Computation of the Metaplectic Kernel

Gopal Prasad   Andrei S. Rapinchuk

Dedicated to G. D. Mostow

Introduction

Let G be an absolutely simple, simply connected algebraic group defined over a global field K. Given a finite (possibly, empty) set S of places of K, we let $G(A(S))$ denote the group of S-adeles (i.e. adeles without the components corresponding to the places in S) of G. Our main concern in this paper is a description of topological central extensions of the form:

$$1 \to I \longrightarrow E \xrightarrow{\pi} G(A(S)) \to 1,$$

where $I = \mathbf{R}/\mathbf{Z}$ is the 1-dimensional compact torus, which split over the group $G(K)$ of K-rational points of G. Study of such central extensions is required for the theory of automorphic forms of fractional weights (the case $S = \emptyset$) and for a solution of the congruence subgroup problem (for applications to the congruence subgroup problem it is enough to consider the case where S contains V_∞^K, the set of archimedean places of K). Since the above extension admits a measurable cross-section, one can show (cf. Mackey [Mc]) that the set of equivalence classes of such extensions is in one-to-one correspondence with the elements of the kernel $M(S,G)$ of the following restriction map: $H^2(G(A(S))) \to H^2(G(K))$, where $H^2(G(A(S)))$ (resp., $H^2(G(K))$) is the second cohomology group of the group $G(A(S))$ (resp., of $G(K)$) defined in terms of measurable (resp., abstract) cochains, with values in I. As the unique nontrivial two-sheeted cover of $G(A)$, for $G = \mathbf{Sp}_{2n}$, $A = A(\emptyset)$, which splits over $G(K)$, was named the metaplectic group by André Weil, $M(S,G)$ is called the *metaplectic kernel.* It is always finite (Theorem 2.4) and its precise computation is the main objective of the present paper.

We shall now briefly recall the relation between the congruence subgroup problem and the metaplectic kernel. Assume that $S \supset V_\infty^K$. The congruence kernel $C(S,G)$, as defined by J-P. Serre, is the kernel of the natural surjective homomorphism $\hat{G} \to \bar{G}$ from the completion $\hat{G}$ of $G(K)$ with respect to the S-arithmetic topology to its completion $\bar{G}$ with respect to the S-congruence subgroup topology. It is well known that if $C(S,G)$ is central in $\hat{G}$ and $G(K)$ is perfect, then $C(S,G)$ is isomorphic to the dual of the metaplectic kernel. We note here that either if G/K is isotropic and is not an outer form of type E_6 of K-rank one, or G/K is anisotropic but not of type A_r, E_6 or ${}^{3,6}D_4$, then $G(K)$ is projectively simple, i.e. it is simple modulo its center (cf. [PR2], Ch. 9). Also, for most of these groups $C(S,G)$ is known to be central (in $\hat{G}$) provided that $\sum_{v\in S} K_v\text{-rank}G \geq 2$ (cf. [Ra3], [R3]).

According to an interesting result of Pierre Deligne, if $C(S,G)$ is central, then no S-arithmetic subgroup in a covering of $\prod_{v\in S} G(K_v)$, of degree larger than the order of $M(\emptyset, G)$, is residually finite. Thus our results on $M(\emptyset, G)$ imply that S-arithmetic subgroups in nonlinear semi-simple groups often fail to be residually finite. A known result in this direction, proved by Raghunathan ([Ra1]), has been used by Toledo ([T]) to construct an example of a smooth complex projective variety whose fundamental group is not residually finite.

In a fundamental work [Mo], Moore, making use of the description given by Robert Steinberg of the (abstract) universal central extension of the group of rational points of a simply connected Chevalley (i.e. split) group over an arbitrary field, found a relation between the norm residue symbols (of local class field theory) and the topological central extensions of $\mathbf{SL}_2(k)$, where k is a local field. Using the uniqueness of the reciprocity law (see Appendix B), which he proved in the same paper, he was able to compute the metaplectic kernel $M(S,G)$ for $G = \mathbf{SL}_2$ and also show that for any Chevalley group the metaplectic kernel is trivial if S contains a noncomplex place and it is a subgroup of $\hat{\mu}(K)$, the dual group of the group $\mu(K)$ of roots of unity in K, if all the places in S are complex. Soon afterwards Matsumoto [Ma], by explicitly constructing certain topological central extensions of $G(A(S))$, was able to prove that in the latter case $M(S,G)$ is in fact equal to $\hat{\mu}(K)$ for any Chevalley group G. Deodhar [D] extended the results of Steinberg and Moore for split groups to quasi-split groups and in particular determined the metaplectic kernel for this class of groups.

The metaplectic kernel for arbitrary K-isotropic groups was computed by Prasad and Raghunathan [PrRa1] who used the general injectivity results of [PrRa2] (cf. Theorem 1.2 below) to reduce the problem first to the groups of K-rank one, and then further to the groups of the form $R_{L/K}(\mathbf{SL}_2)$, where $R_{L/K}$ is the restriction of scalars functor, for which one can use the results of [Mo]. (Note that the papers [PrRa2], [PrRa4] and [Pr2] determine the topological central extensions of the group of rational points of an arbitrary simple, simply connected group over a nonarchimedean local field.) The metaplectic kernel for the group $\mathbf{SL}_{n,D}, n \geq 2$ was computed independently by Bak and Rehmann [BR] using (algebraic) K-theoretic methods. Bak [B] has announced its computation for the classical groups of K-rank≥ 2.

The computation of the metaplectic kernel for anisotropic groups in the present paper has required some new arithmetic, geometric and group-theoretic ideas. The main problem is that though one can still use the local results of [Mo], [D], [PrRa 2, 4] and [Pr2] to describe the topological central extensions of the S-adele group $G(A(S))$, it is very difficult to determine the precise conditions under which such an extension splits over the group $G(K)$. In [Mo] and [D] the local and adelic computations were *preceded* by a description of the (abstract) central extensions of $G(F)$, F an arbitrary (infinite) field, from which the required conditions followed; such a description is not available for even a single anisotropic group. Earlier, Rapinchuk [R1] had determined $M(S,G)$ modulo 2-torsion for $G = \mathbf{SL}_{1,D}$, D an arbitrary central division algebra (see also [Pr1]), in case $S \supset V_\infty^K$, and Klose [Kl] obtained some partial results on the topological central extension of the adele group associated with $\mathbf{GL}_{1,D}$ in case D is a quaternion division algebra. The more precise computation of the metaplectic kernel given in this paper appears to be new for even the simplest anisotropic group $\mathbf{SL}_{1,D}$, where D is a quaternion division algebra.

Here we will prove the following.

Main Theorem. *Let G be an absolutely simple, simply connected algebraic group defined over a global field K, S a finite (possibly, empty) set of places of K. Assume that if G is of type ${}^2A_r$, then S contains all the real places of K at which G is not an inner form. Then, if there is a place v_0 in S which is either nonarchimedean and G is K_{v_0}-isotropic, or it is real and the group $G(K_{v_0})$ is not (topologically) simply connected, the metaplectic kernel $M(S,G)$ is trivial. In general, $M(S,G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$, the dual group of the group $\mu(K)$ of roots of unity in K, and $M(\emptyset,G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$ of index at most two.*

Some remarks concerning the assumptions in the theorem are in order. To establish the theorem we need to prove the vanishing of the following for any finite set V of places not in S:

$$M_V(G) := \mathrm{Ker}(H^2(G(V)) \to H^2(G(K)));$$

where $G(V) := \prod_{v\in V} G(K_v)$ and $H^2(G(V))$ is the second cohomology group of $G(V)$ defined in terms of measurable cochains with values in I. However, in case G/K is of outer type $A_r, r > 1$, and V contains a real place at which it remains outer, we have not been able to prove the required vanishing. This is the reason for the additional restriction on S in case G is of outer type $A_r, r > 1$.

If v_0 is a real place and the group $G(K_{v_0})$ is simply connected (e.g. $G = \mathbf{Spin}(f)$, f a quadratic form in $n \geq 5$ variables of Witt index one over $K_{v_0} = \mathbf{R}$), then $M(S,G) = M(S \cup \{v_0\}, G)$ for any S, in particular, $M(\{v_0\},G) = M(\emptyset,G)$, and $M(\{v_0\},G)$ is in general nontrivial. Also, using the results of [PrRa4] and of the present paper, one can show that if $G = \mathbf{SL}_{1,D}$, and v_0 is a nonarchimedean place of K such that $D_{v_0} = D \otimes_K K_{v_0}$ is a division algebra, then $M(\{v_0\},G)$ need not be trivial, thus the assumption that G is K_{v_0}-isotropic cannot be omitted; see however the results in 4.10 and 5.9.

In many cases, for example, if $G = \mathbf{SL}_{1,D}$, where D is either a quaternion algebra or a central simple algebra of odd degree, or else $G = \mathbf{Spin}(f)$, f a quadratic form in $n \geq 5$ variables, we have been able to prove below that $M(\emptyset,G) = \hat{\mu}(K)$; however, the question whether it is so in general is still open.

As an application of the fact that for any finite set V of nonarchimedean places, $M_V(G)$ vanishes, in §8 we will present a solution of the congruence subgroup problem in the affirmative for the groups of rational points over semi-local subrings of K. For a finite subset V of V_f^K, we let $\mathfrak{o}_V$ denote the subring of K of elements which are integral with respect to all places in V; obviously, $\mathfrak{o}_V$ is a semi-local ring (i.e. it has only finitely many maximal ideals). Assume that G is a K-subgroup of $\mathbf{SL}_n$. The congruence subgroup problem for the group $G(\mathfrak{o}_V) := G(K) \cap \mathbf{SL}_n(\mathfrak{o}_V)$ was considered by Sury [Su], who solved it in the affirmative for the groups of types B_n, C_n and D_n using techniques involved in the proof of the projective simplicity of the groups of rational points of algebraic groups of these types. This suggested that the congruence subgroup problem in the semi-local case is closely related to the problem of determining the structure of normal subgroups of the group of rational points, and in §8 we will prove that, indeed, this is the case. To give a precise statement, we need to recall the conjectured description of normal subgroups of $G(K)$. Let

$$T = \{v \in V_f^K \mid G \text{ is } K_v\text{-anisotropic}\}$$

(this notation will be used throughout the paper). The Platonov-Margulis conjecture asserts that:

Given a noncentral normal subgroup N of $G(K)$, there is an open normal subgroup W of $G(T) = \prod_{v \in T} G(K_v)$ such that $N = G(K) \cap W$; in particular, if $T = \emptyset$ (which is always the case if G is not of type A_r), then $G(K)$ does not have any proper noncentral normal subgroups, i.e. it is projectively simple.

If this conjecture is true for $G(K)$, we say that $G(K)$ has the standard description of normal subgroups. This conjecture has been established for all K-isotropic G (except for certain outer forms of type E_6 of K-rank 1) and also for all K-anisotropic groups of type other than A_r, $r > 1$, E_6 and ${}^{3,6}D_4$.

Theorem. *Suppose K is of characteristic zero, $G(K)$ has the standard description of normal subgroups, and $V \supset T$. Then the congruence subgroup problem for $G(\mathfrak{o}_V)$ has an affirmative solution, i.e. every noncentral normal subgroup of $G(\mathfrak{o}_V)$ is open in $G(\mathfrak{o}_v)$ in the topology induced from the group $G(V)$.*

In view of the vanishing of $M_V(G)$, to prove this theorem, we need only to prove the centrality of the corresponding "congruence kernel". The proof given in §8 of the centrality uses certain techniques devised to prove the congruence subgroup property for arithmetic groups with bounded generation conjectured by the second-named author (cf. [PR3], [R3] and [Lu]).

Finally, we summarize the contents of this paper. In §1, we recall some known results on topological central extensions and derive a few consequences used in the paper; in §2 we analyze the contribution of the archimedean places to $M_V(G)$ and prove the finiteness of the metaplectic kernel. §§3-5 are devoted to the computation of the metaplectic kernel for the groups of type A_r : §3 studies groups of type A_1, §4, arbitrary (inner) forms of type ${}^1A_r$ and §5, outer forms of type ${}^2A_r$. The results for groups of type A_r are used to treat the groups of all other classical types in §6 using their geometric realizations. The groups of exceptional types are considered in §7 using information about their Galois cohomology. In §8 we solve the congruence subgroup problem in the semi-local case. At the end of the paper, there are two appendices. The first is devoted to construction of field extensions of K with prescribed local properties for use in the study of groups of type ${}^2A_r$. The second gives a result related to the uniqueness of the reciprocity law in global class field theory.

ACKNOWLEDGEMENTS. The first-named author received partial support from the National Science Foundation. This joint work began while the second-named author visited the University of Michigan in 1992-94. During the preparation of the final version of this paper he visited the University of Bielefeld as a guest of Fakultät für Mathematik and SFB 343 "Diskrete Strukturen in der Methematik" on a fellowship awarded by the Alexander von Humbolt Foundation (Bonn). For a brief period in 1995, the first-named author also visited the University of Bielefeld as a guest of SFB 343. The support and hospitality of all these institutions is thankfully acknowledged.

1 Preliminaries

In this section we will collect together some results on topological central extensions and draw a few consequences from them for use in this paper.

Notation. k will denote a nonarchimedean local (i.e. locally compact, nondiscrete) field and G an absolutely simple, simply connected group defined over k. For any k-subgroup H of G, $H(k)$ will denote the group of k-rational points of H with the natural locally compact topology induced from that on k, and $H^2(H(k))$ will denote the second cohomology group of $H(k)$ with coefficients in $I = \mathbf{R}/\mathbf{Z}$ defined in terms of measurable cochains. We shall denote by $\mu(k)$ the group of roots of unity in k and by $\hat{\mu}(k)$ its dual group.

We fix a maximal k-split torus S of G and for a root α of G with respect to S, we denote by U_α the corresponding root subgroup; U_α is a unipotent subgroup defined over k. Let G_α denote the k-subgroup generated by U_α and $U_{-\alpha}$. Then G_α is simply connected and k-simple (but it is not always absolutely simple).

The following theorem combines the well known local results of Moore [Mo], Matsumoto [Ma], Deodhar[D] and an observation of Deligne.

Theorem 1.1 *Let G be an absolutely simple, simply connected k-group which is either split or quasi-split over k. Then there exists a natural isomorphism $H^2(G(k)) \to \hat{\mu}(k)$.*

For arbitrary k-isotropic groups Prasad and Raghunathan [PrRa2], have proved that $H^2(G(k))$ is isomorphic to a subgroup of $\hat{\mu}(k)$.

We will summarize in the following theorem an injectivity result which plays an important role in the paper and deduce Proposition 1.3 from it. For split and quasi-split groups the theorem follows from the results of Moore and Deodhar, and for an arbitrary k-isotropic group it was established by Prasad and Raghunathan [PrRa2: Theorem 9.5]. To give a precise statement, recall that in case the root system $\Phi(S,G)$ of G with respect to S is not reduced, then by convention, a root α is long if, and only if, it is divisible, i.e. if $\alpha/2$ is also a root. We note that if G is quasi-split over k, $\Phi(S,G)$ is nonreduced only if G/k is of type ${}^2A_r$ with r even.

Theorem 1.2 *Suppose G is k-isotropic, and let α be a long root in the root system of G with respect to a maximal k-split torus. Then the restriction map $H^2(G(k)) \stackrel{\rho_\alpha}{\to} H^2(G_\alpha(k))$ is injective.*

(It can be shown, for example, by a case-by-case analysis, that this theorem holds also in case $k = \mathbf{R}$.)

If α is not long, ρ_α is not injective in general. However, as the following proposition shows, if G is quasi-split, but not split over k, ρ_β is injective for every root β.

Proposition 1.3 *Suppose G is quasi-split, but not split over k. Then the restriction*

$$H^2(G(k)) \stackrel{\rho_\beta}{\to} H^2(G_\beta(k))$$

is injective for every root β.

Proof. If β is long, then the proposition follows from 1.2. So we assume that β is a short root. If G is of type ${}^2A_r$, with r even, and β is a multipliable root, then $G_{2\beta} \subset G_\beta$ and hence once again the proposition follows from 1.2. Therefore we may (and will) assume further that β is a nonmultipliable short root. Now if G is of type ${}^2A_r$, with r even, then $r > 2$ and the subgroup H generated by the G_α, for α in the subset of all nonmultipliable roots, is an absolutely simple simply connected k-subgroup of type ${}^2A_{r-1}$, and moreover it is quasi-split over k. As H contains G_α for any divisible root α, in view of 1.2, the restriction $H^2(G(k)) \to H^2(H(k))$ is injective. This implies that to prove the proposition for all groups of type ${}^2A_r$, it is enough to prove it for groups of type ${}^2A_r$, with $r(>2)$ odd. We shall therefore assume that in case G is of type ${}^2A_r$, then r is odd.

We fix a Borel subgroup of G defined over k and containing S. This determines an ordering on the set $\Phi(S,G)$ of roots of G. Since $N_G(S)(k)$ acts transitively on the set of roots of a given length, we can evidently assume that β is a short simple root which is connected to a long root α in the Dynkin diagram of the root system $\Phi(S,G)$. Now let H be the subgroup generated by G_α and G_β. Then if G is not a triality form, H is an absolutely simple, simply connected group of type ${}^2A_3$ which is quasi-split over k, and by 1.2, the restriction $H^2(G(k)) \to H^2(H(k))$ is injective. Thus to prove the proposition, we can assume that either G is of type ${}^2A_3$ or it is a triality form. Let K be the smallest Galois extension of k over which G splits.

Let us first take up the case where G is of type ${}^2A_3$. In this case K is a quadratic extension of k and Deodhar has proved the following equality [D: 2.32(*)] (all unexplained notations are from his paper):

$$b_\beta(s, t^{-1}) = b_\alpha(t, N_{K/k}(s)^{-1})^{-1} \text{ for all } s \in K^*, \text{ and } t \in k^*.$$

Now, in the case under consideration, the proposition follows immediately from the fact that there exist some $s \in K^*$ and $t \in k^*$ such that the value of the μ-power norm residue symbol $(t, N_{K/k}(s))$, $\mu := \#\mu(k)$, is a generator of the group $\mu(k)$ of roots of unity in k.

Let us now assume that G is a triality form. In case it is of type ${}^6D_4$, we fix a field extension K' of k of degree 3 contained in K. In case G is of type ${}^3D_4$, we have the following from [D: 2.34(*)]:

$$b_\beta(t, s^{-1}) = b_\alpha(s, N_{K/k}(t)^{-1}) \text{ for all } s \in k^* \text{ and } t \in K^*;$$

and if G is of type ${}^6D_4$, then we have the following (see [D: 2.35]):

$$b_\beta(t, s^{-1}) = b_\alpha(s, N_{K'/k}(t)^{-1}) \text{ for all } s \in k^* \text{ and } t \in K'^*.$$

Since we can find some $s \in k^*$ and $t \in K^*$ (resp. $t \in K'^*$) such that the value of the μ-power norm residue symbol $(s, N_{K/k}(t))$ (resp. $(s, N_{K'/k}(t))$) is a generator of $\mu(k)$, the proposition follows for the triality forms. Thus we have proved the proposition in all cases.

Commutator maps. Our analysis of central extensions in this paper uses commutator maps: Given a central extension

$$1 \to I \longrightarrow E \xrightarrow{\pi} F \to 1, \tag{1}$$

one defines the commutator map $c_\pi\colon F \times F \to E$ as follows. For $x, y \in F$ we pick any lifts $\tilde{x} \in \pi^{-1}(x)$, $\tilde{y} \in \pi^{-1}(y)$, and let

$$c_\pi(x, y) = [\tilde{x}, \tilde{y}],$$

where $[\tilde{x}, \tilde{y}]$ is the commutator $\tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1}$. Since I is contained in the center of E, this commutator depends only on x, y, and not on the choice of the lifts $\tilde{x}, \tilde{y}$; thus c_π is well-defined. Moreover, if (1) is a topological extension, then c_π is a continuous map.

Now let F_1 and F_2 be two subgroups of F which commute elementwise (an important particular case is $F_1 = F_2$, a commutative subgroup of F). Then $c_\pi(F_1 \times F_2) \subset I$, and the restriction $\mathfrak{c}_\pi$ of c_π to $F_1 \times F_2$ is bimultiplicative. So, if one of the groups F_i is perfect (if π is continuous, it suffices to assume that the commutator subgroup is dense), then $\mathfrak{c}_\pi$ is forced to be trivial, and we conclude the following.

Lemma 1.4 *If two subgroups F_1, F_2 of F commute elementwise, then so do their pullbacks $\pi^{-1}(F_1)$, $\pi^{-1}(F_2)$, provided that one of the groups is its own (topological) commutator.*

Our proof of the main theorem for the groups of type A_r will use a formula due to Kazhdan and Patterson [KPa: 0.1.5] for the commutator of lifts of two elements lying in a maximal torus of the group $G = \mathbf{SL}_n$. We shall describe this formula now. Let $\ell_1, \ldots, \ell_s$ be field extensions of k such that $[\ell_1 : k] + \ldots + [\ell_s : k] = n$. Using the sum of corresponding regular representations, one imbeds $C_0 = R_{\ell_1/k}(\mathbf{GL}_1) \times \ldots \times R_{\ell_s/k}(\mathbf{GL}_1)$ into $\mathbf{GL}_n$ as a maximal k-torus. Let $C = C_0 \cap \mathbf{SL}_n$ be the corresponding maximal torus in $\mathbf{SL}_n$.

Proposition 1.5 *If the topological central extension*

$$1 \to I \longrightarrow E \xrightarrow{\pi} G(k) \to 1$$

corresponds to the element $\chi \in \hat{\mu}(k)$ (see 1.1), then for $a = (a_1, \ldots, a_s)$, $b = (b_1, \ldots, b_s)$ in $C(k)$ and $\tilde{a} \in \pi^{-1}(a)$, $\tilde{b} \in \pi^{-1}(b)$,

$$[\tilde{a}, \tilde{b}] = \chi(\prod_{i=1}^{s} (a_i, b_i)_i),$$

where $(\star, \star)_i$ is the μ-power norm residue symbol on ℓ_i, $\mu := \#\mu(k)$.

A simple consequence of this result is the following well known:

Lemma 1.6 *Let $G = \mathbf{SL}_n$ and C be the diagonal maximal torus of G. If $n \geq 3$, the restriction map $H^2(G(k)) \to H^2(C(k))$ is injective.*

Indeed, let $x \in \mathrm{Ker}(H^2(G(k)) \to H^2(C(k)))$ and $\chi \in \hat{\mu}(k)$ be the associated character (1.1). Consider the following elements of $C(k)$:

$$a = \mathrm{diag}(\alpha^{-1}, \alpha, 1, \ldots, 1),\ b = \mathrm{diag}(1, \beta, \beta^{-1}, 1, \ldots, 1),\quad \alpha, \beta \in k^*.$$

The extension

$$1 \to I \longrightarrow E \xrightarrow{\pi} G(k) \to 1$$

corresponding to x splits over $C(k)$, implying that $[\tilde{a}, \tilde{b}] = 1$ for any lifts $\tilde{a} \in \pi^{-1}(a)$, $\tilde{b} \in \pi^{-1}(b)$. Then the formula in the preceding proposition yields $\chi((\alpha, \beta)) = 1$ for any $\alpha, \beta \in k^*$; where $(\star, \star)$ is the μ-power norm residue symbol on k. Hence $\chi = 1$ and x is trivial.

Notations. *In the rest of this paper we will use the following notation:* K will be a fixed global field (i.e., either a number field or the function field of a curve over a finite field), and G an absolutely simple, simply connected algebraic group defined over

K. We shall often view G as a K-subgroup of $\mathbf{SL}_N$ in terms of a fixed imbedding. For any commutative ring C, $G(C)$ will then denote the group $G \cap \mathbf{SL}_N(C)$.

For a global field F, V^F will denote the set of all places of F, V_∞^F (resp., V_f^F) the subset of archimedean (resp., nonarchimedean) places ($V_\infty^F = \emptyset$ if char $F > 0$). $\mu(F)$ will denote the finite group of roots of unity in F and $\hat{\mu}(F)$ its dual.

T will denote the set of nonarchimedean places where G is anisotropic. Following the usual practice, we shall also use "T" to denote a torus. We trust this will not cause any confusion.

For a nonarchimedean place v of K, $\mathfrak{o}_v$ will denote the ring of integers in the completion K_v and $\mathfrak{p}_v$ the maximal ideal of $\mathfrak{o}_v$. For a finite set S of places of K, $A(S)$ will denote the K-algebra of S-adeles, i.e. the restricted direct product of the K_v, $v \notin S$; $A := A(\emptyset)$. If S contains all the archimedean places, we shall denote by $\mathfrak{o}(S)$, the ring of elements in K which are integral at all $v \notin S$.

For a K-variety X, and a commutative K-algebra C, $X(C)$ will denote the set of C-rational points of X. If v is a place of K, then $X(K_v)$ will be assumed to carry the natural locally compact topology induced from that on K_v. For a finite set V of places of K, $X(V)$ will denote the product $\prod_{v \in V} X(K_v)$ with the product topology.

If L is a given finite extension of K, and v is a place of K, then $\bar{v} \mid v$ will denote a place $\bar{v}$ of L lying over v. If v has a unique extension to L, then the completion of L with respect to the unique extension will be denoted by L_v in the sequel.

Given a finite-dimensional semi-simple K-algebra A and a positive integer n, $\mathbf{GL}_{n,A}$ (resp. $\mathbf{SL}_{n,A}$) will denote the reductive (resp. semi-simple) algebraic K-group whose group of C-rational points, for any commutative K-algebra C, is the group $GL_n(A \otimes_K C)$ (resp. $SL_n(A \otimes_K C)$). In particular, $\mathbf{GL}_1$ is a one dimensional split torus. If L/K is a finite (seperable) extension, then $R_{L/K}(\mathbf{GL}_1)$ (resp., $R^{(1)}_{L/K}(\mathbf{GL}_1)$) is the K-torus associated with the multiplicative group of L (resp., with the group $L^{(1)}$ of elements of norm 1 in the extension L/K).

For simplicity, we shall denote the i-th cohomology group of a locally compact topological group $\mathcal{G}$, with coefficients in $I = \mathbf{R}/\mathbf{Z}$, defined in terms of measurable cochains, by $H^i(\mathcal{G})$. We note that Wigner ([Wi]) has shown that for all zero-dimensional groups, the cohomology groups defined in terms of measurable cochains coincide with the cohomology groups defined in terms of continuous cochains. We also note that for the cohomology theory based on measurable cochains, the Künneth formula is valid and the Lyndon-Hochschild-Serre spectral sequence is available. We mention that cohomological techniques are not extensively used in this paper, and whenever possible, we work with the central extension corresponding to a second cohomology class rather than with the cohomology class itself.

For a finite set V of places of K, we shall denote the kernel of the natural restriction map $H^2(G(V)) \to H^2(G(K))$ by $M_V(G)$.

Local sections. We will frequently use the fact that any topological central extension admits a continuous local section.

Lemma 1.7 *Let V be a finite set of places of K and $G(V) = \prod_{v \in V} G(K_v)$. Given a topological central extension*

$$1 \to I \longrightarrow E \xrightarrow{\pi} G(V) \to 1,$$

there exists an open neighborhood Ω of the identity in $G(V)$ and a continuous map $\theta: \Omega \to E$ (a "local section") such that $\pi \circ \theta = id_\Omega$ and $\theta(xy) = \theta(x)\theta(y)$ for any $x, y \in \Omega$ such that $xy \in \Omega$.

PROOF. Let V_1 (resp., V_2) be the set of all archimedean (resp., nonarchimedean) places in V, $F_i = G(V_i)$. Then $G(V) = F_1 \times F_2$, and by Lemma 1.4 the subgroups $E_1 = \pi^{-1}(F_1)$ and $E_2 = \pi^{-1}(F_2)$ of E commute elementwise. Since the simply connected covering of F_1 is its universal topological central extension, there exists a local section $\theta_1: \Omega_1 \to E_1$ over a suitable open neighborhood Ω_1 of the identity in F_1. On the other hand, there clearly exists a continuous group-theoretic section $\theta_2: \Omega_2 \to E_2$ over a suitable open subgroup Ω_2 of F_2. Then we let $\Omega = \Omega_1 \times \Omega_2$ and define a local section $\theta: \Omega \to E$ by the formula: $\theta((x_1, x_2)) = \theta_1(x_1)\theta(x_2)$.

A consequence of this fact that we will use most is the following: Let Ω be as above, and let Θ be an open neightborhood of the identity in $G(V)$ such that $\Theta\Theta \subset \Omega$. *If elements $x, y \in \Theta$ commute, then so do any lifts $\tilde{x} \in \pi^{-1}(x)$, $\tilde{y} \in \pi^{-1}(y)$.*

1.8. Adelic results. We begin by observing that if a place v of K is either archimedean, or it is nonarchimedean and G is K_v-isotropic, then the affirmative solution of the Kneser-Tits problem over local fields ([PrRa3]) implies that $H^1(G(K_v)) = 1$. Hence, for any finite set V of such places and $G(V) = \prod_{v \in V} G(K_v)$,

$$H^2(G(V)) = \prod_{v \in V} H^2(G(K_v)).$$

On the other hand, the discussion in [PrRa1: 2.2-2.3] shows that for almost all nonarchimedean v's, $H^1(G(\mathfrak{o}_v))$ vanishes, and the restriction homomorphism $H^2(G(K_v)) \to H^2(G(\mathfrak{o}_v))$ is trivial. (It is, in fact, not hard to prove using Proposition 2.5.7.1 of [L : Ch. V] that if K is a number field, then for almost all nonarchimedean v, both $H^1(G(\mathfrak{o}_v))$ and $H^2(G(\mathfrak{o}_v))$ vanish.) Collecting these facts together, one obtains the following description of $H^2(G(A(S)))$ (cf. [Mo: Theorem 12.1]): For any finite S' which contains S, and also all the nonarchimedean places where G is anisotropic,

$$H^2(G(A(S))) = H^2(G(S' - S)) \times \prod_{v \notin S'} H^2(G(K_v)). \tag{2}$$

Note the following consequence: There exists a finite S_0 containing all the archimedean places such that for any $\mathcal{S} \supset S_0$, the restriction map

$$H^2(G(A(\mathcal{S}))) \to \prod_{v \notin \mathcal{S}} H^2(G(\mathfrak{o}_v))$$

is trivial. This remark allows one to express the commutator of lifts of elements of the adele group in terms of "local" commutators. Let

$$1 \to I \longrightarrow E \xrightarrow{\pi} G(A(S)) \to 1$$

be a topological central extension. Fix a finite set S' containing S, all the archimedean places, and also all the nonarchimedean places where G is anisotropic. For $a = (a_v), b = (b_v) \in G(A(S))$, we let $a' = (a_v)_{v \in S'-S}$, $b' = (b_v)_{v \in S'-S}$ and pick $\tilde{a}' \in \pi^{-1}(a')$, $\tilde{b}' \in \pi^{-1}(b')$, $\tilde{a}_v \in \pi^{-1}(a_v)$, $\tilde{b}_v \in \pi^{-1}(b_v)$.

Lemma 1.9 *For $\tilde{a} \in \pi^{-1}(a)$, $\tilde{b} \in \pi^{-1}(b)$,*

$$[\tilde{a}, \tilde{b}] = [\tilde{a}', \tilde{b}'] \cdot \prod_{v \notin S'} [\tilde{a}_v, \tilde{b}_v],$$

and the product is convergent with respect to the family of finite subsets of the complement of S'.

Indeed, it follows from Lemma 1.4 that the groups $\pi^{-1}(G(S' - S))$ and $\pi^{-1}(G(A(S')))$ commute elementwise, and this implies that

$$[\tilde{a}, \tilde{b}] = [\tilde{a}', \tilde{b}'][\tilde{a}'', \tilde{b}''],$$

where $a'' = a(a')^{-1}$, $b'' = b(b')^{-1}$ and $\tilde{a}'' \in \pi^{-1}(a'')$, $\tilde{b}'' \in \pi^{-1}(b)$. Next, it follows from the above that there exists a finite set $\mathcal{S} \supset S'$ such that $H^1(\prod_{v \notin \mathcal{S}} G(\mathfrak{o}_v))$ vanishes, the restriction map $H^2(G(A(\mathcal{S}))) \to H^2(\prod_{v \notin \mathcal{S}} G(\mathfrak{o}_v))$ is trivial and $a_v, b_v \in G(\mathfrak{o}_v)$ for $v \notin \mathcal{S}$. If a_1, b_1 and a_2, b_2 are the projections of a'', b'' on $G(\mathcal{S} - S')$ and $G(A(\mathcal{S}))$ respectively, then again

$$[\tilde{a}'', \tilde{b}''] = [\tilde{a}_1, \tilde{b}_1][\tilde{a}_2, \tilde{b}_2]$$

and

$$[\tilde{a}_1, \tilde{b}_1] = \prod_{v \in \mathcal{S} - S'} [\tilde{a}_v, \tilde{b}_v]$$

for any lifts $\tilde{a}_i, \tilde{b}_i$ of a_i, b_i respectively. On the other hand, by our construction, there exists a unique continuous group-theoretic section $\varphi\colon \prod_{v \notin \mathcal{S}} G(\mathfrak{o}_v) \to E$ of π over $\prod_{v \notin \mathcal{S}} G(\mathfrak{o}_v)$, and it is easy to see that the product $\prod_{v \notin \mathcal{S}} [\tilde{a}_v, \tilde{b}_v]$ converges to $[\varphi(a_2), \varphi(b_2)]$.

Lifts of automorphisms. Another tool used in the proof of the main theorem is the lifting of automorhisms to the central extension under consideration. Given a topological central extension

$$1 \to I \to E \xrightarrow{\pi} F \to 1 \tag{3}$$

of a locally compact topological group F, we say that $\tilde{\epsilon} \in \mathrm{Aut}(E)$ is *a lift* of $\epsilon \in \mathrm{Aut}(F)$ if $\pi(\tilde{\epsilon}(x)) = \epsilon(\pi(x))$ for any $x \in E$.

Proposition 1.10 *(i)* *If $\Gamma \subset F$ is an abstract subgroup and $\phi_i : \Gamma \to E$ $(i = 1, 2)$ are two group-theoretic sections of (3) over Γ (i.e. $\pi \circ \phi_i = \mathrm{id}_\Gamma$), then their restrictions to $[\Gamma, \Gamma]$ coincide.*

(ii) Suppose $\epsilon \in \mathrm{Aut}(F)$ can be lifted to $\tilde{\epsilon} \in \mathrm{Aut}(E)$. If $\Gamma \subset F$ is an ϵ-stable subgroup and $\phi : \Gamma \to E$ is a group-theoretic section of (3) over Γ, then $\phi(\epsilon(x)) = \tilde{\epsilon}(\phi(x))$ for all $x \in [\Gamma, \Gamma]$.

(iii) If $\epsilon, \tilde{\epsilon}$ are as in (ii), and $\Delta \subset F$ is a closed ϵ-stable subgroup such that $H^i(\Delta)$ vanishes for $i = 1, 2$, then there exists a unique continuous section $\phi : \Delta \to E$ of (3) over Δ, and for this section we have $\phi(\epsilon(x)) = \tilde{\epsilon}(\phi(x))$ for all $x \in \Delta$.

(iv) Suppose $F = F_1 \times F_2$ and $H^1(F_i)$ vanishes for at least one i, and let $\epsilon \in \mathrm{Aut}(F)$ be of the form $\epsilon = (\epsilon_1, \epsilon_2)$ where $\epsilon_i \in \mathrm{Aut}(F_i)$. Assume that each ϵ_i $(i = 1, 2)$ can be lifted to an automorphism $\tilde{\epsilon}_i$ of $E_i = \pi^{-1}(F_i)$ acting trivially on I. Then ϵ can also be lifted to $\tilde{\epsilon} \in \mathrm{Aut}(E)$ acting trivially on I.

PROOF. In the set-up of (i), the map $\chi(x) = \phi_1(x)\phi_2(x)^{-1}$ is easily seen to be a homomorphism of Γ into I (since (3) is a central extension), and the required fact follows. To prove (ii), we apply (i) to the sections ϕ and ψ, $\psi(x) = \tilde{\epsilon}^{-1}(\phi(\epsilon(x)))$. The assertion (iii) immediately follows from (i) and (ii). Finally, according to Lemma 1.4, the assumptions in (iv) imply that E_1 and E_2 commute elementwise. An arbitrary element $e \in E$ can be written in the form $e = e_1 e_2$, $e_i \in E_i$, and we set $\tilde{\epsilon}(e) = \tilde{\epsilon}_1(e_1)\tilde{\epsilon}_2(e_2)$. It is easily verified that $\tilde{\epsilon}$ is a well-defined automorphism of E.

1.11. We will need the existence of a lift in the following special case. Let $G = \mathbf{SL}_{1,D}$, $H = \mathbf{GL}_{1,D}$, where D is a quaternion central simple algebra over K. As observed in [PrRa2: 5.2], for a nonarchimedean $v \notin T$, the natural action of $H(K_v)$ on $H^2(G(K_v))$ is trivial (this is not true for the abstract cohomology, nor for the measurable cohomology if v is real). Using this observation, we prove the following:

Proposition 1.12 *(i) Let V be a finite set of places of K. Then there is an open subgroup W of $H(V)$ such that given a topological central extension*

$$1 \to I \longrightarrow E \xrightarrow{\pi} G(V) \to 1,$$

of $G(V)$, for any $a \in W$, the automorphism $\epsilon_a = \mathrm{Int}\ a$ lifts to an automorphism $\tilde{\epsilon}_a$ of E.

(ii) Given a finite set S_0 of places of K containing $T \cup V_\infty^K$ and a topological central extension

$$1 \to I \longrightarrow E \xrightarrow{\rho} G(A(S_0)) \to 1,$$

(1) the automorphism $\epsilon_a = \mathrm{Int}\ a$, $a \in H(A(S_0))$, admits a unique lift $\tilde{\epsilon}_a$ to E;

(2) for $a = (a_v) \in H(A(S_0))$, $b = (b_v) \in G(A(S_0))$ and $\tilde{b} \in \rho^{-1}(b)$, we have

$$\tilde{\epsilon}_a(\tilde{b})(\tilde{b})^{-1} = \prod_{v \notin S_0} (\tilde{\epsilon}_{a_v}(\tilde{b}_v)(\tilde{b}_v)^{-1}), \tag{4}$$

where $\tilde{b}_v \in \rho^{-1}(b_v)$ *and* $\tilde{\epsilon}_{a_v}$ *is the lift of the inner automorphism corresponding to the element* $(1, \ldots, 1, a_v, 1, \ldots)$.

(Note that the product above which is infinite, is understood in the sense of natural convergence, see the proof.)

PROOF. (i) If K is of characteristic zero, for W we take $\prod_{v\in V} K_v^* \cdot G(V)$ which is an open subgroup of $H(V)$. Any element $a \in W$ can be written in the form $a = x \cdot b$, where $x \in \prod_{v\in V} K_v^*$, $b \in G(V)$, and then the inner automorphism $\mathrm{Int}\,\tilde{b}$, for any $\tilde{b} \in \pi^{-1}(b)$ is a lift of ϵ_a.

In case K is of positive characteristic we need to argue differently. First of all, since by Künneth formula, $H^2(G(V-T)) = \prod_{v\in V-T} H^2(G(K_v))$, we conclude from the observation in [PrRa2: 5.2] that $H(V-T)$ acts trivially on $H^2(G(V-T))$, and this implies that for any $x \in H(V-T)$, ϵ_x admits a unique lift to an automorphism of $\mathcal{E} := \pi^{-1}(G(V-T))$. Indeed, since the cohomology class in $H^2(G(V-T))$ corresponding to $\pi \mid \mathcal{E}$ is fixed under ϵ_x, there exists an endomorphism $\tilde{\epsilon}_x : \mathcal{E} \to \mathcal{E}$ such that the following diagram is commutative:

$$\begin{array}{ccccccccc}
1 & \to & I & \longrightarrow & \mathcal{E} & \xrightarrow{\pi} & G(V-T) & \to & 1 \\
 & & \| & & \downarrow \tilde{\epsilon}_x & & \downarrow \epsilon_x & & \\
1 & \to & I & \longrightarrow & \mathcal{E} & \xrightarrow{\pi} & G(V-T) & \to & 1.
\end{array}$$

Since $G(V-T) = [G(V-T), G(V-T)]$, the lift $\tilde{\epsilon}_x$ is unique. This implies, in particular, that $\tilde{\epsilon}_{x^{-1}} = (\tilde{\epsilon}_x)^{-1}$, and hence, $\tilde{\epsilon}_x$ is an automorphism of $\mathcal{E}$.

Now, in view of Proposition 1.10 (iv), it suffices to show that ϵ_x, for any x in $W_0 = \prod_{v\in T}(1+\mathfrak{P}_v)$, where $\mathfrak{P}_v$ is the valuation ideal in the division algebra $D_v = D \otimes_K K_v$, can be lifted to the induced extension

$$1 \to I \longrightarrow \pi^{-1}(G(T)) \longrightarrow G(T) \to 1.$$

(Then $W = W_0 \times \prod_{v\in V-T} H(K_v)$ will do.) According to [PrRa4: 7.1], for every $v \in T$, $H^2(G(K_v))$ vanishes, so there exists a continuous group-theoretic section $\varphi_v : G(K_v) \to \pi^{-1}(G(T))$. Then $\varphi = \prod_{v\in T} \varphi_v : G(T) \to \pi^{-1}(G(T))$ is a continuous (but not necessarily a group-theoretic) section. Any element g of $\pi^{-1}(G(T))$ can be uniquely written as $g = i \cdot \varphi(b)$, $i \in I$, $b \in G(T)$, and we define $\tilde{\epsilon}_x$ by setting $\tilde{\epsilon}_x(g) = i \cdot \varphi(\epsilon_x(b))$. Using the fact that W_0 acts trivially on $G(T)/[G(T), G(T)]$ (indeed, it follows from Riehm [Ri: §5] that $[G(T), G(T)] = G(T) \cap W_0$), one readily verifies that $\tilde{\epsilon}_x$ thus defined is a (continuous) group automorphism.

