Invent. math. 85, 73-117 (1986)

Inventiones mathematicae

On the congruence subgroup problem, II

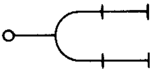
M.S. Raghunathan

Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay 400005, India

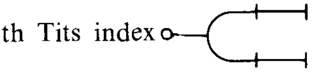
This is a sequel to my earlier paper of the same title (Raghunathan, 1976). Most of the results here are announced there in somewhat vague terms.

Let k be a global field and V its set of valuations. For $v \in V$, let k_v denote the completion of k at v and for non-archimedean v, $\mathfrak{O}_v$ the ring of integers in k_v. We fix once for all a non-empty finite subset S of V containing the set ∞ of all archimedean valuations. We denote by A the ring of S-integers in k. Let G be a connected simply connected absolutely almost simple k-algebraic group and $G(k)$ the group of k-rational point of G. A subgroup $\Gamma \subset G(k)$ is an S-arithmetic subgroup if for some (and therefore any) faithful k-representation ρ: $G \to \mathrm{GL}(n_\rho)$, $\Gamma \cap \rho^{-1}\mathrm{GL}(n_\rho, A)$ has finite index in both Γ and $\rho^{-1}(\mathrm{GL}(n_\rho, A))$. An S-arithmetic group is an S-congruence group if for some (therefore any) faithful k-representation ρ of G, Γ contains a subgroup of the form $G(\rho, a) = \{x \in G(k) \mid \rho(x) \in \mathrm{GL}(n_\rho, A),\ \rho(x) \equiv 1 \bmod \mathfrak{a}\}$ where $\mathfrak{a} = \mathfrak{a}(\rho)$ is a non-zero ideal in A.

Now the family of S-arithmetic (resp. S-congruence) groups form a fundamental system of neighbourhoods of the identity for the structure of a topological group, whose completion we denote $\hat{G}(a)$ (resp. $\hat{G}(c)$). Then $\hat{G}(a)$ and $\hat{G}(c)$ are locally compact groups and there is a natural map π: $\hat{G}(a) \to \hat{G}(c)$ induced by the identity map of $G(k)$. It is not difficult to see that π is surjective. The group $\hat{G}(a)$ is naturally isomorphic to the S-adèle group of G (this is a consequence of the fact the $G(k)$ is dense in the S-adéle group of G: Platonov (1970) for number fields and Prasad (1977) for all fields. The congruence subgroup problem (for (G, S)) is the determination $C(S, G) = \mathrm{kernel}\,\pi$. That is the main aim of this paper.

To formulate our results in precise form, we need to introduce the (normal) subgroup $G(k)^+$ of $G(k)$ generated by unipotent elements contained in unipotent radicals of k-parabolic subgroups. For a wide class of groups, it is known that $G(k) = G(k)^+$. (At the date of this writing in fact, it is known that $G(k)/G(k)^+$ is always *finite abelian* and in fact trivial except possibly in the case when G is a k-form of E_6 of k-rank 1 with anisotropic kernel a special unitary group in 2 variables over a involutive cubic division algebra of the second kind; the Tits index of such a group is . We then have

Main theorem. *Assume that G is isotropic over k and that $\sum_{v\in S} k_v$-rank $G \geqq 2$. Let $\hat{G}(a)^+$ be the closure of $G(k)^+$ in $\hat{G}(a)$. Then $\hat{G}(a)^+ \to \hat{G}(c)$ is (surjective and) a central extension. (Consequently) $C(S,G)$ is a 2-step solvable group with $C(S,G)/C^+(S,G) \simeq G(k)/G(k)^+$ where $C^+(S,G)$ is the kernel of $\hat{G}(a)^+ \to \hat{G}(c)$.*

When k-rank $G \geqq 2$, the theorem is proved in Raghunathan (1976). We will therefore confine ourselves to the case when **k-rank $G=1$**. We note that $C(S,G) = C^+(S,G)$ except possibly in the case when G is a k-rank 1 (outer form E_6) with Tits index  and anisotropic kernel k-isomorphic to a special unitary group in 2 variables over a cubic division algebra D with an involution of the second kind, the centre of D being a quadratic extension over k. Using now Prasad and Raghunathan (1983) we obtain immediately the following

Corollary. $C^+(S,G)$ is isomorphic to a quotient of $\mu(k)$, the group of roots of unity in k; it is trivial if one of the following two conditions hold:

(i) S contains a non-archimedean valuation.

(ii) There is a $v\in S$ such that k_v is real and the relative k_v-root space of G corresponding to any long root is of dimension 1.

Note. It is proved in Prasad and Raghunathan (1983) that if $C(S,G)$ is central in $\hat{G}(a)$, then $C(S,G)$ is isomorphic to a quotient of $\mu(k)$ and in fact is trivial if (G,S) satisfy one of the two conditions above; however the proof there actually yields the analogous statement for $C^+(S,G)$ if it is central in $\hat{G}(a)^+$: in fact the "relative fundamental group" of $(\hat{G}(c), G(k)^+)$ is the group $C^+(S,G)$.

Our method of proof involves the use of yet another family of subgroups of $G(k)$. Fix a faithful k-representation ρ once and for all and for any ideal $\mathfrak{a} \neq 0$ in A, let $G(\mathfrak{a}) = \{x \in G(k) \mid \rho(x) \in \mathrm{GL}(n),\ \rho(x) \equiv 1 \,(\mathrm{mod}\, \mathfrak{a})\}$: $\{G(\mathfrak{a}) \mid \mathfrak{a}$ a nonzero ideal in $A\}$ is evidently a fundamental system of S-congruence subgroups. Let $E(\mathfrak{a})$ denote the subgroup of $G(\mathfrak{a})$ generated by unipotents in $G(\mathfrak{a})$ which are contained in unipotent radicals of k-parabolic subgroups. (From a theorem of Margulis (1979), it is known that every $E(\mathfrak{a})$ $(\mathfrak{a} \neq 0)$ is in fact an arithmetic subgroup; we will however not make use of that result but in fact obtain it as a consequence of our theorems: this is perhaps not altogether pointless as the techniques of Margulis have a completely different flavour as opposed to our purely algebraic methods – for instance we make no use of the fact that arithmetic groups are lattices). The $\{E(\mathfrak{a}) \mid \mathfrak{a}$ a non zero ideal$\}$ serve to define yet another topological group structure on G whose completion is denoted $\hat{G}(e)$. This last topology on $G(k)$ is finer than that defined by S-arithmetic groups (Raghunathan, 1976, Theorem 2.1). Consequently the main result would follow from

Theorem A. *Let $\hat{G}(e)^+$ be the closure of $G(k)^+$ in $\hat{G}(e)$. If k-rank $G=1$ and $\sum_{v\in S} k_v$-rank $G \geqq 2$, $\hat{G}(e)^+ \to \hat{G}(c)$ is (surjective and is) a central extension of $\hat{G}(c)$.*

As in Raghunathan (1976) we obtain from Theorem A the following corollaries (apart from the main theorem) under the hypothesis in the theorem.

Corollary 1. *Every normal infinite subgroup of an S arithmetic group in $G(k)$ is S-arithmetic.*

The proof is entirely the same as that in Raghunathan (1976, Theorem 2.1).

Corollary 2. *$[\Gamma, \Gamma]$ has finite index in Γ for any S-arithmetic group Γ in G.*

Corollary 3. *Let ρ be a finite dimensional representation of an S-arithmetic group Γ over a field of characteristic zero. Then either kernel ρ has finite index in Γ or* $\operatorname{char} k=0$ *and there is a subgroup Γ' of finite index in Γ such that $\rho|\Gamma'$ extends to a rational representation of $R_{k/Q} G$.*

(See Raghunathan (1976) Chapter 7; Margulis (1979) proves Corollary 3 by other methods.)

The method of proof of Theorem A is along the following lines. In Chapter 1 we establish the theorem in the special case when G is *quasi split*. This follows the same ideas as Serre (1970) closely. In Chapter 2 we give a method of construction of universal central extension of S-adéle groups of G in terms of generators and relations: the universal extension is obtained as a quotient of the free product of two opposing unipotent S-adéle groups by certain relations; we also establish a partial converse. In Chapter 3 we show that $\hat{G}(e)^+$ when written as a natural quotient of the free product of opposing unipotent adéle groups satisfies all the relations required for central extensions of $\hat{G}(c)$. This is achieved by imbedding quasi-split k-groups (cf. Chapter 5) in G for which we know the truth of Theorem thereby obtaining relations in $\hat{G}(e)$ and then proving that the relations obtained in this fashion generate all the necessary relations. Unfortunately the method fails to cover a few cases which are treated in § 4 by techniques analogous to those in § 1. Chapter 5 is an Appendix containing a general result (over arbitrary fields k) on k-rank 1 algebraic groups which seems to be of independent interest. We show the following:

Let G be a k-rank 1 semisimple algebraic group and U a maximal connected unipotent k-subgroup normalised by a k split torus S. Let $u \in U(k)$ be any unipotent element $\neq 1$. Then there is a quasi split semisimple k-group H a k-split torus $T \subset H$, a unipotent k-subgroup V in H normalised by T and a k-morphism f: $H \to G$ such that $f(T) = S$ and $x \in f(V(k))$.

The methods of this paper can in fact to applied to groups of k-rank $G \geqq 2$ but we have not carried this out for two reasons: the earlier proof in Raghunathan (1976) seems to be pleasanter; secondly the notational complexity that would be inevitable in dealing with higher rank groups would perhaps render the exposition much less clear.

We end this introduction with some remarks on completions of topological groups. In the outline of proof given above we have spoken of "the" completion of a certain topological group. This requires some justification (I am indebted to J.-P. Serre for pointing out to me the need for exercising some care in this). The ensuing discussion will clarify this point and will also be useful for us later. If B is a topological group it carries a canonical left translation invariant uniform structure denoted $V(l)$ in the sequel. Analogously it has also a right translation invariant uniform structure $V(r)$. We denote the completion of B with respect to $V(l)$ (resp. $V(r)$) by $\hat{B}(l)$ (resp. $\hat{B}(r)$). If the topological group structure on B satisfies the Condition (*) or the equivalent condition (**) below, then we have a natural homeomorphism Φ: $\hat{B}(l) \to \hat{B}(r)$ making the diagram

$$\begin{tikzcd} & B \arrow[dl, "i_l"'] \arrow[dr, "i_r"] & \\ \hat{B}(l) \arrow[rr, "\Phi"] & & \hat{B}(r) \end{tikzcd}$$

commutative where i_l (resp. i_r) is the natural inclusion of B in the completion $\hat{B}(l)$ (resp. $\hat{B}(r)$).

Condition (*). *Each Cauchy filter for $V(l)$ is a Cauchy filter for $V(r)$ and conversely.*

Condition (**). *Let τ: $B \to B$ denote the map $x \to x^{-1}$, $x \in B$. Then if F is a Cauchy filter for $V(l)$, so is $\tau(F)$.*

If the Condition (*) and hence also (**) is satisfied, then Φ enables us to identify $\hat{B}(l)$ and $\hat{B}(r)$ and we denote the space $\hat{B}(l)$ simply $\hat{B}$ (and will freely identify it with $\hat{B}(r)$ as well). For B satisfying Condition (*), it is easily checked that $\hat{B}$ is indeed a topological group, the group operation extending that in B. In the sequel when we speak of completions of topological groups we will only be considering topological groups satisfying Condition (*). We may - and we will therefore freely consider such completions as topological groups (complete both in the left and right invariant uniform structures). In fact *all topological groups B we will be interested in this paper will satisfy the following Condition C* which is stronger than Condition (*) (or (**)) as can be verified quite easily:

Condition C. *The identity element in B admits a fundamental system $\mathscr{V}$ of neighbourhoods such that*

(i) *each $V \in \mathscr{V}$ is a subgroup of B*

(ii) *there is an open subgroup Γ of B such that Γ normalises all $\mathscr{V} \in V$.*

(It is evident that the topological group structure on $G(k)$ defined by declaring the $\{G(\mathfrak{a}) | \mathfrak{a}$ a non-zero ideal in $A\}$ (resp. $\{E(\mathfrak{a}) | \mathfrak{a}$ a non zero ideal in $A\}$) as a fundamental system of neighbourhoods of the identity satisfies the Condition C introduced above, with $G(A)$ playing the role of Γ.)

Finally I would like to draw the attention of the readers to earlier work on the subject: Mennicke (1965), Bass et al. (1964) (the group SL(n) $n>2$ over Q) Bass et al. (1967) (SL(n) and Sp($2n$) $n>2$ over global fields) Matsumoto (1969) (Chevalley groups), Vaserstein (1973) (classical groups of rank$\geqq 2$) Serre (1970) (SL(2)), Bak and Rehman (1982) (SL(n) over division algebras with $n \geqq 2$) and Kneser (1979) (spin groups over number fields).

§ 1. The quasi-split k-group of k-rank 1

1.1. Notation. Throughout this chapter we will use the following notation.

k will denote a global field.

K a quadratic Galois extension of k with Gal(K/k) as the Galois group and

$a \mapsto \bar{a}$ denoting the non-trivial element of Gal(K/k).

Σ (resp. $\tilde{\Sigma}$) will be the set of valuations of k (resp. K)

k_v (resp. K_v) for $v \in \Sigma$ (resp. $\tilde{\Sigma}$) the completion of k (resp. K) with respect to v and

$\mathfrak{O}_v$ (resp. $\tilde{\mathfrak{O}}_v$) the ring of integers in k_v (resp. K_v), v non-archimedean $S \neq \emptyset$ a fixed finite set of valuations of k containing all the archimedean valuations and

$\tilde{S}$ the set of valuations of K lying over those in S, A (resp. $\tilde{A}$) the ring of S-integers in k (resp. K):

$$A = \{x \in k \mid x \in \mathfrak{O}_v \text{ for all } v \notin S\}$$

$$(\text{resp. } \tilde{A} = \{x \in K \mid x \in \tilde{\mathfrak{O}}_v \text{ for all } v \notin \tilde{S}\}).$$

Also, let $A^* = \{a \in \tilde{A} \mid \bar{a} = -a\}$. (If k is of characteristic 2, $A^* = A$.) We sometimes refer to elements of A^* as purely imaginary.

In the sequel we will have to use frequently the following ideals in A and $\tilde{A}$. In general, if $\mathfrak{q}$ is an ideal in A, $\tilde{\mathfrak{q}}$ will denote $\mathfrak{q}\tilde{A}$. The ideals we are interested in are

$\mathfrak{f}$ $=$ maximal $\tilde{A}$-ideal contained in the A-submodule $A + A^*$ of $\tilde{A}$; $\mathfrak{f}$ is non-zero if the characteristic of $k \neq 2$.

$\mathfrak{f}_0 = \mathfrak{f} \cap A$. In general $\tilde{\mathfrak{f}}_0 \subset \mathfrak{f}$ but $\tilde{\mathfrak{f}}_0$ may not equal $\mathfrak{f}$.

$\mathfrak{t}$ $= \{\text{trace } x \mid x \in \tilde{A}\}$ (an ideal in A).

$\mathfrak{s}$ $=$ ideal generated by A^* in $\tilde{A}$.

$\mathfrak{s}_0 = A \cap \mathfrak{s}$.

The ideals $\mathfrak{t}$ and $\mathfrak{s}_0$ are always non-zero (in all characteristics).

