integral order $\mathscr{R}$ in Cayley's definite octonions, whose definition we review below (also see [**G96**, § 4] or [**EG97**, § 1]). The automorphism scheme of $\mathscr{R}$ will turn out to be the unique semisimple $\mathbf{Z}$-group of type G_2 that is $\mathbf{R}$-anisotropic. What is even more striking is that the order $\mathscr{R}$ can be used to construct $\mathbf{Z}$-models of absolutely simple non-split connected semisimple $\mathbf{Q}$-groups of other exceptional types; see § 6 below.

We refer the reader to Appendix B for a review of general background related to octonion algebras over rings, including a discussion of the *split* octonion algebra Λ_{R} over any (commutative) ring R and proofs that any automorphism of the underlying algebra of an octonion R-algebra respects the octonionic norm and conjugation (as is classical over fields) and that any octonion R-algebra is isomorphic to Λ_{R} étale-locally over $\mathrm{Spec}(\mathrm{R})$.

Cayley's definite octonion algebra was first described as a non-associative algebra with anti-involution over $\mathbf{R}$, but its multiplication table actually gives an algebra $\mathbf{O}$ over $\mathbf{Q}$. As a rational vector space of dimension 8, it has the form

$$\mathbf{O} = \mathbf{Q} \cdot 1 \oplus \mathbf{Q} \cdot e_1 \oplus \cdots \oplus \mathbf{Q} \cdot e_7$$

with the multiplication law determined by

$$e_i^2 = -1,$$

$$e_i \cdot e_{i+1} \cdot e_{i+3} = -1,$$

where in the last identity the subscript is calculated modulo 7 and the multiplication among the indicated ordered triples is associative. This gives seven copies of Hamilton's rational quaternion algebra inside $\mathbf{O}$. If three distinct elements e_i do not lie in one of these quaternion algebras, one finds that they anti-associate. For example,

$$(e_1 \cdot e_2) \cdot e_3 = -e_1 \cdot (e_2 \cdot e_3).$$

There is an algebra anti-involution $x \mapsto x^*$ of $\mathbf{O}$ called *conjugation* that is defined by $e_i^* = -e_i$, and the trace and norm

$$\mathrm{Tr}(a) = a + a^*, \ \ \mathrm{N}(a) = a \cdot a^* = a^* \cdot a$$

take values in $\mathbf{Q}$, with every $a \in \mathbf{O}$ satisfying $a^2 - \mathrm{Tr}(a) \cdot a + \mathrm{N}(a) = 0$. In particular, if $a \notin \mathbf{Q}$ then $\mathbf{Q}[a]$ is a quadratic field.

The norm $\mathrm{N} : \mathbf{O} \to \mathbf{Q}$ is a positive-definite quadratic form and $\mathrm{N}(aa') = \mathrm{N}(a)\mathrm{N}(a')$, so $\mathbf{O}$ is an octonion division algebra (see Definition B.4). Its associated bilinear form is

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

Although multiplication in $\mathbf{O}$ is not associative, it is trace-associative in the sense that $\mathrm{Tr}((x \cdot y) \cdot z) = \mathrm{Tr}(x \cdot (y \cdot z))$ for all $x, y, z \in \mathbf{O}$. This is a general property of octonion algebras (as reviewed in Appendix B).

Lemma 5.1. — *The automorphism scheme* $\mathrm{Aut}_{\mathbf{O}/\mathbf{Q}}$ *is connected semisimple of type* G_2 *over* $\mathbf{Q}$*. It is is* $\mathbf{R}$*-anisotropic and split over* $\mathbf{Q}_p$ *for all primes* p*.*

Proof. — The first assertion is a special case of Theorem B.14 (which is classical over fields), according to which the split property over $\mathbf{Q}_p$ is a consequence of the fact (explained in Example B.3) that $\mathbf{O}_{\mathbf{Q}_p}$ is a split octonion algebra for every p. Since the norm N is positive-definite and $\mathrm{Aut}_{\mathbf{O}/\mathbf{Q}}$ is a closed subgroup of the orthogonal group $\mathrm{O}(\mathbf{O}, \mathrm{N})$ over $\mathbf{Q}$, the $\mathbf{R}$-anisotropicity follows. □

Remark 5.2. — Up to isomorphism, the Cayley octonion algebra $\mathbf{O}$ is the *unique* non-split octonion algebra over $\mathbf{Q}$. By Corollary B.15 this amounts to showing that there is a unique non-split $\mathbf{Q}$-form of G_2. Since G_2 is its own automorphism scheme, we have to show that $\mathrm{H}^1(\mathbf{Q}, \mathrm{G}_2)$ has two elements. By the Hasse principle for simply connected semisimple groups as we discussed after Remark 4.8, $\mathrm{H}^1(\mathbf{Q}, \mathrm{G}_2) \to \mathrm{H}^1(\mathbf{R}, \mathrm{G}_2)$ is bijective. Over any field, a non-split form of G_2 is anisotropic [**Spr**, 17.4.2]. Thus, the uniqueness of the $\mathbf{R}$-anisotropic form of any connected semisimple $\mathbf{R}$-group completes the proof.

An *order* in $\mathbf{O}$ is a $\mathbf{Z}$-lattice containing 1 and stable under multiplication. It is automatically stable under the conjugation. Indeed, obviously $\mathbf{Q}$ meets any order in $\mathbf{Z}$, and if $a \in \mathbf{O}$ is in an order but not in $\mathbf{Q}$ then $\mathbf{Z}[a]$ is an order in the quadratic field $\mathbf{Q}[a]$, so $x^2 - \mathrm{Tr}(a)x + \mathrm{N}(a)$ must be the minimal polynomial of a over $\mathbf{Q}$, forcing $\mathrm{Tr}(a) \in \mathbf{Z}$, so the conjugate $a^* = \mathrm{Tr}(a) - a$ also lies in the order. In particular, the trace and norm are $\mathbf{Z}$-valued on any order in $\mathbf{O}$. By Proposition B.9, every order in $\mathbf{O}$ is contained in a maximal one.

By Corollary B.12, the maximal orders in $\mathbf{O}$ are precisely the orders that are octonion $\mathbf{Z}$-algebras when equipped with the restriction of the norm (so the norm defines a structure of unimodular lattice). Hence, by Theorem B.14, the automorphism scheme of a maximal order in $\mathbf{O}$ is a semisimple $\mathbf{Z}$-group of type G_2. Thus, to make an explicit semisimple $\mathbf{Z}$-group with $\mathbf{Q}$-fiber $\mathrm{G} := \mathrm{Aut}_{\mathbf{O}/\mathbf{Q}}$, we will use a specific maximal order $\mathscr{R}$ in $\mathbf{O}$.

The obvious order

$$\mathscr{S} = \mathbf{Z} \cdot 1 + \mathbf{Z} \cdot e_1 + \cdots + \mathbf{Z} \cdot e_7$$

is maximal at all primes except $p = 2$; equivalently, the trace pairing $\mathrm{Tr}(xy^*) = \langle x, y\rangle$ on $\mathscr{S}$ has discriminant that is a power of 2. Indeed, defining $e_0 = 1$, the elements e_i are pairwise orthogonal and satisfy $\langle e_i, e_i\rangle = 2$, so the discriminant of the quadratic lattice $\mathscr{S}$ is 2^8.

We obtain a maximal order $\mathscr{R}$ containing $\mathscr{S}$ by choosing an index $i \bmod 7$ and adjoining the Hurwitz elements in the three evident copies of Hamilton's rational quaternions which contain e_i. For example, if $i = 1$, we adjoin to $\mathscr{S}$ the three elements

$$h_1 = (1 + e_1 + e_2 + e_4)/2$$

$$h_2 = (1 + e_1 + e_3 + e_7)/2$$

$$h_3 = (1 + e_1 + e_5 + e_6)/2$$

as well as products among these. This defines an order $\mathscr{R}$ containing $\mathscr{S}$ with $\mathscr{R}/\mathscr{S} \simeq (\mathbf{Z}/2\mathbf{Z})^4$. An additional additive generator is

$$h_4 = (e_1 + e_2 + e_3 + e_5)/2$$

(i.e., $\mathscr{R}$ is spanned over $\mathbf{Z}$ by $\mathscr{S}$ and $h_1, \dots, h_4$). This is Coxeter's $\mathbf{Z}$-order. For future reference, we note that the element

$$\alpha = (1 + e_1 + e_2 + \cdots + e_7)/2 = h_1 + h_2 + h_3 - (1 + e_1) \tag{5.1}$$

lies in $\mathscr{R}$. (It satisfies the quadratic equation $\alpha^2 - \alpha + 2 = 0$.)

The positive-definite quadratic form $\mathrm{N} : \mathbf{O} \to \mathbf{Q}$ restricts to a quadratic form $q : \mathscr{R} \to \mathbf{Z}$ whose associated symmetric bilinear form is the restriction to $\mathscr{R}$ of $\langle x, y\rangle = \mathrm{Tr}(xy^*)$. In particular, $q(x) = \langle x, x\rangle/2$ for all $x \in \mathscr{R}$. Since the discriminant of the quadratic lattice $\mathscr{S}$ is equal to 2^8 and the index of $\mathscr{S}$ in $\mathscr{R}$ is 2^4, it follows that the trace pairing is unimodular on $\mathscr{R}$, so $(\mathscr{R}, q)$ is non-degenerate over $\mathbf{Z}$.

By unimodularity, $\mathscr{R}$ is an octonion algebra over $\mathbf{Z}$ with respect to the restriction q of the norm on $\mathbf{O}$, and it is maximal as a $\mathbf{Z}$-order in $\mathbf{O}$. Thus, by Theorem B.14, the automorphism scheme $\mathscr{G} = \mathrm{Aut}_{\mathscr{R}/\mathbf{Z}}$ with $\mathbf{R}$-anisotropic $\mathbf{Q}$-fiber $\mathrm{G} = \mathrm{Aut}_{\mathbf{O}/\mathbf{Q}}$ of type G_2 is a semisimple $\mathbf{Z}$-group (of type G_2). In Example 7.2 we will establish an integral version of Remark 5.2: up to isomorphism, $\mathscr{R}$ is the unique non-split octonion algebra over $\mathbf{Z}$.

Remark 5.3. — Since $(\mathscr{R}, q)$ is a positive-definite non-degenerate quadratic space over $\mathbf{Z}$ with rank 8, it must be the E_8 root lattice. Likewise, the $\mathbf{Z}$-submodule $\mathscr{R}_0$ of elements of trace zero is a positive-definite quadratic lattice that is non-degenerate over $\mathbf{Z}$, so it is isomorphic to the E_7 root lattice.

Multiplication in $\mathscr{R}$ is trace-associative, so we can define a trilinear form $\mathscr{R}^3 \to \mathbf{Z}$ by

$$(x, y, z) \mapsto \mathrm{Tr}(x \cdot (y \cdot z)) = \mathrm{Tr}((x \cdot y) \cdot z). \tag{5.2}$$

This 3-form is alternating on the sublattice $\mathscr{R}_0$, so it induces a map $\wedge^3 \mathscr{R}_0 \to \mathbf{Z}$.

For our work with other exceptional types, it is convenient to relate the Coxeter order $\mathscr{R}$ in the definite octonion algebra $\mathbf{O}$ over $\mathbf{Q}$ and the standard split octonion algebra Λ over $\mathbf{Z}$ that is a maximal order in the split octonion algebra over $\mathbf{Q}$ (as discussed in Appendix B):

Proposition 5.4. — *For every prime p, $\mathscr{R}_{\mathbf{Z}_p} \simeq \Lambda_{\mathbf{Z}_p}$ as octonion algebras over $\mathbf{Z}_p$.*

Proof. — By Example B.3, $\mathscr{R}_{\mathbf{Q}_p}$ is split as an octonion algebra over $\mathbf{Q}_p$. By Proposition B.11, every maximal order in a split octonion algebra over the fraction field of a discrete valuation ring is a split octonion algebra over the valuation ring. Hence, $\mathscr{R}_{\mathbf{Z}_p} \simeq \Lambda_{\mathbf{Z}_p}$. □

6. The construction of some non-split examples

The following result is derived in [**G96**, Prop. 1.2] from work of Tits [**T2**], and we shall explain how it is a consequence of Lemma 4.7.

Proposition 6.1. — *If G is the $\mathbf{Q}$-fiber of a semisimple $\mathbf{Z}$-group then every finite-dimensional representation of $\mathrm{G}_{\overline{\mathbf{Q}}}$ descends to a representation V of G over $\mathbf{Q}$. Moreover, if V' is another $\mathbf{Q}$-descent of the same representation over $\overline{\mathbf{Q}}$ then $\mathrm{V}' \simeq \mathrm{V}$ as G-representations over $\mathbf{Q}$.*

If $\mathrm{V}_{\overline{\mathbf{Q}}}$ is irreducible and admits an invariant non-degenerate quadratic form then V admits a G-invariant non-degenerate quadratic form, unique up to $\mathbf{Q}^\times$-scaling.

Proof. — We can pass to the simply connected cover of G so that G is simply connected, and for the existence aspect we may focus our attention on the descent of irreducible representations since any finite-dimensional representation of a connected semisimple group over a field of characteristic 0 is completely reducible (as we see via semisimplicity of its Lie algebra).

Let us prove uniqueness of the $\mathbf{Q}$-descent up to isomorphism. The set $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}, \mathrm{V}')$ of G-equivariant linear homomorphisms is a finite-dimensional $\mathbf{Q}$-vector space, and its formation commutes with any extension of the ground field. Viewing it as an affine space over $\mathbf{Q}$, the locus of isomorphisms is Zariski-open. This open locus contains a $\overline{\mathbf{Q}}$-point (i.e., $\mathrm{V}_{\overline{\mathbf{Q}}} \simeq \mathrm{V}'_{\overline{\mathbf{Q}}}$), so it is non-empty and hence contains a $\mathbf{Q}$-point. This establishes the desired uniqueness.

Likewise, a non-degenerate invariant quadratic form is equivalent to a symmetric equivariant isomorphism to the dual, so in the absolutely irreducible case Schur's Lemma provides the $\mathbf{Q}$-descent for an invariant non-degenerate quadratic form (upon finding a $\mathbf{Q}$-descent for the representation) and ensures its uniqueness up to $\mathbf{Q}^\times$-scaling.

Let G_0 be the split $\mathbf{Q}$-form of G. The construction of highest-weight representations works for split semisimple Lie algebras over any field of characteristic 0, so also for split simply connected semisimple groups over any field of characteristic 0. Thus, any finite-dimensional irreducible representation ρ of $(\mathrm{G}_0)_{\overline{\mathbf{Q}}} = \mathrm{G}_{\overline{\mathbf{Q}}}$ over $\overline{\mathbf{Q}}$ descends to a representation $\rho_0 : \mathrm{G}_0 \to \mathrm{GL}(\mathrm{V}_0)$ over $\mathbf{Q}$.

By Lemma 4.7, there is a 1-cocycle $c : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{G}_0(\overline{\mathbf{Q}})$ that twists G_0 into G. Composition of c with ρ_0 defines a modified Galois descent datum on the $\overline{\mathbf{Q}}$-vector space $(\mathrm{V}_0)_{\overline{\mathbf{Q}}}$. Such a descent datum arises from a $\mathbf{Q}$-structure V on $(\mathrm{V}_0)_{\overline{\mathbf{Q}}}$, so ρ descends to a representation $\mathrm{G} \to \mathrm{GL}(\mathrm{V})$ over $\mathbf{Q}$. □

The fact that all representations (V, ρ) of G over $\overline{\mathbf{Q}}$ descend to $\mathbf{Q}$ suggests a method to construct semisimple integral models of G (generally not $\mathbf{Q}$-split, or equivalently not $\mathbf{R}$-split): for a faithful ρ any lattice M in V defines a $\mathbf{Z}$-model GL(M) of GL(V), and the Zariski closure of G in GL(M) is a $\mathbf{Z}$-flat affine finite type $\mathbf{Z}$-group with $\mathbf{Q}$-fiber G. We can try to prove that this $\mathbf{Z}$-group is semisimple (in particular, $\mathbf{Z}$-smooth with connected fibers).

Example 6.2. — For Cayley's 8-dimensional $\mathbf{Q}$-algebra $\mathbf{O}$ of definite octonions, the automorphism scheme $\mathrm{G} = \mathrm{Aut}_{\mathbf{O}/\mathbf{Q}}$ is an $\mathbf{R}$-anisotropic connected semisimple $\mathbf{Q}$-group of type G_2 equipped with a faithful representation $\mathrm{G} \hookrightarrow \mathrm{GL}(\mathbf{O})$.

Let $\mathscr{R}$ be Coxeter's integral octonions, a lattice in $\mathbf{O}$ that is a maximal order. By Theorem B.14, the automorphism scheme $\mathscr{G} = \mathrm{Aut}_{\mathscr{R}/\mathbf{Z}}$ is a semisimple $\mathbf{Z}$-group of type G_2, and its generic fiber is G. By construction, the $\mathbf{Z}$-flat $\mathscr{G}$ is a closed subscheme of $\mathrm{GL}(\mathscr{R})$. Thus, $\mathscr{G}$ is the Zariski closure of G in $\mathrm{GL}(\mathscr{R})$ via the faithful representation of G on $\mathbf{O} = \mathscr{R}_{\mathbf{Q}}$.

It is hard to analyze Zariski closures, so we will usually build $\mathbf{Z}$-models by a procedure that yields a closed subgroup scheme of GL(M) having the correct $\mathbf{Q}$-fiber but not *a priori* $\mathbf{Z}$-flat. This often turns out to be the Zariski closure, as follows.

We will find faithful representations $\mathrm{G} \to \mathrm{GL}(\mathrm{V})$ over $\mathbf{Q}$ such that the subgroup G of GL(V) is defined by the preservation of some low-degree elements in the tensor algebra on V and its dual. Some examples of this situation are the standard representations of the classical groups (using determinants, symplectic forms, and quadratic forms) and the minuscule representations of the exceptional groups (cf. [**DGr**]). If these tensors can be defined integrally on M and are suitably non-degenerate on $\mathrm{M}/p\mathrm{M}$ for all primes p then it is reasonable to try to prove that the closed **Z**-subgroup scheme $\mathscr{G}$ of automorphisms of M preserving these integral tensors is a semisimple **Z**-group (in which case by **Z**-flatness $\mathscr{G}$ must coincide with the Zariski closure in GL(M) of $\mathscr{G}_{\mathbf{Q}} = \mathrm{G} \subset \mathrm{GL}(\mathrm{V})$).

The case of G_2 has already been addressed in Example 6.2. To construct non-split simply connected semisimple **Z**-groups of types E_6 and F_4 in this way, we will use a lattice M in a representation V of dimension 27 and the associated lattice End(M) of rank $27^2 = 729$. Verifying that **Z**-groups built in this way are smooth with connected reductive fibers is a local problem, so Proposition 5.4 will reduce the problem to computations with the split octonion algebra Λ over **Z** rather than with $\mathscr{R}$. (See [**GS**, (3.17) in § 2.3] for the use of E_6-constructions with the Coxeter order $\mathscr{R}$ to build the non-split semisimple **Z**-group of type E_7 via a 56-dimensional representation. The case of E_8 is discussed in [**G96**, § 6] using a 248-dimensional representation.)

