Math. Ann. 266, 403–419 (1984)

Mathematische Annalen

Torsion in Cocompact Lattices in Coverings of Spin(2, *n*)

M. S. Raghunathan*

Institut des Hautes Etudes Scientifiques, 35, route de Chartres, F-91440 Bures-sur-Yvette, France

Introduction

Let G be a connected semisimple Lie group with *finite* centre. If G is *linear* and Γ is any *finitely generated* subgroup of G, then it is well known that Γ admits a torsion-free subgroup of finite index. In particular, this is so if Γ is a *lattice* in G. The last assertion fails for certain lattices if G is not linear as was shown by Millson [6]. Deligne devised a general method for deciding when an "arithmetic" lattice in a finite covering of a linear group admits a torsion free subgroup of finite index. He used this method together with available information on the congruence subgroup problem to exhibit further examples of arithmetic lattices which admit no torsion free subgroups of finite index. Deligne's as well as Millson's examples are of lattices which are *not cocompact*. In the present paper we will apply Deligne's ideas to the case of lattices in a covering group $\tilde{\mathscr{G}}$ of the group Spin$(2,n)$, the *real* spin group of a quadratic form of signature $(2,n)$. The necessary ingredients for doing this are provided partially by Kneser [3] and Margulis [5]; these deep results combined with the results of Prasad and Raghunathan [8, 9] enable us to obtain the required information on the (necessarily arithmetic) lattices in question with the help of some abelian class field theory. The main result of the paper is

Main Theorem. *Let $\tilde{\mathscr{G}}$ be the universal covering of* Spin$(2,n)$, *n an odd integer, the spin group of a quadratic form of signature* $(2,n)$. *Let $\tilde{\Gamma}\subset\tilde{\mathscr{G}}$ be any lattice and π_1 ($\simeq\mathbb{Z}$) the kernel of the map $\tilde{\mathscr{G}}\to$* Spin$(2,n)$. *Then $\tilde{\Gamma}\supset 8\pi_1$. In particular, if $\mathscr{G}$ is any finite covering of* Spin$(2,n)$ *of order not dividing* 8, *then $\mathscr{G}_1$ admits no torsion-free lattice.*

Throughout this paper we will deal exclusively with *cocompact* lattices. For non-cocompact lattices Deligne's methods generalize in a straight forward manner in the light of the extensive available information on the congruence subgroup problem [8, 9].

---

* Permanent address: Tata Institute of Fundamental Research, Homi Bhabha Road, 400005 Bombay, India

A brief indication of the method of proof follows. Let k be a numberfield and ∞ its set of archimedean valuations. Let G be a connected simply connected semisimple k-group. Let $\hat{G}(a)$ [resp. $\hat{G}(c)$] denote the completion of $G(k)$ with respect to the family of arithmetic (resp. congruence) subgroups. The k-group G has CSP iff $\hat{G}(a)$ is a central extension of $\hat{G}(c)$. Let $G(\mathbf{A})$ denote the adéle group of G and $M(G)$ the kernel of the restriction homomorphism $H^2(G(A)) \to H^2(G(k))$: the cohomology groups are based on continuous cochains and have coefficients in $\mathbf{T}=\mathbf{R}/\mathbf{Z}$. For $v \in \infty$, k_v denotes the completion of k at v and let G_∞ denote the product of all those $G(k_v)$, $v \in \infty$, which are *not* compact and simply connected. Let $\tilde{G}_\infty$ denote the universal covering of G_∞ and π_1 the kernel of $p: \tilde{G}_\infty \to G_\infty$. With this notation Deligne has proved the following: if G has CSP, there is a homomorphism $\lambda_G: \pi_1 \to \mu(G)$ [= the dual of $M(G)$] such that any lattice $\tilde{\Gamma} \subset \tilde{G}_\infty$ with $p(\tilde{\Gamma})$ an arithmetic subgroup of G_∞ contains the kernel of λ_G. Suppose now that $\mathscr{G}$ is the real Lie group $\mathrm{Spin}(2, n)$, $n \geqq 3$, viz., the spin group of a quadratic form over $\mathbf{R}$ with n positive and 2 negative eigenvalues and $\tilde{\mathscr{G}}$ its universal covering (the fundamental group of $\mathscr{G}$ is isomorphic to $\mathbf{Z}$). Let $\tilde{\Gamma} \subset \tilde{\mathscr{G}}$ be any lattice in $\tilde{\mathscr{G}}$. Then by a theorem of Margulis [1], there is a numberfield $k = k(\tilde{\Gamma})$ with a real valuation v and a k-group $G = G(\tilde{\Gamma})$ such that $G(k_w)$ is compact (and simply connected) for $w \in \infty - \{v\}$ and there is an isomorphism of $\mathscr{G}$ on $G(k_v)$ which takes the image of $\tilde{\Gamma}$ into an arithmetic subgroup of $G(k_v)$. If we make the further hypothesis that n is odd, then one knows that G is necessarily the spin group of a quadratic form over the field k [13]. Now Kneser [3] has shown that such a G has CSP. So we conclude from the theorem of Deligne cited above that for each $\tilde{\Gamma}$, there is a homomorphism

$$\lambda_{G(\tilde{\Gamma})}: (\mathbf{Z})\pi_1(\mathscr{G}) \to \mu(G(\tilde{\Gamma}))$$

whose kernel is contained in $\tilde{\Gamma}$. It suffices then to show that $\mu(G(\tilde{\Gamma}))$ has exponent dividing 8. We prove in fact a more general result.

> Let k be a numberfield and G the spin group of a quadratic form over k in at least five variables. Let N be the order of the group of roots of unity in k. Then $4 \cdot N \cdot M(G) = 0$.

Note that $N=2$ when $k = k(\tilde{\Gamma})$: it admits a real valuation.

The general result on $M(G)$ above is reduced to proving two weaker statements on 3 dimensional groups with the aid of cohomological computations made in [8, 9]. The first of these results is reduced using the work of Moore [14] to a problem on algebraic numberfields which is solved by using some (abelian) class field theory. The second is an assertion about real semisimple groups which is handled by differential geometric methods.

1. The Metaplectic Kernel and a Theorem of Deligne

1.1. Let k be a global field and V its set of valuations. For $v \in V$, let k_v be the completion of k with respect to v, f_v the residue field of k_v, p_v the characteristic of f_v and μ_v the group of roots of unity in k_v^*. If S is a finite subset of V, we denote by $A(S)$ the S-adele ring of k. Let G be a connected, simply connected, semisimple algebraic group over k and for $v \in V$, let $G(k_v) = G_v$. For S as above let $G_S = \pi_{v \in S} G_v$ and $\bar{G}(S)$ the S adele group $G(A(S))$ of G. Let $\mathbf{T}$ be the compact topological group $\mathbf{R}/\mathbf{Z}$ and for any locally compact group B, let $H^2(B)$ denote the second cohomology group of B with coefficients in $\mathbf{T}$ (for the trivial action of B) based on continuous cochains. For each $v \notin S$, the inclusion $G_v \to \bar{G}(S)$ induces a restriction homomorphism r_v of $H^2(\bar{G}(S))$ in $H^2(G_v)$ leading to a homomorphism

$$h: H^2(\bar{G}(S)) \to \Pi_{v \notin S} H^2(G_v).$$

It is proved in [9, Theorem 2.4] that if G is isotropic at all nonarchimedean v not in S, h is an isomorphism. It is also shown there that for each $v \notin S$, the group G_v admits a universal locally compact central extension $\varrho_v: \tilde{G}_v \to G_v$ with kernel denoted $\pi_1(G_v)$, a discrete group and there is a natural isomorphism of the dual $\mathrm{Hom}(\pi_1(G_v), \mathbf{T})$ on $H^2(G_v)$. Moreover, the group $\bar{G}(S)$ admits also a universal locally compact central extension $\varrho: \tilde{\bar{G}}(S) \to \bar{G}(S)$ and we have natural maps $\tilde{G}_v \to \tilde{\bar{G}}(S)$ for $v \notin S$ making the diagram

$$\begin{array}{ccc} \tilde{G}_v & \to & \tilde{\bar{G}}(S) \\ \downarrow & & \downarrow \\ G_v & \to & \bar{G}(S) \end{array}$$

commutative and inducing an isomorphism of the direct sum

$$\coprod_{V \notin S} \pi_1(G_v) \simeq \pi_1(\bar{G}(S)) \quad \left(\overset{\text{def}}{=} \text{kernel } \varrho\right).$$

The group $H^2(\bar{G}(S))$ is then evidently dual to $\pi_1(\bar{G}(S))$ under Pontrjagin duality.