Let $\boldsymbol{G} = \mathrm{SU}(2, 1)$ denote the special unitary group of the hermitian quadratic form in 3 variables (on K) given by the matrix

$$E = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$\boldsymbol{G}$ is the unique (upto k-isomorphism) simply connected quadi-split group of k-rank 1 splitting over K. The k-rational points of $\boldsymbol{G}$ is denoted $\mathrm{SU}(2, 1, K)$ or G:

$$\mathrm{SU}(2, 1, K) = \{g \in \mathrm{GL}(3, K) \mid \det g = 1,\ t_{\bar{g}} E g = E\}.$$

Γ will be the subgroup $G \cap \mathrm{SL}(3, \tilde{A})$ of G. For an ideal $\mathfrak{q} \subset A$, $\tilde{\mathfrak{q}} = \mathfrak{q}\tilde{A}$ and

$$\Gamma(\mathfrak{q}) = \{g \in \Gamma \mid g \equiv \text{Identity } (\text{mod } \tilde{\mathfrak{q}})\}.$$

We denote by $E\Gamma(\mathfrak{q})$ the subgroup generated those unipotents in $\Gamma(\mathfrak{q})$ which are contained in the unipotent radical of a k-parabolic subgroup of $\boldsymbol{G}$. A standard example of the k-points of unipotent radicals of k-parabolic subgroups of $\boldsymbol{G}$ are the following.

$$U^+ = \left\{ \begin{pmatrix} 1 & \xi & \eta \\ 0 & 1 & 0 \\ 0 & -\bar{\eta} & 1 \end{pmatrix} \middle| \text{trace } \xi = \text{Norm } \eta,\ \ \xi, \eta \in K \right\}$$

$$U^{-}=\left\{\left.\begin{pmatrix}1&0&0\\ \xi&1&-\bar{\eta}\\ \eta&0&1\end{pmatrix}\right|\text{trace }\xi=\text{Norm }\eta,\ \xi,\eta\in K\right\}.$$

Thus $E\Gamma(\mathfrak{q})\supset U^{+}\cap\Gamma(\mathfrak{q})$ and $U^{-}\cap\Gamma(\mathfrak{q})$. A third subgroup of G of interest to us is the group

$$\Phi=\left\{\begin{pmatrix}a&b&0\\ c&d&0\\ 0&0&1\end{pmatrix}\in G\,\middle|\,a,d\in A,\ b,c\in A^{*},\ ad\text{-}bc=1\right\}.$$

(It may be remarked that Φ may be realised as a subgroup of the automorphism group of the projective A-module $A+A^{*}$.) For an ideal $\mathfrak{q}\subset A$ we set

$$\Phi(\mathfrak{q})=\Gamma(\mathfrak{q})\cap\Phi.$$

From now on we make the following additional assumption

(*) **The group of $\tilde{S}$-units in K ($\overset{\text{def}}{=}$ units in $\tilde{A}$) is infinite.**

This assumption is equivalent to saying that, in characteristic 0, K is *not* a quadratic imaginary extension of $\mathbb{Q}$ and in all characteristics to saying that $|\tilde{S}|\geqq 2$. We observe that if u is a unit in $\tilde{A}$, the matrix

$$\theta(u)=\begin{pmatrix}u&0&0\\ 0&\bar{u}^{-1}&0\\ 0&0&u^{-1}\bar{u}\end{pmatrix}\text{ belongs to }G\text{ (in fact }\Gamma).$$

In the special case where k has no S-units of infinite order, we see that there are infinitely many $\tilde{S}$-units u such that $u\bar{u}=1$. For such an element u

$$\theta(u)=\begin{pmatrix}u&0&0\\ 0&u&0\\ 0&0&u^{-2}\end{pmatrix};$$

evidently in this case $\theta(u)$ commutes with all of Φ, an observation which will be useful later. A *special* unit in $\tilde{A}$ is a unit in A or a unit u such that $u\bar{u}=1$.

The following result is the main thrust towards the solution of our problem in the present chapter.

1.2. Proposition. *Let l denote the order of the group of roots of unity in K and u a special unit in $\tilde{A}$. (We assume that (*) holds.) There exists an ideal $\mathfrak{r}\subset A$ (independent of u in fact) such that $\mathfrak{r}\neq 0$ and*

$$[\theta(u)^{l^2},\Gamma(\mathfrak{r}\,\mathfrak{q})]\subset E\Gamma(\mathfrak{q})$$

for all ideals $\mathfrak{q}\subset A$.

The basic idea of the proof is derived from that of a similar statement in Serre (1970). In fact the present chapter has nothing very original from the point of view of conceptual development: some technical difficulties are however encountered when one tries to push the ideas of Serre (in the reference cited above) to the case of SU(2, 1), (the unique quasi-split, non-split, rank 1 group).

1.3. Lemma. *Let* $\mathfrak{q}\subset A$ *be any non-zero ideal and* $\gamma=\begin{pmatrix} a & b & c\\ . & . & .\\ . & . & .\end{pmatrix}$ *any element of* $\Gamma(\mathfrak{t}\mathfrak{q})$, (*recall that* $\mathfrak{t}=\{\mathrm{trace}\, x \mid x\in\tilde{A}\}$). *Then there exists* $\varphi\in E\Gamma(\mathfrak{q})$ *such that* $\gamma\varphi$ $=\begin{pmatrix} a' & b' & c'\\ . & . & .\\ . & . & .\end{pmatrix}$ *with* $(a',b')=\tilde{A}$.

Let B denote the set of primes $\mathfrak{p}$ in $\tilde{A}$ dividing b. Let $B_1=\{\mathfrak{p}\in B \mid \mathfrak{p}$ coprime to $a\}$ and $B_2=\{\mathfrak{p}\in B\mid \mathfrak{p}$ divides $a\}$. Then no prime in B_2 can divide $\mathfrak{t}\mathfrak{q}$ since $a\equiv 1 \pmod{\tilde{\mathfrak{t}}\tilde{\mathfrak{q}}}$. It follows that we can find $\lambda\in\tilde{A}$ such that

$$(*)\qquad \begin{aligned} &\lambda\equiv 0 \pmod{\mathfrak{p}} && \text{for } \mathfrak{p}\in B_1\\ &\lambda\equiv 1 \pmod{\mathfrak{p}} && \text{for } \mathfrak{p}\in B_2\\ &\lambda\equiv 0 \pmod{\tilde{\mathfrak{t}}\tilde{\mathfrak{q}}}. \end{aligned}$$

Evidently then $a+\lambda c$ is a unit modulo b: note that either a or c is a unit modulo any $\mathfrak{p}\in B$ and a is a unit modulo $\tilde{\mathfrak{t}}\tilde{\mathfrak{q}}$. Next if λ is chosen to satisfy (*), one sees from our definition of $\mathfrak{t}$ that there exists $\xi\in\tilde{\mathfrak{q}}$ with trace $\xi=\lambda\bar{\lambda}$. Set φ $=\begin{pmatrix} 1 & 0 & 0\\ \xi & 1 & -\bar{\lambda}\\ \lambda & 0 & 1\end{pmatrix}$; then $\varphi\in U^-\cap\Gamma(\mathfrak{q})\subset E\Gamma(\mathfrak{q})$ and $\gamma\varphi$ has the required property. This proves the lemma.

1.4. Lemma. *Let* $\gamma=\begin{pmatrix} a & b & c\\ . & . & .\\ . & . & .\end{pmatrix}$ *be any element of* $\Gamma(\mathfrak{s}_0\mathfrak{q})$ (*recall that* $\mathfrak{s}_0$ $=(\tilde{A}\cdot A^*)\cap A$). *Assume that* $(a,b)=\tilde{A}$. *Then there exists* $\varphi\in E\Gamma(\mathfrak{s}_0\mathfrak{q})$ *such that*

$$\gamma\varphi=\begin{pmatrix} a' & b' & c'\\ . & . & .\\ . & . & .\end{pmatrix}\qquad \textit{with } (a',c')=1 \textit{ and } (a',b')=1.$$

Proof. Let C be the set of prime ideals in $\tilde{A}$ dividing c. Let $C_1=\{\mathfrak{p}\in C\mid \mathfrak{p}$ is coprime to $a\}$ and $C_2=\{\mathfrak{p}\in C\mid \mathfrak{p}$ divides $a\}$. For $\mathfrak{p}\in C$, let $\mathfrak{p}_0=\mathfrak{p}\cap A$. We assert that if $\mathfrak{p}\in C_2$, $\bar{\mathfrak{p}}\in C_2$ as well. To see this observe that we have

$$a\bar{b}+\bar{a}b+c\bar{c}=0$$

and that $(a,b)=\tilde{A}$. Thus if $\mathfrak{p}$ divides a and c it must divide $\bar{a}$; hence $\bar{\mathfrak{p}}$ divides a as well. Now if $\mathfrak{p}$, $\mathfrak{p}'$ are ideals in C such that $\mathfrak{p}\neq\mathfrak{p}'$ and

$$\mathfrak{p}_0=\mathfrak{p}\cap A=\mathfrak{p}'\cap A=\mathfrak{p}'_0$$

we have necessarily $\mathfrak{p}'=\bar{\mathfrak{p}}$ and then both $\mathfrak{p}$ and $\mathfrak{p}'$ belong to the same C_i, $i=1$ or 2.

Consider now the A-submodule $\mathfrak{p}^*=\mathfrak{p}\cap A^*$ of A^* for each $\mathfrak{p}\in C$. It is clear that

$$\mathfrak{p}^*=\mathfrak{p}\cap A^*\supset\mathfrak{p}_0\cdot A^*, \qquad \mathfrak{p}_0=A\cap\mathfrak{p}.$$

Suppose now $\mathfrak{p}\in C_2$; then $\mathfrak{p}\cap A^*\neq A^*$. This is because the ideal generated by A^* in $\tilde{A}$ contains $\tilde{\mathfrak{s}}_0$ and a being congruent to 1 modulo $\tilde{\mathfrak{s}}_0$, the divisor $\mathfrak{p}$ of a must be coprime to $\tilde{\mathfrak{s}}_0$. It follows moreover that $\mathfrak{p}\cap A^*=\mathfrak{p}_0 A^*$; this is because A^* being a rank 1 module over A, $A^*/\mathfrak{p}_0 A^*$ is a simple A-module. It follows now that we can find

$$\lambda_{\mathfrak{p}}\in A^*-\mathfrak{p}^*=A^*-\mathfrak{p}_0 A^*$$

such that for all $\mathfrak{p}\in C_2$, $\lambda_{\mathfrak{p}}=\lambda_{\bar{\mathfrak{p}}}$ (observe that $\mathfrak{p}^*=\bar{\mathfrak{p}}^*$).

Since C_2 is closed under conjugation for $\mathfrak{p}\in C_1$ and $\mathfrak{p}'\in C_2$, $\mathfrak{p}_0\neq\mathfrak{p}'_0$. Also for $\mathfrak{p}\in C_2$, $\mathfrak{p}_0=\mathfrak{p}\cap A$ is coprime to the annihilator of $A^*/(\tilde{\mathfrak{q}}\tilde{\mathfrak{s}}\cap A^*)$. This is because $\tilde{\mathfrak{s}}\tilde{\mathfrak{q}}\cap A^*\supset\mathfrak{s}\mathfrak{q}A^*$ and since $a\equiv 1 \pmod{\tilde{\mathfrak{q}}\tilde{\mathfrak{s}}}$, $\mathfrak{p}_0$ must be coprime to $\mathfrak{q}\mathfrak{s}$.

Applying now the Chinese-remainder theorem to the (projective rank-1) module A^* over A, we see that we can find $\lambda\in A^*$ such that

$$\begin{aligned}
&\lambda\equiv\lambda_{\mathfrak{p}} \pmod{\mathfrak{p}^*} && \text{for } \mathfrak{p}\in C_2\\
&\lambda\equiv 0 \pmod{\mathfrak{p}^*} && \text{for } \mathfrak{p}\in C_1\\
&\lambda\equiv 0 \pmod{A^*\cap\tilde{\mathfrak{q}}\tilde{\mathfrak{s}}}.
\end{aligned}$$

One sees then immediately that the element $a+\lambda b$ is a unit modulo every $\mathfrak{p}\in C$ as well as modulo $\tilde{\mathfrak{q}}\tilde{\mathfrak{s}}$ we conclude that $a+\lambda b$ is coprime to c. Consider now the element

$$\varphi=\begin{pmatrix}1&0&0\\ \lambda&1&0\\ 0&0&1\end{pmatrix}\in E\Gamma(\mathfrak{q}\mathfrak{s}); \qquad \gamma\varphi=\left(\begin{matrix}a+\lambda b & b & c & \\ . & . & . & .\\ . & . & . & \end{matrix}\right.$$

Evidently $\gamma\varphi$ has the required property. This proves the lemma.

Combining Lemmas 1.3 and 1.4, we have

1.5. Lemma. *Let $\gamma\in\Gamma(\mathfrak{s}_0\mathfrak{t}\mathfrak{q})$. Then we can find $\varphi\in E\Gamma(\mathfrak{s}_0\mathfrak{q})$ such that*

$$\gamma\varphi=\begin{pmatrix}a&b&c\\ .&.&.\\ .&.&.\end{pmatrix} \qquad \textit{with } (a,c)=(a,b)=\tilde{A}.$$

1.6. Lemma. *Let $\gamma=\begin{pmatrix}a&b&c\\ .&.&.\\ .&.&.\end{pmatrix}$ be any element of Γ. Then $Aa+A^*b\supset c\bar{c}\tilde{A}$.*

Since $\gamma\in G$, we have $c\bar{c}=-(a\bar{b}+\bar{a}b)$. If $\lambda\in\tilde{A}$ is any element

$$\begin{aligned}
\lambda c\bar{c}&=-\lambda(a\bar{b}+\bar{a}b)=-\lambda a\bar{b}-\bar{\lambda}ab+\bar{\lambda}ab-\lambda\bar{a}b\\
&=-a(\lambda\bar{b}+\bar{\lambda}b)+b(\bar{\lambda}a-\lambda\bar{a})\in Aa+A^*b.
\end{aligned}$$

This proves the lemma.

1.7. Lemma. *Let u be a unit in $\tilde{A}$ and $\gamma \in \Gamma(\mathfrak{q})$ be of the form $\begin{pmatrix} a & b & c \\ . & . & . \\ . & . & . \end{pmatrix}$. Then if $u \equiv 1 \pmod{a\bar{a}}$, $\theta(u)$ and γ commute modulo $E\Gamma(\mathfrak{q})$, $\left(\text{recall that } \theta(u) = \begin{pmatrix} u & 0 & 0 \\ 0 & \bar{u}^{-1} & 0 \\ 0 & 0 & u^{-1}\bar{u} \end{pmatrix}\right)$.*

Let $\eta = c(u^2\bar{u}^{-1} - 1)/a$ and $\xi = \{(u\bar{u} - 1)b + c\bar{\eta}\}/a$. These are elements of $\tilde{\mathfrak{q}}$ as is easily from our assumption that

$$u \equiv 1 \, (\operatorname{mod}(a\bar{a})).$$

Let $\varphi = \begin{pmatrix} 1 & \xi & \eta \\ 0 & 1 & 0 \\ 0 & -\bar{\eta} & 1 \end{pmatrix}$. Then $\varphi \in E\Gamma(\mathfrak{q})$ (A simple calculation shows that trace $\xi = \eta\bar{\eta}$; this takes into account the fact that $a\bar{b} + \bar{a}b + c\bar{c} = 0$). Both elements $\gamma\varphi$ and $\theta(u)\gamma\theta(u)^{-1}$ take the form

$$\begin{pmatrix} a & b + a\xi - c\bar{\eta} & a + c\eta \\ . & . & . \\ . & . & . \end{pmatrix}.$$

It follows again by an easy computation that $(\gamma\varphi) \cdot (\theta(u)\gamma\theta(u)^{-1})$ takes the form

$$\begin{pmatrix} 1 & 0 & 0 \\ . & . & . \\ . & . & . \end{pmatrix}$$

and hence belongs to $U^- \cap \Gamma(\mathfrak{q}) \subset E(\mathfrak{q})$. This proves our contention.

We need one more result before we can prove Proposition 1.2.

1.8. Lemma. *Let l denote the order of the group of roots of 1 in K. Let $d \in Z$ be a prime and d^e the highest power of d dividing l. Let $\mathfrak{q}$ be any ideal in A and $a \in \tilde{A}$ a unit modulo $\tilde{\mathfrak{q}}$. Then there exists $a_0 \in \tilde{A}$ with the following properties*

(i) $a_0 \equiv a \pmod{\mathfrak{q}}$

(ii) $\tilde{A}a_0 = \mathfrak{p}$, *a prime with* $\mathfrak{p} \neq \bar{\mathfrak{p}}$ *or* $\tilde{A}a_0 = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1, \mathfrak{p}_2$ *primes with* $\bar{\mathfrak{p}}_1 \neq \mathfrak{p}_2 \bar{\mathfrak{p}}_1 \neq \bar{\mathfrak{p}}_2$ *and* $\mathfrak{p}_i \neq \bar{\mathfrak{p}}_i$ *for* $i = 1, 2$.

(iii) $\tilde{A}/\tilde{A}a_0$ *contains no unit of order* d^{e+1}.