(ii) Since $H^2(G(A(S_0)))$ has a canonical identification with $\prod_{v\notin S_0} H^2(G(K_v))$ (1.8) we conclude that the natural action of $H(A(S_0))$ on $H^2(G(A(S_0)))$ is trivial. Then an argument similar to the one used above for the extension $\mathcal{E}$ of $G(V-T)$ shows that for any $a \in H(A(S_0))$, the automorphism $\epsilon_a = \mathrm{Int}\, a$ has a unique lift $\tilde{\epsilon}_a$ to an automorphism of E. The uniqueness of the lift also implies that $a \mapsto \tilde{\epsilon}_a$ is a homomorphism of $H(A(S_0))$ into $\mathrm{Aut}(E)$.

To prove the remaining assertion of the proposition, we fix a finite subset $\mathcal{S} = \{v_1, \ldots, v_r\} \subset V^K - S_0$, and introduce the corresponding "truncated" adeles

$$a_r = (a_{v_1}, \ldots, a_{v_r}, 1, \ldots), \quad b_r = (b_{v_1}, \ldots, b_{v_r}, 1, \ldots).$$

Also, let $c_r = a_r^{-1}a$ (so that $a = a_r c_r$), and pick the lifts $\tilde{b}_r$ in such a way that $\tilde{b}_r \to \tilde{b}$. Then

$$\tilde{\epsilon}_a(\tilde{b}_r) \to \tilde{\epsilon}_a(\tilde{b}). \tag{5}$$

On the other hand,

$$\tilde{\epsilon}_a(\tilde{b}_r) = \tilde{\epsilon}_{a_r}(\tilde{\epsilon}_{c_r}(\tilde{b}_r)) = \tilde{\epsilon}_{a_r}(\tilde{b}_r)$$

since $\tilde{\epsilon}_{c_r}(\tilde{b}_r) = \tilde{b}_r$ (indeed, the map $G(\mathcal{S}) \to I$, $g \mapsto \tilde{\epsilon}_{c_r}(\tilde{g})\tilde{g}^{-1}$, being a homomorphism, is forced to be trivial). By a similar argument, we see that

$$\tilde{\epsilon}_{a_r}(\tilde{b}_r)\tilde{b}_r^{-1} = \prod_{i=1}^{r} \tilde{\epsilon}_{a_{v_i}}(\tilde{b}_{v_i})\tilde{b}_{v_i}^{-1},$$

which together with (5) yields the required fact. Proposition 1.12 is proved.

1.13. *A reduction.* As observed in [PrRa1 : 3.5], given a G and a (finite) S, to prove that $M(S,G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$, it suffices to prove that for almost every v, $M(S \cup \{v\}, G)$ is trivial. For the sake of completeness, we will briefly recall this argument.

For any two finite sets $S_1 \subset S_2$ of places of K, we have a factorization

$$G(A(S_1)) = G(A(S_2)) \times G(S_2 - S_1)$$

which allows us to define a map

$$\vartheta_{S_2}^{S_1} \colon H^2(G(A(S_2))) \longrightarrow H^2(G(A(S_1)))$$

with the following properties:

(1) $\vartheta_{S_2}^{S_1}$ is injective and its cokernel is $H^2(G(S_2 - S_1)) \times H^1(G(S_2 - S_1), H^1(G(A(S_2))))$;
(2) $\vartheta_{S_2}^{S_1}(M(S_2, G)) \subset M(S_1, G)$.

Let $S_1 = S$, $S_2 = S \cup \{v\}$, where v is chosen so that $M(S \cup \{v\}, G)$ is trivial and G is K_v-isotropic (this is the case for almost every v). Then $M(S,G)$ is isomorphic to a subgroup of $H^2(G(K_v))$, which in turn is isomorphic to a subgroup of $\hat{\mu}(K_v)$. It follows from Chebotarev's density theorem that the g.c.d. of the numbers $\mu_v = \#\mu(K_v)$ taken over any set containing all but finitely many nonarchimedean places, equals $\mu = \#\mu(K)$. Thus, the image of the imbedding $M(S,G) \hookrightarrow \hat{\mu}(K_v)$ is contained in $\hat{\mu}(K)$, the latter being naturally imbedded in $\hat{\mu}(K_v)$ by the homomorphism dual to the following surjection: $\mu(K_v) \to \mu(K)$, $\xi \mapsto \xi^{t_v}$; $t_v = \mu_v/\mu$.

In the sequel, we will assume that S contains a place v_0 which is either nonarchimedean and G is K_{v_0}-isotropic, or it is real and the group $G(K_{v_0})$ is not (topologically) simply connected, and prove that $M(S,G)$ is trivial. We shall separately prove that $M(\emptyset, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$ of index at most two. In view of the reduction described above, this will prove the main theorem.

2 The archimedean places and $M_V(G)$

Let V be a finite set of places of K. The goal of this section is to prove that $M_V(G) = M_{V_0}(G)$, where V_0 is the set of nonarchimedean places in V. We shall also prove the finiteness of the metaplectic kernel $M(S,G)$.

If v is an archimedean place of K, then the group $G(K_v)$ is connected, and its simply connected covering is at the same time its universal toplological central extension; therefore, $H^2(G(K_v)) = \mathrm{Hom}(\pi_1(G(K_v)), I)$ where $\pi_1(G(K_v))$ is the (topological) fundamental group. It follows that $H^2(G(K_v))$ is trivial either if v is complex, or if it is real and the group $G(K_v)$ is compact (i.e. G is K_v-anisotropic). Since, by the Künneth formula

$$H^2(G(V)) = H^2(G(K_v)) \times H^2(G(V - \{v\})), \tag{1}$$

for any finite set V of places of K and any archimedean $v \in V$, the computation of $M_V(G)$ is reduced to the case where V does not contain any archimedean places v such that the fundamental group $\pi_1(G(K_v))$ is trivial, in particular, any complex or real anisotropic places. On the other hand, if $\pi_1(G(K_v))$ is nontrivial, then it is either $\mathbf{Z}_2$, the cyclic group of order 2, or $\mathbf{Z}$. The first case occurs when a maximal compact subgroup $\mathcal{C}$ of $G(K_v)$ is a semi-simple Lie group, while the second one corresponds to the case where $\mathcal{C}$ is an almost direct product of a one-dimensional compact torus $\mathcal{I}$ and a semi-simple simply connected compact Lie group $\mathcal{C}'$, and then the imbedding $\mathcal{I} \hookrightarrow \mathcal{C}$ induces an isomorphism of fundamental groups (recall that any two maximal compact subgroups of $G(K_v)$ are conjugate and the natural map of fundamental groups $\pi_1(\mathcal{C}) \to \pi_1(G(K_v))$ is an isomorphism, cf. [H]). Furthermore, as the following theorem shows, the computation of $M_V(G)$ can be reduced to the case where V does not contain real places of the first kind.

Theorem 2.1 *Let $\mathcal{V}$ be a subset of V consisting of real places v such that the maximal compact subgroups of $G(K_v)$ are semi-simple. Then $M_V(G) = M_{V'}(G)$, where $V' = V - \mathcal{V}$.*

Proof. It is clearly enough to prove the theorem in the case where $\mathcal{V}$ consists of a single place v. In view of (1), it suffices to show that for any element $x \in M_V(G)$, the image $\varphi(x)$, under the natural projection $\varphi\colon H^2(G(V)) \to H^2(G(K_v))$, is trivial. Fix an x in $M_V(G)$, and let

$$1 \to I \longrightarrow E \xrightarrow{\pi} G(V) \to 1$$

be the corresponding toplogical central extension. Then $\varphi(x)$ corresponds to the extension

$$1 \to I \longrightarrow E_0 = \pi^{-1}(G(K_v)) \xrightarrow{\pi_0} G(K_v) \to 1, \tag{2}$$

where $\pi_0 = \pi \mid E_0$, and we need to show that the extension (2) is trivial. Assume, if possible, that $\varphi(x)$ is nontrivial. We claim that then there exists a maximal K-torus B of G such that $\pi_0^{-1}(B(K_v))$ is noncommutative. Indeed, if

$$1 \to \Gamma \longrightarrow F \xrightarrow{\rho} G(K_v) \to 1$$

is the simply connected covering of the connected Lie group $G(K_v)$, then there exists a commutative diagram :

$$\begin{array}{ccccccccc} 1 & \to & I & \longrightarrow & E_0 & \xrightarrow{\pi_0} & G(K_v) & \to & 1 \\ & & \theta\uparrow & & \delta\uparrow & & \| & & \\ 1 & \to & \Gamma & \longrightarrow & F & \xrightarrow{\rho} & G(K_v) & \to & 1 \end{array}$$

Since $\varphi(x)$ is assumed to be nontrivial, θ, and so also δ, is injective (recall that $\Gamma = \mathbf{Z}_2$). To prove the claim, it suffices to show that there exists a maximal K-torus B of G such that $\rho^{-1}(B(K_v))$ is noncommutative.

Let $\mathcal{C}$ be a maximal compact subgroup of $G(K_v)$ and $\mathcal{T}$ be a maximal torus of $\mathcal{C}$. As we mentioned above, the map $\pi_1(\mathcal{C}) \to \pi_1(G(K_v))$ is an isomorphism, while the map $\pi_1(\mathcal{T}) \to \pi_1(\mathcal{C})$ is known to be surjective (this is a consequence of the fact that $\mathcal{C}/\mathcal{T}$ is simply connected). It follows that there can be no continuous section of ρ over $\mathcal{T}$. Now, since $\mathcal{C}$ is assumed to be semi-simple, the normalizer $N_{\mathcal{C}}(\mathcal{T})$ contains an element w such that the automorphism of the character group $X(\mathcal{T}) = \mathrm{Hom}_{ct}(\mathcal{T}, I)$ induced by Int w has no nontrivial fixed points (the Coxeter element in the Weyl group $N_{\mathcal{C}}(\mathcal{T})/\mathcal{T}$ has this property). Then any element of $\mathcal{T}$ is a commutator of the form $[t, w] = twt^{-1}w^{-1}$, for some $t \in \mathcal{T}$. So, if we assume for a moment that for any $t_1, t_2 \in \mathcal{T}$ satisfying

$$[t_1, w] = [t_2, w] \tag{3}$$

we have

$$[\tilde{t}_1, \tilde{w}] = [\tilde{t}_2, \tilde{w}] \tag{4}$$

for some (equivalently, for arbitrary) lifts

$$\tilde{t}_i \in \rho^{-1}(t_i) \ \ (i = 1, 2), \quad \tilde{w} \in \rho^{-1}(w),$$

we could construct a map

$$\varphi\colon \mathcal{T} \to F, \quad x = [t, w] \mapsto [\tilde{t}, \tilde{w}], \quad \tilde{t} \in \rho^{-1}(t),$$

which would be a well-defined continuous section of ρ over $\mathcal{T}$. Since, as observed above, such a section cannot exist, we conclude that there are elements $t_1, t_2 \in \mathcal{T}$ satisfying

(3), but not (4). Let $h = t_2^{-1} \cdot t_1$, $\tilde{h} = \tilde{t}_2^{-1} \cdot \tilde{t}_1$. Obviously, $\tilde{h} \in \rho^{-1}(h)$, $wh = hw$ but $\tilde{w}\tilde{h} \neq \tilde{h}\tilde{w}$. Now since G is a simply connected group and h and w are two commuting semi-simple elements of $G(K_v)$, there exists a maximal K_v-torus B' of G such that both h and w lie in $B'(K_v)$. As $\tilde{h}$ and $\tilde{w}$ do not commute, $\rho^{-1}(B'(K_v))$ is noncommutative. Then $\rho^{-1}(B(K_v))$ is noncommutative for any torus B met4.tex which is conjugate to B' by an element of $G(K_v)$. Among these conjugates there exists a torus B defined over K (cf. [PR2], §7.1). This proves our claim.

It follows, for example, from the proof of Proposition 7.8 of [PR2], that the closure of $B(K)$ in $B(V)$ is of the form $B(K_v) \times \Omega$, for some open subgroup $\Omega \subset B(V')$, $V' = V - \{v\}$. According to 1.7, there exists an open neighborhood Θ of the identity in $G(V')$ such that for any commuting elements $x, y \in \Theta$, any lifts $\tilde{x} \in \pi^{-1}(x)$, $\tilde{y} \in \pi^{-1}(y)$ commute. By our construction, there are $c, d \in B(K_v)$ such that the lifts $\tilde{c} \in \pi^{-1}(c), \tilde{d} \in \pi^{-1}(d)$ do not commute, and then one can find open neighborhoods W_c and W_d, respectively, of c and d in $B(K_v)$ such that $\tilde{a}\tilde{b} \neq \tilde{b}\tilde{a}$ for any lifts $\tilde{a}$, $\tilde{b}$ of elements $a \in W_c$, $b \in W_d$. In view of the density of $B(K)$ in $B(K_v) \times \Omega$, one can find elements

$$s \in B(K) \cap (W_c \times (\Omega \cap \Theta)), \quad t \in B(K) \cap (W_d \times (\Omega \cap \Theta)).$$

To calculate the commutator $[\tilde{s}, \tilde{t}]$ of the lifts $\tilde{s} \in \pi^{-1}(s)$, $\tilde{t} \in \pi^{-1}(t)$, write s, t in the form $s = s_1 s_2, t = t_1 t_2$, where $s_1 \in W_c$, $t_1 \in W_d$ and $s_2, t_2 \in \Omega \bigcap \Theta$, and pick any lifts $\tilde{s}_i \in \pi^{-1}(s_i)$, $\tilde{t}_i \in \pi^{-1}(t_i)$, $i = 1, 2$. Since the subgroups $\pi^{-1}(G(K_v))$ and $\pi^{-1}(G(V'))$ of E commute elementwise (1.4), we have:

$$[\tilde{s}, \tilde{t}] = [\tilde{s}_1, \tilde{t}_1][\tilde{s}_2, \tilde{t}_2] = [\tilde{s}_1, \tilde{t}_1] \neq 1.$$

On the other hand, since s, t commute in $G(K)$ and π splits over $G(K)$, we should have $[\tilde{s}, \tilde{t}] = 1$. A contradiction, which proves the theorem.

Thus, the computation of $M_V(G)$ is reduced to the case where every archimedean place v in V is real and the maximal compact subgroups of $G(K_v)$ are not semi-simple. Unfortunately, we have not been able to give a uniform proof of the fact that $M_V(G) = M_{V_0}(G)$, so we need to treat each type seperately. First, we consider the groups of type A_1.

Proposition 2.2 *Let G be an absolutely simple simply connected K-group of type A_1. Then for any finite subsets $V_1 \subset V_\infty^K$, $V_2 \subset V_f^K$, and any open subgroup U of $G(V_2)$, the restriction map $H^2(G(V_1)) \to H^2(G(K) \cap U)$ is injective. Consequently, for any finite set V of places of K, $M_V(G) = M_{V_0}(G)$, where V_0 consists of all the nonarchimedean places in V.*

Proof. We begin with some elementary remarks concerning the simply connected covering $\rho: \tilde{\mathcal{G}} \to \mathcal{G}$ of the group $\mathcal{G} = \mathbf{SL}_2(\mathbf{R})$. The maximal compact subgroup SO_2 of $\mathcal{G}$ consists of:

$$\delta(t) = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}, \quad t \in \mathbf{R}.$$

Obviously, there exists an imbedding $\tilde{\delta}: \mathbf{R} \to \tilde{\mathcal{G}}$ such that $\delta(t) = \rho \circ \tilde{\delta}(t)$, and then $\operatorname{Ker} \rho = \tilde{\delta}(2\pi \mathbf{Z})$. So, the element $a = \tilde{\delta}(\pi)$ belongs to the fibre $\rho^{-1}(-1)$ and its square $a^2 = \tilde{\delta}(2\pi)$ generates $\operatorname{Ker} \rho$.

Now let Δ_+ (resp. Δ_-) be the open set of all semi-simple elements of $\mathcal{G}$ with real and *positive* (resp. *negative*) eigenvalues. Using the logarithm and exponential maps it is easily seen that both Δ_+ and Δ_- are contractible. Hence, every connected component of $\rho^{-1}(\Delta_+)$ (resp., of $\rho^{-1}(\Delta_-)$) is mapped under ρ homeomorphically onto Δ_+ (resp. Δ_-); let $\tilde{\Delta}_+$ (resp., $\tilde{\Delta}_-$) be the connected component passing through e, the identity of $\tilde{\mathcal{G}}$, (resp., through $\tilde{\delta}(\pi)$).

Let T be a nontrivial $\mathbf{R}$-split torus of $\mathbf{SL}_2$ and $h \in \mathcal{H} := GL_2(\mathbf{R})$ be an element with positive determinant such that

$$hth^{-1} = t^{-1} \quad \text{for any } \ t \in T.$$

As $\det h > 0$, $h = gs$, where $g \in \mathcal{G}$ and s is a scalar matrix. Then if $\tilde{g} \in \rho^{-1}(g)$, $\tilde{\sigma}_h := \operatorname{Int} \tilde{g}$ lifts the inner automorphism $\sigma_h = \operatorname{Int} h$ and acts trivially on $\operatorname{Ker} \rho \simeq \pi_1(\mathcal{G})$. We claim that

(a) for any $x \in \tilde{T}_+ := \rho^{-1}(T(\mathbf{R})) \cap \tilde{\Delta}_+$, $\tilde{\sigma}_h(x)x = e$,
(b) for any $x \in \tilde{T}_- := \rho^{-1}(T(\mathbf{R})) \cap \tilde{\Delta}_-$, $\tilde{\sigma}_h(x)x = \tilde{\delta}(2\pi)$.

Indeed, both $\tilde{T}_+$ and $\tilde{T}_-$ are connected; on the other hand, the expression $\tilde{\sigma}_h(x)x$ for any $x \in \rho^{-1}(T(\mathbf{R}))$ belongs to $\operatorname{Ker} \rho$, which is discrete. Hence, $\tilde{\sigma}_h(x)x$ is constant along each of $\tilde{T}_+$ and $\tilde{T}_-$. Since $e \in \tilde{T}_+$, we immediately obtain (a). To prove (b), it suffices to show that for $a = \tilde{\delta}(\pi) \in \tilde{T}_-$, $\tilde{\sigma}_h(a)a = \tilde{\delta}(2\pi)$. The latter is equivalent to the fact that $\tilde{\sigma}_h(a) = a$. Since -1 lies in the center of $\mathcal{G}$, and $\tilde{\mathcal{G}}$ is connected, the fiber $\rho^{-1}(-1)$, being discrete, is entirely contained in the center of $\tilde{\mathcal{G}}$. Since $\tilde{\sigma}_h = \operatorname{Int} \tilde{g}$ in the above notations, the required fact follows.

Now we are in a position to prove our proposition. We have: $G = \mathbf{SL}_{1,D}$, D a quaternion central algebra over K. Let $H = \mathbf{GL}_{1,D}$. For any nonarchimedean v, there exists an open subset $\Omega_v \subset G(K_v)$, $\Omega_v \cap \{\pm 1\} = \emptyset$, with the following properties:

(i) Ω_v intersects every open subgroup of $G(K_v)$;

(ii) $G(K_v)$ admits a fundamental system $\{U_v\}$ of neighborhoods of the identity consisting of compact open subgroups normalized by some (fixed) open subgroup N_v such that for any $t \in \Omega_v$, there exists an $h \in N_v$ such that $hth^{-1} = t^{-1}$.

If $D_v = D \otimes_K K_v$ is a division algebra, take $G(K_v) - \{\pm 1\}$ to be Ω_v and for $\{U_v\}$ take the system of congruence subgroups $G(K_v) \cap (1 + \mathfrak{P}_v^l)$, $l \geq 1$, where $\mathfrak{P}_v$ is the valuation ideal in D_v. Then each of the U_v's is a normal subgroup of D_v^*, so that one can take $N_v = D_v^*$. If D_v is not a division algebra, it is isomorphic to $M_2(K_v)$ and $G(K_v) \simeq \mathbf{SL}_2(K_v)$. In this case take N_v to be $\mathbf{GL}_2(\mathfrak{o}_v)$ and take Ω_v to be $\cup_{n \in N_v} nM_v n^{-1}$, where M_v is the set of diagonal matrices in $\mathbf{SL}_2(\mathfrak{o}_v)$ different from ± 1, and for $\{U_v\}$ take the family of congruence subgroups

$$\{g \in \mathbf{SL}_2(\mathfrak{o}_v) \mid g \equiv 1 \bmod \mathfrak{p}_v^l\}, \quad l \geq 1.$$

Obviously, for any $t \in \Omega_v$, there exists an element h with the required property in the N_v-conjugacy class of the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Now, we may assume that the subgroup U in the statement of the proposition is of the form: $U = \prod_{v \in V_2} U_v$, where for every v the corresponding local factor belongs to the family $\{U_v\}$ specified in (ii).

As explained above, it suffices to consider the case where V_1 contains neither a complex place nor any real place at which G is anisotropic, i.e., we may assume that for $v \in V_1$, $K_v = \mathbf{R}$ and G is K_v-isomorphic to $\mathbf{SL}_2$. Let

$$1 \to I \longrightarrow E \xrightarrow{\pi} G(V_1) \to 1 \tag{5}$$

be a topological central extension which splits over the group $G(K) \cap U$. For each $v \in V_1$, let

$$\rho_v : \tilde{\mathcal{G}}(v) \longrightarrow G(K_v)$$

be the simply connected covering. Then

$$\rho_{V_1} : \tilde{\mathcal{G}}(V_1) = \prod_{v \in V_1} \tilde{\mathcal{G}}(v) \longrightarrow G(V_1)$$

is the universal topological central extension of $G(V_1)$, and by the universal property there exists a commutative diagram as follows:

$$\begin{array}{ccccccccc} 1 & \to & I & \longrightarrow & E & \xrightarrow{\pi} & G(V_1) & \to & 1 \\ & & \alpha \uparrow & & \beta \uparrow & & \| & & \\ 1 & \to & \Gamma & \longrightarrow & \tilde{\mathcal{G}}(V_1) & \xrightarrow{\rho_{V_1}} & G(V_1) & \to & 1, \end{array}$$

where $\Gamma = \operatorname{Ker} \rho_{V_1}$. To prove that (5) is a trivial extension we need to show that $\alpha(\Gamma) = \{1\}$. Assume the contrary. Then there exists a proper subgroup Γ' of Γ of finite index containing $\operatorname{Ker} \alpha$. Take the quotient of ρ_{V_1} by Γ':

$$1 \to \Lambda = \Gamma/\Gamma' \longrightarrow F = \tilde{\mathcal{G}}(V_1)/\Gamma' \xrightarrow{\lambda} G(V_1) \to 1. \tag{6}$$

If $\varphi : G(K) \cap U \to E$ is a cross-section of (5), then for $\Sigma = [G(K) \cap U, G(K) \cap U]$, $\varphi(\Sigma)$ is contained in $\operatorname{Im} \beta$, hence there exists a group-theoretic section $\psi : \Sigma \to F$ of the extension (6). We claim that $\psi([\Sigma, \Sigma])$ is dense in F. Indeed, by the weak approximation property for G, $G(K) \cap U$ is dense in $G(V_1)$ which, as $G(V_1) = [G(V_1), G(V_1)]$, implies the density of Σ and $[\Sigma, \Sigma]$. Since λ is a closed map, $M = \overline{\psi([\Sigma, \Sigma])}$ maps onto $G(V_1)$. Thus, $F = \Lambda \cdot M$, i.e. M is a closed subgroup of F of finite index, hence $F = M$ since F is connected. For our argument we will need a slightly stronger fact: if $\Omega = \prod_{v \in V_2} \Omega_v$, then $\psi([\Sigma, \Sigma] \cap \Omega)$ is also dense in F. Indeed, it follows again from the weak approximation property that the closure of $[\Sigma, \Sigma]$ in $G(V_2)$ is open, so by property (i) of the Ω_v's, the intersection $[\Sigma, \Sigma] \cap \Omega$ is nonempty; let g be an element of this set. Obviously, Ω contains a set of the form gU' for some open subgroup $U' \subset U$. Then

$$\psi([\Sigma, \Sigma] \cap \Omega) \supset \psi(g) \cdot \psi([\Sigma, \Sigma] \cap U').$$

On the other hand, $[\Sigma,\Sigma]\cap U'$ is a subgroup of $[\Sigma,\Sigma]$ of finite index, so the density of $\psi([\Sigma,\Sigma])$ implies that of $\psi([\Sigma,\Sigma]\cap U')$, since F is connected.

Being a proper subgroup of Γ, Γ' cannot contain $\mathrm{Ker}\,\rho_v$ for all $v\in V_1$; fix a $w\in V_1$ such that $\mathrm{Ker}\,\rho_w\not\subset\Gamma'$. For $v\in V_1$, let $\tilde\Delta_+(v)$ and $\tilde\Delta_-(v)$ be the open subsets of $\tilde{\mathcal{G}}(v)$ obtained by applying the construction described at the beginning of the proof to the covering ρ_v. Let

$$\tilde W=\tilde\Delta_-(w)\times\prod_{v\in V_1,\ v\neq w}\tilde\Delta_+(v),$$

and let W denote the image of $\tilde W$ in F. In view of the density of $\psi([\Sigma,\Sigma]\cap\Omega)$, there exists a $t\in[\Sigma,\Sigma]\cap\Omega$ such that $\psi(t)\in W$. Let $L=K(t)$; it is a maximal commutative semisimple subalgebra of D. Let $T_0=R_{L/K}(\mathbf{GL}_1)$ and $T=R^{(1)}_{L/K}(\mathbf{GL}_1)$ be the maximal K-tori defined by L in H and G respectively. According to the theorem of Skölem-Noether there exists an $h\in D^*$ such that $\mathrm{Int}\,h\mid L$ is the nontrivial automorphism of L/K, and then the set of elements of H with this property is precisely the coset hT_0. It follows from our construction that

$$h(\prod_{v\in V_1\cup V_2}T_0(K_v))\cap\prod_{v\in V_1\cup V_2}P_v\neq\emptyset,$$

where $P_v=N_v$ for $v\in V_2$, and P_v is the subgroup of $H(K_v)\simeq GL_2(K_v)$ of matrices whose determinant is positive in $K_v=\mathbf{R}$, for $v\in V_1$. Using weak approximation in T_0, we can assume h chosen so that it lies in P_v for every $v\in V_1\cup V_2$. Then, in particular, h normalizes U, and consequently, Σ. Now, if $\tilde\sigma_h$ denotes the lift of $\sigma_h=\mathrm{Int}\,h$ to E as well as F, it follows from 1.10 (ii) that

$$\psi(\sigma_h(x))=\tilde\sigma_h(\psi(x))\quad\text{for any}\ \ x\in[\Sigma,\Sigma].$$

Thus,

$$e=\psi(hth^{-1}t)=\tilde\sigma_h(\psi(t))\psi(t). \tag{7}$$

However, our previous computation shows that the element $\tilde\sigma_h(x)x$, for any $x\in\tilde W$, is a generator of $\mathrm{Ker}\,\rho_w$, which, by our construction, is not contained in Γ'; i.e., it has a nontrivial image in Λ. This implies that since $\psi(t)\in W$, $\tilde\sigma_h(\psi(t))\psi(t)\neq e$. A contradiction, which proves the first assertion of the proposition. To prove the second assertion, it remains to observe that as any cocycle in $H^2(G(V_2))$ restricts trivially to a suitable open subgroup U of $G(V_2)$, the projection of an arbitrary $x\in M_{V_1\cup V_2}(G)$ to $H^2(G(V_1))$ lies in $\mathrm{Ker}(H^2(G(V_1))\to H^2(G(K)\cap U))$ for some U.

Our next result follows immediately from Proposition 2.2.

Proposition 2.3 *Let $G=\mathbf{SU}(h)$, where h is a nondegenerate hermitian form in $n\geq 2$ variables over a quadratic extension L/K. Then for any finite set V of places of K, $M_V(G)=M_{V_0}(G)$, where V_0 consists of all the nonarchimedean places in V.*

PROOF. We may (and will) assume that every archimedean $v \in V$ is real, $[L_{\bar{v}}: K_v] = 2$ for $\bar{v} \mid v$, and the space $L_{\bar{v}}^n$ is not (positive or negative) definite with respect to h. A simple approximation argument shows then that one can pick two orthogonal vectors e_1, e_2 in L^n such that $h(e_1) > 0$ and $h(e_2) < 0$ in $K_v = \mathbf{R}$, for every $v \in V' := V - V_0$. Let $H = \mathbf{SU}(h')$ where h' is the restriction of h to the subspace generated by e_1 and e_2. Then H is a simple simply connected K-group of type A_1, and therefore $M_V(H) = M_{V_0}(H)$ by the previous proposition. On the other hand, a simple topological argument shows that for every $v \in V'$ the map $\pi_1(H(K_v)) \longrightarrow \pi_1(G(K_v))$ of fundamental groups is surjective (in fact, an isomorphism), implying that the restriction map $H^2(G(V')) \to H^2(H(V'))$ is injective, and since $H^2(G(V)) = H^2(G(V')) \times H^2(G(V_0))$, our assertion follows.

Using the same idea as in the proof of the last proposition, i.e. imbedding into a group G under consideration a smaller group H which "captures" the fundamental group of G at real places, and for which the equality $M_V(H) = M_{V_0}(H)$ has already been proved (in most cases one can take for H a group of type A_1), we will prove that $M_V(G) = M_{V_0}(G)$ for most of the groups. The only groups for which this argument does not work, and for which the triviality of $M_V(G)$ has not been established, are certain outer forms of type A_r (i.e. certain special unitary groups). We formulate the expected result for these groups in the form of the following conjecture. To be able to present the main results of this paper in a uniform way, we will assume this conjecture. We shall point out which of our results for the special unitary groups depend on the validity of this conjecture and which do not.

Conjecture (U): *Let $G = \mathbf{SU}(h)$ be the special unitary group of a nondegenerate hermitian form h over a noncommutative division algebra D with involution τ of the second kind (i.e. the center L of D is a quadratic extension of $K = L^{\tau}$). Then for any finite set V of places of K, $M_V(G) = M_{V_0}(G)$, where V_0 consists of all the nonarchimedean places in V.*

The results of this section will be used in the following sections to establish the triviality of $M_V(G)$ for any absolutely simple simply connected K-group G and an arbitrary finite set V of places of K (of course, for the "exceptional" special unitary groups this will depend on the conjecture (U)). It should be noted, however, that the proof of this fact for the groups of type A_1 which will be given in the next section (Proposition 3.2) does not use the preliminary reduction provided by Proposition 2.2 (viz., it applies equally whether or not V contains any archimedean places). The reason for including Proposition 2.2 in this section is that, in our opinion, the technique of its proof will be useful in establishing conjecture (U).

We conclude this section with the following finiteness result.

Theorem 2.4 *Let G be an absolutely simple simply connected algebraic group defined over a global field K. For any (possibly, empty) set S of places of K, the metaplectic kernel $M(S, G)$ is finite.*

This assertion was proved in [PrRa1: Theorem 2.10] if S contains V_∞^K, G is isotropic at v for all $v \notin S$ and $\sum_{v\in S} \mathrm{rank}_{K_v} G \geq 2$. Combining this result with the finiteness of $H^2(G(K_v))$ for any nonarchimedean v (if G is K_v-isotropic, the finiteness follows from [PrRa2: Theorem 9.4], and if G is K_v-anisotropic, it follows from Theorem 8.1 of [PrRa4] as in this case $G(K_v)$ is isomorphic to the group of the form $SL_1(D)$, for a central division algebra D over K_v), one can derive the finiteness of $M(S,G)$ for any S which contains V_∞^K, in particular, for arbitrary S in case K is a function field. Indeed, using, in addition, the well known finiteness of $H^1(G(K_v))$, and arguing by induction on the number of elements in a finite set V of nonarchimedean places of K with the help of the Künneth's formula, we obtain the finiteness of $H^2(G(V))$ for any such V. As we saw in §1.13, for any two finite sets $S_1 \subset S_2$ containing V_∞^K, there exists a map

$$\vartheta_{S_2}^{S_1}\colon H^2(G(A(S_2))) \longrightarrow H^2(G(A(S_1)))$$

whose cokernel is the finite group $H^2(G(S_2-S_1))\times H^1(G(S_2-S_1), H^1(G(A(S_1))))$, and $\vartheta_{S_2}^{S_1}(M(S_2,G)) \subset M(S_1,G)$. Thus, the finiteness of $M(S_2,G)$ implies that of $M(S_1,G)$, and our assertion follows. We observe that as the map $\vartheta_S^{\emptyset}$ imbeds $M(S,G)$ into $M(\emptyset,G)$, to prove Theorem 2.4, it is enough to prove the finiteness of the latter.

If G is K-isotropic, the finiteness of $M(\emptyset,G)$ is a consequence of Theorem 3.4 of [PrRa1]. The remaining case of a K-anisotropic group G over a number field K was considered by Raghunathan (cf. [Ra1], Theorem 2.1) using some topological arguments and the cocompactness of the arithmetic subgroups in $G_\infty := G(V_\infty^K)$. This argument does not appear to work if the group G is K-isotropic. So, one would naturally like to have a proof of the finiteness of $M(\emptyset,G)$ which is equally applicable to both, isotropic and anisotropic, cases. We will now show that the finiteness of $M(\emptyset,G)$ follows immediately from the triviality of $M_\infty(G) := M_{V_\infty^K}(G)$. We begin with the following consequence of the triviality of $M_\infty(G)$.

Lemma 2.5 *There exists a finite subset S_0 of V^K containing V_∞^K, such that for any $S \supset S_0$, $\mathrm{Ker}(H^2(G_\infty) \to H^2(G(\mathfrak{o}(S))))$ is finite.*

Proof. Let

$$1 \to \Gamma \longrightarrow F \xrightarrow{\rho} G_\infty \to 1, \quad \Gamma = \pi_1(G_\infty) \tag{8}$$

be the simply connected covering of G_∞. We claim that

$$\Gamma' = \Gamma \cap [\rho^{-1}(G(K)), \rho^{-1}(G(K))]$$

is of finite index in Γ. Indeed, in the quotient of (8) by Γ':

$$1 \to \Gamma/\Gamma' \longrightarrow F' = F/\Gamma' \xrightarrow{\rho'} G_\infty \to 1,$$

the restriction of ρ' to the image of $[\rho^{-1}(G(K)), \rho^{-1}(G(K))]$ is injective, so ρ' splits over $\Delta = [G(K), G(K)]$ implying that the dual group $(\Gamma/\Gamma')^*$ is imbeddable into the group $M = \operatorname{Ker}(H^2(G_\infty) \to H^2(\Delta))$. Let the index $[G(K) \colon \Delta]$, which is finite by [M1], be l. Considering the corestriction map $\operatorname{Cor}_{\Delta}^{G(K)}$, we find that

$$lM \subset \operatorname{Ker}(H^2(G_\infty) \to H^2(G(K))) = \{0\},$$

so M is a group of exponent l. Since Γ is finitely generated, we obtain that Γ/Γ' is finite, as claimed. Furthermore, by finite generation, there exists a finite set $S_0 \supset V_\infty^K$ such that $\Gamma' = \Gamma \cap [\rho^{-1}(G(\mathfrak{o}(S_0))), \rho^{-1}(G(\mathfrak{o}(S_0)))]$. We will show that this S_0 has the desired property.

Indeed, let

$$1 \to I \longrightarrow E \xrightarrow{\pi} G_\infty \to 1$$

be the extension corresponding to some $x \in \operatorname{Ker}(H^2(G_\infty) \to H^2(G(\mathfrak{o}(S))))$, where $S \supset S_0$. Then we have the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \to & I & \longrightarrow & E & \xrightarrow{\pi} & G_\infty & \to & 1 \\ & & \theta\uparrow & & \delta\uparrow & & \| & & \\ 1 & \to & \Gamma & \longrightarrow & F & \xrightarrow{\rho} & G_\infty & \to & 1 \end{array} \tag{9}$$

Now, if $\varphi \colon G(\mathfrak{o}(S)) \to E$ is a section of π over $G(\mathfrak{o}(S))$, then

$$\delta([\rho^{-1}(G(\mathfrak{o}(S))), \rho^{-1}(G(\mathfrak{o}(S)))]) = [\pi^{-1}(G(\mathfrak{o}(S))), \pi^{-1}(G(\mathfrak{o}(S)))]$$

is contained in $\varphi(G(\mathfrak{o}(S)))$; using this observation together with the commutativity of (9), we find that $\Gamma' = \Gamma \cap [\rho^{-1}(G(\mathfrak{o}(S))), \rho^{-1}(G(\mathfrak{o}(S)))]$ is contained in $\operatorname{Ker}\theta$. This means that under the natural identification of $H^2(G_\infty)$ with $\operatorname{Hom}(\Gamma, I)$, $\operatorname{Ker}(H^2(G_\infty) \to H^2(G(\mathfrak{o}(S))))$ imbeds into the finite group $\operatorname{Hom}(\Gamma/\Gamma', I)$, hence it is finite. The lemma is proved.

Let S be a finite set of places of K, containing the subset S_0 given by Lemma 2.5, such that the groups $H^i(\prod_{v \notin S} G(\mathfrak{o}_v))$, $i = 1, 2$, are trivial (1.8). The factorization $G(A) = G(A_f) \times G_\infty$, where A_f is the ring of finite adeles, gives rise to the factorization $H^2(G(A)) = H^2(G(A_f)) \times H^2(G_\infty)$; let $\varrho \colon H^2(G(A)) \to H^2(G_\infty)$ be the corresponding projection. Obviously, the kernel of the restriction $\varrho \mid M(\emptyset, G)$ coincides with $M(V_\infty^K, G)$, hence it is finite. So, we need to show that $R = \varrho(M(\emptyset, G))$ is also finite. Since $H^2(G_\infty) = \operatorname{Hom}(\pi_1(G_\infty), I)$, and the fundamental group $\pi_1(G_\infty)$ is finitely generated, it is enough to show that R has a finite exponent d. We will show that one can take $d = d_1 d_2$, where d_1 (resp., d_2) is the order of $\operatorname{Ker}(H^2(G_\infty) \to H^2(G(\mathfrak{o}(S))))$ (resp., of $H^2(G(S - V_\infty^K)))$; notice that the finiteness of d_1 follows from the previous lemma, and the finiteness of d_2 was discussed above.

By our construction, for $W = G(S) \times \prod_{v \notin S} G(\mathfrak{o}_v)$, we have:

$$H^2(W) = H^2(G(S)) = H^2(G_\infty) \times H^2(G(S - V_\infty^K)), \tag{10}$$

and ϱ is the composite of the following restriction maps:

$$H^2(G(A)) \xrightarrow{\varrho_1} H^2(W) \xrightarrow{\varrho_2} H^2(G_\infty).$$

If $x \in M(\emptyset, G)$, then obviously $\varrho_1(x) \in \mathrm{Ker}(H^2(W) \to H^2(G(\mathfrak{o}(S))))$, and in view of (10) we obtain that $\varrho(x)^{d_2} \in \mathrm{Ker}(H^2(G_\infty) \to H^2(G(\mathfrak{o}(S))))$. So,

$$\varrho(x)^d = (\varrho(x)^{d_2})^{d_1}$$

is trivial, and the theorem is proved.

3 Groups of type A_1

The goal of this section is to prove

Theorem 3.1 *Let G be an absolutely simple, simply connected K-group of type A_1. Let S be a finite set of places of K which contains a noncomplex place v_0 such that G is K_{v_0}-split. Then the metaplectic kernel*

$$M(S,G) = \mathrm{Ker}(H^2(G(A(S))) \to H^2(G(K)))$$

is trivial.

As is well known, $G = \mathbf{SL}_{1,D}$ for a quaternion central algebra D over K. In the proof of Theorem 3.1 we will use the fact that

$$[G(K), G(K)] = G(K) \cap [G(T), G(T)], \tag{1}$$

where T is the set of all nonarchimedean places v such that G is K_v-anisotropic, or, equivalently, $D_v = D \otimes_K K_v$ is a division algebra. Note that for G of type A_1, $G(K)$ has the standard description of normal subgroups and (1) is a consequence of this description. (1) holds more generally for any group of the form $G = \mathbf{SL}_{1,D}$, where D is a central simple K-algebra of arbitrary degree (cf. [PR2], §9.2).

We begin our proof of Theorem 3.1 by proving first the triviality of $M_V(G)$.

Proposition 3.2 *For a simply connected K-group G of type A_1 and a finite set V of places of K, the restriction map*

$$H^2(G(V)) \to H^2(G(K))$$

is injective.

PROOF. Without any loss of generality, we may (and will) assume that $V \supset T \cup V_\infty^K$. We will prove that a topological central extension

$$1 \to I \to E \xrightarrow{\pi} G(V) \to 1,$$

which admits a splitting $\delta : G(K) \to E$, is trivial, i.e. there exists a continuous group-theoretic section $\rho : G(V) \to E$. To this end, in view of the weak approximation property, it suffices to show that δ is continuous with respect to the topology on $G(K)$ induced from that on $G(V)$. Moreover, since δ is a group homomorphism, we only need to prove that for some open subset $U_0 \subset G(V)$, the restriction of δ to $G(K) \cap U_0$ is continuous.

According to Lemma 1.7, there exists an open neighborhood Ω of the identity in $G(V)$ and a continuous section $\theta : \Omega \to E$ which is a "local homomorphism", i.e. satisfies $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in \Omega$ such that $xy \in \Omega$. We pick a neighborhood of the identity $U \subset \Omega$, which is a pro-p group in case K is of characteristic $p > 0$, contained in $[G(T), G(T)] \times G(V-T)$ and which has the following properties: $U^{-1} = U$, $UUUU \subset \Omega$, and for any $t \in \prod_{v \in V}\{\pm 1\}$, $t \neq 1$, $U \cap tU = \emptyset$. Let $H = \mathbf{GL}_{1,D}$. In case K is of characteristic zero, we let $W = (\prod_{v \in V} K_v^*) \cdot U$; W is an open neighborhood of the identity in $H(V)$. In case K is of positive characteristic, let W be a compact-open subgroup of $H(V)$ which normalizes U and is such that for every $a \in W$, the automorphism $\epsilon_a = \mathrm{Int}\, a$ of $G(V)$ lifts to an automorphism $\tilde{\epsilon}_a$ of E acting trivially on I; see Proposition 1.12 (i).