We first treat the case of the unique non-split simply connected **Q**-group of type E_6 that admits a **Z**-model; this has **R**-rank equal to 2 (see [**G96**, Table 1.3]). The construction rests on the notion of an *Albert algebra*, so let us recall the definition.

For a field k with characteristic $\neq 2, 3$, consider a commutative but not necessarily associative k-algebra C with multiplication $\circ$ having a 2-sided identity e. We say that C is a J-*algebra* if it is equipped with a non-degenerate quadratic form $q : \mathrm{C} \to k$ satisfying three properties: $q(e) = 3/2$, $q(x \circ x) = q(x)^2$ when $\mathrm{B}_q(x, e) = 0$, and $\mathrm{B}_q(x \circ y, z) = \mathrm{B}_q(x, y \circ z)$ for all $x, y, z \in \mathrm{C}$. Such a triple $(\mathrm{C}, \circ, q)$ is called *reduced* if it contains a nontrivial idempotent (i.e., there exists $x \in \mathrm{C} - \{0, e\}$ satisfying $x \circ x = x$). The quadratic form q on C gives rise to a cubic form $\det \in \mathrm{Sym}^3(\mathrm{C}^*)$ via inspection of the constant term of an analogue of the Cayley–Hamilton theorem [**SV**, Prop. 5.1.5]. An explicit formula for this cubic form is

$$\det(x) = \mathrm{B}_q(x \circ x, x)/3 - q(x)\mathrm{B}_q(x, e) + \mathrm{B}_q(x, e)^3/6. \tag{6.1}$$

Informally, reduced J-algebras fall into two classes: those that can be constructed in a simple way from finite-dimensional non-degenerate quadratic spaces over k, and those that are built using 3 × 3 matrices over composition algebras over k. (See [**SV**, Thm. 5.4.5].) Members of the latter class can have dimension 6, 9, 15, or 27, and are precisely the reduced J-algebras for which the cubic form det is absolutely irreducible over k [**SV**, Cor. 5.4.6].

The 27-dimensional examples of this type arise from octonion algebras over k and are called *Albert algebras* (or *exceptional Jordan algebras*). We will focus on Albert algebras over **Q** and finite fields. The reason for our interest in Albert algebras is that automorphisms preserving their associated tensors give rise to simply connected groups of types E_6 and F_4 over fields with characteristic not 2 or 3.

Remark 6.3. — By [**SV**, 5.3.10], automorphisms of an Albert algebra (i.e., linear automorphisms of the underlying vector space preserving the multiplication) preserve the quadratic form q and hence also preserve the cubic form det. There is a converse: the algebra automorphisms are precisely the linear automorphisms that preserve the identity e and the cubic form [**SV**, 5.9.4].

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

$$\mathrm{A} = \begin{pmatrix} a & z & y^* \\ z^* & b & x \\ y & x^* & c \end{pmatrix} \tag{6.2}$$

(The Hermitian condition implies that $a, b, c \in \mathbf{Q}$.) This has a commutative non-associative multiplication defined by $\mathrm{A} \circ \mathrm{A}' := (1/2)(\mathrm{AA}' + \mathrm{A}'\mathrm{A})$ (where AA' and $\mathrm{A}'\mathrm{A}$ denote the usual product of octonionic matrices), with 2-sided identity element e given by the standard matrix identity element. Equipping V with the non-degenerate quadratic form

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

this satisfies the axioms to be a J-algebra.

For diagonal $\mathrm{A}, \mathrm{A}' \in \mathrm{V}$, clearly $\mathrm{A} \circ \mathrm{A}'$ is the usual matrix product. Hence, V contains nontrivial idempotents, so it is a reduced J-algebra. It is in fact an Albert algebra, denoted $\mathrm{H}(\mathbf{O}; 1, 1, 1)$ in the notation of [**SV**, § 5.1], and by [**SV**, (5.11)] the cubic form is:

$$\det(\mathrm{A}) = abc + \mathrm{Tr}(xyz) - a \cdot \mathrm{N}(x) - b \cdot \mathrm{N}(y) - c \cdot \mathrm{N}(z). \tag{6.3}$$

Example 6.4. — For the space V of matrices as in (6.2), consider the $\mathbf{Q}$-group $\mathrm{G} := \mathrm{Aut}_{(\mathrm{V},\det)/\mathbf{Q}}$ of points of GL(V) preserving the cubic form det (but not necessarily the identity). This is a connected semisimple group that is simply connected of type E_6, by [**SV**, 7.3.2]. The same holds for any Albert algebra over any field of characteristic $\neq 2, 3$ in place of (V, Q) over $\mathbf{Q}$.

We claim that $\mathrm{G}_{\mathbf{R}}$ is not split. Note that $\mathrm{H} := \mathrm{Aut}_{\mathbf{O}/\mathbf{Q}}$ is a $\mathbf{Q}$-subgroup of G via

$$(a, b, c, x, y, z) \mapsto (a, b, c, h(x), h(y), h(z))$$

for $h \in \mathrm{H}$, and $\mathrm{H}_{\mathbf{R}}$ is the anisotropic $\mathbf{R}$-form of G_2. The maximal compact subgroups of the group of $\mathbf{R}$-points of a split $\mathbf{R}$-group of type E_6 is of type C_4 [**Kn**, C.4]. Thus, if $\mathrm{G}_{\mathbf{R}}$ is split then the connected compact subgroup $\mathrm{H}(\mathbf{R})$ of type G_2 is contained in a maximal connected compact group of type C_4. In view of the categorical equivalence between the categories of connected compact Lie groups and $\mathbf{R}$-anisotropic connected reductive $\mathbf{R}$-groups, to show that $\mathrm{G}_{\mathbf{R}}$ is not split it suffices to show that the anisotropic $\mathbf{R}$-form of G_2 has no nontrivial $\mathbf{R}$-homomorphism to the anisotropic $\mathbf{R}$-form of $\mathrm{Sp}_8^{\mathrm{ad}}$. Hence, it suffices to show that there is no nontrivial $\mathbf{C}$-homomorphism from G_2 to $\mathrm{Sp}_8^{\mathrm{ad}}$.

Such a map lifts to a nontrivial homomorphism from the simply connected G_2 into the simply connected central cover Sp_8. But over $\mathbf{C}$ there is only one nontrivial 8-dimensional representation of G_2, and it has no invariant symplectic form. Hence, $\mathrm{G}_{\mathbf{R}}$ is not split.

To extend the $\mathbf{Q}$-group G in Example 6.4 to a semisimple $\mathbf{Z}$-group, we introduce an integral structure on V relative to which the cubic form is integral. Let $\mathrm{M} \subset \mathrm{V}$ be the lattice of matrices A as in (6.2) for which $a, b, c \in \mathbf{Z}$ and $x, y, z \in \mathscr{R}$. In an evident manner, $\mathrm{M}_{\mathbf{Z}[1/6]}$ equipped with the quadratic form $\mathrm{Q}|_{\mathrm{M}}$ over $\mathbf{Z}[1/6]$ is an "Albert algebra over $\mathbf{Z}[1/6]$" for which the associated cubic form arises from the integral cubic form $\det : \mathrm{M} \to \mathbf{Z}$ obtained by the restriction of $\det : \mathrm{V} \to \mathbf{Q}$. Let

$$\mathscr{G} = \mathrm{Aut}_{(\mathrm{M},\det)/\mathbf{Z}} \tag{6.4}$$

be the closed $\mathbf{Z}$-subgroup of GL(M) defined by preservation of the cubic form. This is an affine finite type $\mathbf{Z}$-group with $\mathbf{Q}$-fiber G.

Proposition 6.5. — *The* $\mathbf{Z}$*-group* $\mathscr{G}$ *is semisimple* (*so* $\mathbf{Z}$*-smooth with connected semisimple fibers*) *and simply connected of type* E_6.

Proof. — Since the $\mathbf{Q}$-fiber is known to be a connected semisimple $\mathbf{Q}$-group that is simply connected of type E_6, by the $\mathbf{Z}$-flatness criterion in Lemma B.13 it suffices to show that $\mathscr{G}_{\mathbf{F}_p}$ is connected reductive for every prime p. For $p \neq 2, 3$, $\mathrm{M}/p\mathrm{M}$ equipped with the quadratic form $\mathrm{Q}_{\mathbf{F}_p}$ is an Albert algebra whose cubic form is $\det_{\mathbf{F}_p}$. Thus, by [**SV**, 7.3.2], if $p \neq 2, 3$ then $\mathscr{G}_{\mathbf{F}_p} = \mathrm{Aut}_{(\mathrm{M}/p\mathrm{M},\det_{\mathbf{F}_p})/\mathbf{F}_p}$ is connected semisimple and simply connected of type E_6 (smoothness is shown in step (e) of the proof of [**SV**, 7.3.2]). It follows that $\mathscr{G}_{\mathbf{Z}[1/6]}$ is a simply connected semisimple $\mathbf{Z}[1/6]$-group of type E_6.

The theory of Albert algebras is delicate in characteristics 2 and 3, so we now give an alternative approach that applies to all primes on an equal footing. Since $\mathscr{R}_{\mathbf{Z}_p} \simeq \Lambda_{\mathbf{Z}_p}$ as octonion algebras for all p (Proposition 5.4), our problem over $\mathbf{Z}$ is equivalent to one in which the split octonion algebra Λ replace the role of $\mathscr{R}$. To be precise, we define a lattice M_0 of 3×3 Hermitian matrices over Λ similarly to M over $\mathscr{R}$, and we equip M_0 with the integral cubic form δ that is defined similarly to the formula in (6.3), using the trace and norm on Λ. The $\mathbf{Z}$-group scheme

$$\mathscr{G}_0 = \mathrm{Aut}_{(\mathrm{M}_0,\delta)/\mathbf{Z}} \tag{6.5}$$

becomes isomorphic to $\mathscr{G}$ over $\mathbf{Z}_p$ for every p, so our task is equivalent to the assertion that $\mathscr{G}_0$ is reductive over $\mathbf{Z}$ (necessarily simply connected and semisimple of type E_6, in view of our knowledge of the geometric fiber in characteristic 0). We will prove that $\mathscr{G}_0$ is the simply connected Chevalley group of type E_6.

The data $(\mathrm{M}_0, \delta, e)$ that underlies the definition of $\mathscr{G}_0$ is a pointed finite free module of rank 27 equipped with a cubic form. This is the *Freudenthal model* for exceptional Jordan algebras. We will work with the *Tits model*: the triple $(\underline{\mathrm{M}}_0, \underline{\delta}, \underline{e})$ where $\underline{\mathrm{M}}_0 := \mathrm{Mat}_3(\mathbf{Z})^{\oplus 3}$,

$$\underline{\delta}(u, v, w) := \det(u) + \det(v) + \det(w) - \mathrm{Tr}(uvw) \tag{6.6}$$

for $u, v, w \in \mathrm{Mat}_3$, and $\underline{e} := (1, 0, 0)$. A $\mathbf{Z}$-linear isomorphism $\mathrm{M}_0 \simeq \underline{\mathrm{M}}_0$ carrying (δ, e) to $(\underline{\delta}, \underline{e})$ is given in [**GY05**, § 2], so $\mathscr{G}_0$ is thereby identified with the closed $\mathbf{Z}$-subgroup of $\underline{\mathscr{G}}_0 \subset \mathrm{GL}(\underline{\mathrm{M}}_0) = \mathrm{GL}_{27}$ defined by preservation of $\underline{\delta}$. (This closed $\mathbf{Z}$-subgroup is denoted $\underline{\mathrm{H}}$ in [**GY05**, § 3].) The proof that the affine finite type $\mathbf{Z}$-group $\underline{\mathscr{G}}_0$ is semisimple is technical, so we refer the reader to Appendix C for the details (where a maximal $\mathbf{Z}$-torus is also given). □

A refinement of the preceding construction will yield groups of type F_4. The motivation comes from the theory of Albert algebras: over any field not of characteristic 2 or 3, the automorphism scheme of an Albert algebra (i.e., the scheme classifying linear automorphisms that preserve the multiplicative structure, without any assumption concerning preservation of the quadratic form) is connected semisimple of type F_4 [**SV**, 7.2.1]. The smoothness of this automorphism scheme implies (by consideration of its field-valued points and Remark 6.3) that the automorphism scheme preserves the quadratic and cubic forms associated to the Albert algebra.

As a particular case, the automorphism scheme $\mathrm{Aut}_{(\mathrm{V},\circ)/\mathbf{Q}}$ of the multiplicative structure on the Albert algebra $(\mathrm{V}, \circ, \mathrm{Q})$ is a connected semisimple $\mathbf{Q}$-group of type F_4. To construct different forms of F_4 inside a common form of E_6, we will use varying Albert algebra structures $(\circ', \mathrm{Q}')$ on the same 27-dimensional vector space such that the associated cubic forms as in (6.1) coincide.

There is an alternative description of the $\mathbf{Q}$-group $\mathrm{Aut}_{(\mathrm{V},\circ)/\mathbf{Q}}$ that is more convenient for the construction of $\mathbf{Q}$-forms of F_4 admitting an integral model. The key point is that over any field of characteristic not 2 or 3, the automorphisms of the multiplicative structure of an Albert algebra coincide with the linear automorphisms of its underlying vector space that preserve both the cubic form *and* the identity element [**SV**, 5.9.4]. This leads us to consider the closed $\mathbf{Q}$-subgroup scheme $\mathrm{Aut}_{(\mathrm{V},\det,e)/\mathbf{Q}} \subset \mathrm{GL}(\mathrm{V})$ defined by preservation of the cubic form det and the identity e. This is the e-stabilizer under the action on $\{\det = 1\}$ by the group $\mathrm{G} := \mathrm{Aut}_{(\mathrm{V},\det)/\mathbf{Q}}$.

The closed subgroup schemes $\mathrm{Aut}_{(\mathrm{V},\det,e)/\mathbf{Q}}$ and $\mathrm{Aut}_{(\mathrm{V},\circ)/\mathbf{Q}}$ inside $\mathrm{GL}(\mathrm{V})$ are both smooth (due to being $\mathbf{Q}$-subgroups, so Cartier's theorem applies) and they have the same geometric points, so they coincide. In particular, $\mathrm{Aut}_{(\mathrm{V},\det,e)/\mathbf{Q}}$ is connected semisimple of type F_4. The triple $(\mathrm{V}, \det, e)$ has a natural integral structure $(\mathrm{M}, \det, e)$, whereas the Albert algebra structure $(\circ, \mathrm{Q})$ is harder to work with integrally beyond $\mathbf{Z}[1/6]$.

We will be interested in studying the automorphism scheme of $(\mathrm{M}, \det, e)$, as well as of $(\mathrm{M}, \det, \mathrm{E})$ for any $\mathrm{E} \in \mathrm{M}$ satisfying $\det(\mathrm{M}) = 1$. To explain the motivation for introducing varying E, we recall that there is a general construction (described in [**SV**, 5.9.2]) which takes as input an Albert algebra and an arbitrary element e' of the underlying vector space at which the cubic form has value 1 and produces a new quadratic form $q_{e'}$ and a new multiplication law $\circ_{e'}$ constituting a new Albert algebra structure on the same underlying vector space such that the identity element for $\circ_{e'}$ is e' and the cubic form built from $q_{e'}$ and $\circ_{e'}$ as in (6.1) coincides with the initial one. Hence, for any $e' \in \mathrm{V}$ satisfying $\det(e') = 1$, the e'-stabilizer $\mathrm{Aut}_{(\mathrm{V},\det,e')/\mathbf{Q}} \subset \mathrm{GL}(\mathrm{V})$ equals $\mathrm{Aut}_{(\mathrm{V},\circ_{e'})/\mathbf{Q}}$ and hence is also a $\mathbf{Q}$-form of F_4.

The $\mathbf{Z}$-group scheme $\mathscr{G} := \mathrm{Aut}_{(\mathrm{M},\det)/\mathbf{Z}}$ is a (semisimple) $\mathbf{Z}$-model of G by Proposition 6.5, and non-split semisimple $\mathbf{Z}$-groups of type F_4 will be constructed as stabilizer schemes

$$\mathscr{H}_{\mathrm{E}} := \mathrm{Aut}_{(\mathrm{M},\det,\mathrm{E})/\mathbf{Z}} = \mathrm{Stab}_{\mathscr{G}}(\mathrm{E}) \subset \mathscr{G} \subset \mathrm{GL}(\mathrm{M})$$

for varying $\mathrm{E} \in \mathrm{M}$ such that $\det(\mathrm{E}) = 1$. Informally, $\mathscr{H}_{\mathrm{E}}$ is the automorphism scheme of an Albert algebra structure on M with identity E, but we have not defined a notion of Albert algebra when 6 is not a unit in the base ring. (See [**GY05**, § 2–§ 3] for a discussion of quadratic Jordan algebras over **Z**.)

Proposition 6.6. — *For* $\mathrm{E} \in \mathrm{M} \cap \{\det = 1\}$*, the* $\mathbf{Z}$*-group* $\mathscr{H}_{\mathrm{E}}$ *is semisimple of type* F_4.

Proof. — As in the proof of Proposition 6.5, it suffices to check that for all primes p, $(\mathscr{H}_{\mathrm{E}})_{\mathbf{F}_p}$ is connected reductive with dimension independent of p (namely, 52). Using the isomorphism $\mathscr{R}_{\mathbf{Z}_p} \simeq \Lambda_{\mathbf{Z}_p}$, we may reduce to working with $\Lambda_{\mathbf{Z}_p}$ in the role of $\mathscr{R}_{\mathbf{Z}_p}$ for some $\mathrm{E}_{0,p} \in (\mathrm{M}_0)_{\mathbf{Z}_p}$ that might not arise from M_0. By working over algebraically closed fields k of positive characterstic, our problem can be expressed in terms Λ_k, $(\mathrm{M}_0)_k$, and some $\mathrm{E}_{0,k} \in (\mathrm{M}_0)_k$ on which the cubic form δ has value equal to 1.

For $\mathscr{G}_0$ as in (6.5), the action of $\mathscr{G}_0(k)$ on the hypersurface $\{\delta = 1\} \subset (\mathrm{M}_0)_k$ is transitive. (Such transitivity is proved for $\mathscr{G}_0(\mathbf{Z})$ acting on the locus $\{\delta = 1\}$ inside M_0 as the main result in [**Kru**], and the proof via row and column operations carries over with **Z** replaced by any field.) Thus, as $\mathrm{E}_{0,k}$ varies inside $(\mathrm{M}_0)_k$ with $\delta(\mathrm{E}_{0,k}) = 1$, the stabilizer schemes $\mathscr{H}_{\mathrm{E}_{0,k}}$ are conjugate inside $(\mathscr{G}_0)_k$, so it suffices to work with $\mathrm{E}_{0,k}$ arising from a single choice of $\mathrm{E}_0 \in \mathrm{M}_0$ for which $\delta(\mathrm{E}_0) = 1$. We choose E_0 corresponding to the identity matrix.