This lemma is proved in Serre [1970, Lemma 3 of § 2] except for the second condition. To secure the second condition we need a sharpening of Serre's Lemma 4 of § 2 in the cited reference which is used by him to prove his Lemma 3. The sharper version we need is

1.9. Lemma. *Let L be an abelian extension of K and P the set of prime ideals in K which do not ramify in L and do not split completely in L. Let P' be the set of prime ideals of K which are stable under Galois conjugation. Let Q be any finite set of prime ideals in K. Let $\mathfrak{q}$ be any non-zero ideal in A and $a \in \tilde{A}$ a unit modulo*

$\tilde{\mathfrak{q}}$. *Then there exists* $a_0 \in \tilde{A}$ *such that*

(i) $a_0 \equiv a \pmod{\tilde{\mathfrak{q}}}$

(ii) $\tilde{A} a_0 = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ *or* $\tilde{A} a_0 = \mathfrak{p}_1$ *with* $\mathfrak{p}_i \in P - P' - Q$, $\mathfrak{p}_1 \neq \mathfrak{p}_2, \bar{\mathfrak{p}}_2$.

For the sake of completeness we give a proof of Lemma 1.9 and deduce Lemma 1.8 from it. The proofs are essentially those of Serre for the corresponding results with minor modifications.

1.10. Proof of Lemma 1.9. Let $H_{\mathfrak{q}}$ be the ray class group of $\tilde{\mathfrak{q}}$ ($H_{\mathfrak{q}}$ = group of fractionary ideals of $\tilde{A}$ which are coprime to $\mathfrak{q}$, modulo the action of the group $\{x \in K \mid x = \lambda/\mu,\ \lambda, \mu$ coprime to $\mathfrak{q}$ and $x \equiv (1 \bmod \mathfrak{q})\}$. Let $K_{\mathfrak{q}}$ be the abelian extension of K with Galois group isomorphic to $H_{\mathfrak{q}}$ under the isomorphism given by the Artin-reciprocity map. Let $L_{\mathfrak{q}}$ be the composite of $K_{\mathfrak{q}}$ and L. Let $\alpha \in H_{\mathfrak{q}}$ be the image of $\tilde{A} a$ in $H_{\mathfrak{q}}$ and $\tilde{\alpha} \in \mathrm{Gal}(L_{\mathfrak{q}}/K)$ a lift of α. Set $\tilde{\alpha}_1 = \tilde{\alpha}$ if $\tilde{\alpha}$ is non-trivial on L; if $\tilde{\alpha}$ is trivial on L let $\tilde{\alpha}_1$ be any element of $\mathrm{Gal}(L_{\mathfrak{q}}/K)$ which is non-trivial on L and $\tilde{\alpha}_2 = \tilde{\alpha}_1^{-1} \tilde{\alpha}$. We have thus

$$\tilde{\alpha} = \pi \tilde{\alpha}_i \qquad i = 1 \text{ or } i = 1, 2.$$

For each i let $P(i)$ be the set of primes in $\tilde{A}$ whose Frobenius equals $\tilde{\alpha}_i$. Since $\tilde{\alpha}_i|_L$ is non-trivial, these primes cannot split completely in L. Now the set $P(i) - P'$ is infinite: this follows from the Čebotarev density theorem. We can therefore choose $\mathfrak{p}_i$ ($i = 1$ or $i = 1, 2$) such that $\tilde{\alpha}$ is the product $\prod \sigma_i$, σ_i being the Frobenius corresponding to $\mathfrak{p}_i$. Since $P(i) - P'$ is infinite we can, in case $\tilde{\alpha}_1 \neq \tilde{\alpha}$, choose $\mathfrak{p}_1$, $\mathfrak{p}_2$ such that $\mathfrak{p}_1 \neq \mathfrak{p}_2$ or $\bar{\mathfrak{p}}_2$. Then $\prod \mathfrak{p}_i$ being equivalent $a\tilde{A}$ modulo $\{x \in \tilde{A} \mid x \equiv 1 \bmod \mathfrak{q}\}$ the lemma follows

1.11. Proof of Lemma 1.8. To deduce Lemma 1.7 from Lemma 1.8 we use the same arguments as Serre (1970). Take for L the extension $K(\omega)$ where ω is a primitive $(d^{e+1})^{\text{th}}$ root of 1. Then a prime $\mathfrak{p}$ in K splits completely if and only (Norm $p - 1$) is divisible by d^{e+1} i.e. iff $\tilde{A}/\mathfrak{p}$ contains an element of order d^{e+1}.

1.12. Proof of Proposition 1.2. Let $\alpha \in A^*$ be any non-zero element. Let f: $\mathrm{SL}(2, k) \to G$ be the group homomorphism:

$$f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b\alpha & 0 \\ c\alpha^{-1} & d & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, k).$$

Then we can find an ideal $0 \neq \mathfrak{h} \subset A$ such that $f(\mathrm{SL}(2, \mathfrak{h}\mathfrak{q}) \subset \Gamma(\mathfrak{q})$ for all ideals $\mathfrak{q} \subset A$ and if $x \in \mathrm{SL}(2, A)$ with $f(x) \in \Gamma(\mathfrak{h}\mathfrak{q})$, $x \in \mathrm{SL}(2, \mathfrak{q})$ (here for an ideal $\mathfrak{a} \subset A$, $\mathrm{SL}(2, \mathfrak{a}) = \{x \in \mathrm{SL}(2, A) \mid x \equiv \mathrm{Id} \bmod \mathfrak{a}\}$). Now according to Serre (1970)

$$(*) \qquad [\mathrm{SL}(2, A), \mathrm{SL}(2, \mathfrak{q})] \subset E\,\mathrm{SL}(2, \mathfrak{q})$$

where $E\,\mathrm{SL}(2, \mathfrak{q})$ = group generated by unipotents in $\mathrm{SL}(2, \mathfrak{q})$. It is easily seen that

$$f(E\,\mathrm{SL}(2, \mathfrak{h}\mathfrak{q})) \subset E\Gamma(\mathfrak{q}).$$

We conclude from this that if u is a special unit, $\theta(u)$ commutes with $\Phi(\mathfrak{h}\,\mathfrak{q})=\Phi \cap \Gamma(\mathfrak{h}\,\mathfrak{q})$ modulo $E\Gamma(\mathfrak{q})$. In fact u being a special unit

$$\theta(u)=\begin{pmatrix} u & 0 & 0 \\ 0 & u^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{(the case } u\in A)$$

or

$$\theta(u)=\begin{pmatrix} u & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & u^{-2} \end{pmatrix}.$$

In the first case $\theta(u)$ is in the image of $\mathrm{SL}(2, A)$ and $\Phi(\mathfrak{h}\,\mathfrak{q})\subset f(\mathrm{SL}(2, \mathfrak{q})$ and our contention follows from $(*)$. In the second case $\theta(u)$ and Φ commute and the assertion is trivial.

We now set $\mathfrak{r}=\mathfrak{s}_0\,\mathfrak{t}\,\mathfrak{h}$. Suppose now $\gamma\in\Gamma(\mathfrak{q}\,\mathfrak{r})$ and u is a special unit. By Lemma 1.5 modifying γ by an element of $E\Gamma(\mathfrak{h}\,\mathfrak{s}_0\,\mathfrak{q})$. We may assume that

$$\gamma=\begin{pmatrix} a & b & c \\ . & . & . \\ . & . & . \end{pmatrix} \quad (\in\Gamma(\mathfrak{h}\,\mathfrak{s}_0\,\mathfrak{q}))$$

with a coprime to b as well as c. Now from Lemma 1.7, it is clear that there is some power of $\theta(u)$ that commutes with γ modulo $E\Gamma(\mathfrak{q})$. Let N be the smallest integer for which $\theta(u)^N$ commutes with γ modulo $E\Gamma(\mathfrak{q})$. It suffices to show that N divides l^2. Lemma 1.7 shows that if d is a prime in Z, and d^{N_d} the highest power of d dividing N, then N_d divides the order of the unit group of $\tilde{A}/\tilde{A}\,a\,\bar{a}$. The element a depends on γ – it is the first entry of γ – and may be varied by varying γ in its class mod $E\Gamma(\mathfrak{q})$. Consider now the ideal $\tilde{\mathfrak{q}}^+=\tilde{A}\,c\,\bar{c}\,\tilde{\mathfrak{q}}\,\tilde{\mathfrak{h}}\,\tilde{\mathfrak{s}}_0$; then a is unit modulo $\tilde{\mathfrak{q}}^+$. This is because $a\equiv 1 \pmod{\tilde{\mathfrak{q}}\,\tilde{\mathfrak{s}}_0\,\mathfrak{h}}$, $(a, c)=A$ and also $(a, \bar{c}) =\tilde{A}$: the last assertion follows from the equation

$$a\,\bar{b}+\bar{a}\,b+c\,\bar{c}=0$$

and the fact $(a, b)=\tilde{A}$: in fact if $\mathfrak{p}$ is a prime in $\tilde{A}$ dividing $\bar{a}$ and c, it must divide a as well since $(\bar{a}, \bar{b})=\tilde{A}$.

Fix a prime d in Z and choose an element a_0 as in Lemma 1.8 taking for $\mathfrak{q}$ in that Lemma the ideal $\mathfrak{q}^+=\tilde{\mathfrak{q}}^+\cap A$. Then,

$$a_0=a+\lambda, \qquad \lambda\in\tilde{\mathfrak{q}}^+$$

and by Lemma 1.6, we have

$$\lambda=\alpha\,a+\beta\,b$$

with $\alpha\in\mathfrak{s}_0\,\mathfrak{q}\,\mathfrak{h}\,A$ and $\beta\in\mathfrak{s}_0\,\mathfrak{q}\,\mathfrak{h}\,A^*$ so that

$$a_0=(\alpha+1)\,a+\beta\,b.$$

We now claim that $A\cdot(\alpha+1)+A^*\beta=A$. In fact if this were not the case we can find a prime ideal $\mathfrak{p}\subset A$ such that $\mathfrak{p}\supset A(\alpha+1)$ and $\mathfrak{p}\supset A^*\beta$. This implies that

$$\tilde{\mathfrak{p}}\supset a_0\,\tilde{\mathfrak{s}}.$$

Since $\tilde{\mathfrak{p}} \supset \tilde{A}(\alpha+1)$ and $\alpha \equiv 0 \pmod{\tilde{\mathfrak{s}}\tilde{\mathfrak{h}}}$, it follows that $\tilde{\mathfrak{p}}$ divides a_0. But by our choice of a_0 (cf. Property (ii) in Lemma 1.8) no proper ideal of $\tilde{A}$ coming from an ideal of A can divide a_0, a contradiction. Thus

$$A(\alpha+1)+A^*\beta=A.$$

Let $\xi \in A^*$ and $\eta \in A$ be chosen such that $(\alpha+1)\eta-\beta\xi=1$. It follows that

$$\varphi=\begin{pmatrix} \alpha+1 & -\alpha\xi & 0 \\ \beta & \eta-\beta\xi & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \Phi(\mathfrak{h}\mathfrak{q}).$$

Now $\gamma\varphi$ takes the form

$$\begin{pmatrix} a_0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}.$$

Since $\theta(u)$ and φ commute modulo $E\Gamma(\mathfrak{q})$ for a special unit u, we see that the integer N must divide the order of the group of units in $\tilde{A}/\tilde{A}\,a_0\,\bar{a}_0$ (Lemma (1.7)). We conclude that $N_d \leqq 2e_d = 2\max\{e \mid d^e \text{ divides } l\}$: note that $\tilde{A}/\tilde{A}\,a_0\,\bar{a}_0$ is isomorphic to a product of the form $\tilde{A}/\mathfrak{p}_1 \times \tilde{A}/\mathfrak{p}_1$ or of the form $\tilde{A}/\mathfrak{p}_1 \times \tilde{A}/\mathfrak{p}_1 \times \tilde{A}/\mathfrak{p}_2 \times \tilde{A}/\mathfrak{p}_2$ and $\tilde{A}/\mathfrak{p}_i$ ($\simeq \tilde{A}/\mathfrak{p}_i$) has no units of order d^{e+1}. This proves that N divides l^2.

As a corollary to Proposition 1.2 we see that we have

1.12. Proposition. *Let $\hat{\Gamma}(c)$ (resp. $\hat{\Gamma}(e)$) be the projective limit of the $\{\Gamma/\Gamma(\mathfrak{q}) \mid \mathfrak{q}$ a non-zero ideal in $A\}$ (resp. $\{\Gamma/E\Gamma(\mathfrak{q}) \mid \mathfrak{q}$ a non-zero ideal in $A\}$. Let C be the kernel of the natural map $\hat{\Gamma}(e) \to \hat{\Gamma}(c)$. Then for any special unit $u \in A$, $\theta(u)^{l^2}$ centralises C.*

1.13. It is easily seen that there is an element $\lambda \in A$ such that for a non-zero ideal $\mathfrak{b} \subset A$ we have (using the notations of the Introduction)

$$G(\lambda\,\mathfrak{b}) \subset \Gamma(\mathfrak{b}) \quad \text{and} \quad \Gamma(\lambda\,\mathfrak{b}) \subset G(\mathfrak{b})$$
$$E(\lambda\,\mathfrak{b}) \subset E\Gamma(\mathfrak{b}) \quad \text{and} \quad E\Gamma(\lambda\,\mathfrak{b}) \subset E(\mathfrak{b}).$$

One deduces immediately from this that $\hat{\Gamma}(e)$, (resp. $\hat{\Gamma}(c)$) can be identified with the closure of Γ in $\hat{G}(e)$ (resp. $\hat{G}(c)$) and consequently C may be identified with kernel $\pi(e,c)$: $\hat{G}(e) \to \hat{G}(c)$. It follows that the centraliser of C in $G(k)$ is a normal subgroup of $G(k)$ containing $\theta(u)^{l^2}$ for any special unit $u \in \tilde{A}$. This means that the centraliser of C in $G(k)$ is *infinite* and hence is all of $G(k)$. It follows that $\hat{G}(e) \to \hat{G}(c)$ is a central extension proving the main theorem in the special case of quasi split, non split G over k. (When $\boldsymbol{G}$ is *split* over k, $\boldsymbol{G} \simeq \mathrm{SL}(2)$ over k and the main theorem is due to Serre (1970)).

We have established

1.14. Theorem. *The main theorem is true for those G which are* **quasi split** *over k.*

§ 2. Construction of some central extensions

2.1. Notation. As in Chapter 1, k will be a global field Σ the set of its valuations, for $v\in\Sigma$, k_v will denote the completion of k w.r.t. v, S will be a non-empty finite subset of Σ containing all the archimedean valuations and A the ring of S-integers in k. From now on however G will denote a connected absolutely almost simple connected k-algebraic group of k-rank 1. If $L\supset k$ is any extension of k, $G(L)$ will denote the L-rational points of k and $G(L)^+$ the subgroup of $G(L)$ generated by L-rational unipotents contained in the unipotent radical of a *k-parabolic* subgroup of G. We fix once and for all two opposing maximal unipotent k-subgroups $U^{\pm}$ of G. We denote by $P^{\pm}$ the k-parabolic subgroups normalising $U^{\pm}$ and $M=P^+\cap P^-$. For any k-algebraic subgroup H of G, $H(L)$ will denote the L-rational points of H. From the work of Tits (1969) it is known that $U^{\pm}(L)$ generate $G(L)^+$ for all L. Platonov (1969) has shown that $G(L)=G(L)^+$ if L is a local field. Finally, let T denote the central k-split torus in M and N the normaliser of T in G. The following result is well known (Borel and Tits (1965)).

2.2. Lemma. *Let $x\in U(k)\, x\neq 1$. Then there exists unique elements $n(x)\in N(k)$, $f(x), g(x)\in U(k)$ such that*

$$x=f(x)\,n(x)\,g(x).$$

The element $n(x)$ conjugates U (resp. U^-) into U^- (resp. U^+).

2.3. Lemma. *Let $L\supset k$ be an infinite field. Then the set*

$$\Omega^-(L)=\{x\in U^-(L)\mid x=u\,w\,v,\ u\,v\in U(L),\ w\in N(L)\}$$

is Zariski dense in U^- and Zariski open in $U^-(L)$.

