NON-SPLIT REDUCTIVE GROUPS OVER Z

BRIAN CONRAD AND BENEDICT H. GROSS

Introduction

The work of Chevalley ([BIBLE], [Chev61]) and Demazure–Grothendieck [SGA3] provides a satisfactory understanding of the reasons for the existence and uniqueness of "Chevalley groups" over $\mathbf{Z}$. These are the reductive $\mathbf{Z}$-groups that admit a maximal $\mathbf{Z}$-torus (necessarily split: [Con, B.2.6]), and by the Isomorphism Theorem over $\mathbf{Z}$ such groups up to isomorphism correspond to the isomorphism classes of root data. (Many authors require Chevalley groups to be semisimple; this is a matter of convention.)

In view of the Existence Theorem over $\mathbf{Z}$ and $\mathbf{Q}$, the generic fibers of Chevalley groups are precisely the split connected reductive groups over $\mathbf{Q}$ and so are also characterized up to isomorphism by such root data. In particular, if two Chevalley groups over $\mathbf{Z}$ have isomorphic $\mathbf{Q}$-fibers then they are isomorphic over $\mathbf{Z}$. The isomorphism result is not as strong as for Néron models of abelian varieties over $\mathbf{Q}$: if $\mathscr{G}$ and $\mathscr{G}'$ are Chevalley groups then it is not true in general that isomorphisms between their $\mathbf{Q}$-fibers extend to isomorphisms over $\mathbf{Z}$. This is already seen for $\mathscr{G} = \mathscr{G}' = \mathrm{SL}_2$: $\mathrm{Aut}_{\mathbf{Q}}(\mathrm{SL}_2) = \mathrm{PGL}_2(\mathbf{Q})$ but $\mathrm{Aut}_{\mathbf{Z}}(\mathrm{SL}_2) = \mathrm{PGL}_2(\mathbf{Z})$.

There are semisimple $\mathbf{Z}$-groups that are not Chevalley groups. Loosely speaking, these correspond to semisimple $\mathbf{Q}$-groups with "good reduction" at all primes (but non-split over $\mathbf{R}$; see Remark 1.5). Unlike in the split case, in general there exist non-isomorphic semisimple $\mathbf{Z}$-groups with isomorphic $\mathbf{Q}$-fibers (as we shall see in some explicit examples). The aim of these notes is to discuss the theory and examples related to the $\mathbf{Q}$-groups that arise as generic fibers of reductive $\mathbf{Z}$-groups that are not Chevalley groups. (By [Con, 7.3.9], such $\mathbf{Q}$-groups must be non-split since $\mathrm{Pic}(\mathbf{Z}) = 1$.)

In §1 we describe the possibilities for the generic fibers of reductive $\mathbf{Z}$-groups, with an emphasis on the case of semisimple groups whose geometric fibers are absolutely simple and simply connected (and we show that case accounts for the rest via direct products and central isogenies). Then in §2 we introduce Coxeter's order in Cayley's definite octonion algebra over $\mathbf{Q}$, and we use it in §3 to describe examples over $\mathbf{Z}$. Finally, in §4 we explain how to use mass formulas to prove in some cases that the list of $\mathbf{Z}$-models found in §3 for certain $\mathbf{Q}$-groups is exhaustive.

Date: October 27, 2011.

BC was supported by NSF grant DMS-0917686 and BHG was supported by NSF grant DMS-0901102.

1. The generic fiber

We begin by considering the generic fiber of a reductive group $\mathscr{G}$ over $\mathbf{Z}$, and show that it is split over $\mathbf{Q}_p$ for all primes p, and is an inner form of a split group over $\mathbf{R}$. In fact, we will show that $\mathscr{G}$ is split over $\mathbf{Z}_p$ for all primes p and is a pure inner form of a split group over $\mathbf{R}$. More details on what follows can be found in [G96] (and references therein).

Let $\mathscr{G}_0$ be the split form of $\mathscr{G}$ over $\mathbf{Z}$, and let $G = \mathscr{G}_{\mathbf{Q}}$ and $G_0 = (\mathscr{G}_0)_{\mathbf{Q}}$, so G_0 is the split form of G over $\mathbf{Q}$. Let $c(G) \in \mathrm{H}^1(\mathbf{Q}, \mathrm{Aut}_{G_0/\mathbf{Q}})$ denote the class of G as in [Con, 7.1.1], and let $d(G)$ be the image of this class in $\mathrm{H}^1(\mathbf{Q}, \mathrm{Out}_{G_0/\mathbf{Q}})$, where $\mathrm{Out}_{G_0/\mathbf{Q}}$ denotes the étale group $\mathrm{Aut}_{G_0/\mathbf{Q}}/(G_0/Z)$ that is the quotient of $\mathrm{Aut}_{G_0/\mathbf{Q}}$ modulo its identity component G_0/Z, with $Z := Z_{G_0}$. This quotient is a constant group over $\mathbf{Q}$ associated to the automorphism group $\mathrm{Aut}(R, \Delta)$ of the based root datum (R, Δ) for G_0 (equipped with a choice of a split maximal $\mathbf{Q}$-torus T_0 and Borel subgroup $B_0 \supset T_0$; all pairs (T_0, B_0) are $G_0(\mathbf{Q})$-conjugate to each other) [Con, 7.1.9]. Here, Δ is a choice of base of R (or equivalently, a choice of positive system of roots; these choices are permuted simply transitively by $W(R) = W(G_0, T_0) = N_{G_0}(T_0)(\mathbf{Q})/T_0(\mathbf{Q})$), and $\mathrm{Aut}(R, \Delta)$ is finite if and only if G_0 is semisimple.