Switching from the Freudenthal model to the Tits model (as in the proof of Proposition 6.5), we shall work with $\underline{\mathrm{E}}_0 = (1,0,0) \in \underline{\mathrm{M}}_0$ and its scheme-theoretic stabilizer

$$\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0} \subset \underline{\mathscr{G}}_0 \subset \mathrm{GL}(\underline{\mathrm{M}}_0).$$

The cotangent space at $\underline{\mathrm{E}}_0$ to the $\mathbf{Z}$-flat hypersurface $\{\underline{\delta} = 1\}$ in the affine space of $\underline{\mathrm{M}}_0$ is the quotient of $\underline{\mathrm{M}}_0^*$ modulo the span of an explicit $\mathbf{Z}$-linear form. By computation (see [**Yu**]), this is a saturated $\mathbf{Z}$-submodule, so the $\mathbf{Z}$-flat $\{\underline{\delta} = 1\}$ is $\mathbf{Z}$-smooth near $\underline{\mathrm{E}}_0$ and hence is $\mathbf{Z}$-smooth everywhere due to the fiberwise transitive action by $\underline{\mathscr{G}}_0$.

By computation (see [**Yu**]), the surjective $\underline{\mathrm{E}}_0$-orbit map $\underline{\mathscr{G}}_0 \to \{\underline{\delta} = 1\}$ between smooth $\mathbf{Z}$-schemes is surjective between tangent spaces over $\mathbf{Z}$ at the identity and $\underline{\mathrm{E}}_0$, so the stabilizer scheme $\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0}$ is $\mathbf{Z}$-smooth with relative dimension $78-26 = 52$. The generic fiber of $\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0}$ is connected semisimple (by the relation with automorphism schemes of Albert algebras, using $\Lambda_{\mathbf{Q}}$ in place of $\mathbf{O}$), so by [**Co2**, Prop. 3.1.12] the fibers of $\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0} \to \mathrm{Spec}(\mathbf{Z})$ are connected provided that their identity components are reductive. Hence, it suffices to show that $(\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0})^0_{\mathbf{F}_p}$ is reductive for all p (so unlike the arguments for type E_6 in Appendix C, for the F_4-cases we do not have to directly prove connectedness of fibers in positive characteristic).

As in [**GY05**, § 3], an explicit $\mathbf{Z}$-subgroup

$$(\mathrm{SL}_3)^2/\mu' \hookrightarrow \underline{\mathscr{H}}_{\underline{\mathrm{E}}_0} \subset \underline{\mathscr{G}}_0 \tag{6.7}$$

(with μ' the diagonally embedded μ_3) is defined by pre-composing the closed $\mathbf{Z}$-subgroup inclusion (C.1) with $(g_1, g_2) \mapsto (g_1, g_2, g_2)$. The image under (6.7) of the direct product of the diagonal tori in the SL_3's is a closed split $\mathbf{Z}$-subtorus $\underline{\mathscr{S}} \subset \underline{\mathscr{H}}_{\underline{\mathrm{E}}_0}$ of rank 4, so its $\mathbf{Q}$-fiber is a split maximal $\mathbf{Q}$-torus in $(\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0})_{\mathbf{Q}}$.

The geometric connectedness of the $\mathbf{Q}$-fiber of $\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0}$ implies that of the $\mathbf{F}_p$-fibers for all but finitely many p, so the union of the fibral identity components of $\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0}$ is an open $\mathbf{Z}$-subgroup scheme $\underline{\mathscr{H}}^0_{\underline{\mathrm{E}}_0}$; this is $\mathbf{Z}$-smooth but possibly not affine.

Let $\mathfrak{h} = \mathrm{Lie}(\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0}) = \mathrm{Lie}(\underline{\mathscr{H}}^0_{\underline{\mathrm{E}}_0})$, and let Ψ be the root system for $(\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0})_{\mathbf{Q}}$ with respect to $\underline{\mathscr{S}}_{\mathbf{Q}}$. Let I' be the union of the bases of the root systems for the SL_3's in (6.7) relative to their diagonal tori and upper unipotent subgroups. The set I' lies in a unique positive system of roots $\Psi^+ \subset \Psi$, and consists of the non-central vertices of the extended Dynkin diagram for the F_4 root system Ψ (with respect to Ψ^+). The central vertex of the extended diagram is the long simple positive root a_0 that is adjacent to a short simple positive root.

A computation (see [**Yu**]) shows that for $\mathbf{Z}$-basis elements $\mathrm{X}_\pm$ of $\mathfrak{h}_{\pm a_0} \subset \mathfrak{gl}(\underline{\mathrm{M}}_0)$,

$$[\mathrm{X}_+, \mathrm{X}_-] = \pm\mathrm{Lie}(a_0^\vee(\partial_t|_{t=1})),$$

an element of $\mathrm{Lie}(\underline{\mathscr{L}})$ that is part of a $\mathbf{Z}$-basis since no coroots are divisible in the dual of the root lattice for type F_4. Hence, $[\mathfrak{h}_{a_0}, \mathfrak{h}_{-a_0}]$ is a saturated $\mathbf{Z}$-line in $\mathfrak{h}$, so we can argue as in the proof of Theorem C.2 (especially applying Lemma C.1 to $(\underline{\mathscr{H}}^0_{\underline{\mathrm{E}}_0}, \underline{\mathscr{L}})$) to conclude that $(\underline{\mathscr{H}}_{\underline{\mathrm{E}}_0})^0_{\mathbf{F}_p}$ is semisimple of type F_4 for every p. □

Example 6.7. — Consider the semisimple $\mathbf{Z}$-groups $\mathscr{H}_{\mathrm{E}}$ of type F_4 for the following $\mathrm{E} \in \mathrm{M}$ satisfying $\det(\mathrm{E}) = 1$:

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & \alpha & -1 \\ \alpha^* & 2 & \alpha \\ -1 & \alpha^* & 2 \end{pmatrix}$$

where α is defined in (5.1) and $\alpha^2 - \alpha + 2 = 0$.

To determine the $\mathbf{R}$-rank for each of these, recall that the possible $\mathbf{R}$-ranks for type F_4 are 0, 1, and 4. Since $\mathscr{H}_{\mathrm{E}}$ is contained in the $\mathbf{Z}$-group $\mathscr{G}$ in (6.4) whose $\mathbf{Q}$-fiber G has $\mathbf{R}$-rank 2, the $\mathbf{R}$-rank of $\mathscr{H}_{\mathrm{E}}$ is either 0 or 1. The case of rank 0 (i.e., compact group of $\mathbf{R}$-points) occurs precisely when E is in the cone of matrices that are *positive-definite* (in the sense that diagonal entries are positive and 2×2 Hermitian minors obtained by removing the ith row and column for $i = 1, 2, 3$ have evident "determinant" in $\mathbf{R}$ that is positive).

Consequently, among the above three matrices, the stabilizer of the first gives a $\mathbf{Z}$-model for a $\mathbf{Q}$-form of F_4 with $\mathbf{R}$-rank 1 whereas the stabilizers of the other two are $\mathbf{R}$-anistotropic semisimple $\mathbf{Z}$-groups of type F_4. In particular, these latter two examples have isomorphic $\mathbf{Q}$-fibers. We will revisit these $\mathbf{R}$-anisotropic cases in Example 7.4.

7. Counting the integral models

Now we prove that the models of the simply connected groups of types G_2, F_4, and E_6 constructed in § 6 exhaust the possible non-split forms of these groups over $\mathbf{Z}$.

First consider the case of E_6, for which the only non-split simply connected $\mathbf{R}$-form that arises from a simply connected semisimple $\mathbf{Z}$-form is the one with $\mathbf{R}$-rank 2. This $\mathbf{R}$-form arises from the simply connected semisimple $\mathbf{Z}$-group $\mathscr{G}$ in (6.4), and we claim that $\mathscr{G}$ is the only such $\mathbf{Z}$-group, up to isomorphism. In view of the $\mathbf{R}$-isotropicity, such uniqueness over $\mathbf{Z}$ can be deduced from the theorem of strong approximation [**PR**, § 7.4, Thm. 7.12] by a simpler version of the arguments in Appendix A for indefinite spin groups. (The key input needed over $\mathbf{R}$ is that the simply connected $\mathbf{R}$-form G of E_6 with $\mathbf{R}$-rank 2 admits an automorphism not arising from $\mathrm{G}^{\mathrm{ad}}(\mathbf{R})$. This can be built using "conjugate-transpose" on matrices A as in (6.2).) The uniqueness in the non-split $\mathbf{R}$-isotropic F_4-case (with $\mathbf{R}$-rank 1) goes in exactly the same way, and is even easier since the outer automorphism group for F_4 is trivial (and similarly one sees that the non-split $\mathbf{R}$-isotropic cases E_7 and E_8 cases, which must have respective $\mathbf{R}$-ranks 3 and 4, are unique over $\mathbf{Z}$).

In the other cases, the only non-split $\mathbf{R}$-form that occurs is the $\mathbf{R}$-anisotropic one, for which there is a uniquely determined possibility for the generic fiber G over $\mathbf{Q}$ (see Proposition 4.10). The types that arise are listed in Table 1; for types B and D this uses that there exists a rank-n definite quadratic lattice that is non-degenerate over $\mathbf{Z}$ if and only if $n \equiv 0, \pm 1 \bmod 8$. The only types that arise for which $\mathrm{Out}_{\mathrm{G}/\mathbf{Q}} \neq 1$ are D_{4m}. Our task is to enumerate the semisimple $\mathbf{Z}$-groups with $\mathbf{Q}$-fiber isomorphic to a given G, and to do this we will use the mass formula

$$\sum \frac{1}{\#\mathscr{G}_i(\mathbf{Z})} = \prod \frac{1}{2}\zeta(1-d_j) \tag{7.1}$$

as stated in [**G96**, (5.1)].

Remark 7.1. — Let us explain the meaning of the terms on the two sides of (7.1). The sum on the left in (7.1) is taken over the elements of the finite set

$$\mathrm{G}(\mathbf{Q})\backslash\mathrm{G}(\mathbf{Q}\otimes_{\mathbf{Z}}\widehat{\mathbf{Z}})/\mathscr{G}(\widehat{\mathbf{Z}})$$

where $\mathscr{G}$ is a choice of $\mathbf{Z}$-model of G. A representative g_i of a double coset yields a $\mathbf{Z}$-model $\mathscr{G}_i$ with $\mathscr{G}_i(\mathbf{Z}) = \mathrm{G}(\mathbf{Q}) \cap g_i\mathscr{G}(\widehat{\mathbf{Z}})g_i^{-1}$ the corresponding finite group (see [**G99**, Prop. 1.4]).

If $\mathrm{Out}_{\mathrm{G}/\mathbf{Q}} = 1$ (i.e., G is not of type D_{4m}) then these integral models are pairwise non-isomorphic as $\mathbf{Z}$-groups and exhaust the set of semisimple $\mathbf{Z}$-groups with generic fiber isomorphic to G [**G99**, Prop. 2.1, 2.3]. For G of type D_{4m}, the collection remains exhaustive but there is a repetition of the isomorphism class of the $\mathbf{Z}$-group $\mathrm{Spin}(q)$ associated to the even unimodular lattice (M, q) of rank $8m$ precisely when $\mathrm{O}(q)(\mathbf{Z}) = \mathrm{SO}(q)(\mathbf{Z})$, in which case this isomorphism class occurs twice [**G99**, Prop. 2.5]. (The discussion of the left side of (7.1) in [**G96**] has some errors.)

The product on the right side of (7.1) is taken over the degrees d_j of the invariant polynomials for the Weyl group of a maximal torus in G acting on its reflection representation. For the $\mathbf{R}$-anisotropic absolutely simple semisimple $\mathbf{Q}$-groups admitting $\mathbf{Z}$-models, these degrees are given in Table 1. (For type D_{4m}, the final degree invariant is a repetition of $4m$.)

Note that these degrees are all even, so the values $\zeta(1-d_j)$ of the Riemann zeta function are non-zero rational numbers. Explicitly, $\zeta(1-2n) = (-1)^n|\mathrm{B}_n|/2n$, where B_{2n} is the $2n$th Bernoulli number. Since the sum of the degrees is divisible by 4 in all cases, the product of zeta values is a positive rational number.

Type	degrees
B_{4m-1}	$2, 4, 6, \ldots, 8m-2$
B_{4m}	$2, 4, 6, \ldots 8m$
D_{4m}	$2, 4, 6, \ldots, 8m-2, 4m$
G_2	$2, 6$
F_4	$2, 6, 8, 12$
E_8	$2, 8, 12, 14, 18, 20, 24, 30$

Table 1.

The degrees of the invariant polynomials appear due to their relationship to the orders of the finite groups $\mathscr{G}(\mathbf{F}_p)$. For all primes p, the $\mathbf{Z}_p$-split property for $\mathscr{G}_{\mathbf{Z}_p}$ implies that $\mathscr{G}_{\mathbf{F}_p}$ is a split connected semisimple $\mathbf{F}_p$-group that is simply connected and simple, so

$$\#\mathscr{G}(\mathbf{F}_p) = p^{\mathrm{N}} \prod (p^{d_j} - 1).$$

where N is the number of positive roots. For example, when $\mathscr{G} = \mathrm{Aut}_{\mathscr{R}/\mathbf{Z}}$ is the $\mathbf{R}$-anisotropic semisimple $\mathbf{Z}$-group of type G_2, we have

$$\#\mathscr{G}(\mathbf{F}_p) = p^6(p^6 - 1)(p^2 - 1).$$

Taking $p = 2$, we find that $\#\mathscr{G}(\mathbf{F}_2) = 2^6 3^3 7$.

Example 7.2. — For G_2 we have identified an $\mathbf{R}$-anisotropic $\mathbf{Z}$-model, the automorphism scheme $\mathscr{G} := \mathrm{Aut}_{\mathscr{R}/\mathbf{Z}}$ of Coxeter's order $\mathscr{R}$ in the octonions $\mathbf{O}$. We know that the finite group $\mathscr{G}(\mathbf{Z}) = \mathrm{Aut}(\mathscr{R})$ injects into $\mathscr{G}(\mathbf{F}_p)$ for all sufficiently large p (since $\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{F}_p)$ has torsion-free kernel for p sufficiently large, depending on n), so its order divides $\#\mathscr{G}(\mathbf{F}_p) = p^6(p^6-1)(p^2-1)$ for all sufficiently large p.

The gcd of these orders over all $p > m$ for any $m > 0$ is easily checked to be $2^6 3^3 7$. Hence, $\#\mathscr{G}(\mathbf{Z})$ divides $2^6 3^3 7 = 12096$, so

$$\frac{1}{\#\mathscr{G}(\mathbf{Z})} \leqslant \frac{1}{2}\zeta(-1) \times \frac{1}{2}\zeta(-5) = \frac{1}{2^6 3^3 7} \leqslant \frac{1}{\#\mathscr{G}(\mathbf{Z})},$$

forcing equality throughout. In particular, there is a single term in the mass formula, so $\mathscr{G}$ is the unique semisimple $\mathbf{Z}$-group of type G_2 that is $\mathbf{R}$-anisotropic. To be more precise, $\mathscr{G}$ is the unique non-Chevalley semisimple $\mathbf{Z}$-group of type G_2, since (by Proposition 1.3 and Remark 5.2) the $\mathbf{Q}$-fiber of any such $\mathbf{Z}$-group must be the $\mathbf{R}$-anisotropic $\mathbf{Q}$-group $\mathrm{Aut}_{\mathbf{O}/\mathbf{Q}}$. It follows from Corollary B.15 that $\mathscr{R}$ is the *unique* non-split octonion algebra over $\mathbf{Z}$.

The group $\mathscr{G}(\mathbf{Z}) = \mathrm{Aut}(\mathscr{R})$ is identified in [**ATLAS**, p. 14] as an extension of $\mathbf{Z}/2\mathbf{Z}$ by the simple commutator subgroup of $G_2(\mathbf{F}_2)$, where the $\mathbf{Z}/2\mathbf{Z}$ quotient is represented by a non-central element of order 2 in $\mathrm{Aut}(\mathscr{R})$. I do not know what methods were used to make this identification of finite groups;

by using it, the reduction map $f : \mathrm{Aut}(\mathscr{R}) = \mathscr{G}(\mathbf{Z}) \to \mathscr{G}(\mathbf{F}_2) = \mathrm{G}_2(\mathbf{F}_2)$ can be shown to be an isomorphism as follows.

The kernel of f is a normal subgroup whose order is a power of 2 (since the kernel of reduction $\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{F}_p)$ is pro-p), but the above description of $\mathrm{Aut}(\mathscr{R})$ in [**ATLAS**] implies that $\mathrm{Aut}(\mathscr{R})$ has no nontrivial normal 2-subgroup, so $\ker f = 1$. The description also implies that $\mathrm{Aut}(\mathscr{R})$ and $\mathrm{G}_2(\mathbf{F}_2)$ have the same size, since the commutator subgroup of $\mathrm{G}_2(\mathbf{F}_2)$ has index 2, so f is surjective as well.

Example 7.3. — Consider the simply connected semisimple $\mathbf{Z}$-group $\mathscr{G} := \mathrm{Spin}(\mathrm{E}_8)$ of type D_4. The order of the finite group $\mathscr{G}(\mathbf{Z})$ divides $\#\mathscr{G}(\mathbf{F}_p)$ for all sufficiently large primes p. The order of $\mathscr{G}(\mathbf{F}_p)$ is equal to

$$p^{12}(p^2-1)(p^4-1)^2(p^6-1)$$

for all primes p since the degrees of the invariants for the Weyl group are 2, 4, 4, and 6. The gcd of these sizes over all $p > m$ for any $m > 0$ is easily checked to be $2^{14}3^5 5^2 7$, so $\#\mathscr{G}(\mathbf{Z})$ divides $2^{14}3^5 5^2 7$.

But

$$\frac{1}{2}\zeta(-1) \times \frac{1}{2}\zeta(-3) \times \frac{1}{2}\zeta(-3) \times \frac{1}{2}\zeta(-5) = \frac{1}{2^{14}3^5 5^2 7},$$

so exactly as in the previous example we conclude that there is a single term in the mass formula, as we also saw in Remark 4.11 (using the classical mass formula for positive-definite even unimodular lattices). By Remark 7.1, it also follows that $\mathrm{O}(\mathrm{E}_8)(\mathbf{Z}) = \mathrm{SO}(\mathrm{E}_8)(\mathbf{Z})$.

The finite group $\mathscr{G}(\mathbf{Z})$ is identified in [**ATLAS**, p. 85] as a finite group of the form $2^2.\mathrm{O}_8^+(2)$. Here and below we use the notation of [**ATLAS**] for work with finite groups, so $\mathrm{O}_n^+(q)$ denotes the image of $\mathrm{Spin}_n(\mathbf{F}_q)$ in $\mathrm{SO}_n^{\mathrm{ad}}(\mathbf{F}_q)$ and H.J denotes an extension of the group J by the group H (with the extension structure of unknown nature).