1.2. Suppose now that $G(k)$ is *perfect*. Then $G(k)$ admits a universal (discrete) central extension $p: \tilde{G}(k) \to G(k)$ whose kernel is denoted $\pi_1(G(k))$ and we have a natural map: $\pi_1(G(k)) \to \pi_1(\bar{G}(S))$. We denote the cokernel of this map by $\mu(S, G)$. Now from the fact that $\pi_1(G(S))$ is the direct sum of the groups $\pi_1(G(k_v))$ each of which is discrete (in fact finite cyclic of order $|\mu_v|$ or $|\mu_v|/2$: Prasad-Raghunathan [8]) one sees easily that $\mu(S, G)$ is in duality (under Pontrjagin pairing) with the group $M(S, G) =$ kernel of the restriction map $H^2(\bar{G}(S)) \to H^2(G(k))$ induced by the diagonal inclusion of $G(k)$ in $\bar{G}(S)$. In the sequel $M(S, G)$ will be called the *S-metaplectic* kernel of G. When $S = \phi$, we set $\bar{G} = \bar{G}(\phi) = G(A(\phi))$, $M(G) = M(\phi, G)$, and $\mu(G) = \mu(\phi, G)$. The assumption that $G(k)$ is perfect implies that G_v is perfect for all $v \in V$ and hence that G is isotropic over k_v for all non-archimedean v (one expects that the converse is also true but so far only partial results are available: Kneser [3], Platanov-Rapinčuk [7], and Raghunathan [11]).

1.3. Suppose now that $\infty \subset S$. Let $T_S(a)$ [resp. $T_S(c)$] be the topological group structure on $G(k)$ defined by stipulating that the family of S-arithmetic (resp. S congruence) subgroups constitute a fundamental system of neighbourhoods of the identity. We denote by $\hat{G}(S, a)$ [resp. $\hat{G}(S, c)$] the completion of $G(k)$ with respect to $T_S(a)$ [resp. $T_S(c)$]. The group $\hat{G}(S, a)$ is an extension of $\hat{G}(S, c)$ by a profinite group $C(S, G)$ which we call the S-congruence kernel. We will say that G has the S-congruence subgroup property – *SCSP* for short – if $C(S, G)$ is central in $\hat{G}(S, a)$. If $G(k)$ is *perfect*, the group G_S admits a universal central extension $\tilde{G}_S$ and the inclusion $G_S \to \bar{G}$ induces a natural inclusion

$$\pi_1(G_S) \to \pi_1(\bar{G}),$$

where the group $\pi_1(G_S)$ is the kernel of the covering projection

$$\varrho_S : \tilde{G}_S \to G_S \,.$$

Composing with the map $\pi_1(\bar{G}) \to \mu$ $[=\mu(\phi, G)]$ we obtain a homomorphism

$$R_S : \pi_1(G_S) \to \mu \,.$$

The following result is due to Deligne [1].

1.4. Theorem. *Assume that $G(k)$ is perfect and that G has SCSP. Let $p_S : \tilde{G}_S \to G_S$ be the universal covering of G_S and $\Gamma \subset \tilde{G}_S$ a (discrete) subgroup commensurable with $p_S^{-1}(\Phi)$, where Φ is any S-arithmetic subgroup in G_S. Then Γ contains kernel R_S.*

We remark that Deligne does not formulate the result in the above form but his proofs go through in the light of the comments made in the earlier paragraphs. We will be mainly interested in applying this theorem to certain anisotropic Spin groups. Kneser [3, 4] has shown the following:

Let k be a number field and E a vector space of dimension $n \geqq 5$ over k and q a quadratic form on E. Let S be such that we have

$$\sum_{v \in S} (\textit{Witt-index of } q \textit{ at } v) \geqq 2 \,.$$

Then Spin$(q)(k)$ *is perfect and* Spin$q$ *has SCSP.*

Actually our interest in the sequel will be limited to the case of Spin groups of the above kind with $S = \infty$ and such that for at all but one archimedean valuation v_0, q is anisotropic.

2. Finiteness of the Metaplectic Kernel

We continue with notations introduced in Sect. 1. Our aim in this section is to prove the following

2.1. Theorem. *$M(S, G)$ is a torsion group. If G is isotropic at k_v for all $v \notin S$ or if* char$k=0$, *$M(S, G)$ is finite.*

In Prasad and Raghunathan [9, Theorems 2.10 and 3.4] it is shown that $M(S, G)$ is finite if G is isotropic over k or $S \supset \infty$, G is isotropic at v for all $v \notin S$ *and* $\sum_{v \in S} k_v\text{-rank } G \geqq 2$. Now if v is non-archimedean and G is isotropic at k_v then $H^2(G(k_v))$ is finite [8]. It follows that $M(S, G)$ is finite if $S \supset \infty$ and G is isotropic at v for all $v \in S$. Now when G is anisotropic at v and v is non-archimedean G_v is compact and $H^2(G_v)$ is a torsion group and in fact $H^i(G_v)$, $i=1,2$, are finite if char$k=0$ [10, Theorem 4.10]. This leaves out for our consideration only the case when $S \supset \infty$, G is anisotropic over k (and k is of characteristic 0). We may assume $S = \phi$ as $M(S, G)$ has a natural inclusion in $M(G)$. Let $r : H^2(\bar{G}) \to H^2(G_\infty)$ denote the projection induced by the inclusion of G_∞ in $\bar{G}$. It is clear then that the kernel of r restricted to $M(G)$ is precisely $M(\infty, G)$. It is therefore sufficient to show that the image of $M(G)$ in $H^2(G_\infty)$ is finite. Suppose now that U is a compact open subgroup of $\bar{G}(\infty)$. According to Raghunathan [10, Theorem 5.2], $H^2(U)$ is *finite*.

Since U is profinite, it admits an open compact subgroup U' such that for all $\chi_U \in H^2(U)$, χ_U restricts to zero on U'. Let $\Gamma = G(k) \cap U'$. Then we have the following commutative diagram

$$\begin{array}{ccc} \Gamma & \rightarrow & G(k) \\ \downarrow & & \downarrow \\ G_\infty \times U' & \rightarrow & \bar{G} \simeq G_\infty \times \bar{G}(\infty). \end{array}$$

Moreover, $H^2(\bar{G}) \simeq H^2(G_\infty) \times H^2(\bar{G}(\infty))$ as G_∞ is perfect. The map $H^2(\bar{G}) \rightarrow H^2(\Gamma)$ thus factors through $G_\infty \times U'$ and as any $\chi \in M(G)$ is zero on U', we see that χ_∞ the restriction of χ to G_∞ must be trivial on Γ. Since G is anisotropic over k, G_∞/Γ is compact and it suffices therefore to prove the following proposition in order to complete the proof of the theorem.

2.2. **Proposition.** *Let $\mathscr{G}$ be a connected linear semisimple Lie group and Γ a discrete subgroup such that $\mathscr{G}/\Gamma$ is compact. Then the map $H^2(\mathscr{G}) \rightarrow H^2(\Gamma)$ has a finite kernel.*

We consider the action of both $\mathscr{G}$ and Γ on $\mathscr{G}$ by right translations. Then according to van Est [2] there is a spectral sequence E_r^{pq} abutting on the Lie algebra cohomology of $\underline{g}$ = Lie algebra of $\mathscr{G}$, and with $E_2^{pq} \cong H^p(\mathscr{G}, H_t^q(\mathscr{G}, \mathbf{R}))$, the p^{th} cohomology group of $\mathscr{G}$ based on continuous cochains with coefficients in $H_t^q(\mathscr{G}, \mathbf{R})$, the q^{th} cohomology group of $\mathscr{G}$ as a topological space with coefficients in $\mathbf{R}$. Moreover, we have a natural map of this spectral sequence into the Cartan Leray spectral sequence $'E_2^{pq} = H^p(\Gamma, H_t^q(\mathscr{G}, \mathbf{R}))$ of the covering projection $\varrho: G \rightarrow G/\Gamma$ which abuts to $H_t^*(\mathscr{G}/\Gamma, \mathbf{R})$. Now $H^i(\underline{g}, \mathbf{R}) = 0$ for $i = 1, 2$ leading us to an isomorphism.

$$\begin{array}{ccccccc} 0 & \rightarrow & H_t^1(\mathscr{G}, \mathbf{R}) & \simeq & H^2(\mathscr{G}, \mathbf{R}) & \rightarrow & 0 \\ \wr\!| & & \wr\!| & & \wr\!| & & \wr\!| \\ H^1(\underline{g}, \mathbf{R}) & & E_2^{01} & \rightarrow & E_2^{20} & & H^2(\underline{g}, \mathbf{R}). \end{array} \qquad (*)$$