Lemma 1.1. *The class $d(G)$ is trivial.*

Proof. We give two versions of the proof, one using cohomological considerations over $\mathbf{Z}$ and the other using more traditional Galois-theoretic considerations over fields. First we work over $\mathbf{Z}$. Since $\mathrm{Out}_{\mathscr{G}_0/\mathbf{Z}}$ is the constant $\mathbf{Z}$-group associated to $\mathrm{Aut}(R, \Delta)$ (compatibly with the analogous such identification for G_0 over $\mathbf{Q}$), by functoriality relative to $\mathrm{Spec}\,\mathbf{Q} \to \mathrm{Spec}\,\mathbf{Z}$ we see that $d(G)$ arises from a class $d(\mathscr{G})$ in the cohomology set

$$\mathrm{H}^1(\mathbf{Z}, \mathrm{Out}_{\mathscr{G}_0/\mathbf{Z}}) = \mathrm{Hom}(\pi_1(\mathbf{Z}), \mathrm{Aut}(R, \Delta))/\text{conjugacy}.$$

But $\pi_1(\mathbf{Z})$ is trivial (Hermite–Minkowski), so $d(G) = 1$.

To give a proof working more directly over $\mathbf{Q}$, note that $d(G)$ is a conjugacy class of homomorphisms from $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ into $\mathrm{Aut}(R, \Delta)$, so to prove its trivial it suffices (again, by Hermite–Minkowski) to show that $d(G)$ is unramified at all rational primes p. In other words, it suffices to show that the local class $d_p(G) \in \mathrm{H}^1(\mathbf{Q}_p, \mathrm{Aut}(R, \Delta))$ 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 [Con, 5.2.14]. Hence, G splits over a finite unramified extension of $\mathbf{Q}_p$, so $d_p(G)$ is unramified for all p. $\square$

The preceding argument really shows that the class $c(\mathscr{G}) \in \mathrm{H}^1(\mathbf{Z}, \mathrm{Aut}_{\mathscr{G}_0/\mathbf{Z}})$ has trivial image in $\mathrm{H}^1(\mathbf{Z}, \mathrm{Out}_{\mathscr{G}_0/\mathbf{Z}})$, so $\mathscr{G}$ an inner form of $\mathscr{G}_0$ over $\mathbf{Z}$. That is, $c(\mathscr{G})$ arises from a class in $\mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0/\mathscr{Z})$, where $\mathscr{Z} = Z_{\mathscr{G}_0}$. This implies that $\mathscr{G}$ is split over $\mathbf{Z}_p$ (hence G is split over $\mathbf{Q}_p$) for all primes p. Indeed, since $\mathscr{G}$ is an inner form of $\mathscr{G}_0$ over $\mathbf{Z}_p$, $c(\mathscr{G})$ comes from $\mathrm{H}^1(\mathbf{Z}_p, \mathscr{G}_0/\mathscr{Z})$, and this cohomology set vanishes. (Proof: any torsor over $\mathbf{Z}_p$ for a smooth group scheme has a $\mathbf{Z}_p$-point if it has an $\mathbf{F}_p$-point. The existence of an $\mathbf{F}_p$-point for any $\mathscr{G}_0/\mathscr{Z}$-torsor follows from Lang's theorem for homogeneous spaces under smooth connected groups over finite fields [Bor, 16.5(i)].)

Remark 1.2. The splitting property for $\mathscr{G}$ over $\mathbf{Z}_p$ is actually equivalent to the splitting property for G over $\mathbf{Q}_p$ (see [Con, Exer. 7.3.9]).

By [Con, 5.3.1, 5.3.3], there is a unique central isogeny $\mathscr{T} \times \mathscr{G}' \to \mathscr{G}$ over $\mathbf{Z}$, where $\mathscr{T}$ is the maximal central $\mathbf{Z}$-torus in $\mathscr{G}$ and the $\mathbf{Z}$-group $\mathscr{G}'$ is a semisimple normal $\mathbf{Z}$-subgroup of $\mathscr{G}$ (the derived group). All $\mathbf{Z}$-tori are split, since $\operatorname{Spec} \mathbf{Z}$ is a connected normal noetherian scheme and $\pi_1(\operatorname{Spec} \mathbf{Z}) = 1$ (see [Con, B.2.6]). 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, as we now do.