Consider the variety

$$Z = \{(y, z) \in (G - \{\pm 1\}) \times G \mid \mathrm{Trd}_{D/K}(zy) = \mathrm{Trd}_{D/K}(y)\},$$

and the two morphisms

$$\phi : H \times (G - \{\pm 1\}) \to Z, \quad \phi(x, y) = (y\,,\,[x, y]),$$

and

$$\psi : Z \to G, \quad \psi(y, z) = z.$$

It is easy to check both that ϕ is submersive at every point of $H \times (G - \{\pm 1\})$, and that ψ is submersive outside the closed subvariety $\{(y, \pm y^{-2}) \mid y \in G\} \cap Z$ of Z of codimension two. It follows from the Implicit Function Theorem ([S3]) that there exist nonempty open subsets $B_1 \times B_2 \subset G(V) \times G(V)$ and $U_0 \subset U$ such that

(i) $\phi(W \times U) \supset (B_1 \times B_2) \cap Z(V)$;

(ii) $\psi((B_1 \times B_2) \cap Z(V)) \supset U_0$, and no element of U_0 has reduced trace ± 2; in particular, U_0 does not contain ± 1.

Let $\kappa = \psi \circ \phi : (x, y) \mapsto [x, y]$ be the commutator map.

Lemma 3.3 $G(K) \cap U_0 \subset \kappa((W \cap H(K)) \times (U \cap G(K)))$.

Proof. Fix $z \in G(K) \cap U_0$ and consider $Y = \psi^{-1}(z)$ identified with a subvariety of G in terms of its projection on the first component. Y is defined by the equations

$$\begin{cases} \mathrm{Trd}_{D/K}(zy) & = & \mathrm{Trd}_{D/K}(y) \\ \mathrm{Nrd}_{D/K}(y) & = & 1. \end{cases}$$

Since $\mathrm{Trd}_{D/K}((z-1)y)$ (resp., $\mathrm{Nrd}_{D/K}(y)$) is a linear (resp., quadratic) form in the coordinates of y, Y is isomorphic to a quadric in the three-dimensional affine space. Therefore, $Y(K) \neq \emptyset$ if, and only if, $Y(K_v) \neq \emptyset$ for all $v \in V^K$ (Hasse-Minkowski Theorem), and if $Y(K) \neq \emptyset$, then Y is a rational variety and hence it has the weak approximation property with respect to any finite subset of V^K.

Clearly, $z \in B_2$ and there exists some $y_0 \in B_1$ such that $(y_0, z) \in Z(V)$, implying that $Y(K_v) \neq \emptyset$ at least for $v \in V$. However, since $V \supset T$, for $v \notin V$, we have $G(K_v) \simeq \mathbf{SL}_2(K_v)$, implying that z is a commutator in $G(K_v)$ ([Th]), and again $Y(K_v) \neq \emptyset$. Hence, $Y(K) \neq \emptyset$, and Y has the weak approximation property with respect to V. So, there is an element $y_1 \in Y(K) \cap B_1 \subset Y(K) \cap U$. Obviously, the elements zy_1 and y_1 have the same characteristic polynomial, and therefore they are conjugate in $H(K) = D^\star$ (the Skölem-Noether Theorem). In other words, if $X = \{x \in H \mid xy_1x^{-1} = zy_1\}$, $X(K) \neq \emptyset$. But X is a principal homogeneous space of the centralizer $C_H(y_1)$ (which is a Zariski open subset in an affine space), so X has the weak approximation property with respect to V. It follows from condition (i) above that $X(V) \cap W \neq \emptyset$, hence there exists an $x_1 \in X(K) \cap W$. Then $z = [x_1, y_1] \in \kappa((W \cap H(K)) \times (U \cap G(K)))$, as required. The lemma is proved.

To complete the proof of Proposition 3.2, we will show that on $G(K) \cap U_0$, δ coincides with θ, and therefore it is continuous. So, pick a $z \in G(K) \cap U_0$, and using Lemma 3.3, write it in the form $z = [x, y]$, where $x \in H(K) \cap W$, $y \in G(K) \cap U$. If K is of characteristic zero, then by our choice of W, x can be uniquely written in the form $x = \alpha \cdot c$, $\alpha \in \prod_{v \in V} K_v^*$, $a \in U$, and then we let $\tilde{\epsilon}_x$ denote the inner automorphism $\mathrm{Int}\,\tilde{c}$ of E, where $\tilde{c} \in \pi^{-1}(c)$. Obviously, $\tilde{\epsilon}_x$ is a lift of ϵ_x, $\epsilon_x(U) \subset \Omega$ and

$$\theta(\epsilon_x(t)) = \tilde{\epsilon}_x(\theta(t)) \quad \text{for any} \quad t \in U. \tag{2}$$

We claim that (2) also holds if K is of characteristic $p > 0$, where $\tilde{\epsilon}_x$ is the lift of $\epsilon_x = \mathrm{Int}\, x$, which exists by our choice of W. Observe first, that $H^2(G(V))$ is a finite group of order prime to p. Indeed, if D splits over v, then $G(K_v) \simeq \mathbf{SL}_2(K_v)$, and it follows from Theorem 1.1 that the order of $H^2(G(K_v))$ is prime to p, and $H^1(G(K_v))$ obviously vanishes. On the other hand, if $D_v = D \otimes_K K_v$ is a division algebra, then $G(K_v) \simeq \mathbf{SL}_1(D_v)$, the commutator subgroup of $G(K_v)$ is of index prime to p, and hence $H^1(G(K_v))$ is of order prime to p, moreover, the cohomology group $H^2(G(K_v))$ vanishes; see [PrRa4]. These facts, in conjunction with the Künneth formula, imply the above assertion about $H^2(G(V))$. Now it follows that the homomorphism $\varphi\colon U \to I$,

$$\varphi(t) = \tilde{\epsilon}_x^{-1}(\theta(\epsilon_x(t))) \cdot \theta(t)^{-1}$$

takes values in the prime-to-p component of I. Since U is a pro-p group, this implies that φ is trivial, and we obtain (2).

It follows from (2) that

$$\theta(z) = \theta([x, y]) = \tilde{\epsilon}_x(\theta(y))\theta(y)^{-1}. \tag{3}$$

Since $U \subset [G(T), G(T)] \times G(V-T)$, from 1.10 (ii) we conclude that

$$\delta(\epsilon_x(y)) = \tilde{\epsilon}_x(\delta(y)),$$

and therefore,

$$\delta(z) = \delta(\epsilon_x(y)y^{-1}) = \delta(\epsilon_x(y))\delta(y)^{-1} = \tilde{\epsilon}_x(\delta(y))\delta(y)^{-1}. \tag{4}$$

Since $\theta(y)\delta(y)^{-1} \in I$, and $\tilde{\epsilon}_x$ acts trivially on I, comparing (3) and (4), we get $\theta(z) = \delta(z)$, as claimed. Proposition 3.2 is proved.

REMARKS. 1. In the proof of Lemma 3.3, we have employed some ideas first used in [PR1] to prove that if $T = \emptyset$, then $G(K) = [G(K), G(K)]$.

2. In the case where $V \subset V_f^K$, one can give another proof of Proposition 3.2 using Sury's generalization [Su] of Margulis' theorem [M2] describing normal subgroups of $G(K)$: as before, we may assume that $V \supset T$. Consider an abstract group-theoretic section $\delta: G(K) \to E$ and a continuous section $\theta: \Omega \to E$ of π, over $G(K)$ and some open subgroup Ω of $G(V)$, respectively. Then, as is easily seen, δ and θ coincide on $N = [G(K) \cap \Omega,\ G(K) \cap \Omega]$. On the other hand, it follows from [Su] that N is open in $G(K)$ in the topology induced from $G(V)$, and the continuity of δ follows. However, our argument is more direct and allows us to include also archimedean places. Besides, as we will show in §8, once we have an independent proof of Proposition 3.2, the result of [Su] can be derived directly from [M2].

To prove the triviality of the metaplectic kernel, it suffices to establish the following:

Theorem 3.4 *Suppose S contains a noncomplex place v_0 such that $D \otimes_K K_{v_0} \simeq M_2(K_{v_0})$, and let q be a prime. Assume that $q = 2$ if v_0 is real. Then $M(S, G)$ does not contain elements of order q.*

Assuming Theorem 3.4 for a moment, we shall show how it implies Theorem 3.1. Since $M(S, G)$ is finite (Theorem 2.4), its triviality is equivalent to the fact that it does not contain any element of order q, for any prime q. Since there is no restriction on q in Theorem 3.4, if v_0 is nonarchimedean, we obtain the triviality of $M(S, G)$ in this case. However, once we know this, from 1.13 we conclude that for arbitrary S, $M(S, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$. It follows that the mere existence of a real place $v_0 \in V^K$ implies that $M(S, G)$ is of order ≤ 2. If, moreover, v_0 is as in Theorem 3.1, we can use Theorem 3.4, with $q = 2$, to conclude that, in fact, $M(S, G)$ is trivial.

In proving Theorem 3.4, we may obviously assume without loss of generality that $S \cap T = \emptyset$. Now, to begin the argument, we fix an $x \in M(S, G)$ of order q and consider the corresponding extension:

$$1 \to I \longrightarrow E \xrightarrow{\pi} G(A(S)) \to 1. \tag{5}$$

There exists a finite subset $S' \subset V^K$ which contains $S \cup T \cup V_\infty^K$ and also has the following property (cf. [PrRa1: 2.2-2.3]):

For $v \notin S'$, $H^1(\mathcal{C}_0)$ vanishes and the restriction map $H^2(G(K_v)) \to H^2(\mathcal{C}_0)$ is trivial, for some (and consequently, for any) maximal compact subgroup $\mathcal{C}_0$ of $G(K_v)$.

Then

$$H^2(G(A(S))) = H^2(G(S'-S)) \times \prod_{v \notin S'} H^2(G(K_v)),$$

so we can write x in the form $x = (x_{S'-S}, (x_v)_{v \notin S'})$. To prove that $x = 0$, it suffices to make sure that $x_v = 0$ for every $v \notin S'$. (Indeed, assuming this, we would have $x_{S'-S} \in \mathrm{Ker}(H^2(G(S'-S)) \to H^2(G(K)))$, however the latter kernel is trivial by Proposition 3.2.) Let $\chi_v \in \hat{\mu}(K_v)$ be the character corresponding to x_v (see Theorem 1.1). *We need to show that χ_v is trivial for all $v \notin S'$.* Fix a $v_1 \notin S'$. Since by our construction, $D \otimes_K K_v = M_2(K_v)$ for $v = v_0, v_1$, there exists a maximal subfield $L \subset D$ such that the local degree $[L_{\bar{v}} \colon K_v]$ is one for $\bar{v}$ lying above $v = v_i$, $i = 0, 1$ (cf. A.6). Let $B = R_{L/K}(\mathbf{GL}_1)$ be the corresponding maximal K-torus of $H = \mathbf{GL}_{1,D}$, and $B_0 = B \cap G$ be the associated maximal K-torus of G.

Let S_0 be the union of S' and the set of nonarchimedean places ramified in the extension L/K (note that, by our construction, $v_1 \notin S_0$). There is a neighborhood Ω of the identity in $G(S_0 - S)$ such that the extension

$$1 \to I \longrightarrow \pi^{-1}(G(S_0 - S)) \xrightarrow{\pi} G(S_0 - S) \to 1$$

admits a continuous local section over Ω, see 1.7. Next, pick a neighborhood U of the identity contained in $[G(T), G(T)] \times G(S_0 - (S \cup T))$ which has the following properties: $UU \subset \Omega$ and $U \cap tU = \emptyset$, for any $t \in \prod_{v \in S_0 - S}\{\pm 1\}$, $t \neq 1$. A consequence of these properties is that for any elements $a, b \in B_0(S_0 - S) \cap U$, their lifts $\tilde{a}$, $\tilde{b}$ commute in $\pi^{-1}(G(S_0 - S))$. It is convenient to reformulate this fact in a slightly different way. If K is of characteristic zero, let $W = (\prod_{v \in S_0 - S} K_v^*) \cdot U$; W is obviously a neighborhood of the identity in $H(S_0 - S)$. Any $a \in W$ can be written as a product $a = \alpha \cdot c$, where $\alpha \in \prod_{v \in S_0 - S} K_v^*$, $c \in U$ in a unique way, and then the automorphism $\epsilon_a = \mathrm{Int}\, a$ lifts to the automorphism $\tilde{\epsilon}_a = \mathrm{Int}\, \tilde{c}$, for any $\tilde{c} \in \pi^{-1}(c)$. We conclude from the above that for all $a \in B(S_0 - S) \cap W$, and $b \in B_0(S_0 - S) \cap U$, we have

$$\tilde{\epsilon}_a(\tilde{b})\tilde{b}^{-1} = 1 \quad \text{for any} \quad \tilde{b} \in \pi^{-1}(b). \tag{6}$$

Now suppose the characteristic of K is $p > 0$. We assume, as we may, that U chosen above is a pro-p group. Let W be as in Proposition 1.12(i) for $V = S_0 - S$. Then for every $a \in W$, the automorphism $\epsilon_a = \mathrm{Int}\, a$ of $G(S_0 - S)$ admits a lift $\tilde{\epsilon}_a$. We claim that for any $a \in W$ and $b \in U$, (6) still holds. To prove the claim we argue as follows. As we have already seen in the proof of Proposition 3.2, $H^2(G(S_0 - S))$ is a finite group of order prime p. It follows that for a fixed $a \in B(S_0 - S) \cap W$, the map $b \mapsto \tilde{\epsilon}_a(\tilde{b})\tilde{b}^{-1}$ defines a homomorphism of $B(S_0 - S) \cap U$ into I, which takes values in the prime-to-p component of I. As U, and hence $B_0(S_0 - S) \cap U$, is a pro-p group, this implies that $\tilde{\epsilon}_a(\tilde{b})\tilde{b}^{-1} = 1$. Thus (6) holds both in characteristic zero and in positive characteristic.

Now, let us turn to an analysis of the extension (5) over the group $G(A(S_0))$:

$$1 \to I \longrightarrow \pi^{-1}(G(A(S_0))) \xrightarrow{\pi} G(A(S_0)) \to 1.$$

According to Proposition 1.12(ii), the automorphism $\epsilon_a = \mathrm{Int}\ a$, for a in $H(A(S_0))$, admits a unique lift. Hence it follows from Proposition 1.10(iv) that the automorphism $\epsilon_a = \mathrm{Int}\ a$ for $a \in W \times H(A(S_0))$ admits a lift $\tilde{\epsilon}_a$ to E. For $a = (a_v) \in (B(S_0 - S) \cap W) \times B(A(S_0))$ and $b = (b_v) \in (B_0(S_0 - S) \cap U) \times B_0(A(S_0))$, in view of equation (4) of §1, we have

$$\tilde{\epsilon}_a(\tilde{b})\tilde{b}^{-1} = \prod_{v \notin S_0} \tilde{\epsilon}_{a_v}(\tilde{b}_v)(\tilde{b}_v)^{-1}, \tag{7}$$

so, for the computation of $\tilde{\epsilon}_a(\tilde{b})\tilde{b}^{-1}$, it is sufficient to compute the local expressions $\tilde{\epsilon}_{a_v}(\tilde{b}_v)(\tilde{b}_v)^{-1}$, for $v \notin S_0$. There are two different cases to consider where the local degree $[L_{\bar{v}}\colon K_v]$, $\bar{v} \mid v$, is either 2 or 1.

First, let $[L_{\bar{v}}\colon K_v] = 2$. We claim that in this case

$$\tilde{\epsilon}_{a_v}(\tilde{b}_v)(\tilde{b}_v)^{-1} = 1 \tag{8}$$

for any $a_v \in B(K_v), b_v \in B_0(K_v)$. To show this, we let $P = \{b \in B(K_v) \mid \det b \in \mathfrak{o}_v^*\}$. Since $v \notin S_0$, the extension L/K is unramified at v, and consequently, identifying the elements of K_v^* with the corresponding scalar matrices in $\mathbf{GL}_2(K_v)$, we have the following:

$$B(K_v) = K_v^* \cdot P. \tag{9}$$

Obviously, P is compact, and therefore it is contained in a maximal compact subgroup $\mathcal{C}$ of $\mathbf{GL}_2(K_v)$. Then $\mathcal{C}_0 = \mathcal{C} \cap \mathbf{SL}_2(K_v)$ is a maximal compact subgroup of $\mathbf{SL}_2(K_v)$, and by our choice of S_0, $H^1(\mathcal{C}_0)$ vanishes and the restriction map $H^2(\mathbf{SL}_2(K_v)) \to H^2(\mathcal{C}_0)$ is trivial. It follows from (9) that $\mathcal{C}_0$ is invariant under $\epsilon_{a_v} = \mathrm{Int}\, a_v$, and hence there exists a section $\phi\colon \mathcal{C}_0 \to E_v := \pi^{-1}(G(K_v))$, and $\phi(\epsilon_{a_v}(g)) = \tilde{\epsilon}_{a_v}(\phi(g))$ for every $g \in \mathcal{C}_0$; this immediately implies (8).

Consider now the second possibility where $[L_{\bar{v}}\colon K_v] = 1$. In this case, B is diagonalizable over K_v. Fix an element $g \in \mathbf{SL}_2(K_v)$ such that gBg^{-1} is diagonal. Pick some $a_v \in B(K_v)$, $b_v \in B_0(K_v)$, let $ga_vg^{-1} = a'_v$, $gb_vg^{-1} = b'_v$, and

$$a'_v = \mathrm{diag}(a_1, a_2), \quad b'_v = \mathrm{diag}(b, b^{-1}).$$

Then

$$\tilde{\epsilon}_{a_v}(\tilde{b}_v)(\tilde{b}_v)^{-1} = \tilde{\epsilon}_{a'_v}(\tilde{b}'_v)(\tilde{b}'_v)^{-1}. \tag{10}$$

This "commutator" can be computed using either Steinberg's relations in the universal topological central extension of $\mathbf{SL}_2(K_v)$, or else by means of an explicit expression for a 2-cocycle which defines an extension of $\mathbf{GL}_2(K_v)$ inducing the given extension of $\mathbf{SL}_2(K_v)$. Generalizing the formula exhibited earlier by Kubota in 1967 for a 2-cocycle on $\mathbf{SL}_2(K_v)$, Kazhdan and Patterson ([KPa], p. 41) obtained the following expression for a 2-cocycle on $\mathbf{GL}_2(K_v)$:

$$\xi_v(g_1, g_2) = \chi_v[(\frac{\alpha(g_1g_2)}{\alpha(g_1)}, \frac{\alpha(g_1g_2)}{\alpha(g_2)})_v \cdot (\det(g_1), \frac{\alpha(g_1g_2)}{\alpha(g_1)})_v]; \tag{11}$$

where, by definition,

$$\alpha\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} c & \text{if } c \neq 0, \\ d & \text{if } c = 0. \end{cases}$$

Note that the cocycle ξ_v is not continuous since it corresponds to the Steinberg section to be denoted as κ_v, which is not continuous. It can be used to calculate the expression in (10). Indeed, by definition, for any $g_1, g_2 \in \mathbf{GL}_2(K_v)$, we have

$$\kappa_v(g_1g_2) = \kappa_v(g_1)\kappa_v(g_2)\xi_v(g_1, g_2),$$

implying that

$$[\tilde{g}_1, \tilde{g}_2] = \kappa_v(g_1g_2)\kappa_v(g_2g_1)^{-1} \cdot \xi_v(g_1, g_2)^{-1}\xi_v(g_2, g_1).$$

Now, observing that the right-hand side of (10) coincides with $[\tilde{a}'_v, \tilde{b}'_v]$, and that a'_v and b'_v commute in $\mathbf{GL}_2(K_v)$, we conclude that it is equal to

$$\xi_v(a'_v, b'_v)^{-1}\xi_v(b'_v, a'_v) = \chi_v((\frac{a_1}{a_2}, b)_v). \tag{12}$$

Now we fix elements $a \in B(K), b \in B_0(K)$ and compute the expression in (10) for their replicas a_v, b_v in $B(K_v)$. By Hilbert's Theorem 90, b can be written in the form $b = \sigma s/s$ for some $s \in L^\star = B(K)$. Also, let w be the extension of v to L which corresponds to the imbedding $L \hookrightarrow K_v$. Then it follows from the above that

$$\tilde{\epsilon}_{a_v}(\tilde{b}_v)(\tilde{b}_v)^{-1} = \chi_v((\frac{a}{\sigma a}, \frac{\sigma s}{s})_w) = \chi_v((\frac{\sigma a}{a}, s)_w) \cdot \chi_v((\sigma(\frac{\sigma a}{a}), \sigma(s))_w),$$

where $(\star, \star)_w$ is the norm residue symbol on L_w of power $\#\mu(L_w) = \#\mu(K_v)$. Since $w_1 = w$ and $w_2 = w \circ \sigma$ are the two distinct extensions of v to L, we conclude, using the properties of the norm residue symbol, that there exist characters $\chi_{\bar{v}} \in \hat{\mu}(K_v)$, one for each extension $\bar{v} \mid v$ to L, *of order equal to the order of* χ_v, such that

$$\epsilon_{a_v}(\tilde{b_v})(\tilde{b_v})^{-1} = \prod_{\bar{v}|v} \chi_{\bar{v}}((\frac{\sigma a}{a}, s)_{\bar{v}}). \tag{13}$$

Now, if $\kappa: G(K) \to E$ is a splitting of (5) over $G(K)$, then for all $a \in H(K) \cap W$ and $b \in [G(K), G(K)]$, $\kappa(\epsilon_a(b)) = \tilde{\epsilon}_a(\kappa(b))$ (Proposition 1.10(ii)). Since by our choice of U, $B_0(K) \cap U \subset [G(K), G(K)]$, for any $a \in B(K) \cap W$, $b \in B_0(K) \cap U$, we obtain the equality: $\tilde{\epsilon}_a(\tilde{b})\tilde{b}^{-1} = 1$. In view of (7), (8) and (13), this yields the relation:

$$\prod_{v \in V_0} \prod_{\bar{v}|v} \chi_{\bar{v}}((\frac{\sigma a}{a}, s)_{\bar{v}}) = 1 \tag{14}$$

for any $a \in L^{\star} \cap W$ and any $s \in L^{\star}$ such that $\sigma s/s \in U$; where $V_0 = \{v \notin S_0 \mid [L_{\bar{v}}\colon K_v] = 1\}$. Letting $\chi_{\bar{v}} = 1$ for $\bar{v} \mid v$ if $v \notin V_0$, we can rewrite (14) as the following reciprocity law:

$$\prod_{\bar{v} \in V^L} \chi_{\bar{v}}((\frac{\sigma a}{a}, s)_{\bar{v}}) = 1.$$

Fix some extensions $w_0 \mid v_0$ and $w_1 \mid v_1$. By our construction, $\chi_{w_0} = 1$. We shall now prove that χ_{w_1} is trivial. Since $\chi_{\bar{v}}^q = 1$ for every $\bar{v} \in V^L$, and additionally $q = 2$ if v_0 is real, the triviality of χ_{w_1} will immediately follow from the proposition in Appendix B if we can find an $a \in L^*$ such that

$$\begin{array}{ll} w_1(\sigma a/a) = 1, & \text{and} \\ w_0(\sigma a/a) = 1, & \text{if } v_0 \text{ is nonarchimedean,} \\ \sigma a/a < 0 \text{ in } L_{w_0}, & \text{if } v_0 \text{ is real,} \end{array}$$

and moreover, $a \in W$. However, the existence of such an a easily follows from the weak approximation property for L, since the places

$$w_0, \quad w_0 \circ \sigma, \quad w_1 \quad \text{and} \quad w_1 \circ \sigma$$

are pairwise distinct and do not lie over any place in $S_0 - S$.

As the order of χ_{v_1} equals that of χ_{w_1}, we conclude that χ_{v_1} is trivial, this is what was needed to establish Theorem 3.1.

4 Groups of type ${}^1A_r$

In this section we shall prove the following theorem for groups of inner type A_r.

Theorem 4.1 *Let G/K be an absolutely simple, simply connected group of inner type A. Let S be a finite set of places of K containing a place v_0 which is either nonarchimedean and G is K_{v_0}-isotropic, or is real and $G(K_{v_0})$ is not (topologically) simply connected. Then $M(S,G)$ is trivial. Moreover, $M(\emptyset, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$ of index at most 2, and in the following cases it is actually isomorphic to $\hat{\mu}(K)$: (i) $r = 1$, (ii) r is even, (iii) K contains $\sqrt{-1}$, a primitive 4-th root of unity.*

Any group G of the type under consideration is of the form $G = \mathbf{SL}_{m,D}$, where D is a central division algebra over K. However, in our argument it is more convenient to think of G as the group $\mathbf{SL}_{1,\mathcal{A}}$, where $\mathcal{A} = M_m(D)$. Let d be the degree of $\mathcal{A}$ (i.e. the square root of $\dim_K \mathcal{A}$). Then the assumptions about v_0 in the statement of the theorem mean that $\mathcal{A}_{v_0} = \mathcal{A} \otimes_K K_{v_0}$ is not a division algebra if v_0 is nonarchimedean, and is the full matrix algebra $M_d(K_{v_0})$ if v_0 is real.

We begin by proving the triviality of $M_V(G)$.

Proposition 4.2 *For an absolutely simple, simply connected K-group G of inner type A over K and a finite set V of places of K, the restriction map*

$$\rho_V : H^2(G(V)) \longrightarrow H^2(G(K))$$

is injective.

In the sections to follow, we will prove this assertion for groups of all types other than ${}^2A_r$. The idea of the proof in most cases is to find a subgroup $H \subset G$ for which, on the one hand, the restriction map $H^2(G(V)) \to H^2(H(V))$ is injective, and on the other hand, the injectivity of the restriction map $H^2(H(V)) \to H^2(H(K))$ has already been established. As a rule, for such an H, one can take either a suitable subgroup of type A_1, or a certain maximal torus.

Proposition 4.3 *Let G be an arbitrary absolutely simple, simply connected K-group of type other than D; $V_1, V_2 \subset V_f^K$ two finite disjoint subsets, and U an open subgroup of $G(V_2)$. Assume that for each $v \in V_1$, there exists a maximal K_v-torus $C_v \subset G$, which splits over a cyclic Galois extension L_v of K_v, such that the restriction map*

$$\zeta : H^2(G(V_1)) \longrightarrow H^2(\prod_{v \in V_1} C_v(K_v))$$

is injective. Then the restriction map

$$H^2(G(V_1)) \longrightarrow H^2(G(K) \cap U)$$

is also injective. Moreover, if the restriction map $\zeta_v : H^2(G(K_v)) \to H^2(C_v(K_v))$ is injective for every $v \in V_1$ and $V_1 \cap T = \emptyset$, where as before, T is the set of nonarchimedean places of K where G is anisotropic, then ζ is also injective. In particular, taking $V_2 = \emptyset$, the restriction map

$$H^2(G(V_1)) \to H^2(G(K))$$

is injective.

(Recall that, in fact, $T = \emptyset$ if G is not of type A.)

Proof. Since G is not of type D, for each $v \in V_2$, one can pick a maximal K_v-torus $C_v \subset G$ which splits over a cyclic Galois extension L_v of K_v. This assertion is obvious if G is K_v-isomorphic to a group of the form $\mathbf{SL}_{1,\Delta_v}$, Δ_v a central division algebra over K_v, since then one can let $C_v = R^{(1)}_{L_v/K_v}(\mathbf{GL}_1)$ where L_v is a maximal unramified subfield of Δ_v. The case of an arbitrary inner form G/K_v immediately reduces to the case just considered. That is, if $C_0 \subset G$ is a maximal K_v-split torus and $Z = Z_G(C_0)$ is its centralizer, then $H = [Z, Z]$ is a product over K_v of absolutely simple, K_v-anisotropic groups, and each of these factors is K_v-isomorphic to a group of the form $\mathbf{SL}_{1,\Delta_v}$. This implies that there exists a maximal K_v-torus $C_1 \subset H$ which splits over a certain unramified, hence cyclic, extension of K_v. Then $C_v = C_0C_1$ is a maximal K_v

torus of G with the required properties. It remains to consider the cases where G/K_v is either of type ${}^2A_r$ or ${}^2E_6$. In the first case, G is K_v-isomorphic to the special unitary group $\mathbf{SU}(f)$ of a nondegenerate hermitian form f in $n \geq 2$ variables over a quadratic extension L_v/K_v. Fix an orthogonal basis of L_v^n and consider the matrix realization of G in terms of this basis. Then

$$C_v = \{\mathrm{diag}(z_1, \ldots, z_n) \mid z_i \in R^{(1)}_{L_v/K_v}(\mathbf{GL}_1), z_1 \cdots z_n = 1\}$$

is a maximal K_v-torus of G which splits over the quadratic extension L_v/K_v. Finally, if G is of type ${}^2E_6$, then G is known to be quasi-split over K_v (cf. [PR2], Proposition 6.15); let C_v be a maximal K_v-torus of G contained in a Borel subgroup defined over K_v. Then C_v splits over the quadratic extension of K_v over which G becomes an inner form.

Now, using [PR2: Cor. 3 in §7.1], we can find a maximal K-torus $C \subset G$ such that C is conjugate to C_v by an element of $G(K_v)$, for every $v \in V_1 \cup V_2$. We will show that the restriction map $H^2(G(V_1)) \xrightarrow{\omega} H^2(C(K) \cap U)$ is injective. Obviously, ω can be written as the composite of the following two maps:

$$H^2(G(V_1)) \xrightarrow{\xi} H^2(C(V_1)) \xrightarrow{\nu} H^2(C(K) \cap U).$$

The injectivity of ζ immediately implies that of ξ. On the other hand, C has the weak approximation property with respect to $V_1 \cup V_2$ ([PR2: Proposition 7.8]). In particular, $C(K) \cap U$ is dense in $C(V_1)$, so the injectivity of ν is an easy consequence of the following lemma.

Lemma 4.4 *Let C be a K-torus, $V \subset V_f^K$ be a finite subset. If Δ is a dense subgroup of $C(V)$, then the restriction map*

$$H^2(C(V)) \xrightarrow{\theta} H^2(\Delta)$$

is injective.

Proof. Let $x \in \mathrm{Ker}\,\theta$, and let

$$1 \to I \longrightarrow E \xrightarrow{\pi} C(V) \to 1$$

be the corresponding extension. Since the commutator map

$$\varphi: C(V) \times C(V) \to I, \quad (a, b) \mapsto [\tilde{a}, \tilde{b}] \text{ for any } \tilde{a} \in \pi^{-1}(a), \tilde{b} \in \pi^{-1}(b)$$

is (well-defined and) continuous, and is trivial on the dense subgroup $\Delta \times \Delta$, it is trivial identically, i.e. E is commutative. Furthermore, there exists a continuous section $\sigma: W \to E$ of π over a compact-open subgroup W, and an abstract section $\tau: \Delta \to E$ over Δ. Let $\Gamma = W \cap \Delta$. Then ψ defined by $\psi(\gamma) = \sigma(\gamma)\tau(\gamma)^{-1}$ for $\gamma \in \Gamma$, is a homomorphism of Γ to I. As I is injective, ψ can be extended to a homomorphism $\bar{\psi}: \Delta \to I$; define $\bar{\tau}: \Delta \to E$ by the formula: $\bar{\tau}(a) = \tau(a)\bar{\psi}(a)$. Then

$$\bar{\tau} \mid \Gamma = \sigma \mid \Gamma. \tag{1}$$

Since Δ is dense in $C(V)$, we have $C(V) = \Delta W$. Now, we define $\alpha: C(V) \to E$ as follows:

$$\text{for } a = bc \ (b \in \Delta, c \in W) \quad \text{let } \alpha(a) = \bar{\tau}(b)\sigma(c).$$

By virtue of (1), α is well-defined. Since E is commutative, α is a group homomorphism. Finally, α coincides on W with σ, and therefore it is a continuous section for π. Lemma 4.4 is proved.

To prove the last assertion of 4.3, it remains to observe that if $V_1 \cap T = \emptyset$, then $H^1(G(K_v))$ is trivial for every $v \in V_1$, and therefore by the Künneth formula, $H^2(G(V_1)) = \prod_{v \in V_1} H^2(G(K_v))$. So, the injectivity of ζ_v for each $v \in V_1$ obviously implies that of ζ. Proposition 4.3 is thus proved.

For the proof of Proposition 4.2 we need the following proposition, which is proved using Proposition 4.3.

Proposition 4.5 *Assume that G is not of type A_1, and let V_1, V_2, T and U be as in Proposition 4.3. If $V_1 \subset T$, then the restriction map $H^2(G(V_1)) \to H^2(G(K) \cap U)$ is injective.*

PROOF. It follows from Theorem 6.5 in [PR2], that for $v \in T$, the group G is K_v-isomorphic to a group of the form $\mathbf{SL}_{1,D_v}$, where D_v is a central division algebra over K_v. Let $L_v \subset D_v$ be a maximal unramified subfield, and $C_v \simeq R^{(1)}_{L_v/K_v}(\mathbf{GL}_1)$ be the corresponding maximal K_v-torus in G. Then, as shown in [PR2], proof of Theorem 9.12, the result of [PrRa4] on the injectivity of the map $H^2(G(K_v)) \to H^2(C_v(K_v))$ in case D_v is not a quaternion algebra implies the injectivity of $\zeta: H^2(G(V_1)) \longrightarrow H^2(\prod_{v \in V_1} C_v(K_v))$, and the proposition follows from 4.3.

PROOF OF PROPOSITION 4.2. We assume that G/K is of inner type A. In view of Theorem 2.1 and Proposition 3.2, we may (and will) assume that $V \subset V_f^K$, and G is not of type A_1. Let $V_1 = V \cap T$, $V_2 = V - V_1$. Then $H^1(G(V_2))$ is trivial and therefore, by the Künneth formula we have $H^2(G(V)) = H^2(G(V_1)) \times H^2(G(V_2))$. Let

$$x = (x_1, x_2) \in \mathrm{Ker}(H^2(G(V)) \longrightarrow H^2(G(K))).$$

There exists an open subgroup $U \subset G(V_2)$ such that the restriction of x_2 to U is trivial. Then $x_1 \in \mathrm{Ker}(H^2(G(V_1)) \longrightarrow H^2(G(K) \cap U))$, and from Proposition 4.5 we conclude that $x_1 = 0$. Therefore $x_2 \in \mathrm{Ker}(H^2(G(V_2)) \longrightarrow H^2(G(K)))$, and it suffices to prove that the latter kernel is trivial. In other words, we may assume in addition that $V \cap T = \emptyset$.

Now we will introduce new V_1 and V_2. Namely, if, as before, $G = \mathbf{SL}_{1,\mathcal{A}}$, write the algebra $\mathcal{A}_v = \mathcal{A} \otimes_K K_v$, for $v \in V^K$, as $\mathcal{A}_v = M_{n_v}(D_v)$, where D_v is a central division algebra of degree d_v over K_v, and then take

$$V_1 = \{v \in V \mid n_v > 2\} \quad \text{and} \quad V_2 = V - V_1.$$

Again, by the Künneth formula,

$$H^2(G(V)) = H^2(G(V_1)) \times H^2(G(V_2)).$$

Let $x = (x_1, x_2) \in \mathrm{Ker}(H^2(G(V)) \to H^2(G(K)))$. Just as above, there exists an open subgroup U of $G(V_2)$ such that the restriction of x_2 to U is trivial, and then $x_1 \in \mathrm{Ker}(H^2(G(V_1)) \to H^2(G(K) \cap U))$. To use Proposition 4.3 to conclude that $x_1 = 0$, it is enough to verify that for every $v \in V_1$, there exists a maximal K_v-torus C_v of G, which splits over a cyclic extension of K_v, such that $\zeta_v\colon H^2(G(K_v)) \to H^2(C_v(K_v))$ is injective. Such a C_v is constructed as follows. With notations as above, let $L_v \subset D_v$ be a maximal unramified subfield. Take

$$C_v = \underbrace{(R_{L_v/K_v}(\mathbf{GL}_1) \times \ldots \times R_{L_v/K_v}(\mathbf{GL}_1))}_{n_v} \bigcap \mathbf{SL}_{n_v,D_v}.$$

Then C_v splits over L_v, which is a cyclic extension of K_v. Let

$$H_v = \mathbf{SL}_{n_v,L_v} \quad \subset \quad \mathbf{SL}_{n_v,D_v} = G.$$

Note that $H_v \simeq R_{L_v/K_v}(SL_{n_v})$. As shown in [PrRa2], Proposition 8.42, the restriction map $H^2(G(K_v)) \to H^2(H_v(K_v))$ is injective. Now, let $B \subset \mathbf{SL}_{n_v,L_v}$ be the diagonal torus. Since $n_v > 2$, according to 1.6 the restriction map $H^2(H_v(K_v)) \to H^2(B(K_v))$ is injective, and then, so is the composite map

$$H^2(G(K_v)) \longrightarrow H^2(H_v(K_v)) \longrightarrow H^2(B(K_v)).$$

However $B \subset C_v$, implying the injectivity of ζ_v.

So, it remains to prove that the restriction $H^2(G(V_2)) \to H^2(G(K))$ is injective. Obviously, $V_2 = \emptyset$ if d is odd, so we assume that d is even. Let $V_0 = \{v \in V_f^K \mid d_v \neq 1\}$, and let L/K be an extension of degree $d/2$ such that L_v is an unramified field extension of K_v of degree $d/2$ for all $v \in V_0$. Furthermore, let M/K be a quadratic extension linearly disjoint from L/K and satisfying the following local conditions:

$M_w = K_v$ for $w \mid v,\ v \in V_2$;

M_v/K_v is a totally ramified quadratic extension for $v \in V_0 - V_2$;

$M_w = \mathbf{C}$ for $w \mid v,\ v \in V_\infty^K$.

Then $F = LP$ imbeds in $\mathcal{A}$ as a maximal subfield (cf. Appendix A). Let Δ be the centralizer of L in $\mathcal{A}$, $\mathcal{H} = \mathbf{SL}_{1,\Delta}$ be the corresponding L-group and $H = R_{L/K}(\mathcal{H})$. It follows from Proposition 3.2 that $H^2(H(V_2)) \to H^2(H(K))$ is injective. On the other hand, for $v \in V_2$, there is an identification of G over K_v with $\mathbf{SL}_{2,D_v}$ such that under this identification, H gets identified with the subgroup $\mathbf{SL}_{2,L_v} \subset \mathbf{SL}_{2,D_v}$, and then $H^2(G(K_v)) \to H^2(H(K_v))$ is injective by Proposition 8.42 of [PrRa2]. Since $H^2(G(V_2)) = \prod_{v \in V_2} H^2(G(K_v))$, this implies the injectivity of $H^2(G(V_2)) \to H^2(H(V_2))$, and completes the proof of Proposition 4.2.

The next step in the proof of the triviality of $M(S,G)$ in Theorem 4.1, is reduction to the case where $d = p$ is a prime. As above, let $V_0 = \{v \in V_f^K \mid d_v \neq 1\}$, and let $S' = S \cup V_0 \cup V_\infty^K$. Then

$$H^2(G(A(S))) = H^2(G(S'-S)) \times \prod_{v \notin S'} H^2(G(K_v)).$$

Let $x = (x_{S'-S}, (x_v)_{v \notin S'}) \in M(S,G)$. It suffices to prove that $x_v = 0$ for each $v \notin S'$. (Indeed then, $x_{S'-S} \in \mathrm{Ker}(H^2(G(S'-S)) \to H^2(G(K)))$; since the latter is trivial by Proposition 4.2, we obtain $x = 0$, as required.) Fix $v_1 \notin S'$. By our assumption, $\mathcal{A}_{v_0} = M_{n_{v_0}}(D_{v_0})$, where $n_{v_0} > 1$ if v_0 is nonarchimedean, and $n_{v_0} = d$ (i.e. $d_{v_0} = 1$) if v_0 is real. Let p be a prime divisor of n_{v_0}, and let L/K be an extension of degree $m = d/p$, with the following local properties:

L_v is a field extension of K_v of degree m for all $v \in V_0$;
$L \otimes_K K_{v_1} = K_{v_1}^m$;

$$L \otimes_K K_v = \begin{cases} \mathbf{C}^{m/2} & \text{if } v \text{ is real, } v \neq v_0 \text{ and } m \text{ is even,} \\ \mathbf{R}^m & \text{if } v = v_0 \text{ is real.} \end{cases}$$

Furthermore, let M/K be an extension of degree p, linearly disjoint from L/K, such that

M_v is a field extension of degree p linearly disjoint from L_v/K_v, for all $v \in V_0 - \{v_0\}$;

$M \otimes_K K_{v_i} = K_{v_i}^p$ for $i = 0, 1$;

$M \otimes_K K_v = \mathbf{C}$ for real $v \neq v_0$ if $p = 2$.

Then $F = LM$ imbeds into $\mathcal{A}$ as a maximal subfield (note that if v_0 is real, then by assumption $\mathcal{A}_{v_0}$ is the full matrix algebra over K_{v_0}, and there is no local obstruction to the imbedding at v_0) . Let $\mathcal{B}$ be the centralizer of L in $\mathcal{A}$; $\mathcal{B}$ is a central simple algebra over L of degree p; we will denote the L-group $\mathbf{SL}_{1,\mathcal{B}}$ by $\mathcal{H}$ and let $H = R_{L/K}(\mathcal{H})$. Now, assume triviality of the metaplectic kernel in the situation described in Theorem 4.1, for the groups corresponding to simple algebras of prime degree. Clearly, $M(S,H) \simeq M(\mathcal{S},\mathcal{H})$, where $\mathcal{S}$ consists of all extensions of places from S to L. Since the class of $\mathcal{B}$ in the Brauer group of L coincides with the image of the class of $\mathcal{A}$ under the natural map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ (cf. [Pi: §13.3]), it follows from our construction that $\mathcal{B}$ splits completely over any extension of v_0 to L; besides, if v_0 is real then so are all its extensions. This means that the conditions of Theorem 4.1 are satisfied for $\mathcal{H}$ and $\mathcal{S}$, and therefore $M(S, H)$ is trivial. In particular, the restriction of x_{v_1} to $H(K_{v_1})$ is trivial. On the other hand, $G \simeq \mathbf{SL}_d$ over K_{v_1}, and $C = R^{(1)}_{F/K}(\mathbf{GL}_1)$ is a maximal K_{v_1}-split torus in G. Being the maximal semi-simple subgroup of the centralizer in G of $R^{(1)}_{L/K}(\mathbf{GL}_1)$, the subgroup H contains the 3-dimensional root subgroup G_α for some root α of G with respect to C. Since all the roots in this case have the same length, by Theorem 1.2, the restriction map $H^2(G(K_{v_1})) \to H^2(H(K_{v_1}))$ is injective. Hence, $x_{v_1} = 0$, as required.