From the spectral sequence $'E_r$ we obtain the following exact sequence:

$$H_t^1(\mathscr{G}/\Gamma, \mathbf{R}) \xrightarrow{\varrho^*} H_t^1(\mathscr{G}, \mathbf{R}) \longrightarrow H^2(\Gamma, \mathbf{R}), \qquad (**)$$

where ϱ^* is the map induced by ϱ. We will presently establish the following

2.3. **Claim.** *ϱ^* is the trivial map.*

We first complete the proof of Proposition 2.2 assuming the claim. It is immediate from the claim and the sequence (*) and (**) above $H^2(\mathscr{G}, \mathbf{R}) \rightarrow H^2(\Gamma, \mathbf{R})$ is injective. Let $V = H^2(\mathscr{G}, \mathbf{R})$ and $W = H^2(\Gamma, \mathbf{R})$. Let V_Z (resp. W_Z) denote the kernel of the map $H^2(\mathscr{G}, \mathbf{R}) \rightarrow H^2(\mathscr{G})$ [resp. $H^2(\Gamma, \mathbf{R}) \rightarrow H^2(\Gamma)$]. Evidently, we have a commutative diagram with exact rows and i and j injections

$$\begin{array}{ccccccc} 0 \rightarrow & V_Z & \rightarrow & V & \rightarrow & H^2(\mathscr{G}) \\ & {\scriptstyle i}\downarrow & & {\scriptstyle j}\downarrow & & \downarrow \\ 0 \rightarrow & W_Z & \rightarrow & W & \rightarrow & H^2(\Gamma). \end{array}$$

The map $V \to H^2(\mathscr{G})$ has finite cokernel and V_Z spans V as a real vector space and $W_Z = \operatorname{Image} H^2(\Gamma, Z)$ in W is discrete. It follows that $j(V) \cap W_Z$ contains V_Z as a subgroup of finite index. Hence $j^{-1}(W_Z)/V_Z$ is finite. Since $V \to H^2(\mathscr{G})$ has a finite cokernel, $H^2(\mathscr{G}) \to H^2(\Gamma)$ has a finite kernel.

We have to prove the claim.

2.4. *Proof of Claim 2.3.* Let K be a maximal compact subgroup of $\mathscr{G}$. As $K \to \mathscr{G}$ is a homotopy equivalence we have to show that the map $K \to \mathscr{G}/\Gamma$ induces the trivial map in the first cohomology of these spaces with coefficients in **R** (we have assumed that $K \to \mathscr{G}/\Gamma$ is an inclusion; this is easily secured by assuming that Γ is torsion free – $\mathscr{G}$ is a linear group!). Let $X = K \backslash G$ be the Riemannian symmetric space and $Y = X/\Gamma$. Then $\mathscr{G}/\Gamma \to Y$ is a principal K-fibration. The transgression in this fibration takes each non-zero element of $H_t^1(K, \mathbf{R})$ $(= E_2^{01})$ into a second cohomology class in $H_t^2(Y, \mathbf{R})$ $(= E_2^{20})$ which is represented by a non-zero $\mathscr{G}$*-invariant* form on X projected to Y. This is easily seen by a comparison with the compact dual; and such a form is harmonic, hence is non-zero in cohomology.

3. Lattices in Spin(2, *n*), *n* odd

3.1. In this section $\mathscr{G}$ will denote the real Spin group of a quadratic from $\underline{q}$ in $(n+2) \geqq 5$ variables with Witt-index 2 and n is assumed *odd*. The pairity condition on n has the following consequence: if k is a number field with a valuation v such that $k_v \simeq \mathbf{R}$ and G is a (simply connected) k-algebraic group with $\mathscr{G} \simeq G(k_v)$, then G is necessarily the Spin group $\operatorname{Spin} q$ of a quadratic form q over k which, over k_v, is equivalent to $\underline{q}$: this is known from the classification of algebraic groups [13]. In view of this the arithmetricity of lattices in $\mathscr{G}$ proved by Margulis [5] has the following formulation. Given a cocompact lattice $\Gamma \subset \mathscr{G}$, there is a totally real number field $k = k(\Gamma)$, an archimedean valuation $v = v(\Gamma)$ of k and an anisotropic quadratic form $q = q(\Gamma)$ in $(n+2)$-variables on k with the following properties:

(i) $k_v \simeq \mathbf{R}$.

(ii) If $v' \neq v$ is archimedean, q is anisotropic over $k_{v'}$,

(iii) Over k_v $(\simeq \mathbf{R})$, q is equivalent to $\underline{q}$.

(iv) The equivalence of q and $\underline{q}$ over **R** may be so chosen that under the induced isomorphism $\mathscr{G} \simeq \operatorname{Spin} q(k_v)$, Γ maps into a subgroup of $\operatorname{Spin} q(k_v)$ which is commensurable with an arithmetic subgroup of $\operatorname{Spin} q(k_v)$.

3.2. *Remark.* As $(n+2) \geqq 5$, we note that the Hasse-principle implies that $k(\Gamma)$ above cannot be **Q**.

3.3. The fundamental group $\pi_1(\mathscr{G})$ of $\mathscr{G}$ is isomorphic to **Z**. Let $r: \tilde{\mathscr{G}} \to \mathscr{G}$ be the universal covering. We identify $\pi_1(\mathscr{G})$ with kernel r. If $\Phi \subset \tilde{\mathscr{G}}$ is a cocompact lattice, $r(\Phi)$ is a cocompact lattice in $\mathscr{G}$ and hence determines a (totally real) number field k, a (real) valuation of v of k and a quadratic, form q as above [all depending on $r(\Phi)$]. According to Theorem 1.4, there is a homomorphism $\lambda: \pi_1(\mathscr{G}) \to M(\operatorname{Spin} q)$ such that Φ contains kernel λ [λ depends on the k-group $\operatorname{Spin} q$ but not on the arithmetic lattice $r(\Phi)$]. Since $\pi_1(\mathscr{G})$ is *cyclic* to prove the main result it suffices to show that $8M(\operatorname{Spin} q) = 0$ for any q as above. We have in fact the following more general result.

3.4. **Theorem.** *Let k be a number field and q a quadratic form on a k-vector space E with* $\dim E \geqq 5$. *Let μ_k be the group of roots of unity in k and $N = |\mu_k|$. Then* $4N(M(\mathrm{Spin}\, q)) = 0$.

3.5. In the sequel we denote by G the group Spin$q$. Let $x \in H^2(G)$ be such that $z = 4Nx \neq 0$. If x is a torsion free element, then according to Theorem 2.1, x has a non-zero restriction to $G(k)$. We will, therefore, assume that x is a torsion element. Let p be any prime and p^t the highest power of p dividing μ_k we may assume then that x is a p-torsion element such that $4p^t x \neq 0$ while $4p^{t+1}x = 0$. Under this assumption we will show that x restricts to a non-zero element on $G(k)$. Let $V(x) = \{v \in V | 4p^t x_v \neq 0\}$ (here x_v is the restriction of x to G_v). Evidently, $V(x)$ is non-empty. We will now choose a 3-dimensional non-degenerate-for-q k-subspace $E(x)$ of E as follows. If $V(x)$ contains a non-archimedean place w, $q(x)$, the restriction of q to $E(x)$ is anisotropic at all real archimedean places and isotropic at w as well as at all $v \in V - \infty$ with $p_v = p$. If $V(x) \subset \infty$, $q(x)$ is assumed to be anisotropic at all but one $w \in \infty$ with $w \in V(x)$ and the natural map of Spin$q(x)(k_v)$ in $G(k_v)$ induces in the fundamental groups a homomorphism whose cokernel has order 2. Such a choice of $E(x)$ is possible as is seen easily from the density of $E(k)$ in any finite product of the $E(k_v)$. The choice of $E(x)$ as above is motivated by.

