Available online at www.sciencedirect.com
ScienceDirect
Advances in Mathematics 207 (2006) 646–660
ADVANCES IN Mathematics
www.elsevier.com/locate/aim

On the existence of isotropic forms of semi-simple algebraic groups over number fields with prescribed local behavior

Gopal Prasad [a,*], Andrei S. Rapinchuk [b]

[a] *Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA*
[b] *Department of Mathematics, University of Virginia, Charlottesville, VA 22904, USA*

Received 26 July 2005; accepted 3 January 2006

Available online 17 February 2006

Communicated by Johan de Jong

Dedicated to Günter Harder

Abstract

This note is a follow-up on the paper [A. Borel, G. Harder, Existence of discrete cocompact subgroups of reductive groups over local fields, J. Reine Angew. Math. 298 (1978) 53–64] of A. Borel and G. Harder in which they proved the existence of a cocompact lattice in the group of rational points of a connected semi-simple algebraic group over a local field of characteristic zero by constructing an appropriate form of the semi-simple group over a number field and considering a suitable S-arithmetic subgroup. Some years ago A. Lubotzky initiated a program to study the subgroup growth of arithmetic subgroups, the current stage of which focuses on "counting" (more precisely, determining the asymptotics of) the number of lattices of bounded covolume (the finiteness of this number was established in [A. Borel, G. Prasad, Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups, Publ. Math. Inst. Hautes Études Sci. 69 (1989) 119–171; Addendum: Publ. Math. Inst. Hautes Études Sci. 71 (1990) 173–177] using the formula for the covolume developed in [G. Prasad, Volumes of S-arithmetic quotients of semi-simple groups, Publ. Math. Inst. Hautes Études Sci. 69 (1989) 91–117]). Work on this program led M. Belolipetsky and A. Lubotzky to ask questions about the existence of *isotropic* forms of semi-simple groups over number fields with prescribed local behavior. In this paper we will answer these questions. A question of similar nature also arose in the work [D. Morris, Real representations of semisimple Lie algebras have $\mathbb{Q}$-forms, in: Proc. Internat. Conf. on Algebraic Groups and Arithmetic, December 17–22, 2001, TIFR, Mumbai, 2001, pp. 469–490] of D. Morris (Witte) on a completely different topic. We will answer that question too.

* Corresponding author.
E-mail addresses: gprasad@umich.edu (G. Prasad), asr3x@virginia.edu (A.S. Rapinchuk).

0001-8708/$ – see front matter
doi:10.1016/j.aim.2006.01.001

Keywords: Forms of semi-simple algebraic groups; Galois cohomology

1. Introduction

This note is a follow-up on the paper [2] of A. Borel and G. Harder in which they proved the existence of a cocompact lattice in the group of rational points of a connected semi-simple algebraic group over a local field of characteristic zero by constructing an appropriate form of the semi-simple group over a number field and considering a suitable S-arithmetic subgroup. Some years ago A. Lubotzky [4] initiated a program to study the subgroup growth of arithmetic subgroups, the current stage of which focuses on “counting” (more precisely, determining the asymptotics of) the number of lattices of covolume $\leqslant c$ (the finiteness of this number was established in [3] using the formula for the covolume developed in [8]). Work on this program led M. Belolipetsky and A. Lubotzky to ask questions about the existence of *isotropic* forms of semi-simple groups over number fields with prescribed local behavior. The existence of an isotropic form is of course equivalent to the existence of an *irreducible* noncocompact lattice. Interestingly enough, a question of similar nature also came up in the work [5] of D. Morris (Witte) on a completely different topic. The goal of this note is to elaborate on the Galois cohomological techniques of [2] in order to prove a theorem that answers these questions.

In this note, K will denote an algebraic number field, and we let V^K (respectively V_r^K) denote the set of all (respectively real) places of K, and for a place v of K, K_v will denote the completion of K at v. Given a connected absolutely simple algebraic group G defined over K, we let $\Delta(G,K)$ denote the Tits index of G over K (cf. [10,11]), and let $\Delta(G,K)_d$ denote the set of distinguished (circled) vertices of $\Delta(G,K)$. Unless explicitly mentioned otherwise, $\overline{G}$ will denote the adjoint group of G which will be identified with the group $\mathrm{Int}\, G$ of inner automorphisms. Given a field extension P/K, a P-form of G that corresponds to an element of $H^1(P,\overline{G})$[1] will be called an *inner twist* of G (over P). An inner twist of a split group is called an *inner form*. A semi-simple group which is not an inner form is called an *outer form*. In this note, K-forms with prescribed local behavior will be constructed as inner twists of a given quasi-split group.

To formulate our main theorem, fix an absolutely simple simply connected algebraic group G_0 defined and quasi-split over (the number field) K. Let $\overline{G}_0$ be the adjoint group of G_0, and let T_0 be the centralizer of a maximal K-split torus of G_0 (then T_0 is a maximal K-torus of G_0). Let $\Omega_1,\dots,\Omega_r$ be the orbits of the $*$-action of the absolute Galois group $\mathcal{G}_K$ on $\Delta(G_0,K)$ (we recall that r coincides with the K-rank of G_0). Let L denote the minimal Galois extension of K over which G_0 splits (in other words, L is the extension of K that corresponds to the kernel of the action of $\mathcal{G}_K$ on $\Delta(G_0,K)$).

Theorem 1. *Fix a nonarchimedean $v_0 \in V^K$, and assume that for each $v \in V^K \setminus \{v_0\}$ we are given an inner twist $G^{(v)}$ of G_0 over K_v so that $G^{(v)}$ is quasi-split over K_v for all but finitely many v. Then*

[1] As usual, for an algebraic group H defined over a (perfect) field P, $H^i(P,H) = H^i_c(\mathcal{G}_P, H(\overline{P}))$ where $\mathcal{G}_P = \mathrm{Gal}(\overline{P}/P)$ is the absolute Galois group.

(i) *There exists an inner twist G of G_0 over K such that G is K_v-isomorphic to $G^{(v)}$ for all $v \neq v_0$.*

(ii) *A K-isotropic G with the property described in* (i) *can exist only if there is an $i \in \{1, 2, \dots, r\}$ such that*

$$\Omega_i \subset \Delta\big(G^{(v)}, K_v\big)_d \quad \text{for all } v \neq v_0, \tag{1}$$

and the K-rank of G cannot exceed the number of orbits satisfying (1).