Taking $\mathscr{G}$ to be a semisimple $\mathbf{Z}$-group, by [Con, Exer. 6.5.3] there exists a unique central isogeny $\widetilde{\mathscr{G}} \to \mathscr{G}$ with $\widetilde{\mathscr{G}}$ a simply connected semisimple $\mathbf{Z}$-group. By [Con, 6.4.4], any fiberwise nontrivial simply connected semisimple group over a scheme S is a Weil restriction $\mathrm{R}_{S'/S}(H)$ for a finite étale cover $S' \to S$ and a simply connected semisimple S'-group H whose fibers $H_{s'}$ are *absolutely simple.* In the case $S = \operatorname{Spec} \mathbf{Z}$, necessarily S' is a disjoint union of copies of $\operatorname{Spec} \mathbf{Z}$ (once again, by the result of Hermite and Minkowski that $\pi_1(\operatorname{Spec} \mathbf{Z}) = 1$). Thus, the $\mathbf{Z}$-group $\widetilde{\mathscr{G}}$ decomposes as a direct product $\prod \mathscr{G}_i$ where each $\mathscr{G}_i$ is a simply connected semisimple $\mathbf{Z}$-group whose geometric fibers are absolutely simple. We shall therefore concentrate on the description of the connected semisimple $\mathbf{Q}$-groups G that are absolutely simple, simply connected, and split over $\mathbf{Q}_p$ for all rational primes p. (In §3 we will address the construction of explicit $\mathbf{Z}$-models.) Our shift in attention to such G over $\mathbf{Q}$ does not lose contact with the existence of a good integral structure:

Lemma 1.3. *Let H be a connected semisimple $\mathbf{Q}$-group that is absolutely simple, simply connected, and split over $\mathbf{Q}_p$ for all p. Then there exists a semisimple $\mathbf{Z}$-group $\mathscr{H}$ such that $H \simeq \mathscr{H}_{\mathbf{Q}}$.*

Note that typically $\mathscr{H}$ is not uniquely determined. We will exhibit explicit examples of such non-uniqueness later.

Proof. By direct limit arguments (viewing $\mathbf{Q}$ is a direct limit of its finitely generated $\mathbf{Z}$-subalgebras $\mathbf{Z}[1/d]$), we can extend H to a smooth affine group with connected fibers over some $\operatorname{Spec} \mathbf{Z}[1/N]$. Since the generic fiber H is semisimple, by openness of the locus of semisimple fibers [Con, 3.1.9(1), 3.1.12] this group has semisimple restriction over some dense open locus $\operatorname{Spec} \mathbf{Z}[1/M] \subset \operatorname{Spec} \mathbf{Z}[1/N]$ (with $M \in N\mathbf{Z}$). For each prime p dividing M, a split $\mathbf{Z}_p$-model of the split $\mathbf{Q}_p$-fiber specifies a $\mathbf{Z}_{(p)}$-model for G [BLR, 6.2/D.4(b)]. These finitely many local models glue to the $\mathbf{Z}[1/M]$-model to define a semisimple group over $\mathbf{Z}$ with generic fiber G (cf. the proof of [BLR, 1.4/1]). $\square$

Over any number field k (where Hermite–Minkowski is no longer available), any connected reductive k-group H that splits at all finite places must be an inner form of the split group H_0 of the same type. Indeed, this amounts to the triviality of the associated class in $\mathrm{H}^1(k, \operatorname{Aut}(R, \Delta))$ (where (R, Δ) is the based root datum of H_0), and a continuous homomorphism from $\operatorname{Gal}(\overline{k}/k)$ into a discrete group is trivial if it is locally trivial at all finite places (since any finite Galois group over a number field is generated by its decomposition groups at the finite places, by a weak form of the Chebotarev Density Theorem). Hence, even without recourse to special properties of $\mathbf{Z}$, our splitting hypothesis on G at all finite places forces it to be an inner form of G_0 over $\mathbf{Q}$.

Beware that over a general field k, the restriction map

$$\mathrm{H}^1(k, H_0/Z_{H_0}) \to \mathrm{H}^1(k, \mathrm{Aut}_{H_0/k})$$

can *fail* to be injective (but it has trivial kernel as a map of pointed sets, due to the semi-direct product structure $\mathrm{Aut}_{H_0/k} \simeq (H_0/Z_{H_0}) \rtimes \mathrm{Out}_{H_0/k}$ [Con, 7.1.6]). Examples are given in [Con, Exer. 7.3.3(iii)] over any global field. Explicitly, if $H_0 = \mathrm{SL}_n$ for $n > 1$ then $H_0/Z_{H_0} \to \mathrm{Aut}_{H_0/k}$ is the natural map $\mathrm{PGL}_n \to \mathrm{Aut}_{\mathrm{SL}_n/k}$ defined by the conjugation action of $\mathrm{PGL}_n = \mathrm{GL}_n/\mathbf{G}_m$, and the induced map on H^1's carries the n-torsion Brauer class of a rank-n^2 central simple algebra A over k to the isomorphism class of the k-group $\mathrm{SL}_1(A)$ of units of A with reduced norm 1. But if A is not 2-torsion in the Brauer group (e.g., A is a division algebra over a global or non-archimedean local field and $n > 2$) then the opposite algebra A^{opp} defines a different n-torsion Brauer class from that of A but their associated k-groups $\mathrm{SL}_1(A^{\mathrm{opp}}) = \mathrm{SL}_1(A)^{\mathrm{opp}}$ and $\mathrm{SL}_1(A)$ are k-isomorphic (via inversion).