3.6. **Lemma.** *If $E(x)$ is chosen as above the element x in $H^2(\bar{G})$ restricts to a non-zero element y in $H^2(\bar{H})$, where $H = \mathrm{Spin}\, q(x)$ is considered as a subgroup of G for the natural inclusion. Moreover, if $V(x) \not\subset \infty$, $p^t y_v = 0$ for $v \in \infty$ and $2p^t y_w \neq 0$ (w as above). If $V(x) \subset \infty$, there is a unique $w \in \infty$ such that $2p^t y_v \neq 0$ for $v \in V$ if and only if $v = w$.*

Proof. In the case when $V(x) \subset \infty$ this is immediate from our choice of $E(x)$. Assume then that $V(x) \not\subset \infty$. In this case the result is an easy consequence of [8, Theorem 9.5]. According to that theorem we have the following: let B be a maximal k_w-split torus in G and Φ the k_w-root system of G with respect to B. Let d be a dominant root in Φ for some ordering on the character group of B. Let $G(d)$ denote the k_w-rank 1, k_w-subgroup of G determined by d. Then $H^2(G_w) \to H^2(G(d)_w)$ is injective. Now suppose first that k_w-rank $G \geqq 2$ (this is the case always if $\dim E \geqq 7$). Then $G(d) \pm SL_2$ over k_w. Let E' be a k_w-subspace of E of dimension 5 containing $E(x)$ and G' the Spin group of q', the restriction of q to E'. We assume that q' is non-degenerate and has Witt-index $\geqq 2$. Then it is easy to see that Spinq' contains a conjugate (over k_w) of $G(d)$. Consequently, the restriction map $H^2(G_w) \to H^2(\mathrm{Spin}\, q'(k_w))$ is injective. Now Spin$q' = G'$ is a split group of type B_2 ($= C_2$) and Spin$q(x)$ is the subgroup k_w-isomorphic to SL_2 corresponding to a short root in this root system. From the work of Moore [14] one knows that $H^2(G'_w) \to H^2(\mathrm{Spin}\, q(x)_w)$ has a kernel of order 2. This proves the lemma when k_w-rank $G \geqq 2$; when the k_w-rank is 1, $\dim E = 5$ and we know from [8, Proposition 8.44] that if $E' \supset E(x)$ is a suitable 4-dimensional subspace and q' the restriction of q to E', $H^2(G_w) \to H^2((\mathrm{Spin}\, q')_w)$ is injective. Now Spin$q' \simeq R_{K/k_w} SL_2$ over k_w for a quadratic extension K of k_w; from the work of Moore [1] (see also [8, Sect. 5.4]) the map $SL_2 \to R_{K/k_w} SL_2$ induces in H^2 a map with kernel of order 2; and Spin$q \to$ Spinq' can be identified under a suitable isomorphism with this inclusion. This proves the lemma.

Lemma 3.6 now reduces the problem to the following two results on 3-dimensional groups: note that the Spin group in 3 variables is a 3-dimensional group: it is either isomorphic to SL_2 or the group $SL_{1,D}$ of elements of reduced norm 1 in a quaternion division algebra.

3.7. **Theorem.** *Let D be a quaternion division algebra over k which is anisotropic at every real place of k and split at all k_v with v finite and $p_v = p$ a fixed prime. Let G be the k-group $SL_{1,D}$ and $\chi \in H^2(\bar{G})$ be such that the following holds: there is a $w \in V - \infty$ at which D is split and $2p^t\chi_w \neq 0$ while $p^{t+1}\chi = 0$ or $2p^{t+1}\chi = 0$ according as p is odd or $p = 2$. Then χ restricts to a non-zero element in $H^2(G(k))$. (Recall that p^t is the highest power of p dividing $|\mu_k|$.)*

3.8. **Theorem.** *Let G be a 3-dimensional simply connected semisimple group over k and v an archimedean valuation. Then the map $H^2(G_v) \to H^2(G(k))$ is injective.*

4. Proof of Theorem 3.7

4.1. The notations are those of Theorem 3.7. Let ζ be a primitive p^tth root of unity in k and $l = k(\zeta^{1/p})$. Let K be a quadratic extension of k contained in D with the following properties: For $v = w$ or $p_v = p$, K imbeds in k_v and K is linearly disjoint from l. To see that such a K exists we argue as follows. Let Ω be the (finite) collection of all quadratic subfields of l. For each $l' \in \Omega$ pick $v(l')$ in $V - \infty$ distinct from w and the v with $p_v = p$ such that l' is linearly disjoint from $k_v(l')$ (Čebotarev's approximation theorem) and D splits over $k_{v(l')}$. We will also assume that $v(l') \neq v(l'')$ if $l' \neq l''$. Then using weak approximation one sees that we can find K such that $K \otimes_k k_v \simeq k_v \times k_v$ if $v = w$ or if $p_v = p$ while for each $l' \in \Omega$, $K \otimes_k k_{v(l')} \simeq k_{v(l')} \times k_{v(l')}$. Thus there exists a quadratic subfield $K \subset D$ with the required properties.

We will need

4.2. **Lemma.** *Let $v \in V$ be a non-archimedean with $p_v \neq p$. Let M_v be a maximal compact subgroup of G_v. Then $H^2(M_v)$ has no p-torsion.*

Proof. G_v is either isomorphic to $SL_2(k_v)$ or the group D_v^1 of reduced norm 1 elements in D_v, a division algebra. In the former case M_v may be identified with $SL_2(O_v)$(O_v ring of integers in k_v); in the latter case $M_v = D_v^1$. Let N_v be the normal subgroup $\{x \in SL_2(O_v) | x \equiv 1 \bmod \pi\}$ if $M_v \simeq SL_2(O_v)$, $\pi \in O_v$ a uniformizing parameter, while $N_v = \{x \in D_v^1 | x \equiv 1 \bmod \pi\}$, π a uniformizing parameter in D_v if D_v is a division algebra. Then N_v is a pro-p_v-group. Further, $M_v/N_v \simeq SL_2(f_v)$ or M_v/N_v is cyclic accordings as $M_v \simeq SL_2(O_v)$ or $M_v \simeq D_v$. In either case $H^2(M_v/N_v)$ has no p-torsion (Schur [12] when $M_v/N_v \simeq SL_2(f_v)$; in the other case the group is in fact trivial). Since N_v is a pro-p_v-group $H^i(N_v, E)$ for any continuous N_v-module E is a p_v-torsion subgroup if $i > 0$. The lemma now follows from the Hochschild-Serre spectral sequence for M_v and N_v.

4.3. Let $V' = \{v \in V - \infty | v \neq w,\ p_v \neq p$ and l is linearly disjoint from $k_v\}$. As l is a cyclic extension of k, we know from the Čebotarev approximation theorem that V' is an *infinite* set. Now if $v \in V'$, we claim that $p^t\chi_v = 0$: this is seen as follows: if D does not split at v, this follows from Lemma 4.2; if D splits at v, $G_v \simeq SL_2(k_v)$ and $H^2(SL_2(k_v)) \simeq \mu_v$ and since $v \in V'$, the p-sylow subgroup μ_v is a cyclic group of order

p^t. This proves our contention. Let $S=\{v\in V-\infty | v=w \text{ or } p=p_v\}$. Let $V_1=V'\cup\infty\cup S$ and set

$$\Gamma=\{t\in K^* | t \text{ a unit in } K\otimes_k k_v \text{ for } v\in V_1\}.$$

Also let $K^1=\{t\in K^* | N_{K/k}(t)=1\}$ and $\Gamma^1=\Gamma\cap K^1$. Then we can find a maximal compact subgroup $\prod_{v\in V} M_v$, each M_v a maximal compact subgroup of G_v, such that Γ^1 maps into M_v under the natural inclusion of $G(k)$ in G_v for $v\in V_1$. It follows that the diagonal inclusion of Γ^1 $[\subset G(k)]$ in $\bar{G}$ factors through the subgroup $\prod_{v\in V_1} M_v \times \prod_{v\in V'} G_v \times \prod_{v\in S} G_v \times G_\infty$ (the second factor being a restricted direct product). Since $H^2(M_v)$, $v\in V_1$ has no p-torsion, $H^2(G_\infty)=0$ and $p^t\chi_v=0$ for $v\in V'$, we see that the restriction of $y=p^t\chi$ to Γ^1 is the same as the restriction of $z=\{y_v\}_{v\in S}\in H^2\left(\prod_{v\in S} G_v\right)$ to Γ^1. It suffices therefore to show that the restriction of z to Γ^1 is non-zero. Now the group $K_v^1=\{x\in K_V=K\otimes_k k_v | N_{K_v/k_v}(x)=1\}$ can evidently be identified with the diagonal group in $SL_2(k_v)$ $(=G_v)$ for $v\in S$. Each element y_v, $v\in S$, can be represented be a unique Steinberg-Cocycle c_v' on $G_v=SL_2(k_v)$; the cocycle c_v' has a restriction c_v to K_v^1 which determines c_v'; further, c_v is a bimultiplicative map of K_v^1 in $\mathbf{T}$ satisfying $c_v(a,b)=c_v(b,a)^{-1}$: all this is due to Moore [14]. Now the cohomology group $H^2(\Gamma^1)$ may be identified with the group of all alternating bimultiplicative maps of Γ^1 in $\mathbf{T}$ and the cocycle c_v represents the trivial class if and only if c_v takes values in $\{\pm 1\}\subset\mathbf{T}$. As y_v is a p-torsion class if p is odd and a 4 torsion class if $p=2$, it is immediate that on $\prod_{v\in S} K_v^1 \times \prod_{v\in S} K_v^1$, $c=\prod_{v\in S} c_v$ defines an alternating $\mathbf{T}$-valued bimultiplicative map such that c^2 is not identically equal to 1. Define $u(a,b)=c(a,b)c(b,a)^{-1}=c^2(a,b)$ so that u is non-trivial. Now u factors through $\prod_{v\in S} K_v^1/(K_v^1)^p \times \prod_{v\in S} K_v^1/(K_v^1)^p$. It follows that it suffices to show that we have

$$\Gamma_1\cdot\prod_{v\in S}(K_v^1)^p=\prod_{v\in S} K_v^1.$$

Since $t\to t/\sigma(t)$, $t\in K^*$, maps K^* onto K^1 and extends to a continuous surjection of $\prod_{v\in S} K_v^*$ on $\prod_{v\in S} K_v^1$ (σ here is the Galois-conjugation), we need only establish the following:

4.4 **Proposition.** $\Gamma\cdot\prod_{v\in S}(K_v^*)^p=\prod_{v\in S} K_v^*$.

Proof. Let $\tilde{V}$ denote the set of valuations of K and $S\subset V$ the subset of those valuations $u\in\tilde{V}$ which lie over those in S. For $v\in\tilde{V}$, K_v will denote the completion of K at v. Let I denote the idéle group of K. Let $L=K\otimes_k l$. Then $(L:K)=(l:k)$ by choice and L/K is a *cyclic* extension. Let $B_L\subset I$ denote the open subgroup of finite index in I determined by L under the Artin-reciprocity law. We identify K_v^*, $v\in\tilde{V}$, with the corresponding subgroup of I and let U_v denote the unit group of K_v^*. Let

$B=K^*\cdot\prod_{v\in\tilde{\infty}} K_v^*\cdot\prod_{v\in V-\tilde{\infty}} U_v$ (here $\tilde{\infty}$ denotes the set of archimedean valuations of K). Finally, we set

$$B'=K^*\prod_{v\in\tilde{\infty}} K_v^*\prod_{v\in\tilde{V}-\tilde{S}-\tilde{\infty}} U_v\prod_{v\in\tilde{S}} U_v^p.$$

Clearly, we have $B'\subset B$. Let E be the abelian extension of K corresponding to the subgroup $B'\cap B_L$ of $I: B/B'\cap L\simeq \mathrm{Gal}(E/K)$. Let r denote the natural map $\mathrm{Gal}(E/k)\to\mathrm{Gal}(L/K)$ and set

$$\Omega=\{u\in\mathrm{Gal}(E/K)|r(u) \text{ generates } \mathrm{Gal}(L/K)\}.$$

Then Ω generates $\mathrm{Gal}\,E/K$ so that any $u\in\mathrm{Gal}\,E/K)$ can be written as a product $\pi\sigma_i$ with $\sigma_i\in\Omega$. Now according to Čeboratev's theorem for each i, there is a valuation $v_i\in\tilde{V}-\tilde{S}-\tilde{\infty}$ such that σ_i is the Frobenius at v_i. Since σ_i maps (under r) onto a generator of $\mathrm{Gal}(L/K)$, $v_i\in\tilde{V}'=\{v\in\tilde{V}|v$ lies over a valuation in $V'\}$. Let π_i be a uniformizing parameter in K_{v_i} and let $\alpha=\prod_i \pi_i$ (in the idele group I). Then α maps to u in $I/B'\cap B_L$. Suppose now that $u\in B/B'\cap B_L$; then $\alpha\in B$ so that $\alpha=\lambda\varrho u_0$, where $\lambda\in K^*$, $\varrho\in\prod_{v\in\tilde{\infty}} K_v^*$, and $u_0\in\prod_{v\in\tilde{V}-\tilde{\infty}} U_v$. This means that the principal idele λ is a unit at all $v\in\tilde{V}-\tilde{\infty}$ other than the v_i. Clearly, then, $\lambda\in\Gamma$. As the image of α in $\prod_{v\in\tilde{S}} K_v^*$ is trivial and so is the image of ϱ. Consequently, λ^{-1} and u_0 have the same in image $\left(\prod_{v\in S} U_v\subset\right)\prod_{v\in S} K_v^*$. The homomorphism $\prod_{v\in S} U_v\to B/B'$ is evidently surjective and u may be taken as the image of an element $g\in\prod_{v\in\tilde{S}} U_v$. It is clear then that g and α have the same image in I/B'. Since λ and ϱ are in B', $u_0g^{-1}\in B'$. We conclude that the projection $\bar{u}_0$ of u_0 in $\prod_{v\in\tilde{S}} K_v^*$ is of the form $g\gamma\xi$, $\gamma\in K^*$, $\xi\in\prod_{v\in\tilde{S}} U_v^p$. As g and ξ are units, γ is a unit. Evidently, $\lambda^{-1}\gamma^{-1}$ is in Γ and maps into the same element as g in $\prod_{v\in\tilde{S}} K_v^*/(K_v^*)^p$. This shows that

$$\Gamma\cdot\prod_{v\in\tilde{S}}(K_v^*)^p\supset\prod_{v\in\tilde{S}} U_v.$$

It now suffices to show that for each $v\in\tilde{S}$, Γ contains an element h_v which is a uniformizing parameter in K_v and is a unit at $K_{v'}$, for $v'\in\tilde{S}$, $v'\neq v$. For this let $\pi_v\in K_v^*$ be a uniformizing parameter at v and τ_v its image in the Galois group I/B of the Hilbert classified H. Let s denote the natural map $\mathrm{Gal}\,E/K\to\mathrm{Gal}\,H/K$. Then $\tau_v=\prod_i s(\sigma_i)$ with $\sigma_i\in\Omega$. Each σ_i is the Frobenius at v_i for some $v_i\in V'$ (Čebotarev's theorem). It follows that the ideal in K determined by π_v is equivalent in the ideal class group to a product of prime ideals corresponding to elements in V'. In other words we can find $\lambda\in K^*$ such that $\eta=\lambda\pi_v$ in the idele group has all components $\eta_{v'}$ units for $v'\in\tilde{V}'$. In particular, λ^{-1} is a unit at all $v'\in S-\{v\}$ and it is a uniformizing parameter in K_v. This proves the proposition.

5. Proof of Theorem 3.8

As in Theorem 3.8 let k be a numberfield and k_v its completion with respect to an archimedean valuation v. Let G be a simply connected 3-dimensional semisimple k-algebraic group. Then we have to show that the natural map

$$H^2(G(k_v)) \to H^2(G(k))$$

is injective. If $k_v \simeq \mathbf{C}$ or if G is an anisotropic over k_v ($\simeq \mathbf{R}$), the group $G(k_v)$ is simply connected and consequently $H^2(G(k_v))$ is trivial. Thus, we need only consider the case when $k_v \simeq \mathbf{R}$ and G splits over k_v. In the sequel we will assume this to hold. We denote $G(k_v)$ by $\mathscr{G}$ in the rest of this chapter.

5.2. The main result can be reformulated as follows:
Let

$$1 \to T \to \hat{\mathscr{G}} \xrightarrow{p} \mathscr{G} \to 1 \qquad (*)$$

be locally compact central extension of $\mathscr{G}$ *by* T; *if this extension* (*) *splits over* $G(k)$ *then it splits*. Suppose then that (*) is a central extension and $\tau: G(k) \to \hat{\mathscr{G}}$ is a splitting of (*) over $G(k)$. We observe first that $\hat{\mathscr{G}}$ carries a natural structure of a Lie group making p (real) analytic so that p is in particular a principal analytic fibration with T as fibre. Since $\mathscr{G} = G(k_v) \simeq SL_2(\mathbf{R})$, it is homotopy equivalent to the unit circle and hence all analytic circle fibrations over $\mathscr{G}$ are trivial. We conclude therefore that there is an analytic map $\sigma: \mathscr{G} \to \hat{\mathscr{G}}$ such that $p \circ \sigma$ is the identity map of $\mathscr{G}$. We define now an analytic map $\hat{C}: \mathscr{G} \times \mathscr{G} \to \hat{\mathscr{G}}$ as follows: for $x, y \in \mathscr{G}$, choose elements $\hat{x}, \hat{y} \in \hat{\mathscr{G}}$ such that $p(\hat{x}) = x$, $p(\hat{y}) = y$; then the commutator $[\hat{x}, \hat{y}] \overset{\text{def}}{=} \hat{x}\hat{y}\hat{x}^{-1}\hat{y}^{-1}$ of $\hat{x}$ and $\hat{y}$ depends only on x and y and not on the choice of $\hat{x}$ and $\hat{y}$ and we set $\hat{C}(x, y) = [\hat{x}, \hat{y}]$. Evidently,

$$\hat{C}(x, y) = [\sigma(x), \sigma(y)]$$

so that $\hat{C}$ is *analytic*. Also we denote that if $x, y \in G(k)$, $\hat{C}(x, y) = \tau([x, y])$. Now if (*) splits, it has a unique splitting ϱ, say, and we would have $\hat{C}(x, y) = \varrho([x, y])$: in other words $\hat{C}$ would factor through $C: \mathscr{G} \times \mathscr{G} \to \mathscr{G}$, where for $x, y \in \mathscr{G}$, $C(x, y) = [x, y]$ $(= xyx^{-1}y^{-1})$. We will establish the converse.