Now, we may (and will) assume that $G = \mathbf{SL}_{1,\mathcal{A}}$, where $\mathcal{A}$ is a central simple algebra of prime degree $p > 2$. To establish Theorem 4.1 it is sufficient to prove the following (cf. the argument after the statement of Theorem 3.4):

Theorem 4.6 *Let q be a prime. Assume that $q = 2$ if v_0 is real. Then $M(S, G)$ contains no elements of order q.*

Proof. We fix a finite set $S' \supset S \cup V^K_\infty$ such that for $v \notin S'$ the following is true:

(i) $\mathcal{A} \otimes_K K_v \simeq M_p(K_v)$;

(ii) for some (and consequently, for all) maximal compact subgroup $\mathcal{C}_v$ of $G(K_v)$, the restriction map $H^2(G(K_v)) \to H^2(\mathcal{C})$ is trivial (cf. 1.8).

Then,
$$H^2(G(A(S))) = H^2(G(S' - S)) \times \prod_{v \notin S'} H^2(G(K_v)),$$
and it is enough to show that if $x = (x_{S'-S}, (x_v)_{v \notin S'}) \in M(S, G)$ is an element of order q, then $x_v = 0$ for all $v \notin S'$. Fix a $v_1 \notin S'$. It follows from A.6 that there exists a maximal subfield $L \subset \mathcal{A}$ which is a cyclic extension of K, and such that $[L_{w_i} \colon K_{v_i}] = 1$ for $w_i \mid v_i$, $i = 0, 1$. Let σ be a generator of the Galois group of L/K. Let $C = R^{(1)}_{L/K}(\mathbf{GL}_1)$ be the maximal torus of G corresponding to L. Our proof is based on an analysis of the commutator $[\tilde{a}, \tilde{b}]$ for $a, b \in C(A(S))$, where
$$1 \to I \longrightarrow E \xrightarrow{\pi} G(A(S)) \to 1$$
is the extension corresponding to x and $\tilde{a} \in \pi^{-1}(a), \tilde{b} \in \pi^{-1}(b)$. As observed in 1.7, there exists an open neighborhood of the identity U in $G(S' - S)$ such that for $a, b \in C(S' - S) \cap U$ we have $[\tilde{a}, \tilde{b}] = 1$. So, if $a = (a_v)$, $b = (b_v) \in U \times C(A(S'))$, then
$$[\tilde{a}, \tilde{b}] = \prod_{v \notin S'} [\tilde{a_v}, \tilde{b_v}]$$
(Lemma 1.9), so it is enough to calculate the local commutators $[\tilde{a_v}, \tilde{b_v}]$ for $v \notin S'$. There are two different cases to consider ($w \mid v$): (i) $[L_w \colon K_v] = p$, and (ii) $[L_w \colon K_v] = 1$.

We assert that in the first case, for any $a_v, b_v \in C(K_v)$, $[\tilde{a_v}, \tilde{b_v}] = 1$. Indeed, in this case C is K_v-anisotropic, hence $C(K_v)$ is compact and is contained in a maximal compact subgroup $\mathcal{C}_v$ of $G(K_v)$. Since by our choice of S', π splits over $\mathcal{C}_v$, and therefore, $\tilde{a}_v, \tilde{b}_v$ commute, as claimed.

In the second case C is a K_v-split maximal torus of $G \simeq \mathbf{SL}_p$, so there exists a $g \in G(K_v)$ such that gCg^{-1} is the diagonal torus. Now, if x_v corresponds to the character $\chi_v \in \hat{\mu}(K_v)$ (see 1.1), then for $a_v, b_v \in C(K_v)$ of the form

$$a_v = g^{-1}\mathrm{diag}(a_1, \ldots, a_p)g, \quad b_v = g^{-1}\mathrm{diag}(b_1, \ldots, b_p)g,$$

we have

$$[\tilde{a_v}, \tilde{b_v}] = \chi_v(\prod_{i=1}^{p}(a_i, b_i)_v);$$

where $(\star, \star)_v$ is the norm residue symbol on K_v of power $\mu_v = \#\mu(K_v)$; cf. 1.5. It follows that, if for elements $a, b \in C(K)$, we denote their replicas in $C(K_v)$ by a_v, b_v, then the corresponding commutator equals

$$[\tilde{a_v}, \tilde{b_v}] = \chi_v(\Pi_v(a, b)) \quad \text{where,} \quad \Pi_v(a, b) = \prod_{i=0}^{p-1}(\sigma^i(a), \sigma^i(b))_w,$$

w is some extension of v to L, and $(\star, \star)_w$ is the norm residue symbol on $L_w = K_v$ of power μ_v. By Hilbert's Theorem 90, any $a, b \in C(K)$ can be written in the form

$$a = \frac{\sigma(s)}{s}\ ,\ b = \frac{\sigma(t)}{t}$$

for some $s, t \in L^\star$. Given such a and b, we have:

$$\begin{aligned}
&\Pi_v(a, b) \\
&= \prod_{i=0}^{p-1}(\sigma^i(\frac{\sigma s}{s}), \sigma^i(\frac{\sigma t}{t}))_w \\
&= \prod_{i=0}^{p-1}(\sigma^{i+1}(s), \sigma^{i+1}(t))_w \cdot \prod_{i=0}^{p-1}(\sigma^i(s), \sigma^i(t))_w \cdot \prod_{i=0}^{p-1}(\sigma^i(s), \sigma^{i+1}(t))_w^{-1} \cdot \prod_{i=0}^{p-1}(\sigma^{i+1}(s), \sigma^i(t))_w^{-1} \\
&= \prod_{i=0}^{p-1}(\sigma^i(\frac{s^2}{\sigma(s)\sigma^{-1}(s)}), \sigma^i(t))_w.
\end{aligned}$$

Since $w_1 = w$, $w_2 = w \circ \sigma$, $\ldots$, $w_p = w \circ \sigma^{p-1}$ are the distinct extensions of v to L, it follows from the properties of the norm residue symbol that there exist characters $\chi_{\bar{v}} \in \hat{\mu}(K_v)$, one for each extension $\bar{v}$ of v to L, *of order equal to the order of* χ_v such that

$$[\tilde{a}_v, \tilde{b}_v] = \prod_{\bar{v}|v}\chi_{\bar{v}}((\frac{s^2}{\sigma(s)\sigma^{-1}(s)}, t)_{\bar{v}}).$$

Now, since π splits over $G(K)$, for $a, b \in C(K)$ we should have $[\tilde{a}, \tilde{b}] = 1$. So, letting $V' = \{v \in V^K - S' \mid [L_w : K_v] = 1\}$, we conclude from the above computation that if $s, t \in L^\star$ are such that $\sigma(s)/s$, $\sigma(t)/t \in C(K) \cap U$, then

$$\prod_{v \in V'} \prod_{\bar{v} | v} \chi_{\bar{v}}((\frac{s^2}{\sigma(s)\sigma^{-1}(s)}, t)_{\bar{v}}) = 1. \tag{2}$$

Setting $\chi_{\bar{v}} = 1$ for $\bar{v} \mid v$, $v \notin V'$, we can rewrite (2) in the form of a reciprocity law

$$\prod_{\bar{v} \in V^L} \chi_{\bar{v}}((\frac{s^2}{\sigma(s)\sigma^{-1}(s)}, t)_{\bar{v}}) = 1.$$

Since $\chi_{w_0} = 1$ for $w_0 \mid v_0$, and additionally, $\chi_{\bar{v}}^q = 1$ for all $\bar{v} \in V^L$, and $q = 2$ in case v_0 is real, in order to use the proposition in Appendix B to conclude that $\chi_{w_1} = 1$ for $w_1 \mid v_1$ (and hence $\chi_{v_1} = 1$, or, equivalently, $x_{v_1} = 0$), we need to make sure that there exists an $s \in L^\star$ such that

$$\begin{array}{ll} w_1(s^2/(\sigma(s)\sigma^{-1}(s))) = 1, & \text{and} \\ w_0(s^2/(\sigma(s)\sigma^{-1}(s))) = 1 & \text{if } v_0 \text{ is nonarchimedean,} \\ s^2/(\sigma(s)\sigma^{-1}(s)) < 0 \text{ in } L_{w_0} & \text{if } v_0 \text{ is real.} \end{array}$$

However, the existence of such an $s \in L^\star$ is guaranteed by the weak approximation property for L since the places

$$w_0,\ w_0 \circ \sigma,\ w_0 \circ \sigma^{-1},\ w_1,\ w_1 \circ \sigma,\ \text{ and } w_1 \circ \sigma^{-1}$$

are pairwise distinct and do not lie over places from $S' - S$. Thus the proof of the triviality of $M(S, G)$ in Theorem 4.1 is complete.

Now we turn to the proof of the last two assertions of Theorem 4.1. Let $G = \mathbf{SL}_{1,\mathcal{A}}$, where $\mathcal{A}$ is a central simple algebra over K of degree d, with no restriction on d now. As observed in 1.13, the fact that for an arbitrary S, $M(S, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$ is a consequence of what we have already proved. So, it remains only to be prove that if $\mu = \#\mu(K)$, then the order of $M(\emptyset, G)$ is at least $\mu/2$, and in fact is equal to μ either if $\mathcal{A}$ is a quaternion algebra, or if d, the degree of $\mathcal{A}$, is odd, or else if K contains $\sqrt{-1}$, a primitive 4-th root of unity. This follows from

Proposition 4.7 *Let p be a prime divisor of μ, and p^α be the maximal power of p dividing μ. Then*

(i) if $p > 2$, then $M(\emptyset, G)$ has an element of order p^α;

(ii) if $p = 2$, then $M(\emptyset, G)$ has an element of order at least $p^{\alpha-1}$, and moreover, it has an element of order p^α in each of the following cases: (a) $\alpha \geq 2$, (b) d is odd, (c) A is a quaternion algebra.

We begin the proof by drawing the following consequence from Matsumoto's construction of the metaplectic extensions for split groups.

Lemma 4.8 *Let $\mathcal{G}$ be an absolutely simple, simply connected K-group which splits over a finite extension L/K. Then $M(\emptyset, \mathcal{G})$ contains an element y of order divisible by the order s of the group $N_{L/K}(\mu(L))$. Moreover, for every nonarchimedean $v \in V^K$ such that $L_{\bar{v}} = K_v$, for all $\bar{v} \mid v$, the order of the projection $y_v \in H^2(\mathcal{G}(K_v))$ is exactly s.*

Proof. Let A_L be the adele-ring of L. According to [Ma], there exists an extension

$$1 \to I \longrightarrow E \xrightarrow{\pi} \mathcal{G}(A_L) \to 1,$$

splitting over $\mathcal{G}(L)$, such that the corresponding element $x \in M(\emptyset, \mathcal{G}/L)$,

$$M(\emptyset, \mathcal{G}/L) := \operatorname{Ker}(H^2(\mathcal{G}(A_L)) \to H^2(\mathcal{G}(L))),$$

has order $\mu_L = \#\mu(L)$. Consider the natural imbedding $\mathcal{G}(A) \hookrightarrow \mathcal{G}(A_L)$, and the induced extension

$$1 \to I \longrightarrow \pi^{-1}(\mathcal{G}(A)) \longrightarrow \mathcal{G}(A) \to 1. \tag{3}$$

We claim that the order of the element y of $M(\emptyset, \mathcal{G})$ corresponding to (3) is divisible by s. Indeed, x corresponds to a character $\chi \in \hat{\mu}(L)$ of order μ_L in the sense that the characters $\chi_w \in \hat{\mu}(L_w)$, for $w \in V^L$, describing x as an element of $H^2(\mathcal{G}(A_L)) = \prod_w H^2(\mathcal{G}(L_w))$ have the following form:

$$\chi_w = \chi \circ [\mu_w/\mu_L], \tag{4}$$

where for an integer m, $[m]$ denotes the endomorphism $\zeta \mapsto \zeta^m$, and μ_w is equal to $\#\mu(L_w)$ if w is noncomplex, and is 0 otherwise. Pick $v \in V_f^K$ such that $[L_{\bar{v}} \colon K_v] = 1$ for all extensions $\bar{v} \mid v$ (then, in particular, $\mathcal{G}$ splits over K_v). Obviously, the v-component y_v is the restriction of

$$(x_{\bar{v}})_{\bar{v}|v} \in \prod_{\bar{v}|v} H^2(\mathcal{G}(L_{\bar{v}}) = H^2(\prod_{\bar{v}|v} \mathcal{G}(L_{\bar{v}}))$$

via the imbedding $\mathcal{G}(K_v) \hookrightarrow \mathcal{G}(L \otimes_K K_v) = \prod_{\bar{v}|v} \mathcal{G}(L_{\bar{v}})$. It suffices to show that the order of y_v equals s. It follows from (4) that the Steinberg cocycle attatched to $x_{\bar{v}}$ is

$$\chi((\star, \star)_{\bar{v}}^{\mu_{\bar{v}}/\mu_L}) = \chi([\star, \star]_{\bar{v}})$$

where $(\star, \star)_{\bar{v}}$ (resp. $[\star, \star]_{\bar{v}}$) is the norm residue symbol on $L_{\bar{v}}$ of power $\mu_{\bar{v}}$ (resp. μ_L). However, for any imbedding $\sigma \colon L \hookrightarrow \bar{K}_v$ we have the following "functoriality" property:

$$[\sigma(a), \sigma(b)]_{\bar{v}} = \sigma^{-1}([a, b]_{\bar{v} \circ \sigma}),$$

implying that for $a, b \in K^\star$ we have

$$[a, b]_{\bar{v} \circ \sigma} = \sigma([a, b]_{\bar{v}}).$$

Therefore, the Steinberg cocycle corresponding to y_v is $\chi(N_{L/K}([\star,\star]_{\bar{v}}))$, and the lemma follows.

To prove Proposition 4.7, we will apply Lemma 4.8 to $\mathcal{G} = G$ (in proving the analogous assertion for groups of other types in §§6-7, $\mathcal{G}$ will often be different from G.) Obviously, we may assume that K contains a nontrivial p-th root of unity (otherwise there is nothing to prove), in particular the characteristic of K is different from p. Now, if p does not divide d, we may take for L any maximal subfield in $\mathcal{A}$. Then the p-primary component $\mu(K)_p$ (= the set of elements of $\mu(K)$ of p-power order) is clearly contained in $N_{L/K}(\mu(L))$, and the proposition is proved. Now assume that $p \mid d$, and let $d = p^\delta \cdot l$, $(l,p) = 1$. Let F be an extension of K of degree l such that F_v/K_v is a field extension of degree l for all v for which $\mathcal{A}_v \not\simeq M_d(K_v)$. If ζ_{p^β} is a primitive p^β-th root of unity, then for β sufficiently large and for $L = F(\zeta_{p^\beta})$, the degree $[L_w\colon K_v]$ is divisible by n for all v such that $\mathcal{A}_v \not\simeq M_d(K_v)$ and all $w \mid v$, implying that L is a splitting field for $\mathcal{A}$.

Lemma 4.9 *Let p^γ be the maximal power of p dividing $\mu_F = \#\mu_F$. Then for any $\beta \geq \gamma$ and for $L = F(\zeta_{p^\beta})$, we have:*

(i) if $p > 2$, then $N_{L/F}(\mu(L))$ contains an element of order p^γ;

(ii) if $p = 2$, then $N_{L/F}(\mu(L))$ contains an element of order p^γ if $\gamma \geq 2$.

PROOF. Considering the action of $\mathrm{Gal}(L/F)$ on the roots of unity, we set up an identification of $\mathrm{Gal}(L/F)$ with a subgroup $\Gamma \subset \mathcal{Z} = (\mathbf{Z}/p^\beta\mathbf{Z})^\star$. Since Γ acts trivially on ζ_{p^γ}, and $\gamma \geq 1$, we have

$$\Gamma \subset \mathcal{Z}_\gamma = \{a \in \mathbf{Z}/p^\beta\mathbf{Z} \mid a \equiv 1 (\mathrm{mod}\, p^\gamma)\}.$$

Then $N_{L/F}(\mu(L))$ contains

$$\zeta = \prod_{a \in \mathcal{G}_\gamma} a(\zeta_{p^\beta}) = \prod_{j=0}^{p^{\beta-\gamma}-1} (\zeta_{p^\beta})^{(1+p^\gamma j)} = \zeta_{p^\beta}^m;$$

where $m = p^{\beta-\gamma} + p^\gamma(\frac{1}{2}(p^{\beta-\gamma}-1)p^{\beta-\gamma}) = p^{\beta-\gamma} + \frac{1}{2}p^\beta(p^{\beta-\gamma}-1)$. If p is odd then $\zeta = (\zeta_{p^\beta})^{p^{\beta-\gamma}} = \zeta_{p^\gamma}$, is a primitive p^γ-th root of unity. If $p = 2$, then $m = p^{\beta-\gamma} + p^{\beta-1}(p^{\beta-\gamma}-1)$, so if $\beta > \gamma$, $p^{\beta-\gamma}-1$ is odd, and consequently, $\zeta = -\zeta_{p^\gamma}$. This implies that if $\gamma \geq 2$, ζ is a primitive p^γ-th root of unity. (In the remaining case, $\gamma = 1$, we (unfortunately) have $\zeta = 1$.) Lemma 4.9 is proved.

Now if $p > 2$, then as follows from Lemma 4.9, the p-primary component $\mu(F)_p$ of $\mu(F)$ is contained in $N_{L/F}(\mu(L))$. On the other hand, since $l = [F\colon K]$ is prime to p, we have

$$\mu(K)_p = (\mu(K)_p)^l = N_{F/K}(\mu(K)_p) \subset N_{F/K}(\mu(F)_p).$$

So, $\mu(K)_p \subset N_{F/K}(N_{L/F}(\mu(L)) = N_{L/K}(\mu(L))$, as required. The same argument applies if $p = 2$ but $\alpha \geq 2$.

This covers all cases in Proposition 4.7 except for the following: $p = 2$, $\alpha = 1$ and $\mathcal{A}$ is a quaternion algebra. The argument here is based on a different idea and works, in fact, without additional assumptions about p and α. However, before proceeding to this argument we observe that the above discussion allows us to establish as a by-product the following fact.

4.10. *If v_0 is a nonarchimedean place such that $\mathcal{A}_{v_0} = \mathcal{A} \otimes_K K_{v_0}$ is a division algebra and p is the characteristic of the residue field of K_{v_0}, then in case $p > 2$, $M(\{v_0\}, G)$ has no p-torsion.* Of course, there is nothing to prove in case K is of positive characteristic, so we assume that K is of characteristic zero. Let $L = F(\zeta_{p^\beta})$ be a splitting field for $\mathcal{A}$ as above. We have the following commutative diagram:

$$\begin{array}{lcl} M(\emptyset, G/L) & \xrightarrow{\delta_1} & M(\emptyset, G) \\ \delta_3 \downarrow & & \delta_4 \downarrow \\ \prod_{w|v_0} H^2(G(L_w)) & \xrightarrow{\delta_2} & H^2(G(K_{v_0})). \end{array}$$

Using the argument given in [PrRa4: 8.2], one shows that the image of the composite map $\delta_2 \circ \delta_3$ contains an element of order equal to the order of the p-primary component $\hat{\mu}(K)_p$. Since $M(\emptyset, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$, we conclude that the restriction of δ_4 to the p-primary component $M(\emptyset, G)_p$ is injective, implying the triviality of $M(\{v_0\}, G)_p$.

Now, to complete the proof of Proposition 4.7, we need to handle only the case $\mathcal{A} = D$, D a quaternion division algebra. Let σ be the standard involution of D, h the hyperbolic σ-hermitian form on D^2 and $H = \mathbf{SU}(h)$. Clearly, H is a simply connected group of type C_2. If $\{e_1, e_2\}$ is an orthogonal basis, then the transformations of the form

$$\begin{cases} e_1 \mapsto g_1 e_1 \\ e_2 \mapsto g_2 e_2 \end{cases} \qquad g_1, g_2 \in G = \mathbf{SL}_{1,D},$$

constitute a K-subgroup of H, identifiable with $G \times G$. Any splitting field L for G splits also H, and each factor in $G \times G$ corresponds to a long-root subgroup with respect to a suitable L-split maximal torus in H. Let us identify G with one of these factors. Now, since $C_2 = B_2$, H is isomorphic to the spinor group of a nondegenerate quadratic form f in 5 variables. Take $g = f \perp (-f)$ and $C = \mathbf{Spin}(g)$. Clearly, C is K-split, so by [Ma] there exists an element $x \in M(\emptyset, C)$ of order $\mu = \mu_K$; moreover, $x = (x_v)$, where $x_v (\in H^2(C(K_v)))$ has order μ for every noncomplex v. We assert that the restriction of x to $G(A)$ is an element $y \in M(\emptyset, G)$ of order equal to the order of x. If $v \in V_f^K$ is such that G is K_v-split, then $H^2(G(K_v))$ is a direct factor of $H^2(G(A))$ and the corresponding component y_v of y is the image of x_v under the restriction map $H^2(C(K_v)) \to H^2(G(K_v))$. So, it suffices to show that this map is injective (in fact, an isomorphism). However, since the Witt index of f over K_v is 2, the restriction map $H^2(C(K_v)) \to H^2(H(K_v))$ is injective (cf. [PrRa1], Proposition 1.9). On the other hand, G is identified (over K_v) with a long-root subgroup of H with respect to a K_v-split maximal torus in H, therefore the map $H^2(H(K_v)) \to H^2(G(K_v))$ is also injective; this finishes the proof of 4.7.

5 Groups of type ${}^2A_r$

In this section we shall prove the following analog of Theorem 4.1 for groups of type ${}^2A_r$.

Theorem 5.1 *Let G be an absolutely simple, simply connected group of type ${}^2A_r$ ($r > 1$) over a global field K. Let S be a finite set of places of K containing a place v_0 which is either nonarchimedean and G is K_{v_0}-isotropic, or v_0 is real and $G(K_{v_0})$ is not (topologically) simply connected. Assume that Conjecture (U) of §2 holds for any finite subset V of $V^K - S$. Then $M(S, G)$ is trivial. If moreover, Conjecture (U) holds for an arbitrary finite set V of places of K, then $M(\emptyset, G)$ is isomorphic to a subgroup of $\mu(\hat{K})$ of index at most two.*

It is well known (see, for example, [PR2], §2.3) that G can be realized as a special unitary group $\mathbf{SU}(f)$, where f is a nondegenerate hermitian form on the m-dimensional vector space D^m, D being a central division algebra over a quadratic extension L of K, provided with an involution σ of the second kind which restricts to the nontrivial automorphism of L/K. However, for our purposes it is more convenient to describe this group in a slightly different way: Let $\mathcal{A} = M_m(D)$ and F be the matrix of f with respect to the standard basis of D^m. Let $n = \sqrt{\dim_L \mathcal{A}}$. Define an involution τ on $\mathcal{A}$ by the formula

$$\tau((a_{ij})) = F(a_{ji}^{\sigma})F^{-1}.$$

Then $\mathbf{SU}(f)$ can be identified with $\mathbf{SU}(\mathcal{A}, \tau) = \{x \in \mathbf{SL}_{1,\mathcal{A}} \mid x\tau(x) = 1\}$. In the sequel, we will mostly use the realization of G as $\mathbf{SU}(\mathcal{A}, \tau)$. For real v_0, the condition that $G(K_{v_0})$ is not (topologically) simply connected is equivalent to the condition that if $[L_{w_0} : K_{v_0}] = 1$, $w_0 \mid v_0$, then $\mathcal{A} \otimes_K K_{v_0} \simeq M_n(K_{v_0}) \oplus M_n(K_{v_0})$, and if $[L_{w_0} : K_{v_0}] = 2$, then G is K_{v_0}-isotropic.

If $n = 2$, then G is of type A_1; since this case has already been treated in §3, we may (and will) assume in this section that $n > 2$.

As in the previous two sections, we begin by proving the triviality of $M_V(G)$.

Proposition 5.2 *Let V be a finite set of places of K such that Conjecture (U) holds for V. Then the restriction map*

$$\rho_V : H^2(G(V)) \to H^2(G(K))$$

is injective.

PROOF. Since Conjecture (U) holds for V, Ker ρ_V = Ker ρ_{V_0}; where V_0 is the subset of V consisting of all the nonarchimedean places. Therefore, after replacing V by V_0 we may assume that $V \subset V_f^K$. Let $V_1 = V \cap T$, $V_2 = V - V_1$, where, as before, $T = \{v \in V_f^K \mid G \text{ is } K_v\text{-anisotropic }\}$. Then

$$H^2(G(V)) = H^2(G(V_1)) \times H^2(G(V_2)).$$

For any $x = (x_1, x_2) \in \operatorname{Ker} \rho_V$, there exists an open subgroup $U \subset G(V_2)$ such that the restriction of x_2 to U is trivial. It follows that

$$x_1 \in \operatorname{Ker}(H^2(G(V_1)) \longrightarrow H^2(G(K) \cap U)),$$

and by Proposition 4.5, $x_1 = 0$ (recall that n is assumed to be > 2). Then

$$x_2 \in \operatorname{Ker}(H^2(G(V_2)) \xrightarrow{\rho_{V_2}} H^2(G(K))),$$

and it remains to prove that Ker $\rho_{V_2} = 0$. Thus we are reduced to the case where $V \cap T = \emptyset$. To proceed with the proof, we need to introduce another V_1 and V_2. Let V_1 be the set of $v \in V$ such that G is K_v-isomorphic to a group of the form $\mathbf{SL}_{2,\Delta_v}$ for some division algebra Δ_v over K_v ; $V_2 = V - V_1$. We claim that for every $v \in V_2$, there exists a maximal K_v-torus C_v, whose splitting field is a cyclic extension of K_v, such that the restriction map $H^2(G(K_v)) \to H^2(C_v(K_v))$ is injective. This was established for the case $[L_w : K_v] = 1$, $w \mid v$, in the course of proof of Proposition 4.2, and it follows for the case $[L_w : K_v] = 2$ from

Lemma 5.3 *Let $v \in V_f^K$ be such that $[L_w : K_v] = 2$, $w \mid v$. Then there exists a maximal K_v-torus $C \subset G$ which splits over L_w and such that the restriction map*

$$H^2(G(K_v)) \longrightarrow H^2(C(K_v))$$

is injective.

PROOF. As is well known, G is K_v-isomorphic to the special unitary group $\mathbf{SU}(g)$ of a nondegenerate isotropic hermitian form g on L_w^d, $d \geq 3$. Let $e_1, \ldots, e_d$ be a basis of L_w^d with respect to which g has the following form:

$$g(x_1, \ldots, x_d) = (x_1 x_2^\tau + x_2 x_1^\tau) + \alpha_3 x_3 x_3^\tau + \cdots + \alpha_d x_d x_d^\tau, \tag{1}$$

where τ denotes the nontrivial automorphism of L_w/K_v, $\alpha_i \in K_v$. We will show that for C one can take the following torus:

$$C = \{(c_1, \ldots, c_d) \in R_{L/K}(\mathbf{GL}_1)^2 \times R^{(1)}_{L/K}(\mathbf{GL}_1)^{d-2} \mid c_1 c_2^\tau = 1, \text{ and } c_1 c_2 \ldots c_d = 1\}. \tag{2}$$

We imbed C into G, letting its elements act on the basis vectors by homotheties: $c(e_i) = c_i e_i$.

Let $h = x_1 x_2^\tau + x_2 x_1^\tau$ and $H = \mathbf{SU}(h)$. Then H is K_v-isomorphic to $\mathbf{SL}_2$, and is, in fact, a long-root subgroup (with respect to a suitable maximal K_v-split torus of G); so by Theorem 1.2, the restriction map

$$\rho : H^2(G(K_v)) \longrightarrow H^2(H(K_v))$$

is injective. Now, let $x \in \mathrm{Ker}(H^2(G(K_v)) \to H^2(C(K_v)))$, $x \neq 0$, and

$$1 \longrightarrow I \longrightarrow E \xrightarrow{\pi} G(K_v) \longrightarrow 1$$

be the central extension corresponding to x. Then $y = \rho(x)$ corresponds to the induced extension:

$$1 \longrightarrow I \longrightarrow E' = \pi^{-1}(H(K_v)) \xrightarrow{\pi} H(K_v) \longrightarrow 1,$$

of $H(K_v)$. Let $\chi \in \mu(\hat{K_v})$ be the character associated with y (Theorem 1.1). Let $\alpha \in L_w$, $\beta \in K_v$, and consider the following two elements of $C(K_v)$:

$$a = (\alpha, (\alpha^{-1})^\tau, \alpha^{-1}\alpha^\tau, 1, \ldots, 1); \quad b = (\beta, \beta^{-1}, 1, \ldots, 1).$$

Since x restricts trivially to $C(K_v)$, for any two lifts $\tilde{a} \in \pi^{-1}(a)$, $\tilde{b} \in \pi^{-1}(b)$, we have

$$[\tilde{a}, \tilde{b}] = 1. \tag{3}$$

Let us now calculate this commutator in a different way. Clearly, C normalizes H, and the automorphism induced on H by Int a coincides with the automorphism ϵ_c obtained as a restriction of $\mathrm{Int}\, c$ under the imbedding $\mathbf{SL}_2 \subset \mathbf{GL}_2$, where $c = \mathrm{diag}(\gamma, 1)$, $\gamma = N_{L_w/K_v}(\alpha)$. As in §3, we let $\tilde{\epsilon}_c$ denote the lift of ϵ_c to E', and then using equation (12) of §3, we obtain that

$$[\tilde{a}, \tilde{b}] = \tilde{\epsilon}_c(\tilde{b})\tilde{b}^{-1} = \chi((\gamma, \beta)_v), \tag{4}$$

where, as usual, $(\star, \star)_v$ is the norm residue symbol on K_v of power $\mu_v = \#\mu(K_v)$. Comparing (3) and (4) we get $\chi((\gamma, \beta)_v) = 1$ for every $\gamma \in N_{L_w/K_v}(L_w^\star)$, $\beta \in K_v^\star$. But as we will show in a moment, this will imply that χ is trivial, thereby proving the lemma. Indeed, for any $\gamma \in K_v^\star$, $\gamma^2 \in N_{L_w/K_v}(L_w^\star)$, so by our assumption $\chi((\gamma^2, \beta)_v) = \chi^2((\gamma, \beta)_v) = 1$, implying at least that χ^2 is trivial. If we assume that χ is of order two, then for a fixed $\gamma \in K_v^\star$, the fact that $\chi((\gamma, \beta)_v) = 1$, for any $\beta \in K_v^\star$ entails $\gamma \in K_v^{\star 2}$. Consequently, in our setting, $N_{L_w/K_v}(L_w^\star) \subset K_v^{\star 2}$. A contradiction, since by local class field theory $[K_v^\star : N_{L_w/K_v}(L_w^\star)] = 2$, while $| K_v^\star / K_v^{\star 2} | \geq 4$. Lemma 5.3 is proved.

Now a straight forward argument using Proposition 4.3 shows that Ker $\rho_V =$ Ker ρ_{V_1}, i.e. we may assume that V consists entirely of places v such that G is K_v-isomorphic to $\mathbf{SL}_{2,\Delta_v}$ (if $n = \sqrt{\dim_L \mathcal{A}}$ is odd then $V_1 = \emptyset$ and the proof is complete). Let V_0 be the union of V_∞^K with the set of all $v \in V_f^K$ such that G is not K_v-quasi-split (note that in view of our assumption about V, $V_0 \supset V$). Also, fix some $v_1 \notin V_0$ with the property $[L_{w_1} : K_{v_1}] = 2$, $w_1 \mid v_1$, and construct an extension F/K of degree n as follows:

Let M/K be an extension of degree $n/2$ satisfying the following local requirements:

(1_M) $M \otimes_K K_v \simeq K_v^{n/2}$ for any $v \in V_0 \cup \{v_1\}$ such that $[L_w : K_v] = 2$, $w \mid v$;

(2_M) $M \otimes_K K_v$ is is an unramified field extension of K_v for any nonarchimedean $v \in V_0$ such that $[L_w : K_v] = 1$, $w \mid v$.

Furthermore, let N denote a quadratic extension of K, which is linearly disjoint from M over K and has the following properties:

(1_N) $N \otimes_K K_v \simeq K_v^2$ if either $v \in V \cup \{v_1\}$, $v \in V_0 - V$ and $[L_w : K_v] = 2$, $w \mid v$.

(2_N) $N \otimes_K K_v$ is a totally ramified quadratic extension of K_v for any nonarchimedean $v \in V_0 - V$ such that $[L_w : K_v] = 1$, $w \mid v$;

(3_N) $N \otimes_K K_v = \mathbf{C}$ for any real v such that $[L_w : K_v] = 1$.

Let $F = MN$. Then F (resp. $P = FL = F \otimes_K L$) is an extension of K (resp. L) of degree n. Indeed, in view of (1_M), (1_N), we have $F \otimes_K K_{v_1} \simeq K_{v_1}^n$, and therefore F (and even F', the normal closure of F over K) and L are linearly disjoint over K, since by our construction $L_{w_1} = L \otimes_K K_{v_1}$ is an extension of K_{v_1} of degree 2. Define an automorphism θ of P over K by the formula $\theta = \mathrm{id}_F \otimes_K \sigma$ (clearly, $\theta \mid L = \sigma$). We claim that there exists an imbedding

$$\epsilon : (P, \theta) \hookrightarrow (\mathcal{A}, \tau),$$

of algebras with involutions. Indeed, since F' and L are linearly disjoint over K, by Proposition A.2, it is enough to prove the existence of local imbeddings

$$\epsilon_v : (P \otimes_K K_v, \theta) \hookrightarrow (\mathcal{A} \otimes_K K_v, \tau),$$

and in fact we need to take care only of $v \in V_0$ (cf.[PR2], p. 340). However, if $[L_w : K_v] = 2$, then by our construction $F \otimes_K K_v \simeq K_v^n$, and the existence of ϵ_v follows from Proposition A.4. By Proposition A.3, for $v \in V_0$ with the property $[L_w : K_v] = 1$, the condition for the existence of ϵ_v is as follows: if $\mathcal{A} \otimes_K K_v \simeq M_{m_v}(\Delta_v) \oplus M_{m_v}(\Delta_v^\circ)$, where Δ_v is a division algebra over K_v, Δ_v° is the opposite algebra, then for any extension $\bar{v} \mid v$, the degree $[F_{\bar{v}} : K_v]$ should be divisible by the degree of Δ_v. However, by our construction for real v's we have $F_{\bar{v}} = \mathbf{C}$, and for nonarchimedean v's the degree $[F_{\bar{v}} : K_v]$ equals either $n/2$ or n, depending on whether or not v belongs to V, yielding the desired property.

Let us identify P with its image under ϵ. Put $R = ML$, and let $\mathcal{B}$ denote the centralizer of R in $\mathcal{A}$. Then $\mathcal{B}$ is τ-invariant, let $H_0 = \mathbf{SU}(\mathcal{B}, \tau)$; clearly, H_0 is a simple group of type A_1 defined over M. Take $H = R_{M/K}(H_0)$. Then it follows from the results of §§3-4 that the maps:

$$H^2(G(V)) \to H^2(H(V)) \text{ and } H^2(H(V)) \to H^2(H(K))$$

are injective, implying the injectivity of ρ_V. Proposition 5.2 is proved.

Now we are ready to give reduction to the case where the algebra $\mathcal{A}$ has prime degree (over L). Let $W = S \cup V_0$, where V_0 is the same as in the proof of Proposition 5.2. Then

$$\begin{aligned} H^2(G(A(S))) &= H^2(G(W-S)) \times H^2(G(A(W))) \\ &= H^2(G(W-S)) \times \prod_{v \notin W} H^2(G(K_v)). \end{aligned}$$

Let $x = (x_{W-S}, (x_v)_{v \notin W})) \in M(S, G)$. Assuming the theorem for the special unitary groups of algebras of prime degree, we will show that $x_v = 0$ for all $v \notin W$. Then

$$x_{W-S} \in \operatorname{Ker}(H^2(G(W-S)) \longrightarrow H^2(G(K))),$$

and since this kernel is trivial by Proposition 5.2, it will follow that $x = 0$.

Fix some $v_1 \notin W$. As we will show below, one can construct a K-subgroup H of G of the form $H = R_{E/K}(H')$, where E/K is an extension of degree n/p (p is a suitable prime divisor of n) and $H = \mathbf{SU}(\mathcal{B}, \tau)$, $\mathcal{B}$ is a central simple algebra over EL of dimension p^2 with involution τ of the second kind, having the following properties:

(1_H) H is K_{v_0}-isotropic and, moreover, if v_0 is real, then $H(K_{v_0})$ is not simply connected;

(2_H) the restriction map $\eta_{v_1} : H^2(G(K_{v_1})) \to H^2(H(K_{v_1}))$ is injective.

The imbedding $H \hookrightarrow G$ induces a map $\phi : M(S, G) \to M(S, H)$. Assuming the Theorem for H', we get $M(S, H) = \{0\}$. So, $\phi(x) = 0$, implying $\eta_{v_1}(x_{v_1}) = 0$, and therefore, $x_{v_1} = 0$ because η_{v_1} is injective.

To construct H with the properties (1_H), (2_H) above (note that this construction will depend on the choice of v_1), we need to fix another place $v_2 \notin W \cup \{v_1\}$, which extends uniquely to a place w_2 of L (then $[L_{w_2} : K_{v_2}] = 2$). Our choice of p, a prime divisor of n, is subject to only one condition: if $[L_{w_0} : K_{v_0}] = 1$ and $A \otimes_K K_{v_0} \simeq M_{m_{v_0}}(\Delta_{v_0}) \oplus M_{m_{v_0}}(\Delta^{\circ}_{v_0})$, where Δ_{v_0} is a division algebra over K_{v_0} and $\Delta^{\circ}_{v_0}$ is the opposite algebra, then p should divide m_{v_0} ($m_{v_0} > 1$ since, by our assumption, G is K_{v_0}-isotropic). Taking into account the fact that $\Delta_{v_0} = K_{v_0}$ if v_0 is real, and $[L_{w_0} : K_{v_0}] = 1$, $w_0 \mid v_0$, it is not difficult to see that there exists a tower of extensions $F \supset E \supset K$, $[F : E] = p$, $[E : K] = n/p$, with the following local properties:

(i) for $v = v_0$,

if $[L_w : K_v] = 2$, then $E \otimes_K K_v = K_v^{(n/p)}$ and $F \otimes_K K_v = L_w \oplus K_v^{(n-2)}$;
if $[L_w : K_v] = 1$, then $E_{\bar{v}} = E \otimes_K K_v$ is a field and
$F \otimes_E E_{\bar{v}} = E^p_{\bar{v}}$ for v nonarchimedean, and $F \otimes_K K_v = K_v^n$ for v real.

(ii) for $v = v_1$,

if $[L_w : K_v] = 2$, then

$$E \otimes_K K_v = \begin{cases} L_w^m, & n/p = 2m \\ L_w^m \oplus K_v, & n/p = 2m+1; \end{cases}$$

$$F \otimes_K K_v = \begin{cases} L_w^l, & n = 2l \\ L_w^l \oplus K_v, & n = 2l+1; \end{cases}$$

if $[L_w : K_v] = 1$, then $F \otimes_K K_v = K_v^n$.

(iii) $F \otimes_K K_{v_2} \simeq K_{v_2}^n$;

(iv) for $v \in V_0, v \neq v_0$,
$F \otimes_K K_v \simeq K_v^n$ if $[L_w : K_v] = 2$;
$F \otimes_K K_v \simeq R_v^{m_v}$ if $[L_w : K_v] = 1$, $\mathcal{A} \otimes_K K_v \simeq M_{m_v}(\Delta_v) \oplus M_{m_v}(\Delta_v^\circ)$,
and $R_v \subset \Delta_v$ is some maximal subfield.

Now, take $P = FL = F \otimes_K L$, $\theta = \mathrm{id}_F \otimes_K \sigma$. As before, since the normal closure F' of F over K is linearly disjoint from L, to prove the existence of an imbedding

$$\epsilon : (P, \theta) \hookrightarrow (\mathcal{A}, \tau),$$

it suffices to establish the existence of local imbeddings

$$\epsilon_v : (P \otimes_K K_v, \tau) \hookrightarrow (\mathcal{A} \otimes_K K_v, \tau),$$

for all $v \in V_0$. However, the existence of local imbeddings easily follows from Propositions A.3, A.4 in view of conditions $(i), (iv)$. We identify P with its image in $\mathcal{A}$ under ϵ; let $R = EL$ and $\mathcal{B}$ be the centralizer of R in $\mathcal{A}$. We will now show that $H = R_{E/K}(H')$, where $H' = \mathbf{SU}(\mathcal{B}, \tau)$ satisfies the requirements $(1_H), (2_H)$, above. Let $N = (R_{R/K}(\mathbf{GL}_1) \cap G)^\circ$ (the identity component) be the torus in G corresponding to R, and $C = C_G(N)$ be its centralizer. Then C is a reductive subgroup in G, whose connected center is N and the semisimple part $[C, C]$ is H. It follows from (i) that N is K_{v_0}-anisotropic, while the maximal torus $N' \subset G$ associated with P and containing N is K_{v_0}-isotropic; this implies that H is K_{v_0}-isotropic. Besides, if v_0 is real and $[L_{w_0} \colon K_{v_0}] = 1$, $w_0 \mid v_0$, then by our construction any extension $\bar{v}_0$ of v_0 to E is again real and the group H' is $E_{\bar{v}_0}$-isomorphic to $\mathbf{SL}_p$, this implies that the group $H(K_{v_0})$ is not simply connected. Furthermore, in view of (ii), N' contains a maximal K_{v_1}-split torus $M' \subset G$. Let M be the maximal K_{v_1}-split subtorus of N. It is easy to see that the $(L \otimes_K K_{v_1})$-linear span of $N(K_{v_1})$ is $R \otimes_K K_{v_1}$, which implies that C coincides with the connected centralizer of M. Therefore, H contains a root subgroup G_α corresponding to some root $\alpha \in \Phi(M', G)$. If $[L_{w_1} : K_{v_1}] = 1$, then G is K_{v_1}-isomorphic to SL_n; in particular, all roots have the same length, and the injectivity of the map

$$\kappa_\alpha : H^2(G(K_{v_1})) \to H^2(G_\alpha(K_{v_1})),$$

and consequently, the injectivity of η_{v_1} in (2_H) follows immediately from Theorem 1.2. If $[L_{w_1} : K_{v_1}] = 2$, the injectivity of κ_α is a consequence of Proposition 1.3.