2.4. Definition. f: $\Omega^-(L)\to U(L)$, g: $\Omega^-(L)\to U(L)$ and n: $\Omega^-(L)\to N(L)$ are the maps given by

$$x=f(x)\,n(x)\,g(x),\qquad x\in\Omega^-(L).$$

2.5. Consider now the free product $G^*(L)=U^+(L)*U^-(L)$ of $U^+(L)$ and $U^-(L)$. To avoid confusion, when we consider an element $u\in U^{\pm}(L)$ as an element of $G^*(L)$ we will denote it by u^*. For $x\in\Omega^-(L)$, let

$$n^*(x)=(f(x)^*)^{-1}\cdot x^*\cdot(g(x^*))^{-1}.$$

If π^*: $G^*(L)\to G(L)^+$ is the natural map, evidently $\pi^*(n^*(x))=n(x)$ for all $x\in\Omega^-(L)$. Let $R(L)$ be the normal subgroup of $G^*(L)$ generated by $E^+\cup E^-$ where

$$E^{\pm}=\{(n^*(x)\,a^*\,n^*(x)^{-1})\,((n(x)\,a\,n(x)^{-1})^*)^{-1}\mid x\in\Omega^-(L),\ a\in U^{\pm}(L)\},$$

and

$$\tilde{G}(L)=G^*(L)/R(L).$$

2.6. Proposition. *$R(L)$ is in the kernel of π^*: $G^*(L)\to G(L)^+$. Under the map $\tilde{\pi}$: $\tilde{G}(L)\to G(L)^+$ induced by π^*, $\tilde{G}(L)$ is a central extension of $G(L)^+$.*

For $x \in U^+(L)$ or $U^-(L)$, we denote by $\tilde{x}$, x considered as an element of $\tilde{G}(L)$. For $x \in \Omega^-(L)$, let $\tilde{f}(x) = \widetilde{f(x)}$, $\tilde{g}(x) = \widetilde{g(x)}$ and $\tilde{n}(x) =$ Image of $n^*(x)$ in $\tilde{G}(L)$. We fix $\tau \in U^-(k) - \{1\} \subset \Omega^-(L)$ and denote $\tilde{n}(\tau)$ by $\tilde{w}$. Let $\tilde{M}(L)$ be the group generated by $\{\tilde{n}(\alpha) \cdot \tilde{n}(\beta) \mid \alpha, \beta \in \Omega^-(L)\}$. With this notation we will first establish the following

2.7. Claim. Any element $\varphi \in \tilde{G}(L)$ can be expressed as a product

$$\varphi = \tilde{x}\, \tilde{\xi}\, \tilde{u}\, \tilde{w}\, \tilde{z}\, \tilde{v}$$

where $x, u, v \in U(L)$, $\xi \in \Omega^-(L)$ and $\tilde{z} \in \tilde{M}(L)$.

Let $\tilde{G}'$ be the subset of elements of $\tilde{G}(L)$ which can be expressed in this form. Now $\Omega^-(L)$ and $U^+(L)$ are contained in $\tilde{G}'$ (this follows easily from the definition of $\tilde{M}(L)$ and $\Omega^-(L)$). Further from Lemma 2.2, it is easy to see that $\Omega^-(L) \cdot \Omega^-(L) = U^-(L)$. Thus it suffices to show that $\tilde{G}'$ is stable under left multiplication by

$$\{x \mid x \in U^+(L) \text{ or } \Omega^-(L)\}.$$

For $U^+(L)$ this is obvious. Suppose now

$$\varphi = \tilde{x}\, \tilde{\xi}\, \tilde{u}\, \tilde{w}\, \tilde{z}\, \tilde{v}$$

is as above and $\eta \in \Omega^-(L)$. Then we have

$$\tilde{\eta} = \tilde{f}(\eta)\, \tilde{n}(\eta)\, \tilde{g}(\eta)$$

so that

$$\begin{aligned} \tilde{\eta}\, \varphi &= \tilde{f}(\eta)\, \tilde{n}(\eta)\, \tilde{g}(\eta)\, \tilde{x}\, \tilde{\xi}\, \tilde{u}\, \tilde{w}\, \tilde{z}\, \tilde{v} \\ &= \tilde{f}(\eta)\, \tilde{\lambda}\, \tilde{a}\, \tilde{\mu}\, \tilde{m}\, \tilde{v} \end{aligned}$$

where

$$\begin{aligned} &\lambda (= n(\eta)\, g(\eta) \cdot x\, n(\eta)^{-1}) \in U^-(L) \\ &a (= n(\eta)\, \xi\, n(\eta)^{-1}) \in U^+(L) \\ &\mu (= n(\eta)\, u\, n(\eta)^{-1}) \in U^-(L) \\ &\tilde{m} (= \tilde{n}(\eta)\, \tilde{w}\, \tilde{z}) \in \tilde{M}(L). \end{aligned}$$

Now in view of the relations $R(L)$ again,

$$\begin{aligned} \tilde{a} &= \tilde{n}(\eta)\, (\tilde{f}(\xi)\, \tilde{n}(\xi)\, \tilde{g}(\xi))\, \tilde{n}(\eta)^{-1} \\ &= \tilde{\alpha}\, \tilde{w}\, \tilde{p}\, \tilde{\beta} \end{aligned}$$

where $\alpha, \beta \in U^-(L)$ and $\tilde{p} \in \tilde{M}(L)$. We see now that

$$\tilde{\eta}\, \varphi = \tilde{f}(\eta)\, \tilde{\gamma}\, \tilde{w}\, \tilde{\delta}\, \tilde{h}\, \tilde{v}$$

where $\gamma, \delta \in U^-(L)$ and $\tilde{h} \in \tilde{M}(L)$: note that $\tilde{M}(L)$ normalises $U^+(L)$ and $U^-(L)$. Again conjugating $\tilde{w}$ past $\tilde{\delta}$ we see that

$$\tilde{\eta}\, \varphi = \tilde{f}(\eta)\, \tilde{\gamma}\, \tilde{d}\, \tilde{w}\, \tilde{h}\, \tilde{v}$$

with $d \in U(L)$. Let $\Omega = \{\theta \in \Omega^-(L) \mid \gamma\theta^{-1} \in \Omega^-(L)\}$ and $n(\theta)\, g(\theta)\, d n(\theta)^{-1} \in \Omega^-(L)\}$. Since $\Omega^-(L)$ is Zariski open in $U^-(L)$ it is immediate that Ω is *non-empty*. Pick any $\theta_1 \in \Omega$ and set $\gamma\theta_1^{-1}=\theta_2$. Then we have

$$\tilde\eta\,\varphi=\tilde f(\eta)\,\tilde\theta_2\,\tilde f(\theta_1)\,\tilde n(\theta_1)\,\tilde g(\theta_1)\,\tilde d\,\tilde w\,\tilde h\,\tilde v$$

and by the choice of θ_1, $n(\theta_1)\,g(\theta_1)\,d\,n(\theta_1)^{-1}=\Psi\in\Omega^-(L)$ so that we have

$$\begin{aligned}\tilde\eta\,\varphi&=\tilde f(\eta)\,\tilde\theta_2\,\tilde f(\theta_1)\,\tilde\Psi\,\tilde n(\theta_1)\,\tilde w\,\tilde h\,\tilde v\\&=\tilde f(\eta)\,\tilde\theta_2\,\tilde f(\theta_1)\,\tilde f(\Psi)\,\tilde n(\Psi)\,\tilde g(\Psi)\,\tilde h_1\,\tilde v\end{aligned}$$

with $\tilde h_1\in\tilde M(L)$. Since $\tilde h_1$ can be conjugated past $\tilde g(\Psi)$ to give an element of the form $\tilde h_1\cdot\tilde c$ with $c\in U(L)$ and $\tilde f(\theta_1)\,\tilde f(\Psi)\in U(L)$ as well the desired result follows. This proves Claim 2.7.

2.8. Completion of the proof of Proposition 2.6. Suppose now that $\varphi\in$kernel of $\tilde\pi$. Then we have setting

$$\varphi=\tilde x\,\tilde\xi\,\tilde u\,\tilde w\,\tilde z\,\tilde v$$

(with $x, u, v\in U(L)$, $\xi\in\Omega^-(L)$ and $\tilde z\in\tilde M(L)$)

$$1=\pi(\varphi)=x\,\xi\,u\,w\,z\,v$$

where $z=\pi(\tilde z)$ normalises both $U(L)$ and $U^-(L)$ and hence belongs to M. This leads to

$$\xi=x^{-1}\,v^{-1}\,z^{-1}\,w^{-1}\,u^{-1}$$

so that

$$f(\xi)=x^{-1}\,v^{-1}\quad\text{and}\quad g(\xi)=u^{-1}.$$

But then

$$\begin{aligned}\varphi&=\tilde v^{-1}\,\tilde f(\xi)^{-1}\,\tilde\xi\,\tilde g(\xi)^{-1}\,\tilde w\,\tilde z\,\tilde v\\&=\tilde v^{-1}\,\tilde n(\xi)\,\tilde w\,\tilde z\,\tilde v\\&=\tilde n(\xi)\,\tilde w\,\tilde z\,\tilde v_1\quad\text{with } v_1\in U(L).\end{aligned}$$

But this means

$$1=\pi(\varphi)=n(\xi)\,w\,z\,v_1$$

so that (on account of the uniqueness of the decomposition $P(L)=M(L)\,U(L)$, $v_1=1$. Thus

$$\varphi=\tilde n(\xi)\,\tilde w\,\tilde z\in\tilde M(L).$$

Since φ normalises $U(L)$ and $U^-(L)$ and projects to 1 under π, we conclude that φ must centralise $U(L)$ and $U^-(L)$ (in $\tilde G(L)$) and hence all of $\tilde G(L)$.

2.9. Proposition. *The extension constructed above is a universal central extension* i.e. *if f: $G_1\to G(L)^+$ is any central extension with $[G_1, G_1]=G_1$, there is a unique homomorphism f_1: $\tilde G(L)\to G_1$ such that $f\,f_1=\tilde\pi$.*

We use the following fact proved in Deodhar [1978, Theorem 1.9]. The map π^*: $G^*(L)\to G(L)^+$ factors through G_1. It suffices therefore to show that E^+ and E^- are in the kernel of this map of $G^*(L)$ in G_1. But this is clear since the action of G_1 on itself factors through the quotient $G(L)^+$.

2.10. Remark. The proposition proved above is a refinement (in the case of rank 1 groups) of Deodhar's theorem which concerns itself with the case $k=L$.

The generators given for $R(L)$ are much more economical than those given by Deodhar. (In the special case of quasi split groups Deodhar's theorem was obtained much earlier by Steinberg (1962).) Finally, note that Propositions 2.6. and 2.9 are valid for any field k. We will however need them only in the case when k is a global field and L is a completion of k. Our aim now is to obtain Adelic versions of these results. We begin with a result on Adèle groups of isotropic groups.

For a k-algebraic group H we denote by $H(A(S))$, the S-Adele group associated to H. With this notation we have

2.11. Proposition. *$G(A(S))$ is generated by $U^+(A(S))$ and $U^-(A(S))$ as a (n abstract) group (not merely as a topological group).*

For any $v \notin S$, $G(k_v)$ is generated by $U^+(k_v)$ and $U^-(k_v)$ as a group. This follows from the results of Platonov (1969). (If M is the common normalizer of U^+ and U^-, $U^+(k_v)$, $U^-(k_v)$ and $M(k_v)$ generate $G(k_v)$ so that the group generated $U^+(k_v)$ and $U^-(k_v)$ is normalised by $G(k_v)$ etc.) This means that we can replace S by any larger finite subset S_0 (as far as the proof of this proposition is concerned). We want to choose S_0 with the following properties. There is a reduced connected closed A_0-subscheme $\mathscr{H}$ of $\mathrm{GL}(n)$ ($A_0 = S_0$-integers in k) which is isomorphic to G over k, the inclusion $\mathscr{H} \hookrightarrow \mathrm{GL}(n)$ being a closed immersion. Moreover we want that for all $v \notin S_0$, the reduction modulo $\mathfrak{p}_v$, $\mathscr{H} \otimes_{A_0} A_0/\mathfrak{p}_v$ of $\mathscr{H}$ ($\mathfrak{p}_v$ = prime ideal in A_0 corresponding to v) is a connected simply connected reduced group-scheme over the residue field F_v. To the subgroups $U^\pm$ of G correspond in a natural fashion (unique) reduced closed subschemes $\mathscr{V}^\pm$ of $\mathscr{H}$. We assume that $\mathscr{V}^\pm$ admit good reductions modulo $\mathfrak{p}_v$, $v \notin S_0$ and that the F_v-rational points of $\mathscr{V}^+$ and $\mathscr{V}^-$ generate $\mathscr{H}(F_v)$. Let $\mathfrak{h}$ denote the A_0-Lie subalgebra of $M(n,k)$ corresponding to $\mathscr{H}$. Let $E_1, \dots, E_r$ be linearly independent *elementary* nilpotent matrices in $M(n, A_0)$ such that $M(n,k) = \mathfrak{h}_k + \sum_{i=1}^{k} k E_i$ where $\mathfrak{h}_k$, the k-span of $\mathfrak{h}$ can be identified with the Lie algebra $\mathfrak{g}$ of G. Suppose now that $X \in \mathfrak{h}$ is tangential to the centre of U^+, then $\mathfrak{g}$ is known to be the linear span (over k) of $\{\operatorname{Ad} g(X) | g \in H(A_0)^+\}$, $H(A_0)^+$ being the group generated by $U^\pm(A_0)$. We fix then conjugates $X_1, \dots, X_q$ (under $H(A_0)^+$) of X in $\mathfrak{h}$ which form a k-basis of $\mathfrak{g}$. For each X_i, $1 \leqq i \leqq q$ (resp. E_j, $1 \leqq j \leqq r$). We have unipotent 1-parameter subgroups of G i.e. morphisms φ_i, (resp. Ψ_j) $t \mapsto X_i(t)$ (resp. $t \mapsto E_j(t)$ of the additive group G_a in G such that X_i (resp. E_j) is tangential to φ_i (resp. Ψ_j). Then the map

$$\alpha\colon \prod_{(q+r)\text{ copies}} G_a \to \mathrm{GL}(n)$$

given by $(t_1, \dots, t_r, t_{r+1}, \dots, t_{r+q}) \to \prod_{1 \leqq j \leqq r} E_j(t_j) \cdot \prod_{1 \leqq i \leqq q} X_i(t_{j+r})$ the product taken in the natural order – has Jacobian of maximal rank at $(0, 0, \dots, 0) \in \prod G_a$. We assume S_0 so chosen that this polynomial map $\alpha(t \to \{\alpha_{ij}(t)\}_{1 \leqq i, j \leqq n})$ has all coefficients in the *ring* A_0 and the determinant of the Jacobian matrix of this map at $(0, \dots, 0)$ (it is a map k^{n^2} in $M(n,k) = k^{n^2}$) is a *unit* in A_0. For the local field k_v, $v \notin S_0$, this has the following implication. The natural map $\alpha_v\colon k_v \times \dots$

$\times k_v \to \mathrm{GL}(n, k_v)$ gives an analytic isomorphism of $\mathfrak{p}_v \times \ldots \times \mathfrak{p}_v$ onto $\mathrm{GL}(n, \mathfrak{p}_v) = \{u \in \mathrm{GL}(n, \mathfrak{O}_v) | u \equiv 1 \ (\mathrm{mod}\, \mathfrak{p}_v)\}$. (This follows easily from the usual proof of the inverse function theorem using the method of majorants.)

Next, we can find a k-representation ρ of $\mathrm{GL}(n)$ on a vector space W and a k-rational vector $w_0 \in W$ such that G is precisely the isotropy of w_0 in $\mathrm{GL}(n)$ and moreover the orbit map $g \to \rho(g) w_0$ is an immersion of $\mathrm{GL}(n)/G$ in W. This means of course that if ρ denotes the induced map of $M(n,k)$ in $\mathrm{End}(W)$, ρ is injective on the k-span of the E_i. Moreover, it is not difficult to see that after enlarging S_0, we can assume that w_0 belongs to a free A_0-submodule L in W of maximal rank containing the $\rho(E_i) w_0$, $1 \leqq i \leqq r$ as part of a A_0-basis of L such that we have for $t_i \in \mathfrak{p}_v$, $1 \leqq i \leqq r$,

$$\sum_{i=1}^{r} \rho(E_i(t_i)) \cdot w_0 \equiv \sum_{i=1}^{r} t_i \rho(E_i) w_0 \ (\mathrm{mod} \sum_{1 \leqq i, j \leqq r} t_i t_j L).$$

This shows in particular that

$$\prod_{i=1}^{r} \rho(E_i(t_i)) \prod_{j=1}^{q} \rho(X_j(t_{j+r})) w_0 = w_0$$

for $t_i \in \mathfrak{p}_v$ if and only if $t_i = 0$ for $1 \leqq i \leqq r$. We conclude then that for a suitable finite set S_0, the map α_v, $v \notin S_0$ induces an analytic isomorphism of $\mathfrak{p}_v \times \ldots \times \mathfrak{p}_v$ (q-factors) *onto* $G(\mathfrak{p}_v)$, the group $\{u \in G \cap \mathrm{GL}(n, \mathfrak{O}_v) | u \equiv 1 \ \mathrm{mod}\, \mathfrak{p}_v\}$. It is immediate from this that the group $\prod_{v \notin S_0} G(\mathfrak{p}_v)$ is contained in the abstract group generated by $\prod_{v \notin S_0} U^{\pm}(\mathfrak{O}_v)$. In fact we have proved more: there is an integer m such that any element of $\prod_{v \notin S_0} G(\mathfrak{p}_v)$ can be expressed as a word of length less than m in the elements of $\prod_{v \notin S_0} U^{\pm}(\mathfrak{O}_v)$. We will improve further on this: we will show that (at least after enlarging S_0 still further if necessary) that every element of $\prod_{v \notin S_0} G(\mathfrak{O}_v)$ is expressible as a word in the elements $\prod_{v \notin S_0} U^{\pm}(\mathfrak{O}_v)$ of length bounded above by a fixed integer. In order to do this we choose S_0 so that for all $v \notin S_0$, the reduction $\mathscr{H}_v \,\mathrm{mod}\, \mathfrak{p}_v$ of $\mathscr{H}$ is a smooth semisimple group scheme over the residue field and is also such that $\mathscr{V}^{\pm}$ admit smooth reductions which are unipotent radicals of opposing parabolic groups. Using then strong approximation for unipotent groups and the Bruhat-decompositions over the residue fields it is easily concluded that any $x \in \prod_{v \notin S_0} G(\mathfrak{O}_v)$ is expressible as a word in the elements of $\prod_{v \notin S_0} U^{\pm}(\mathfrak{O}_v)$ of length bounded above at least modulo $\prod_{v \notin S_0} G(\mathfrak{p}_v)$; the earlier assertion about $\prod_{v \notin S_0} G(\mathfrak{p}_v)$ now leads to the following observation which we record as a lemma for future use.