Thus, as a general rule, the isomorphism type for G retaining how it is an "inner form" of G_0 can involve more information than the isomorphism type of G as an abstract linear algebraic group over $\mathbf{Q}$ (i.e., as a mere "form" of G_0). One can ask if such non-injectivity may occur over $\mathbf{Q}$ when using only classes that are split at all finite places, as these are the only such classes of interest to us. To avoid a significant digression into the general classification of forms of semisimple groups over fields, we will not address the matter here except to say that the trickiest case is E_6. (Since the split simply connected group G_0 of type E_6 has center μ_3, for non-archimedean local k we get a natural connecting map $\mathrm{H}^1(k, G_0/Z_{G_0}) \to \mathrm{H}^2(k, \mu_3) = \mathrm{Br}(k)[3] = \mathbf{Z}/3\mathbf{Z}$. This is bijective, and the two non-trivial classes yield the same form of E_6 in $\mathrm{H}^1(k, \mathrm{Aut}_{G_0/k})$; it has k-rank 2 and relative root system of type G_2.)

Our main interest is just to make an exhaustive list of possibilities over $\mathbf{Q}$, so we are content to work in $\mathrm{H}^1(\mathbf{Q}, G_0/Z)$ rather than with its image in $\mathrm{H}^1(\mathbf{Q}, \mathrm{Aut}_{G_0/\mathbf{Q}})$. More specifically, since G *does* extend to some semisimple $\mathbf{Z}$-group $\mathscr{G}$ (by Lemma 1.3), it follows from Lemma 1.1 that the class $c(G) \in \mathrm{H}^1(\mathbf{Q}, \mathrm{Aut}_{G_0/\mathbf{Q}})$ lifts to a class $c'(G) \in \mathrm{H}^1(\mathbf{Q}, G_0/Z)$ that arises from $\mathrm{H}^1(\mathbf{Z}, \mathscr{G}_0/\mathscr{Z})$. It follows from Lang's theorem that $c'(G)$ is split at all finite places (just like $c(G)$, by hypothesis on the $\mathbf{Q}$-group G). We aim to describe all possibilities for such $c'(G)$, which is to say that we fix a realization of G as an inner form of G_0 over $\mathbf{Q}$ that is split *as an inner form* over each $\mathbf{Q}_p$.

The Hasse principle for adjoint semisimple groups [PR, Thm. 6.22] says that the map of pointed sets

$$\mathrm{H}^1(\mathbf{Q}, G_0/Z) \to \prod_v \mathrm{H}^1(\mathbf{Q}_v, G_0/Z)$$

is injective (not just that it has trivial kernel!), so the class $c'(G) \in \mathrm{H}^1(\mathbf{Q}, G_0/Z)$ is determined completely by the class $c'_\infty(G)$ in $\mathrm{H}^1(\mathbf{R}, G_0/Z)$ (since the local classes $c'_p(G)$ are all trivial). In particular, $c'_\infty(G)$ determines the $\mathbf{Q}$-isomorphism class of G (as this isomorphism class is the image of $c'(G)$ in $\mathrm{H}^1(\mathbf{Q}, \mathrm{Aut}_{G_0/\mathbf{Q}})$). For example, if $c'_\infty(G) = 1$ then $G \simeq G_0$ as $\mathbf{Q}$-groups. We have an exact sequence of pointed sets

$$\mathrm{H}^1(\mathbf{R}, Z) \to \mathrm{H}^1(\mathbf{R}, G_0) \to \mathrm{H}^1(\mathbf{R}, G_0/Z) \overset{\delta_\infty}{\to} \mathrm{H}^2(\mathbf{R}, Z).$$

Since the center Z of the absolutely simple $\mathbf{Q}$-group G_0 is isomorphic to μ_n or to $\mu_2 \times \mu_2$ (by inspection of the classification of irreducible root systems), the determination of the Brauer group of $\mathbf{Q}$ shows that the image $\delta_\infty(c'_\infty(G))$ in $\mathrm{H}^2(\mathbf{R}, Z)$ is trivial. Indeed, the sum of the local invariants of a global division algebra must be zero, and $\delta_p(c'_p(G))$ is clearly the trivial class for all primes p. Hence, the class $c'_\infty(G)$ (which we have seen determines the isomorphism class of the group G over $\mathbf{Q}$) is in the image of $\mathrm{H}^1(\mathbf{R}, G_0)$, which is to say that G is a pure inner form of G_0 over $\mathbf{R}$.

Remark 1.4. The pointed set $\mathrm{H}^1(\mathbf{R}, G_0)$ is finite, and can be computed using methods of Serre [S97, Ch. III, §4.5] and Borovoi [Brv]. Here we simply describe which real simple groups G occur.