So now let $G = \mathbf{SU}(\mathcal{A}, \tau)$, where $\dim_L \mathcal{A} = p^2$, p is a prime. If $p = 2$, then G is of type A_1, the case already considered in §3. Therefore, we assume that $p > 2$. It suffices to show that there exists a finite set W of places of K containing $S \cup T \cup V_\infty^K$, where, as before, T is the set of nonarchimedean places at which G is anisotropic, with the following property:

($\star$) *For any* $x \in M(S,G)$ *of prime order, and any* $v \notin W$, *we have* $\delta_v(x) = 0$, *where* $\delta_v : H^2(G(A(S))) \to H^2(G(K_v))$ *is induced by the imbedding* $G(K_v) \hookrightarrow G(A(S))$.

Indeed, since $M(S,G)$ is finite (Theorem 2.4), its trivialty is equivalent to the absence of nontrivial elements of prime order. As

$$H^2(G(A(S))) = H^2(G(W-S)) \times \prod_{v \notin W} H^2(G(K_v)),$$

assertion ($\star$) will imply that the set of elements of prime order in $M(S,G)$ is imbeddable into

$$\mathrm{Ker}(H^2(G(W-S)) \to H^2(G(K))) = \{0\}$$

(cf. Proposition 5.2), and we will have proved the theorem.

In a large part of our argument, v_0 will be assumed to satisfy the following additional condition:

($\star\star$) v_0 *either splits over* L *or is nonarchimedean.*

As before, let V_0 be the set consisting of $v \in V^K$, which is either archimedean, or is nonarchimedean and G is not quasi-split over K_v. Note that for nonarchimedean $v \in V_0$, we automatically have $L_v = K_v$. Indeed, if $v \in V_f^K$ and $[L_v : K_v] = 2$, then G is isomorphic over K_v to the special unitary group $\mathbf{SU}(h)$, where h is a hermitian form over L_v/K_v in p variables, which is K_v-quasi-split since p is odd. For any nonarchimedean $v \in V_0$, the group G is K_v-isomorphic to $\mathbf{SL}_{1,\Delta}$, where Δ is a division algebra of degree p over K_v; in particular, G is K_v-anisotropic.

We fix a finite set W of places of K which contains $S \cup T \cup V_0$, and all places ramified in L/K, and in case K is of characteristic zero, all dyadic places, and all those v's such that for some $w \mid v$, the extension $L_w/\mathbf{Q}_l$ is ramified, where l is the prime corresponding to v.

Next, fix an element $x \in M(S,G)$ of some prime order q, and let

$$1 \longrightarrow I \longrightarrow E \xrightarrow{\pi} G(A(S)) \longrightarrow 1 \tag{5}$$

be the corresponding extension. Also, fix $v_1 \notin W$ and pick a quadratic extension F/K, linearly disjoint from L over K, and having the following local properties:

$$\begin{array}{lll} F_{\bar{v}} = K_v & \text{for} & v \in V_0 \text{ and any } \bar{v} \mid v \\ L_{\bar{v}_i} = F_{v_i} & \text{for} & i = 0, 1, \text{ and any } \bar{v}_i \mid v_i. \end{array} \tag{6}$$

It follows from the above that if $v_i \in V_0$, then $i = 0$ and $v_0 \in V_\infty^K$. However, in this case, due to ($\star\star$), we have $L_{v_0} = K_{v_0}$, hence the conditions in (6) are not incompatible. Now, using Proposition A.7, we can construct a cyclic extension E/F of degree p such that E/K is a Galois extension with dihedral Galois group, and which has the following local properties:

$$\begin{array}{rll} E_{\bar{v}} = K_v & \text{for} & v \in V_\infty^K \cup \{v_0, v_1\} \text{ and any } \bar{v} \mid v \\ [E_v : F_v] = p & \text{for} & v \in V_0 \cap V_f^K, \end{array} \tag{7}$$

Let θ be an element of order 2 in $\mathrm{Gal}(E/K)$, $M = E^\theta$, and $P = ML$. Since E and L are linearly disjoint over K, for $R = PF = EL$ we have the following natural decomposition:

$$\mathrm{Gal}(R/K) = \mathrm{Gal}(E/K) \times \mathrm{Gal}(L/K). \tag{8}$$

We shall let τ denote the nontrivial element of $\mathrm{Gal}(L/K)$ and also the element $(\mathrm{id}_E, \tau) \in \mathrm{Gal}(R/K)$, as well as, its restriction to P.

Lemma 5.4 *(P, τ) is imbeddable into $(\mathcal{A}, \tau)$.*

It follows from the results in Appendix A that it is sufficient to establish the existence of local imbeddings

$$\epsilon_v : (P \otimes_K K_v, \tau) \hookrightarrow (\mathcal{A} \otimes_K K_v, \tau)$$

for $v \in V_0$. However, if $v \in V_\infty^K$ and G is not K_v-quasi-split, then $[L_v : K_v] = 2$. Since in this case $M \otimes_K K_v \simeq K_v^p$, the existence of ϵ_v follows from Proposition A.4. On the other hand, if $v \in V_0 \cap V_f^K$, then $L_v = K_v$, and the existence of ϵ_v follows from Proposition A.3 and the second condition in (7).

Clearly, the Galois closure of P over K is R. From (8) it is clear that the Galois group $\mathrm{Gal}(R/K)$ has the following presentation:

$$\mathrm{Gal}(R/K) = < \sigma, \theta, \tau \mid \sigma^p = \tau^2 = \theta^2 = [\sigma, \tau] = [\tau, \theta] = 1, \theta^{-1}\sigma\theta = \sigma^{-1} > .$$

Using this presentation we see that the following is a complete list of cyclic subgroups of $\mathrm{Gal}(R/K)$ up to conjugacy:

(i) $< \sigma\tau >$, order $= 2p$;

(ii) $< \sigma >$, order $= p$;

$(iii)_1$ $< \tau >$;

$(iii)_2$ $< \tau\theta >$;

$(iii)_3$ $< \theta >$;

(iv) $< e >$.

(Note that the subgroups in items $(iii)_j$ are all of order two.)

We will identify P with a τ-stable field contained in $\mathcal{A}$ in terms of an imbedding provided by Lemma 5.4. Let $B = R_{P/K}(\mathbf{GL}_1) \cap G$ be the corresponding maximal K-torus in G. The following lemma provides a rich supply of elements in $B(K)$.

Lemma 5.5 *For any $s \in R^\star$, the element $a = \tau\alpha/\alpha$, where $\alpha = N_{R/P}(\sigma s/s)$, belongs to $B(K)$.*

Indeed, a belongs to $\mathbf{U}(\mathcal{A}, \tau)$. On the other hand,

$$N_{P/L}(a) = \frac{\tau(N_{P/L}(\alpha))}{N_{P/L}(\alpha)} = \frac{\tau(N_{R/L}(\sigma s/s))}{N_{R/L}(\sigma s/s)} = 1.$$

Let $W_1 = W \cup V(R)$, where $V(R)$ is the set of nonarchimedian places in V^K which are ramified in R (clearly, $v_1 \notin W_1$). According to (1.7), there exists an open neighborhood of the identity U in $G(W_1 - S) = \prod_{v \in W_1 - S} G(K_v)$, such that for any two commuting elements $a, b \in U$, the elements $\tilde{a} \in \pi^{-1}(a)$, $\tilde{b} \in \pi^{-1}(b)$ also commute. The proof of Theorem 5.1, just as the proof of Theorem 4.1, uses the formula for the commutator $[\tilde{a}, \tilde{b}]$ of lifts $\tilde{a} \in \pi^{-1}(a)$, $\tilde{b} \in \pi^{-1}(b)$ of elements $a, b \in B(K) \cap U$ (in fact, we will only deal with elements of the form described in Lemma 5.5). By (1.9) it is enough to calculate the local commutators $[\tilde{a}_v, \tilde{b}_v]$, where a_v, b_v denote the images a, b under the imbedding $G(K) \hookrightarrow G(K_v)$, $\tilde{a}_v \in \pi^{-1}(a_v)$, $\tilde{b}_v \in \pi^{-1}(b_v)$. By our construction, any $v \notin W_1$ is unramified in the extension R/K, and therefore the corresponding local Galois group is cyclic. Fix an extension $u \mid v$ such that $\mathrm{Gal}(R_u/K_v)$ is one of the groups in the above list. We should distinguish between two cases when it belongs, respectively, to types (i) and (ii), or to the remaining types.

We claim that in the first case, $[\tilde{a}_v, \tilde{b}_v] = 1$. Indeed, it suffices to show that the restriction map

$$H^2(G(K_v)) \longrightarrow H^2(B(K_v))$$

is trivial. According to Theorem 1.1, $H^2(G(K_v))$ is a cyclic group of order $\mu_v = \#\mu(K_v)$. On the other hand, P_u/L_w is extension of degree p, and therefore, $B(K_v) = F \times Q$, where F is a cyclic group of order prime to l, the characteristic of the residue field of K_v, and Q is a certain pro-l group, so $H^2(B(K_v))$ is an l-group. Since by our construction μ_v is prime to l (if K is of positive characteristic, this is immediate, and if K is of characteristic zero it is a consequence of our assumption that the extension $P_u/\mathbf{Q}_l$ is unramified and $l \neq 2$), our assertion follows.

Next, we take up the second case. If $\mathrm{Gal}(R_u/K_v)$ belongs to $(iii)_3$ or (iv), then $[L_w : K_v] = 1$, and G is K_v-isomorphic to $\mathbf{SL}_p$. Moreover, B is conjugate to the diagonal torus in $\mathbf{SL}_p$, so for computation of the commutator we can use the formula given in Proposition 1.5. To handle the case $[L_w : K_v] = 2$, observe that since $\#\mu(K_v)$ is prime to l, surjectivity of the norm map on the residue fields implies that

$$N_{L_w/K_v}(\mu(L_w)) = \mu(K_v),$$

so we may use the following:

Lemma 5.6 *Let g be a nondegenerate hermitian form on L_w^d, $d \geq 3$, defined in terms of the nontrivial element of* $\mathrm{Gal}(L_w/K_v)$ *and $G = \mathbf{SU}(g)$ be naturally imbedded into $F = R_{L_w/K_v}(\mathbf{SL}_d)$. Assume that* *(i)* L_w/K_v *is unramified;*

(ii) $N_{L_w/K_v}(\mu(L_w)) = \mu(K_v)$.

Then
($\bullet$) $H^2(G(K_v))$ *has order equal to* μ_v *and the restriction map*

$$\phi_v : H^2(F(K_v)) \to H^2(G(K_v))$$

is surjective.
($\bullet\bullet$) *For* $x \in H^2(F(K_v)) = H^2(SL_d(L_w))$*, corresponding to* $\lambda \in \hat{\mu}(L_w)$*,* $\phi_v(x) = 0$ *if, and only if,* λ *restricts trivially to* $\mu(K_v) \subset \mu(L_w)$*, or, equivalently, the character*

$$\lambda \circ N_{L_w/K_v} \in \hat{\mu}(L_w)$$

is trivial.

Proof. In terms of a suitable basis of L_w^d, g is given by equation (1) in the proof of Lemma 5.3; let C be the maximal torus described by equation (2) in the proof of the same lemma. Since $H^2(G(K_v))$ is a cyclic group of order dividing $\mu_v = \#\mu(K_v)$ (cf. [PrRa1], Theorem 9.4), it suffices to show that the image of the composite map

$$H^2(F(K_v)) \longrightarrow H^2(G(K_v)) \longrightarrow H^2(C(K_v))$$

contains an element of order μ_v. Let $x \in H^2(F(K_v)) = H^2(SL_d(L_w))$ be an element corresponding to a character $\lambda \in \hat{\mu}(L_w)$ of order $\#\mu(L_w)$, and let

$$1 \longrightarrow I \longrightarrow E \xrightarrow{\pi} F(K_v) \longrightarrow 1$$

be the corresponding extension. To show that x restricts to an element of order μ_v in $H^2(C(K_v))$, it is enough to find $a, b \in C(K_v)$ such that for some $\tilde{a} \in \pi^{-1}(a)$, $\tilde{b} \in \pi^{-1}(b)$, the commutator $[\tilde{a}, \tilde{b}]$ has order μ_v. Take

$$a = (\alpha, (\alpha^\tau)^{-1}, \alpha^{-1}\alpha^\tau, 1, \ldots, 1),$$

$$b = (\beta, (\beta^\tau)^{-1}, \beta^{-1}\beta^\tau, 1, \ldots, 1),$$

$\alpha, \beta \in L_w^\star$. Then by Proposition 1.5, we have

$$[\tilde{a}, \tilde{b}] = \lambda((\alpha,\beta)_w \cdot ((\alpha^\tau)^{-1}, (\beta^\tau)^{-1})_w \cdot (\alpha^{-1}\alpha^\tau, \beta^{-1}\beta^\tau)_w) = \lambda(N_{L_w/K_v}((\alpha, \beta^2/\beta^\tau)_w)), \quad (9)$$

where $(\star,\star)_w$ is the norm residue symbol on L_w of power $\#\mu(L_w)$. Take for β a prime element in K_v. Since L_w/K_v is unramified, $\beta = \beta^2/\beta^\tau$ remains prime in L_w, and therefore there exists $\alpha \in L_w^\star$ such that $(\alpha,\beta)_w$ is a generator of $\mu(L_w)$. Then in view of (9) and condition (ii), the elements a, b are as required, this proves ($\bullet$). Since $H^2(F(K_v))$ is cyclic of order $\mu_w = \#\mu(L_w)$, assertion ($\bullet\bullet$) is a consequence of the fact that Ker ϕ_v and the subgroup $\Sigma \subset \hat{\mu}(L_w)$ of elements vanishing on $\mu(K_v)$ have the same order, equal to μ_w/μ_v. Finally, by virtue of (ii), $\lambda \in \hat{\mu}(L_w)$ falls into Σ if and only if the composition $\lambda \circ N_{L_w/K_v}$ is a trivial character of $\mu(L_w)$. Lemma 5.6 is proved.

It follows from Lemma 5.6, and the discussion preceding it, that for any $v \notin W$, there exists $\lambda_v \in \hat{\mu}(L_w)$ $(w \mid v)$ such that $x_v = \delta_v(x)$ is obtained as restriction of the cocycle in $H^2(SL_p(L_w))$ corresponding to λ_v. Put

$$\chi_v = \begin{cases} \lambda_v & \text{if } [L_w : K_v] = 1, \\ \lambda_v \circ N_{L_w/K_v} & \text{if } [L_w : K_v] = 2. \end{cases}$$

We shall prove that $\chi_{v_1} = 1$. For this, we will need the expression for the local commutator in terms of χ_v when $\mathrm{Gal}(R_u/K_v)$ belongs to one of the cases $(iii)_j$ or (iv). First, suppose that we are not in the case $(iii)_3$. Then $R_u = L_w$, and therefore B is diagonalizable over L_w, i.e. $gBg^{-1} \subset D_p$ for some $g \in GL_p(L_w)$. Moreover, if

$$a^v = g^{-1}\mathrm{diag}(a_1, \ldots, a_p)g, \; b^v = g^{-1}\mathrm{diag}(b_1, \ldots, b_p)g,$$

then

$$[\tilde{a}^v, \tilde{b}^v] = \chi_v(\prod_{i=1}^{p}(a_i, b_i)_w). \tag{10}$$

Note that for $a, b \in B(K)$, the product in (10) is equal to

$$\Pi_v(a, b) = \prod_{i=0}^{p-1}(\sigma^i(a), \sigma^i(b))_u;$$

where $(\star, \star)_u$ is the norm residue symbol on R_u of power $\#\mu(L_w)$. Let us calculate $\Pi_v(a, b)$ for elements a, b of the form described in Lemma 5.5; let

$$a = \tau\alpha/\alpha, \qquad b = \tau\beta/\beta, \tag{11}$$

where $\alpha = N_{R/P}(\sigma s/s)$, $\beta = N_{R/P}(\sigma t/t)$ for some $s, t \in R^\star$. Observing that $b = c \cdot \theta(c)$, where

$$c = \frac{\tau\sigma(t) \cdot t}{\tau(t) \cdot \sigma(t)},$$

and that $\theta(a) = a$, we see that

$$(\sigma^i(a), \sigma^i(b))_u = (\sigma^i(a), \sigma^i(c))_u \cdot ((\sigma^i\theta)(a), (\sigma^i\theta)(c))_u$$

Furthermore, using the formula for c and the fact that $\tau(a) = a^{-1}$, we obtain

$$
\begin{aligned}
&\prod_{i=0}^{p-1}(\sigma^i(a),\sigma^i(c))_u\\
&=\prod_{i=0}^{p-1}(\sigma^i(a),\sigma^{i+1}\tau(t))_u\cdot\prod_{i=0}^{p-1}(\sigma^i(a),\sigma^i(t))_u\cdot\prod_{i=0}^{p-1}(\sigma^i(a),\sigma^i\tau(t))_u^{-1}\cdot\prod_{i=0}^{p-1}(\sigma^i(a),\sigma^{i+1}(t))_u^{-1}\\
&=\prod_{i=0}^{p-1}(\sigma^i(\frac{a}{\sigma^{-1}(a)}),\sigma^i(t))_u\cdot\prod_{i=0}^{p-1}(\sigma^i(\frac{a}{\sigma^{-1}(a)}),\sigma^i\tau(t))_u^{-1}\\
&=\prod_{i=0}^{p-1}(\sigma^i(\frac{a}{\sigma^{-1}(a)}),\sigma^i(t))_u\cdot\prod_{i=0}^{p-1}(\sigma^i\tau(\frac{a}{\sigma^{-1}(a)}),\sigma^i\tau)(t)_u. \qquad (12)
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
\prod_{i=0}^{p-1}(\sigma^i\theta(a),\sigma^i\theta(c))_u &= \prod_{i=0}^{p-1}(\theta\sigma^i(a),\theta\sigma^i(c))_u\\
&=\prod_{i=0}^{p-1}(\theta\sigma^i(\frac{a}{\sigma^{-1}(a)}),\theta\sigma^i(t))_u\cdot\prod_{i=0}^{p-1}(\theta\sigma^i\tau(\frac{a}{\sigma^{-1}(a)}),\theta\sigma^i\tau(t))_u. \qquad (13)
\end{aligned}
$$

Combining (12) and (13), we get

$$
\Pi_v(a,b)=\prod_{\omega}(\omega(\frac{a}{\sigma^{-1}(a)}),\omega(t))_u, \qquad (14)
$$

where ω runs through $\mathrm{Gal}(R/K)$.

The case $(iii)_3$ (i.e. where $\mathrm{Gal}(R_u/K_v)$ is generated by θ) is different from others, for here the torus B does not split over L_w. To be more precise, in this case

$$
P\otimes_L L_w = L_w\oplus R_u^m, \qquad (15)
$$

where $m=(p-1)/2$. (Indeed, one easily checks that all extensions u_i of w to P are obtained as restrictions of the following places of R: $\bar{u}\circ\sigma^i$, $i=0,\ldots,m$. Besides, by our construction P is fixed by θ, so $P_{u_o}=L_w$. On the other hand, neither of $\sigma^i(P)$, $i=1,\ldots,m$, is fixed by θ, implying that $P_{u_i}=P_u$, hence (15).) In terms of decomposition (15), an element $a\in C(K_v)$ has components $a,\sigma^1(a),\ldots,\sigma^m(a)$. So it follows from Proposition 1.5 that

$$
[\tilde{a}^v,\tilde{b}^v]=\lambda_v(\Pi_v(a,b)),\ \text{where } \Pi_v(a,b)=(a,b)_{u_0}\cdot\prod_{i=1}^{m}(\sigma^i(a),\sigma^i(b))_u. \qquad (16)
$$

Now, assume again that a,b are of the form (11). Then it follows from the properties of the norm residue symbol (cf. [S2], p. 209) that $(a,b)_{u_0}=(a,c)_u$. Besides, for any i

we have $(\sigma^i(a), \sigma^i(\theta(c)))_u = (\sigma^{-i}(a), \sigma^{-i}(c))_u$. Taking all this into account and arguing as above, we obtain that

$$\Pi_v(a,b) = \prod_{i=0}^{p-1} (\sigma^i(\frac{a}{\sigma^{-1}a}), \sigma^i(t))_u \cdot \prod_{i=0}^{p-1} (\sigma^i \tau(\frac{a}{\sigma^{-1}a}), \sigma^i \tau(t))_u. \tag{17}$$

In spite of the apparent differences in formulas (14) and (17), they allow us to obtain the following uniform formula for local commutators: if $v \notin W$, there exist characters $\chi_{\bar{v}} \in \hat{\mu}(L_w)$, one for each extension $\bar{v} \mid v$, of order equal to the order of χ_v, such that

$$[\tilde{a}^v, \tilde{b}^v] = \prod_{\bar{v}|v} \chi_{\bar{v}}((\frac{a}{\sigma^{-1}(a)}\ ,\ t)_{\bar{v}}); \tag{18}$$

where $(\star, \star)_{\bar{v}}$ is the norm residue symbol on $R_{\bar{v}}$ of power $\#\mu(L_w)$. On the other hand, since the central extension (5) splits over $G(K)$, $[\tilde{a}, \tilde{b}] = 1$, which in view of (18) leads to the relation

$$\prod_{v \in V_1} \prod_{\bar{v}|v} \chi_{\bar{v}}((\frac{a}{\sigma^{-1}(a)}\ ,\ t)_{\bar{v}}) = 1, \tag{19}$$

which holds for all $t \in R^\star$, and $a = a(s) (s \in R^\star)$ constructed in Lemma 5.5 so that a and $b := b(t)$ belong to the open subset U chosen above; V_1 above consists of places $v \notin W$ such that for some extension $u \mid v$, the Galois group $\mathrm{Gal}(R_u/K_v)$ is one of the groups in items $(iii)_j$ or (iv) of the above list. Taking $\chi_{\bar{v}} = 1$ for $\bar{v} \mid v$, $v \notin V_1$, we can rewrite (19) in the form of a reciprocity law:

$$\prod_{\bar{v} \in V^P} \chi_{\bar{v}}((\frac{a}{\sigma^{-1}(a)}, t)_{\bar{v}}) = 1.$$

By our assumption, $x \in M(S, G)$ was taken to be of prime order q, so for all $\bar{v}$ we have $\chi_{\bar{v}}^q = 1$. Now, to apply Proposition B.1 we need the following:

Lemma 5.7 *For $s \in R^\star$, let $a = a(s)$ be the element constructed in Lemma 5.5, $v \in V^K$, u be its extension to R as above.*

(i) If $v \in V_f^K$ and $Gal(R_u/K_v)$ belongs to one of the types $(iii)_2$ or (iv), then there exists a $s \in R^\star$ such that for the corresponding element a we have $u(a/\sigma^{-1}(a)) = 1$.

(ii) If v is real and $R_u = K_v$, then there exists a $s \in R^\star$ such that $a(s)$ is negative in the completion $R_u = \mathbf{R}$.

(iii) For $\bar{s} \in R^\star$, if $\bar{a} = a(\bar{s})$, then taking $\bar{s}$ sufficiently close to s with respect to all places $u \circ \omega$, $\omega \in Gal(R/K)$, we can make $\bar{a}/\sigma^{-1}(\bar{a})$ as close to $a/\sigma^{-1}(a)$, with respect to u, as we desire.

Proof. (i) is obtained by direct computations. We have

$$\frac{a}{\sigma^{-1}(a)} = \frac{\tau(\alpha)/\alpha}{\sigma^{-1}(\tau(\alpha)/\alpha)} = \frac{\tau(\alpha) \cdot \sigma^{-1}(\alpha)}{\alpha \cdot (\tau\sigma^{-1})(\alpha)}$$

$$= \frac{\tau((\sigma s/s)\cdot\theta(\sigma s/s))\cdot\sigma^{-1}((\sigma s/s)\cdot\theta(\sigma s/s))}{(\sigma s/s)\cdot\theta(\sigma s/s)\cdot\tau\sigma^{-1}((\sigma s/s)\cdot\theta(\sigma s/s))}$$

$$= \frac{s^2\cdot\tau\theta\sigma(s)^2\cdot\tau\sigma(s)\cdot\theta\sigma^2(s)\cdot\theta(s)\cdot\tau\sigma^{-1}(s)}{\tau(s)^2\cdot\theta\sigma(s)^2\cdot\sigma(s)\cdot\tau\theta\sigma^2(s)\cdot\tau\theta(s)\cdot\sigma^{-1}(s)}.$$

It follows that if $\mathrm{Gal}(R_u/K_v)$ is generated by $\tau\theta$, then

$$u(\frac{a}{\sigma^{-1}(a)}) = u(s) + (u\circ\sigma)(s) + (u\circ\tau\sigma^2)(s) + (u\circ\tau\sigma^{-1})(s)$$

$$-(u\circ\tau)(s) - (u\circ\sigma^2)(s) - (u\circ\sigma^{-1})(s) - (u\circ\tau\sigma)(s).$$

Now, since the order of σ is > 2, all places $u\circ\omega$,

$$\omega\in\Omega = \{\sigma,\sigma^{-1},\sigma^2,\tau,\tau\sigma,\tau\sigma^{-1},\tau\sigma^2\},$$

are different from u, and therefore by weak approximation, there exists $s\in R^\star$ such that

$$u(s) = 1 \text{ and } (u\circ\omega)(s) = 0 \text{ for } \omega\in\Omega.$$

From the above computations it follows that this element satisfies (i). Next, let $\mathrm{Gal}(R_u/K_v)$ be trivial. Then

$$u(\frac{a}{\sigma^{-1}(a)}) = 2(u(s) + (u\circ\tau\theta\sigma)(s) - (u\circ\tau)(s) - (u\circ\theta\sigma)(s)) + (u\circ\tau\sigma)(s)$$

$$+(u\circ\theta\sigma^2)(s) + (u\circ\theta)(s) + (u\circ\tau\sigma^{-1})(s) - (u\circ\sigma)(s) - (u\circ\tau\theta\sigma^2)(s)$$

$$-(u\circ\tau\theta)(s) - (u\circ\sigma^{-1})(s). \tag{20}$$

Let

$$\Omega_1 = \{e,\tau,\theta\sigma,\tau\theta\sigma\},\ \Omega_2 = \{\sigma,\sigma^{-1},\tau\sigma,\tau\sigma^{-1},\theta,\tau\theta,\theta\sigma^2,\tau\theta\sigma^2\}.$$

Then Ω_1 and Ω_2 are disjoint, and all the elements listed above in these sets are distinct. So by weak approximation one can find $s\in R^\star$ such that

$$(u\circ\theta)(s) = 1 \text{ and } (u\circ\omega)(s) = 0 \text{ for } \omega\in\Omega_1\cup\Omega_2 - \{\theta\}.$$

Again, it easily follows from the above formula that this s satisfies our requirements, proving (i). An obvious multiplicative analog of (20) shows that in the set-up of (ii), it suffices to pick $s\in R^\star$ which is negative in $R_u\circ\theta$ and positive in all $R_{u\circ\omega}$, $\omega\in\Omega_1\cup\Omega_2-\{\theta\}$. Assertion (iii) is obvious. Lemma 5.7 is proved.

We now first take up the case where v_0 is nonarchimedean. Since $\chi_{\bar v_0} = 1$ for $\bar v_0 \mid v_0$, to prove that $\chi_{\bar v_1} = 1$ it is enough to find $s\in R^\star$ such that the corresponding $a = a(s)$ belongs to U, and the condition

$$\bar v(\frac{a}{\sigma^{-1}(a)}) = 1 \tag{21}$$

is satisfied for $\bar{v} = \bar{v}_0, \bar{v}_1$ (some fixed extensions of v_0, v_1). However, the existence of such s immediately follows from Lemma 5.7 (i) and (ii), since by our construction, $\mathrm{Gal}(R_{\bar{v}_i}/K_{v_i})$ for $i = 0, 1$, is either trivial or is generated by $\tau\theta$.

Next, let v_0 be real. Once we have considered the case of v_0 nonarchimedean, then by (1.9) the order of $M(S, G)$ cannot exceed 2 since the existence of *a real* $v_0 \in V^K$ implies that $\mu(K) = \{\pm 1\}$). So, q can only be equal to 2. To apply the above argument using Proposition B.1, we need to show that there exits an $s \in R^\star$ such that for $a = a(s)$, $a/\sigma^{-1}(a) < 0$ in $R_{\bar{v}_0} = \mathbf{R}$ and $a/\sigma^{-1}(a)$ satisfies (21) for $\bar{v} = \bar{v}_1$. Again, this immediately follows from Lemma 5.7, since by our construction $\mathrm{Gal}(R_{\bar{v}_0}/K_{v_0})$ is trivial.

We will now drop the assumption $(\star\star)$, i.e. we will prove the triviality of $M_V(G)$ also where v_0 is real, $[L_{w_0} : K_{v_0}] = 2$, $w_0 \mid v_0$, and G is K_{v_0}-isotropic. Without loss of generality, we may assume that S does not contain any nonarchimedean places where G is anisotropic (i.e. in our previous notation, $S \cap T = \emptyset$), and therefore

$$H^2(G(A)) = H^2(G(S)) \times H^2(G(A(S))). \tag{22}$$

Suppose there is a nontrivial element $c \in M(S, G)$. Then the element $c' = (1_S, c)$ (defined in terms of (22)) is a nontrivial element of $M(\emptyset, G)$. Again, as above, it follows from (1.13) that $M(\emptyset, G)$ is of order at most two. To derive a contradiction, we will show that the order of $M(\emptyset, G)$ is exactly two, and its nontrivial element restricts to a nontrivial element in $H^2(G(K_{v_0}))$. For this, consider $\mathcal{A}$ as a vector space over K, and introduce on it the following quadratic form:

$$f(x, y) = \mathrm{Trd}_{\mathcal{A}/L}(x\tau(y)).$$

Then G acts on $\mathcal{A}$ by left translations: $a \mapsto ga$, $(a \in \mathcal{A},\ g \in G)$.This action obviously preserves f, so we have an imbedding $G \hookrightarrow \mathbf{SO}(f)$. Since G is simply connected, this imbedding lifts to an imbedding $G \hookrightarrow \mathbf{Spin}(f) = H$. The property that we need in our argument of this imbedding is the following:

Lemma 5.8 *The restriction map* $\rho : H^2(H(K_{v_0})) \to H^2(G(K_{v_0}))$ *is injective on the set of elements of order 2.*

Proof. We begin with the following simple observation. Let $Y = \mathbf{C}^n$, h be the nondegenerate hermitian form on Y defined as follows:

$$h(z_1, \ldots, z_n) = a_1 N(z_1) + \ldots + a_n N(z_n),$$

where $a_i \in \mathbf{R}$, and for $z = x + iy$, $N(z) = x^2 + y^2$ is the norm of z. Let

$$\varphi(x_1, y_1, \ldots, x_n, y_n) = a_1(x_1^2 + y_1^2) + \ldots + a_n(x_n^2 + y_n^2)$$

be the corresponding quadratic form on Y, regarded as vector space over $\mathbf{R}$. Then $\mathbf{SU}(h) \subset \mathbf{SO}(\varphi)$, and by the simply connectedness of $\mathbf{SU}(h)$ we obtain an imbedding

$$G' = \mathbf{SU}(h) \hookrightarrow \mathbf{Spin}(\varphi) = H'.$$

If $n > 2$ (which is the case in our set up), then the restriction map $H^2(H'(\mathbf{R})) \to H^2(G'(\mathbf{R}))$ is injective. Indeed, it suffices to show that the map of the fundamental groups $\pi_1(G'(\mathbf{R})) \to \pi_1(H'(\mathbf{R}))$ is surjective. We may assume that not all the a_i's are of the same sign (otherwise, both the fundamental groups are trivial); let $a_1, \ldots, a_l$ be positive, and $a_{l+1}, \ldots, a_n$ be negative. Then one easily verifies that the map $\pi_1(Z) \to \pi_1(H'(\mathbf{R}))$, where $Z = \{\mathrm{diag}(z, 1, \ldots, 1, z^{-1}) \mid z \in \mathbf{C}, N(z) = 1\}$, is already surjective.

Now, identify $\mathcal{A} \otimes_K K_{v_0}$ with $M_p(\mathbf{C})$ in such a way that τ has the form

$$\tau((x_{ij})) = F(\bar{x}_{ji})F^{-1}$$

where $F = \mathrm{diag}(a_1, \ldots, a_p)$, $a_i \in \mathbf{R}$, and the bar denotes complex conjugation. Then G can be identified with $\mathbf{SU}(h)$ where h is as above (with n replaced by p), and $M_p(\mathbf{C})$ as a G-module is isomorphic to Y^p, $Y = \mathbf{C}^p$ with standard action of G on Y. Let φ be the quadratic form on Y as above, $H' = \mathbf{Spin}(\varphi)$. As we noted above, the restriction map $\rho_0 : H^2(H'(\mathbf{R})) \to H^2(G(\mathbf{R}))$ is injective. Obviously, f coincides with the orthogonal sum of p copies of φ, and there are two imbeddings of H' into $H = \mathbf{Spin}(f)$: the first is given by the diagonal action of H' on $Y^p = M_p(\mathbf{C})$, and the second is given by the action only on the first component. Let ρ_1, ρ_2 be the corresponding restriction maps from $H^2(H(\mathbf{R}))$ to $H^2(H'(\mathbf{R}))$. Then $\rho_1 = \mathbf{p} \cdot \rho_2$ where $\mathbf{p}$ stands for multiplication by p. It follows from simple topological considerations that ρ_2 is injective. Since p is odd, we conclude that ρ_1 is injective on the set of elements of order 2. Hence $\rho = \rho_0 \circ \rho_1$ is also injective on this set, and the lemma has been proved.

5.9. Let $g = f \perp (-f)$ and $C = \mathbf{Spin}(g)$, then the restriction map $H^2(C(K_{v_0})) \to H^2(H(K_{v_0}))$ is injective. Since g is a hyperbolic form, C is K-split, and therefore according to [Ma], there exists an element $y \in M(\emptyset, C)$ of order two. It is a consequence of the fact that $M(\{v_0\}, C)$ is trivial that y projects onto a nontrivial element of $H^2(C(K_{v_0}))$. Then combining Lemma 5.8 with the injectivity result mentioned above, we conclude that y restricts to an element of order two in $M(\emptyset, G)$, with nontrivial projection to $H^2(G(K_{v_0}))$, as required.

To complete the proof of Theorem 5.1, it only remains to show that $M(\emptyset, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$ of index at most two, where $G = \mathbf{SU}(\mathcal{A}, \tau)$, $\mathcal{A}$ a central simple algebra of degree n (n arbitrary now) over L, with involution τ. The argument here is analogous to the proof of Proposition 4.7. Let p be a prime divisor of $\mu = \#\mu(K)$ (then, of course, p is different from the characteristic of K), p^α be the maximal power of p dividing μ, so that $\mu = p^\alpha \cdot m$ and the g.c.d. $(p, m) = 1$. We need to show that $M(\emptyset, G)$ contains an element of order p^α (resp. $p^{\alpha - 1}$) if $p \neq 2$ (resp. $p = 2$). Obviously, G admits a splitting field P of degree $2n$ over K, so if p is prime to $2n$, $N_{P/K}(\mu(P))$ contains an element of order p^α; this, in view of Lemma 4.8, implies that an element of this order exists also in $M(\emptyset, G)$.

Now, assume that p is an odd prime divisor of n. Then G has a splitting field of the form $P = F(\zeta_{p^\beta})$, where F is an extension of L of degree m, ζ_{p^β} is a primitive p^β-th root of unity and β is sufficiently large. It follows from Lemma 4.9, and the argument follwing it, that $N_{P/K}(\mu(P))$ contains an element of order p^α, and again by Lemma 4.8, the same is true for $M(\emptyset, G)$. It remains to consider the case $p = 2$. If $\alpha = 1$, then there is nothing to prove. Otherwise, it follows from Lemma 4.9 that by picking a splitting field P of the form $P = F(\zeta_{2^\beta})$, where F/L is a suitable extension of odd degree, we can ensure that $N_{P/L}(\mu(P))$ contains an element of order 2^α. Then $N_{P/K}(\mu(P))$ will contain an element of order at least $2^{\alpha-1}$, completing the proof.

Also, observe that the argument given in 4.10 can be used to show that if S contains a nonarchimedean place v_0 at which G is anisotropic, and p is the characteristic of the residue field of K_{v_0}, then in case $p \neq 2$, $M(S, G)$ has no p-torsion.

6 Groups of other classical types

The previous three sections, which contain the computation of the metaplectic kernel for the groups of type A, actually constitute the most difficult part of the proof of the main theorem. In this and the next section we will complete the proof for groups of all other types via a certain reduction process to the groups of type A. This reduction is based on the following simple observation:

Lemma 6.1 *Let G be an absolutely simple, simply connected K-group, and S a finite set of places of K. Assume that $M_V(G) = \mathrm{Ker}(H^2(G(V)) \to H^2(G(K)))$ is trivial for any finite set V of places of K, and that for almost every $v \notin S$ (i.e. with possibly finitely many exceptions), there exists a K-subgroup H of G such that: (a) $M(S, H)$ is trivial, and (b) the restriction map $\eta_v \colon H^2(G(K_v)) \to H^2(H(K_v))$ is injective. Then $M(S, G)$ is trivial.*

Proof. Let V_0 be a finite set of places of K containing $S \cup T \cup V_\infty^K$, and also all those $v \notin S$ for which a subgroup H of G with the two properties described in the lemma does not exist. We have

$$H^2(G(A(S))) = H^2(G(V_0 - S)) \times \prod_{v \notin V_0} H^2(G(K_v)),$$

so any x in $M(S, G)$ can be written in the form $x = (x_{V_0 - S}, (x_v)_{v \notin V_0})$. Fix a $v \notin V_0$, and consider the corresponding subgroup H of G given by the lemma. From the commutative diagram

$$\begin{array}{ccc} M(S,G) & \longrightarrow & M(S,H) \\ \downarrow & & \downarrow \\ H^2(G(K_v)) & \xrightarrow{\eta_v} & H^2(H(K_v)), \end{array}$$

using the triviality of $M(S, H)$ and the injectivity of η_v, we conclude that $x_v = 0$. This implies that $x_{V_0 - S}$ is contained in $M_{V_0 - S}(G)$, which is trivial by our assumption, so the lemma is proved.

This section is devoted to groups of classical types; these are treated using their geometric realizations. It is a well known consequence of Harder's theorem on the vanishing of the Galois cohomology of simply connected, semi-simple groups over global function fields that over such a field any absolutely simple group of type other than A is isotropic ([Ha]). Since for the isotropic groups, the metaplectic kernel has already been computed in [PrRa1], *we shall assume in this and the next section that K is of characteristic zero, i.e. it is a number field.* We note that most of our arguments work without any restriction on the characteristic of K; however, at a few places it is convenient to assume that the characteristic is not 2.

We will assume that S contains a place v_0, which is either nonarchimedean, or is real and the group $G(K_{v_0})$ is not (topologically) simply connected and, using Lemma 6.1, prove that $M(S,G)$ is trivial. We will also separately prove that $M(\emptyset,G)$ is a subgroup of $\hat{\mu}(K)$ of index at most 2. In view of the reduction described in 1.13, this will prove the main theorem for all groups of classical types.

First, we consider the group $G = \mathbf{Spin}(f)$, where f is a nondegenerate quadratic form over K in $r \geq 5$ variables (then G is of type D, if r is even, and of type B, if r is odd). For technical reasons, in case $r = 5$, it is convenient to use the identification $B_2 = C_2$ and to consider this case as pertaining to the series C. On the other hand, in view of the identification $D_3 = A_3$, the case $r = 6$ has actually already been considered. If v_0 is real, then the condition that $G(K_{v_0})$ is not (topologically) simply connected is equivalent to the condition that the Witt index of f over K_{v_0} is ≥ 2.

Lemma 6.2 *Let f be a nondegenerate quadratic form over K and V a finite set of places of K. Assume that for every v in V, the Witt index of f over K_v is $\geq d$, where d is a positive integer. Then there exists a subform g of f in $2d$ variables with Witt index d over every completion K_v, $v \in V$.*

PROOF. An obvious inductive argument shows that it suffices to consider the case $d = 1$, i.e. to show that if f is K_v-isotropic for every $v \in V$, then there exists a binary subform g of f with the same property. The subspace over K_v generated by a pair of vectors a_v, b_v is the hyperbolic plane if, and only if,

$$(a_v \mid b_v)^2 - f(a_v)f(b_v) \in K_v^{*2},$$

where $(\ \mid\ )$ denotes the bilinear form associated with f. Clearly, if this condition holds for a certain pair a_v, b_v, it holds for any other pair which is sufficiently close to this one. So, for every $v \in V$, picking a pair a_v, b_v over K_v, which spans a hyperbolic plane, we can use the weak approximation property to find a pair a, b over K such that the subspace generated by this pair is isotropic over K_v, for all v in V. This proves the lemma.

Now, pick an arbitrary $v_1 \notin S \cup V_\infty^K$. Since $r \geq 7$, for any nonarchimedean v, the Witt index of f over K_v is ≥ 2. We have observed above that if v_0 is real, the

Witt index of f over K_{v_0} is also ≥ 2. Now, according to Lemma 6.2, there exists a 4-dimensional subform g of f with Witt index 2 over K_{v_i}, $i = 0, 1$. We claim that the subgroup $H = \mathbf{Spin}(g)$ of G has properties (a) and (b) of Lemma 6.1. Indeed, as is well known, H is isomorphic over K either to the direct product $H_1 \times H_2$ of two groups of type A_1, or to a group of the form $R_{L/K}(\mathcal{H})$, where L/K is a quadratic extension, and $\mathcal{H}$ is a group of type A_1 defined over L. Since the rank of H over K_{v_0} is 2, in the first case both the H_i's are K_{v_0}-isotropic, while in the second case v_0 splits over L, and $\mathcal{H}$ is isotropic at both the extensions of v_0. In either case, Theorem 3.1 implies that $M(S, H)$ is trivial (note that if $H = R_{L/K}(\mathcal{H})$, then $M(S, H) = M(\mathcal{S}, \mathcal{H})$, where $\mathcal{S}$ consists of all extensions of places from S to L). On the other hand, the injectivity of the restriction map $H^2(G(K_{v_1})) \to H^2(H(K_{v_1}))$ follows from Proposition 1.9 of [PrRa1] since the Witt index of g over K_{v_1} is ≥ 2.