Let (M, q) be the positive-definite quadratic space with $\mathrm{disc}(q) = 1$ for which $(\mathrm{M}, \mathrm{B}_q)$ is the even unimodular E_8 root lattice. The group $\mathscr{G}^* = \mathrm{O}(q)$ is an $\mathbf{R}$-anisotropic $\mathbf{Z}$-form of O_8. The finite group $\mathscr{G}^*(\mathbf{Z})$ coincides with $\mathrm{W}(\mathrm{E}_8)$ inside $\mathrm{GL}(\mathrm{M})$, and by [**Bou**, VI, Exer. 4.1] its quotient by $\langle -1 \rangle$ maps isomorphically onto the group $\mathrm{O}(q)(\mathbf{F}_2) = \mathrm{O}_8(\mathbf{F}_2)$ that is an extension of $\mathbf{Z}/2\mathbf{Z}$ by $\mathrm{O}_8^+(2)$, so it has the same order as $\mathscr{G}(\mathbf{Z})$.

Example 7.4. — The case of F_4 is more interesting. We consider the unique $\mathbf{Q}$-form G that is $\mathbf{R}$-anisotropic and admits a $\mathbf{Z}$-model. The invariants for the Weyl group have degrees 2, 6, 8 and 12 and we find the mass is equal to

$$\frac{1}{2}\zeta(-1) \times \frac{1}{2}\zeta(-5) \times \frac{1}{2}\zeta(-7) \times \frac{1}{2}\zeta(-11) = \frac{691}{2^{15}3^6 5^2 7^2 13}.$$

Since this is not the reciprocal of an integer, there must be more than one semisimple $\mathbf{Z}$-group with $\mathbf{Q}$-fiber isomorphic to G. By Proposition 6.6 and the remarks in Example 6.7, the Hermitian 3×3 determinant-1 matrices over $\mathscr{R}$ given by

$$\mathrm{I} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{E} = \begin{pmatrix} 2 & \alpha & -1 \\ \alpha^* & 2 & \alpha \\ -1 & \alpha^* & 2 \end{pmatrix}$$

yield respective simply connected semisimple **Z**-groups $\mathscr{H}_{\mathrm{I}}$ and $\mathscr{H}_{\mathbf{E}}$ of type F_4 as closed **Z**-subgroups of the unique non-split simply connected semisimple **Z**-group of type E_6 (given in (6.4)).

The integral points of these groups are identified on [**ATLAS**, pp. 85, 89] if one accepts that the group schemes $\mathscr{H}_{\mathrm{E}}$ as considered in Proposition 6.6 coincide with automorphism schemes for certain quadratic Jordan algebras over **Z**. Assuming that this identification is correct, we obtain isomorphisms $\mathscr{H}_{\mathrm{I}}(\mathbf{Z}) = 2^2.\mathrm{O}_8^+(2).\mathrm{S}_3$ and $\mathscr{H}_{\mathbf{E}}(\mathbf{Z}) = {}^3\mathrm{D}_4(2).3$ respectively. These two finite groups have orders $2^{15}3^65^27$ and $2^{12}3^57^213$ respectively. Since

$$\frac{691}{2^{15}3^65^27^213} = \frac{1}{2^{15}3^65^27} + \frac{1}{2^{12}3^57^213},$$

$\mathscr{H}_{\mathrm{I}}$ and $\mathscr{H}_{\mathbf{E}}$ are the *only* **R**-anisotropic semisimple **Z**-groups of type F_4 (granting that we have correctly identified the groups $\mathscr{H}_{\mathrm{I}}(\mathbf{Z})$ and $\mathscr{H}_{\mathbf{E}}(\mathbf{Z})$)! For more details on $\mathscr{H}_{\mathbf{E}}$ and its relation with the Leech lattice, see [**EG96**].

The mass for the integral models of G becomes large as the degrees of the invariant polynomials for the Weyl group increase. Indeed, for even d the rational number $\frac{1}{2}\zeta(1-d)$ is equal to $\zeta(d)(d-1)!/(2\pi i)^d$, which is approximately $(d-1)!/(2\pi i)^d$ when $d \geqslant 4$. For G of type E_8 the corresponding product of the values $\frac{1}{2}\zeta(1-d_j)$ is approximately 13934.49. Hence there are at least 13935 pairwise non-isomorphic **R**-anisotropic semisimple **Z**-groups of type E_8 that have **Q**-fiber equal to G (by Proposition 4.10). Inside the adjoint representation Lie(G) of G over **Q**, each **Z**-model $\mathscr{G}$ of G determines a positive-definite quadratic lattice $\mathrm{Lie}(\mathscr{G}) \subset \mathrm{Lie}(\mathrm{G})$ of rank 248 using the **Z**-valued quadratic form $q : \mathrm{X} \mapsto (-1/120)\mathrm{Tr}(\mathrm{ad}(\mathrm{X})^2)$, and this lattice is equipped with a $\mathscr{G}$-invariant alternating 3-form $\wedge^3(\mathrm{Lie}(\mathscr{G})) \to \mathbf{Z}$ defined by

$$\begin{aligned} \mathrm{X} \wedge \mathrm{Y} \wedge \mathrm{Z} \mapsto \mathrm{B}_q([\mathrm{X},\mathrm{Y}],\mathrm{Z}) &= (-1/60)\mathrm{Tr}(\mathrm{ad}([\mathrm{X},\mathrm{Y}])\mathrm{ad}(\mathrm{Z})) \\ &= (1/60)(\mathrm{Tr}(\mathrm{ad}(\mathrm{Y})\mathrm{ad}(\mathrm{X})\mathrm{ad}(\mathrm{Z})) \\ &\quad -\mathrm{Tr}(\mathrm{ad}(\mathrm{X})\mathrm{ad}(\mathrm{Y})\mathrm{ad}(\mathrm{Z}))). \end{aligned}$$

Probably most models $\mathscr{G}$ satisfy $\mathscr{G}(\mathbf{Z}) = 1$. If these groups generally are trivial then it would be interesting to determine the others. Some examples are constructed in [**G96**, § 6].

Appendix A
Indefinite quadratic lattices via group schemes

In this appendix, we use the cohomological formalism from § 3 to prove a classical fact in the theory of quadratic forms over $\mathbf{Z}$:

Theorem A.1. — *An indefinite quadratic lattice* (M, q) *non-degenerate over* $\mathbf{Z}$ *is determined up to isomorphism by its signature.*

The hypothesis of non-degeneracy over $\mathbf{Z}$, or equivalently $|\mathrm{disc}(q)| \in \{1, 2\}$, is essential. Setting aside the peculiar case of rank-2 quadratic lattices (M, q), for which $\mathrm{SO}(q)_{\mathbf{Q}}$ is a torus rather than semisimple, in the case of ternary quadratic lattices (i.e., rank 3) the size of the genus of (M, q) can be an arbitrarily large power of 2 in the indefinite case as $|\mathrm{disc}(q)|$ grows. See [**Ear**] for a discussion of this issue, as well as examples.

Proof. — The indefiniteness implies that the rank n is at least 2. For rank 2, necessarily $q \simeq q_2$. Indeed, (M, q) is a form of $(\mathbf{Z}^2, q_2)$ for the étale topology since O_2 is smooth, so the Isom-scheme $\mathrm{I} = \mathrm{Isom}(q_2, q)$ is a right torsor for the $\mathbf{Z}$-group scheme O_2 that is an extension of $\mathbf{Z}/2\mathbf{Z}$ by $\mathrm{SO}_2 = \mathbf{G}_{\mathrm{m}}$. Hence, it suffices to show that $\mathrm{H}^1(\mathbf{Z}, \mathrm{O}_2) = 1$, which in turn reduces to the vanishing of $\mathrm{H}^1(\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ and $\mathrm{H}^1(\mathbf{Z}, \mathbf{G}_{\mathrm{m}})$. The vanishing of $\mathrm{H}^1(\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ is a consequence of Proposition 3.9 because $\pi_1(\mathrm{Spec}(\mathbf{Z})) = 1$, and the vanishing of $\mathrm{H}^1(\mathbf{Z}, \mathbf{G}_{\mathrm{m}})$ expresses the fact that the Dedekind domain $\mathbf{Z}$ has trivial class group. Thus, we may and do focus on the case where $n \geqslant 3$, so $\mathrm{SO}(q)$ is a semisimple $\mathbf{Z}$-group scheme.

The signature determines the sign of the discriminant, and the parity of the rank determines if $|\mathrm{disc}(q)|$ equals 1 or 2 (using the non-degeneracy hypothesis over $\mathbf{Z}$). Hence, if (M', q') is another such quadratic lattice with the same signature then its discriminant coincides with that of (M, q). Consider the Isom-scheme $\mathrm{I} = \mathrm{Isom}(q, q')$ over $\mathbf{Z}$. This is an fppf right $\mathrm{O}(q)$-torsor over $\mathbf{Z}$.

Lemma A.2. — *The class of* I *in* $\mathrm{H}^1(\mathbf{Z}, \mathrm{O}(q))$ *arises from* $\mathrm{H}^1(\mathbf{Z}, \mathrm{SO}(q))$*.*

Proof. — If n is even then $\mathrm{O}(q)/\mathrm{SO}(q) = \mathbf{Z}/2\mathbf{Z}$, and $\mathrm{H}^1(\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) = 0$, so the case of even n is settled. Assume instead that n is odd, so $\mathrm{O}(q)/\mathrm{SO}(q) = \mu_2$. It suffices to show that the map $\mathrm{H}^1(\mathbf{Z}, \mathrm{O}(q)) \to \mathrm{H}^1(\mathbf{Z}, \mu_2)$ kills the class of I. By fppf Kummer theory (reviewed in the proof of Lemma A.4 below), $\mathrm{H}^1(\mathbf{Z}, \mu_2) = \mathbf{Z}^\times/(\mathbf{Z}^\times)^2$. The image in here of the class of I is $\mathrm{disc}(q)/\mathrm{disc}(q') = 1$. □

By Lemma A.2, there is an $\mathrm{SO}(q)$-torsor I' over $\mathbf{Z}$ whose class $[\mathrm{I}']$ is carried to that of I under the map

$$\mathrm{H}^1(\mathbf{Z}, \mathrm{SO}(q)) \to \mathrm{H}^1(\mathbf{Z}, \mathrm{O}(q)).$$

For every prime p we have $\mathrm{H}^1(\mathbf{Z}_p, \mathrm{SO}(q)) = 1$ (Proposition 3.10), so $\mathrm{I}'_{\mathbf{Z}_p}$ is a trivial torsor over $\mathbf{Z}_p$ and hence so is $\mathrm{I}_{\mathbf{Z}_p}$. In other words, for every p we have $\mathrm{I}(\mathbf{Z}_p) \neq \varnothing$, so $q'_{\mathbf{Z}_p} \simeq q_{\mathbf{Z}_p}$. The signatures of q' and q agree by hypothesis, so $q'_{\mathbf{Q}} \simeq q_{\mathbf{Q}}$ by the Hasse–Minkowski theorem. We want to deduce that $q' \simeq q$ over $\mathbf{Z}$.

Necessarily $\mathrm{I}'(\mathbf{R})$ is non-empty. Indeed, it suffices to check that the map $\mathrm{H}^1(\mathbf{R}, \mathrm{SO}(q)) \to \mathrm{H}^1(\mathbf{R}, \mathrm{O}(q))$ has trivial kernel. Such triviality amounts to the surjectivity of the natural map $\mathrm{O}(q)(\mathbf{R}) \to (\mathrm{O}(q)/\mathrm{SO}(q))(\mathbf{R}) = \{\pm 1\}$ (via determinant), which is verified by inspection of a diagonal form for $q_{\mathbf{R}}$.

We shall lift the cohomology class $[\mathrm{I}']$ to a class $[\widetilde{\mathrm{I}}] \in \mathrm{H}^1(\mathbf{Z}, \mathrm{Spin}(q))$ such that $\widetilde{\mathrm{I}}(\mathbf{R})$ is non-empty. This property is deeper than the lifting of $[\mathrm{I}]$ to $[\mathrm{I}']$, since the existence of an $\mathbf{R}$-point in a lifted $\mathrm{Spin}(q)$-torsor over $\mathbf{Z}$ will not be automatic.

Consider the central extension of fppf affine $\mathbf{Z}$-groups

$$1 \to \mu_2 \to \mathrm{Spin}(q) \to \mathrm{SO}(q) \to 1. \tag{A.1}$$

We aim to prove that $\mathrm{H}^1(\mathbf{Z}, \mathrm{Spin}(q)) \to \mathrm{H}^1(\mathbf{Z}, \mathrm{SO}(q))$ is surjective, and to understand its fibers (so as to control $\mathbf{R}$-points). To clarify the cohomological methods to be used, it is better to first consider a generalization of (A.1). Let

$$1 \to \mathrm{C} \to \mathrm{G} \xrightarrow{f} \mathrm{G}' \to 1 \tag{A.2}$$

be a central extension of fppf affine group schemes over a scheme S. Using fppf cohomology, there is a natural action of $\mathrm{H}^1(\mathrm{S}, \mathrm{C})$ on $\mathrm{H}^1(\mathrm{S}, \mathrm{G})$ arising from the translation action on G by its central subgroup C. The description of $\mathrm{H}^1(f)$ via pushout of torsors along f (carrying the isomorphism class of a right G-torsor E to the isomorphism class of $\mathrm{E} \times^{\mathrm{G}} \mathrm{G}'$) makes it clear that the $\mathrm{H}^1(\mathrm{S}, \mathrm{C})$-action leaves $\mathrm{H}^1(f)$ invariant, so each non-empty fiber of $\mathrm{H}^1(f)$ is a union of $\mathrm{H}^1(\mathrm{S}, \mathrm{C})$-orbits.

Lemma A.3. — *The action of* $\mathrm{H}^1(\mathrm{S}, \mathrm{C})$ *on each non-empty fiber of* $\mathrm{H}^1(f)$ *is transitive.*

Proof. — Over the distinguished point in $\mathrm{H}^1(\mathrm{S}, \mathrm{G})$, such transitivity expresses the exactness of the diagram of pointed sets

$$\begin{tikzcd} \mathrm{H}^1(\mathrm{S}, \mathrm{C}) \arrow[r] & \mathrm{H}^1(\mathrm{S}, \mathrm{G}) \arrow[r, "\mathrm{H}^1(f)"] & \mathrm{H}^1(\mathrm{S}, \mathrm{G}') \end{tikzcd}$$

associated to (A.2); see [**Co1**, Prop. B.3.2] for a proof of such exactness (written over fields, but in a manner that works over any scheme).

Now consider a general right G-torsor E, and the fiber of $\mathrm{H}^1(f)$ through the class [E] of E. Let $\mathrm{E}' = \mathrm{E} \times^{\mathrm{G}} \mathrm{G}'$ be the associated right G'-torsor obtained by pushout. Since C is central in G, we have $\mathrm{E}' = \mathrm{E}/\mathrm{C}$, and ${}_{\mathrm{E}}\mathrm{G} := \mathrm{Aut}_{\mathrm{G}}(\mathrm{E})$ is an fppf form of G that naturally contains C with quotient ${}_{\mathrm{E}'}\mathrm{G}' := \mathrm{Aut}_{\mathrm{G}'}(\mathrm{E}')$. Denote the quotient map ${}_{\mathrm{E}}\mathrm{G} \to {}_{\mathrm{E}'}\mathrm{G}'$ as ${}_{\mathrm{E}}f$.

The technique of "twisting by fppf torsors" (explained in [**Co1**, § B.3.2] over fields, but in a style that works over any scheme) defines a natural $\mathrm{H}^1(\mathrm{S},\mathrm{C})$-equivariant bijection $t_{\mathrm{E}} : \mathrm{H}^1(\mathrm{S},\mathrm{G}) \simeq \mathrm{H}^1(\mathrm{S}, {}_{\mathrm{E}}\mathrm{G})$ carrying [E] to the distinguished point. (This corresponds to translation by $-[\mathrm{E}]$ in the commutative case.) We likewise have $t_{\mathrm{E}'}$, and it is easy to check that the diagram

$$\begin{tikzcd}
\mathrm{H}^1(\mathrm{S},\mathrm{G}) \arrow[r, "\mathrm{H}^1(f)"] \arrow[d, "t_{\mathrm{E}}"'] & \mathrm{H}^1(\mathrm{S},\mathrm{G}') \arrow[d, "t_{\mathrm{E}'}"] \\
\mathrm{H}^1(\mathrm{S},{}_{\mathrm{E}}\mathrm{G}) \arrow[r, "\mathrm{H}^1({}_{\mathrm{E}}f)"] & \mathrm{H}^1(\mathrm{S},{}_{\mathrm{E}'}\mathrm{G}')
\end{tikzcd}$$

commutes. Thus, the transitivity of the $\mathrm{H}^1(\mathrm{S},\mathrm{C})$-action on the fiber through the class of E is a consequence of the exactness of $\mathrm{H}^1(\mathrm{S},\mathrm{C}) \to \mathrm{H}^1(\mathrm{S},{}_{\mathrm{E}}\mathrm{G}) \to \mathrm{H}^1(\mathrm{S},{}_{\mathrm{E}}\mathrm{G}')$. □

There is also an exact sequence of pointed sets

$$\mathrm{H}^1(\mathrm{S},\mathrm{G}) \to \mathrm{H}^1(\mathrm{S},\mathrm{G}') \overset{\delta}{\to} \mathrm{H}^2(\mathrm{S},\mathrm{C})$$

with right term that is an instance of derived functor cohomology on abelian fppf sheaves. (If G or G′ are S-smooth then their H^1's can be computed using the étale topology as well, but when C is not S-smooth then Čech-theoretic methods are insufficient to construct δ.) The key to constructing δ with the desired exactness properties is that the derived functor H^2 on abelian sheaves has an interpretation in terms of gerbes (analogous to the interpretation of H^1 via torsors); see [**Co1**, Prop. B.3.3] for a self-contained discussion of this issue (written over fields, but in a manner that works verbatim over any scheme).