For types A and C, the Galois cohomology sets $\mathrm{H}^1(\mathbf{R}, \mathrm{SL}_n)$ and $\mathrm{H}^1(\mathbf{R}, \mathrm{Sp}_{2n})$ both reduce to a single element, and there are no non-split examples. In the orthogonal case, for type B we have the groups $\mathrm{Spin}(r, s)$ where $r - s \equiv \pm 1 (\mathrm{mod}\ 8)$ and for type D we have the groups $\mathrm{Spin}(r, s)$ where $r - s \equiv 0 (\mathrm{mod}\ 8)$.

For G_2 one gets both real forms, of real ranks 0 and 2, and for F_4 one gets all three real forms of ranks 0, 1, and 4. For E_6 one gets the real inner forms of ranks 2 and 6 and for E_7 the real forms of ranks 3 and 7. Finally, for E_8 one gets all three real forms, of ranks 0, 4, and 8.

Remark 1.5. We can refine the assertion that $G \simeq G_0$ over $\mathbf{Q}$ if the inner form class $c'_\infty(G) \in \mathrm{H}^1(\mathbf{R}, G_0/Z)$ over $\mathbf{R}$ is trivial: if the $\mathbf{Q}$-group G that is split at all finite places of $\mathbf{Q}$ is also split over $\mathbf{R}$ then G is $\mathbf{Q}$-isomorphic to G_0 (i.e., split over $\mathbf{Q}$). Indeed, it suffices to show that the map $\mathrm{H}^1(\mathbf{R}, G_0/Z) \to \mathrm{H}^1(\mathbf{R}, \mathrm{Aut}_{G_0/\mathbf{Q}})$ has trivial kernel, and this holds because $\mathrm{Aut}_{G_0/\mathbf{Q}}(\mathbf{R}) \to \mathrm{Out}_{G_0/\mathbf{Q}}(\mathbf{R})$ is surjective.

More generally, the same reasoning shows that if G is a connected reductive group over a global field k and it splits at all places of k then it is k-split. To explain this, first note that the everywhere-local splitting property is inherited by the maximal central torus as well as by the semisimple derived group, so it suffices to separately treat the cases when G is a torus or when G is semisimple. The torus case is clear (as its splitting field over k is split at all places of k and hence equals k), so we may assume that G is semisimple and even simply connected (by consideration of the simple connected central cover).

Let G_0 be the split simply connected k-group of the same type as G. The class $c(G) \in \mathrm{H}^1(k, \mathrm{Aut}_{G_0/k})$ has trivial image in $\mathrm{H}^1(k, \mathrm{Out}_{G_0/k}) = \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(k_s/k), \mathrm{Aut}(R(G), \Delta))$, so $c(G)$ is the image of a class $c'(G) \in \mathrm{H}^1(k, G_0/Z_{G_0})$. For every place v of k, the local class $c'_v(G) \in \mathrm{H}^1(k_v, G_0/Z_{G_0})$ has trivial image in $\mathrm{H}^1(k_v, \mathrm{Aut}_{G_0/k})$ and hence is trivial (since $\mathrm{Aut}_{G_0/k}(k_v) \to \mathrm{Out}_{G_0/k}(k_v)$ is surjective for all v). Thus, by the Hasse principle for adjoint semisimple k-groups, $c'(G) = 1$ and hence $c(G) = 1$ as desired.

The Hasse principle for simply connected semisimple groups over number fields [PR, Thm. 6.6] and the theorem of Kneser–Bruhat–Tits on the vanishing of $\mathrm{H}^1(\mathbf{Q}_p, G_0)$ [PR, Thm. 6.4] imply that the natural map of pointed sets $\mathrm{H}^1(\mathbf{Q}, G_0) \to \mathrm{H}^1(\mathbf{R}, G_0)$ is injective. But this archimedean localization map is also surjective [PR, Prop. 6.17] (as is also the case for any connected linear algebraic group over $\mathbf{Q}$), so it is actually bijective. Hence, for each of the real forms described in Remark 1.4, there exists a unique connected semisimple $\mathbf{Q}$-group G that becomes this form over $\mathbf{R}$ and is split over $\mathbf{Q}_p$ for all rational primes p. Such G arise as the generic fiber of a simply connected semisimple $\mathbf{Z}$-group $\mathscr{G}$ (Lemma 1.3), but there may be more than one such $\mathscr{G}$ up to isomorphism as a $\mathbf{Z}$-group (as we shall see in some later examples).

In the above classification of the generic fibers of simply connected semisimple groups over $\mathbf{Z}$ with absolutely simple fibers, we have used the triviality of both the fundamental group $\pi_1(S)$ and the Brauer group $\mathrm{H}^2(S, \mathbf{G}_m)$ for $S = \operatorname{Spec} \mathbf{Z}$. These groups need not be trivial for $S = \operatorname{Spec} A$ when A is the ring of integers in a number field k, and that makes the description of the generic fibers of reductive groups over A more involved.