5.3. **Lemma.** *If* $\hat{C}$ *factors through* C, *the extension* (*) *is split.*

Proof. Since $\hat{C}$ factors through C, there is a map $\lambda: \mathscr{G} \to \hat{\mathscr{G}}$ such that $\hat{C} = \lambda \circ C$. Suppose $X \subset \mathscr{G}$ is the set of critical values of C, then the restriction of C to $E = \mathscr{G} \times \mathscr{G} - C^{-1}(X)$ is a submersion; consequently, λ would be analytic on $C(E)$ and hence provide an analytic section over $C(E)$ for the map $p: \hat{\mathscr{G}} \to \mathscr{G}$. Now $\hat{C}$ clearly maps $\mathscr{G} \times \mathscr{G}$ into the commutator subgroup $[\hat{\mathscr{G}}, \hat{\mathscr{G}}]$ of $\hat{\mathscr{G}}$; this last group is a connected Lie subgroup whose Lie algebras maps isomorphically onto that of $\mathscr{G}$. Consequently, we have a connected covering group $\tilde{\mathscr{G}} \to \mathscr{G}$ and a continuous bijection $i: \tilde{\mathscr{G}} \to [\hat{\mathscr{G}}, \hat{\mathscr{G}}]$ and a continuous map $\lambda': C(E) \to \tilde{\mathscr{G}}$ such that $\lambda|_{C(E)} = i \circ \lambda'$. Evidently λ' is a section for the covering map $\tilde{\mathscr{G}} \to \mathscr{G}$ over $C(E)$. We will now show that $C(E) = \mathscr{G} - \{\pm 1\}$. Once this is granted the complement of $C(E)$ in $\mathscr{G}$ consists of two points so that the map $\pi_1(C(E)) \to \pi_1 \mathscr{G}$ of fundamental groups is an isomorphism; as the covering $\tilde{\mathcal{G}} \to \mathcal{G}$ is trivial over $C(E)$, it is trivial. Thus to prove Lemma 5.3, we need only show that we have the following

5.4. **Assertion.** *The critical values of C is the set $\{1\}$. Further image $C = \mathcal{G} - \{-1\}$.*

Proof. We identify, as usual, the tangent space at any point to $\mathcal{G}$ (resp. $\mathcal{G} \times \mathcal{G}$) with Lie $\mathcal{G}$, where Lie $\mathcal{G}$ is the Lie algebra of $\mathcal{G}$. With this identification the tangent map $dC_{(g,h)}$ of C at a point $(g,h) \in \mathcal{G} \times \mathcal{G}$ is given by the following: let $X, Y \in$ Lie $\mathcal{G}$; then

$$dC_{(g,h)}(X, Y) = \mathrm{Ad}\, g\{X - \mathrm{Ad}\, h(X) + \mathrm{Ad}\, h(Y - \mathrm{Ad}\, g^{-1}(Y))\}$$

as is seen by a straightforward calculation. It is now easy to see that the orthogonal complement of image $dC_{(g,h)}$ in Lie $\mathcal{G}$ with respect to the Killing form on Lie $\mathcal{G}$ is the space

$$\mathrm{Ad}\, g\, \mathrm{Ad}\, h(\text{centralizer } h \cap \text{centralizer } g^{-1});$$

and centralizer $h \cap$ centralizer $g^{-1} \neq 0$ iff h and g commute i.e. iff $C(g,h) = 1$. This proves the first assertion.

To prove the second assertion we note first that if $u \in \mathcal{G}$ is unipotent, it can be put in upper triangular form and then is easily seen to be a commutator in the upper triangular group itself. On the other hand, if we fix $\lambda \in \mathbf{R}$, $\lambda > 0$ and set $t = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, we have for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{R})$ (i.e. $ad - bc = 1$),

$$\mathrm{trace}\,[t, g] = 2 - bc(\lambda - \lambda^{-1})^2;$$

and we can choose g so that bc takes any given real value. We see therefore that any semisimple element not equal to ± 1 in $SL_2(\mathbf{R})$ has a conjugate which is a commutator and is thus itself a commutator. It is also clear from the above that we may obtain as a commutator any element which is not semisimple but has both eigenvalues equal to (-1) – we need only choose g such that $bc(\lambda - \lambda^{-1})^2 = 4$. [Note that any two such elements are conjugate in $GL(2, \mathbf{R})$ and the commutator set is stable under conjugation in $GL(2, \mathbf{R})$.] Thus we have only to show that -1 is not a commutator in $SL(2, \mathbf{R})$. If $-1 = g \cdot hg^{-1}h^{-1}$ we conclude that g and $-g$ commute with each other and are conjugates. Now this would mean the eigenvalues of g are of the form $(\lambda, -\lambda)$ so that $\lambda^{-1} = -\lambda$, i.e. $\lambda^2 = -1$. In other words after a conjugation one can assume that

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

and then $hg^{-1}h^{-1}$ is necessarily $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. However, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ are not conjugates in $SL_2(\mathbf{R})$; they are conjugates by the permutation matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ which has determinant -1; if they were conjugates in $SL_2(\mathbf{R})$, the centralizer of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in $GL_2(\mathbf{R})$ would contain an element of determinant -1, a contradiction.

This proves assertion 5.4.

5.5. The commutator map $C:\mathscr{G}\times\mathscr{G}\to\mathscr{G}$ admits a factorization $m\circ f$, where

$$f:\mathscr{G}\times\mathscr{G}\to\mathscr{G}\times\mathscr{G}$$

is defined by

$$f(x,y)=(xyx^{-1},y^{-1})$$

and $m:\mathscr{G}\times\mathscr{G}\to\mathscr{G}$ is the multiplication in $\mathscr{G}$. The map f evidently maps E into the set

$$W=\{(x,y)\in\mathscr{G}\times\mathscr{G}|x\neq\pm1,\ y\neq\pm1,\ \operatorname{trace}(x-y^{-1})=0\}.$$

We assert that W is a closed codimension 1 submanifold of

$$\Omega=\{(x,y)\in\mathscr{G}\times\mathscr{G}|x\neq\pm1,\ y\neq\pm1\}$$

and that f is a submersion of E in W. That W is a codimension 1 closed analytic submanifold in Ω follows from the fact that the map $(x,y)\to\operatorname{trace}(x-y^{-1})$ of $\mathscr{G}\times\mathscr{G}$ in $\mathbf{R}$ has no critical points in Ω as is easily checked. To prove that f is a submersion we observe that the tangent map $df_{(a,b)}$ of f at $(a,b)\in\mathscr{G}\times\mathscr{G}$ is given by the following formula: for $X,Y\in\operatorname{Lie}\mathscr{G}$,

$$df_{(a,b)}(X,Y)=(\operatorname{Ad}a(\operatorname{Ad}b^{-1}(X)-X+Y),\ -\operatorname{Ad}b(Y)).$$

The kernel $df_{(a,b)}$ is thus seen to be the space

$$\{(X,0)\in\operatorname{Lie}\mathscr{G}\times\operatorname{Lie}\mathscr{G}|\operatorname{Ad}b^{-1}(X)=X\};$$

and this has dimension 1 if $b\neq\pm1$ – as is indeed the case if $(a,b)\in E$. It follows that $f:E\to W$ is a submersion.