A minor modification of the above argument allows us to establish the triviality of $M_V(G)$ as well. Let V_1 be the set of all $v \in V$ such that the Witt index of f over K_v is ≤ 1. Obviously, any v in V_1 is real, and the group $G(K_v)$ is topologically simply connected, implying that $H^2(G(K_v))$ is trivial. Let V_2 be the union of V_1 and the set of all complex v in V, and $V_0 = V - V_2$. Since G is isotropic at all nonarchimedean places, we have

$$H^2(G(V)) = \prod_{v \in V} H^2(G(K_v)) = \prod_{v \in V_0} H^2(G(K_v)).$$

Let g be a 4-dimensional subform of f with local Witt index 2 at every v in V_0. Using Proposition 1.9 of [PrRa1] if v is nonarchimedean, and a simple topological argument if v is real, we conclude that $H^2(G(K_v)) \to H^2(H(K_v))$ is injective for any $v \in V_0$. Therefore, the restriction map $H^2(G(V)) \to H^2(H(V))$ is injective. On the other hand, from the above description of the structure of H it is plain that Proposition 3.2 applies to give the triviality of $M_V(H)$. Combining these facts, we obtain the triviality of $M_V(G)$. Now Lemma 6.1 implies that $M(S, G)$ is trivial.

Finally, to prove that for $G = \mathbf{Spin}(f)$, $M(\emptyset, G)$ is isomorphic to $\hat{\mu}(K)$, we argue as at the end of §4. We let $h = f \perp (-f)$ and $\mathcal{G} = \mathbf{Spin}(h)$. Since h is split over K, by a theorem of Matsumoto [Ma], there exists an element x in $M(\emptyset, \mathcal{G})$ of order $\mu = \#\mu(K)$. Moreover, it is a consequence of Matsumoto's construction that for every place v, the order of the projection x_v of x on $H^2(\mathcal{G}(K_v))$ is equal to μ. As for any nonarchimedean v, the Witt index of f over K_v is ≥ 2, under the restriction map $H^2(\mathcal{G}(K_v)) \to H^2(G(K_v))$, x_v maps onto an element y_v of order μ (cf. Proposition 1.9 of [PrRa1]). On the other hand, one can think of y_v as the projection on $H^2(G(K_v))$ of the element $y \in M(\emptyset, G)$, obtained from x by restriction. It follows that the order of y is μ, proving the required fact.

Next, consider the case $G = \mathbf{SU}(f)$, where f is a hermitian form in $n \geq 2$ variables over a quaternion division algebra D/K, with respect to the standard involution $^-$ of D; such a G is of type C_n. If v_0 is real and $D_{v_0} = D \otimes_K K_{v_0}$ is a division algebra, then

$G(K_{v_0})$ is simply connected (cf. [H : §9.4]). It follows that the condition that $G(K_{v_0})$ is not (topologically) simply connected is equivalent to the condition that $D_{v_0} = D \otimes_K K_{v_0}$ is the matrix algebra $M_2(K_{v_0})$ (and then $G \simeq \mathbf{Sp}_{2n}$ over K_{v_0}). Now, if $D_{v_0} \simeq M_2(K_{v_0})$, the construction of a K-subgroup H of G, having properties (a) and (b) of Lemma 6.1, is especially easy: for H one takes the unitary group of the one dimensional subspace $e \cdot D$, spanned by any anisotropic vector $e \in D^n$. Indeed, such an H is isomorphic to $\mathbf{SL}_{1,D}$, and since v_0 splits D, $M(S, H)$ is trivial by Theorem 3.1. On the other hand, for any v which splits D, the group G can be identified over K_v with the symplectic group $\mathbf{Sp}_{2n}$, and under this identification H corresponds to the naturally imbedded subgroup $\mathbf{Sp}_2 \subset \mathbf{Sp}_{2n}$. So, H is a long-root subgroup of G with respect to an appropriate maximal K_v-split torus, and the injectivity of the restriction map $H^2(G(K_v)) \to H^2(H(K_v))$ follows from Theorem 1.2.

The other case (i.e. where v_0 is nonarchimedean and D_{v_0} is a division algebra) requires a little more work. First of all, observe that it suffices to consider the case $n = 2$. In fact, if G' is the unitary group of a nondegenerate two-dimensional subspace of D^n, then one easily checks that for any v, G' contains a long-root subgroup with respect to a suitable maximal K_v-split torus. Now if v is nonarchimedean, then from Theorem 1.2, and if v is archimedean, then by a simple topological argument, we deduce the injectivity of the restriction map $H^2(G(K_v)) \to H^2(G'(K_v))$. Since G is isotropic at every nonarchimedean place, $H^2(G(A(S))) = \prod_{v \notin S} H^2(G(K_v))$, and therefore the restriction map $H^2(G(A(S))) \to H^2(G'(A(S)))$ is also injective. This implies the injectivity of the map $M(S, G) \to M(S, G')$, and so it will suffice to establish that $M(S, G')$ is trivial. Hence, in the sequel we assume $n = 2$. In this case, the construction of H described in the next lemma is a generalization of the construction given in [PrRa1: 1.7].

Lemma 6.3 *Given a finite set V of nonarchimedean places of K, there exists a K-subgroup H of G, which is either the direct product $\mathcal{H}_1 \times \mathcal{H}_2$ of two simply connected K-subgroups $\mathcal{H}_i$ of type A_1, or is a group of the form $R_{L/K}(\mathcal{H})$, where L/K is a quadratic extension and $\mathcal{H}$ is a simply connected L-group of type A_1, such that H is K_v-quasi-split and the restriction map $H^2(G(K_v)) \to H^2(H(K_v))$ is injective for every v in V.*

Proof. Let e_1, e_2 be an orthogonal basis of D^2 with respect to f, $\alpha_i = f(e_i) \in K^\star$. Since for any anisotropic vector $e \in D^2$, $f(e \cdot D_v^\star) = K_v^\star$, using the weak approximation property, we may replace e_2 by a multiple, so that $-\alpha_1/\alpha_2 \in K_v^{\star 2}$ for all $v \in V$. Now, let V_0 be the subset of V consisting of those v for which $D_v = D \otimes_K K_v$ is a division algebra, and let $M \subset D$ be a maximal subfield such that $M_{\bar{v}}/K_v$ is an unramified quadratic extension for $v \in V_0$, and $M_{\bar{v}} = K_v$ for $v \in V - V_0$, $\bar{v} \mid v$. Let $M = K(a)$, $a^2 \in K$.

Now let $\mathcal{A} = M_2(D)$, and define the involution τ of $\mathcal{A}$ by the formula

$$\tau\colon x \mapsto F^{-1} x^* F,$$

where $F = \operatorname{diag}(\alpha_1, \alpha_2)$ is the matrix of f, and $(x_{ij})^* = (\bar{x}_{ji})$. Then our unitary group $G = \mathbf{SU}(f)$ is given by the equation

$$x\tau(x) = 1.$$

Let $b \in \mathcal{A}$ be the following element:

$$\begin{pmatrix} 0 & a \\ (\alpha_1/\alpha_2)\bar{a} & 0 \end{pmatrix}.$$

It is easy to verify that $\tau(b) = b$ and $b^2 = (\alpha_1/\alpha_2) \cdot a\bar{a} = -(\alpha_1/\alpha_2)a^2 \in K^\star$. Let H be the centralizer of b in G. First of all, we claim that over the algebraic closure $\bar{K}$, H is a semi-simple group of type $A_1 + A_1$. Indeed, let $\delta \in \bar{K}$ be such that $\delta^2 = b^2$. Then for $b' = \delta^{-1}b$, $b'^2 = 1$, and therefore, $b'\tau(b') = 1$. However, an easy verification shows that the centralizer of any noncentral element of order two in $G \simeq \mathbf{Sp}_4$ is isomorphic to $\mathbf{Sp}_2 \times \mathbf{Sp}_2$, i.e. it is a semi-simple group of type $A_1 + A_1$, and of course, H coincides with the centralizer of b'. To figure out the arithmetic properties of H, we consider the centralizer $\mathcal{B}$ of b in $\mathcal{A}$. Clearly, $\mathcal{B}$ is a quaternion algebra over $L = K(b)$, if L is a quadratic extension of K, and is the direct sum $\mathcal{B}_1 \oplus \mathcal{B}_2$ of two quaternion algebras over K, if $L = K \oplus K$. The involution τ acts as the identity on L; in particular, τ induces an involution of $\mathcal{B}$, and H is the unitary group of $\mathcal{B}$ with respect to the restriction of τ. The fact that H is semi-simple means that, in the first case, τ restricts to the canonical involution of $\mathcal{B}$ over L, and in the second case, it restricts to the direct sum of the canonical involutions of $\mathcal{B}_i$. Then H equals $R_{L/K}(\mathcal{H})$, where $\mathcal{H} = \mathbf{SL}_{1,\mathcal{B}}$, in the first case, and it equals $\mathcal{H}_1 \times \mathcal{H}_2$, where $\mathcal{H}_i = \mathbf{SL}_{1,\mathcal{B}_i}$ in the second case. It follows from our construction that $L_{\bar{v}}/K_v$ is an unramified quadratic extension if $v \in V_0$, and $L_{\bar{v}} = K_v$ if $v \in V - V_0$, $\bar{v} \mid v$. In the second case, the verification of the required properties of H is almost immediate. Viz., here $b^2 \in K_v^{\star 2}$, i.e. $\delta \in K_v^\star$ and $b' \in G(K_v)$. Thus, the above identification of the imbedding $H \subset G$ with the imbedding $\mathbf{Sp}_2 \times \mathbf{Sp}_2 \subset \mathbf{Sp}_4$ is defined over K_v. Since each of these factors is a long-root subgroup in $\mathbf{Sp}_4$, we obtain the injectivity of the restriction $H^2(G(K_v)) \to H^2(H(K_v))$; moreover, H is obviously K_v-split.

Now suppose that $L_{\bar{v}}/K_v$ is an unramified quadratic extension. The proof that H has the required properties in this case uses Proposition 8.44 of [PrRa2]. It was shown there that there exists a K_v-subgroup F of G isomorphic to $R_{P/K_v}(\mathbf{SL}_2)$, where P is an unramified maximal subfield of D_v (at this point it is convenient to distinguish between $L_{\bar{v}}$ and P) such that the restriction map $H^2(G(K_v)) \to H^2(F(K_v))$ is injective. Now to complete the proof, we will show that F and H are conjugate by an element of $G(K_v)$. In principle, this could be done by brute force; however, we prefer an indirect argument. The construction of F is as follows: let h_1, h_2 be a basis of D_v^2, with respect to which f has the matrix

$$\begin{pmatrix} 0 & s \\ -s & 0 \end{pmatrix},$$

where $s \in D_v^*$ is such that $\mathrm{Int}\, s$ induces the nontrivial automorphism of some maximal unramified subfield P of D_v (such a basis always exists); then $F = R_{P/K_v}(\mathbf{SL}_2)$ with respect to this basis. Obviously, $M_2(P)$ is the centralizer of P in $M_2(D_v)$, and F is the corresponding unitary group. It suffices to show that P is conjugate to $L_{\bar{v}}$ by an element from $G(K_v)$. Since both P and $L_{\bar{v}}$ are unramified quadratic extensions of K_v, by the Skölem-Noether Theorem, there exists $g \in GL_2(D_v)$ such that $gPg^{-1} = L_{\bar{v}}$. Then, from the fact that τ acts as the identity on both the fields, we conclude that $\tau(g) \cdot g$ belongs to the centralizer of P, i.e. to $M_2(P)$. On the other hand, τ restricted to $M_2(P)$ is the involution of the latter such that the space of symmetric elements coincides with P (this follows from the fact that the corresponding unitary group is semi-simple), implying that for t in $M_2(P)$, $\tau(t) \cdot t = \det t$. Therefore, there exists $t \in M_2(P)$ such that $\tau(g) \cdot g = \tau(t) \cdot t$, and then $g' = gt^{-1}$ is the required unitary element which conjugates P to $L_{\bar{v}}$. The proof of Lemma 6.3 is now complete.

To exhibit a subgroup H of G having properties (a) and (b) of Lemma 6.1, pick a $v_1 \notin S \cup V_\infty^K$, and take the subgroup H constructed in Lemma 6.3 for $V = \{v_0, v_1\}$. Then in view of Theorem 3.1, it is clear from the structure of H that $M(S, H)$ is trivial. On the other hand, by Lemma 6.3, the restriction $H^2(G(K_{v_1})) \to H^2(H(K_{v_1}))$ is injective.

Now we will prove the triviality of $M_V(G)$ for any finite set V of places of K. For the same reason as above, it suffices to consider the case where $n = 2$. To begin with, observe that $M_V(G) = M_{V_0}(G)$, where V_0 consists of all the nonarchimedean v in V. Indeed, let $V' = V - V_0$, and let F be the unitary group of a nondegenerate one-dimensional subspace of D^2. Since $F \simeq \mathbf{SL}_{1,D}$, $M_V(F)$ is trivial, and it is enough to show that the restriction map $H^2(G(V')) \to H^2(F(V'))$ is injective. However, if $v \in V'$ is such that $D_v = D \otimes_K K_v$ is a division algebra, then the group $G(K_v)$ is topologically simply connected, so $H^2(G(K_v))$ vanishes, and the restriction $H^2(G(K_v)) \to H^2(F(K_v))$ is trivially injective. Otherwise, $D_v = M_2(K_v)$, and there is an identification of G with $\mathbf{Sp}_4$ over K_v under which F gets identified with the canonically imbedded subgroup $\mathbf{Sp}_2 \subset \mathbf{Sp}_4$. So again the restriction $H^2(G(K_v)) \to H^2(F(K_v))$ is injective, proving the required fact. Thus, we may assume that V consists entirely of nonarchimedean places. Consider the subgroup H of G constructed in Lemma 6.3 for our V. Since G is isotropic at every nonarchimedean places, $H^2(G(V)) = \prod_{v \in V} H^2(G(K_v))$, and we conclude from Lemma 6.3 that the restriction $H^2(G(V)) \to H^2(H(V))$ is injective; in particular, the map $M_V(G) \to M_V(H)$ is injective. But according to Proposition 3.2, $M_V(H)$ is trivial, so $M_V(G)$ is trivial too. Lemma 6.1 now implies that $M(S, G)$ is trivial.

To prove that $M(\emptyset, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$ of index at most 2, observe that G splits over any quadratic extension L/K which splits the underlying quaternion algebra D. Since $N_{L/K}(\mu(L))$ is a subgroup of $\mu(K)$ of index at most 2, our assertion follows from Lemma 4.8 applied to $\mathcal{G} = G$.

To conclude the proof of the main theorem for classical groups, consider the case where G is the simply connected cover of the special unitary group $\mathbf{SU}(f)$ of a nondegenerate skew-hermitian form f in $n \geq 4$ variables over a quaternion central division algebra D over K, with respect to the standard involution (denoted as $^-$) of D (recall that such a G is of type D_n).

If $v \in V^K$ is such that $D_v := D \otimes_K K_v$ is isomorphic to $M_2(K_v)$, then G/K_v is isomorphic to the spinor group $\mathbf{Spin}(\tilde{f}_v)$ of a quadratic form $\tilde{f}_v$ in $2n$ variables over K_v which is obtained as follows. Pick an orthogonal basis $e_1, \ldots, e_n$ of D^n, and let $a_i = f(e_i)$ (we write $f(x)$ instead of $f(x,x)$). Fix an isomorphism $\nu_v : D_v \simeq M_2(K_v)$, and consider the involution τ_v of $M_2(K_v)$ that corresponds to $^-$ (in other words, let $\tau_v = \nu_v \circ {}^- \circ \nu_v^{-1}$). Then τ_v can be described by the formula $\tau_v(x) = c_v x^t c_v^{-1}$, where ^{t} denotes the matrix transpose and c_v in $M_2(K_v)$ is a skew-symmetric matrix. Then for every $i = 1, \ldots, n$, $A_i = \nu_v(a_i)c_v$ is a symmetric matrix and $\tilde{f}_v$ is the form with the matrix $\mathrm{diag}(A_1, \ldots, A_n)$. It is well known that if v_0 is real and D_{v_0} is a division algebra, then the fundamental group $\pi_1(G(K_{v_0}))$ is isomorphic to $\mathbf{Z}$ (in fact, the maximal compact subgroup of $G(K_{v_0})$ in this case is isomorphic to $\tilde{\mathbf{U}}(n)$, the two-sheeted covering of the compact unitary group $\mathbf{U}(n)$, cf. [H : §9.4]). So, the assumption that $G(K_{v_0})$ is not simply connected means that if $D_{v_0} \simeq M_2(K_{v_0})$, then the Witt index of the corresponding quadratic form $\tilde{f}_{v_0}$ is ≥ 2.

We need the following analog of Lemma 6.3:

Lemma 6.4 *Let V be a finite set of places of K. Assume that for every real v in V such that $D_v \simeq M_2(K_v)$, the Witt index of the quadratic form $\tilde{f}_v$ corresponding to f is ≥ 2. Then there exists a K-subgroup H of G of the form $R_{L/K}(\mathcal{H})$, where L/K is a quadratic extension, $L_{\bar{v}} = K_v$, $\bar{v} \mid v$, if v is real, and $\mathcal{H}$ is a simply connected L-group of type A_1, having the following properties for every v in V: (a) H is K_v-isotropic, and moreover, (b) the restriction map $H^2(G(K_v)) \to H^2(H(K_v))$ is injective.*

Proof. First, let us recall the following elementary fact (cf. [Sc]): For any place v where D splits, an element a of $D_v^\star$ is contained in $f(D_v^n)$ if, and only if, the binary quadratic form with matrix $\nu_v(a)c_v$ is equivalent to a subform of $\tilde{f}_v$. So, for every real v in V such that $D_v \simeq M_2(K_v)$, one can can pick an $s_v \in D_v^n$ so that for $a_v = f(s_v)$, the matrix $\nu_v(a_v)c_v$ is (positive or negative) definite. Using the weak approximation property and a continuity argument, we see that there exists an s in D^n such that for $a = f(s)$, the matrix $\nu_v(a)c_v$ is definite for any real v ($\in V$) such that $D_v \simeq M_2(K_v)$. Let W be the orthogonal complement of s in D^n. Then for every v in V, there exists a t_v in $W \otimes_K K_v$ such that $f(t_v) = -a$. In case $D_v \simeq M_2(K_v)$, this follows from our construction and the assumption that the Witt index of $\tilde{f}_v$ is ≥ 2 if v is real, and from the fact that a nondegenerate quadratic form over K_v in ≥ 6 variables contains any binary form as a subform if v is nonarchimedean. On the other hand, if D_v is a division algebra, then a skew-hermitian form over D_v in ≥ 3 variables represents any skew-symmetric element in D_v (cf. [Sc]). Now fix a nonarchimedean place $v^0 \notin V$ such that

$D_{v^0} \simeq M_2(K_{v^0})$. Using the above argument we can pick an anisotropic $t_{v^0} \in W \otimes_K K_{v^0}$ so that $\det(\nu_{v^0}(a \cdot f(t_{v^0}))) \notin K_{v^0}^{\star 2}$. Obviously, for any v, the set $\Omega_v = \{f(h) \mid h \in t_v \cdot D_v^\star\}$ is open in the set of all skew-symmetric elements of $D_v^\star$, so there exists a $t \in W$ such that $f(t) \in \Omega_v$ for every v in $V \cup \{v^0\}$.

Let g denote the restriction of f to the D-subspace spanned by s and t, and H be the simply connected cover of the group $\mathbf{SU}(g)$. Then H is a semi-simple K-group of type $D_2 = A_1 + A_1$. Hence, H is K-isomorphic either to the direct product $\mathcal{H}_1 \times \mathcal{H}_2$ of two K-groups of type A_1, or to a group of the form $R_{L/K}(\mathcal{H})$, where L/K is a quadratic extension and $\mathcal{H}$ is an L-group of type A_1. We claim that in our setting the second possibility holds. Indeed, our claim is equivalent to the fact that H is an outer form over K. However, by our construction, H/K_{v^0} is isomorphic to $\mathbf{Spin}(\tilde{g}_{v^0})$, and the discriminant of the quadratic form $\tilde{g}_{v^0}$ is not a square in K_{v^0}. So, H is an outer form over K_{v^0}, and therefore over K. If $v \in V$ is such that $D_v \simeq M_2(K_v)$, then $\tilde{g}_v$ has Witt index 2. So, H splits over K_v, and Proposition 1.9 of [PrRa1] if v is nonarchimedean, and a simple topological argument if v is archimedean, yields the injectivity of the restriction map $H^2(G(K_v)) \to H^2(H(K_v))$. If D_v is a division algebra, then g is the 2-dimensional hyperbolic form over D_v, implying that H is K_v-isomorphic to $\mathbf{SL}_2 \times \mathbf{SL}_{1,D_v}$. Besides, it is easy to check that the factor $\mathbf{SL}_2$ is a long-root subgroup of G/K_v with respect to a suitable maximal K_v-split torus, hence the injectivity of the restriction $H^2(G(K_v)) \to H^2(H(K_v))$ in case v is nonarchimedean (Theorem 1.2). To establish the injectivity for a real v, it suffices to observe that the imbedding $H(K_v) \subset G(K_v)$ gives rise to an imbedding of the respective maximal compact subgroups $\tilde{\mathbf{U}}(2) \subset \tilde{\mathbf{U}}(n)$, which are the 2-sheeted coverings of the compact unitary groups $\mathbf{U}(2) \subset \mathbf{U}(n)$. Since the imbedding $\mathbf{U}(2) \subset \mathbf{U}(n)$ induces an isomorphism of the fundamental groups, our assertion follows. The proof of Lemma 6.4 is complete.

Now given a $v_1 \notin S \cup V_\infty^K$, the K-subgroup H of G constructed in Lemma 6.4 for $V = \{v_0, v_1\}$, satisfies Lemma 6.1 (we have already observed above that if v_0 is real, then the hypothesis of Lemma 6.4 holds). In fact, $M(S, H) = M(\mathcal{S}, \mathcal{H})$, where $\mathcal{S}$ is the set of all extensions of places in S to L. Also, if v_0 is real, then so are both of its extensions, and $\mathcal{H}$ is isotropic with respect to at least one of these. Using this observation, we obtain from Theorem 3.1 that $M(S, H)$ is trivial. The assertion about the injectivity of the map $H^2(G(K_{v_1})) \to H^2(H(K_{v_1}))$ is a part of Lemma 6.4.

It remains to establish the triviality of $M_V(G)$. Let V_0 be the set of real v in V such that $D_v \simeq M_2(K_v)$ and the Witt index of $\tilde{f}_v$ is ≤ 1; $V' := V - V_0$. Then for any $v \in V_0$, the group $G(K_v)$ is topologically simply connected, implying that $H^2(G(K_v))$ vanishes, and hence $M_V(G) = M_{V'}(G)$. So we may assume that V satisfies the assumptions of Lemma 6.4. Let H be the subgroup of G given by Lemma 6.4. Since at every nonarchimedean place, G is isotropic, we conclude from Lemma 6.4(b) that the restriction map $H^2(G(V)) \to H^2(H(V))$ is injective. Hence, the map $M_V(G) \to M_V(H)$ is also injective. On the other hand, Proposition 3.2 implies that $M_V(H)$ is trivial for any V. This proves the triviality of $M_V(G)$. Lemma 6.1 now applies to give the triviality of $M(S,G)$.

To prove that $M(\emptyset,G)$ is a subgroup of $\hat{\mu}(K)$ of index at most 2, we need to combine the argument given for the spinor group of a quadratic form and for the special unitary group of a hermitian form over a quaternion division algebra. Namely, with the notations as above, we let $h = f \perp (-f)$, and let $\mathcal{G}$ denote the simply connected cover of the special unitary group $\mathbf{SU}(h)$. Obviously, $\mathcal{G}$ splits over every quadratic extension L/K which splits the underlying quaternion algebra D. It follows from Lemma 4.8 that $M(\emptyset,\mathcal{G})$ has an element x of order at least $\#\mu(K)/2$, such that the projection $x_v \in H^2(\mathcal{G}(K_v))$ has the same order as x for every nonarchimedean v such that $L_{\bar{v}} = K_v$. However, at any such v, G can be identified with the spinor group $\mathbf{Spin}(\tilde{f})$ naturally imbedded in $\mathcal{G} \simeq \mathbf{Spin}(\tilde{h})$. Since the Witt index of $\tilde{f}$ over K_v is ≥ 2, we obtain the injectivity of the restriction map $H^2(\mathcal{G}(K_v)) \to H^2(G(K_v))$, which implies that the image of x under the restriction map $M(\emptyset,\mathcal{G}) \to M(\emptyset,G)$ has order equal to that of x; this completes the argument.

As is well known (see, for example, [PR2 : §2.3]), the three types of classical groups considered in this section, plus the split symplectic groups $\mathbf{Sp}_{2r}$, exhaust all groups of types B_r, C_r and D_r (except for ${}^{3,6}D_4$). The results of Moore [Mo] and Matsumoto [Ma] for split groups imply the main theorem for split symplectic groups, and thus we have established the main theorem for all classical groups.

7 Groups of exceptional types

In this section, we will complete the proof of the main theorem. As in the previous section, we assume that S contains a place v_0, which is either nonarchimedean, or is real and $G(K_{v_0})$ is not (topologically) simply connected, and prove that $M(S,G)$ is trivial by constructing, in each of the groups under consideration, a subgroup satisfying Lemma 6.1. To give this construction, we make use of some results on Galois cohomology (cf. [PR2], Ch. 6). To simplify our presentation, *we assume here that K is of characteristic zero, i.e. it is a number field.* As recalled in the previous section, if G is of type other than A, and K is a global function field, then G/K is isotropic, and for such groups, $M(S,G)$ has already been computed in [PrRa1].

We begin by considering the groups of types E_7, E_8, F_4 and G_2, which, as the following statement shows, split over a suitable quadratic extension of K.

Proposition 7.1 *Let G be an absolutely simple, simply connected algebraic group of one of the types E_7, E_8, F_4 or G_2, defined over a global field K, and let V be a finite set of places of K such that G splits over K_v for every $v \in V$. Then there exists a maximal K-torus T of G, which is anisotropic over K and splits over a quadratic extension L/K such that $L_{\bar{v}} = K_v$ for every $v \in V$, $\bar{v} \mid v$.*

Proof. Since the Dynkin diagrams of the types E_7, E_8, F_4 and G_2 do not have any nontrivial symmetries, G is the Galois twist ${}_\xi G_0$ of the corresponding split group G_0, for some $\xi \in H^1(K, \bar{G}_0)$, where $\bar{G}_0 = G_0/Z$ is the adjoint group. First, we show that there exists a quadratic extension L/K such that the image ξ_L of ξ in $H^1(L, \bar{G}_0)$ is trivial, and $L_{\bar{v}} = K_v$ for every $v \in V$. Let V_0 be the set of all v's such that ξ_v, the image of ξ in $H^1(K_v, \bar{G}_0)$, is nontrivial; V_0 is finite and disjoint from V. Define L by the following local conditions:

(*i*) $L_{\bar{v}} = K_v$ for all $v \in V$;

(*ii*) $[L_{\bar{v}}: K_v] = 2$ for any nonarchimedean $v \in V_0$, and $L_{\bar{v}} = \mathbf{C}$ for any archimedean $v \in V_0$.

In view of the Hasse principle for the Galois cohomology of adjoint groups (cf. [PR2], Theorem 6.22), to establish the triviality of ξ_L, it is sufficient to establish that of its image ξ_{L_w} in $H^1(L_w, \bar{G}_0)$, for every $w \in V^L$. But the triviality of ξ_{L_w} is obvious except, possibly, in the case where G is of type E_7 and w lies over some nonarchimedean $v \in V_0$. In this case, $H^2(K_v, Z) = \mathrm{Br}(K)_2$, and therefore the image of ξ_v in $H^2(K_v, Z)$ becomes trivial over L_w. Now, since $H^1(K_v, G_0) = \{1\}$, this implies that ξ_{L_w} is trivial.

So G splits over L. Let B be a Borel subgroup of G defined over L such that $T := B \cap B^{\sigma}$ (where σ is a generator of $\mathrm{Gal}(L/K)$) is a maximal K-torus of G (cf. [PR2], Lemma 6.17). As $T = B \cap B^{\sigma}$, σ takes all positive roots in $\Phi(T, G)$ (with respect to the ordering defined by B) to negative roots. However, for the root systems under consideration, the only automorphism with this property is multiplication by -1, which shows that T is anisotropic over K, and it splits over L.

A K-torus T which is anisotropic over K and splits over some quadratic extension L of K is called *admissible* (or, more precisely, *L/K-admissible*), and a semi-simple group containing an admissible maximal torus, is called *admissible*. This terminology was introduced by Weisfeiler [W] who developed an efficient structure theory of admissible groups. His crucial observation was that since σ, the generator of $\mathrm{Gal}(L/K)$, acts on the character group $X(T)$ as multiplication by -1, for any root $\alpha \in R$, the root subgroup G_α, generated by the one-parameter unipotent root subgroups U_α and $U_{-\alpha}$, is defined over K (observe that G_α is a simple, simply connected group of type A_1, and therefore it is isomorphic to the group $\mathbf{SL}_{1,D}$, for some quaternion algebra D over K). These root subgroups will be used to construct in a group G of one of the types E_7, E_8, F_4, or G_2, a subgroup H with the properties described in Lemma 6.1.

Groups of type F_4 and G_2: First of all, observe that a group G of any of these two types must split over K_{v_0}. Indeed, any group of type E_8, F_4 or G_2 splits at any nonarchimedean place (cf. [Ti]). If v_0 is real, then the fact that $G(K_{v_0})$ is not topologically simply connected implies that G should at least be K_{v_0}-isotropic. However, a group of type G_2 is isotropic if, and only if, it is split (cf. [Ti]). On the other hand, there exists only one nonsplit isotropic $\mathbf{R}$-form of type F_4, and this form has relative rank one. The maximal compact subgroups of the group of $\mathbf{R}$-points of this form are isomorphic to the spinor group of a positive-definite quadratic form in 9 variables (cf. [H]), which is topologically simply connected. This implies that the group of real points itself is simply connected, hence our claim.

Let v be an arbitrary place not in $S \cup V_\infty^K$. It follows from the above that Proposition 7.1 applies to $V = \{v_0, v\}$; let T be a maximal torus given by this proposition. Pick an arbitrary *long* root α in the root system $\Phi = \Phi(T, G)$, and let $H = G_\alpha$. Then H splits over K_{v_0}, and therefore, $M(S, H)$ is trivial by Theorem 3.1. On the other hand, T is a maximal K_v-split torus in a K_v-split group G, and H is a long-root subgroup, hence the restriction map $H^2(G(K_v)) \to H^2(H(K_v))$ is injective (1.2).

Groups of type E_7 and E_8: Let v be an arbitrary place outside $S \cup V_\infty^K$ such that G is K_v-split (since all forms of these types are inner, almost all places of K have this property). Let T be a maximal K-torus of G given by Proposition 7.1 for $V = \{v\}$, and L be its splitting field. If v_0 is nonarchimedean, let H be the subgroup generated by the root subgroups G_α and G_β for a pair of adjacent (in the Dynkin diagram) simple roots α, β. Then H is a simple, simply connected *admissible* group of type A_2 which splits over L, hence $H \simeq \mathbf{SU}(\varphi)$, where φ is a hermitian form in 3 variables over L/K. It follows that H is K_{v_0}-isotropic, and therefore $M(S, H)$ is trivial (Theorem 5.1). If v_0 is real, then it is obvious, for example, from the Cartan decomposition and the conjugacy of maximal compact tori in real Lie groups, that there exists a root $\alpha \in \Phi(T, G)$ such that the root subgroup G_α is K_{v_0}-isomorphic to $\mathbf{SL}_2$. Then for $H = G_\alpha$, $M(S, H)$ is again trivial. The injectivity of the restriction map of the second cohomology groups, at v, follows from Theorem 1.2.

Now we will establish the triviality of $M_V(G)$ for these four types. In view of Theorem 2.1, we may (and will) assume that V contains neither any complex places, nor any real places v such that the maximal compact subgroups of $G(K_v)$ are semi-simple. But it follows from [H] that for G of any of the types E_8, F_4 or G_2, and any archimedean place v, every maximal compact subgroup of $G(K_v)$ is semi-simple, and the proof for these types is reduced to the case where V consists entirely of nonarchimedean places. To carry out this reduction for groups of type E_7, observe that if T is an admissible maximal torus in G splitting over L, then $L_{\bar{v}} = \mathbf{C}$ for any real $v \in V$, since in the real split form of type E_7, the maximal compact subgroups of the group of $\mathbf{R}$-points are semi-simple (cf. [H]). Therefore, $T(K_v)$ is a maximal compact torus in the real Lie group $G(K_v)$, so the map $\pi_1(T(K_v)) \to \pi_1(G(K_v))$ is surjective. Let H denote the subgroup of G generated by the root subgroups G_α for $\alpha = \alpha_i$ $(i \neq 2)$ and $\tilde{\alpha}$, where the simple roots are labelled as in [Bu], Table VI (cf. also the figure below), and $\tilde{\alpha}$ is the maximal root. Then H is an admissible group of type A_7 containing T and defined over K. It follows from the above that the map $\pi_1(H(K_v)) \to \pi_1(G(K_v))$ is surjective, implying that the restriction map $H^2(G(K_v)) \to H^2(H(K_v))$ is injective. Since $M_V(H)$ is trivial (cf. §§4, 5), this implies that $M_V(G) = M_{V_0}(G)$, where V_0 consists of all the nonarchimedean places in V, yielding the desired reduction.

So, assume now that V consists of nonarchimedean places only. Our proof of the triviality of $M_V(G)$ in this case applies equally to groups of type E_6 (both inner and outer forms), and that is why at this point we include these in our consideration. In view of Proposition 4.3, it suffices to find, for any nonarchimedean v, a maximal K_v-torus C_v of G, which splits over a cyclic extension of K_v, such that the restriction map $\zeta_v\colon H^2(G(K_v)) \to H^2(C_v(K_v))$ is injective.

Lemma 7.2 *Let G be an absolutely simple, simply connected K-group of one of the following types: ${}^{1,2}E_6$, E_7, E_8, F_4 or G_2; and v be a nonarchimedean place of K such that G is K_v-quasi-split. If C_v is a maximal K_v-torus of G contained in a Borel subgroup defined over K_v, then the restriction map $\zeta_v\colon H^2(G(K_v)) \to H^2(C_v(K_v))$ is injective.*

(Note that C_v splits over K_v if G is not of type ${}^2E_6$, and over a quadratic extension of K_v if it is of type ${}^2E_6$.)

PROOF. Let L be the splitting field of C_v, and Φ be the root system of G with respect to C_v. If G is not of type G_2, let $\alpha, \beta \in \Phi$ be two adjacent simple roots (simple with respect to the ordering on Φ obtained by fixing a Borel subgroup defined over K_v and containing C_v), α, β are assumed to be long if G is of type F_4, and are assumed to be fixed by the Galois group of L/K_v if G is of type ${}^2E_6$. Let H_v be the subgroup of G generated by the root subgroups G_α and G_β. Then H_v is an absolutely simple, simply connected group of type A_2 which is defined and split over K_v; so it is K_v-isomorphic to $\mathbf{SL}_3$, $S_v := C_v \cap H_v$ is a maximal K_v-split torus of H_v. Since H_v contains a root subgroup corresponding to a long relative root, the restriction map $H^2(G(K_v)) \to H^2(H_v(K_v))$ is injective (1.2). On the other hand, by Lemma 1.6, the restriction map $H^2(H_v(K_v)) \to H^2(S_v(K_v))$ is also injective, implying the injectivity of ζ_v.

If G is of type G_2, for H_v we take the subgroup of G generated by the G_α, where α runs through all the long roots of Φ. As is well known, H_v is again a simple, simply connected group of type A_2, and we can argue as before.

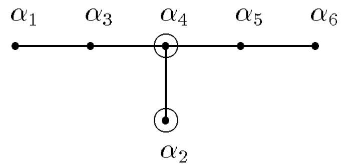
If G is of one of the types E_8, F_4 or G_2, then it splits over any nonarchimedean completion K_v, and therefore Lemma 7.2 applies. Furthermore, if G is of type ${}^2E_6$ over K_v, then it is K_v-quasi-split (cf. [PR2], Prop. 6.15), and again one can use Lemma 7.2. What remains to be done is to construct a "nice" torus in the case where G/K_v is a nonsplit form of type ${}^1E_6$ or E_7.

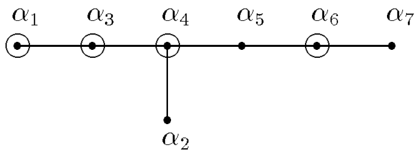
Lemma 7.3 *Let G be an absolutely simple, simply connected group of type ${}^1E_6$ or E_7, and v be a nonarchimedean place of K such that G is not K_v-split. If C_v is a maximal K_v-torus of G which contains a maximal K_v-split torus S_v, then the restriction map $H^2(G(K_v)) \to H^2(C_v(K_v))$ is injective.*

PROOF. It is enough to show that the restriction $H^2(G(K_v)) \to H^2(S_v(K_v))$ is already injective. Let Φ_v be the (relative) root system of G with respect to S_v, and let $\Phi_v^\bullet$ be the subsystem of nonmultipliable roots in Φ_v (i.e. $\alpha \in \Phi_v$ belongs to $\Phi_v^\bullet$ if, and only if, $2\alpha \notin \Phi_v$). As is shown in [BoT1: 7.2], there exists a split semi-simple K_v-subgroup H_v of G, which contains S_v, and whose root system with respect to S_v is $\Phi_v^\bullet$. This H_v

has the following property: If an $\alpha \in \Phi_v^\bullet$ is the restriction of only one root in $\Phi(C_v, G)$, then the relative root subgroup G_α is contained in H_v. Moreover, since G is simply connected, so is H_v ([BoT2: 4.6]). Let Φ^0 be the subset of the root system Φ of G, with respect to C_v, consisting of the roots with trivial restriction to S_v. Then for the inner forms, S_v is the identity component of the intersection $\bigcap_{\alpha \in \Phi^0} \operatorname{Ker} \alpha$, implying that the character group $X(S_v)$ is naturally identified with the quotient $X(C_v)/X^0$, where X^0 is the subgroup of characters which are linear combinations of roots in Φ^0 with rational coefficients, and two roots $\alpha, \beta \in \Phi$ restrict to the same relative root if and only if their difference $(\alpha - \beta)$ lies in X^0.

The Tits indices (cf. [Ti]) of the groups under consideration are:





Using Tables V and VI in [Bu], it is easy to check that the maximal root $\tilde{\alpha}$ of the root system of type E_6 (resp. E_7) is the only root with coefficients 2 at α_2, and 3 at α_4 (resp. coefficient 2 at α_1). So, if we let α denote the relative root obtained as the restriction of $\tilde{\alpha}$, then in either case $\tilde{\alpha}$ is the only root that restricts to α. Obviously, α is the maximal root in the corresponding relative root system. It follows that the relative root subgroup G_α is contained in the split subgroup H_v, and Theorem 1.2 implies the injectivity of the restriction map $H^2(G(K_v)) \to H^2(H_v(K_v))$. On the other hand, the root system $\Phi_v^\bullet$ is of type G_2 in the case of E_6, and of type F_4 in the case of E_7; arguing as in the proof of Lemma 7.2, we obtain the injectivity of the restriction $H^2(H_v(K_v)) \to H^2(S_v(K_v))$. This proves the lemma.

Remark. Let G and S_v be as in the preceding lemma, then the centralizer $Z_G(S_v)$ of S_v contains a maximal K_v-torus C_v which splits over an unramified extension of K_v. This is clear from the fact that the commutator subgroup of $Z_G(S_v)$ is a direct product of certain groups of the form $\mathbf{SL}_{1,D}$, where D is a central division algebra over K_v.

It remains to observe that according to Proposition 7.1 any group G of one of the types E_7, E_8, F_4, or G_2, splits over a suitable quadratic extension L/K, and as $N_{L/K}(\mu(L))$ is a subgroup of $\mu(K)$ of index at most 2, Lemma 4.8 implies that $M(\emptyset, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$ of index at most 2.

Groups of type E_6: For a pair (G, F) consisting of a field F and an absolutely simple, simply connected F-group G of type E_6, we introduce the following property:

$(*)$ *G is F-isotropic, and in the F-index of G, the vertex α_2 (in the Dynkin diagram above) is distinguished.*

Proposition 7.4 *Let G be an absolutely simple, simply connected K-group of type E_6; V be a finite set of places of K such that for every $v \in V$, the pair (G, K_v) satisfies $(*)$.*

Then there exists a quadratic extension L/K, such that $L_{\bar{v}} = K_v$, for every $v \in V$ and the pair (G, L) satisfies $(*)$.

PROOF. Let G_0 be the quasi-split group such that G is the Galois twist ${}_\xi G_0$, for a suitable class $\xi \in H^1(K, \bar{G}_0)$, where $\bar{G}_0 = G_0/Z$ is the adjoint group of G_0. Let C_0 be a maximal K-torus in a Borel subgroup of G_0 defined over K. Labelling simple roots as above, we let C'_0 denote the identity component of $\bigcap_{i \neq 2} \operatorname{Ker} \alpha_i$, $H_0 = [Z_{G_0}(C'_0), Z_{G_0}(C'_0)]$ (obviously, H_0 is generated by the G_{α_i}'s, for $i \neq 2$), and $\bar{H}_0 = H_0/Z$ (as is well known, and easy to see, Z, the center of G_0, is contained in H_0). We need to find a quadratic extension L/K such that $L_{\bar{v}} = K_v$ for $v \in V$, and the image ξ_L of ξ in $H^1(L, \bar{G}_0)$ belongs to the image of the map $H^1(L, \bar{H}_0) \to H^1(L, \bar{G}_0)$. We claim that this is the case for any quadratic extension L with the following local properties:

(i) $L_{\bar{v}} = K_v$ for $v \in V$,

(ii) $L_{\bar{v}} = \mathbf{C}$ for any archimedean $v \notin V$.