2. Coxeter's integral octonions

To provide examples of non-split semisimple groups over $\mathbf{Z}$, we will introduce one remarkable integral structure: Coxeter's integral order R in Cayley's definite octonions (cf. [EG98, §1]). The automorphism scheme of R is the unique group of type G_2 over $\mathbf{Z}$ that is compact over $\mathbf{R}$. What is even more striking is that the order R can be used to construct integral reductive models for all of the other simple non-split real groups described in Remark 1.4.

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

$$\mathbf{O} = \mathbf{Q}.1 + \mathbf{Q}.e_1 + ... + \mathbf{Q}.e_7$$

with the multiplication law given by

$$e_i^2 = -1,$$
$$e_i.e_{i+1}.e_{i+3} = -1,$$

where in the last identity the subscript is calculated modulo 7 and the multiplication is associative. This gives seven copies of Hamilton's rational quaternion algebra $\mathbf{H}$ 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

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

The automorphism scheme $G = \mathrm{Aut}_{\mathbf{O}/\mathbf{Q}}$ of this algebra is the form of G_2 over $\mathbf{Q}$ that is compact over $\mathbf{R}$ and split over $\mathbf{Q}_p$ for all rational primes p. To make a reductive group over $\mathbf{Z}$ with generic fiber G, we will construct an order R in $\mathbf{O}$ with the property that R/pR is an octonion algebra over $\mathbf{Z}/p\mathbf{Z}$, for all primes p. The obvious order

$$S = \mathbf{Z}.1 + \mathbf{Z}.e_1 + ... + \mathbf{Z}.e_7$$

enjoys this property for all primes except $p = 2$.

We obtain a maximal order R containing S by choosing an index $i \bmod 7$ and adjoining the Hurwitz elements in the three quaternion algebras which contain e_i. For example, if $i = 1$, we adjoin to 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 R containing S with $R/S \simeq (\mathbf{Z}/2\mathbf{Z})^4$. An additional additive generator is

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

This is Coxeter's integral order R. For future reference, we note that the element

$$\alpha = (1 + e_1 + e_2 .... + e_7)/2 = h_1 + h_2 + h_3 - (1 + e_1)$$

lies in R.

The anti-involution of **O** which is defined by $e_i^* = -e_i$ stabilizes R, and the trace and norm

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

take integral values on R. Every element of R satisfies a monic integral quadratic polynomial: $a^2 - \mathrm{Tr}(a).a + \mathrm{N}(a) = 0$. For example, α satisfies the quadratic equation $\alpha^2 - \alpha + 2 = 0$. The integral symmetric bilinear form

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

is even, unimodular, and positive-definite on R, so the underlying lattice is the E_8 root lattice. The submodule R_0 of elements of trace zero is isomorphic to the E_7 root lattice.

Finally, since multiplication in R is trace-associative, an integral 3-form on R may be defined by

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

This 3-form is alternating on the sublattice R_0, so it induces a map $\wedge^3 R_0 \to \mathbf{Z}$.

3. The construction of some non-split examples

If G is the generic fiber of a reductive group over $\mathbf{Z}$, then all of the irreducible representations $G \to \mathrm{GL}(V)$ are defined over $\mathbf{Q}$. This fact, which is derived in [G96, Prop. 1.2] from work of Tits [T], suggests a method of construction of integral forms of G as follows. An integral structure on $\mathrm{GL}(V)$ is obtained by choosing a lattice L in V. For certain representations, the subgroup G of $\mathrm{GL}(V)$ is characterized by its invariants of small degree in the tensor algebra on V and its dual (cf. [DG]). If these tensors can be defined integrally on L and are suitably non-degenerate on L/pL for all primes p, then subgroup preserving the lattice L with its integral tensors will be a model for G over $\mathbf{Z}$. To illustrate this method, we first consider some semisimple $\mathbf{Q}$-groups that are not simply connected, and then we pass to their simply connected central covers.

For type D_n, let V be the standard representation of dimension $2n$. This representation is orthogonal, and the quotient $G/\mu_2 = \mathrm{SO}(V)$ is equal to the subgroup of $\mathrm{SL}(V)$ which preserves the symmetric bilinear form. Over $\mathbf{R}$, we have shown that the signature of V is (r, s) with $r \equiv s \bmod 8$ (cf. [S73, Ch. V, Cor. 1]). This, and the fact that the space V is split over $\mathbf{Q}_p$ for all primes p, determines the orthogonal space V over $\mathbf{Q}$, and hence the group $\mathrm{SO}(V)$.

Example 3.1. Suppose that $r = s + 8k$ with $k \geq 0$. We can construct an integral model for $\mathrm{O}(V)$ as the stabilizer of the even unimodular lattice $L = s.H + k.\mathrm{E}_8$, where H is a hyperbolic plane over $\mathbf{Z}$ and E_8 is the positive-definite root lattice underlying Coxeter's integral octonions. As is explained in [Con, App. C] for fiberwise non-degenerate quadratic forms over any ring, the $\mathbf{Z}$-group $\mathrm{O}(L)$ is smooth over $\mathbf{Z}[1/2]$ with disconnected fibers and to define its semisimple identity component $\mathrm{SO}(L)$ over $\mathbf{Z}$ (and not just over $\mathbf{Z}[1/2]$) we cannot simply use the determinant, but need to work with the even Clifford algebra (cf. [Con, App. C]).