(iii) *Assume that v_0* does not *split in L if L/K is a quadratic extension. Then the existence of $i \in \{1, 2, \dots, r\}$ satisfying* (1) *is sufficient for the existence of a K-isotropic form G as in* (i)*, and there exists a K-form whose K-rank is precisely the number of orbits satisfying* (1).

2. Results on Galois cohomology

Proposition 1. *Let H be a connected semi-simple algebraic K-group. Then for any nonarchimedean $v_0 \in V^K$, the map*

$$H^1(K, H) \longrightarrow \bigoplus_{v \neq v_0} H^1(K_v, H)$$

is surjective.

A proof is obtained by repeating verbatim the argument given in [2] to prove Theorem 1.7. It relies on the following lemma which is actually established in the proof of Proposition 1.6 of loc. cit., where the argument is attributed to J. Tate. The proofs of both, the preceding proposition and the following lemma, will be omitted here.

Lemma 1. *Let M be a finite commutative $\mathcal{G}_K$-module. Then for any nonarchimedean $v_0 \in V^K$, the map*

$$H^2(K, M) \longrightarrow \bigoplus_{v \neq v_0} H^2(K_v, M)$$

is surjective.

For convenience of later reference, we recall here the well-known exact sequence of global class field theory that connects the Brauer groups of K and of all the K_v's (this result is usually referred to as the Hasse–Brauer–Noether Theorem, cf. [1, Chapter VII, 9.6], or [6, §18.4] for details):

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_{v \in V^K} \mathrm{Br}(K_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0. \tag{HBN}$$

It follows from this that for any nonarchimedean $v_0 \in V^K$ the natural map

$$\mathrm{Br}(K) \longrightarrow \bigoplus_{v \neq v_0} \mathrm{Br}(K_v)$$

is an isomorphism. Another consequence is given in the following lemma which can be used in place of Lemma 1 to prove a variant of Theorem 1 in which v_0 is a real place, G_0 is K-split, and its center is either trivial or it is K-isomorphic to μ_2 or to $\mu_2 \times \mu_2$ (here, and in the sequel, for a positive integer n, μ_n denotes the kernel of the nth power map of GL_1 into itself).

Lemma 2. *If v_0 is a real place, the homomorphism*

$$H^2(K, \mu_2) \longrightarrow \bigoplus_{v \neq v_0} H^2(K_v, \mu_2)$$

is an isomorphism.

Proof. Since for any field extension P/K, $H^2(P, \mu_2) = \mathrm{Br}(P)_2$, and for all v, $H^2(K_v, \mu_2) = \mathbb{Z}/2\mathbb{Z}$, the claim immediately follows from (HBN). □

Next, we prove the following strengthening of Proposition 1.

Proposition 2. *Let H be a connected reductive K-group, and let Z be the central torus of H. Fix a nonarchimedean $v_0 \in V^K$. Then either of the following two conditions* (a) *Z is K-split, or* (b) *Z splits over a quadratic extension L/K and v_0 does not split in L, implies that the map*

$$H^1(K, H) \longrightarrow \bigoplus_{v \neq v_0} H^1(K_v, H)$$

is surjective.

We need the following.

Lemma 3. *Let Z be a K-torus and v_0 be a nonarchimedean place of K. Then under either of the conditions* (a) *and* (b) *stated in Proposition* 2*, the maps*

$$H^i(K, Z) \longrightarrow \bigoplus_{v \neq v_0} H^i(K_v, Z),$$

for $i = 1, 2$, are isomorphisms.

Proof. It is well known (cf., for example, [12]) that Z is isomorphic to $\prod_{j=1}^{d} Z_j$, where for $j \leqslant d$, Z_j is one of the following three tori:

$$T_1 = \mathrm{GL}_1, \quad T_2 = R_{L/K}(\mathrm{GL}_1) \quad \text{or} \quad T_3 = R^{(1)}_{L/K}(\mathrm{GL}_1).$$

So it is enough to prove our claim for each of these "elementary" tori T_j, using the assumption on v_0 if $j = 2$ or 3. For $T = T_1$ or T_2, by Hilbert's Theorem 90, we have $H^1(P, T) = \{1\}$ for any field extension P/K, so our assertion for $i = 1$ is immediate. Let $i = 2$. The maps $H^2(K, T_j) \to \bigoplus_{v \neq v_0} H^2(K_v, T_j)$ for $j = 1, 2$ are equivalent respectively to the maps

$$\mathrm{Br}(K) \longrightarrow \bigoplus_{v \neq v_0} \mathrm{Br}(K_v) \quad \text{and} \quad \mathrm{Br}(L) \longrightarrow \bigoplus_{w \notin W_0} \mathrm{Br}(L_w),$$

where W_0 is the set of all extensions of v_0 to L, and since by our assumption W_0 reduces to a single element, our assertion follows from (HBN).

The torus T_3 is the first term of the following short exact sequence

$$1 \longrightarrow T_3 \longrightarrow T_2 \xrightarrow{\nu_{L/K}} T_1 \longrightarrow 1, \tag{2}$$

where $\nu_{L/K}$ is the norm map from L to K. Then the map

$$H^1(K, T_3) \longrightarrow \bigoplus_{v \neq v_0} H^1(K_v, T_3)$$

is equivalent to the map

$$K^\times/\nu_{L/K}\big(L^\times\big) \xrightarrow{\rho} \bigoplus_{v \neq v_0} K_v^\times/\nu_{L_w/K_v}\big(L_w^\times\big)$$