We conclude that if $\mathrm{H}^2(\mathrm{S},\mathrm{C}) = 0$ then $\mathrm{H}^1(\mathrm{S},\mathrm{G}) \to \mathrm{H}^1(\mathrm{S},\mathrm{G}')$ is surjective with fibers that are the $\mathrm{H}^1(\mathrm{S},\mathrm{C})$-orbits. Hence, $\mathrm{H}^1(\mathbf{Z},\mathrm{Spin}(q)) \to \mathrm{H}^1(\mathbf{Z},\mathrm{SO}(q))$ is surjective with fibers that are the $\mathrm{H}^1(\mathbf{Z},\mu_2)$-orbits provided that $\mathrm{H}^2(\mathbf{Z},\mu_2) = 1$. This vanishing is a special case of:

Lemma A.4. — *For any integer $d > 0$, $\mathrm{H}^2(\mathbf{Z},\mu_d) = 1$.*

Proof. — The d-power Kummer sequence $1 \to \mu_d \to \mathbf{G}_{\mathrm{m}} \overset{t^d}{\to} \mathbf{G}_{\mathrm{m}} \to 1$ is exact for the fppf topology, so the general equality $\mathrm{Pic}_{\mathrm{fppf}}(\mathrm{S}) = \mathrm{Pic}(\mathrm{S})$ for any scheme (by fppf descent theory) and the vanishing of $\mathrm{Pic}(\mathbf{Z})$ imply that $\mathrm{H}^2(\mathbf{Z},\mu_d)$ is identified with the d-torsion subgroup of the fppf cohomology group $\mathrm{H}^2(\mathbf{Z},\mathbf{G}_{\mathrm{m}})$. It is a theorem of Grothendieck [**BrIII**, 11.7(1)] that for any scheme S and integer i, the natural map $\mathrm{H}^i(\mathrm{S}_{\text{ét}},\mathrm{G}) \to \mathrm{H}^i(\mathrm{S}_{\mathrm{fppf}},\mathrm{G})$ is bijective for any commutative smooth affine S-group G. By applying this with $\mathrm{S} = \mathrm{Spec}(\mathbf{Z})$ and $\mathrm{G} = \mathbf{G}_{\mathrm{m}}$, we are reduced to proving the vanishing of the étale cohomology group $\mathrm{H}^2(\mathbf{Z}, \mathbf{G}_{\mathrm{m}})$. Such vanishing is a consequence of calculations with class field theory [**Mil**, III, Ex. 2.22(f)]. $\square$

By inspection, $\mathrm{H}^1(\mathbf{Z}, \mu_2) \to \mathrm{H}^1(\mathbf{R}, \mu_2)$ is an isomorphism. Thus, $\mathrm{H}^1(\mathbf{Z}, \mu_2)$ acts transitively on fibers for $\mathrm{H}^1(\mathbf{R}, \mathrm{Spin}(q)) \to \mathrm{H}^1(\mathbf{R}, \mathrm{SO}(q))$. We know that $[\mathrm{I}]$ lifts to a class $[\mathrm{I}'] \in \mathrm{H}^1(\mathbf{Z}, \mathrm{SO}(q))$, and that $[\mathrm{I}'_{\mathbf{R}}] = 1$. Hence, the fiber over $[\mathrm{I}'_{\mathbf{R}}] = 1$ in $\mathrm{H}^1(\mathbf{R}, \mathrm{Spin}(q))$ contains the trivial class. By using $\mathrm{H}^1(\mathbf{Z}, \mu_2)$-translations, we conclude that there is a right $\mathrm{Spin}(q)$-torsor $\widetilde{\mathrm{I}}$ over $\mathbf{Z}$ lying over I' (hence over I) such that $\widetilde{\mathrm{I}}(\mathbf{R})$ is non-empty.

In the language of torsor pushouts,

$$\mathrm{I} = \widetilde{\mathrm{I}} \times^{\mathrm{Spin}(q)} \mathrm{O}(q).$$

Thus, if $\widetilde{\mathrm{I}}(\mathbf{Z}) \neq \varnothing$ then $\mathrm{I}(\mathbf{Z}) \neq \varnothing$, as desired. Since $\widetilde{\mathrm{I}}(\mathbf{R})$ is non-empty, $\widetilde{\mathrm{I}}(\mathbf{Q})$ is non-empty because the natural map $\mathrm{H}^1(\mathbf{Q}, \mathrm{Spin}(q)) \to \mathrm{H}^1(\mathbf{R}, \mathrm{Spin}(q))$ is injective: this injectivity is a consequence of the Hasse principle for simply connected semisimple $\mathbf{Q}$-groups [**PR**, § 6.1, Thm. 6.6] and the vanishing theorem of Kneser–Bruhat–Tits for degree-1 cohomology of simply connected semisimple groups over non-archimedean local fields ([**PR**, § 6.1, Thm. 6.4], [**BT**, Thm. 4.7(ii)]).

Now we combine the existence of a $\mathbf{Q}$-point on $\widetilde{\mathrm{I}}$ with strong approximation (for indefinite spin groups) to find a $\mathbf{Z}$-point on $\widetilde{\mathrm{I}}$. The indefiniteness hypothesis on the signature implies that $\mathrm{Spin}(q)_{\mathbf{R}}$ is $\mathbf{R}$-isotropic (since its central isogenous quotient $\mathrm{SO}(q_{\mathbf{R}})$ is certainly isotropic). Thus, exactly as in the proof of Proposition 2.13, $\mathrm{Spin}(q)(\mathbf{Q})$ is dense in the space $\mathrm{Spin}(q)(\mathbf{A}^\infty)$ of points valued in the ring $\mathbf{A}^\infty = \mathbf{Q} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$ of finite adeles. But $\widetilde{\mathrm{I}}_{\mathbf{Q}} \simeq \mathrm{Spin}(q)_{\mathbf{Q}}$ as affine $\mathbf{Q}$-schemes of finite type since $\widetilde{\mathrm{I}}(\mathbf{Q})$ is non-empty, so $\widetilde{\mathrm{I}}(\mathbf{Q})$ is dense in $\widetilde{\mathrm{I}}(\mathbf{A}^\infty)$. Using the $\mathbf{Z}$-structure $\widetilde{\mathrm{I}}$ on the $\mathbf{Q}$-scheme $\widetilde{\mathrm{I}}_{\mathbf{Q}}$, we obtain the open subset $\widetilde{\mathrm{I}}(\widehat{\mathbf{Z}}) \subset \widetilde{\mathrm{I}}(\mathbf{A}^\infty)$. This open set is equal to $\prod_p \widetilde{\mathrm{I}}(\mathbf{Z}_p)$, and it is non-empty because $\mathrm{H}^1(\mathbf{Z}_p, \mathrm{Spin}(q)) = 1$ for every p (Proposition 3.10). The non-empty intersection of the non-empty open set $\widetilde{\mathrm{I}}(\widehat{\mathbf{Z}})$ and the dense subset $\widetilde{\mathrm{I}}(\mathbf{Q})$ is $\widetilde{\mathrm{I}}(\mathbf{Z})$, so we are done. $\square$

Appendix B
Octonion algebras over rings

An *octonion algebra* over a commutative ring R is a finite locally free R-module A of rank 8 equipped with a quadratic form $\nu : \mathrm{A} \to \mathrm{R}$ (called the *norm*) and a possibly non-associative R-algebra structure admitting a 2-sided identity e such that (A, ν) is a non-degenerate quadratic space and $\nu(xy) = \nu(x)\nu(y)$ for all $x, y \in \mathrm{A}$.

The element $\nu(e) \in \mathrm{R}$ is idempotent, so Zariski-locally on $\mathrm{Spec}(\mathrm{R})$ it is equal to 0 or 1, and it satisfies $\nu(x) = \nu(x)\nu(e)$ for all $x \in \mathrm{A}$, so $\nu(e) = 1$ since ν is non-degenerate. Since $\mathrm{R} \to \mathrm{A}$ via $r \mapsto re$ is injective, we often write r rather than re when viewing R inside A.

We define

$$\langle \cdot, \cdot \rangle := \mathrm{B}_\nu$$

to be the symmetric bilinear form associated to the norm form, and define the *conjugation*

$$x^* := \langle x, e \rangle - x,$$

so $e^* = e$ and $x^{**} = x$. The R-linear map $\mathrm{T} : \mathrm{A} \to \mathrm{R}$ defined by $\langle \cdot, e \rangle$ is called the *trace*. For all $x \in \mathrm{A}$, clearly $x + x^* = \mathrm{T}(x)$ and

$$\begin{aligned} \nu(x^*) = \nu(\mathrm{T}(x)e - x) &= \mathrm{T}(x)^2\nu(e) - \langle \mathrm{T}(x)e, x \rangle + \nu(x) \\ &= \mathrm{T}(x)^2 - \mathrm{T}(x)\langle e, x \rangle + \nu(x) \\ &= \nu(x). \end{aligned}$$

Since A has even rank, non-degeneracy of the quadratic space (A, ν) implies that $\langle \cdot, \cdot \rangle$ is perfect. Using this, there are a number of basic identities whose proofs over fields in [**SV**, § 1.2–1.4] work verbatim over any commutative base ring. In particular, as in [**SV**, § 1.2–1.3],

$$x^2 - \mathrm{T}(x)x + \nu(x) = 0 \tag{B.1}$$

and $xx^* = \nu(x) = x^*x$ for all $x \in \mathrm{A}$, $(xy)^* = y^*x^*$ for all $x, y \in \mathrm{A}$, and

$$\langle xy, z \rangle = \langle y, x^*z \rangle, \;\; \langle x, yz \rangle = \langle xz^*, y \rangle$$

for all $x, y, z \in \mathrm{A}$. Setting $y = e$ in this final identity, we get

$$\langle x, y \rangle = \mathrm{T}(xy^*)$$

for all $x, y \in \mathrm{A}$. Note that by the quadratic relation (B.1), for any $x \in \mathrm{A}$ the R-subalgebra of A generated by x is commutative and associative.

The general identities (as in [**SV**, Lemma 1.3.3])

$$x(x^*y) = \nu(x)y = (yx)x^* \tag{B.2}$$

imply

$$\langle xy, xz \rangle = \langle y, x^*(xz) \rangle = \langle y, \nu(x)z \rangle = \nu(x)\langle y, z \rangle$$

and likewise $\langle xz, yz \rangle = \nu(z)\langle x, y \rangle$ for any $x, y, z \in \mathrm{A}$, so (upon subtituting $z + w$ for z in this final identity) for any $x, y, z, w \in \mathrm{A}$ we have

$$\langle xz, yw \rangle + \langle xw, yz \rangle = \langle x, y \rangle \langle z, w \rangle. \tag{B.3}$$

One proves exactly as over fields in [**SV**, § 1.4] the *Moufang identities*

$$(xy)(zx) = x((yz)x), \;\; x(y(xz)) = (x(yx))z, \;\; y(x(zx)) = ((yx)z)x$$

and their consequences:

$$x(xy) = x^2y, \ \ (xy)y = xy^2 \tag{B.4}$$

and the alternating property of the trilinear *associator*

$$[x, y, z] = (xy)z - x(yz).$$

Note also that multiplication is *trace-associative* in the sense that $\mathrm{T}((xy)z) = \mathrm{T}(x(yz))$:

$$\mathrm{T}((xy)z) = \langle xy, z^*\rangle = \langle x, z^*y^*\rangle = \langle x, (yz)^*\rangle = \mathrm{T}(x(yz)).$$

The identity (B.1) says that A is a *degree-*2 *algebra* in the sense of [**McC**, (0.6), (0.7)]. Since e is part of a basis of A Zariski-locally on Spec(R), the pair (T, ν) consisting of a linear form $\mathrm{T} : \mathrm{A} \to \mathrm{R}$ and a quadratic form $\nu : \mathrm{A} \to \mathrm{R}$ satisfying (B.1) for all $x \in \mathrm{A}$ is *unique*, by [**McC**, Prop. 2.2, Prop. 2.3(vi)]. This implies:

Proposition B.1. — *Every* R*-algebra automorphism of* (A, e) *preserves* ν*, and hence preserves* T *and the conjugation.*

On $\mathrm{Mat}_2(\mathrm{R})$, we have the standard involution $x \mapsto x^*$ defined by conjugation of the transpose against the standard Weyl element $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. This is used in:

Definition B.2. — The *split octonion* R*-algebra* is the R-module $\Lambda_{\mathrm{R}} := \mathrm{Mat}_2(\mathrm{R}) \oplus \mathrm{Mat}_2(\mathrm{R})$ equipped with the multiplication law

$$(x, y)(z, w) = (xz + wy^*, x^*w + zy)$$

and the norm form $\nu(x, y) = \det(x) - \det(y)$.

It is straightforward to check (using that $xx^* = \det(x)$ on $\mathrm{Mat}_2(\mathrm{R})$ and $x^* = -x$ on $\mathfrak{sl}_2(\mathrm{R})$) that Λ_{R} is an octonion algebra with identity $(1, 0)$, trace $(x, y) \mapsto \mathrm{Tr}(x)$ (usual matrix trace), conjugation $(x, y)^* = (x^*, -y)$, and underlying quadratic space isomorphic to the standard split quadratic space (R^8, q_8) of rank 8. Over a field, up to isomorphism the split octonion algebra is the only one whose norm admits isotropic vectors (i.e., $a \in \mathrm{A} - \{0\}$ such that $\mathrm{N}(a) = 0$) [**SV**, 1.8.1].

Example B.3. — Let K be a non-archimedean local field. Every non-degenerate quadratic space over K with dimension $\geqslant 5$ admits an isotropic vector, so any octonion algebra over K is isomorphic to Λ_{K}.

Definition B.4. — A pair of elements x, y in an octonion algebra (A, ν) over R are *inverse* to each other if the R-linear left and right multiplication maps ℓ_x, ℓ_y, r_x, r_y are invertible and satisfy $\ell_x = \ell_y^{-1}$ and $r_x = r_y^{-1}$, and $x \in \mathrm{A}$ is a *unit* if x admits a (necessarily unique) inverse. If R is a field then A is an *octonion division algebra* if every nonzero element of A is a unit.

By (B.2), an element $x \in \mathrm{A}$ is a unit if and only if $\nu(a) \in \mathrm{R}^\times$, in which case $\nu(a)^{-1}a^*$ is the inverse of a. Thus, an octonion algebra over a field k is a division algebra precisely when the norm is k-anisotropic (e.g., positive-definite when $k = \mathbf{Q}, \mathbf{R}$). The units of an octonion algebra do not form a group under multiplication because multiplication is non-associative.

The main result of this appendix is the following theorem over rings that relativizes a classical fact over fields. The proof is an adaptation of the argument over fields in [**vdBS**, (2.4)–(2.5)], bringing in some elementary commutative algebra in order to control freeness of module structures.

Theorem B.5. — *If an octonion algebra over a local ring* R *has underlying quadratic space that is split then it is a split algebra; i.e., isomorphic to* Λ_{R}. *Every octonion algebra over a ring* C *becomes split over an affine étale cover of* C.

Proof. — We begin by explaining why the second part follows from the first, so consider an octonion algebra over a ring C. Over some affine étale cover Spec(C′) of Spec(C) we can split the underlying even-rank non-degenerate quadratic space [**SGA7**, XII, Prop. 1.2]. By "spreading out" over Spec(C′), we can identify the octonion algebra with $\Lambda_{\mathrm{C}'}$ Zariski-locally over Spec(C′) *provided* that we can do so over the local rings of C′. Hence, it suffices to apply the first assertion of the theorem to the local rings of C′.

Let R be a local ring, with residue field k, and let (A, ν) be an octonion algebra over R whose underlying quadratic space is isomorphic to (R^8, q_8). In particular, A has an R-basis $\{a_i\}$ consisting of isotropic vectors. Since the element $e \in \mathrm{A}$ is part of an R-basis, by perfectness of $\langle\cdot,\cdot\rangle$ some $a = \sum r_i a_i$ satisfies $1 = \langle e, a\rangle = \sum r_i \langle e, a_i\rangle$, so $\langle e, a_{i_0}\rangle \in \mathrm{R}^\times$ for some i_0. By unit scaling of such an a_{i_0}, we thereby obtain an isotropic $a \in \mathrm{A}$ that is part of an R-basis of A and satisfies $\langle e, a\rangle = 1$.

The pair $\{e, a\}$ is part of an R-basis of A: by locality of R and freeness of A it suffices to check this in A_k over the residue field k, and there we use that $\langle e, a\rangle = 1$ and $\langle a, a\rangle = 2\nu(a) = 0$. Since $\nu(a-e) = \nu(a) - \langle a, e\rangle + \nu(e) = 0 - 1 + 1 = 0$, the elements a and $e - a$ provide a decomposition

$$e = x_0 + y_0$$

with isotropic $x_0, y_0 \in \mathrm{A}$ that satisfy $\langle x_0, y_0\rangle = 1$. The split hypothesis on the quadratic space over R has done its work.

The pair $\{x_0, y_0\}$ is an R-basis of a direct summand H of A, either by construction or by repeating the argument used with $\{e, a\}$ above, and visibly (H, ν) is a hyperbolic plane over R. In particular, $\langle\cdot,\cdot\rangle$ is perfect on H, so by perfectness of $\langle\cdot,\cdot\rangle$ on the free R-module A it follows that $\mathrm{A} = \mathrm{H} \oplus \mathrm{H}^\perp$ for the orthogonal complement $\mathrm{H}^\perp$ of H in A that must be a free R-module of rank 6.

Since $\nu(x_0) = 0$ and

$$\mathrm{T}(x_0) = \langle x_0, e\rangle = \langle x_0, x_0 + y_0\rangle = 2\nu(x_0) + \langle x_0, y_0\rangle = 1,$$

we see that $x_0^* = e - x_0 = y_0$ and (via the relation (B.1) for x_0) that $x_0^2 = x_0$. Likewise, $y_0^2 = y_0$ and $y_0^* = e - y_0 = x_0$. Clearly $x_0 y_0 = x_0(e - x_0) = 0$ and $y_0 x_0 = 0$, so x_0 and y_0 are orthogonal idempotents summing to e that are swapped by conjugation. In particular, $\mathrm{H}^\perp$ is stable under left multiplication by x_0 and y_0; e.g., if $z \in \mathrm{H}^\perp$ then

$$\langle x_0, x_0 z\rangle = \nu(x_0)\langle e, z\rangle = 0,\ \ \langle y_0, x_0 z\rangle = \langle x_0^* y_0, z\rangle = \langle y_0^2, z\rangle = \langle y_0, z\rangle = 0.$$

Hence, it is reasonable to consider the R-submodules

$$\text{(B.5)}\qquad \mathrm{M} = \{x \in \mathrm{H}^\perp \mid x_0 x = x\},\ \ \mathrm{N} = \{y \in \mathrm{H}^\perp \mid y_0 y = y\}$$

inside $\mathrm{H}^\perp$.

By (B.4) and the idempotent property of x_0 we see that $x_0\mathrm{M} = \mathrm{M} = x_0\mathrm{H}^\perp$, and likewise $y_0\mathrm{N} = \mathrm{N} = y_0\mathrm{H}^\perp$. The condition in (B.5) defining M inside $\mathrm{H}^\perp$ can also be written as "$y_0 x = 0$", and similarly with N using x_0. Since $\mathrm{A} = \mathrm{H} \oplus \mathrm{H}^\perp$, it follows that $x_0\mathrm{A} = \mathrm{R}x_0 \oplus \mathrm{M}$ and $y_0\mathrm{A} = \mathrm{R}y_0 \oplus \mathrm{N}$ (both direct sums inside A). Thus, $x_0\mathrm{A}$ is killed by left multiplication against y_0 and likewise $y_0\mathrm{A}$ is killed by left multiplication against x_0, so $x_0\mathrm{A} \cap y_0\mathrm{A} = 0$ since this intersection is killed by left multiplication against $x_0 + y_0 = e$.

Clearly $\mathrm{A} = x_0\mathrm{A} + y_0\mathrm{A}$, so we conclude that the R-modules

$$\mathrm{M}_0 := x_0\mathrm{A} = \mathrm{R}x_0 \oplus \mathrm{M},\ \ \mathrm{N}_0 := y_0\mathrm{A} = \mathrm{R}y_0 \oplus \mathrm{N}$$

satisfy $\mathrm{M}_0 \oplus \mathrm{N}_0 = \mathrm{A}$. Thus, M_0 and N_0 are each finite free modules, due to being direct summands of the finite free module A over the local ring R, so likewise their respective direct summands M and N are also finite free R-modules. The equality $\mathrm{M}_0 \oplus \mathrm{N}_0 = \mathrm{A} = \mathrm{H} \oplus \mathrm{H}^\perp$ with $\mathrm{H} = \mathrm{R}x_0 \oplus \mathrm{R}y_0$ forces the R-linear map $\mathrm{M} \oplus \mathrm{N} \to \mathrm{H}^\perp$ to be an isomorphism.