When $s > 0$, $\mathrm{SO}(L)$ is the unique integral model of $\mathrm{SO}(V)$ up to isomorphism. When $s = 0$, so the bilinear form on V is positive-definite, the even unimodular lattices in V other than $L = k.\mathrm{E}_8$ are enumerated by the Minkowski–Siegel mass formula (cf. [S73, Ch. V, 2.3]).

A similar construction works for the adjoint group of type B_n, using the standard orthogonal representation V of dimension $2n + 1$. We take G to be the group $\mathrm{SO}(V)$ of points in $\mathrm{SL}(V)$ preserving the symmetric bilinear form. This bilinear form has signature (r, s) over $\mathbf{R}$ with $r \equiv s \pm 1 \bmod 8$, and it is split over $\mathbf{Q}_p$ for all primes p, so G is split over every $\mathbf{Q}_p$.

Example 3.2. Suppose, for example, that $r = s + 8k - 1$ with $k \geq 1$. Then we can construct an integral model for $\mathscr{O}(V)$ as the stabilizer of the even lattice $L = s.H + (k-1).\mathrm{E}_8 + \mathrm{E}_7$ of determinant ± 2. This group is not smooth in characteristic 2, but decomposes over $\mathbf{Z}$ as a product of μ_2 and an integral form of $\mathrm{SO}(V)$.

The simply connected groups of type B and D can be constructed over $\mathbf{Z}$ using the Clifford algebras of the above orthogonal lattices L. Since the resulting $\mathbf{Q}$-groups are split at all finite primes p, one finds that the associated central simple algebras over $\mathbf{Q}$ (the Clifford algebra for type B, and the even Clifford algebra for type D) are matrix algebras.

To construct models of the simply connected simple exceptional groups $\mathrm{G}_2, \mathrm{D}_4, \mathrm{F}_4, \mathrm{E}_6, \mathrm{E}_7$ and E_8 over $\mathbf{Z}$, we use distinguished lattices L in their simplest representations V, of dimensions 7, 24, 26, 27, 56, and 248 [G96, §4]. To verify that the models are indeed smooth with connected reductive fibers is a local problem. In the cases discussed below, this can be resolved by appealing to the work of Gan and Yu ([GY03], [GY05]), who gave an explicit construction (via lattices) of the buildings of the simply connected exceptional groups of type G_2, D_4, F_4, and E_6.

Example 3.3. The automorphism scheme $G = \mathrm{Aut}_{R/\mathbf{Z}}$ is a non-split group of type G_2 over $\mathbf{Z}$, with $G(\mathbf{R})$ compact. The lattice in the 7-dimensional representation V is $L = R_0$, with its symmetric bilinear form and alternating trilinear form defined over $\mathbf{Z}$.

Example 3.4. We will now construct a model of the simply connected non-split group G of type D_4 over $\mathbf{Z}$ which exhibits triality ($\mathrm{Out}_{G/\mathbf{Z}} \simeq S_3$). To do this, we use the direct sum V of the three orthogonal 8-dimensional representations of G to obtain a faithful representation of dimension 24. We can identify V with the direct sum $\mathbf{O} \oplus \mathbf{O} \oplus \mathbf{O}$, and

$$G = \{(a, b, c) \in \mathrm{SO}(\mathbf{O})^3 \mid \mathrm{Tr}(xyz) = \mathrm{Tr}(a(x)b(y)c(z))\}$$

is the subgroup of $\mathrm{SO}(\mathbf{O})^3$ preserving the trilinear form $\mathrm{Tr}(xyz)$ on the direct sum (recall that multiplication in $\mathbf{O}$ is trace-associative). To obtain an integral model, we consider the stabilizer of the lattice $L = R^3 \subset \mathbf{O}^3$ with its four integral tensors of degree 2 and 3.

Example 3.5. To construct integral models for the groups of type F_4, we first treat the case of the non-split group of type E_6. The minuscule representation V of dimension 27 for the inner form G of E_6 which has rank 2 over $\mathbf{R}$ and is split at all finite primes p is given by the action on the vector space V of 3×3 Hermitian symmetric matrices over $\mathbf{O}$:

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

The group G is the subgroup of $\mathrm{SL}(V)$ which preserves the cubic form

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

The stabilizer of the lattice $L \subset V$ where a, b, c are in $\mathbf{Z}$ and x, y, z are in R gives an integral form of G. Moreover, each non-split group of type F_4 is a subgroup of G which stabilizes an element E in V with $\det(E) = 1$.

There are three orbits of $G(\mathbf{Z})$ on such elements in L. They are represented by the matrices:

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

where we recall that $\alpha = (1 + e_1 + e_2 + ... + e_7)/2$. The first gives an integral model for the form of F_4 of rank 1 over $\mathbf{R}$, and the second two matrices are positive-definite and give integral models for the form of F_4 which is anisotropic over $\mathbf{R}$.