(we pick one extension w for each $v \in V^K$). By class field theory, there is an exact sequence

$$0 \longrightarrow K^\times/\nu_{L/K}\big(L^\times\big) \longrightarrow \bigoplus_{v} K_v^\times/\nu_{L_w/K_v}\big(L_w^\times\big) \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

and $K_{v_0}^\times/\nu_{L_{w_0}/K_{v_0}}(L_{w_0}^\times) \simeq \mathbb{Z}/2\mathbb{Z}$, so the fact that ρ is an isomorphism follows. Finally, the assertion for $i = 2$ follows from the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^2(K, T_3) & \longrightarrow & H^2(K, T_2) & \longrightarrow & H^2(K, T_1) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \bigoplus_{v \neq v_0} H^2(K, T_3) & \longrightarrow & \bigoplus_{v \neq v_0} H^2(K, T_2) & \longrightarrow & \bigoplus_{v \neq v_0} H^2(K, T_1)
\end{array}$$

as the middle and the right vertical arrows are isomorphisms. □

Proof of Proposition 2. Let $\overline{H} = H/Z$. Then we have the following exact sequence:

$$1 \longrightarrow Z \longrightarrow H \longrightarrow \overline{H} \longrightarrow 1, \tag{3}$$

which induces the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
H^1(K, Z) & \xrightarrow{\lambda_1} & H^1(K, H) & \xrightarrow{\lambda_2} & H^1(K, \overline{H}) & \xrightarrow{\lambda_3} & H^2(K, Z) \\
\downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} \\
\bigoplus_{v \neq v_0} H^1(K_v, Z) & \xrightarrow{\nu_1} & \bigoplus_{v \neq v_0} H^1(K_v, H) & \xrightarrow{\nu_2} & \bigoplus_{v \neq v_0} H^1(K_v, \overline{H}) & \xrightarrow{\nu_3} & \bigoplus_{v \neq v_0} H^2(K_v, Z).
\end{array}$$

Let $x \in \bigoplus_{v \neq v_0} H^1(K_v, H)$. Since $\overline{H}$ is semi-simple, α_3 is surjective (Proposition 1), so there exists $y \in H^1(K, \overline{H})$ such that $\alpha_3(y) = \nu_2(x)$. Furthermore, as

$$\alpha_4\big(\lambda_3(y)\big) = \nu_3\big(\alpha_3(y)\big) = \nu_3\big(\nu_2(x)\big) = 0,$$

the injectivity of α_4 (Lemma 3) implies that $\lambda_3(y) = 0$, and hence, $y = \lambda_2(z)$ for some $z \in H^1(K, H)$. Then $\nu_2(\alpha_2(z)) = \alpha_3(\lambda_2(z)) = \nu_2(x)$. It follows from Proposition 42 in [9, Chapter I, §5.7], that

$$x = a \cdot \alpha_2(z) \quad \text{for some } a \in \bigoplus_{v \neq v_0} H^1(K_v, Z)$$

(we refer to loc. cit. for all unexplained notations). Using Lemma 3, pick $b \in H^1(K, Z)$ so that $\alpha_1(b) = a$. Then for $w = b \cdot z$ we have $\alpha_2(w) = a \cdot \alpha_2(z) = x$ as required. □

Theorem 2. *Let G be a semi-simple simply connected algebraic K-group, H be a connected reductive K-subgroup of G and Z be the central torus of H. Furthermore, let F be a K-subgroup of the center of G which is contained in H. Set $\overline{G} = G/F$, $\overline{H} = H/F$, and picking a nonarchimedean place v_0 of K, consider the following diagram*:

$$\begin{array}{ccc} H^1(K, \overline{H}) & \xrightarrow{\omega} & H^1(K, \overline{G}) \\ \alpha \downarrow & & \downarrow \rho \\ \bigoplus_{v \neq v_0} H^1(K_v, \overline{H}) & \xrightarrow{\sigma} & \bigoplus_{v \neq v_0} H^1(K_v, \overline{G}). \end{array}$$

Then in each of the following cases: (a) *Z splits over K,* (b) *Z splits over a quadratic extension L/K and v_0 does not split in L,* (c) *the semi-simple subgroup $D = [H, H]$ is simply connected and contains F, we have $\rho(\operatorname{Im}\omega) = \operatorname{Im}\sigma$.*

Proof. In cases (a) and (b), our claim immediately follows from the corresponding cases in Proposition 2. So, it remains to consider case (c).

Suppose $x = \sigma(y)$, where $x = (x_v) \in \bigoplus_{v \neq v_0} H^1(K_v, \overline{G})$, and $y = (y_v) \in \bigoplus_{v \neq v_0} H^1(K_v, \overline{H})$. Since the map

$$H^1(K, \overline{H}) \xrightarrow{\alpha_r} \prod_{v \in V_r^K} H^1(K_v, \overline{H})$$

is surjective [7, Proposition 6.17], we can choose $z \in H^1(K, \overline{H})$ so that

$$\alpha_r(z) = (y_v)_{v \in V_r^K}.$$

Let $w = \omega(z)$. Twisting $\overline{H}$ and $\overline{G}$ by a cocycle representing z and the associated $\overline{G}$-valued cocycle respectively, we get the following commutative diagram:

$$\begin{array}{ccc} H^1(K, {}_z\overline{H}) & \xrightarrow{\tilde{\omega}} & H^1(K, {}_w\overline{G}) \\ \tilde{\alpha}\big\downarrow & & \big\downarrow\tilde{\rho} \\ \bigoplus_{v \neq v_0} H^1(K_v, {}_z\overline{H}) & \xrightarrow{\tilde{\sigma}} & \bigoplus_{v \neq v_0} H^1(K_v, {}_w\overline{G}). \end{array}$$

It is enough to show that if $\tilde{x} = (\tilde{x}_v) \in \bigoplus_{v \neq v_0} H^1(K_v, {}_w\overline{G})$ corresponds to x under the bijection

$$\bigoplus_{v \neq v_0} H^1(K_v, {}_w\overline{G}) \simeq \bigoplus_{v \neq v_0} H^1(K_v, \overline{G})$$

(cf. [9, Chapter I, §5.3]), then $\tilde{x} \in \tilde{\rho}(\operatorname{Im} \tilde{\omega})$; notice that now $\tilde{x}_v = 1$ for all $v \in V_r^K$.