2.12. Lemma. *Let $U^{\pm}(\mathfrak{O})$ denote the product $\prod_{v \notin S} U^{\pm}(\mathfrak{O}_v)$. Let φ be the map of the m-fold product $\prod U^{+}(\mathfrak{O}) \times U^{-}(\mathfrak{O})$ (of $U^{+}(\mathfrak{O}) \times U^{-}(\mathfrak{O})$ with itself) into $G(A(S))$ given by*

$$\{(u_i^{+}, u_i^{-}) | 1 \leqq i \leqq m\} \to \prod_{i=1}^{m} u_i^{+} u_i^{-}$$

(taken in the natural order 1 *to* m*). Then the image of* φ *contains an open compact subgroup of* $G(A(S))$ *for some integer* $m>0$.

Now to conclude the proof of Proposition 2.11, we note first the $G(k)^+\cdot M=G(A(S))$ for any open subgroup M of $G(A(S))$ (and $G(k^+)$ is the group generated by $U^+(k)$ and $U^-(k)$. (This is a consequence of strong approximation for $U^\pm$ combined with the truth of the Kneser-Tits conjecture for local fields (Platanov (1969))); and we can choose for M an open subgroup contained in the image of φ as in Lemma 2.12 above.

2.13. Corollary. *The natural map* $U^+(A(S))*U^-(A(S))\to G(A(S))$ *is surjective.*

We end this chapter with two final results on central extensions of Adéle groups.

2.14. Proposition. *Let* $i^\pm$: $U^\pm(A(S))\to G(A(S))$ *denote the natural inclusions. Let* $\tilde G$ *be a second countable topological group and* π: $\tilde G\to G(A(S))$ *a continuous homomorphism. Suppose that we have continuous inclusions* $j^\pm$: $U^\pm(A(S))\to G$ *with the following properties*

(i) $j^\pm(U^\pm(A(S)))$ *generate* $\tilde G$ *as a topological group.*

(ii) *For* $v,w\notin S$, $v\neq w$, *either of the subgroups* $j^\pm(U^\pm(k_v))$ *and* $j^\pm(U^\pm(k_w))$ *commute with each other.*

(iii) *The natural map* f_v: $U^+(k_v)*U^-(k_v)\to\tilde G$ *contains* $R(k)$ (cf. § 2.5 for the definition) *in its kernel.*

(iv) $\pi\cdot j^\pm=i^\pm$.

Then π *is a central extension of* $G(A(S))$.

Let $\tilde G'$ be the abstract group generated by the images of $j^\pm$. We will first show that π': $\tilde G'\to G(A(S))$ is a central extension, π' being the restriction of π. Suppose $x\in\ker\pi'$, then x can be expressed in the form

$$x=g_1\cdot h_1\cdot g_2\cdot h_2\dots g_m\cdot h_m$$

with $g_i\in j^+(U^+(A(S)))$ and $h_i\in j^-(U^-(A(S)))$. In the sequel we identify $j^\pm(U^\pm(A(S)))$ with $U^\pm(A(S))$ themselves so that g_i (resp. h_i) will be regarded as elements of $U^+(A(S))$ (resp. $U^-(A(S))$. Using the fact that $U^\pm(A(S))$ is a restricted product each g_i (resp. h_i) can be expressed a limit of products of the form $\prod_{w\in S'} g_i(w)$ (resp. $\prod_{w\in S'} h_i(w)$) S' a finite set of valuations in the complement of S and $g_i(w)$, (resp. $h_i(w)$) in $U^+(k_w)$ (resp. $U^-(k_w)$). In view of (ii) we can express x as the limit of products of the form

$$x(S')=\prod_{w\in S'}(g_1(w)\,h_1(w)\,g_2(w)\,h_2(w)\dots g_m(w)\cdot h_w(w)).$$

That $\pi(x)$ is identity means that $\pi(x(S'))$ is identity for each S' so that each $x(w)$ is in the kernel of π. Now according to (iii) the kernel of f_w contains $R(k)$ and hence a simple continuity argument shows that it contains $R(k_w)$ as well. It follows now (Proposition 2.6) that $x(w)$ commutes with $U^\pm(k_w)$. By (ii) $x(w)$ commutes with $U^\pm(k_v)$ for $v\neq w$. Thus $x(w)$ is in the centre of $\tilde G$; as this holds for all w, x is in the centre of $\tilde{G}'$. Thus $\pi'\colon \tilde{G}'\to G(A(S))$ is a central extension. Let C' be the kernel of $\tilde{G}'$ and C the closure of C' in $\tilde{G}$. Clearly $\tilde{G}'C$ is again a central extension of $G(A(S))$. It suffices to show that $\tilde{G}'C$ is *closed* in $\tilde{G}$. For this, we know from Corollary 2.12 that there exists a *compact* subset M in $\tilde{G}'$ which maps onto an *open* subgroup of $G(A(S))$ under π. Suppose now that $E \subset \tilde{G}'C$ is a subset whose closure in $\tilde{G}$ is compact, then $\pi(\bar{E})$ ($\bar{E}$ = closure of E) is compact and hence contained in a finite union of translates of $\pi(M)$. It follows that we can find a *compact* subset F of $\tilde{G}'$ such that $\pi(F)\supset\pi(E)$ and FC is closed in $\tilde{G}$.

The second result is a partial converse to the previous one.

2.15. Proposition. *Let $\pi\colon \tilde{G}\to G(A(S))$ be a topological central extension and $j^{\pm}\colon U(A(S))\to\tilde{G}$ be continuous inclusions with $\pi\cdot j^{\pm}=i^{\pm}$. Then for $v\neq w$, $v,w\notin S$ each of $U^{\pm}(k_v)$ commutes with both $U^{\pm}(k_w)$. For each $v\notin S$ the natural map f_v: $U^{+}(k_v)*U^{-}(k_v)\to\tilde{G}$ contains $R(k)$ in its kernel.*

The second statement is immediate from Proposition 2.6. To prove the first fix $x\in U^{\pm}(k_w)$ (identified as a subgroup of $U^{\pm}(A(S))$ which in turn are treated as subgroups of $\tilde{G}$. Then the map $t\to t\times t^{-1}x^{-1}$ defines a homomorphism of the subgroup $\tilde{G}_v$ generated by $U^{\pm}(k_v)$ into the kernel of π (which is central). This homomorphism is moreover trivial on $\tilde{G}_v\cap\ker\pi$ and the quotient $\tilde{G}_v/\tilde{G}_v \cap\ker\pi$ is precisely $G(k_v)$, a group equal to its own commutator. It follows that this homomorphism is trivial proving our contention.

§ 3. The main theorem for $|S|\geqq 2$ and a special case

3.1. We continue with the notation introduced in Chapter 2 (specifically 2.1). We assume throughout this chapter that

$$\sum_{v\in S} k_v\text{-rank } G\geqq 2.$$

This hypothesis is satisfied if either of the two following conditions hold.

A. $|S|\geqq 2$.

B. $S=\{v\}$, k_v-rank $M'=0$, $M'\neq\{1\}$, k_v-rank $G\geqq 2$.

Recall that $M'=[M,M]$, M being the intersection $P^{+}\cap P^{-}$. If T is the central split torus in M, then $M=Z(T)$ is the centraliser of T. Let $x\in U^{-}(k)$ be any element with $x\neq 1$. As already observed in Lemma 2.2 we have

$$x=f(x)\cdot n(x)\cdot g(x)$$

with $f(x)$, $g(x)\in U^{+}(k)$ and $n(x)\in N(k)$ (N = normaliser of T). For $x\in U^{-}(k)$, $x\neq 1$, let $H(x)$ denote the k-subgroup of G generated by x, $n(x)$ and T. Then according to the main theorem of the Appendix (§ 5) $H(x)\simeq \mathrm{SL}(2)$ over k or there is a finite extension l of k and a quadratic Galois extension L of l such that over k, $H(x)\simeq R_{l/k}\mathrm{SU}(h)$, h a hermitian form in 3 variables over L with Witt index 1. Let $V^{-}(x)=H(x)\cap U^{-}$; then $V^{-}(x)$ is defined over k and is the unipotent radical of a minimal k-parabolic subgroup in H. Let U_1^- be the commutator subgroup of U^-. Then U^-/U_1^- is a vector space E over k and the image $\tilde{V}^-$ of $V^-(x)$ in U^-/U_1^- is a linear subspace. We also know that U_1^- is central in U^- and that $U_1^-(k)=[U^-(k), U^-(k)]$. Consequently, if $\Gamma\subset U^-(k)$ is a subset whose image in $E(k)$ generates all of $E(k)$, then Γ generates $U^-(k)$. These remarks enable us to establish the following

3.2. Lemma. *Assume that* (A) *or* (B) *of 3.1 holds. There is an element* $x\in U^-(k)$, $x\neq 1$ *such that the following two conditions hold*

(i) $U^-(k)$ *is the smallest subgroup of* $U^-(k)$ *containing* $V^-(x)$ (k) *and stable under* $M(k)$.

(ii) $\sum_{v\in S} k_v\text{-rank}\, H(x)\geqq 2$.

Proof. In the light of the comments at the end of 3.1 to show that $x\in U^-(k)$, $x\neq 1$, satisfies the first of these conditions, it suffices to prove that $E(k)$ is generated as an $M(k)$-module by $\tilde{V}^-(k)$. Since $\tilde{V}^-(k)$ is a *vector subspace* one may pass to the Zariski closures. From the chevalley commutation relations one establishes easily that E as a rational M-module is generated by a single element. Thus we have proved the set $\{x\in U^-(k),\ x\neq 1 \mid U^-(k)$ is the smallest $M(k)$-stable subgroup of $U^-(k)$ containing $V^-(x)\}$ is *Zariski open* in $U^-(k)$ and *non-empty* in $U^-(k)$. In view of this it suffices to show that the set

$$Y=\{x\in U^-(k) \mid x\neq 1,\ \sum_{v\in S} k_v\text{-rank}\, H(x)\geqq 2\}$$

is open and nonempty in the topology on k induced by the diagonal imbedding $k\to\prod_{v\in S} k_v$. When $|S|=2$, $Y=U^-(k)$ so we assume that $S=\{v\}$ and thus (B) holds. Now when (B) holds we have the following implications. Since $\sum_{v\in S} k_v$-rank $G\geqq 2$, M contains k_v-split torus of dimension $\geqq 2$. Since M' remains anisotropic over k_v, M must admit a central k_v-split torus of dimension $\geqq 2$. From the general structure theory (Borel and Tits (1965)) one knows that the centre of M has dimension at most 2. We see therefore that the centre of M contains a k-torus C *anisotropic over* k and *split* over k_v. This has also the implication that $U^\pm$ are not abelian. It follows that the k-root system $\Phi=\{\pm\alpha, \pm 2\alpha\}$ where α is a k-root such that the corresponding root space $\mathfrak{g}(\alpha)$ (in the Lie algebra $\mathfrak{g}$ of G) is tangential to U^+. Let T_v be a maximal k_v-split torus in M. Then $T_v=T\cdot C$ and it is a maximal k_v-split torus in G itself. Let $X^*(T_v)$ denote the character group of T_v and Φ_v the k_v-root system of G with respect to T_v. Introduce a linear ordering on $X^*(T_v)$ such that $\chi\in X^*(T_v)$ is positive if $\chi|T=r\cdot\alpha$ with $r>0$. Let Δ_v be the simple system for this ordering. Evidently $|\Delta_v|=2$. From the fact that C is anisotropic over k but splits over k_v one sees easily that every $\varphi\in\Delta_v$ restricts to α. Let $\Delta_v=\{\varphi,\psi\}$. Then φ and ψ have the same length: if they have different lengths, we will have a k_v-root of the form $p\varphi+q\psi$ with $p+q>2$ and then $(p\varphi+q\psi)|T=(p+q)\cdot\alpha$ would be a root, a contradiction. It follows that Δ_v is a root system of type A_2. It follows that we can find a k_v-imbedding λ: $\mathrm{SL}(3)\to G$ carrying diagonal matrices into

M and the upper and lower triangular unipotent subgroups of SL(3) into $U^{\pm}$ and the group $\left\{\begin{pmatrix} t & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & t^{-1}\end{pmatrix} \middle| t\in\bar{k}_v\right\}$ into T. Let $y=\begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \beta & \gamma & 1\end{pmatrix}\in \mathrm{SL}(3,k_v)$ with $\beta\neq 0$; then y admits a Bruhat decomposition of the form

$$y=\xi\begin{pmatrix} 0 & 0 & -\beta^{-1} \\ 0 & 1+\alpha\beta^{-1}\gamma & 0 \\ \beta & 0 & 1\end{pmatrix}\eta=\xi\cdot v(y)\cdot\eta,\quad \text{say}$$

with ξ,η upper triangular unipotent matrices in $\mathrm{SL}(3,k_v)$. It follows that $\lambda(y)\in\Omega^-(k_v)$ $(=\{x\in U^-(k_v)|x=f(x)\cdot n(x)\cdot g(x)$ with $f(x), g(x)\in U^+(k_v)$ and $n(x)\in N(k_v)\})$ and that $n(\lambda(y))=\lambda(v(y))$. Clearly $v(y)^2=\begin{pmatrix} -1 & 0 & 0 \\ 0 & \theta^2 & 0 \\ 0 & 0 & -1\end{pmatrix}$ where $\theta=1+\alpha\beta^{-1}\gamma$. It is clear from this that $v(y)^2$ generates a subgroup $\Gamma(y)$ which is *not* relatively compact modulo $\lambda^{-1}(T(k_v))$ iff $v(1+\alpha\beta^{-1}\gamma)\neq 0$. Now chose $\alpha,\beta,\gamma\in k_v$ such that $1+\alpha\beta^{-1}\gamma$ is not a v-adic unit and let $x\in U^-(k)$ be a close approximation to $\lambda(y)$ in the v-adic topology on $U^-(k_v)$. If the approximation is sufficiently close, $n(x)^2$ will be close enough to $\lambda(v|y)^2)$ to ensure that it generates a subgroup which is not relatively compact modulo $\lambda^{-1}(T(k_v))$. It follows that the group Γ_x generated by $n(x)^2$ in $M(k_v)$ does not have compact closure modulo $T(k_v)$. But from the structure of $\mathrm{SU}(h)$ it is clear that this means that k_v-rank $H(x)\geqq 2$. The argument shows that the set of $\{x\in U^-(k)|x\neq 1,\ k_v$-rank $H(x)\geqq 2\}$ is open in the v-adic topology as well. This completes the proof of Lemma 3.2.