We claim that the R-submodules M_0 and N_0 in A are isotropic in the sense that $\langle\cdot,\cdot\rangle$ has vanishing restriction to each. To check the isotropicity of M_0, note that if $x, x' \in \mathrm{M}$ then

$$\langle x, x'\rangle = \langle x_0 x, x_0 x'\rangle = \nu(x_0)\langle x, x'\rangle = 0,$$

and for $\lambda \in \mathrm{R}$ we have

$$\langle x, \lambda x_0\rangle = \lambda\langle x_0 x, x_0 e\rangle = \lambda\nu(x_0)\mathrm{T}(x) = 0.$$

Since moreover $\langle x_0, x_0\rangle = 2\nu(x_0) = 0$, the isotropicity of M_0 is established. The case of N_0 goes similarly.

Lemma B.6. — *The free* R*-modules* M *and* N *have rank equal to* 3.

Proof. — Since M_0 and N_0 are direct summands of the finite free module A, the induced k-linear maps $(\mathrm{M}_0)_k \to \mathrm{A}_k$ and $(\mathrm{N}_0)_k \to \mathrm{A}_k$ are injections onto isotropic subspaces of the quadratic space $(\mathrm{A}_k, \nu_k) \simeq (k^8, q_8)$ in which the maximal isotropic subspaces have dimension 4. Thus, M_0 and N_0 have rank $\leqslant 4$. Their ranks add up to 8, so each has rank equal to 4. Hence, their respective direct summands M and N must be free over R of rank 3. □

Lemma B.7. — *Conjugation on* A *acts on* M *and* N *via negation, and*

$$\mathrm{M} = \{x \in \mathrm{H}^\perp \,|\, xx_0 = 0\}, \;\; \mathrm{N} = \{y \in \mathrm{H}^\perp \,|\, yy_0 = 0\}.$$

Proof. — Since $\mathrm{M} \subset \mathrm{H}^\perp \subset (\mathrm{R}e)^\perp$, the trace vanishes on M. Hence, conjugation on M is negation. For $x \in \mathrm{M}$, applying conjugation to the equality $x_0 x = x$ for all $x \in \mathrm{M}$ gives $x^* x_0^* = x^*$ for such x, or equivalently $-xx_0^* = -x$. But $x_0^* = e - x_0$ since $\mathrm{T}(x_0) = 1$, so $-x(e - x_0) = -x$. Thus, $xx_0 = 0$. Similarly, $yy_0 = 0$ for $y \in \mathrm{N}$. This proves the containments "$\subseteq$" in place of the desired module equalities.

To prove the reverse containments, since $\mathrm{H}^\perp = \mathrm{M} + \mathrm{N}$ it remains to show that right multiplication r_{x_0} by x_0 acts injectively on N, and likewise for r_{y_0} on M. But $r_{x_0} + r_{y_0}$ is the identity map and $r_{y_0}|_\mathrm{N} = 0$, so $r_{x_0}|_\mathrm{N}$ is the identity on N. The case of r_{y_0} goes similarly. □

Lemma B.8. — *If $x, x' \in \mathrm{M}$ then $xx' \in \mathrm{N}$, and if $y, y' \in \mathrm{N}$ then $yy' \in \mathrm{M}$. If $x \in \mathrm{M}$ and $y \in \mathrm{N}$ then $xy \in \mathrm{H}$.*

Proof. — Since $\langle x_0, x\rangle = 0$ (as $\mathrm{M} \subset \mathrm{H}^\perp$), (B.3) gives

$$\langle x_0, xx'\rangle + \langle x_0 x', x\rangle = \langle x_0, x\rangle\langle e, x'\rangle = 0.$$

But $x_0 x' = x'$, and $\langle x', x\rangle = 0$ since M is isotropic, so $\langle x_0, xx'\rangle = 0$. Since $\langle y_0, x\rangle = 0$ (as $\mathrm{M} \subset \mathrm{H}^\perp$) and $y_0 x' = 0$, likewise $\langle y_0, xx'\rangle = 0$. Thus, $xx' \in \mathrm{H}^\perp$. The alternating property of associators gives that

$$x_0(xx') - (x_0 x)x' = -(x(x_0 x') - (xx_0)x'),$$

and we have $x_0 x = x$ and $x_0 x' = x'$ since $x, x' \in \mathrm{M}$, so $x_0(xx') = (xx_0)x' = 0$ (by Lemma B.7). Thus, xx' lies in $\{z \in \mathrm{H}^\perp \,|\, x_0 z = 0\} = \mathrm{N}$. The proof that $yy' \in \mathrm{M}$ proceeds similarly.

Finally, to show $xy \in \mathrm{H}$, it is equivalent to show $xy \in (\mathrm{H}^\perp)^\perp = (\mathrm{M} \oplus \mathrm{N})^\perp$. Hence, it suffices to show that $\langle xy, x'\rangle$ and $\langle xy, y'\rangle$ vanish for any $x' \in \mathrm{M}$ and $y' \in \mathrm{N}$. But $\langle xy, x'\rangle = \langle y, x^* x'\rangle = -\langle y, xx'\rangle$, and this vanishes because $xx' \in \mathrm{N}$ and N is isotropic. Similarly, $\langle xy, y'\rangle = \langle x, y' y^*\rangle = -\langle x, y' y\rangle = 0$ since $yy' \in \mathrm{M}$ and M is isotropic. □

Since $\langle\cdot,\cdot\rangle$ is perfect on A and H, it is perfect on $\mathrm{H}^\perp = \mathrm{M} \oplus \mathrm{N}$ with each of M and N isotropic of rank 3. Hence, $\langle\cdot,\cdot\rangle$ identifies M and N as R-linear duals of each other, so we can choose R-bases $\{x_1, x_2, x_3\}$ of M and $\{y_1, y_2, y_3\}$ of N such that $\langle x_i, y_j\rangle = \delta_{ij}$.

By Lemma B.8 we have $x_1x_2 = \sum \lambda_j y_j$ for unique $\lambda_j \in \mathrm{R}$. The dual-basis property gives that $\lambda_j = \langle x_1x_2, x_j\rangle$, and the isotropicity of M implies that $\langle x_1x_2, x_1\rangle = \nu(x_1)\langle x_2, e\rangle = 0$ and $\langle x_1x_2, x_2\rangle = \nu(x_2)\langle x_1, e\rangle = 0$, so $x_1x_2 = \lambda y_3$ for $\lambda := \langle x_1x_2, x_3\rangle \in \mathrm{R}$. Likewise,

$$x_2x_3 = \langle x_2x_3, x_1\rangle y_1, \ \ x_3x_1 = \langle x_3x_1, x_2\rangle y_2.$$

Since $x^2 = 2\nu(x) = 0$ for $x \in \mathrm{M}$, and conjugation on M is negation, it follows that the trilinear form $\langle xx', x''\rangle$ on M is alternating. Hence,

$$\langle x_2x_3, x_1\rangle = -\langle x_2x_1, x_3\rangle = \langle x_1x_2, x_3\rangle = \lambda$$

and similarly $\langle x_3x_1, x_2\rangle = \lambda$, so

$$x_ix_{i+1} = \lambda y_{i+2}$$

with subscripts in $\{1, 2, 3\}$ treated modulo 3. Likewise, $x_{i+1}x_i = -\lambda y_{i+2}$ by applying conjugation, so this tells us how to multiply pairs in the R-basis $\{x_1, x_2, x_3\}$ of M

Next, we turn to products x_iy_j and y_ix_j between bases of M and N. The products x_iy_j lie in H by Lemma B.8, so $x_iy_j = \lambda_{ij}x_0 + \lambda'_{ij}y_0$ for some $\lambda_{ij}, \lambda'_{ij} \in \mathrm{R}$. Hence,

$$\lambda_{ij} = \langle x_iy_j, y_0\rangle = \langle x_i, y_0y_j^*\rangle = -\langle x_i, y_0y_j\rangle = -\langle x_i, y_j\rangle = -\delta_{ij}$$

since left multiplication by y_0 on N is the identity map, and

$$\lambda'_{ij} = \langle x_iy_j, x_0\rangle = \langle y_j, x_i^*x_0\rangle = -\langle y_j, x_ix_0\rangle = 0$$

since right multiplication by x_0 on M vanishes (Lemma B.7). We have shown that $x_iy_j = \delta_{ij}x_0$, and in the same way one shows $y_ix_j = \delta_{ij}y_0$.

By design, left multiplication ℓ_{x_0} by x_0 is the identity on M and kills N, and by Lemma B.7 right multiplication r_{x_0} by x_0 kills M (so $r_{y_0} = 1 - r_{x_0}$ is the identity on M) and r_{y_0} kills N (so $r_{x_0} = 1 - r_{y_0}$ is the identity on N).

The only remaining information for a complete description of the R-bilinear multiplication law is the determination of products among elements in the R-basis $\{y_1, y_2, y_3\}$ of N. But recall that $x_1x_2 = \lambda y_3$, so the alternating property of associators gives that $\lambda(y_3y_1)$ equals

$$\begin{aligned}(\lambda y_3)y_1 = (x_1x_2)y_1 &= x_1(x_2y_1) - ((x_1y_1)x_2 - x_1(y_1x_2))\\ &= x_1(0) - (-x_0x_2 - x_1(0))\\ &= x_2.\end{aligned}$$

This forces $\lambda \in \mathrm{R}^\times$ since x_2 is part of an R-basis of A, so we may replace x_3 with $(1/\lambda)x_3$ and replace y_3 with λy_3 to arrange that $\lambda = 1$. Hence, $y_3y_1 = x_2$, and by the same arguments $y_iy_{i+1} = x_{i+2}$ (with subscripts in $\{1, 2, 3\}$ treated modulo 3).

We have completely determined the multiplication law, and there are no parameters at all. Hence, up to isomorphism there is at most one possibility for the octonion R-algebra with split underlying quadratic space. But Λ_{R} is such an octonion algebra, so it is the only one. This completes the proof of Theorem B.5. □

Now we turn our attention to the situation over Dedekind domains. Let R be a Dedekind domain with fraction field K, and let (O, ν) be an octonion algebra over K. Before we study R-orders in O (i.e., R-lattices containing e that are stable under multiplication), we prove:

Proposition B.9. — *There exist* R*-orders in* O*. Every* R*-order lies in a maximal one.*

Proof. — We first show that R-orders exist. By choosing a K-basis of O containing the identity e and expressing the K-bilinear multiplication in terms of "structure constants" in K relative to this K-basis, denominator-chasing in the structure constants produces a nonzero $r \in \mathrm{R}$ for which the chosen K-basis spans an $\mathrm{R}[1/r]$-order in $\mathrm{O}[1/r]$.

The problem is now localized to each of the finitely many maximal ideals of R containing r, so we may assume R is a discrete valuation ring. Using the bijective correspondence between R-lattices in O and $\widehat{\mathrm{R}}$-lattices in $\mathrm{O}_{\widehat{\mathrm{K}}}$ (with $\widehat{\mathrm{K}} := \mathrm{Frac}(\widehat{\mathrm{R}}) = \mathrm{K} \otimes_{\mathrm{R}} \widehat{\mathrm{R}}$), we may assume R is also complete. Hence, for any finite extension K' of K, the integral closure R' of R in K' is an R-finite discrete valuation ring.

The R-lattices in a finite-dimensional K-vector space V are precisely the finitely generated R-submodules that are open with respect to the natural topology. Thus, for any finite extension K' of K and R'-lattice L' in $\mathrm{V}_{\mathrm{K}'}$, $\mathrm{L}' \cap \mathrm{V}$ is an R-lattice in V. It therefore suffices to construct an order after a finite extension on the ground field. Hence, we may assume O is split, so a K-isomorphism $\mathrm{O} \simeq \Lambda_{\mathrm{K}}$ provides an R-order, namely Λ_{R}. This completes the proof of the existence of R-orders in general.

Now we return to the setting of a general Dedekind domain R, and consider an R-order A in O. We need to show that A is contained in a maximal R-order. The R-order A meets K in exactly R, so for any $a \in \mathrm{A}$ not in K we see that $\mathrm{R}[a]$ is a finite flat commutative and associative R-algebra of rank 2 since it is contained in the R-lattice A and a satisfies the monic quadratic relation

$$a^2 - \mathrm{T}(a)a + \nu(a) = 0$$

over K with $a \notin \mathrm{K}$. This is the *unique* monic quadratic relation satisfied by a over K. The characteristic polynomial of a-multiplication on $\mathrm{R}[a]$ is a monic quadratic polynomial over R satisfied by a, so we conclude that $\mathrm{T}(a), \nu(a) \in \mathrm{R}$. Since $a + a^* = \mathrm{T}(a)$, it follows that $a^* \in \mathrm{A}$ for any $a \in \mathrm{A}$.

To summarize, the trace $\mathrm{T}(x) = x + x^*$ and norm $\nu(x) = xx^*$ are R-valued on A, and A is stable under the conjugation. In particular, the non-degenerate K-valued bilinear form $\langle x, y\rangle = \mathrm{T}(xy^*)$ on O has R-valued restriction to A, so A is contained in its own dual R-lattice $\mathrm{A}' \subset \mathrm{O}$. Any R-order $\mathrm{A}^{\#}$ containing A therefore satisfies $\mathrm{A}^{\#} \subset \mathrm{A}^{\#'} \subset \mathrm{A}'$, so by a noetherian R-module argument we see that A is contained in a maximal R-order. □

Example B.10. — Any octonion algebra A over a Dedekind domain R is a maximal R-order in its generic fiber. Indeed, perfectness of the R-bilinear trace pairing $\mathrm{T}(xy^*)$ on the octonion algebra over R implies that A is its own dual R-lattice, so there is no room for it to be contained in a strictly larger R-order.

As a special case, if R is a Dedekind domain with fraction field K then Λ_{R} is a maximal R-order in the split octonion algebra Λ_{K} over K. Conversely:

***Proposition B.11* (van der Blij, Springer)**. — *Let* R *be a Dedekind domain with fraction field* K*. Every maximal* R*-order* A *in the split octonion algebra* Λ_{K} *over* K *is an octonion algebra over* R *with respect to the* R*-valued restriction of the norm. If* R *is a discrete valuation ring then* A *is split and* $\mathrm{Aut}(\Lambda_{\mathrm{K}})$ *acts transitively on the set of maximal* R*-orders in* Λ_{K}*.*

In particular, if $\mathrm{R} \to \mathrm{R}'$ *is an extension of Dedekind domains and* $\mathrm{K} \to \mathrm{K}'$ *the corresponding extension of fraction fields then scalar extension to* R' *carries maximal* R*-orders in* Λ_{K} *to maximal* R'*-orders in* $\Lambda_{\mathrm{K}'}$

Proof. — To prove that A is an octonion algebra, we have to check non-degeneracy over R for A viewed as a quadratic space via the R-valued norm form on A. Since the rank is 8, which is even, it is equivalent to check perfectness of the R-bilinear trace pairing $\mathrm{Tr}(xy^*)$. We may localize to the case that R is a discrete valuation ring, as this preserves maximality of an order over the Dedekind base, so we now we may assume R is a principal ideal domain.

It is shown in [**vdBS**, (3.1)–(3.3)], using a characterization of maximal orders in terms of the quadratic form, that if R is a principal ideal domain then any maximal order A admits an R-basis relative to which the underlying quadratic space is (R^8, q_8). Thus, A has a norm form that is non-degenerate over R, so A is an octonion algebra over R. Assuming moreover that R is a discrete valuation ring, by Theorem B.5 the octonion algebra A must be isomorphic to Λ_{R}. In such cases, if A' is any maximal R-order in Λ_{K} then we have isomorphisms $\mathrm{A} \simeq \Lambda_{\mathrm{R}} \simeq \mathrm{A}'$ as octonion algebras over R, so localizing to K provides an automorphism of Λ_{K} carrying A to A'. □

Corollary B.12. — *Let* (O, ν) *be an octonion algebra over the fraction field* K *of a Dedekind domain* R *whose residue fields at maximal ideals are finite.*

Every maximal R*-order* A *in* O *is an octonion algebra with respect to the restriction* $\nu|_{\mathrm{A}} : \mathrm{A} \to \mathrm{R}$.

Proof. — The problem is to prove that the R-valued bilinear form $\mathrm{T}(xy^*)$ on A is perfect. For this purpose we may localize to the case when R is a discrete valuation ring, and then extend scalars to $\widehat{\mathrm{R}}$ since this does not affect the property of being a maximal order. Now K is a non-archimedean local field, so O is a split octonion algebra (Example B.3). Thus, Proposition B.11 may be applied to conclude. □

The study of automorphism schemes of octonion algebras requires the following flatness criterion from [**GY03**, Prop. 6.1]:

Lemma B.13. — *Let* S *be a connected Dedekind scheme and* $f : \mathrm{X} \to \mathrm{S}$ *a finite type map with a section* $e \in \mathrm{X}(\mathrm{S})$ *such that each fiber* X_s *is reduced and irreducible with dimension independent of* s*. Then* f *is flat.*

Proof. — By localizing, we may assume $\mathrm{S} = \mathrm{Spec}(\mathrm{R})$ for a discrete valuation ring R with fraction field K. Let $j : \mathrm{Z} \hookrightarrow \mathrm{X}$ be the schematic closure of the open immersion $i : \mathrm{X}_{\mathrm{K}} \to \mathrm{X}$, so j is defined by the kernel $\mathscr{I}$ of the K-localization map of quasi-coherent sheaves $\mathscr{O}_{\mathrm{X}} \to i_*(\mathscr{O}_{\mathrm{X}_{\mathrm{K}}})$. In particular, $\mathscr{O}_{\mathrm{Z}} \subset i_*(\mathscr{O}_{\mathrm{X}_{\mathrm{K}}})$, so $\mathscr{O}_{\mathrm{Z}}$ is torsion-free over the Dedekind R and hence Z is R-flat. It therefore suffices to show that j is an isomorphism.