By our assumption, $F \subset D$, so we can consider $\overline{D} = D/F$. As D is normal in H, the twist ${}_z\overline{D}$ makes sense. Furthermore, since D is simply connected, for any nonarchimedean $v \in V^K$, the natural map

$$H^1(K_v, {}_z\overline{D}) \xrightarrow{\iota_v} H^1(K_v, {}_z\overline{G})$$

is a bijection as each of those sets is in a natural bijective correspondence with $H^2(K_v, F)$ (cf. [7, Corollary to Theorem 6.20]). Since $\tilde{x}_v = 1$ for all $v \in V_r^K$, we conclude that there exists $\tilde{a} \in \bigoplus_{v \neq v_0} H^1(K_v, {}_z\overline{D})$ that maps to $\tilde{x}$ under the composition of the maps

$$\bigoplus_{v \neq v_0} H^1(K_v, {}_z\overline{D}) \longrightarrow \bigoplus_{v \neq v_0} H^1(K_v, {}_z\overline{H}) \xrightarrow{\tilde{\sigma}} \bigoplus_{v \neq v_0} H^1(K_v, {}_w\overline{G}).$$

Since ${}_z\overline{D}$ is semi-simple, by Proposition 1 there exists $\tilde{b} \in H^1(K, {}_z\overline{D})$ that maps to $\tilde{a}$ under the map $H^1(K, {}_z\overline{D}) \to \bigoplus_{v \neq v_0} H^1(K_v, {}_z\overline{D})$. Then $\tilde{c} =$ image of $\tilde{b}$ in $H^1(K, {}_z\overline{H})$ has the property that $\tilde{\rho}(\tilde{\omega}(\tilde{c})) = \tilde{x}$, as required. □

3. Proof of Theorem 1 and some applications

By our assumption, for each $v \neq v_0$, the group $G^{(v)}$ is obtained from G_0 by twisting with a cocycle representing an element of $H^1(K_v, \overline{G}_0)$, so assertion (i) of Theorem 1 follows from (in fact, is equivalent to) the surjectivity of the map

$$H^1(K, \overline{G}_0) \longrightarrow \bigoplus_{v \neq v_0} H^1(K_v, \overline{G}_0),$$

which is furnished by Proposition 1. (As we have already noted above, Proposition 1, and consequently assertion (i) of Theorem 1, are implicitly contained in [2].)

Assertion (ii) is immediate: it follows from the description of the Tits index that for any field extension P/K, $\Delta(G, K)_d \subset \Delta(G, P)_d$. So, in our set-up, if G is K-isotropic, $\Delta(G, K)_d$ is nonempty and is contained in $\Delta(G, K_v)_d$ for all $v \neq v_0$. Since $\Delta(G, K)_d$ is invariant under the

$*$-action and the K-rank of G equals the number of Galois-orbits in $\Delta(G, K)_d$, our assertion follows.

To prove (iii), we let I denote the set of all $i \in \{1, \ldots, r\}$ for which the orbit Ω_i satisfies (1), and let Z_0 be the K-subtorus of T_0 ($\subset G_0$) defined by the condition: $\alpha(t) = 1$ for all simple roots $\alpha \notin \Omega = \bigcup_{i \in I} \Omega_i$. Let S_0 be the maximal K-split subtorus of Z_0. We note that the dimension of S_0 equals the number of Galois-orbits in Ω. Let H_0 be the centralizer of Z_0 in G_0 and $\overline{H}_0$ be the image of H_0 in $\overline{G}_0$. For each $v \neq v_0$, since all the vertices contained in Ω are distinguished in the Tits index of the K_v-form $G^{(v)}$, this group is obtained from G_0 by Galois-twist by a cocycle representing an element

$$x_v \in \mathrm{Im}\big(H^1(K_v, \overline{H}_0) \to H^1(K_v, \overline{G}_0)\big)$$

(cf. [10, 16.4.8]). Now, consider the following commutative diagram:

$$\begin{array}{ccc} H^1(K, \overline{H}_0) & \xrightarrow{\ \ \omega\ \ } & H^1(K, \overline{G}_0) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\rho} \\ \bigoplus_{v \neq v_0} H^1(K_v, \overline{H}_0) & \xrightarrow{\ \ \sigma\ \ } & \bigoplus_{v \neq v_0} H^1(K_v, \overline{G}_0). \end{array}$$

If G_0 is a triality form of type D_4, we may (and we will) assume that H_0 is not a torus, for otherwise, $G^{(v)} \simeq G_0$ for all $v \neq v_0$, and we can take $G = G_0$. Then there can be only one Galois-orbit Ω that satisfies (1), viz. the orbit consisting of the central vertex. But in this case the center of G_0 is contained in the semi-simple subgroup $[H_0, H_0]$.

We note that the torus T_0, and hence also the central torus Z_0 of H_0, splits over L, and if G_0 is not a triality form of type D_4, then $[L : K] \leqslant 2$. Now, by Theorem 2, in all cases, there exists $y \in H^1(K, \overline{H}_0)$ such that $\rho(\omega(y)) = (x_v)$. Let $z = \omega(y)$. Then the group $G = {}_zG_0$ is K_v-isomorphic to $G^{(v)}$ for all $v \neq v_0$, and it contains Z_0, so its K-rank is $\geqslant \dim S_0 =$ the number of Galois-orbits satisfying (1). On the other hand, by (ii), the K-rank can not exceed this number, proving all our claims.

Remark 1. The above proof shows that if the center of G is contained in $[H_0, H_0]$, then the assumption that v_0 does not split in L if the latter is a quadratic extension of K is not necessary (see condition (c) in Theorem 2), however the following example shows that the assumption cannot be dropped in the general case.