3.3. We are now in a position to prove the main theorem using the results of Chapters 1 and 2 if A or B of 3.1 is satisfied. Recall that we fixed an imbedding G in $\mathrm{GL}(n)$ and defined $\hat{G}(c)$ as the S-adéle group of G viz the completion of $G(k)$ with respect to the family $\{G(\mathfrak{b})=x\in G\cap\mathrm{GL}(n,A),\ x\equiv 1 \bmod \mathfrak{b}\}$, $\mathfrak{b}$ a non-zero ideal in A. We also set $E(\mathfrak{b})=$group generated by $\{x\in G(\mathfrak{b})|x$ belongs to a maximal unipotent k-subgroup of $G\}$ and defined $\hat{G}(e)^+$ as the completion of $G(k)^+$ with respect to $\{E(\mathfrak{b})|\mathfrak{b}$ a nonzero ideal in A$\}$. Consider now the inclusion of $U^{\pm}(k)\rightarrow G(k)^+$. Since the $\{E(\mathfrak{b})\cap U^{\pm}(k)|\mathfrak{b}$ a non-zero ideal in A$\}$ is a fundamental system of congruence subgroups in $U^{\pm}(k)$, the closure of $U^{\pm}(k)$ in $\hat{G}(e)$ may be identified with the S-adéle group $U^{\pm}(A(S))$ of $U^{\pm}$. We see then that we have inclusions $j^{\pm}$: $U^{\pm}(A(S))\rightarrow\hat{G}(e)^+$ and we will show that all the hypotheses of Proposition 2.14 hold for the projection π: $\hat{G}(e)^+\rightarrow\hat{G}(c)=G(A(S))$. (That π is surjective is proved in Raghunathan [1976, Prop. 1.21]. That proof is essentially repeated in the next chapter: see Proposition 4.6.) The inclusions $j^{\pm}$: $U^{\pm}(A(S))\rightarrow\hat{G}(e)^+$ are evidently compatible with π and the natural inclusions $i^{\pm}$: $U^{\pm}(A(S))\rightarrow G(A(S))=\hat{G}(c)$. Since $U^{\pm}(k)$ generate $G(k)^+$ condition (i) of 2.14 holds. As has already been remarked condition (iv) holds. Assume now that (ii) holds. Then we assert that (iii) holds as well. Once condition (ii) holds the element $\tilde{n}(x)$, $x\in U^-(k)$, $x\neq 1$ can be written as product

$$\prod_{v\notin S}\tilde{n}(x)_v=\prod_{v\notin S}\tilde{f}(x)_v^{-1}\cdot\tilde{x}_v\cdot\tilde{g}(x)_v^{-1}$$

where $x = f(x) \cdot n(x) \cdot g(x)$ with $f(x), g(x) \in U^+(k)$ and $n(x) \in N(k)$ and for an element $\xi \in U^{\pm}(A(S))$, $\tilde{\xi}$ is ξ considered as an element of $\hat{G}(e)$ i.e. $\tilde{\xi} = j^{\pm}(\xi)$ and

$$\tilde{n}(x) = \tilde{f}(x)^{-1} \cdot \tilde{x} \cdot \tilde{g}(x)^{-1}.$$

Using the relation

$$\tilde{n}(x) \cdot \tilde{u}\, \tilde{n}(x)^{-1} = (n(x) \cdot u\, n(x)^{-1})^{\sim}$$

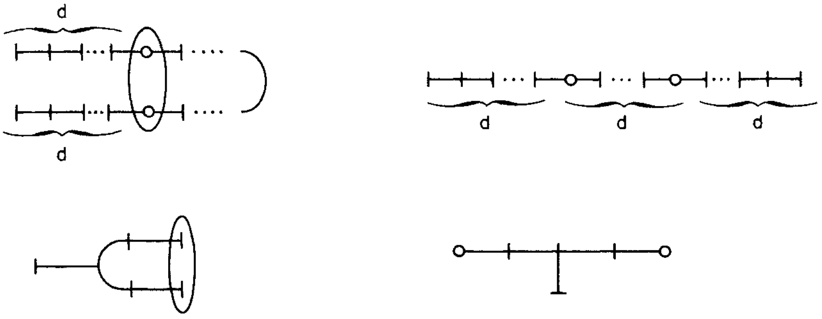
which holds for $x \in U^-(k)$, $x \neq 1$ and $u \in U^{\pm}(k)$ and the assumption that (ii) holds, it is clear that condition (iii) holds.

We are yet to establish that condition (ii) holds viz. that $j^{\pm}(U^{\pm}(k_v))$ and $j^{\pm}(U^{\pm}(k_w))$ commute for $v, w \notin S$, $v \neq w$. To see this choose x as in Lemma 3.2. Then by the results of Chapter 1, $j^-(V^-(x)(k_v))$ and $j^+(V(x)(k_w))$ where $V^{\pm}(x) = H(x) \cap U^{\pm}$ commute if $v \neq w$ (we have also made use of Proposition 2.15). Now consider the action of $M(k)$ on $j^+(U^+(k_w)) \times j^-(U^-(k_v))$. This action evidently factors through the natural action of $M(k_w) \times M(k_v)$ on $U^+(k_w) \times U^-(k_v)$, $v \neq w$. Now from the density of $M(k)$ in $M(k_w) \times M(k_v)$ and the fact that $V^+(x)(k_w)$ and $V^-(x)(k_v)$ commute and the first condition satisfied by x in Lemma 3.2, one sees easily that $j^+(U^+(k_w))$ and $j^-(U^-(k_v))$ commute. This shows condition (ii) of 2.14 satisfied. We have therefore shown

3.4. Theorem. *$\hat{G}(e)^+ \to \hat{G}(c)$ is a central extension if $|S| \geqq 2$ or if $S = \{v\}$ and k_v-*rank *$M' = 0$.*

3.5. In the next chapter we take up the case when $S = \{v\}$ and k_v-rank $M' \geqq 1$. Actually the techniques are such as to cover all cases when $\sum_{v \in S} k_v\text{-rank}\, M' \geqq 1$ – i.e. the cardinality of S is irrelevant in the proofs. Thus there is some overlap between the results of this chapter and the next. Unfortunately we have not been able to device a neat common approach to handle both cases simultaneously. As will be seen the methods in chapter 1 and chapter 4 have a lot in common. Finally when $|S| = 1$ relatively few groups are covered by the results in this chapter. In fact the possible Tits indices of groups satisfying (B) over k and k_v, $S = \{v\}$, are listed below.

Index over k *Index over k_v*



§ 4. The main theorem (continued)

4.1. We continue with the notations of the previous chapters (Chapters 2, 3 and the Introduction). Thus we fix a faithful k-representation $\rho\colon G \to \mathrm{GL}(n)$ and denote by $G(A)$ the group $\{x \in G(k) \mid \rho(x) \in \mathrm{GL}(n, A)\}$. We denote by I the family of non-zero ideals in A and for $\mathfrak{b} \in I$ recall that

$$G(\mathfrak{b}) = \{x \in G(A) \mid \rho(x) \equiv 1 \ (\mathrm{mod}\ \mathfrak{b})\}.$$

$E(\mathfrak{b})$ = group generated by $\{x \in G(\mathfrak{b}) \mid x$ belongs to a maximal unipotent k subgroup of $G\}$.

We have denoted by $\hat{G}(c)$ and $\hat{G}(e)^+$ the completions of $G(k)^+$ for the two topologies defined above. We will now introduce a third family of subgroups of $G(k)$. For a k-parabolic subgroup Q, let $Q' = [Q, Q]$. Then Q' is defined over k and contains the unipotent radical V of Q. If $Q = L \cdot V$, L reductive k-subgroup, is a Levi decomposition of Q over k and $L' = [L, L]$, evidently $Q' = L' \cdot V$ and L' is semisimple. For $\mathfrak{b} \in I$, let $Q'(\mathfrak{b}) = Q' \cap G(\mathfrak{b})$ (more generally for any k-subgroup H of G, $H(\mathfrak{b}) = H \cap G(\mathfrak{b})$). For $\mathfrak{b} \in I$, let $F(\mathfrak{b})$ be the subgroup of $G(k)$ generated by $\{Q'(\mathfrak{b}) \mid Q$ a minimal k-parabolic subgroup of $G\}$. Then the $\{F(\mathfrak{b}) \mid \mathfrak{b} \in I\}$ is a fundamental system of neighbourhoods of 1 in $G(k)$ for the structure of a topological group. We denote the corresponding completion by $\hat{G}(f)$. The inclusions $E(\mathfrak{b}) \hookrightarrow F(\mathfrak{b}) \hookrightarrow G(\mathfrak{b})$, $\mathfrak{b} \in I$ define continuous maps

$$\hat{G}(e)^+ \to \hat{G}(f)^+ \to \hat{G}(c)$$

of the corresponding completions of $G(k)$. In the present chapter we have to deal with the case when $|S| = 1$ so that $S = \{v\}$ and k_v-rank of $M' \geqq 1$ (recall that $M' = [M, M]$, $M = P^+ \cap P^-$; M is the centraliser of its maximal k-split torus in G). The condition $\sum_{v \in S} k_v$-rank $M' \geqq 1$ has the implication that for any proper k parabolic subgroup Q of G, $Q'(\mathfrak{b}) \neq V(\mathfrak{b})$, V the unipotent radical. A converse also holds: if $\sum_{v \in S} k_v$-rank $M' = 0$, $Q'(\mathfrak{b}) = V(\mathfrak{b})$, for all ideals $\mathfrak{b} \in I$ contained in a suitably chosen fixed ideal $\mathfrak{b}_0 \in I$. This is because we can find $\mathfrak{b}'_0 \in I$ such that $L'(\mathfrak{b}'_0) = 1$ for any Levi supplement L in Q. Since G has only finitely many $G(A)$ - conjugacy classes k-parabolic subgroups we see that the $\mathfrak{b}_0$ above can be chosen to be independent of Q (see Borel (1969), Behr (1969), Harder (1969)).

2. The remarks made in 4.1 clearly show that if $\sum_{v \in S} k_v$-rank $M' = 0$ then $\hat{G}(e)^+ \xrightarrow{\pi(e,f)} \hat{G}(f)^+$ is an *isomorphism*. We will now obtain more information on $\pi(e, f)$ when $\sum_{v \in S} k_v$-rank $M' > 0$. Although we have only the case when $|S| = 1$ left to be considered, the arguments used below make no use of the assumption that $|S| = 1$ so that we will not make that assumption. Some of the results proved below overlap with similar ones in Raghunathan (1976) but we have given detailed complete proofs to make the exposition self contained – and more importantly – pleasanter. We will begin by proving a known consequence of strong approximation which however is not set down in print.

4.3. Lemma. *Let H be a simply connected k-simple group with S-rank $H(=\sum_{v\in S} k_v$-rank $H)\geqq 1$. Let N be a non central subgroup of $H(k)$ normalised by an S-arithmetic subgroup Γ of H. Then the closure of N in $H(k)$ in the S-congruence ($=S$-adèle) topology is an open subgroup.*

Proof. Let $H(A(S))$ be the S-adèle group of H and $\bar\Gamma$ (resp. $\bar N$) the closure of Γ (resp. N) in $H(A(S))$. Then $\bar\Gamma$ is an open subgroup of $H(A(S))$ and hence contains a product of the form $\prod_{v\notin S}\bar\Gamma_v$ with $\bar\Gamma_v$ a compact open subgroup of $H(k_v)$ and $\bar\Gamma_v$ a maximal compact subgroup for almost all v. The group N being non-central in $H(k)$, the Zariski closure of N in H is all of H. From this it is easy to conclude that the closure of the group $[N,\bar\Gamma_v]$ ($=$group generated by $\{nxn^{-1}x^{-1}|n\in N, x\in\bar\Gamma_v\}$) is open in $G(k_v)$ for all $v\notin S$ and equals $\bar\Gamma_v$ for almost all v. (This is seen from a careful look at the structure of maximal compact subgroups in the $H(k_v)$). It is now clear from this that $\bar N$ is open in $H(A)$. The lemma follows easily from this.

4.4 Corollary. (i) *The closure $\tilde G(\mathfrak{b})$ of $E(\mathfrak{b})$ $\mathfrak{b}\in I$ in the S-adèle topology in $G(k)$ is open.*

(ii) *Let $M'=[M,M]$ the commutator subgroup of M. If $\sum_{v\in S} k_v$-*rank $M'\geqq 1$, *then for $\mathfrak{b}\in I$, $E(\mathfrak{b})\cap M'$ contains in its closure, in the S-adèle topology on $M'(k)$, an open subgroup of $M''(k)$ where M'' is the product of all the k-simple factors of M' which are isotropic over k_v for some $v\in S$.*

Proof. The first assertion is immediate from Lemma 3.3. To deduce the second assertion from Lemma 3.3, it suffices to show that for $\mathfrak{b}\in I$, $E(\mathfrak{b})\cap M''$ is Zariski dense in M''. To prove this consider the Zariski open set $B=U^-P^+$ in G. Then $E(\mathfrak{b})\cap B$ is Zariski dense in G. If we set $g=\beta(g)\cdot p(g)$ with $\beta(g)\in U^-$, $p(g)\in P^+$ then $g\to\beta(g)$ and $g\to p(g)$ are k-morphisms of B onto U^- and P^+ respectively. In particular $\beta(E(\mathfrak{b})\cap B)$ is Zariski dense in P^+. Let $g\in E(\mathfrak{b})$ and $J(g)=\{\theta\in M''(\mathfrak{b})|\theta u(g)\theta^{-1}u(g)^{-1}\in U^-(\mathfrak{b})\}$. Then $J(g)$ contains a congruence subgroup of $M''(\mathfrak{b})$. It follows that if $\theta\in J(g)$, $g\in E(\mathfrak{b})$,

$$\theta g^{-1}\theta^{-1}\cdot\theta u(g)\theta^{-1}u(g)^{-1}\cdot g\in E(\mathfrak{b}) \quad \text{i.e.}$$

$$\theta\cdot p(g)^{-1}\cdot\theta^{-1}\cdot p(g)\in E(\mathfrak{b}).$$

Varying $g\in B\cap E(\mathfrak{b})$ and $\theta\in J(g)$ we see that $E(\mathfrak{b})\cap{}''P^+$ where $''P^+=M''\cdot U^+$ is Zariski dense in $''P^+$. Now $''P^+$ being the semidirect product of $M''\cdot U^+$ we can write any $x\in{}''P^+$ in the form $\varphi(x)\cdot\psi(x)$ with $\varphi(x)\in M''(k)$, $\psi(x)\in U^+(k)$, φ,ψ being k-morphisms. It follows that there is a $\lambda\in A$ such that $\varphi(x)\in M''(\lambda^{-1}\cdot\mathfrak{b})$ and $\psi(x)\in U(\lambda^{-1}\mathfrak{b})$ if $x\in P''(\mathfrak{b})$. It is now clear that $\varphi(''P\cap E(\lambda\mathfrak{b}))\subset E(\mathfrak{b})$ so that $E(\mathfrak{b})\cap M''$ is Zariski dense in M''.

4.5. Corollary. *The closure of* $E(\mathfrak{b})$, $\mathfrak{b}\in I$ *in $\hat G(f)^+$ is an open subgroup. Equivalently for* $\mathfrak{b}\in I$, *there is a* $\mathfrak{b}'$ *in I such that for any* $\mathfrak{a}\in I$,

$$E(\mathfrak{b})\cdot F(\mathfrak{a})\supset F(\mathfrak{b}').$$

Proof. Let Q be a minimal k parabolic subgroup of G, V its unipotent radical and $Q=L\cdot V$ a Levi decomposition of Q. Let $L'=[L,L]$ and L'' the product of all its k-simple factors which are k_v-isotropic for some $v\in S$. Then according to the Corollary 4.4 above, there is an ideal $\mathfrak{b}'(L,V)$ such that for any $\mathfrak{a}\in I$,

$$E(\mathfrak{b})\cdot F(\mathfrak{a})\supset M''(\mathfrak{b}'(L,V))$$

and we may assume $\mathfrak{b}'(L,V)$ so chosen that

$$M''(\mathfrak{b}'(L,V))=M'(\mathfrak{b}'(L,V)),$$

and that $\mathfrak{b}'(L,V)\subset\mathfrak{b}$. It follows that $E(\mathfrak{b})F(\mathfrak{a})$ contains $Q'(\mathfrak{b}'(Q))$ for some $\mathfrak{b}'(Q)\in I$ depending on Q. Now we may assume that $\mathfrak{b}'(Q)=\mathfrak{b}'(Q_1)$ if Q and Q_1 are conjugate by an element of $G(A)$. Since G has only finitely many $G(k)$-conjugacy classes of minimal k-parabolic subgroups we can find $\mathfrak{b}'\in I$ independent of the minimal k-parabolic subgroup Q such that $Q'(\mathfrak{b}')\subset E(\mathfrak{b})\cdot F(\mathfrak{a})$ for any $\mathfrak{a}\in I$. This proves our contention.