Indeed, since the map

$$\delta_K \colon H^1(K, \bar{H}_0) \to H^2(K, Z)$$

is surjective ([PR2: Theorem 6.20]), there exists a $\zeta \in H^1(K, \bar{H}_0)$ such that $\delta_K(\zeta) = \omega_K(\xi)$, where $\omega_K \colon H^1(K, \bar{G}_0) \to H^2(K, Z)$. Let $G' = {}_\zeta G_0$, $H' = {}_\zeta H_0$, etc., and let $\nu \in H^1(K, \bar{G}')$ be the class such that $G = {}_\nu G'$. Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccc} H^1(L, H') & \xrightarrow{\beta_1} & H^1(L, \bar{H}') & \xrightarrow{\beta_2} & H^2(L, Z) \\ \downarrow \epsilon_1 & & \downarrow \epsilon_2 & & \| \\ H^1(L, G') & \xrightarrow{\gamma_1} & H^1(L, \bar{G}') & \xrightarrow{\gamma_2} & H^2(L, Z). \end{array} \tag{1}$$

We wish to show that the image ν_L of ν in $H^1(L, \bar{G}')$ belongs to the image of ϵ_2. By our construction, $\gamma_2(\nu_L)$ is trivial, hence $\nu_L = \gamma_1(\rho)$ for a suitable $\rho \in H^1(L, G')$. On the other hand, for any archimedean place w of L, there exists a $\theta_w \in H^1(L_w, \bar{H}')$ such that $\nu_{L_w} = (\epsilon_2)_w(\theta_w)$. This is immediate if w does not lie over a place in V; otherwise, ν_{K_v} belongs to the image of the map $H^1(K_v, \bar{M}') \to H^1(K_v, \bar{G}')$, where $M' = {}_\zeta Z_{G_0}(C'_0)$ and $\bar{M}' = M'/Z$. However, as $\bar{M}'/\bar{H}'$ is a one-dimensional K_v-split torus, the map $H^1(K_v, \bar{H}') \to H^1(K_v, \bar{M}')$ is surjective and the required fact follows. By looking at the local analog of the diagram (1) at w, we conclude that $\theta_w = (\beta_1)_w(\mu_w)$, $\mu_w \in H^1(L_w, H')$. Since $H^1(L_w, Z) = \{1\}$, the map $H^1(L_w, G') \to H^1(L_w, \bar{G}')$ is injective, and therefore $(\epsilon_1)_w(\mu_w) = \rho_w$, for any archimedean place w of L. By [PR2 : Theorem 6.6], the maps

$$\varphi \colon H^1(L, H') \to \prod_{w \in V_\infty^L} H^1(L_w, H'),$$

$$\psi \colon H^1(L, G') \to \prod_{w \in V_\infty^L} H^1(L_w, G')$$

are bijective. It follows that if $\mu \in H^1(L, H')$ is such that $\varphi(\mu) = (\mu_w)$, then $\epsilon_1(\mu) = \rho$, and the proposition is proved.

Analyzing the classification of real algebraic groups (cf. [Ti]) and E. Cartan's list of symmetric spaces (cf. [H]), we see that if v_0 is real, and G is an inner form of type E_6 over K_{v_0} such that the group $G(K_{v_0})$ is not topologically simply connected, then G is K_{v_0}-split (the only other inner form of type E_6 is a form of $\mathbf{R}$-rank 2, and any maximal compact subgroup of the group of $\mathbf{R}$-points of this form is of type F_4, hence it is simply connected). On the other hand, if v is any place of K such that G is isotropic at v, and moreover, it is an outer form if v is real, then (G, K_v) satisfies $(*)$. This implies that the pair (G, K_{v_0}) satisfies $(*)$. Let v be an arbitrary nonarchimedean place of K such that G is K_v-quasi-split. Let L/K be a quadratic extension given by Proposition 7.4 for $V = \{v_0, v\}$, and let σ be the nontrivial automorphism of L/K. Then the vertex α_2 becomes distinguished over L. In the conjugacy class of maximal parabolic L-subgroups corresponding to the root α_2, we can choose a parabolic subgroup P such that $M := P \cap P^\sigma$ is a maximal reductive subgroup of P (cf. [PR2: Lemma 6.17′]). M is obviously defined over K, and $M = B \cdot H$ (an almost direct product), where $H = [M, M]$ is a simple, simply connected group of type A_5, and B is a one-dimensional L/K-admissible torus. Since the K_{v_0}-rank of G is > 1 in all cases (cf. [Ti]), H is K_{v_0}-isotropic. Besides, if v_0 is real and G is an inner form over K_{v_0}, then, as we observed above, G is K_{v_0}-split, implying that H is also K_{v_0}-split. On the other hand, if G is an outer form over K_{v_0}, then so is H. In all cases, Theorem 4.1 and the proof of Theorem 5.1 show that the projection of $M(S, H)$ to $H^2(H(A(S \cup V_\infty^K)))$ is trivial (this does not depend on Conjecture (U)). Furthermore, H contains a root subgroup with respect to a maximal K_{v_1}-split torus in G containing B, and therefore the restriction map $H^2(G(K_v)) \to H^2(H(K_v))$ is injective. This implies that for any $x \in M(S, G)$, the v-component x_v is trivial. So, arguing as in the proof of Lemma 6.1 we see that to complete the proof of the main theorem for groups of type E_6, we need to establish the triviality of $M_V(G)$.

Lemmas 7.2 and 7.3, in conjunction with Proposition 4.3, yield the triviality of $M_V(G)$ for the case where V consists entirely of nonarchimedean places. On the other hand, in view of Theorem 2.1, we may assume that V does not contain any place v which is either complex, or is real and the maximal compact subgroups of $G(K_v)$ are semi-simple. However, if G is an inner form over K, it follows from the tables in [Ti] and [H] that any archimedean place is of one of these kinds, and there is nothing to prove. What remains to be proven is that if G is of type ${}^2E_6$, and v is a real place in V such that the maximal compact subgroups in $G(K_v)$ are not semi-simple, then

$$M_V(G) = M_{V - \{v\}}(G). \tag{2}$$

At this point, it is convenient to assume that G is K-anisotropic (this assumption does not restrict generality, since the results in [PrRa1] imply the triviality of $M_V(G)$ for any isotropic group). Let L/K be a totally imaginary quadratic extension, linearly disjoint (over K) from the quadratic extension over which G becomes an inner form, and let σ be the nontrivial automorphism of L/K. As is shown in [PR2], p. 385, the vertices α_2 and α_4 in the L-index of G are distinguished. In the conjugacy class of parabolic L-subgroups corresponding to the subset $\{\alpha_1, \alpha_3, \alpha_5, \alpha_6\}$ of simple roots, we choose a P such that $M := P \cap P^\sigma$ is a maximal reductive subgroup of P. Obviously, $M = B \cdot H$ (an almost direct product), where $H = [M, M]$ and B is a 2-dimensional L/K-admissible torus. Also, $R =$ the centralizer of H in G, is a simple, simply connected K-group of type A_2 (it is generated by G_{α_2} and $G_{\tilde{\alpha}}$, $\tilde{\alpha}$ the maximal root); moreover, since R contains B as a maximal torus, it is isomorphic to $\mathbf{SU}(\phi)$, where ϕ is a hermitian form in 3 variables over L/K. It follows that $M_V(R)$ is trivial, and to establish (2), we need only prove the following:

Lemma 7.5 *The restriction map $H^2(G(K_v)) \to H^2(R(K_v))$ is injective.*

Proof. It suffices to show that the map $\pi_1(B(K_v)) \xrightarrow{\iota} \pi_1(G(K_v))$ is surjective. Since $K_v = \mathbf{R}$ and $L_v = \mathbf{C}$, the group $B(K_v)$ is compact. It follows from our choice of v that $G(K_v)$ contains a maximal compact torus of dimension 6 (cf. [H]), hence $M(K_v)$ should also contain such a torus. In this case $H(K_v)$ contains a compact torus of dimension 4, and since H is of type $A_2 + A_2$, we conclude that H is K_v-isomorphic to the product over K_v of two copies of the compact form $\mathbf{SU}_3$. In particular, $H(K_v)$, and hence also $M(K_v)$, is a compact group. Let $\mathcal{C}$ be a maximal compact subgroup of $G(K_v)$ which contains $M(K_v)$; by our choice of v, $\mathcal{C}$ is the product of a one-dimensional central (compact topological) torus $\mathcal{S}$ and a semi-simple simply connected Lie group $\mathcal{C}'$. Since $\mathcal{S}$ centralizes $H(K_v)$, it is contained in $B(K_v)$. It is known that $\mathcal{C}'$ is, in fact, simple of type D_5 (cf. [H]), implying that the order of $\mathcal{S} \cap \mathcal{C}'$ divides 4, and therefore the cokernel of the map $\pi_1(\mathcal{S}) \to \pi_1(\mathcal{C})$ is of order dividing 4. As $\mathcal{S} \subset B(K_{v0})$, we conclude that the order of Coker ι is a divisor of 4. On the other hand, since $M(K_v)$ contains a maximal torus of $\mathcal{C}$, the map $\pi_1(M(K_v)) \to \pi_1(G(K_v))$ is surjective. At the same time, $M(K_v) = B(K_v)H(K_v)$, and the intersection $B \cap H$ is of order 3, which implies that the order of Coker ι divides 3. Thus, Coker ι is trivial, and we have proved the lemma.

Finally, let us show that $M(\emptyset, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$ of index at most two. First, let G be an inner form. The element in $H^2(K, Z)$ obtained from the cocycle which twists the split group into G becomes trivial over a suitable cubic extension F_1/K. Now, if F_2/K is an arbitrary totally imaginary extension (if K itself is totally imaginary, one can take $F_2 = K$, otherwise a suitable quadratic extension F_2/K will do), then $F = F_1F_2$ is a splitting field for G. With such a choice of F, $[\mu(K) : N_{F/K}(\mu(F))]$ divides 6, and then in view of Lemma 4.8, $M(\emptyset, G)$ is isomorphic to a subgroup of $\hat{\mu}(K)$ of index dividing 6. This proves the required fact if K does not contain a primitive third root of unity. Otherwise, K is totally imaginary, and for a sufficiently large β, $F = K(\zeta_{3^\beta})$, where ζ_{3^β} is a primitive 3^β-th root of unity, is a splitting field. Then by Lemma 4.10, $\mu(K) = N_{P/K}(\mu(P))$ and $M(\emptyset, G) = \hat{\mu}(K)$.

Now, if G is an outer form, we have to extend first K to L, the quadratic extension over which G becomes inner, and then use the splitting fields as above. Since G certainly has a splitting field F/K of degree 12, we conclude that the index of $M(\emptyset, G)$ in $\hat{\mu}(K)$ divides 12. This gives the required fact if K does not contain ζ_3 and ζ_4, a primitive third and fourth root of unity respectively. If K contains ζ_3, then for F one can take $L(\zeta_{3^\beta})$, with β sufficiently large. It follows from the above that

$$N_{F/K}(\mu(F)) = N_{L/K}(N_{F/L}(\mu(F))) = N_{L/K}(\mu(L))$$

has index at most two in $\mu(K)$, and we are done. In the last remaining case K contains ζ_4 but not ζ_3, we take for F any cubic extension of L which splits G, and then again $N_{F/K}(\mu(F))$ has index at most two in $\mu(K)$, completing the argument.

Groups of types $^{3,6}D_4$: In view of the results of [PrRa1], we need consider only the anisotropic forms of type $^{3,6}D_4$. So we shall assume in the sequel that G is an anisotropic group of type $^{3,6}D_4$. Let E denote the minimal Galois extension of K over which G becomes inner. Also, let $F = E$ if E/K is of degree 3, and let F be a subextension of E of degree 3 over K if E/K is of degree 6. We need the following analog of Proposition 7.1 for this case:

Proposition 7.6 *Let V be a finite set of places of K such that G is K_v-quasi-split for every $v \in V$. There exists a quadratic extension L/K, which is linearly disjoint from E/K, and has the following properties: G is quasi-split over L, and $L_{\bar{v}} = K_v$ for every $v \in V$ and $\bar{v} \mid v$.*

PROOF. We have: $G = {}_{\xi}G_0$, where G_0 is the corresponding quasi-split group and $\xi \in H^1(K, \bar{G}_0)$, $\bar{G}_0 = \bar{G}_0/Z$ being the adjoint group. We will construct a quadratic extension L/K such that the image ξ_L of ξ under the restriction map $H^1(K, \bar{G}_0) \to H^1(L, \bar{G}_0)$ is trivial. Let V_0 be the set of all places v of K such that the image ξ_v of ξ in $H^1(K_v, \bar{G}_0)$ is nontrivial; then V_0 is finite, and disjoint from V. Let ν be the image of ξ in $H^2(K, Z)$. As a Galois module, Z is isomorphic to $R^{(1)}_{F/K}(\mu_2)$, where $\mu_2 = \{\pm 1\}$, and therefore, for any extension, L/K which is linearly disjoint from E/K, there is a natural map

$$\theta_L \colon H^2(L, Z) \to H^2(L, R_{F/K}(\mu_2)) = \mathrm{Br}(FL)_2,$$

which is injective. For any nonarchimedean $v \in V_0$, let $M(v)$ be a quadratic extension of K_v which is linearly disjoint from $E_{\bar{v}}$, $\bar{v} \mid v$; then the image of $\theta_K(\nu)$ in $\mathrm{Br}(FM(v))$ is trivial. Now let L/K be a quadratic extension linearly disjoint from E/K, with the following local properties:

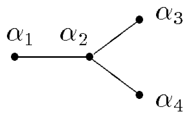
(i) $L_{\bar{v}} = K_v$ for $v \in V$,

(ii) $L_{\bar{v}} = M(v)$ for any nonarchimedean $v \in V_0$,

(iii) $L_{\bar{v}} = \mathbf{C}$ for any archimedean $v \in V_0$.

Then, by the Hasse-Brauer-Noether Theorem, θ_L takes ν_L, the image of ν in $H^2(L,Z)$, to the trivial element, implying that ν_L is itself trivial. Since the Galois cohomology of a simply connected group over a nonarchimedean local field is trivial, we conclude that for any $w \in V_f^L$, the image ξ_w of ξ_L in $H^1(L_w, \bar{G}_0)$ is trivial. On the other hand, for any $v \in V_\infty^K$ such that ξ_v is nontrivial, we have $L_{\bar{v}} = \mathbf{C}$, implying that ξ_w is, in fact, trivial for any $w \in V^L$. In view of the Hasse principle for the Galois cohomology of adjoint groups, this yields the triviality of ξ_L, as required. The proposition is proved.

7.7 Now we need to recall some constructions from ([PR2], §6.8), used therein to prove the Hasse principal for triality forms of type D_4. Fix a quadratic extension L/K linearly disjoint from E/K, $\mathrm{Gal}(L/K) = <\sigma>$, over which G possesses a Borel subgroup B; by Lemma 6.17 of [PR2] we may (and will) assume that the intersection $C = B \cap \sigma(B)$ is a maximal K-torus of G. The splitting field of C is LE, and if we lift σ to an element of $\mathrm{Gal}(LE/K) = \mathrm{Gal}(L/K) \times \mathrm{Gal}(E/K)$ by letting it act trivially on E, then its action on the character group $X(C)$ is just multiplication by -1. It follows that if we label simple roots in $\Phi(C,G)$ as in [Bu], Table IV:



then for $\alpha = \alpha_2$, or $\tilde{\alpha}$, the maximal root, the corresponding root subgroup G_α is defined over K. Let H be the subgroup of G generated by G_{α_2} and $G_{\tilde{\alpha}}$; H is an absolutely simple, simply connected admissible K-group of type A_2, and hence it is isomorphic to $\mathbf{SU}(\psi)$, where ψ is a hermitian form over L/K in 3 variables.

Lemma 7.8 *Let v be nonarchimedean. Assume that if G is K_v-quasi-split, then $L_{\bar{v}} = K_v$, $\bar{v} \mid v$. Then the restriction map $H^2(G(K_v)) \to H^2(H(K_v))$ is injective.*

Proof. If G is quasi-split over K_v, our assertion follows from Theorem 1.2. Hence we assume that G is not quasi-split over K_v. Then, as any triality form of type D_4 is automatically K_v-quasi-split (cf. [PR2 : Proposition 6.15]), the group G/K_v is none of these, so it is isomorphic either to $\mathbf{Spin}(f)$, f a quadratic form in 8 variables of Witt index 2, or to the simply connected cover of $\mathbf{SU}(h)$, h a skew-hermitian form in 4 variables (of Witt index 1 or 2) over a quaternion central division algebra D/K with respect to the natural involution of D.

First, we consider the case where $G = \mathbf{Spin}(f)$. We may assume that G is an inner form over K_v since otherwise it is quasi-split. Then C is an $L_{\bar{v}}/K_v$-admissible torus. If we let g denote the norm form of $L_{\bar{v}}/K_v$, then there exists a basis with respect to which f has the following form:

$$f(x_1, \ldots x_8) = a_1 g(x_1, x_2) + \ldots + a_4 g(x_7, x_8),$$

and C can be identified with $R^{(1)}_{L_{\bar{v}}/K_v}(\mathbf{GL}_1)^4$. After choosing a different basis,if necessary, we can assume that H is identified with the special unitary group $\mathbf{SU}(\varphi)$, where φ is the hermitian form over $L_{\bar{v}}/K_v$ in 3 variables with coefficients a_1, a_2, a_3, and $\mathbf{SU}(\varphi)$ is naturally imbedded in G. Now, to prove the injectivity of the map $H^2(G(K_v)) \to H^2(H(K_v))$, we may appropriately change the basis to make $a_1 = 1, a_2 = -1$. Let $f' = g(x_1, x_2) - g(x_3, x_4)$, and let φ' be the corresponding 2-dimensional hermitian form. Then $G' = \mathbf{Spin}(f')$ is the direct product of two factors, H_1 and H_2, each of which is isomorphic to $\mathbf{SL}_2$, and is in fact, a root subgroup in G corresponding to a long (relative) root; hence the injectivity of the map $H^2(G(K_v)) \to H^2(H_i(K_v))$ for $i = 1, 2$. To complete the proof, it remains to observe that $H' = \mathbf{SU}(\varphi')$ coincides with one of these factors (the easiest way to see this is to notice that the unitary group $\mathbf{U}(\varphi')$ is contained in $\mathbf{SO}(f') = H_1H_2$ (almost direct product), and therefore it is not possible that the projection of H' on both factors is nontrivial, since a semi-simple subgroup of $\mathbf{SO}(f')$, which projects onto both H_1 and H_2, can not commute with any nontrivial torus).

Now we turn to the case where G is the simply connected cover of $\mathbf{SU}(h)$, h as above. Recall that a subgroup of a reductive algebraic group is called *regular* if it is normalized by a maximal torus. We claim that H contains a regular K_v-subgroup H', isomorphic to $\mathbf{SL}_2$. To give an explicit construction of such an H', we realize H as $\mathbf{SU}(\varphi)$, where φ is the hermitian form over $L_{\bar{v}}/K_v$ with matrix $\mathrm{diag}(-1, 1, a)$, and then for H' take the special unitary group of the subform of φ with the matrix $\mathrm{diag}(-1, 1)$. Obviously, H' is a regular subgroup of H; on the other hand, H is centralized by a subtorus of C of dimension 2, hence our claim. Now, by looking at the natural 8-dimensional representation of $\mathbf{SO}_8$, we conclude that the subspace W of D^4, fixed pointwise by $H(K_v)$, has dimension 2 (over D), and therefore, H is contained in the simply connected cover G_0 of the special unitary group of the orthogonal complement $W^{\perp}$. As is well known, $G_0 = G_1 \times G_2$, where $G_1 = \mathbf{SL}_2$ and $G_2 = \mathbf{SL}_{1,D}$. This implies that $H = G_1$. However, G_1 is a root subgroup corresponding to a long relative root (with respect to a suitable maximal split torus of G), hence the injectivity of $H^2(G(K_v)) \to H^2(H(K_v))$. The lemma is proved.

Now let v_0 be nonarchimedean. Given a nonarchimedean v_1, we pick L/K as in Proposition 7.6, satisfying $L_{\bar{v}_1} = K_{v_1}$ if G is K_{v_1}-quasi-split. Then it immediately follows from Lemma 7.8 that the subgroup H constructed above satisfies Lemma 6.1.

To consider the case of real v_0, we need to make one preliminary observation. For a root $\alpha \in \Phi(C, G)$, let $G(\alpha)$ be the subgroup of G generated by the root subgroup G_α and all of its Galois conjugates. It is easy to check that either $G(\alpha) = G_\alpha$ (i.e. G_α is defined over K), or G_α is defined over a subextension F of E of degree 3 over K, and then $G(\alpha) = R_{F/K}(G_\alpha)$. Now, if v_1 is a nonarchimedean place such that $L_{\bar{v}_1} = K_{v_1}$, $\bar{v}_1 \mid v_1$ (in particular, G is K_{v_1}-quasi-split), then for any $\alpha \in \Phi(C, G)$, the group $G(\alpha)$ contains a root subgroup with respect to the relative root obtained as the restriction of α (it suffices to check this for a simple root, in which case it is verified by a direct computation), and therefore the restriction map $H^2(G(K_{v_1})) \to H^2(G(\alpha)(K_{v_1}))$ is injective (1.3).

Now we will construct a subgroup H of G with the properties described in Lemma 6.1. Take a v_1 such that the group G is K_{v_1}-quasi-split. If G is also K_{v_0}-quasi-split, we can pick L such that $L_{\bar{v}_i} = K_{v_i}$ for $i = 0, 1$, $\bar{v}_i \mid v_i$,. Let C be as in 7.7, and $H = G_{\alpha_2}$. It follows from the above discussion that H is a K-subgroup of type A_1 which splits over K_{v_0}, hence the triviality of $M(S, H)$. On the other hand, as we have just observed, the restriction map $H^2(G(K_{v_1})) \to H^2(H(K_{v_1}))$ is injective.

So, now we may assume that G is not K_{v_0}-quasi-split. We claim that in our set-up, this, in conjunction with the assumption that $G(K_{v_0})$ is not topologically simply connected, implies that G becomes an inner form over K_{v_0} (i.e. $E_{\bar{v}_0} = K_{v_0}$). Indeed, outer forms of this type over $\mathbf{R}$ are isomorphic to $\mathbf{Spin}(f)$, where f is a quadratic form of the signature $(s, 8-s)$, where s is odd. The assumption that $G(K_{v_0})$ is not topologically simply connected amounts to saying that $s \neq 1, 7$. So, s can only be 3 or 5, in which case G is K_{v_0}-quasi-split.

We choose L in such a way that $L_{\bar{v}_1} = K_{v_1}$. As we observed above, there exists a root $\alpha \in \Phi(C, G)$ such that the group G_α is K_{v_0}-isotropic. Let $H = G(\alpha)$. Then one easily verifies that H is as required. (The verification is immediate if H is of type A_1, otherwise $H = R_{F/K}(\mathcal{H})$ where $\mathcal{H}$ is a group of type A_1 and F is a subfield of E of degree 3 over K. Then $M(S, H) = M(\mathcal{S}, \mathcal{H})$, where $\mathcal{S}$ consists of all extensions of places in S to F. By our construction, all extensions of v_0 are real, and $\mathcal{H}$ is isotropic with respect to one of these, so the triviality of $M(\mathcal{S}, \mathcal{H})$ follows.)

It remains to verify the triviality of $M_V(G)$. To begin with, we show that

$$M_V(G) = M_{V_0}(G),$$

where V_0 consists of all nonarchimedean places in V. It suffices to show that given an archimedean $v \in V$,

$$M_V(G) = M_{V-\{v\}}(G). \tag{3}$$

Obviously, we may suppose that v is real and $G(K_v)$ is not topologically simply connected. As we saw above, if G is an outer form over K_v, this assumption implies that G is K_v-quasi-split. In this case, pick an L such that $L_{\bar{v}} = K_v$, and let $H = G_{\alpha_2}$. Then the restriction map $H^2(G(K_v)) \to H^2(H(K_v))$ is injective, which, in view of the triviality of $M_V(H)$, implies (3). Now let G be inner over K_v. Then there exists a root $\alpha \in \Phi(C, G)$ such that the root subgroup G_α is K_v-isotropic, which in this case implies the injectivity of the restriction map $H^2(G(K_v)) \to H^2(G_\alpha(K_v))$. Now we let $H = G(\alpha)$, and arguing as above, obtain (3).

So, we may suppose that V consists entirely of nonarchimedean places, and again let H be the subgroup generated by G_{α_2} and $G_{\tilde{\alpha}}$. Since G is isotropic with respect to any nonarchimedean place, Lemma 7.8 implies the injectivity of the restriction map $H^2(G(V)) \to H^2(H(V))$. However, the triviality of $M_V(H)$ has already been established, from which the triviality of $M_V(G)$ now follows.

Finally, we prove that $M(\emptyset, G)$ is a subgroup of $\hat{\mu}(K)$ of index at most two. Pick a totally imaginary quadratic extension L/K over which G is quasi-split (cf. Proposition

7.6), and choose a maximal K-torus C as in 7.7. Then the group $H = G_{\alpha_2}$ is defined over K and splits over L. There exists an imbedding $G \hookrightarrow \mathcal{G}$ of G into L-split L-group $\mathcal{G}$ of type F_4 such that H is identified with a long-root subgroup of $\mathcal{G}$ with respect to a suitable maximal L-split torus. According to [Ma], there exists an element $x \in M(\emptyset, \mathcal{G})$ of order $\#\mu(L)$, and it follows from Theorem 1.2 that x restricts to an element $y \in M(\emptyset, H/L)$ of the same order. Now, we conclude from the proof of Lemma 4.8 that by restricting y to $H(A)$ using the canonical imbedding $H(A) \hookrightarrow H(A_L)$, we obtain an element of $M(\emptyset, H)$ of order divisible by $\#N_{L/K}(\mu(L))$. This implies that if we restrict our original x to $G(A)$ using the imbeddings

$$G(A) \hookrightarrow G(A_L) \hookrightarrow \mathcal{G}(A_L),$$

we get an element of $M(\emptyset, G)$ whose order is divisible by $\#N_{L/K}(\mu(L))$. Since

$$[\mu(K) \colon N_{L/K}(\mu(L))] \leq 2,$$

this completes the proof.

8 The congruence subgroup problem over semi-local number rings

We shall assume here that K is a number field. For a finite set V of nonarchimedean places of K, let $\mathfrak{o}_V$ denote the subring consisting of elements in K which are integral with respect to all places in V, i.e.

$$\mathfrak{o}_V = \{a \in K \mid v(a) \leq 1 \text{ for all } v \in V_f^K\}.$$

Clearly, $\mathfrak{o}_V$ is a semi-local ring. Now, let G be a simple, simply connected algebraic K-subgroup of $\mathbf{SL}_N$. The goal of this section is to show that for the group $G(\mathfrak{o}_V) := G(K) \cap SL_N(\mathfrak{o}_V)$, the congruence subgroup problem *always* has positive solution. The precise statement of this result, and the subsequent argument, make essential use of the notion of the congruence kernel, which imitates the original definition for S-arithmetic subgroups given by Serre. We introduce two topologies on the group $G(K)$, τ_a and τ_c, called the *arithmetic* topology and the *congruence* topology, respectively. In τ_a, the family of all normal subgroups of finite index in $\Gamma := G(\mathfrak{o}_V)$ (note that, in fact, any noncentral normal subgroup in Γ has finite index, cf. [M1]) constitute a fundamental system of neighborhoods of the identity, whereas in τ_c, the congruence subgroups $\Gamma(\mathfrak{a})$ corresponding to the nonzero ideals $\mathfrak{a} \subset \mathfrak{o}_V$, constitute a fundamental system of neighborhoods of the identity. Then letting $\widehat{G}$ and $\overline{G}$ denote the completions of $G(K)$ with respect to τ_a and τ_c, we have the following exact sequence:

$$1 \to C \longrightarrow \widehat{G} \xrightarrow{\pi} \overline{G} \to 1, \tag{1}$$

where π is the natural projection and $C = \operatorname{Ker} \pi$ is the *congruence kernel.*

Theorem 8.1 *Suppose that $G(K)$ has the standard description of normal subgroups, and V contains all the nonarchimedian places where G is anisotropic. Then C is trivial, i.e. every noncentral normal subgroup of Γ contains the congruence subgroup $\Gamma(\mathfrak{a})$ for some ideal $\mathfrak{a}$.*

Proof. To begin with, notice that the congruence completion $\overline{G}$ can be identified with $G(V) = \prod_{v \in V} G(K_v)$. This immediately follows from the weak approximation theorem for G (cf.[PR2], Theorem 7.8) and the observation that the congruence topology τ_c on $G(K)$ coincides with the topology induced via the diagonal imbedding $G(K) \hookrightarrow G(V)$. In our argument we will use the following generalization of Proposition 3.2 of [Ra2] (cf. also Proposition 9.3 of [PR2]).

For a subset $X \subset G(K)$, let $\overline{X}$ (resp., $\widehat{X}$) denote the closure of X in $\overline{G}$ (resp., $\widehat{G}$).

Proposition 8.2 *There exists a τ_c-open subgroup U of Γ with the following property: for any noncentral normal subgroup $N \subset \Gamma$ and any $x \in \overline{N} \cap \Gamma$, we have*

$$R(N, x) := Z(N, x)(\overline{N} \cap \Gamma) \supset U,$$

where $Z(N, x) = \{y \in \Gamma \mid yxy^{-1}x^{-1} \in N\}$.

(Note that $R(N, x)$ coincides with the closure of $Z(N, x)$ in Γ with respect to τ_c.)

We begin with the following lemma.

Lemma 8.3 *There exists an open compact subgroup U_0 of $G(V)$ such that for any maximal K-torus $B \subset G$, the closure $\overline{B(K)} \subset B(V)$ contains $B(V) \cap U_0$.*

Proof. Let r be the rank of G and G_{rs} be the set of regular semi-simple elements in G. Since K is of characteristic zero, for any integer $n > 0$, the set of n-th powers $(G(V))^n$ is an open neighborhood of the identity (this is the only place in our argument where the assumption about the characteristic is used), hence it contains an open compact subgroup $W = W(n)$. Obviously, for any maximal K-torus B of G, $(B \cap G_{rs})(V) \cap W$ is dense in $B(V) \cap W$. On the other hand, the inclusion $W \subset G(V)^n$ implies that

$$(B \cap G_{rs})(V) \cap W \subset B(V)^n.$$

So, it is enough to prove the following: There exists an $n = n(r)$ such that for any K-torus B of dimension r, we have the inclusion:

$$\overline{B(K)} \supset B(V)^n. \tag{2}$$

We will show that for $n(r)$ one can take any positive integer which is divisible by the order of any finite subgroup of the group $GL_r(\mathbf{Z})$ (for example, $n(r)$ equal to the index in $GL_r(\mathbf{Z})$ of the congruence subgroup $GL_r(\mathbf{Z}, 3)$ modulo 3 will do). Fix any $n = n(r)$ with this property, and let B be an arbitrary K-torus of dimension r. If L is the minimal splitting field of B, then the natural action of the Galois group $\mathrm{Gal}(L/K)$

on the character group of B gives a faithful representation in $GL_r(\mathbf{Z})$, in particular, the order of $\mathrm{Gal}(L/K)$ divides n. Let $H = R_{L/K}(B)$, and let $\eta: H \to B$ be the "norm" map (cf., for example, the proof of Proposition 6.7 of [PR2]). Obviously, $N = \mathrm{Ker}\ \eta$ is a K-defined subtorus of H. As B splits over L, by Hilbert's Theorem 90 one has

$$H^1(K, H) = H^1(L, B) = 1.$$

Picking an L-isomorphism $B \to (\mathbf{GL}_1)^r$, and applying the restriction of scalars functor, we obtain a K-isomorphism $H \to R_{L/L}(\mathbf{GL}_1)^r$. Thus, H is quasi-split over K, in particular, it has the weak approximation property with respect to any finite set of places. This implies that $\overline{B(K)} \supset \eta(H(V))$, and it remains to be shown that

$$\eta(H(V)) \supset B(V)^n. \tag{3}$$

Corresponding to the exact sequence

$$1 \to N \longrightarrow H \xrightarrow{\eta} B \to 1,$$

one has the exact sequence

$$H(V) \xrightarrow{\eta} B(V) \longrightarrow \prod_{v \in V} H^1(K_v, N). \tag{4}$$

By our construction, N splits over L, which implies that for any $v \in V^K$, $H^1(K_v, N) = H^1(L_w/K_v, N)$, where $w \mid v$. However, the order of the Galois group $\mathrm{Gal}(L_w/K_v)$ divides that of $\mathrm{Gal}(L/K)$, which in turn divides n. This implies that the extreme right term of (4) is annihilated by multiplication by n, so (3) holds . The lemma is proved.

Proof of Proposition 8.2. Let U_0 be a compact-open subgroup given by the preceding lemma; without loss of generality we may assume that U_0 is a normal subgroup of $\overline{\Gamma}$. We will show that one can then take $U = \Gamma \cap U_0$. Let $U_{rs} = U \cap G_{rs}$, where, as in the proof of Lemma 8.3, G_{rs} is the set of regular semisimple elements in G. Then $U_{rs}^{-1} = U_{rs}$. Since U (resp., G_{rs}) is Zariski dense (resp., Zariski open) in G, we conclude that $U = U_{rs}U_{rs}$. Therefore, it suffices to show that $R(N, x)$ contains U_{rs}. Pick $z \in U_{rs}$, and let B denote the maximal K-torus in G containing z, $B_r = B \cap G_{rs}$. Consider the map

$$\eta: G(V) \times B_r(V) \to G(V),$$

given by: $\eta(g, b) = gbg^{-1}$. It follows from the Inverse Function Theorem (cf. [PR2], §3.1) that η is an open map. So if $U_1 \supset U_2 \supset \ldots$ is a descending chain of normal subgroups of $\overline{\Gamma}$ converging to (e), then $W_i = \eta(U_i, B_r(V))$ is open in $G(V)$ for every $i \geq 1$, and therefore $\overline{N} \subset W_i N$ (indeed, for any $n \in \overline{N}$, the set $n(W_i)^{-1}$ is an open neighborhood of n, and hence meets N). In particular, we can write

$$x = \eta(u_i, b_i) y_i$$

for some $u_i \in U_i$, $b_i \in B_r(V)$ and $y_i \in N$. It follows that the element xy_i^{-1} is regular, and for its centralizer C_i in G, we have

$$u_i^{-1}C_i(V)u_i = B(V).$$

Consider the open sets

$$\Omega_i = u_i z u_i^{-1}(\overline{N} \cap U_0), \qquad i \geq 1.$$

Clearly, $\Omega_i \subset U_0$ and $\Omega_i \cap C_i(V) \neq \emptyset$. Now it follows from our choice of U_0 that for every i one can pick an element $z_i \in C_i(K) \cap \Omega_i$. Since $u_i \to e$ and $\overline{N}$ is open in $G(V)$, for sufficiently large i, we have

$$z^{-1}z_i \in \Gamma \cap ((z^{-1}u_i z u_i^{-1})\overline{N}) = \Gamma \cap \overline{N}.$$

It remains to observe that by our construction, $z_i \in Z(N, x)$, and therefore the last inclusion implies that $z \in R(N, x)$, as required. Proposition 8.2 is proved.

In the notation introduced in the first paragraph, we have:

Proposition 8.4 *Let $x \in C$ and $Z_{\widehat{G}}(x)$ be the centralizer of x in $\widehat{G}$. Then*

$$\pi(Z_{\widehat{G}}(x)) \supset \overline{U},$$

where U is the open subgroup of Γ introduced in Proposition 8.2.

Proof. Let $N_1 \supset N_2 \supset \ldots$ be a descending chain of normal subgroups of Γ of finite index constituting a neighborhood base for τ_a at the identity. Then

$$C = \varprojlim \overline{N_i}/\widehat{N_i} = \varprojlim (\Gamma \cap \overline{N_i})/N_i. \tag{5}$$

For every $i \geq 1$, pick an element $x_i \in \Gamma \cap (x\widehat{N_i})$; since $x \in C$, we automatically have $x_i \in \Gamma \cap \overline{N_i}$. Then

$$Z(N_1, x_1) \supset Z(N_2, x_2) \supset \ldots \quad \text{and} \quad \bigcap_i \widehat{Z(N_i, x_i)} = Z_{\widehat{\Gamma}}(x). \tag{6}$$

In view of

$$\bigcap_i \overline{N_i} = C, \tag{7}$$

(6) implies that

$$\bigcap_i \widehat{Z(N_i, x_i)}\overline{N_i} = Z_{\widehat{\Gamma}}(x)C. \tag{8}$$

Indeed, the left-hand side of (8) contains the right-hand side. To prove the opposite inclusion, pick an arbitrary z from the left-hand side of (8), and for every $i \geq 1$ write it as

$$z = z_i n_i, \qquad \text{where } z_i \in \widehat{Z(N_i, x_i)}, \quad n_i \in \overline{N_i}.$$

Then we can choose convergent subsequences $z_{i_k} \to z_0$, $n_{i_k} \to n_0$. It follows from (6),(7) that $z_0 \in Z_{\widehat{\Gamma}}(x)$, $n_0 \in C$, and (5) is proved.

Since π is a closed map, to prove the proposition it suffices to show that $\pi(Z_{\widehat{\Gamma}}(x)) \supset U$. Fix $u \in U$, and consider the fiber $F = \pi^{-1}(u)$. It follows from Proposition 8.2 that $F \cap (\widehat{Z(N_i, x_i)\overline{N_i}}) \neq \emptyset$ for every i. Since F is compact, this fact combined with (8) implies that $F \cap Z_{\widehat{\Gamma}}(x)C \neq \emptyset$, i.e. $u \in \pi(Z_{\widehat{\Gamma}}(x))$, as required. Proposition 8.4 is proved.

Another important ingredient of the proof is the following:

Proposition 8.5 *If $D \subset C$ is an open subgroup which is normal in $\hat{G}$, then $D = C$.*

PROOF. Consider the quotient of (1) by D:

$$1 \to L = C/D \longrightarrow H = \widehat{G}/D \xrightarrow{\theta} \overline{G} \to 1. \tag{9}$$

Since C is a profinite group (cf.(5)) and D is its open subgroup, L is finite. While proving the congruence subgroup property for S-arithmetic groups with bounded generation, it was established in [R3], [PR3] that if $G(K)$ has the standard description of normal subgroups and S is disjoint from T (where T is the set of nonarchimedian places where G is anisotropic), then any such extension with finite L (or more generally, with L satisfying the finiteness condition (F) in Serre's book [S1]) is central. Obviously, in our situation the condition on S has to be replaced by the assumption that $V \supset T$, and then the argument from *loc. cit.* yields the centrality of (9). For the sake of completeness, we reproduce this argument here.

The positive solution of the Kneser-Tits conjecture over local fields ([PrRa3] and [PR2: §7.2]) implies that for $v \notin T$, the group $G(K_v)$ does not have any proper subgroups of finite index; it follows that the group $G(V-T) = \prod_{v \in V-T} G(K_v)$ does not have any such subgroup either. On the other hand, Z, the centralizer of L in H, is a closed normal subgroup of finite index in H, and we conclude that $\theta(Z) \supset G(V-T)$; in other words, $Z_1 = Z \cap \theta^{-1}(G(V-T))$ maps surjectively onto $G(V-T)$. Since the groups $G(T)$ and $G(V-T)$ commute elementwise, for any $r \in R = \theta^{-1}(G(T))$, $z \in Z_1$, the commutator $[r, z]$ falls into L, and for r fixed the map $\phi_r\colon Z_1 \to L$, $\phi_r(z) = [r, z]$ is a homomorphism. Now pick any finite subset $\Delta \subset R$, and consider the homomorphism $\phi_\Delta\colon Z_1 \to L^d$, $\phi_\Delta(z) = (\phi_r(z))_{r \in \Delta}$, where $d = \#\Delta$. Again, the fact that $Z(\Delta) = \operatorname{Ker}\phi_\Delta$ is of finite index in Z_1, implies that $\theta(Z(\Delta)) = G(V-T)$, i.e. $\theta^{-1}(G(V-T)) = Z(\Delta)\cdot L$. This being true for any finite Δ, we conclude, using the finiteness of L, that $\theta^{-1}(G(V-T)) = Z_2 \cdot L$ where $Z_2 = \bigcap_\Delta Z(\Delta)$. Hence,

$$\theta(Z_2) = G(V-T) \tag{10}$$

(note that by our construction, Z_2 is the centralizer of R in Z_1). Furthermore, we claim that

$$L \subset Z_2. \tag{11}$$

Indeed, for $v \in T$, the group $G(K_v)$ is compact, and consequently, R is a profinite group. On the other hand, by virtue of (10), $H = R \cdot Z_2$, implying that H/Z_2 is profinite too. So, if (11) does not hold, there exists an open normal subgroup P of H, of finite index, which does not contain L. Then $N = P \cap G(K)$ is a normal subgroup of finite index in $G(K)$, and since we assumed the standard description of normal subgroups in $G(K)$, there should exist an open normal subgroup $W \subset G(V)$ with the property $N = G(K) \cap W$. Obviously, we have $P \cap G(K) = \theta^{-1}(W) \cap G(K)$, so taking the closure we obtain $P = \theta^{-1}(W)$; in particular, $P \supset L$, a contradiction. Thus, (11) is proved.

It follows from (11) that $Z \supset R$, so in fact $Z \supset R \cdot Z_2 = H$, i.e. L belongs to the center of H.