Let L/K be a quadratic extension, $G_0 = \mathrm{SU}_4(L/K)$ be the quasi-split group of type ${}^2A_3$ associated with L, and v_0 be a nonarchimedean place of K which splits in L. Pick a nonarchimedean place v_1 that does not split in L, and let $G^{(v_1)}$ be an outer form of type ${}^2A_3$ of K_{v_1}-rank 1. We claim that there is no isotropic K-form G of G_0 such that $G \simeq G_0$ over K_v for all $v \neq v_0, v_1$, and $G \simeq G^{(v_1)}$ over K_{v_1}. Indeed, if G is such a form, then by looking at the Tits indices of groups of type ${}^2A_n$ (cf. [11]) we conclude that the extreme vertices of the Tits index of G over K are distinguished. Then an analysis of the Tits indices of groups of type ${}^1A_n$ shows that G splits over K_{v_0}. This means that if $x \in H^1(K, \overline{G}_0)$ is the cohomology class that corresponds to G and $y \in H^2(K, F)$, where F is the center of G_0, is the image of x under the map $H^1(K, \overline{G}_0) \to H^2(K, F)$, then the map

$$H^2(K, F) \longrightarrow \bigoplus_v H^2(K_v, F), \tag{4}$$

takes y to $\tilde{y} = (y_v)$ where $y_v = 1$ for all $v \neq v_1$ (because $x_v = 1$ for these v's) and $y_{v_1} \neq 1$ (because $x_{v_1} \neq 1$ and the map $H^1(K_{v_1}, \overline{G}_0) \to H^2(K_{v_1}, F)$ is a bijection). We will now apply the theorems of Poitou and Tate (cf. [9, Chapter II, §6.3]) to show that $\tilde{y}$ cannot belong to the image of the map (4). Let $\widehat{F}$ be the dual of F. Consider

$$P^0(K, \widehat{F}) = \prod_{v \in V^K} H^0(K_v, \widehat{F}) \quad \text{and} \quad P^2(K, F) = \bigoplus_{v \in V^K} H^2(K_v, F),$$

where for v real, $H^0(K_v, \widehat{F})$ is the modified 0th cohomology group as in 1.3 of [2]. There are natural maps $j_0 : H^0(K, \widehat{F}) \to P^0(K, \widehat{F})$ and $j_2 : H^2(K, F) \to P^2(K, F)$ (notice that j_2 is precisely the map in (4)), and a nondegenerate pairing

$$P^0(K, \widehat{F}) \times P^2(K, F) \longrightarrow \mathbb{Q}/\mathbb{Z} \tag{5}$$

such that $\operatorname{Im} j_2$ is the orthogonal complement of $\operatorname{Im} j_0$ with respect to this pairing. The pairing (5) restricts to a nondegenerate pairing $H^0(K_{v_1}, \widehat{F}) \times H^2(K_{v_1}, F) \to \mathbb{Q}/\mathbb{Z}$, so $y_{v_1} \neq 1$ implies that y_{v_1} is not orthogonal to $H^0(K_{v_1}, \widehat{F})$. But since v_1 does not split in L, we have $\operatorname{Gal}(L/K) = \operatorname{Gal}(L_{w_1}/K_{v_1})$ which implies that $H^0(K_{v_1}, \widehat{F}) = H^0(K, \widehat{F})$, and therefore y_{v_1} is not orthogonal to the image of $H^0(K, \widehat{F})$ in $H^0(K_{v_1}, \widehat{F})$. It follows that $\tilde{y}$ is not orthogonal to the image of j_0, so $\tilde{y} \notin \operatorname{Im} j_2$, a contradiction. Thus, an isotropic K-form G cannot exist.

Remark 2. A variant of the construction used in the previous remark also yields an example of absolutely simple simply connected groups G_1 and G_2 defined over local fields L_1 and L_2 respectively, both G_1 and G_2 of type A_3 over the algebraic closures of their fields of definitions, such that there is no algebraic group G defined and *isotropic* over a global field K, with $K_{v_i} \simeq L_i$ and $G(K_{v_i}) \simeq G_i(L_i)$, for $i = 1, 2$, for some places v_1 and v_2 of K.

Let L_1 and L_2 be any two noncomplex local fields. Let G_1 be the special unitary group $\mathrm{SU}(f)$ of a hermitian form f in four variables, over a quadratic extension of L_1, of Witt index one, and let G_2 be the group $\mathrm{SL}_{2,D}$, where D is the quaternion division algebra with center L_2. Then for any global field K, two places v_1 and v_2 of K, any K-group G such that $G(K_{v_i}) \simeq G_i(L_i)$, for $i = 1, 2$, is anisotropic over K. Indeed, given such a G, the distinguished vertices in the Tits index of G over K_{v_1} are precisely the two extreme vertices, whereas in the Tits index of G over K_{v_2}, the only distinguished vertex is the middle vertex. This implies that the Tits index of G over K cannot have distinguished vertices at all (cf. assertion (ii) of Theorem 1), so G is K-anisotropic.

Theorem 1 yields a Galois-cohomological argument for the existence of a $\mathbb{Q}$-form, of any absolutely simple simply connected algebraic $\mathbb{R}$-group, with some special properties, thereby answering in the affirmative the question asked in Remark 6.2 of [5]. The precise formulation of this result is as follows.

Proposition 3. (*Cf.* [5, Proposition 6.1].) *Let G^{∞} be an absolutely simple simply connected algebraic $\mathbb{R}$-group. There exists a $\mathbb{Q}$-group G such that*

(1) *$G \simeq G^\infty$ over $\mathbb{R}$;*
(2) *G is quasi-split over $\mathbb{Q}_p$, for every odd prime p;*
(3) *$\mathbb{Q}$-rank $G = \mathbb{R}$-rank G;*
(4) *G splits over $\mathbb{Q}(i)$.*

Proof. Let P be $\mathbb{Q}$ or $\mathbb{Q}(i)$ depending on whether G^∞ is an inner or outer form over $\mathbb{R}$, and let G_0 be the quasi-split $\mathbb{Q}$-form of G^∞ that splits over P, but does not split over $\mathbb{Q}$ if $P \neq \mathbb{Q}$. Since the 2-adic place does not split in $\mathbb{Q}(i)$, by Theorem 1 there exists an inner twist G of the $\mathbb{Q}$-group G_0, whose $\mathbb{Q}$-rank equals the $\mathbb{R}$-rank of G^∞, such that $G \simeq G^\infty$ over $\mathbb{R}$ and $G \simeq G_0$ over $\mathbb{Q}_p$, for all $p \neq 2$. Now it only remains to show that G splits over $L := \mathbb{Q}(i)$. Since G_0 splits over L, in view of the Hasse principle for $\overline{G}_0$, i.e., the injectivity of the map

$$H^1(L, \overline{G}_0) \longrightarrow \bigoplus_{w \in V^L} H^1(L_w, \overline{G}_0)$$