4.6. Proposition. *Let* $\pi(e,c)$ (resp. $\pi(e,f)$)) *be the homomorphism of* $\hat{G}(e)^+$ *in* $\hat{G}(c)$ (resp. $\hat{G}(f)^+$) *induced by the inclusions* $\{E(\mathfrak{b})\to G(\mathfrak{b})|\mathfrak{b}\in I\}$ (resp. $\{E(\mathfrak{b})\to F(\mathfrak{b})|\mathfrak{b}\in I\}$. *Then* $\pi(e,c)$ (resp. $\pi(e,f)$) *is onto.*

Proof. We will prove the assertion for $\pi(e,c)$. The proof for $\pi(e,f)$ is analogous and uses Corollary 4.5 instead of Corollary 4.4(i). Let $\mathfrak{b}_n$ be a sequence of ideals in I such that any $\mathfrak{b}\in I$ contains $\mathfrak{b}_n$ for some n. From the density of $G(k)$ in $\hat{G}(e)$ and $\hat{G}(c)$ and the openess of $G(A)$ in the S-adéle topology of $G(k)$, one sees easily that the surjectivity of $\pi(e,c)$ is equivalent to the surjectivity of the map of projective limits

$$\varprojlim_n G(A)/E(\mathfrak{b}_n)\to\varprojlim_n G(A)/\tilde{G}(\mathfrak{b}_n)$$

where $\tilde{G}(\mathfrak{b}_n)$ is the closure in $G(k)$ of $E(\mathfrak{b}_n)$ for the S-adéle topology. ($\tilde{G}(\mathfrak{b}_n)$ form a fundamental system of open neighbourhoods of 1 in $G(k)$ for the S-adéle topology: Corollary 4.4(i).) Suppose now that $\{x_n\in G(A)/\tilde{G}(\mathfrak{b}_n)|1\leq n<\infty\}$ is an element of the projective limit. It suffices to construct a sequence $y_n\in G(A)/E(\mathfrak{b}_n)$ such that y_n maps to x_n (resp. y_{n-1}) under the natural map of $G(A)/E(\mathfrak{b}_n)$ onto $G(A)/\tilde{G}(\mathfrak{b}_n)$ (resp. $G(A)/E(\mathfrak{b}_{n-1})$). We will define y_n inductively. Assume y_n chosen for $n<N$ with the requisite properties. Let y' (resp. y'') be an element of $G(A)/E(\mathfrak{b}_N)$ which maps to x_N (resp. y_{N-1}) under the natural map. Then $y'\cdot y''^{-1}\in\tilde{G}(\mathfrak{b}_{N-1})/E(\mathfrak{b}_N)$. It follows that we can find $z\in E(\mathfrak{b}_{N-1})$ such that $y'\cdot y''^{-1}\in z\cdot G(\mathfrak{b}_N)/E(\mathfrak{b}_N)$. Clearly then the element zy'' maps to y_{N-1} in $G(A)/E(\mathfrak{b}_{N-1})$ and to x_N in $G(A)/\tilde{G}(\mathfrak{b}_n)$. This proves the proposition.

We will now establish

4.7. Theorem. $\hat{G}(e)^+$ *is a central extension of* $\hat{G}(f)^+$.

Proof. Let Q be a minimal k-parabolic subgroup with a Levi-decomposition $Q=L\cdot V$, L reductive, V unipotent radical, defined over k. Let Q^- be the opposing parabolic to Q determined by Q so that $L=Q\cap Q^-$. Let $L'=[L,L]$ and L''

the product of all the k-simple factors of L' which are isotropic over k_v for some $v \in S$. Let $DL(\mathfrak{b}) = L''(\mathfrak{b}) \cdot E(\mathfrak{b})/E(\mathfrak{b})$ and $\hat{D}L$ the projective limit of the $DL(\mathfrak{b})$, $\mathfrak{b} \in I$. Then $\hat{D}L$ has a natural identification with a subgroup of $\hat{G}(e)$ contained in kernel $\pi(f, e)$. Let Ψ be the subgroup of $G(k)$ generated by $V(A)$ and $V^-(A)$. Then since $[V^{\pm}(A), L''(\mathfrak{b})] \subset V^{\pm}(\mathfrak{b}) \subset E(\mathfrak{b})$ we see that Ψ centralises $\hat{D}L$. Since $[R(k), L''(\mathfrak{b})]$ is trivial where R is the central split torus in L, we conclude that the group generated by $R(k)$ and Ψ is in the centraliser of $\hat{D}L$. But it is easy to see that $R(k)$ and Ψ generate all of $G(k)^+$. Now from Corollary 4.5, it is easily seen that the image $\hat{D}L$ in $F(\mathfrak{b})/E(\mathfrak{b})$ contains a subgroup of the form $E(\mathfrak{b}) \cdot L''(\mathfrak{b}')/E(\mathfrak{b})$ where $\mathfrak{b}' \in I$ is an ideal depending on L and $\mathfrak{b}$. If we set $Q'' = L'' \cdot V$, then Q'' is independent of the choice of L and we see that for $\mathfrak{b} \in I$ there is an ideal $\mathfrak{b}'' = \mathfrak{b}(Q)$ such that the image of $\hat{D}L$ in $F(\mathfrak{b})/E(\mathfrak{b})$ contains $Q''(\mathfrak{b}'') \cdot E(\mathfrak{b})/E(\mathfrak{b})$. As $[G(k)^+, \hat{D}(L)]$ is trivial, setting $G(A)^+ = G(k)^+ \cap G(A)$, we have

$$[Q''(\mathfrak{b}''), G(A)^+] \subset E(\mathfrak{b}).$$

Now $\mathfrak{b}'' = \mathfrak{b}''(Q'')$ can be taken to be the same for all k-parabolics Q in the same $G(A)$-conjugacy class. As there are only finitely many $G(A)^+$-conjugacy classes of k-parabolic subgroups in G, we can find a single ideal $\mathfrak{b}_0$ such that

$$[Q''(\mathfrak{b}_0), G(A)^+] \subset E(\mathfrak{b})$$

for all k-parabolic subgroups Q i.e. $[F(\mathfrak{b}_0), G(A)^+] \subset E(\mathfrak{b})$. In the projective limit this means that $G(A)^+$ centralises $\ker \pi(e, f)$. Since $G(A)^+$ is infinite and $G(k)^+$ has no proper infinite normal subgroup containing $G(A)^+$ and the centraliser of kernel $\pi(e, f)$ in $G(k)$ is a normal subgroup of $G(k)$, we conclude that kernel $\pi(e, f)$ is central in $\hat{G}(e)^+$.

4.8. Recall that we denote by B the Zariski open subset $U^- \cdot P^+$ of G. For $g \in B$ we defined $p(g)$, $\beta(g)$ by setting

$$g = \beta(g) \cdot p(g) \qquad \beta(g) \in U^- \quad \text{and} \quad p(g) \in P^+.$$

Then as already remarked $g \to \beta(g)$ and $g \to p(g)$ are k morphisms of B onto U^- and P^+ respectively inducing an isomorphism of algebraic varieties of B on $U^- \times P^+$. Suppose now that $g \in B \cap G(\mathfrak{b})$ - note $B \cap G(\mathfrak{b})$ is Zariski dense in G. Let

$$J(g) = \{\theta \in M(\mathfrak{b}) \mid \theta\, u(g)\, \theta^{-1} u(g)^{-1} \in U^-(\mathfrak{b})\}.$$

Then we know that $J(g)$ contains a congruence subgroup $M(\mathfrak{b}(g))$ of $M(\mathfrak{b})$. In particular the Zariski closure of $J(g)$ contains M'', the product of all those k-simple factors of M' which are isotropic over k_v for some $v \in S$. We will now obtain some more precise information on the ideal $\mathfrak{b}(g)$. Let V denote the representation space for ρ. This means that V is equipped with a k-basis. We assume as we may that this k-basis is compatible with the decomposition of V into weight spaces with respect to T. Let r be the largest positive half-integer such that $r\alpha$ is a weight of T. (Then all other weights of T are of the form $r\alpha - m\alpha$ or $r\alpha - m/2 \cdot \alpha$ where m is an integer.) Let $V(r\alpha)$ be the weight space of $r\alpha$ and N its dimension. Let $\bigwedge^N V = W$ and W^* the dual of W. Let $\mu = N \cdot r \cdot \alpha$ and

$W(\mu)$ (resp. $W^*(-\mu)$) be the eigen space of T in W (resp. W^*) corresponding to the eigen character μ (resp. $-\mu$). Then $\dim W(\mu) = \dim W^*(-\mu) = 1$ ($W(\mu) \simeq \bigwedge^{N} V(r\alpha)$) and these are non-degenerately paired. The basis of V determines moreover bases of W and W^* in a natural fashion so that whenever $\rho(g) \in \mathrm{GL}(n, A)$, g in its action on W and W^* leaves the A-span of these bases stable; moreover the two A-spans are non-degenerately paired over A. It follows that there are *integral* vectors $w \in W(\mu)$ and $w^* \in W^*(-\mu)$ with respect to these bases such that $\langle w, w^* \rangle = 1$.

Now define a k-regular function f on G by setting

$$f(g) = \langle g \cdot w, w^* \rangle.$$

Then f is a polynomial in the entries of $\rho(g)$ with *coefficients* in the ring A. It is well known and not difficult to see that B can be characterised as the (affine) open subset

$$\{g \in G \mid f(g) \neq 0\}.$$

It follows that the coordinate ring of B over k is precisely $k[X_{ij}]_{1 \leqq i, j \leqq n}(f^{-1})$ where X_{ij} is the k-regular function $g \to (i, j)^{\text{th}}$ entry of $\rho(g)$. Since $g \to p(g)$ is a k-morphism we can find polynomial P_{ij}, P'_{ij} (in (n^2+1)-variables) $1 \leqq i, j \leqq n$ with coefficients in k such that for $g \in B$

$$p_{ij}(g) \, (\overset{\text{def}}{=} (i,j)^{\text{th}} \text{ entry of } p(g)) = P_{ij}(X_{kl}, f^{-1})_{1 \leqq k, l \leqq n}(g)$$
$$p'_{ij}(g) \, (\overset{\text{def}}{=} (i,j)^{\text{th}} \text{ entry of } p(g)^{-1}) = P'_{ij}(X_{kl}, f^{-1})_{1 \leqq k, l \leqq n}(g).$$

It is now easy to deduce that there exist an integer N' and an element $t' \in A$ such that for all $g \in B \cap G(t'\mathfrak{b})$, $\mathfrak{b}$ *any* ideal in I,

$$f(g)^{N'}(p_{ij}(g) - \delta_{ij}) \in \mathfrak{b}$$
$$f(g)^{N'}(p'_{ij}(g) - \delta_{ij}) \in \mathfrak{b}.$$

A standard argument now shows that there exist $t \in A$ and an integer $N > 0$ such that

$$p(g)^{-1} \cdot \theta \cdot p(g) \, \theta^{-1} \in P^+(\mathfrak{b})$$

for all $g \in G(t\mathfrak{b}) \cap B$ and $\theta \in M((f(g)^N))$. In other words we may assume that $\mathfrak{b}(g) = (f(g)^N)$ so that

$$J(g) \supset M((f(g))^N).$$

This has the following consequence which we record as

4.9. Lemma. *If* $g \in G(t\mathfrak{b}) \cap B$ *and* $\theta \in M((f(g)^N)$ *then* $g^{-1} \theta g \theta^{-1} \in F(\mathfrak{b})$.

Proof. We have

$$\begin{aligned} \theta g \theta^{-1} &= \theta \cdot \beta(g) \cdot p(g) \, \theta^{-1} \\ &= \theta \cdot \beta(g) \, p(g) \, \theta^{-1} \cdot \theta \, p(g)^{-1} \cdot \theta^{-1} \cdot p(g) \cdot p(g)^{-1} \, \theta \, p(g) \, \theta^{-1} \\ &= \theta \, \beta(g) \, \theta^{-1} \, p(g) \cdot (p(g)^{-1} \, \theta \, p(g) \, \theta^{-1}) \\ &= \beta(g) \, p(g) \cdot p(g)^{-1} \, \beta(g)^{-1} \cdot \theta \, \beta(g) \, \theta^{-1} \, p(g) \, (\operatorname{mod} P(\mathfrak{b})) \\ &= g \cdot \{p(g)^{-1} \, \beta(g)^{-1} \, \theta \, \beta(g) \, \theta^{-1} \, p(g)\} \cdot (\operatorname{mod} F(\mathfrak{b})). \end{aligned}$$

Since $g\in G(\mathfrak{b})$ as also $\theta g\theta^{-1}$ and $p(g)^{-1}\beta(g)^{-1}\theta\beta(g)^{-1}\theta^{-1}p(g)=\xi$ evidently belongs to the maximal unipotent k-subgroup $p(g)^{-1}U^{-}p(g)^{-1}$ we see that $\xi\in F(\mathfrak{b})$ so that $g^{-1}\theta g\theta^{-1}\in F(\mathfrak{b})$.

4.10. Corollary. *For $g\in G(t\mathfrak{b})$ let $\Gamma(g)$ be the subgroup of $M(k)$ generated by $M((f(gh))^N$ for all $h\in F(t\mathfrak{b})$ such that $gh\in B$. Then*

$$[\Gamma(g), g]\subset F(b).$$

4.11. Theorem. *If $\sum_{v\in S} k_v$-rank $M'>0$, $\hat{G}(f)^+$ is a central extension of $\hat{G}(c)$.*

Proof. Let C denote the kernel of $\pi(f, c)$. Then the centraliser of C in $G(k)^+$ is a normal subgroup N of $G(k)^+$. Since $G(k)^+$ admits no proper infinite normal subgroup, it suffices to show that there is an infinite subgroup Γ of $M(k)$ contained in all the $\Gamma(g)$, $g\in G^*(t\mathfrak{b})$ where $G^*(\mathfrak{a})$ for $\mathfrak{a}\in I$ the closure in $G(k)$ of $F(\mathfrak{a})$ in the S-adéle topology. (We know from 3.4 that $G^*(\mathfrak{a})$ is open in the S-adéle topology; this combined with Corollary 3.10 gives the desired conclusion.) Now let $g\in G^*(t\mathfrak{b})$ $h_1\in F(t\mathfrak{b})$ be such that $gh_1\in B\cap G^*(t\mathfrak{b})$ and let $\mathfrak{a}=(f(gh_1)^N)$. Since $F(t\mathfrak{b})$ is dense in $G^*(t\mathfrak{b})$ in the S-adéle topology we can find $h_2\in F(t\mathfrak{b})$ such that $gh_1h_2\in G(t\mathfrak{a}\mathfrak{b})$. Since $f(1)=1$ and f has coefficients in A, one sees that $f(gh_1h_2)\equiv 1 \pmod{\mathfrak{a}}$. The theorem now follows from the lemma below (Lemma 4.12) taking for H in that lemma the group M'' which is product of all those k-simple factors of M' which are isotropic over k_v for some $v\in S$.

4.12. Lemma. *Let H be a k-simple group with S-rank $H\geqq 1$. Let $H\subset \mathrm{GL}(n)$ be an imbedding of H as a k-subgroup of $\mathrm{GL}(n)$. Let $H(A)=H\cap\mathrm{GL}(n, A)$ and for an ideal $\mathfrak{b}\subset A$, $H(\mathfrak{b})=\{x\in H(A)\,|\,x\equiv 1 \bmod \mathfrak{b}\}$. Then there is a subgroup $\Gamma\subset H(A)$ of finite index such that for any pair $\mathfrak{b}$, $\mathfrak{b}'$ of coprime ideals $H(\mathfrak{b})\cdot H(\mathfrak{b}')\supset\Gamma$.*

Proof. Let **B** be the closure of $H(\mathbf{A})$ in the S-adéle group $H(\mathbf{A})$ of A. Then **B** contains a product of the form $\prod_{v\notin S} B_v$ where each B_v is compact and open in $G(k_v)$ and B_v is a maximal compact subgroup of $G(k_v)$ for almost all v. Also for almost all v, say $v\notin S'$ $(S'\supset S)$

$$H(k_v)\cap \mathrm{GL}(n, \mathfrak{O}_v)=B_v$$

and we may assume that for $v\in S'-S$

$$B_v=\{x\in H(k_v)\cap\mathrm{GL}(n, \mathfrak{O}_v)\,|\,x\equiv 1 \bmod \mathfrak{p}_v^{n_v}\}$$

where n_v, $v\in S'$ are suitably chosen integers. Now let $\Gamma=H(A)\cap\prod_{v\notin S} B_v$. We claim that $H(\mathfrak{b})\cdot H(\mathfrak{b}')\supset\Gamma$. If $\mathfrak{b}=\prod_{v\notin S}\mathfrak{p}_v^{b_v}$, then the closure of $H(\mathfrak{b})$ contains the group $\{x\in B_v\,|\,x\equiv 1 \pmod{\mathfrak{p}_v^{b_v}}\}$. Similarly if $\mathfrak{b}'=\prod_{v\notin S}\mathfrak{p}_v^{b'_v}$, the closure of $H(\mathfrak{b}')$ contains the groups

$$\{x\in B_v\,|\,x\equiv 1 \pmod{\mathfrak{p}_v^{b'_v}}\}.$$

The assumption that $(\mathfrak{b}, \mathfrak{b}')=A$ now readily yields the conclusion that $H(\mathfrak{b})\cdot H(\mathfrak{b}')$ contains in its closure $\prod_{v\notin S'} B_v$ and hence $H(\mathfrak{b})\cdot H(\mathfrak{b}')\supset\Gamma$.