Any map to X from a flat R-scheme factors through Z because the ideal $\mathscr{I} \subset \mathscr{O}_{\mathrm{X}}$ consists of sections killed by K-localization, which is to say are R-torsion. Hence, $e : \mathrm{Spec}(\mathrm{R}) \to \mathrm{X}$ factors through Z, so Z has non-empty special fiber Z_0. By R-flatness, $\dim \mathrm{Z}_0 = \dim \mathrm{Z}_{\mathrm{K}}$, yet the K-fiber $\mathrm{Z}_{\mathrm{K}} = \mathrm{X}_{\mathrm{K}}$ has the same dimension as X_0 by hypothesis, so the closed immersion $j_0 : \mathrm{Z}_0 \hookrightarrow \mathrm{X}_0$ is surjective since X_0 is irreducible. Thus, j_0 is defined by a nilpotent ideal, yet X_0 is reduced, so j_0 is an isomorphism. Hence, $j^\sharp : \mathscr{O}_{\mathrm{X}} \twoheadrightarrow j_*(\mathscr{O}_{\mathrm{Z}})$ becomes an isomorphism modulo a uniformizer π of R, so R-flatness of $j_*(\mathscr{O}_{\mathrm{Z}})$ implies $\mathscr{I}/(\pi) = \ker(j_0^\sharp)$. This kernel vanishes since j_0 is an isomorphism, so by Nakayama's Lemma the coherent $\mathscr{I}$ has vanishing stalks along the locus X_0 where π vanishes. It also has vanishing stalks along X_{K} since j_{K} is an isomorphism, so $\mathscr{I} = 0$. Hence, $\mathrm{X} = \mathrm{Z}$ is R-flat. □

Theorem B.14. — *For any octonion algebra* A *over a ring* R*, the affine finite type automorphism scheme* $\mathrm{Aut}_{\mathrm{A}/\mathrm{R}}$ *of the algebra is a semisimple* R*-group scheme of type* G_2*. This* R*-group is split if* $\mathrm{A} \simeq \Lambda_{\mathrm{R}}$*.*

Proof. — To prove that $\mathrm{Aut}_{\mathrm{A}/\mathrm{R}}$ is a semisimple R-group of type G_2, it suffices to work étale-locally over Spec(R). Hence, by Theorem B.5 we may assume $\mathrm{A} = \Lambda_{\mathrm{R}}$. Using base change from $\mathrm{Spec}(\mathbf{Z})$, it remains to show that $\mathrm{Aut}_{\Lambda/\mathbf{Z}}$ is a split semisimple $\mathbf{Z}$-group of type G_2.

By [**SV**, 2.3.5, 2.4.5], the automorphism scheme of an octonion algebra over a field k is connected semisimple (in particular, smooth) of type G_2. The explicit construction in (the proof of) [**SV**, 2.3.1] provides a k-homomorphism $f : \mathrm{T} \rightarrow \mathrm{Aut}_{\Lambda_k/k}$ from a 2-dimensional split k-torus T with $\ker f \simeq \mu_2$, so $f(\mathrm{T})$ is a split maximal k-torus in $\mathrm{Aut}_{\Lambda_k/k}$. Hence, $\mathrm{Aut}_{\Lambda/\mathbf{Z}} \rightarrow \mathrm{Spec}(\mathbf{Z})$ has fibers that are split connected semisimple groups of type G_2. Lemma B.13 ensures that this **Z**-group is flat, hence semisimple. Since the **Q**-fiber is split, by Proposition 1.3 the semisimple **Z**-group $\mathrm{Aut}_{\Lambda/\mathbf{Z}}$ is a Chevalley group. □

Corollary B.15. — *For any ring* R*, the assignment* $\mathrm{A} \mapsto \mathrm{Aut}_{\mathrm{A}/\mathrm{R}}$ *is a bijection from the set of isomorphism classes of octonion algebras over* R *to the set of isomorphism classes of semisimple* R*-groups of type* G_2*.*

Proof. — Since $\mathrm{G}_2 = \mathrm{Aut}_{\Lambda/\mathrm{R}}$, by Theorem B.5 the set of isomorphism classes of octonion algebras over R is identified with the étale cohomology set $\mathrm{H}^1(\mathrm{R}, \mathrm{G}_2)$. But G_2 is its own automorphism scheme over **Z** by (3.2), so this cohomology set also classifies isomorphism classes of semisimple R-groups of type G_2. Under this identification of the cohomology set as classifying both structures over R, the cohomology class of A corresponds to the Isom-scheme $\mathrm{Isom}(\Lambda_{\mathrm{R}}, \mathrm{A})$ as a right G_2-torsor and the cohomology class of $\mathrm{Aut}_{\mathrm{A}/\mathrm{R}}$ corresponds to the Isom-scheme $\mathrm{Isom}(\mathrm{Aut}_{\Lambda/\mathrm{R}}, \mathrm{Aut}_{\mathrm{A}/\mathrm{R}})$ as a right torsor for $\mathrm{Aut}_{\Lambda/\mathrm{R}} = \mathrm{G}_2$. Hence, we just have to check that the map of Isom-schemes

$$\mathrm{Isom}(\Lambda_{\mathrm{R}}, \mathrm{A}) \rightarrow \mathrm{Isom}(\mathrm{Aut}_{\Lambda_{\mathrm{R}}/\mathrm{R}}, \mathrm{Aut}_{\mathrm{A}/\mathrm{R}})$$

is an isomorphism. By working étale-locally on R and using Theorem B.5 we may assume $\mathrm{A} = \Lambda_{\mathrm{R}}$, in which case the isomorphism assertion amounts to the fact that G_2 is its own automorphism scheme via conjugation action. □

Appendix C

An explicit Chevalley group of type E_6

As is explained in the main text, the proof of Proposition 6.5 reduces to the analogue for the closed **Z**-subgroup scheme $\underline{\mathscr{G}}_0 = \mathrm{Aut}_{(\underline{\mathrm{M}}_0, \underline{\delta})/\mathbf{Z}} \subset \mathrm{GL}(\underline{\mathrm{M}}_0)$ defined in terms of the Tits model for exceptional Jordan algebras over **Z**. Its **Q**-fiber has been seen to be a simply connected semisimple group of type E_6. Our aim is to show that $\underline{\mathscr{G}}_0$ is a Chevalley group over **Z**. It is hard to see (especially locally at 2 and 3) that this **Z**-group is flat or has connected fibers.

We first record a lemma concerning the behavior of certain roots and their associated coroots under smooth degeneration of a reductive group over the fraction field of a discrete valuation ring. This lemma will be applied to a smooth group scheme that is *not* known to be affine.

Lemma C.1. — *Let* R *be a discrete valuation ring with fraction field* K *and residue field k, and let* G *be a locally closed smooth* R*-subgroup of some* GL_n*. Assume* G_K *is connected reductive and* G_k *is connected. Let* $\mathrm{T} \subset \mathrm{G}$ *be a closed split* R*-subtorus that is fiberwise maximal, and consider the weight space decomposition*

$$\mathfrak{g} = \mathfrak{t} \oplus (\oplus_{a\in\Phi}\, \mathfrak{g}_a)$$

over R *for the* T*-action on* $\mathfrak{g}$*, where* $\Phi := \Phi(\mathrm{G}_\mathrm{K}, \mathrm{T}_\mathrm{K})$*.*

Let $a \in \Phi \subset \mathrm{X}(\mathrm{T}_\mathrm{K}) = \mathrm{X}(\mathrm{T})$ *be a root such that the* R*-line* $[\mathfrak{g}_a, \mathfrak{g}_{-a}] \subset \mathfrak{t}$ *is saturated. Using the natural identifications* $\mathrm{X}_*(\mathrm{T}_\mathrm{K}) = \mathrm{X}_*(\mathrm{T}) = \mathrm{X}_*(\mathrm{T}_{\overline{k}})$ *and likewise for character groups,* $a_{\overline{k}}$ *occurs in* $\Phi(\mathrm{G}_{\overline{k}}/\mathscr{R}_u(\mathrm{G}_{\overline{k}}), \mathrm{T}_{\overline{k}})$ *and its associated coroot is* $(a^\vee)_{\overline{k}}$*.*

The saturatedness hypothesis can fail; an example with residue characterisic 0 is the relative identity component of the degeneration of PGL_2 to a connected solvable group in [**SGA3**, XIX, § 5].

Proof. — We may and do assume $k = \overline{k}$. Let $\mathrm{T}_a \subset \mathrm{T}$ be the unique R-subtorus of relative codimension 1 that is killed by a. (It corresponds to the quotient of $\mathrm{X}(\mathrm{T})/\mathbf{Z}a$ by its torsion subgroup.). Although G might not be affine, for any closed R-subtorus $\mathrm{S} \subset \mathrm{G}$ the scheme-theoretic centralizer $\mathrm{Z}_\mathrm{G}(\mathrm{S})$ exists as a smooth closed R-subgroup scheme of G. Indeed, for affine G this is a standard fact (see [**SGA3**, XI, 5.3] or [**Co2**, 2.2.4]), and more generally $\mathrm{G} \cap \mathrm{Z}_{\mathrm{GL}_n}(\mathrm{S})$ represents the centralizer functor. To check that this intersection is R-smooth, we first note that smoothness of its fibers is clear by the theory for smooth connected affine groups over fields, so the problem is to prove R-flatness of $\mathrm{Z}_\mathrm{G}(\mathrm{S})$ in general. By the local flatness criterion, it suffices to check on infinitesimal closed fibers over Spec(R). But these infinitesimal fibers are affine, so smoothness over the artinian quotients of R follows from the known affine case (over any base ring).

Let $\mathrm{U} = \mathscr{R}_u(\mathrm{G}_k)$. The R-group $\mathrm{Z}_\mathrm{G}(\mathrm{T}_a)$ has connected fibers (see [**Bor**, 11.12]) and the scheme-theoretic intersection $\mathrm{Z}_\mathrm{G}(\mathrm{T}_a)_k \cap \mathrm{U}$ is smooth since it is the centralizer for the natural T_a-action on the smooth affine k-group U, so $\mathrm{Z}_\mathrm{G}(\mathrm{T}_a)_k \cap \mathrm{U} = \mathscr{R}_u(\mathrm{Z}_\mathrm{G}(\mathrm{T}_a)_k)$ by [**Bor**, 13.17, Cor. 1(a)] (which gives equality on geometric points). Hence, the map

$$\mathrm{Z}_\mathrm{G}(\mathrm{T}_a)_k/(\mathrm{Z}_\mathrm{G}(\mathrm{T}_a)_k \cap \mathrm{U}) = (\mathrm{Z}_\mathrm{G}(\mathrm{T}_a)_k \cdot \mathrm{U})/\mathrm{U} \to \mathrm{G}_k/\mathrm{U}$$

is a closed k-subgroup inclusion that contains T_k and has Lie algebra coinciding with $\mathrm{Lie}(\mathrm{G}_k/\mathrm{U})^{\mathrm{T}_a}$. Consequently, we may replace G with $\mathrm{Z}_\mathrm{G}(\mathrm{T}_a)$ to reduce to the case $\Phi(\mathrm{G}_\mathrm{K}, \mathrm{T}_\mathrm{K}) = \{\pm a\}$.

Let $\mathfrak{u} = \mathrm{Lie}(\mathrm{U})$. Clearly $\mathfrak{u}$ is a T_k-stable subspace of

$$\mathfrak{g}_k = (\mathfrak{g}_k)_a \oplus (\mathfrak{g}_k)_{-a} \oplus \mathfrak{t},$$

and $\mathfrak{u} \cap \mathfrak{t}_k = 0$ since $\mathrm{U} \cap \mathrm{T}_k = 1$ scheme-theoretically, so by consideration of weight space decompositions with respect to T_k we see that $\mathfrak{u} \subset (\mathfrak{g}_k)_a \oplus (\mathfrak{g}_k)_{-a}$. The quotient $\mathfrak{g}_k/\mathfrak{u} = \mathrm{Lie}(\mathrm{G}_k/\mathrm{U})$ is the Lie algebra of a connected reductive k-group with maximal torus T_k, so its set of nontrivial T_k-weights is stable under negation. Hence, the same holds for $\mathfrak{u}$.

By hypothesis $[\mathfrak{g}_a, \mathfrak{g}_{-a}]$ is a saturated R-line inside $\mathfrak{t}$, so inside the special fiber $\mathfrak{g}_k$ the 1-dimensional Lie subalgebras $(\mathfrak{g}_k)_{\pm a}$ have commutator equal to a line in $\mathfrak{t}_k$. Hence, the lines $(\mathfrak{g}_k)_{\pm a}$ cannot both lie in $\mathfrak{u}$. This leaves only the option $\mathfrak{u} = 0$, which is to say $\mathrm{U} = 1$. In other words, G_k is connected reductive. (If we permit ourselves to apply the remarkable [**SGA3**, XVI, 5.2(i)], the relatively affine hypothesis in the definition of a reductive group scheme can be relaxed to "separated and finitely presented" and hence G is a reductive R-group, so we would be done. We prefer to avoid invoking that deep result, and so will proceed without it via more elementary methods.)

Clearly $\Phi(\mathrm{G}_k, \mathrm{T}_k) = \{\pm a\}$ via the identification $\mathrm{X}(\mathrm{T}_k) = \mathrm{X}(\mathrm{T}_\mathrm{K})$, and we have an associated coroot $(a_k)^\vee \in \mathrm{X}_*(\mathrm{T}_k) = \mathrm{X}(\mathrm{T}_\mathrm{K})$ that we need to show is equal to $(a^\vee)_k$. Since GL_n is a smooth affine R-group and T_a is a closed R-subtorus, the quotient sheaf $\mathrm{GL}_n/\mathrm{T}_a$ for the étale topology on the category of R-schemes is represented by a finite type affine R-scheme and the map $\mathrm{GL}_n \to \mathrm{GL}_n/\mathrm{T}_a$ is a T_a-torsor for the étale topology. (See [**SGA3**, VIII, Thm. 5.1] or [**Oes**, III, § 2.3].) By étale descent for locally closed immersions, it follows that the central quotient R-group $\overline{\mathrm{G}} := \mathrm{G}/\mathrm{T}_a$ exists as an R-smooth locally closed subscheme of the affine R-scheme $\mathrm{GL}_n/\mathrm{T}_a$, and $\overline{\mathrm{G}}$ is R-smooth since G is R-smooth.

The separated finite type smooth R-group $\overline{\mathrm{G}}$ has $\overline{\mathrm{T}} := \mathrm{T}/\mathrm{T}_a$ as a closed fiberwise maximal R-subtorus, and its Lie algebra $\overline{\mathfrak{g}}$ is equal to $\mathfrak{g}_a \oplus \overline{\mathfrak{t}} \oplus \mathfrak{g}_{-a}$. On the fibers over K and k the formation of coroots attached to roots of connected reductive groups is compatible with the formation of *central* quotients. Thus, to prove that $(a^\vee)_k = (a_k)^\vee$ it suffices to focus attention on the pair $(\overline{\mathrm{G}}, \overline{\mathrm{T}})$.

Since $\overline{\mathrm{T}}$ has 1-dimensional fibers over Spec(R), a cocharacter of T is determined by its pairing against the character a. In particular, since $\langle a_\mathrm{K}, (a_\mathrm{K})^\vee \rangle = 2 = \langle a_k, (a_k)^\vee \rangle$, the cocharacter $a^\vee$ of T over R extending $(a_\mathrm{K})^\vee$ has k-fiber $(a_k)^\vee$. □

Here is the main result of this appendix.

Theorem C.2. — *The* **Z**-*group* $\underline{\mathscr{G}}_0$ *is simply connected and semisimple of type* E_6.

Proof. — Letting $\mu \subset (\mathrm{SL}_3)^3$ be the diagonally embedded μ_3, consider the **Z**-homomorphism

$$j : (\mathrm{SL}_3)^3/\mu \hookrightarrow \underline{\mathscr{G}}_0 \subset \mathrm{GL}(\underline{\mathrm{M}}_0) \tag{C.1}$$

as defined in [**GY05**, § 3]:

$$j(g_1, g_2, g_3) : (u, v, w) \mapsto (g_2 u g_3^{-1}, g_3 v g_1^{-1}, g_1 w g_2^{-1}).$$

An fppf-local computation shows that $\ker j = 1$, so j is a closed immersion because any monomorphism of group functors from a reductive group scheme to an affine group scheme of finite presentation is a closed immersion (see [**SGA3**, XVI, 1.5(a)] or [**Co2**, Thm. 5.3.5]).

Let the closed **Z**-subtorus $\underline{\mathscr{T}}_0 \subset \underline{\mathscr{G}}_0$ be the image under (C.1) of the product of the diagonal tori in the SL_3's, so its **Q**-fiber $\underline{\mathrm{T}}_0$ is a split maximal **Q**-torus in the 78-dimensional **Q**-fiber $\underline{\mathrm{G}}_0 = (\underline{\mathscr{G}}_0)_{\mathbf{Q}}$ of type E_6. A tedious but elementary fppf-local computation in $\mathrm{GL}(\underline{\mathrm{M}}_0)$ using weight spaces in $\underline{\mathrm{M}}_0$ and the cubic form $\underline{\delta}$ shows that $\underline{\mathscr{T}}_0$ is its own scheme-theoretic centralizer in $\underline{\mathscr{G}}_0$. This will be used in our proof that $\underline{\mathscr{G}}_0$ has connected fibers over $\mathrm{Spec}(\mathbf{Z})$.

Denote the union of the bases of the root systems for the SL_3's in (C.1) relative to their diagonal tori and upper unipotent subgroups as

$$\mathrm{I} \subset \mathrm{X}(\underline{\mathscr{T}}_0) = \mathrm{X}(\underline{\mathrm{T}}_0). \tag{C.2}$$

This set lies in a unique positive system of roots $\Phi^+ \subset \Phi := \Phi(\underline{\mathrm{G}}_0, \underline{\mathrm{T}}_0)$, and it consists of the roots associated to non-central vertices of the extended diagram for the E_6 root system Φ with respect to Φ^+.

There are two 27-dimensional fundamental representations for E_6, swapped by the nontrivial outer (i.e., diagram) automorphism. By inspection of the highest $\underline{\mathrm{T}}_0$-weight on $(\underline{\mathrm{M}}_0)_{\mathbf{Q}}$ relative to our choice of Φ^+, the representation $(\underline{\mathrm{M}}_0)_{\mathbf{Q}}$ is a 27-dimensional fundamental representation of the split simply connected semisimple **Q**-group $\underline{\mathrm{G}}_0$ of type E_6.

Lemma C.3. — *The fibers $(\underline{\mathscr{G}}_0)_{\mathbf{F}_p}$ are smooth of dimension* 78.

Proof. — Let $\underline{e}_0 \in \underline{\mathscr{G}}_0(\mathbf{Z})$ denote the identity section. The cubic form $\underline{\delta}$ is given by an explicit formula (6.6), so preservation of $\underline{\delta}$ on $\mathbf{Z}[\varepsilon]$-points yields explicit elements in the cotangent space $\underline{e}_0^*(\Omega^1_{\mathrm{GL}(\underline{\mathrm{M}}_0)/\mathbf{Z}}) = \mathfrak{gl}(\underline{\mathrm{M}}_0)^* = \mathfrak{gl}_{27}^*$ over **Z** such that the quotient by their **Z**-span is the cotangent space $\underline{e}_0^*(\Omega^1_{\underline{\mathscr{G}}_0/\mathbf{Z}})$. By computation (see [**Yu**]), the span of this set of linear forms over **Z** is saturated in the **Z**-dual of $\mathfrak{gl}(\underline{\mathrm{M}}_0)$, so $\underline{e}_0^*(\Omega^1_{\underline{\mathscr{G}}_0/\mathbf{Z}})$ is a finite free **Z**-module. Hence, its linear dual $\mathrm{Lie}(\underline{\mathscr{G}}_0)$ is a free module whose formation commutes with any base change.