[7, Theorem 6.22], it is enough to show that G splits over all completions of L. But for completions at nondyadic places (including the archimedean ones), this immediately follows from our construction. Let w_2 be the (unique) dyadic place of L. Let $x \in H^1(L, \overline{G}_0)$ be the element that corresponds to G/L, and let $y \in H^2(L, F)$ be the image of x under the map $H^1(L, \overline{G}_0) \to H^2(L, F)$, where F is the center of G_0. For $w \in V^L$, we let x_w and y_w denote the images of x and y in $H^1(L_w, \overline{G}_0)$ and $H^2(L_w, F)$ respectively. If $w \neq w_2$, then x_w is trivial, implying that y_w is trivial. But over L, F is either isomorphic to μ_n for some n, or to $\mu_2 \times \mu_2$, so we infer using (HBN) that y_{w_2} is also trivial. Now since the natural map $H^1(L_{w_2}, \overline{G}_0) \to H^2(L_{w_2}, F)$ is a bijection [7, Corollary to Theorem 6.20], we conclude that x_{w_2} is trivial, so x is trivial. □

Remark 3. Any real representation of a semi-simple $\mathbb{Q}$-group G as in Proposition 3 is defined over $\mathbb{Q}$, see [5].

The following two propositions, which are needed in a forthcoming joint paper of Belolipetsky and Lubotzky on counting arithmetic subgroups of covolume $\leqslant c$, are proved by a simple modification of the proof of Proposition 3.

Proposition 4. *Let K be a number field, L be a totally imaginary quadratic extension of K. Fix a nonarchimedean place v_0 of K which does not split in L. Assume that for every archimedean place v of K, we are given an absolutely simple simply connected algebraic K_v-group $G^{(v)}$. We assume that the groups $G^{(v)}$ are of the same absolute type for all archimedean v, and if V_r^K is nonempty, then the $G^{(v)}$'s are either all inner forms or all outer forms over K_v $(= \mathbb{R})$ for $v \in V_r^K$. Then there exists a K-group G such that*

(1) *G is K_v-isomorphic to $G^{(v)}$ for every archimedean place v of K;*
(2) *G is quasi-split over K_v for every nonarchimedean place v of K different from v_0;*
(3) *G splits over L.*

Proof. Let $P = L$ if V_r^K is nonempty, and for every $v \in V_r^K$, $G^{(v)}$ is an outer form; in all other cases let $P = K$. Let G_0 be the absolutely simple simply connected quasi-split K-group of same absolute type as the given $G^{(v)}$'s, and which splits over P, but does not split over K if $P \neq K$.

By Theorem 1(i), there exists an inner twist G of G_0 over K which is K_v-isomorphic to $G^{(v)}$ for all archimedean places v, and which is quasi-split at v for all nonarchimedean $v \neq v_0$. Arguing as in the proof of Proposition 3, we see that G splits over L. □

Proposition 5. *Let K be a number field and L be a quadratic extension of K. Let v_0 be a nonarchimedean place of K which does not split in L. Assume that for each archimedean place v of K, we are given an absolutely simple simply connected algebraic K_v-group $G^{(v)}$ so that all the $G^{(v)}$'s are of same absolute type and additionally if for a real place v, $G^{(v)}$ is an inner form over K_v $(=\mathbb{R})$, then $G^{(v)}$ is K_v-split and v splits in L, and if $G^{(v)}$ is an outer form over K_v, then v does not split in L. Then there exists a K-group G such that*

(1) *G is K_v-isomorphic to $G^{(v)}$ for every archimedean place v of K;*
(2) *G is quasi-split over K_v for every nonarchimedean place v of K different from v_0;*
(3) *G splits over L.*

Proof. Let $P = L$ if there is a real place v such that $G^{(v)}$ is an outer form over K_v, otherwise, let P equal K. Let G_0 be the absolutely simple simply connected quasi-split K-group of same absolute type as the given $G^{(v)}$'s, and which splits over P, but does not split over K if $P \neq K$. By Theorem 1(i), there exists an inner twist G of G_0 over K which is K_v-isomorphic to $G^{(v)}$ for all archimedean places v, and which is quasi-split at v for all nonarchimedean $v \neq v_0$. Arguing as in the proof of Proposition 3, we see that G splits over L. □

Remark 4. We recall that $\mathbb{R}$-anisotropic groups of types A_n $(n > 1)$, D_{2n+1} and E_6, are outer forms, and the ones of remaining types are inner forms, cf. [11].

Remark 5. (1) The condition in Proposition 4 that for all $v \in V_r^K$, the $G^{(v)}$'s are either inner forms or all are outer forms over K_v is needed to ensure the truth of assertion (3). Indeed, suppose K has two real places v_1 and v_2, and take $G^{(v_1)} = \mathrm{SL}_{2,D}$, where $D = \mathbb{H}$ is the quaternion division algebra over $\mathbb{R}$. Then a K-group G which is K_{v_1}-isomorphic to $G^{(v_1)}$ and which is anisotropic at v_2 must be an outer form of type A_3. Let ℓ be the quadratic extension of K over which G is inner. Then v_1 splits in ℓ and v_2 does not. Now if G splits over a quadratic extension L/K as in Proposition 4, then necessarily $L = \ell$, which, of course, is impossible for a totally imaginary L.

(2) Likewise, without the condition that v_0 does not split over L, assertion (3) of Proposition 4 is false in general. For example, $G = \mathrm{Spin}(f)$, where $f = x^2 + y^2 + z^2$, is the only form of SL_2 that is anisotropic over $\mathbb{R}$ and splits over $\mathbb{Q}_p$ for all $p \neq 2$. However, G does not split over $L = \mathbb{Q}(\sqrt{-7})$.

4. Uniqueness

In this section we briefly address the question of the uniqueness of an inner twist G of G_0 over K which is K_v-isomorphic to a given inner twist $G^{(v)}$ of G_0 over K_v for every $v \in V^K \setminus \{v_0\}$, where v_0 is a fixed nonarchimedean place of K. Clearly, the uniqueness is essentially equivalent to the injectivity of the map

$$\alpha : H^1(K, \overline{G}_0) \to \bigoplus_{v \neq v_0} H^1(K_v, \overline{G}_0).$$

Let F be the center of G_0. It is the kernel of the natural K-isogeny $G_0 \to \overline{G}_0$. Let L be the minimal Galois extension of K over which G_0 becomes an inner form (i.e., it splits).