Once the centrality of (9) has been established, the triviality of L is deduced from the triviality of $M_V(G)$ by a standard argument, which we recall now. Consider the initial segment of the Lyndon-Hochschild-Serre spectral sequence corresponding to (9):

$$H^1(G(V)) \xrightarrow{\varphi} H^1(H) \longrightarrow H^1(L)^{G(V)} \xrightarrow{\psi} H^2(G(V)).$$

Since L is central, the middle term, $H^1(L)^{G(V)}$, is equal to $\hat{L}$, the Pontrjagin dual of L. In view of our assumption that $V \supset T$, the standard description of normal subgroups in $G(K)$ together with the weak approximation property imply that $[G(K), G(K)] = G(K) \cap [G(V), G(V)]$, which is exactly equivalent to the assertion that φ is an isomorphism. On the other hand, since (9) splits over $G(K)$, the image of ψ is contained in $M_V(G) = \mathrm{Ker}(H^2(G(V)) \to H^2(G(K)))$, which is trivial. Hence L is also trivial, and the proof of Proposition 8.5 is complete.

Now we are in a position to complete the proof of triviality of C. Assume that $C \neq 1$, and let $C_0 \subset C$ be a fixed maximal open normal subgroup (so that $F = C/C_0$ is a finite simple group). Then,

$$C_1 = \bigcap_{g \in \widehat{G}} (gC_0g^{-1})$$

is a closed subgroup in C, and C is normal in $\hat{G}$, so we may take the quotient of (1) by C_1:

$$1 \to M = C/C_1 \longrightarrow H = \widehat{G}/C_1 \xrightarrow{\theta} \overline{G} \to 1.$$

Besides, M is isomorphic to the product of a certain number of copies of F :

$$M \simeq \prod_{i \in I} F_i, \quad \text{where } F_i = F \quad \forall i.$$

Consider the two cases, where F is respectively a cyclic group of prime order and a nonabelian finite simple group.

Case 1. Let Z denote the centralizer of M in H. Since M is abelian, we have $M \subset Z$, and it follows from Proposition 8.3 that for any $x \in M$, the centralizer $Z_H(x)$ contains $\theta^{-1}(\overline{U})$, implying the inclusion $Z \supset \theta^{-1}(\overline{U})$. Then $\pi(Z)$ is a normal subgroup of $\overline{G}$ containing $\overline{U}$. Since any noncentral normal subgroup of $G(K_v)$ has finite index (cf.

[PR2], Prop. 3.17), it follows that the index $[\overline{G} : \pi(Z)]$, and therefore also the index $[H : Z]$, is finite. Now, pick some proper open subgroup M_0 of M. Then

$$M_1 = \bigcap_{h \in H} (hM_0h^{-1}) \tag{12}$$

is again open in M, and besides, is normal in H. Obviously, the pull-back of M_1 under the canonical homomorphism $C \longrightarrow C/C_1$ yields a proper open subgroup in C normal in $\widehat{G}$, but such a subgroup cannot exist by Proposition 8.4, a contradiction.

Case 2. The action of H by conjugation defines a homomorphism $H \longrightarrow \mathrm{Aut}(M)$. Obviously, in the case under consideration,

$$\mathrm{Aut}(M) = S_I \ltimes \prod_{i \in I} \mathrm{Aut}(F_i)$$

(semi-direct product), where S_I is the symmetric group on the set I, and we may consider the induced homomorphism $\beta\colon H \longrightarrow S_I$. Let $N = \mathrm{Ker}\beta$. Now, pick an $i \in I$, and consider the element

$$x = (1, \ldots, 1, a, 1, \ldots)$$

for some nonidentity element $a \in F_i$. Clearly, $\beta(Z_H(x))$ fixes i, and since $M \subset N$, we conclude from Proposition 2 that

$$\theta^{-1}(\overline{U}) \subset \beta^{-1}(S_I(i)),$$

where $S_I(i)$ is the stabilizer of i. This being true for every i, we eventually obtain that $\theta^{-1}(\overline{U}) \subset N$. Arguing as above, we deduce from this inclusion that $[H : N] < \infty$, i.e. the image $\beta(H)$ is finite. This immediately implies that for any open subgroup $M_0 \subset M$, the subgroup M_1 given by (12) is again open, so we can conclude the argument exactly as in the previous case. Theorem 8.1 is proved.

Remark. Usually, the computation of the congruence kernel consists of two parts: the proof of its centrality, and, computation of the corresponding metaplectic kernel; and these parts are independent. In our argument, these parts are not singled out explicitly; however, the triviality of $M_V(G)$ is used in the proof of Proposition 8.5, which plays a crucial role also in that part of the argument that actually corresponds to the proof of centrality. So it is worth mentioning that, in fact, one can make this part of the argument completely independent of the computation of the weak metaplectic kernel (and therefore, in a sense, "absolutely" uniform) by some minor modifications (which, however, make the proof more technical).

Appendix A On maximal subfields in simple algebras

In our argument, we need to construct maximal subfields in simple algebras (with or without involution) with special local behavior. For this purpose we use the following method: first we construct an abstract extension of the center having an appropriate degree and some specific properties, and then, using a certain imbedding criterion, show that the field under consideration can be imbedded into our algebra as a maximal subfield. An important feature of the imbedding criteria in question is that they have the form of a local-to-global principle, and in fact we need to check only finitely many local conditions.

First, we formulate for convenience of reference, a well-known result for algebras without involution (cf. [Pi], §18.4).

Proposition A.1 *Let $\mathcal{A}$ be a central simple algebra over an algebraic number field K, $\dim_K \mathcal{A} = n^2$, and let P/K be a field extension of degree n. The existence of a K-imbedding $\theta : P \hookrightarrow \mathcal{A}$ is equivalent to the existence of local imbeddings $\theta_v : P \otimes_K K_v \hookrightarrow \mathcal{A}_v := \mathcal{A} \otimes_K K_v$ for all $v \in V^K$. Furthermore, if $\mathcal{A}_v = M_{m_v}(\Delta_v)$, where Δ_v is a division algebra over K_v, and d_v is the degree of Δ_v, then θ_v exists if and only if for any extension $\bar{v} \mid v$, the degree $[P_{\bar{v}} : K_v]$ is divisible by d_v.*

It is well-known that a reductive K-group G is quasi-split at almost all places (cf.[PR2], Theorem 6.7); applying this fact to $G = \mathbf{SL}_1(\mathcal{A})$ one gets $d_v = 1$, for almost all v. It follows that the existence of θ can be guaranteed by specifying the behavior of P at finitely many places.

The analogs of these results for algebras with involution are not so well-known. Let $\mathcal{A}$ be a central simple algebra over a global field L, $\dim_L \mathcal{A} = n^2$, τ be an involution on $\mathcal{A}$ of the second kind, and $K = L^\tau$ be the field of τ-invariant elements. First, we prove a local-global principle for imbedding a field extension P/L of degree n provided with an automorphism of order two, into $(\mathcal{A}, \tau)$ as algebras with involution. (Note that this assertion was implicitly established in [PR2], §6.7, in the course of the proof of the Hasse principle for Galois cohomology of simple simply connected groups of type ${}^2A_r$, however, in view of its importance for our argument, we give a detailed proof.)

Proposition A.2 *Let P/L be an extension of degree n, with an automorphism σ of order two such that $\sigma \mid L = \tau$. Assume that either n is odd or $F = P^\sigma$ satisfies the following condition:*

(LD) the normal closure of F is linearly disjoint from L over K.

Then the existence of an L-imbedding $\theta \colon (P, \sigma) \hookrightarrow (\mathcal{A}, \tau)$ such that

$$\theta \circ \sigma = \tau \circ \theta, \tag{1}$$

is equivalent to the existence of local $(L \otimes_K K_v)$-imbeddings

$$\theta_v : (P \otimes_K K_v, \sigma) \hookrightarrow (\mathcal{A} \otimes_K K_v, \tau),$$

satisfying

$$\theta_v \circ \sigma = \tau \circ \theta_v, \tag{2}$$

for all $v \in V^K$.

Proof. By Proposition A.1, the existence of local imbeddings implies at least the existence of an L-imbedding $\epsilon : P \hookrightarrow \mathcal{A}$ as algebras without involution. We will modify ϵ by an inner automorphism so as to make it respect involutions. Since the imbeddings ϵ and $\tau \circ \epsilon \circ \sigma$ of P into $\mathcal{A}$ agree on L, by the Skölem-Noether Theorem there exists $h \in \mathcal{A}^\star$ with the property

$$\epsilon(\sigma(x)) = h\tau(\epsilon(x))h^{-1} \tag{3}$$

for all $x \in P$. We have

$$\epsilon(x) = \epsilon(\sigma^2(x)) = h\tau(\epsilon(\sigma(x)))h^{-1} = (h\tau(h)^{-1})\epsilon(x)(h\tau(h)^{-1})^{-1},$$

i.e. $h\tau(h)^{-1} \in \tilde{P} = \epsilon(P)$. Say $h\tau(h)^{-1} = \epsilon(a)$, $a \in P$. An easy computation shows that $\sigma(a)a = 1$, and therefore by Hilbert's Theorem 90, $a = b\sigma(b)^{-1}$ for some $b \in P$. Then the element $\tilde{h} = \epsilon(b)^{-1}h$ is τ-symmetric. As (3) holds if we replace h by $\tilde{h}$, we may (and will) assume, to begin with, that h is τ-symmetric.

By the Skölem-Noether Theorem, every θ_v can be written as

$$\theta_v(x) = g_v^{-1}\epsilon(x)g_v, \tag{4}$$

for some $g_v \in (\mathcal{A} \otimes_K K_v)^\star$, and we are going to look for the required θ among the imbeddings of the form

$$\theta(x) = g^{-1}\epsilon(x)g, \quad g \in A^\star. \tag{5}$$

It readily follows from (2)-(4) that

$$g_v\tau(g_v)h^{-1} = \epsilon(t_v), \tag{6}$$

for some $t_v \in (P \otimes_K K_v)^\star$. Similarly, for θ to satisfy (1), we need to find a g such that

$$g\tau(g) = \epsilon(t)h, \tag{7}$$

for some $t \in P^\star$. It is easy to check that an element of the form $\epsilon(c)h$ is τ-symmetric if and only if c is σ-symmetric. This means that we have to look for t in $F = P^\sigma$, while $t_v \in (F \otimes_K K_v)^\star$ for every $v \in V^K$.

Now, if K is of positive characteristic, then using the vanishing of the Galois cohomology of the special unitary group associated with $\mathcal{A}$ ([Ha]), and repeating the argument given on p. 363 of [PR2], one shows that a τ-symmetric element $x \in \mathcal{A}^\star$ can be written in the form $g\tau(g)$ for some $g \in \mathcal{A}^\star$ if, and only if, $\mathrm{Nrd}_{\mathcal{A}/L}(x) \in N_{L/K}(L^\star)$. In our situation, this means that we need to show that $a = \mathrm{Nrd}_{\mathcal{A}/L}(h)^{-1}$ can be written in the form:

$$a = N_{F/K}(t)N_{L/K}(s), \tag{8}$$

for some $t \in F$, $s \in L$. It turns out that if K is of characteristic zero, our problem is equivalent to solving the equation (8), however this reduction requires some additional argument.

For $v \in V^K$, we let

$$\Sigma(v) = \{a\tau(a) \mid a \in (\mathcal{A} \otimes_K K_v)^\star\ \}.$$

Given $t \in F^\star$, by Landherr's Theorem (cf.[PR], Theorem 6.27) (7) can be solved for $g \in \mathcal{A}^\star$ if, and only if,

$$\epsilon(t)h \in \Sigma(v) \tag{9}$$

for all v. Using the remark on p. 363 of [PR2] once more, we see that (8) for $v \in V_f^K$ is equivalent to

$$\mathrm{Nrd}_{A/L}(\epsilon(t)h) \in N_{(L\otimes_K K_v)/K_v}((L \otimes_K K_v)^\star).$$

So, it suffices to prove that $a = \mathrm{Nrd}_{A/L}(h)^{-1}$ can be written in the form (8) for $t \in F$, $s \in L$ in such a way that (9) is satisfied *only* for $v \in V_\infty^K$. However, a short argument (cf. Lemma 6.27 of [PR2]) shows that the last requirement can, in fact, be omitted. Indeed, if (9) has a solution $(t, s) \in F^\star \times L^\star$, then the variety

$$X = \{(x, y) \in R_{F/K}(\mathbf{GL}_1) \times R_{L/K}(\mathbf{GL}_1) \mid N_{F/K}(x)N_{L/K}(y) = a\}$$

is a principal homogeneous space, trivial over K, of the torus

$$R = \{(x, y) \in R_{F/K}(\mathbf{GL}_1) \times R_{L/K}(\mathbf{GL}_1) \mid N_{F/K}(x)N_{L/K}(y) = 1\}.$$

It follows that X has the weak approximation with respect to V_∞^K (cf. Proposition 7.8 in [PR2]). If g_v, t_v are as in (6), the pair (t_v, s_v), $s_v = \mathrm{Nrd}_{\mathcal{A}\otimes_K K_v/L\otimes K_v}(g_v)$, is a solution of (9) over K_v. Besides, for any $v \in V_\infty^K$, the set $\Sigma(v)$ is open in the set of τ-symmetric elements of $(\mathcal{A} \otimes_K K_v)^\star$. So, taking a solution (t, s) to (9) with t-component sufficiently close to t_v for all $v \in V_\infty^K$, we will ensure (8) for those v.

If n is odd, then (9) can be solved explicitly: one can take $t = a$, $s = a^{(1-n)/2}$ (note that $a \in K^\star$ since h is τ-symmetric). In the general case, we need the so called multinorm principle (Proposition 6.11 of [PR2]). Its assumptions are satisfied in view of (LD), and therefore one can solve (9) for $t \in F^\star$, $s \in L^\star$ if and only one can solve the corresponding local problem

$$a = N_{(F\otimes_K K_v)/K_v}(t^v)N_{(L\otimes_K K_v)/K_v}(s^v),$$

for $t^v \in (F \otimes_K K_v)^\star$, $s^v \in (L \otimes_K K_v)^\star$, for every $v \in V^K$. However, as already noted above, one can take the pair (t_v, s_v) for a local solution at v. Proposition A.2 is proved.

It can be shown (cf.[PR2], p. 340) that if $G = \mathbf{SU}(\mathcal{A}, \tau)$ is quasi-split over K_v (which is, as we mentioned above, the case for almost all v), then θ_v in Proposition A.2 exists automatically. We will not describe here the precise conditions for the existence of θ_v in general, but will limit ourselves to two particular cases needed in §5:

Firstly, suppose $[L_w : K_v] = 1$. Then $\mathcal{A}_v \simeq M_{m_v}(\Delta_v) \oplus M_{m_v}(\Delta_v^0)$, where Δ_v is a division algebra over K_v, Δ_v^0 is the opposite algebra. Letting d_v denote the index of Δ_v, we have the following easy consequence of Proposition A.1.

Proposition A.3 *In the notations as above, the existence of θ_v is equivalent to the divisibility of $[F_{\bar v} : K_v]$ by d_v, for any extension $\bar v \mid v$ to $F = P^\sigma$.*

Now, let $[L_w : K_v] = 2$. Then $G = \mathbf{SU}(\mathcal{A}, \tau)$ is K_v- isomorphic to some special unitary group $\mathbf{SU}_n(L_w, h_v)$.

Proposition A.4 *If $F \otimes_K K_v \simeq K_v^n$, then θ_v exists.*

Proof. Pick an orthogonal basis of L_w^n. Then with respect to this basis h_v looks as follows:

$$h_v(x_1, \ldots, x_n) = \alpha_1 x_1 x_1^\tau + \cdots + \alpha_n x_n x_n^\tau$$

for some $\alpha_i \in K_v$. Then $(\mathcal{A} \otimes_K K_v, \tau)$ is isomorphic as algebra with involution to $(\mathcal{B} = M_n(L_w), \theta)$ where θ is given by the formula

$$\theta((x_{ij})) = H(x_{ji}^\tau)H^{-1}, \quad H = \mathrm{diag}(\alpha_1, \ldots, \alpha_n). \tag{10}$$

On the other hand, $P \otimes_K K_v = (F \otimes_K K_v) \otimes_{K_v} L_w$ is isomorphic to L_w^n with the following action of σ:

$$\sigma((x_1, \ldots, x_n)) = (x_1^\tau, \ldots, x_n^\tau). \tag{11}$$

It follows from (10)-(11) that the imbedding

$$P \otimes_K K_v \hookrightarrow \mathcal{B}, \ (x_1, \ldots, x_n) \mapsto \mathrm{diag}(x_1, \ldots, x_n),$$

respects involutions. Proposition A.4 is proved.

Also, in the special case of central simple algebras of dimension p^2, p a prime, we need to construct maximal subfields which are cyclic Galois extensions of the center and have prescribed local behavior. This is done using the Grunewald-Wang theorem (cf. [AT], [To]). For the sake of completeness, we include here a particular case of the latter, which is sufficient for our purposes.

Proposition A.5 *Let K be a global field, V_1, V_2 be two finite sets of noncomplex places of K, and p be a prime. Assume that V_2 consists entirely of nonarchimedean places if $p \neq 2$. Then there exists a cyclic extension E/K of degree p such that*

$$[E_{\bar v} \colon K_v] = \begin{cases} 1, & v \in V_1, \\ p, & v \in V_2, \end{cases}$$

where $\bar v \mid v$.

We recall briefly the main steps of the proof, for we will use a similar argument in the unitary situation. The main case is $p \neq \mathrm{char}\, K$. Let J_K denote the idele group of K. We identify $K^\star$ with the group of principal ideles, and for each $v \in V^K$ we let i_v denote the natural imbedding of $K_v^\star$ into J_K. By the global class field theory, the construction of P is equivalent to finding a (continuous) character $\chi : J_K \to I = \mathbf{R}/\mathbf{Z}$ of order p, trivial on $K^\star$ and such that the induced character $\chi_v = \chi \circ i_v$ of $K_v^\star$ is trivial for $v \in V_1$

and nontrivial for $v \in V_2$. The construction of such χ is carried out backwards, starting with a *prescribed* χ_v. Viz., pick a finite subset $S \subset V^K$ containing $V_1 \cup V_2 \cup V_\infty^K$, so that

$$J_K = J_K^S K^\star; \tag{12}$$

where J_K^S is the group of S-integral ideles. Next, introduce χ_v for $v \in S$ as follows: $\chi_v = 1$ for $v \in S - V_2$, and χ_v is a character of $K_v^\star$ of order p for $v \in V_2$, and define

$$\chi_S : K_S^\star = \prod_{v \in S} K_v^\star \to I, \ \chi_S((x_v)) = \prod_{v \in S} \chi_v(x_v).$$

Now in view of (12), to construct χ with the required properties, it suffices to construct a character

$$\psi_S : U_S = \prod_{v \notin S} U_v \longrightarrow I,$$

of order p, where U_v is the group of v-adic units, such that

$$\chi = \chi_S \cdot \psi_S : J_K^S \longrightarrow I$$

restricts trivially to $\Gamma_S = J_K^S \cap K^\star$. Let $\Delta = \Gamma_S \cap \ker \chi_S$; we may assume that $\Gamma_S \neq \Delta$. One shows that there exists $v_0 \notin S$, relatively prime to p, such that

$$\Gamma_S \cap U_{v_0}^p = \Delta,$$

and in this case

$$\Gamma_S/\Delta \overset{\alpha}{\simeq} U_{v_0}/U_{v_0}^p.$$

Thinking of χ_S as a character of Γ_S/Δ, we can define the character

$$x \mapsto [\chi_S(\alpha^{-1}(x))]^{-1}$$

of $U_{v_0}/U_{v_0}^p$, and lift it to the character χ_{v_0} of U_{v_0}. Then putting $\chi_v = 1$ for $v \notin S \cup \{v_0\}$, $\psi_S = \prod_{v \notin S} \chi_v$, we obtain the required character.

The case where K is of positive characteristic p is much simpler and can be handled using Artin-Schreier construction. As usual, let $\wp(t) = t^p - t$. For any $v \in V^K$, $\wp(K_v)$ is an open subgroup of the additive group K_v^+. Now, for every $v \in V_2$ we pick $a_v \in K_v - \wp(K_v)$. By the weak approximation property, there exists $a \in K$ such that $a \in \wp(K_v)$ for $v \in V_1$, and $a \in a_v + \wp(K_v)$ for $v \in V_2$. Then the extension $K(\wp^{-1}(a))$ (i.e. the extension obtained by adjoining a root of the polynomial $X^p - X - a$) is as required. The proposition is proved.

A.6. Now if $\mathcal{A}$ is a central simple algebra of prime degree p over a global field K, and $V \subset V^K$ is a finite subset consisting of places v such that $\mathcal{A}_v = \mathcal{A} \otimes_K K_v$ is isomorphic to $M_p(K_v)$, then there exists a maximal subfield $E \subset \mathcal{A}$ which is cyclic over K and such that $[E_{\bar{v}} : K_v] = 1$ for all $v \in V$, $\bar{v} \mid v$. Indeed, let $V_1 = V$ and let V_2 be the set of $v \in V^K$ such that $\mathcal{A}_v$ is a division algebra (obviously, V_2 is contained in V_f^K).

Let E/K be the extension obtained by applying the previous proposition to these V_1 and V_2. Then it follows from Proposition A.1 that E is as required.

We need also a unitary version of Proposition A.5.

Proposition A.7 *Let F be a (seperable) quadratic extension of a global field K. Let V_1, V_2 be two finite sets of places of K, and p be an odd prime. Assume that V_2 consists entirely of nonarchimedean places v such that $F_w = K_v$, $w \mid v$. Then there exists a Galois extension E/K with dihedral Galois group $Gal(E/K)$ of order $2p$ which contains F, and for which*

$$[E_{\bar{v}}\colon F_w] = \begin{cases} 1, & v \in V_1, \\ p, & v \in V_2, \end{cases}$$

where $w \mid v$, $\bar{v} \mid w$.

Proof. Let σ be the generator of $\mathrm{Gal}(F/K)$. As in the previous proposition, we first consider the main case where p is different from the characteristic of K. By the global class field theory, to construct the required E we need to construct a character $\chi : J_F \to I$, of order p, trivial on $F^\star$, satisfying $\chi \circ \sigma = \chi^{-1}$, and such that $\chi_w := \chi \circ i_w$ is trivial for $w \in \bar{V}_1$, and nontrivial for $w \in \bar{V}_2$, where $\bar{V}_i$ is the set of all extensions of places from V_i to F, $i_w : F_w^\star \to J_F$ is the natural imbedding. As in the proof of the previous proposition, pick a finite σ-invariant subset $S \subset V^F$ containing $\bar{V}_1 \cup \bar{V}_2 \cup V_\infty^F$ and having the property $J_F = J_F^S F^\star$. For $w \in S_0 = \bar{V}_1 \cup V_\infty^F$ we let $\chi_w = 1$. Furthermore, any $v \in V_2$ has two distinct extensions $w', w'' \in V_2$; each of the completions $F_{w'}$, $F_{w''}$ can be identified with K_v, and σ acts on $F_{w'}^\star \times F_{w''}^\star$ by switching the factors. Let χ_v be a character of order p of the group

$$(K_v^\star \times K_v^\star)/K_v^\star \simeq K_v^\star,$$

where $K_v^\star$ is imbedded diagonally. Identifying $F_{w'}^\star \times F_{w''}^\star$ with $K_v^\star \times K_v^\star$, we get a character $\chi_v : F_{w'}^\star \times F_{w''} \to I$ with the property $\chi_v \circ \sigma = \chi_v^{-1}$. Now, define a character χ_S on $F_S^\star = \prod_{w \in S} F_w^\star$ as $\prod_{w \in S_0} \chi_w \cdot \prod_{v \in V_2} \chi_v$. To complete the construction of the required χ, it remains to construct a character

$$\psi_S : \prod_{\bar{v} \notin S} U_w \to I,$$

such that $\psi_S \circ \sigma = \psi_S^{-1}$, and $\chi = \chi_S \cdot \psi_S$ is trivial on $\Gamma_S = J_F^S \cap F^\star$.

Let $\Delta = \Gamma_S \cap \ker \chi_S$; we may assume that $\Delta \neq \Gamma_S$. We will show below that there exists a place v_0 of K, which is relatively prime to p, and over which F splits, such that

$$\Gamma_S \cap U_{w_0}^p = \Delta, \tag{13}$$

where $w_0 \mid v_0$. We identify $F_{w_0'}^\star \times F_{w_0''}^\star$ with $K_{v_0} \times K_{v_0}$ as above, and consider the following subgroup:

$$B = U_{v_0}(U_{w_0'} \times U_{w_0''}) \subset H = U_{w_0'} \times U_{w_0''}.$$

Using (13) and the fact that $\chi_S \circ \sigma = \chi^{-1}$, it is easy to show that

$$\Gamma_S \cap B = \Delta,$$

and consequently

$$\Gamma_S/\Delta \overset{\beta}{\simeq} H/F.$$

Define χ_{v_0} as a character of H lifting the character

$$x \mapsto [\chi_S(\beta^{-1}(x))]^{-1}$$

of H/F, and put $\chi_w = 1$ for $w \in \mathcal{S} = S \cup \{w_0', w_0''\}$. Then the character

$$\psi_S = \prod_{w \notin \mathcal{S}} \chi_w \cdot \chi_{v_0}$$

of $U_S = \prod_{w \notin S} U_w$ is as required.

It remains to establish the existence of a v_0 satisfying (13) (this part of argument was omitted in the proof of Proposition A.4, but here we supply the details). Let

$$M_1 = F(\zeta_p, \sqrt[p]{\Gamma_S}), F_2 = L(\zeta_p, \sqrt[p]{\Delta}),$$

where ζ_p is a primitive p-th root of unity. Since Γ_S and Δ are finitely generated and σ-invariant, both M_1 and M_2 are Galois extensions of K. Arguing as in ([To], p.218), we conclude that M_1/M_2 is cyclic of degree p. By Chebotarev's Density Theorem, there exists a v_0 which is not a restriction of a place from S, and v_0 is relatively prime to p, and such that $M_2 \subset K_{v_0}$ and $M_{1\bar{v}_0}/K_{v_0}$, $\bar{v}_0 \mid v_0$, is cyclic of degree p. One easily verifies that the v_0 is as required.

In the remaining case where p equals the characteristic of K, one argues as follows. For every $v \in V_2$, there exists $a_v \in F \otimes K_v$ such that $\sigma(a_v) - a_v \notin \wp(F \otimes_K K_v)$. Using the weak approximation property, we pick $b \in F$ such that $b \in \wp(F \otimes_K K_v)$ for $v \in V_1$, and $b \in a_v + \wp(F \otimes_K K_v)$ for $v \in V_2$, and let $c = \sigma(b) - b$. Then the field extension $E = F(\wp^{-1}(c))$ is as required. The proposition is proved.

It is not always true that given a central simple algebra $\mathcal{A}$ over a global field L with involution τ of the second kind, $K = L^\tau$, there always exists a maximal subfield P of A which is a Galois extension of K with dihedral Galois group $\mathrm{Gal}(P/K)$, even if the degree of $\mathcal{A}$ is prime (however, obstructions arise only at real places). For this reason, we had to use a more sofisticated construction in §5.

Appendix B On the uniqueness of the reciprocity law

Let F be a finite extension of the global field K; $\mu(F)$ be the group of all roots of unity in F, and $\mu = \#\mu(F)$. For a non-complex place v of F, we let $\mu(F_v)$ denote the group of all roots of unity in F_v, and let $\mu_v = \#\mu(F_v)$; by convention, $\mu(F_v) = \{1\}$

and $\mu_v = 0$ if v is complex. Let $(\star,\star)_v$ be the norm residue symbol on F_v of power μ_v (if v is complex, then by definition $(\star,\star)_v \equiv 1$). The norm residue symbols satisfy the following relation known as Artin's reciprocity law, or, the product formula:

$$\prod_v (x,y)_v^{\mu_v/\mu} = 1 \quad \text{for all} \quad x, y \in F^*$$

(the product is taken over all places of F). An important ingredient in the computation of the metaplectic kernel for isotropic groups is the uniqueness of this reciprocity law, proved by Moore ([Mo], Theorem 7.4) in the following form: Suppose that for every place v of F, one is given a character $\chi_v \in \hat{\mu}(F_v)$ so that

$$\prod_v \chi_v((x,y)_v) = 1, \tag{1}$$

for all $x, y \in F^*$. Then there exists a character $\chi \in \hat{\mu}(F)$ such that $\chi_v = \chi \circ \tau_v$, where $\tau_v \colon \mu(F_v) \longrightarrow \mu(F)$ is the homomorphism of raising to the power μ_v/μ. A consequence of this uniqueness is that *if χ_{v_0} is trivial for at least one noncomplex place v_0, then $\chi_v = 1$ for all v.*

In the computation of the metaplectic kernel for anisotropic groups, one encounters a "reciprocity law" of form (1), but which only holds for pairs (x,y) in a rather small subset $\Omega_1 \times \Omega_2$ of $F^* \times F^*$ (cf. §§3-5). The uniqueness of such a "reciprocity law" in the case where F is a cyclic Galois extension of K, and $\Omega_1 = \Omega_2$ coincides with $F^{(1)}$, the group of elements with norm 1 in the extension F/K, was analyzed in [Pr1]. For our computation (of the metaplectic kernel) we do not need a general uniqueness result, hence we limit ourselves to stating the following proposition which suffices for our purposes. It was proved by the second-named author (see [R1], Proposition 4); for the convenience of the reader, we reproduce the proof here.

To give a precise statement, we fix a finite set V of places of F and let $\Omega_2 = F^* \cap U$, where U is an open neighborhood of the identity in $\prod_{v \in V} F_v^*$.

Proposition B *Let Ω_1 be a subset of F^*, and Ω_2 be as above. Suppose reciprocity law (1) holds for all pairs $(x,y) \in \Omega_1 \times \Omega_2$, and there exists a prime p such that $\chi_v^p = 1$ for all v. Let $v_1, v_2 \in V^F - V$ be two noncomplex places such that*

(1) if $p > 2$, then both v_1 and v_2 are nonarchimedean;

(2) there exists an $a \in \Omega_1$ such that $v(a) = 1$ (i.e. a is a uniformizing element in F_v) for $v \in \{v_1, v_2\} \cap V_f^F$, and for $v \in \{v_1, v_2\}$ such that $F_v = \mathbf{R}$, $a < 0$.

If $\chi_{v_1} = 1$, then $\chi_{v_2} = 1$.

Proof. Let $[x,y]_v = (x,y)_v^{\mu_v/(\mu_v,p)}$, where (μ_v, p) is the g.c.d. of μ_p and p. Obviously, $[x,y]_v$ is the norm residue symbol on F_v of power p if p divides μ_v and is identically one otherwise. For every $v \in V^F$, there is a character θ_v, of the subgroup

$\mu(F_v)_p$ generated by the elements of order p in $\mu(F_v)$, such that $\theta_v([x,y]_v) = \chi_v((x,y)_v)$ for all $x, y \in F_v^*$. Then

$$\prod_v \theta_v([x,y]_v) = 1 \quad \text{for all} \quad (x,y) \in \Omega_1 \times \Omega_2, \tag{2}$$

and we need to prove that if $\theta_{v_1} = 1$, $\theta_{v_2} = 1$.

Of course, there is nothing to prove if μ_{v_2} is prime to p, so we may assume that ζ_p, a primitive p-th root of unity, is contained in F_{v_2}. Let $L = F(\zeta_p)$, and fix some extensions w_1, w_2 of v_1, v_2 to L. Let $a \in \Omega_1$ be such that $v_i(a) = 1$. If $p = 2$, then $L_{w_i} = K_{v_i}$, and if $p > 2$, then by our assumption the v_i, i=1,2, are nonarchimedean, and the ramification index $e(w_i \mid v_i)$ is $\leq (p-1)$; in particular, it is prime to p, and therefore $g.c.d.(w_i(a), p) = 1$. We need the following elementary lemma:

Lemma B *For $w \in V^L$, denote by $\{\star,\star\}_w$ the norm residue symbol on L_w of power p. Let a be as above, and assume that for each $w \in V^L$, a p-th root of unity ξ_w is given so that the following conditions are satisfied:*

(i) $\xi_w = 1$ for almost all w;

(ii) $\prod_w \xi_w = 1$;

(iii) for every w, there exists a $c_w \in L_w^*$ with the property $\{a, c_w\}_w = \xi_w$.

Then there exists a $c \in L^*$ such that $\{a, c\}_w = \xi_w$ for all w.

The proof is left to the reader (see, [CF : Exercise 2.16]).

We apply this lemma, in our situation, letting $\xi_{w_1} = \zeta_p^{-1}$, $\xi_{w_2} = \zeta_p$, $\xi_w = 1$ if $w \neq w_1, w_2$, and using the same a as above. Conditions (i) and (ii) of the lemma visibly hold, and (iii) follows from the fact that $w_i(a) = 1$ and g.c.d.$(w_i(a), p) = 1$. As a result, we obtain an element $c \in L^*$ for which

$$\{a,c\}_w = \begin{cases} \zeta_p^{-1}, & w = w_1, \\ \zeta_p, & w = w_2, \\ 1, & w \neq w_1, w_2. \end{cases} \tag{3}$$

We claim that one can pick a $c \in L^*$, so that it satisfies (3), and moreover, $N_{L/F}(c) \in \Omega_2$. Indeed, there exists an open neighborhood W of the identity in $\prod_{w \in \bar{V}} L_w^*$, where $\bar{V}$ consists of all extensions of places in V to L, such that $N_{L/F}(L^* \cap W) \subset \Omega_2$. It follows from the weak approximation property that the imbedding

$$N_{L(\sqrt[p]{a})/L}(L(\sqrt[p]{a})^*) \hookrightarrow N_{L_w(\sqrt[p]{a})/L_w}(L_w(\sqrt[p]{a})^*) =: N_{\bar{V}}$$

is dense; in particular,

$$N_{\bar{V}} \subset W \cdot N_{L(\sqrt[p]{a})/L}(L(\sqrt[p]{a})^*). \tag{4}$$

Since $v_1, v_2 \notin V$, it follows from (3) that $c \in N_{\bar{V}}$. But then in view of (4), there exists an $x \in N_{L(\sqrt[p]{a})/L}(L(\sqrt[p]{a})^*)$ such that $cx^{-1} \in W$, and this element satisfies our requirements.

Now suppose $c \in L^*$ satisfies (3), and moreover, $b = N_{L/F}(c)$ belongs to $\Omega_2(= F^* \cap U)$. If p divides μ_v, then

$$[a, b]_v = \prod_{w|v} \{a, c\}_w;$$

otherwise, $[a, b]_v = 1$. It follows that the product on the left-hand side of (2) is equal to $\theta_{v_2}(\zeta_p)$. But this product must be 1, and we conclude that $\theta_{v_2} = 1$. The proposition is proved.

References

[AT] E. Artin and J. Tate: *Class Field Theory.* Benjamin, New York, 1974

[B] A. Bak: *Le problème de sous-groupes congruence et le problème métaplectique pour le groupes classiques de rang > 1.* C.R. Acad. Sci. Paris, **292** (1981), 307-310

[BR] A. Bak and U. Rehmann: *The congruence subgroup and metaplectic problems for $SL_{n\geq 2}$ of division algebras.* J. Algebra, **78** (1982), 475-547

[BoT1] A. Borel and J. Tits: *Groupes reductifs.* Publ. Math. I.H.E.S., **27** (1965), 55-150

[BoT2] A. Borel and J. Tits: *Complements à l'article "Groupes reductifs".* Publ. Math. I.H.E.S., **41** (1972), 253-276

[Bu] N. Bourbaki: *Groupes et algèbres de Lie, Chap. 4-6.* Hermann, Paris, 1968

[CF] J. W. S. Cassels and A. Fröhlich (editors), *Algebraic number theory* (Proc. Instructional Conf., Brighton, 1965), Academic Press, London, and Thompson, Washington, D.C., 1967

[D] V. Deodhar: *On central extensions of rational points of algebraic groups.* Amer. J. Math., **100** (1978), 303-386

[Ha] G. Harder: *"Uber die Galoiskohomologie halbeinfacher algebraischer Gruppen.* J. reine und angew. Math., **274-275** (1975), 125-138

[H] S. Helgason: *Differential Geometry and Symmetric Spaces.* Academic Press, New York, 1962

[KPa] D. A. Kazhdan and S. J. Patterson: *Metaplectic Forms.* Publ. Math. I.H.E.S., **59** (1984), 35-142

[Kl] J. Klose: *Metaplektische Erweiterungen von Quaternionenschiefkörpern.* Math. Z., **193** (1986), 625-649

[L] M. Lazard: *Groupes analytiques p-adiques.* Publ. Math. I.H.E.S. **26** (1965), 5-219

[Lu] A. Lubotzky: *Subgroup growth and congruence subgroups.* Invent. Math. **119** (1995), 267-295

[M1] G. A. Margulis: *Finiteness of quotient groups of discrete groups.* Funct. Anal. Appl., **13** (1979), 178-187

[M2] G. A. Margulis: *On the multiplicative group of a quaternion algebra over a global field.* Soviet Math. Dokl., **21** (1980), 780-784

[Mc] G. W. Mackey: *Les ensembles Borélien et les extensions des groupes.* J. Math. Pures Appl. **36** (1957), 171-178

[Ma] H. Matsumoto: *Sur les sous-groupes arithmétiques des groupes semi-simples déployés.* Ann. Sci. École Norm. Sup. **2** (1969), 1-62

[Mo] C. Moore: *Group extensions of p-adic and adelic linear groups.* Publ. Math. I.H.E.S. **35** (1968), 157-222

[PR1] V. P. Platonov and A. S. Rapinchuk: *On the group of rational points of three-dimensional groups.* Soviet Math. Dokl., **20** (1979), 693-697

[PR2] V. P. Platonov and A. S. Rapinchuk: *Algebraic Groups and Number Theory* , "Pure and Applied Mathematics" series, Vol. 139, Academic Press, New York, 1993

[PR3] V. P. Platonov and A. S. Rapinchuk: *Abstract properties of S-arithmetic groups and the congruence subgroup problem.* Russian Acad. Sci. Izv. Math., **40**(1993), 455-476

[Pi] R. Pierce: *Associative Algebras.* Springer Verlag, Heidelberg, 1982

[Pr1] G. Prasad: *A variant of a theorem of Calvin Moore.* C.R. Acad. Sci. Paris, **302** (1986), 405-408

[Pr2] G. Prasad: *Computation of $H^2(SL_1(D), \mathbf{R}/\mathbf{Z})$.* In preparation

[PrRa1] G. Prasad and M. S. Raghunathan: *On the congruence subgroup problem: Determination of the metaplectic kernel.* Invent. Math. **71** (1983), 21-42

[PrRa2] G. Prasad and M. S. Raghunathan: *Topological central extensions of semi-simple groups over local fields.* Ann. Math. **119** (1984), 143-268

[PrRa3] G. Prasad and M. S. Raghunathan: *On the Kneser-Tits problem.* Comment. Math. Helv. **60** (1985), 107-121

[PrRa4] G. Prasad and M. S. Raghunathan: *Topological central extensions of $SL_1(D)$.* Invent. Math. **92** (1988), 645-689

[Ra1] M. S. Raghunathan: *Torsion in Cocompact Lattices in coverings of* $\mathbf{Spin}(2, n)$. Math. Ann. **266** (1984), 403-419

[Ra2] M. S. Raghunathan: *On the group of norm 1 elements in a division algebra.* Math. Ann. **279** (1988), 457-484

[Ra3] M. S. Raghunathan: *The congruence subgroup problem.* Proc. Hyderabad Conf. on Alg. Groups (ed. by S.Ramanan with the cooperation of C. Musili and N. M. Kumar.) Manoj Prakashan, 1991, 465-494

[R1] A. S. Rapinchuk: *Multiplicative arithmetic of division algerbras over number fields and the metaplectic problem.* Math. USSR Izvestiya, **31** (1988), 349-379

[R2] A. S. Rapinchuk: *Combinatorial theory of arithmetic groups.* Preprint of the Institute of Mathematics, Acad. Sci. of Belarus (Minsk), No 20 (420), 1990

[R3] A. S. Rapinchuk: *Congruence subgroup problem for algebraic groups: old and new.* Astérisque, **209** (1992), 73-84

[Ri] C. Riehm: *The norm 1 group of $\mathfrak{p}$-adic division algebra.* Amer. J. Math. **92** (1970), 499-523.

[S1] J-P. Serre: *Cohomologie Galoisienne.* Lect. Notes Math. No **5**, Springer Verlag, Heidelberg, 1994

[S2] J-P. Serre: *Corps Locaux.* Hermann, Paris (1969)

[S3] J-P.Serre: *Lie Algebras and Lie Groups.* Lect. Notes Math. No **1500**, Springer Verlag, Heidelberg, 1992

[Sc] W. Scharlau: *Quadratic and hermitian forms.* Springer Verlag, Heidelberg, 1985

[Su] B. Sury: *Congruence subgroup problem for anisotropic groups over semi-local rings.* Proc. Indian Acad. Sci., **101** (1991), 87-110

[Th] R. G. Thompson: *Commutators in the special and general linear groups.* Trans. Amer. Math. Soc. **101** (1961), 16-33

[Ti] J. Tits: *Classification of algebraic semisimple groups.* Algebraic Groups and Discontinuous Subgroups, Proc. Symp. Pure Math., vol. **9** , Amer. Math. Soc., Providence, R.I., 1966, 33-62

[T] D. Toledo: *Projective varieties with non-residually finite fundamental group.* Publ. Math. I.H.E.S., **77** (1993), 103-119

[To] G.Tomanov: *On Grunwald-Wang's theorem.* J. reine und angew. Math. **389** (1988), 209-220

[W] B. Weisfeiler: *Semi-simple algebraic groups splitting over a quadratic extension.* Math. USSR Izvestiya **5** (1971), 57-73

[Wi] D. Wigner: *Algebraic cohomology of topological groups.* Trans. A.M.S., **178** (1973), 83-93

G. P.
Department of Mathematics
University of Michigan
Ann Arbor MI 48109-1003
USA
e-mail: gprasad@math.lsa.umich.edu

A. R.
Current address:
Fakultät für Mathematik
Universität Bielefeld
Postfach 10 01 31 33615 Bielefeld
Germany
e-mail: rapin@mathematik.uni-bielefeld.de

Permanent address:
Institute of Mathematics
Academy of Sciences of Belarus
ul.Surganova 11
Minsk 220072
Belarus