5.6. **Claim.** *$\hat{\mathscr{C}}$ factors through f to an analytic map of $P=f(E)$ in $\hat{\mathscr{G}}$.*

Proof. Since $f:E\to W$ is a submersion, it suffices to show that $\hat{\mathscr{C}}$ is constant along the fibres of f. If $(a,b)\in\mathscr{G}\times\mathscr{G}$ then any point in the fibre of f through (a,b) is necessarily of the form (ax,b) with $x\in$ centralizer of b. Clearly, $\hat{C}(ax,b)=\sigma(a)\,\sigma(x)\,\sigma(b)\,\sigma(x)^{-1}\sigma(a)^{-1}\sigma(b)^{-1}$ and it suffices to show that $\sigma(x)$ and $\sigma(y)$ commute whenever x and y commute. This is true if in addition x and y belong to $G(k):[\sigma(x),\sigma(y)]=\tau([x,y])$. If B is a torus in G defined over k, $B(k)$ is dense in $B(\mathbf{R})$ so that by continuity we have to $[\sigma(x),\sigma(y)]=1$ if $x,y\in B(\mathbf{R})$. For a pair (x,y) of semisimple elements with $[x,y]=1$, it follows that $[\sigma(x),\sigma(y)]=1$ because x and y can be conjugated simultaneously into $B(\mathbf{R})$ for a suitable k-torus B in G. Suppose now that x is not semisimple; then we can, after a conjugation in $GL_2(\mathbf{R})$ assume that $x=\begin{pmatrix}\varepsilon & 1\\ 0 & \varepsilon\end{pmatrix}$ with $\varepsilon=\pm1$ and y then takes the form $\begin{pmatrix}\varepsilon' & \alpha\\ 0 & \varepsilon'\end{pmatrix}$ with $\alpha\in\mathbf{R}$. Now $\sigma\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$ commutes with $\sigma(g)$ for any semisimple g and hence for any $g\in\mathscr{G}$ by continuity. We may therefore assume $\varepsilon=\varepsilon'=1$ in the above:

$x=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, $y=\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}$. Let p_n/q_n, $p_n, q_n \in Z$ be a sequence of rational numbers converging to α. Let $x_n=\begin{pmatrix}1 & 1/q_n\\ 0 & 1\end{pmatrix}$ and $y_n=\begin{pmatrix}1 & p_n/q_n\\ 0 & 1\end{pmatrix}$. Then

$$[\sigma(x), \sigma(y_n)]=[\sigma(x_n)^{q_n}, \sigma(x_n)^{p_n}]=1.$$

Taking the limit as n tends to ∞, we conclude that $[\sigma(x), \sigma(y)]=1$.

5.7. Since $C: E\to\mathscr{G}-\{\pm 1\}$ is a surjective submersion so is $P\xrightarrow{m}\mathscr{G}-\{\pm 1\}$. We have seen above that there is analytic map $\hat{m}: P\to\hat{\mathscr{G}}$ such that $\hat{C}=\hat{m}\circ f$ on E. We will now show the following which in the light of Lemma 5.3 proves the theorem.

5.8. **Assertion.** *$\hat{m}$ is constant along the fibres of the map $m: P\to\mathscr{G}-\{\pm 1\}$ and hence factors through m.*

Proof. Let J be the fibre product of P with itself over $\mathscr{G}-\{\pm 1\}=S$, say:

$$J=\{(p,q)\in P\times P \mid \hat{m}(p)=\hat{m}(q)\}.$$

We will show that J is connected. We observe first that E is connected: it is easy to see that $C^{-1}(1)$ is an analytic subset of codimension 2 in $\mathscr{G}\times\mathscr{G}$. Hence $P=f(E)$ is connected. Also the fibres of C being real algebraic sets have finitely many connected components. Consequently the same holds for the fibres of $m: \hat{P}\to S$. It is immediate that we have then the following: for each $s\in S$, there is a neighbourhood $N(s)$ of s with the following property: *given* any connected component F of $m^{-1}(s)$ $(\subset P)$ there is a point $p\in F$, an open neighbourhood $\tilde{N}(p)$ of p and a diffeomorphism $\Phi_p: N(s)\times\Omega(p)\to\tilde{N}(p)$, where $\Omega(p)$ is an open set in $\mathbf{R}^2$ such that $m\circ\Phi_p(x,y)=x$ for $x\in N(s)$, $y\in\Omega(p)$. As a consequence we note that if $\gamma: [a,b]\to N(s)$ is any continuous path in $N(s)$ with $\gamma(a)=s$ there is a path $\tilde{\gamma}: [a,b]\to P$ such that *$\tilde{\gamma}(a)$ belongs to any prescribed connected component* of $\hat{m}^{-1}(s)$. Suppose now $\alpha=(p,q)\in J$ and $s_0\in S$ is any fixed point. We will show that there is a path $u: [0,T]\to J$ such that $u(0)=\alpha$ and $u(T)=(p',q')$ with $m(p')=m(q')=s_0$. For this let $\gamma: [0,1]\to P$ be any path with $\gamma(0)=p$ and $\gamma(1)=p'$, p', any point of $m^{-1}(s_0)$ (in P). Choose $\{t_i \mid 1\leqq i\leqq r\}$ in $[0,1]$ such that $t_1=0$, $t_r=1$ and $t_i<t_{i+1}$ for $1<i<r$ and $\hat{m}\cdot\gamma([t_i,t_{i+1}])\subset N(\hat{m}(\gamma)(t_i))$. We now define paths $\xi_i: [2i+1, 2i+2]\to P$ for $1<i<r-1$ inductively as follows. Let $\gamma_i: [2i+1, 2i+2]\to P$ be the path defined by $\gamma_i(t)=\gamma(\varrho_i(t))$, where ϱ_i is a linear homeomorphism of $[t_i, t_{i+1}]$ onto $[2i+1, 2i+2]$. Let $\bar{\gamma}_i=m\circ\gamma_i$.

Then $\gamma_i([2i+1, 2i+2])\subset N(\gamma_i(2i+1))$ so that we can find a path $\xi_i: [2i+1, 2i+2]\to P$ with $\xi_i(2i+1)$ belonging to any connected component of $m^{-1}(\gamma_i(2i+1))$ we want. Assume ξ_i defined for $i<j$ and choose ξ_j with $\xi_j(2j+1)$ in the same connected component as $\xi_{j-1}(2j)$. To start the induction ξ_1 is chosen so that $\xi_1(1)$ is in the same connected component of $m^{-1}(\gamma_1(1))$ as the point q. Define now a path $\xi: [0, 2r]\to P$ as follows:

$$\xi|_{[2j+1, 2j+2]}=\xi_j \quad \text{for} \quad 0<j<r$$

while $\xi|_{[2j,2j+1]}$ is a path in $\hat{m}^{-1}(\gamma_j(2j+1))$ joining $\xi_{j-1}(2j)$ and $\xi_j(2j+1)$. Let $\eta:[0,2r]\to P$ be the path given by

$$\eta|_{[2j+1,2j+2]}=\gamma_j$$

while $\eta|_{[2j,2j+1]}$ is the constant path with value $\gamma_{j-1}(2j)=\gamma_j(2j+1)$. Then $t\to(\xi(t),\eta(t))$, $t\in[0,2r]$ gives a path joining (p,q) to $(p',q')\in J$ with $\hat{m}(p')=\hat{m}(q')$. Now to prove the connectedness of J it suffices to show that for a suitable $s_0\in S$, $\hat{m}^{-1}(s_0)$ $(\subset P)$ is connected. Let $s_0=\begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix}$ with $\lambda>0$ and $\lambda\notin 1$. Let

$$F=\{(x,y)\in W\subset\mathscr{G}\times\mathscr{G}|m(x,y)=x\cdot y=s_0\}.$$

If $(x,y)\in F$, we have trace $x=$ trace y^{-1} and since $y^{-1}=s_0^{-1}x$; we see then that if we set $x=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ (with $ad-bc=1$), we have necessarily $d=a\lambda^{-1}$. Now (x,y) belong to P iff x and y^{-1} are conjugates in $SL_2(\mathbf{R})$. The elements x and y^{-1} are conjugates in $GL_2(\mathbf{R})$ as trace $x=$ trace y^{-1}. Now $x=\begin{pmatrix}a & b\\ c & a\lambda^{-1}\end{pmatrix}$ while $s_0^{-1}x=y^{-1}$ $=\begin{pmatrix}a\lambda^{-1} & b\lambda^{-1}\\ c\lambda & a\end{pmatrix}$. Since $\lambda>0$ we may conjugate y^{-1} by a diagonal matrix in $SL_2(\mathbf{R})$ to obtain the element $z=\begin{pmatrix}a\lambda^{-1} & b\\ c & a\end{pmatrix}$. Now if the eigenvalues of x (and hence also z) are both real and *distinct*, x and z are conjugates in $SL_2(\mathbf{R})$. We need therefore consider only the case when the eigenvalues of x are either both equal or when they are not real. But this means that $2\geqq|\text{trace}\,x|=|a|(1+\lambda^{-1})$, i.e. $|a|\leqq 2/(1+\mu)$, where $\mu=\lambda^{-1}>0$ is distinct from 1. We have then $bc=ad-1=a^2\mu-1\leqq 4\mu/(1+\mu)-1<0$. Thus, b,c are both nonzero and are of opposite signs. Conjugating x and z by a suitable diagonal matrix we see then that x and y^{-1} are conjugates iff $\begin{pmatrix}a & u\\ -u & au\end{pmatrix}$ and $\begin{pmatrix}au & u\\ -u & a\end{pmatrix}$ are conjugates for a suitable $u\neq 0$; and these last two elements are conjugates of each other under $\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$. We see thus that F is the fibre $\hat{m}^{-1}(s_0)$ in P. On the other hand, F can be identified with