Theorem 3.

(1) *α is injective if and only if*

$$\beta : H^2(K, F) \to \bigoplus_{v \neq v_0} H^2(K_v, F)$$

is injective.

(2) *Let $P = L$ if $[L : K] \neq 6$, and let P be a cubic extension of K contained in L otherwise. Then β is injective if and only if v_0 does not split in P (i.e., $P \otimes_K K_{v_0}$ is a field).*

Proof. (1) Suppose first that β is injective, and let $\delta : H^1(K, \overline{G}_0) \to H^2(K, F)$ be the canonical map. If $x, y \in H^1(K, \overline{G}_0)$ are such that $\alpha(x) = \alpha(y)$, then $\delta(x)$ and $\delta(y)$ have the same image under β, and therefore $\delta(x) = \delta(y)$. Since v_0 is nonarchimedean, there is a natural bijection $H^1(K_{v_0}, \overline{G}_0) \simeq H^2(K_{v_0}, F)$ (cf. [7, Corollary of Theorem 6.20]), so x and y have the same image in $H^1(K_{v_0}, \overline{G}_0)$. Thus, x and y have the same image under the map $H^1(K, \overline{G}_0) \to \bigoplus_v H^1(K_v, \overline{G}_0)$, and it follows from the Hasse principle for adjoint groups [7, Theorem 6.22] that $x = y$. Conversely, suppose β is not injective, and pick a nonzero $s \in \operatorname{Ker} \beta$. Since δ is surjective [7, Theorem 6.20], one can pick $x \in H^1(K, \overline{G}_0)$ so that $\delta(x) = s$. Let $(x_v)_{v \in V_r^K}$ be the image of x in $\prod_{v \in V_r^K} H^1(K_v, \overline{G}_0)$. Using the fact that $s \in \operatorname{Ker} \delta$, we see from a relevant exact sequence that (x_v) lifts to $(\tilde{x}_v) \in \prod_{v \in V_r^K} H^1(K_v, G_0)$. Using the surjectivity of

$$H^1(K, G_0) \longrightarrow \prod_{v \in V_r^K} H^1(K_v, G_0)$$

[7, Proposition 6.17], we find $\tilde{x} \in H^1(K, G_0)$ that maps to $(\tilde{x}_v)$. Let y be the image of $\tilde{x}$ in $H^1(K, \overline{G}_0)$. Then $\alpha(x)$ and $\alpha(y)$ have the same v-components for all archimedean v in view of our construction, and for nonarchimedean $v \neq v_0$ due to the bijection $H^1(K_v, \overline{G}_0) \simeq H^2(K_v, F)$, the triviality of $H^1(K_v, G_0)$ [7, Theorem 6.4], and the fact that $s \in \operatorname{Ker} \beta$. Thus, $\alpha(x) = \alpha(y)$; however, $x \neq y$ because $\delta(x) = s \neq 0 = \delta(y)$.

(2) We begin with the following lemma which is an easy consequence of the theorems of Poitou and Tate.

Lemma 4. *Let M be a finite $\mathcal{G}_K$-module, and $\widehat{M}$ be its dual. Let v_0 be a nonarchimedean place of K.*

(1) *If the map $\mu : H^2(K, M) \to \bigoplus_{v \in V^K} H^2(K_v, M)$ is injective and $H^0(K, \widehat{M}) = H^0(K_{v_0}, \widehat{M})$, then the map $\eta : H^2(K, M) \to \bigoplus_{v \neq v_0} H^2(K_v, M)$ is also injective.*

(2) *If $H^0(K, \widehat{M}) \neq H^0(K_{v_0}, \widehat{M})$, then η is not injective.*

Proof. (1) Let $x \in \operatorname{Ker} \eta$. Since μ is injective, to prove that $x = 0$ it is enough to show that $x_{v_0} =$ the image of x in $H^2(K_{v_0}, M)$, is trivial. But it follows from the theorems of Poitou and Tate that x_{v_0} is orthogonal to $H^0(K, \widehat{M}) = H^0(K_{v_0}, \widehat{M})$ under the natural pairing $H^0(K_{v_0}, \widehat{M}) \times$

$H^2(K_{v_0}, M) \to \mathbb{Q}/\mathbb{Z}$. Since the latter is nondegenerate [9, Chapter II, §5.8], we get $x_{v_0} = 0$ as required.

(2) Since $H^0(K, \widehat{M}) \neq H^0(K_{v_0}, \widehat{M})$, there exists a nonzero $x_{v_0} \in H^2(K_{v_0}, M)$ that is orthogonal to $H^0(K, \widehat{M})$. According to Poitou and Tate, there exists $x \in H^2(K, M)$ the image of which in $H^2(K_v, M)$ is zero for all $v \neq v_0$, and is x_{v_0} for $v = v_0$. Clearly, x is a nonzero element in $\operatorname{Ker} \eta$. □

It is known [7, p. 332] that F is one of the following groups:

(a) μ_n,
(b) $\mu_2 \times \mu_2$,
(c) $R_{L/K}(\mu_2)$, if G_0 is an outer form of type D_{2n},
(d) $R^{(1)}_{L/K}(\mu_n)$, where $n > 2$ (as $R^{(1)}_{L/K}(\mu_2) \simeq \mu_2$, $n = 2$ belongs to the case (a)), and
(e) $R^{(1)}_{P/K}(\mu_2)$, where $[P : K] = 3$; notice that here P is the same as in the statement of part (2) of the theorem.