The flat closure in $\underline{\mathscr{G}}_0$ of the generic fiber $\underline{\mathrm{G}}_0$ is a **Z**-flat closed subgroup scheme. By **Z**-flatness, the fibers of this closed subgroup scheme over $\mathrm{Spec}(\mathbf{Z})$ all have the same dimension, and this common dimension (namely, $\dim(\underline{\mathrm{G}}_0) = 78$) is a lower bound on the dimension of the fibers of $\underline{\mathscr{G}}_0$ over $\mathrm{Spec}(\mathbf{Z})$. But we just saw that the Lie algebra of every fiber has dimension equal to the dimension for the smooth **Q**-fiber, so $\dim(\underline{\mathscr{G}}_0)_{\mathbf{F}_p} \geqslant \dim \mathrm{Lie}((\underline{\mathscr{G}}_0)_{\mathbf{F}_p})$ for every prime p. The opposite inequality always holds, so we are done. □

Since the **Q**-fiber of $\underline{\mathscr{G}}_0$ is geometrically connected, so are the fibers at all but finitely many primes. Hence, the union of the fibral identity components of $\underline{\mathscr{G}}_0$ is a (possibly non-affine) open **Z**-subgroup scheme $\underline{\mathscr{G}}_0^0 \subset \underline{\mathscr{G}}_0$, and it is **Z**-flat by Lemma B.13, so it is **Z**-smooth. However, it does not follow formally from these properties that $\underline{\mathscr{G}}_0$ is **Z**-smooth, as it might fail to be **Z**-flat in the presence of disconnected fibers. (As an illustration of what can go wrong, the reduced closed **Z**-subgroup of $\mathrm{SL}_n \times (\mathbf{Z}/2\mathbf{Z})_{\mathbf{Z}}$ obtained by removing the open subscheme of $\mathrm{SL}_n \times \{1\}_{\mathbf{Z}}$ away from a single positive characteristic p is a non-flat affine finite type **Z**-group that coincides with SL_n over $\mathbf{Z}[1/p]$ and has smooth disconnected $\mathbf{F}_p$-fiber.)

The $\underline{\mathscr{T}}_0$-action on the finite free **Z**-module $\mathfrak{g} := \mathrm{Lie}(\underline{\mathscr{G}}_0) = \mathrm{Lie}(\underline{\mathscr{G}}_0^0)$ decomposes $\mathfrak{g}$ as a direct sum of weight spaces whose ranks and weights can be read off from the **Q**-fiber. Hence, the saturated submodule $\mathrm{Lie}(\underline{\mathscr{T}}_0) \subset \mathfrak{g}$ coincides with $\mathfrak{g}^{\underline{\mathscr{T}}_0}$ and for each $a \in \Phi$ there is a rank-1 weight space $\mathfrak{g}_a \subset \mathfrak{g}$ such that

$$\mathfrak{g} = \mathrm{Lie}(\underline{\mathscr{T}}_0) \oplus (\oplus_{a\in\Phi}\, \mathfrak{g}_a).$$

Thus, for any prime p, the line $(\mathfrak{g}_a)_{\mathbf{F}_p}$ is the a-weight space in $\mathfrak{g}_{\mathbf{F}_p}$ via the natural identification of the character groups of $\underline{\mathrm{T}}_0$ and $(\underline{\mathscr{T}}_0)_{\mathbf{F}_p}$. Note that the $\mathbf{F}_p$-torus $(\underline{\mathscr{T}}_0)_{\mathbf{F}_p}$ is maximal in $(\underline{\mathscr{G}}_0)_{\mathbf{F}_p}$ because its weight-0 space in $\mathfrak{g}_{\mathbf{F}_p}$ is $\mathrm{Lie}(\underline{\mathscr{T}}_0)_{\mathbf{F}_p} = \mathrm{Lie}((\underline{\mathscr{T}}_0)_{\mathbf{F}_p})$ (or because $\underline{\mathscr{T}}_0$ is its own scheme-theoretic centralizer in $\underline{\mathscr{G}}_0$).

Lemma C.4. — *For any field k of characteristic $p > 0$, the identity component of $(\underline{\mathscr{G}}_0)_k$ is a simple semisimple group of type* E_6.

Proof. — We may assume k is algebraically closed. Let $\mathrm{G} = (\underline{\mathscr{G}}_0)_k$, $\mathrm{T} = (\underline{\mathscr{T}}_0)_k$, $\mathrm{U} = \mathscr{R}_u(\mathrm{G}) = \mathscr{R}_u(\mathrm{G}^0)$, and $\mathfrak{u} = \mathrm{Lie}(\mathrm{U})$. Since $\mathrm{Lie}(\mathrm{T}) = \mathfrak{g}_k^{\mathrm{T}}$, the T-weights that occur on $\mathfrak{u}$ are nontrivial.

Since $\mathfrak{g}_k/\mathfrak{u}$ is the Lie algebra of the connected reductive k-group G^0/U containing T as a maximal torus, the set of nontrivial T-weights supported on this quotient is stable under negation. The same therefore holds for $\mathfrak{u}$.

Let Δ be the basis of Φ^+ and choose $a \in \Delta$ that is not a central vertex in the Dynkin diagram (i.e., a also lies in the set I from (C.2)). The closed **Z**-subgroup (C.1) provides a closed **Z**-subgroup $\mathrm{SL}_2 \subset \mathrm{SL}_3 \subset \underline{\mathscr{G}}_0$ whose **Z**-fiber is generated by the $\pm a_{\mathbf{Q}}$-root groups for $(\underline{\mathrm{G}}_0, \underline{\mathrm{T}}_0)$. This SL_2 meets $\underline{\mathscr{T}}_0$ in the diagonal **Z**-subgroup $\underline{\mathrm{D}} \subset \mathrm{SL}_2$ and has Lie algebra $\mathfrak{sl}_2 \subset \mathfrak{g}$ over **Z** equal to $\mathfrak{g}_{-a} \oplus \mathrm{Lie}(\underline{\mathrm{D}}) \oplus \mathfrak{g}_a$ with $\mathfrak{g}_{\pm a}$ equal to the $\underline{\mathrm{D}}$-root spaces in $\mathfrak{sl}_2$. Hence, the root spaces $\mathfrak{g}_{\pm a}$ have commutator equal to the *saturated* **Z**-line $\mathrm{Lie}(\underline{\mathrm{D}}) \subset \mathfrak{sl}_2 \subset \mathrm{Lie}(\underline{\mathscr{T}}_0)$. By applying Lemma C.1 to $(\underline{\mathscr{G}}_0^0, \underline{\mathscr{T}}_0)_{\mathbf{Z}_{(p)}}$, a cannot occur as a T-weight in $\mathfrak{u}$ and the coroot for a_k with respect to $(\mathrm{G}^0/\mathrm{U}, \mathrm{T})$ equals the k-fiber $(a^\vee)_k$ of the coroot $a^\vee$ via the natural identification $\mathrm{X}_*(\underline{\mathrm{T}}_0) = \mathrm{X}_*(\underline{\mathscr{T}}_0) = \mathrm{X}_*(\mathrm{T})$.

Thus, up to sign, the only possibilities for T-weights on $\mathfrak{u}$ are the roots in Φ^+ whose expansion in the basis Δ involves the simple positive root a_0 corresponding to the central vertex in the extended Dynkin diagram. Since $\Phi(\mathrm{G}^0/\mathrm{U}, \mathrm{T})$ contains the set I of roots corresponding to the non-central vertices in the extended diagram of type E_6, $\Phi(\mathrm{G}^0/\mathrm{U}, \mathrm{T})$ rationally spans the character group of T. Hence, the connected reductive group G^0/U is semisimple.

We are going to compute the root datum for $(\mathrm{G}^0/\mathrm{U}, \mathrm{T})$ and see that it agrees with the one attached to the $\mathbf{Q}$-fiber $(\underline{\mathrm{G}}_0, \underline{\mathrm{T}}_0)$. This would imply that the connected semisimple group G^0/U is simple of type E_6, and then dimension considerations force $\mathrm{U} = 1$.

Our task is to show $\Phi(\mathrm{G}^0/\mathrm{U}, \mathrm{T})$ admits Δ as a basis and that $(a^\vee)_k$ is the coroot attached to a_k for each $a \in \Delta$. We have already seen that $\Delta - \{a_0\} \subset \Phi(\mathrm{G}^0/\mathrm{U}, \mathrm{T})$, and that if $a \in \Delta - \{a_0\}$ then the coroot attached to a_k is the k-fiber of $a^\vee$. The remaining task is to analyze a_0.

A computation (see [**Yu**]) shows that for $\mathbf{Z}$-basis elements $\mathrm{X}_\pm$ of $\mathfrak{g}_{\pm a_0} \subset \mathfrak{gl}(\underline{\mathrm{M}}_0)$,

$$[\mathrm{X}_+, \mathrm{X}_-] = \pm \mathrm{Lie}(a_0^\vee(\partial_t|_{t=1})).$$

This is part of a $\mathbf{Z}$-basis of $\mathrm{Lie}(\underline{\mathscr{T}}_0)$ since no coroots are divisible in the dual of the root lattice for type E_6. Hence, $[\mathfrak{g}_{a_0}, \mathfrak{g}_{-a_0}]$ is a saturated $\mathbf{Z}$-line in $\mathfrak{g}$, so Lemma C.1 applied to $(\underline{\mathscr{G}}_0^0, \underline{\mathscr{T}}_0)_{\mathbf{Z}_{(p)}}$ ensures that $a_0 \in \Phi(\mathrm{G}^0/\mathrm{U}, \mathrm{T})$ and $(a_0)_k$ has coroot $(a_0^\vee)_k$. In particular, Δ is a basis of $\Phi(\mathrm{G}^0/\mathrm{U}, \mathrm{T})$ (see [**Bou**, VI, § 1.7, Cor. 3 to Prop. 20]), so we are done. □

It remains to show that the geometric closed fibers of $\underline{\mathscr{G}}_0 \to \mathrm{Spec}(\mathbf{Z})$ are connected. For an algebraically closed field k of characteristic $p > 0$, consider the smooth fiber $\mathrm{G} := (\underline{\mathscr{G}}_0)_k$ and its maximal torus $\mathrm{T} := (\underline{\mathscr{T}}_0)_k$. By Lemma C.4, G^0 is simple and semisimple of type E_6. The action of G on G^0 is classified by a k-homomorphism $f : \mathrm{G} \to \mathrm{Aut}_{\mathrm{G}^0/k}$ to the automorphism scheme of G^0. The closed subgroup scheme $\ker f \subset \mathrm{G}$ centralizes G^0 and hence centralizes T. Since $\underline{\mathscr{T}}_0$ is its own scheme-theoretic centralizer in $\underline{\mathscr{G}}_0$, T is its own scheme-theoretic centralizer in G (not just in G^0). Thus, $\ker f \subset \mathrm{T} \subset \mathrm{G}^0$, so G is disconnected if and only if f maps onto $\mathrm{Out}_{\mathrm{G}^0/k} = \mathbf{Z}/2\mathbf{Z}$.

We have to rule out the existence of $g \in \mathrm{G}(k)$ whose action on G^0 is via a nontrivial outer automorphism. Assume such a g exists. Its action on the representation space $(\underline{\mathrm{M}}_0)_k$ gives an isomorphism between the semisimplified k-fiber of a 27-dimensional fundamental representation of E_6 and its twist under a nontrivial outer automorphism. Thus, the sets of T-weights (with multiplicity) occuring in these representations coincide. This equality is a characteristic-free assertion in character groups of maximal tori, from which it follows that a 27-dimensional fundamental representation of E_6 in characteristic 0 is isomorphic to its twist by the nontrivial outer automorphism of E_6. Since there is no such isomorphism in characteristic 0, there is no such g. □

References

[A] M. Aschbacher, *The* 27*-dimensional module for* E_6*.* I, Inv. Math. **89** (1987), pp. 159-195.

[AT] E. Artin, J. Tate, *Class field theory*, AMS Chelsea, Providence, 2009.

[BLG] P. A. Bjerregaard, O. Loos, C. M. González, *Derivations and automorphisms of Jordan algebras in characteristic two*, Journal of Algebra **285** (2005), pp. 146–181.

[vdBS] F. van der Blij, T. Springer, *The arithmetic of octaves and the group* G_2, Indag. Math, **21** (1959), pp. 406–418.

[Bor] A. Borel, *Linear algebraic groups*, Springer–Verlag, New York, 1991.

[Brv] M. Borovoi, *Galois cohomology of real reductive groups and real forms of simple Lie algebras*, Funct. Anal. **22** (1988), pp. 135–136.

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Springer–Verlag, New York, 1990.

[Bou] N. Bourbaki, *Lie groups and Lie algebras* (Ch. 4–6), Springer–Verlag, New York, 2002.

[BT] F. Bruhat, J. Tits, *Groupes algébrique sur un corps local. III.*, J. Fac. Univ. Tokyo, Sect. IA **34** (1987), pp. 671–698.

[Chev61] C. Chevalley, *Certains schémas de groupes semi-simples*, Sém. Bourbaki **219**, 1960/61, 219–234.

[Chev97] C. Chevalley, *The algebraic theory of spinors*, Springer–Verlag, 1997.

[BIBLE] C. Chevalley, *Classification des groupes algébriques semi-simples* (avec la collaboration de P. Cartier, A. Grothendieck, M. Lazard), Collected Works, volume 3, Springer–Verlag, 2005.

[Co1] B. Conrad, *Finiteness theorems for algebraic groups over function fields*, Compsitio Math. **148** (2012), pp. 555-639.

[Co2] B. Conrad, *Reductive group schemes*, these Proceedings.

[CS] J.H. Conway, N.J.A. Sloan, *Low-dimensional lattices* IV*. The mass formula*, Proc. of the Royal Soc. of London, Series A **419** (1988), pp. 259–286.

[ATLAS] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *ATLAS of finite groups* (1st ed.), Claredon Press, Oxford, 1985.

[DGr] P. Deligne, B. Gross, *On the exceptional series and its descendants*, C. Rendus Acad. Sci. Paris **335** (2002), pp. 877-881.

[SGA7] P. Deligne, N. Katz, *Groupes de monodromie en géométrie algébrique* II, LNM 340, Springer–Verlag, New York, 1973.

[DGa] M. Demazure, P. Gabriel, *Groupes algébriques*, Masson & North–Holland, 1970.

[SGA3] M. Demazure, A. Grothendieck, *Schémas en groupes* I, II, III, Lecture Notes in Math **151, 152, 153**, Springer-Verlag, New York, 1970.

[Ear] A.G. Earnest, *Minimal discriminants of indefinite ternary quadratic forms having a specified class number*, Mathematika **35** (1988), no. 1, pp. 95–100.

[EG96] N. Elkies, B. Gross, *The exceptional cone and the Leech lattice*, IMRN **14** (1996), pp. 665–698.

[EG97] N. Elkies, B. Gross, *Embeddings into the integral octonions*, Pacific J. Math **181** (1997), Issue 3: Olga Tausky Memorial Issue, pp. 147–158.

[GY03] W. Gan, J.-K. Yu, *Schémas en groupes et immeubles des groupes exceptionnels sur un corps local. Première partie: Le groupe* G_2, Bull. Soc. Math. France **131** (2003), pp. 307–358.

[GY05] W. Gan, J.-K. Yu, *Schémas en groupes et immeubles des groupes exceptionnels sur un corps local. Deuxième partie: Les groupes* F_4 *et* E_6, Bull. Soc. Math. France **133** (2005), pp. 159–196.

[G96] B. Gross, *Groups over* **Z**, Invent. math. **124** (1996), pp. 263–279

[G99] B. Gross, *On simply connected groups over* **Z** *with* $\mathrm{G}(\mathbf{R})$ *compact*, in "Integral Quadratic Forms and Lattices", Contemp. Math. **249** (1999), pp. 113–118.

[GS] B. Gross, G. Savin, *Motives with Galois group of type* G_2*: an exceptional theta correspondence*, Compositio Math. **114** (1998), no. 2, pp. 153–217.

[EGA] A. Grothendieck, *Eléments de Géométrie Algébrique*, Publ. Math. IHES **4, 8, 11, 17, 20, 24, 28, 32**, 1960–7.

[BrIII] A. Grothendieck, *Le groupe de Brauer III: exemples et compléments*, in "Dix Exposés sur la cohomologie des schémas", North-Holland, Amsterdam, 1968, pp. 88–188.

[Ha] G. Harder, *Halbeinfache Gruppenschemata über Dedekindringen*, Inv. Math. **4** (1967), pp. 165–191.

[HM] D. Husemöller, J. Milnor, *Symmetric bilinear forms*, Ergebnisse der Mathematik und ihrer Grenzgebiete **73**, Springer–Verlag, New York, 1973.

[Kn] A. Knapp, *Lie groups: beyond an introduction* (2nd ed.), Birkhauser, New York, 2002.

[Knus] M-A. Knus, *Quadratic and hermitian forms over rings*, Grundlehren der mathematischen Wissenschaften **294**, Springer–Verlag, New York, 1991.

[Knut] D. Knutson, *Algebraic spaces*, Lecture Notes in Math. **203**, Springer-Verlag, New York, 1971.

[Kru] S. Krutelevich *On the canonical form of a* 3 *by* 3 *Hermitian matrix over the ring of split octonions* J. Algebra **253** (2002), pp. 276–295.

[Loos] O. Loos, *On algebraic groups defined by Jordan pairs*, Nagoya Math J. **74** (1979), pp. 23–66.

[McC] K. McCrimmon, *Non-associative algebras with scalar involution*, Pacific Journal of Math., **116** (1985), pp. 85–109.

[Mil] J. Milne, *Étale cohomology*, Princeton Math Series **33**, Princeton Univ. Press, Princeton, 1980.

[Oes] J. Oesterlé, *Groupes de type multiplicatif et sous-tores des schémas en groupes*, these Proceedings.

[PR] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics **139**, Academic Press, 1994.

[Pras] G. Prasad, *Strong approximation for semisimple groups over function fields*, Annals of Math **105**, no. 3 (1977), pp. 553–572.

[PY06] G. Prasad, J-K. Yu, *On quasi-reductive group schemes*, Journal of Algebraic Geometry **15**(2006), 507–549.

[S73] J.-P. Serre, *A course in arithmetic*, Springer–Verlag GTM **7**, 1973.

[S79] J-P. Serre, *Local fields*, Springer–Verlag GTM **67**, 1979.

[S97] J.-P. Serre, *Galois cohomology*, Springer–Verlag, New York, 1997.

[Sp] T. Springer, *Jordan algebras and algebraic groups*, Springer–Verlag, New York, 1973.

[Spr] T. A. Springer, *Linear algebraic groups* (2nd ed.), Birkhäuser, New York, 1998.

[SV] T. Springer, F. Veldkamp, *Octonions, Jordan algebras, and exceptional groups*, Springer Monographs in Mathematics, Springer–Verlag, New York, 2000.

[T1] J. Tits, "Classification of algebraic semisimple groups" in *Algebraic groups and discontinuous groups*, Proc. Symp. Pure Math. **9**, AMS, 1966, pp. 33–62.

[T2] J. Tits, *Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque*, J. reine ang. Math. **247** (1971), pp. 196–220.

[Yu] J.-K. Yu, Mathematica code for computation with semisimple groups of type F_4 and E_6 over **Z**, including justification of correctness, freely available at `http://math.stanford.edu/~conrad/Zgpcode.pdf`.

April 7, 2014

Brian Conrad, Math Dept., Stanford University, Stanford, CA 94305, USA
E-mail : `conrad@math.stanford.edu` • *Url :* `http://smf.emath.fr/`