$$\left\{\begin{pmatrix}a & b\\ c & a\mu\end{pmatrix}\in M_2(\mathbf{R})|\mu a^2-bc=1\right\}$$

and this set – a conic in $\mathbf{R}^3$ – is evidently connected as $\mu>0$. We see therefore that F and hence J is connected. Let D denote the set of elements $(p,q)\in J$ with $p=(x,y)$, $q=(z,w)$ with (x,y) and (z,w) belonging to $f(G(k)\times G(k))$. Then since $\hat{m}(p)=\hat{m}(q)$ for $(p,q)\in D$ the analytic function $\Phi:J\to\mathscr{G}$ given by $\Phi(p,q)=\hat{m}(p)\hat{m}(q)^{-1}$ is constant (equal to 1) on D. Since J is connected it suffices then to establish the following

5.9. **Assertion.** *The closure of D contains an open subset of J.*

Proof. Consider the following subset $\mathcal{M}$ of $\mathcal{G}\times\mathcal{G}\times\mathcal{G}\times\mathcal{G}$:

$$\mathcal{M}=\{(a,b,x,y)|a,b\in\mathcal{G},\ [a,b]\neq 1,\ x\in Z(a),\ y\in Z([a,b])\},$$

where for $g\in\mathcal{G}$, $Z(g)$ denotes the centralizer of g in $\mathcal{G}$. It is easy to see that $\mathcal{M}$ is a submanifold of $\mathcal{G}\times\mathcal{G}\times\mathcal{G}\times\mathcal{G}$ of dimension 8. In fact, $\mathcal{M}$ is the **R**-points of a subvariety M of $G\times G\times G\times G$ defined over k. Since $G(k)$ is dense in $\mathcal{G}$ and for $g\in G(k)$, $Z(g)(k)$ is dense in $Z(g)(\mathbf{R})$ we see that $M(k)$ is dense in $\mathcal{M}$.

Let $F:\mathcal{M}\to\mathcal{G}\times\mathcal{G}\times\mathcal{G}\times\mathcal{G}$ be the map defined as follows:

$$\begin{aligned}F(a,b,x,u)&=(aba^{-1},a^{-1},uabxa^{-1}u^{-1},ux^{-1}b^{-1}u^{-1})\\&=(f(a,b),f(uau^{-1},ubxu^{-1})).\end{aligned}$$

Then F is an analytic map of M into J as is easily seen. The differential of F at $(a,b,1,1)$ is given by the following formula: let $X,Y\in\operatorname{Lie}\mathcal{G}$, $Z\in z(a)$, the centralizer of a in Lie $\mathcal{G}$ and $T\in z([a,b])$, the centralizer of $[a,b]$ in Lie $\mathcal{G}$; then

$$dF_{(a,b,1,1)}(X,Y,Z,T)=(X',Y',Z',T'),$$

where

$$X'=\operatorname{Ad}a((\operatorname{Ad}b^{-1}-1)X+Y,$$

$$Y'=-\operatorname{Ad}b(Y),$$

$$Z'=X'+Z+\operatorname{Ad}ab^{-1}a^{-1}(T)-T,$$

and

$$T'=Y'-\operatorname{Ad}bZ+\operatorname{Ad}bT-T.$$

Thus, if X,Y,Z,T is in the kernel of $dF_{(a,b,1,1)}$, then $Y=0$, $X\in z(b)$, $Z\in\operatorname{Image}(\operatorname{Ad}b^{-1}-1)\cap z(a)$. If a and b are semisimple and $Z\neq 0$ this would mean that $z(a)$ and $z(b)$ are orthogonal to each other with respect to the Killing form on Lie $\mathcal{G}$. Thus, if we assume – such a choice of a and b in $\mathcal{G}$ is possible – that

$$2\operatorname{trace}ab-\operatorname{trace}a\ \operatorname{trace}b\neq 0,$$

then $z(a)$ is not orthogonal to $z(b)$ so that $Z=0$. Once $Z=0$, one concludes that $T\in z(aba^{-1})\cap z(b)$; and then $T=0$ if aba^{-1} does not commute with b. We see therefore that if $(a,b)\in\mathcal{G}\times\mathcal{G}$ is so chosen that a and b are semisimple, $2\operatorname{trace}ab-\operatorname{trace}a\ \operatorname{trace}b\neq 0$ and aba^{-1} and b do not commute, then at $(a,b,1,1)$ the differential of F has a kernel of dimension 1. Since $\dim J=7$ while $\dim M=8$, we conclude that there is an open subset U of M such that $F(U)$ is open in J. Since $M(k)\cap U$ is dense in U and $F(M(k)\cap U)\subset D$, Assertion 5.9 follows.

Acknowledgements. My thanks are due to Gopal Prasad for many interesting discussions. He drew my attention to Deligne's work and also pointed out a gap in the initial "proof" I had. Modhav Nori essentially proved for me Proposition 4.4; it is a pleasure to acknowledge his help. Finally, I thank the referee for patiently pointing out a large number of printing errors in the original manuscript and for suggestions for improving the exposition.

References

1. Deligne, P.: Extensions centrales non résiduellement finies de groupes arithmétiques. C.R. Acad. Sci. Paris, Ser. A–B **287**, n° 4, A203–A208 (1978)
2. van Est, W.T.: A generalization of the Cartan-Leray spectral sequence. Nederl. Akad. Wentensch. Proc. Ser. A **61**, I 399–405; II 406–413 (1958)
3. Kneser, M.: Orthogonal Gruppen über algebraischen Zahlkörpern. J. Reine angew. Math. **196**, 213–220 (1956)
4. Kneser, M.: Normalteiler ganzzahliger Spingruppen. J. Reine angew. Math. **311/312**, 191–214 (1979)
5. Margulis, G.A.: Discrete groups of motions of manifolds of non-positive curvature (Russian). Proc. Int. Cong. Math., Vancouver 1974; English transl. AMS (2) **109**, 33–45 (1977)
6. Millson, J.: Real vector bundles with discrete structure group. Topology **18**, 83–89 (1979)
7. Platanov, V.P., Rapnĭcuk: Dokl. Akad. Nauk SSSR **266** (1982)
8. Prasad, G., Raghunathan, M.S.: Topological central extensions of semi-simple groups over local fields. Preprint to appear in Ann. Math. **119** (1984)
9. Prasad, G., Raghunathan, M.S.: On the congruence subgroup problem: Determination of the "Metaplectic kernel". Invent. Math. **71**, 21–42 (1983)
10. Raghunathan, M.S.: On the congruence subgroup problem. Publ. Math. IHES **46**, 107–161 (1976)
11. Raghunathan, M.S.: On the group of norm 1 elements in a division algebra. Preprint IHES (1984)
12. Schur, I.: Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. J. Reine angew. Math. **132**, 85–137 (1907)
13. Tits, J.: Classification of algebraic semisimple groups. Algebraic groups and discontinuous subgroups. Proc. Symp. Pure Math. **9**, pp. 33–62. Providence, R.I.: Am. Math. Soc.
14. Moore, C.: Group extensions of p-adic and adelic linear groups. Publ. Math. IHES **35**, 157–222 (1968)

Received March 21, 1983

Added in Proof. The conclusions of the main theorem are also valid for the groups $\mathrm{Sp}(2n, R)$, $n > 1$. This follows from the following facts: any lattice Γ in $\mathrm{Sp}(2n, R)$ is arithmetic; if G is an algebraic k-group over a number field k with $G(k_v) \simeq \mathrm{Sp}(2n, R)$ for some archimedean valuation v, then G admits a k-subgroup H such that $\pi_1(H(k_v)) \simeq \pi_1(G(k_v))$ and H is of type C_2, i.e. H is of type B_2; our contention now follows from the main theorem.