4. Counting the integral models

The models of the simply connected groups of type G_2, D_4, F_4, and E_6 that we have constructed in the previous section exhaust the possible non-split forms of these groups over $\mathbf{Z}$. In the case of E_6, where the real group has rank 2, this follows from the theorem of strong approximation [PR, Thm. 7.12]. In the other cases, where the real group is compact, we need to use the mass formula [G96, (5.1)],[G98]:

$$\sum 1/\#G_i(\mathbf{Z}) = \prod \frac{1}{2}\zeta(1-d_j).$$

The sum on the left side of this identity is taken over the different integral models and $G_i(\mathbf{Z})$ is the corresponding finite group. The product on the right side 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. In the case when $G(\mathbf{R})$ is compact, these degrees are all even, and hence the values of the Riemann zeta function $\zeta(1-d_j)$ are non-zero rational numbers.

Example 4.1. For G_2 we have identified one integral model using the automorphisms of Coxeter's order in the octonions. The finite group $G(\mathbf{Z}) = \mathrm{Aut}_{\mathbf{Z}}(R)$ has order $12096 = 2^6 3^3 7$, and is isomorphic to $\mathrm{G}_2(\mathbf{Z}/2\mathbf{Z})$ under reduction modulo 2. On the other hand, the degrees of the invariants for the Weyl group of G_2 are 2 and 6, and we have

$$\frac{1}{2}\zeta(-1) \times \frac{1}{2}\zeta(-5) = 1/2^6 3^3 7.$$

Hence there exists a unique model of G_2 over $\mathbf{Z}$ which is compact over $\mathbf{R}$.

Example 4.2. The integral form of D_4 that we have described has $G(\mathbf{Z}) = G(\mathbf{Z}/2\mathbf{Z}) = 2^2.\mathrm{O}_8^+(2)$ of order $2^{14}3^5 5^2 7$. In this case, the degrees of the invariants for the Weyl group are 2, 4, 4, and 6. Since

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

we have identified the unique model over $\mathbf{Z}$ which is compact over $\mathbf{R}$.

Example 4.3. The case of F_4 is more interesting. Here the invariants for the Weyl group have degrees 2, 6, 8 and 12 and we find the mass is equal to

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

and there must be more than one integral model. The two positive-definite, Hermitian symmetric, 3×3 matrices of determinant 1 over R

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

give integral forms G_i of F_4 inside E_6.

The finite groups $G_i(\mathbf{Z})$ inject modulo 2 onto the subgroups $2^2.\mathrm{O}_8^+(2).S_3$ and ${}^3\mathrm{D}_4(2).3$ of $\mathrm{F}_4(2)$ respectively. These two finite groups have orders $2^{15}3^6 5^2 7$ and $2^{12}3^5 7^2 13$. Since

$$691/2^{15}3^6 5^2 7^2 13 = 1/2^{15}3^6 5^2 7 + 1/2^{12}3^5 7^2 13$$

there are precisely two integral models. The model stabilizing the matrix E acts on a positive-definite even, integral lattice L of rank 26 and determinant 3 with no roots [EG96, §8]. The corresponding lattice for the model stabilizing I is $L = \mathrm{E}_8 + \mathrm{E}_8 + \mathrm{E}_8 + \mathrm{A}_2$.

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 $(d-1)!/(2\pi i)^d$. For G of type E_8 with $G(\mathbf{R})$ compact, the degrees d_j of the 8 generating invariants are 2, 8, 12, 14, 18, 20, 24, and 30. The corresponding product of the values $\frac{1}{2}\zeta(1-d_j)$ is approximately 13934.49. Hence there are at least 13935 models for E_8 over $\mathbf{Z}$. Each model determines a positive-definite, even integral lattice L of rank 248 with an alternating 3-form $\wedge^3 L \to \mathbf{Z}$ inside the adjoint representation of G. It seems likely that most models will have $G(\mathbf{Z}) = 1$. If so, it would be interesting to determine the others. Some examples were constructed in [G96, §7].

References

[Bor] A. Borel, *Linear algebraic groups*, Spirnger–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. 63–64

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

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

[BIBLE] C. Chevalley, *Classification des groupes algébriques semi-simples* (with Cartier, Grothendieck, Lazard), Collected Works, volume 3, Springer–Verlag, 2005.

[Con] B. Conrad, *Reductive group schemes* (SGA3 summer school, 2011).

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

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

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

[EG98] N. Elkies, B. Gross, *Embeddings into the integral octonions*, Pacific J. Math: Olga Tausky Memorial Issue (1998), pp. 147–158

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

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

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

[G98] B. Gross, *On simply connected groups over* **Z** *with* $G(\mathbf{R})$ *compact* in "Integral Quadratic Forms and Lattices Contemp. Math." **249** (1998), pp. 113–118.

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

[S73] J.-P. Serre *A course in arithmetic* Springer GTM **7** (1973).

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

[T] J. Tits, *Représentations linéaires irréducibles d'un groupe réductif sur un corps quelconque*, J. Crelle **247** (1971), pp. 196–220.