To be able to use Lemma 4, we first need to check that in all these cases the map

$$H^2(K, F) \xrightarrow{\gamma} \bigoplus_{v \in V^K} H^2(K_v, F)$$

is injective. In fact, this follows immediately from (HBN) in the cases (a)–(c), and with some additional computations also in the remaining cases (d), (e) (cf. [7, Lemma 6.19]). However, one can give a uniform proof using Theorem A in [9, Chapter II, §6.3], due to Poitou and Tate. According to this result, $\operatorname{Ker} \gamma$ is dual to the kernel of

$$H^1(K, \widehat{F}) \xrightarrow{\varepsilon} \prod_v H^1(K_v, \widehat{F}),$$

so it is enough to show that $\operatorname{Ker} \varepsilon$ is trivial. We notice that it follows from Chebotarev's Density Theorem that for any number field k the map

$$H^1(k, \mathbb{Z}/n\mathbb{Z}) \longrightarrow \prod_{w \in V^k} H^1(k_w, \mathbb{Z}/n\mathbb{Z}),$$

where $\mathbb{Z}/n\mathbb{Z}$ is considered as a trivial $\mathcal{G}_k$-module, is injective. Since $\widehat{\mu_n} = \mathbb{Z}/n\mathbb{Z}$, this immediately gives the desired result in the cases (a)–(c). To consider the cases (d) and (e), we let L denote the Galois closure of P. Then for F in the cases (d) and (e), we have $\widehat{F} \simeq \mathbb{Z}/n\mathbb{Z}$ as a $\mathcal{G}_L$-modules, so the map $H^1(L, \widehat{F}) \to \prod_{w \in V^L} H^1(L_w, \widehat{F})$ is injective. From the inflation–restriction exact sequence

$$0 \longrightarrow H^1(L/K, \widehat{F}) \longrightarrow H^1(K, \widehat{F}) \longrightarrow H^1(L, \widehat{F})$$

and its local analogs, we see that to prove the injectivity of ε, it is now enough to prove the injectivity of

$$H^1(L/K, \widehat{F}) \longrightarrow \prod_{v, w|v} H^1(L_w/K_v, \widehat{F}). \tag{6}$$

But the Galois group $\mathrm{Gal}(L/K)$ is one of the following groups: $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, or the symmetric group S_3, hence has cyclic Sylow subgroups. It follows from the Chebotarev Density Theorem that all Sylow subgroups appear as local Galois groups $\mathrm{Gal}(L_w/K_v)$, so the injectivity of (6) follows from the well-known fact that for a finite group $\mathcal{G}$, any $\mathcal{G}$-module A and any i, the homomorphism

$$H^i(\mathcal{G}, A) \longrightarrow \bigoplus_p H^i(\mathcal{G}_p, A),$$

where the sum runs over all prime divisors p of the order of $\mathcal{G}$ and $\mathcal{G}_p$ is a Sylow p-subgroup of $\mathcal{G}$, is injective.

Now, to complete the proof of assertion (2) of the theorem, we need to check that $H^0(K, \widehat{F}) = H^0(K_{v_0}, \widehat{F})$ is equivalent to the assertion that v_0 does not split in P. There is nothing to prove in the cases (a) and (b). In the case (c), $H^0(K, \widehat{F})$ has order two, while $H^0(K_{v_0}, \widehat{F})$ has order four or two depending on whether v_0 splits or not in P. In the case (d), $H^0(K, \widehat{F})$ again has order two, while $H^0(K_{v_0}, \widehat{F})$ has order n if v_0 splits in P, and order two if it does not. In the case (e), the group $H^0(K, \widehat{F})$ is trivial, and so is the group $H^1(K_{v_0}, \widehat{F})$ if v_0 does not split in P. On the other hand, if $P \otimes_K K_{v_0} = K_{v_0} \oplus K_{v_0} \oplus K_{v_0}$, then $H^0(K_{v_0}, \widehat{F})$ has order four, and if $P \otimes_K K_{v_0} = K_{v_0} \oplus Q$, where Q is a quadratic extension of K_{v_0}, then $H^0(K_{v_0}, \widehat{F})$ has order two, proving assertion (2) in all the cases. □

Remark 6. The uniqueness assertion does not hold in general if v_0 is a real place since the map $H^1(K, G_0) \to \prod_{v \in V_r^K} H^1(K_v, G_0)$ is a bijection, whereas the image of the map $H^1(K_{v_0}, G_0) \to H^1(K_{v_0}, \overline{G}_0)$ is often nontrivial.

Acknowledgments

We acknowledge partial support from the Institute for Advanced Study, the NSF (grants DMS-0400640 and DMS-0502120) and from the BSF (grant # 200071). We thank Mikhail Belolipetsky, Alex Lubotzky, Dave Morris and Dipendra Prasad for their questions and comments, and Jean-Pierre Serre for his interest in this work. Finally, we are grateful to the anonymous referee whose suggestions helped to improve the exposition.

References

[1] J.W.S. Cassels, A. Frölich (Eds.), Algebraic Number Theory, Academic Press, 1967.
[2] A. Borel, G. Harder, Existence of discrete cocompact subgroups of reductive groups over local fields, J. Reine Angew. Math. 298 (1978) 53–64.
[3] A. Borel, G. Prasad, Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups, Publ. Math. Inst. Hautes Études Sci. 69 (1989) 119–171; Addendum: Publ. Math. Inst. Hautes Études Sci. 71 (1990) 173–177.
[4] A. Lubotzky, Subgroup growth and congruence subgroups, Invent. Math. 119 (1995) 267–295.
[5] D. Morris, Real representations of semisimple Lie algebras have $\mathbb{Q}$-forms, in: Proc. Internat. Conf. on Algebraic Groups and Arithmetic, December 17–22, 2001, TIFR, Mumbai, 2001, pp. 469–490.
[6] R.S. Pierce, Associative Algebras, Grad. Texts in Math., vol. 88, Springer, 1982.
[7] V.P. Platonov, A.S. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, 1993.
[8] G. Prasad, Volumes of S-arithmetic quotients of semi-simple groups, Publ. Math. Inst. Hautes Études Sci. 69 (1989) 91–117.
[9] J.-P. Serre, Galois Cohomology, Springer, 1997.

[10] T.A. Springer, Linear Algebraic Groups, second ed., Birkhäuser, 1998.
[11] J. Tits, Classification of algebraic semisimple groups, in: Algebraic Groups and Discontinuous Groups, in: Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., 1966, pp. 33–62.
[12] V.E. Voskresenskii, Algebraic Groups and Their Birational Invariants, Transl. Math. Monogr., vol. 179, Amer. Math. Soc., 1998.