4.13. Corollary (to 3.11). *If* $\sum_{v\in S} k_v$-rank $M'\geqq 1$, $\hat{G}(e)^+\to\hat{G}(c)$ *is a central extension.*

Proof. The extensions $\hat{G}(f)^+\to\hat{G}(c)$ and $\hat{G}(e)^+\to\hat{G}(f)^+$ are central. Let $z\in$kernel of $\pi(e,c)$ and $g\in G(k)^+$. Then since $\hat{G}(f)^+\to\hat{G}(c)$ is central $g z g^{-1} z^{-1}\in$kernel $\pi(e,f)$. For fixed z, $g\to g z g^{-1} z^{-1}$ is then a homomorphism of $G(k)^+$ in kernel $\pi(e,f)$. Since $G(k)^+$ is perfect this homomorphism is trivial. As $z\in$kernel $\pi(e,c)$ is arbitrary, $G(k)^+$ centralises kernel of $\pi(e,c)\cdot G(k)^+$ being dense in $\acute{G}(e)$ the corollary follows.

§ 5. Appendix: Imbedding quasi split groups

We prove in this appendix a result of some independent interest on semisimple algebraic k-groups of k-rank 1 over an *arbitrary* field k. Let G be such a group and T a maximal k-split torus and $Z(T)$ (resp. N) its centraliser (resp. normaliser). Let Φ be the k-root system of G with respect to T. Let U be a maximal unipotent k-subgroup of G normalised by T and $\alpha\in\Phi$ the unique k-root such that the Lie algebra $\mathfrak{u}$ of U is spanned by eigen spaces of T corresponding to the characters $\{r\alpha \mid r>0$ an integer$\}$. Then $\Phi=\{\pm\alpha\}$ or $\{\pm\alpha, \pm 2\alpha\}$. Let U^- be the unique opposing maximal unipotent k-subgroup of G to U also normalised by T. Finally let U' denote the centre of U: note that $U\neq U'$ if and only if $2\alpha\in\Phi$ and in that case $U'=[U,U]$. We denote by N the normaliser of T in G. Then we have for each $z\in U(k)$, $z\neq 1$, the Bruhat decomposition

$$z=f(z)\cdot n(z)\cdot g(z)$$

with $f(z)$, $g(z)\in U^-(k)$ and $n(z)\in N(k)$ uniquely determined by z. With this notation our main result in this Appendix is the following.

5.1. Theorem. *Let* $x, y\in U(k)$ *with either* $x=y$ *and* $x^2\neq 1$ *or* $x, y\in U'(k)$, $x\neq 1$, $y\neq 1$. *Let* $H=H(x,y)$ *be the smallest algebraic subgroup of* G *containing* T, x, y *and* $n(x)$. *Then there is a finite (not necessarily separable) extension* k' *of* k, *an absolutely almost simple simply connected quasi split* k'*-group* H' *of* k'-rank 1 *and a central isogeny* F: $R_{k'/k}H'\to H$ *with the following properties. There is a maximal* k'*-split torus* T' *in* H' *such that the (unique) maximal* k*-split torus* T_0 *in* $R_{k'/k}T'(\subset R_{k'/k}H')$ *maps onto* T. *Moreover there is a maximal unipotent* k*-subgroup* U_0 *in* $R_{k'/k}H'$ *normalised by* T_0 *such that* $F\mid U_0$ *is a (separable) immersion and there exist* $x_0, y_0\in U_0(k)$ *with* $F(x_0)=x$ *and* $F(y_0)=y$. *The field* k' *is separable over* k *if and only if* $n(x)\cdot n(y)$ *is a semisimple element of* $G(k)$.

Remarks. The group H' is isomorphic either to SL(2) or to SU(h), the special unitary group of a hermitian form of Witt index 1 in 3 variables over a quadratic Galois extension l' of k'.

5.2. We consider first a special case. Let $\tau\in T$ be an element such that $\alpha(\tau)=-1$. Then τ represents a k-rational point of the adjoint group so that $\tau U(k)\tau^{-1}=U(k)$. The special case we consider is the case when $\tau x\tau^{-1}=x^{-1}$ and $x=y$. Observe that if $x\in U'$ then $\tau x\tau^{-1}=x^{-1}$. And if $x\in U'$ and $x=y$ Theorem 5.1 for such a pair follows from Theorem 7.2 of Borel and Tits (1965). It turns out the argument given there yields a proof also in the case $x=y$, $\tau x\tau^{-1}=x^{-1}$ (even if $x\notin U'$). This is done as follows. Let $E=U/U'$ and $\bar{x}$=image of x in $U/\bar{U}$. Then E is a vector space over k on which elements $t\in T$ act through the homothesy by $\alpha(t)$. Let $V\subset E$ be the 1-dimensional vector space (over k) determined by $\bar{x}$ and $\tilde{V}$ the inverse image of V in U. The commutator map $(\xi,\eta)\rightarrow\xi\eta\xi^{-1}\eta^{-1}$ of $U\times U$ in U' factors through to an *alternating* k-bilinear map $E\times E\rightarrow U'$. Since $\dim V=1$, and U' is *central* in U, we see that $\tilde{V}$ is *abelian*. It is evidently T-stable. We claim that the sequence

$$1\longrightarrow U'\longrightarrow\tilde{V}\xrightarrow{\pi}V\longrightarrow 1$$

admits a T-equivariant k-splitting r: $V\rightarrow\tilde{V}$ with $x\in r(V(k))$. When $\operatorname{char}k\neq 2$, consider the morphism $\xi\rightarrow\tau\xi\tau^{-1}\xi$ of $\tilde{V}$ into U' $(\subset\tilde{V})$. It is easily checked that on U' this induces the *isomorphism* $\xi\rightarrow\xi^2$ and that the kernel which contains x maps isomorphically onto V. This shows that the above sequence admits a T-equivariant k-splitting. When $\operatorname{char}k=2$, $\xi^2=\tau\xi\tau^{-1}\xi^{-1}=1$ for all $\xi\in\hat{V}$: this holds for $\xi\in U'$ as U' is a vector space over k; it holds for all txt^{-1}, $t\in T$ by assumption and $\tilde{V}$ is generated by U' and $\{txt^{-1}|t\in T\}$. Let $k[\tilde{V}]$ (resp. $k[V]$ resp. $k[U']$) denote the algebra of k-regular functions on $\tilde{V}$ (resp. V, resp. U'). Let $P(\tilde{V})$ (resp. $P(V)$, resp. $P(U')$ be the k-linear subspace of functions f in $k[\tilde{V}]$ (resp. $k[V]$, resp. $k[U']$) which satisfy

$$\Delta_{\tilde{V}}f=f\otimes 1+1\otimes f$$
$$(\text{resp. } \Delta_V f=f\otimes 1+1\otimes f$$
$$\text{resp. } \Delta_{U'}f=f\otimes 1+1\otimes f)$$

where $\Delta_{\tilde{V}}$ (resp. Δ_V, resp. $\Delta_{U'}$) is the diagonal map in $k[\tilde{V}]$ (resp. $k[V]$, resp. $k[U']$) defined by the group structure. Now since $\xi^2=1$ for all $\xi\in\tilde{V}$, $\tilde{V}$ is a vector space (over $\bar{k}$) and it follows that $P(\tilde{V})$ generates $k[\tilde{V}]$ as an algebra and the map $P(\tilde{V})\rightarrow P(U')$ is onto. Also since $P(\tilde{V})$ and $P(U')$ are T-stable and the T-action on these spaces are completely reducible one concludes that if $P(\tilde{V})\rightarrow P(U')$ admits a splitting r as a T-module. Now U' is a vector space over k with T acting on it through the character 2α. It is easy to see then that $P(U')$ contains $\dim U'$-dimensional vector subspace $P_0(U')$ such that $k[U']$ is the symmetric algebra on $P_0(U')$ and $t\in T$ acts on $P_0(U')$ as multiplication by $\alpha(t)^{-2}$. The T-module homomorphism r: $P_0(U')\rightarrow P(\tilde{V})\hookrightarrow k[\tilde{V}]$ evidently provides a splitting of the sequence

$$1\longrightarrow U'\longrightarrow\tilde{V}\xrightarrow{\pi}V\longrightarrow 1.$$

It follows that $\tilde{V}$ decomposes as a direct product $U'\times V_0$ where V_0 is a T-stable subgroup of $\tilde{V}$ which maps isomorphically onto V under π. The element $x\in\tilde{V}(k)$ goes over under this isomorphism into a pair (x',x_0) in $U'\times V_0$. Let $V(x)=\{(t^2x',tx_0)|t\in\bar{k}\}$ where V_0 is given the k vector space structure through the isomorphism $\pi|V_0$: $V_0\xrightarrow{\sim}V$ (and on U' we take the natural k-vector space structure). Then $V(x)$ is a k-subgroup of $\tilde{V}$ *containing* x and $\pi|_{V(x)}$: $V(x)\rightarrow V$ is clearly an *isomorphism*: $V(x)$ can be characterised as the Zariski closure of $\{t \times t^{-1} | t \in T\}$. We have thus proved

5.3. Lemma. *Assume that $\tau x \tau^{-1} = x^{-1}$. Then the Zariski closure of $\{t x t^{-1} | t \in T\}$ is a T-stable k-subgroup of U which is isomorphic to a 1-dimensional vector space with T acting through the character α.*

5.4. Once we have this lemma the method of Borel and Tits [1965, Theorem 7.2] carries over almost verbatim to our situation. We note that we have $\tau \xi \tau^{-1} = \xi^{-1}$ for all $\xi \in V(x)$ so that any $\xi \neq 1$ in $V(x)$ admits a Bruhat-decomposition of the form

$$\xi = \alpha \cdot n \cdot \alpha$$

with $\alpha \in U^{-}$ and $n \in N(T)$. Thus we have proved the theorem in the special case when $\tau x \tau^{-1} = x^{-1}$.

5.5. In the sequel we assume that $\tau x \tau^{-1} x \neq 1$ and $x = y$ or that $x, y \in U'$, $x \neq 1$, $y \neq 1$. We will take up the case when all the simple factors of G over the algebraic closure are of classical type. We may clearly assume that G is simply connected: this is because any central k-isogeny induces an isomorphism of maximal unipotent subgroups (and carries a maximal k-split torus to a maximal k-split torus). It is also obvious that we can assume that G is k-simple. Any k-simple group is k isomorphic to a group of the form $R_{l/k} H$ where l is a finite separable extension of k and H is an absolutely almost simple l-algebraic group. It is immediate now that we can assume that G *is absolutely almost simple* (and simply connected). *We will make this assumption in the sequel.* Let $X(T)$ be the character group of T. Then $X(T) \simeq Z$. Let λ be the unique generator of $X(T)$ which is a positive multiple of α. If $z \in U'(k)$, $z \neq 1$, one knows from a result of Borel and Tits (1965, Theorem 7.2) that there is a k-isomorphism φ_z: $\mathrm{SL}_2 \to H$ of SL_2 onto a k subgroup H of G such that λ_z (diagonals) $= T$ and $\varphi_z \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = z$. Using this imbedding and standard facts about representations of SL_2 it is easy to conclude the following: if ρ is an irreducible representation of G, then there is a positive integer $n(\rho)$ such that the weights of ρ with respect to T are $\{-n(\rho)\lambda + 2r\lambda | r$ an integer $0 \leqq r \leqq n(\rho)$. It may be remarked that $\alpha = \lambda$ or 2λ according as $2\alpha \in \Phi$ or $2\alpha \notin \Phi$. All the observations made so far are applicable without the assumption that G is of classical type over $\bar{k}$. The following proposition however is valid only when G is of classical type over $\bar{k}$.

5.6. Proposition. *If G is simply connected and of classical type over $\bar{k}$, then G admits a representation ρ such that the only weights of ρ with respect to T are $(\lambda, 0, -\lambda)$ or $(\lambda, -\lambda)$ according as 2α is or is not a root in Φ and the kernel of ρ, the induced representation of the Lie algebra, is central and consists of semisimple elements.*

5.7. This can for instance be checked using the Tits' classification (Tits, 1969). We will however give a proof using only classification over $\bar{k}$. In order to this, let T^* be a maximal torus in G and $X(T^*)$ its group of characters and introduce a linear ordering in $X(T^*)$ such that for $\varphi \in X(T^*)$, if $\varphi | T$ is a *positive* multiple of α, then $\varphi>0$. Let Δ^* be the simple root system of G with respect to T^* and the ordering chosen above. Let Φ^* be the root system of G with respect to T^* and for $\varphi\in\Phi^*$ and $\theta\in\Delta^*$, let

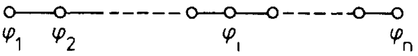
$$\varphi=\sum_{\theta\in\Delta^*} m_\theta(\varphi)\cdot\theta.$$

Let $\beta\in\Phi^*$ be the highest root in the ordering on $X(T^*)$. Then if $\Delta_0=\{\theta\in\Delta^*|\theta|_T=\alpha\}$, $\beta|T=\sum_{\theta\in\Delta_0} m_\theta(\beta)\cdot\alpha$. It follows that $\sum_{\theta\in\Delta_0} m_\theta(\beta)\leqq 2$ (and hence $|\Delta|_0\leqq 2$). Suppose now that Λ is a dominant weight for the root system Φ^* and ρ is any representation of G obtained by reduction of an irreducible representation in characteristic zero with dominant weight Λ. Then it is not difficult to see that the weights of ρ with respect to T are of the form

$$(-p\lambda,(-p+2)\lambda,\ldots,(p-2)\lambda,p\lambda)$$

where $p=\sum_{\theta\in\Delta_0} m_\theta(\Lambda)$. It is clear then that it suffices to show that if G is of classical type, we can find a dominant weight Λ such that $\sum_{\theta\in\Delta_0} m_\theta(\Lambda)=1$. We consider the different classical types separately.

5.8. Δ^* of type A_n, $|\Delta|_0=1$. The Dynkin diagram has the form (with $\Delta_0=\{\varphi_i\}$ say).



Let Λ be the dominant weight of natural representation, i.e. the fundamental weight corresponding to the root φ_n, say; then we have

$$\Lambda=\sum_{1\leqq j\leqq n} j\,\varphi_j/(n+1).$$

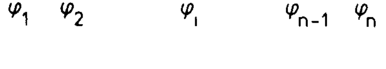
Sin $m_{\varphi_i}(\beta)=1$ $(\beta=\sum_{1\leqq j\leqq n}\varphi_j)$, we see that 2α is not a root so that $\alpha=2\lambda$. Evidently, $\Lambda|T=(i\,\varphi_i/n+1)|T=i\,\alpha|(n+1)$ necessarily an integral multiple of λ. We conclude then that $(n+1)=2i$ and $\Lambda|T=\lambda$.

5.9. Type A_n, $|\Delta|_0=2$. The Dynkin diagram is as above and $\Delta_0=\{\varphi_h,\varphi_i\}$ for some h, i with $1\leqq h<i\leqq n$. We take the same Λ as above and conclude that

$$\begin{aligned}\Lambda|T&=(h\,\varphi_h+i\,\varphi_i)|(n+1)|\,T=(h+i)\,\alpha/n+1|\,T\\&=(h+i)\,\lambda/(n+1)\end{aligned}$$

(as $\lambda=\alpha$: 2α is a root in this case) and $h+i=n+1$ is the only possible way in which $\Lambda|T$ can be an integral multiple of λ and then $\Lambda|T=\lambda$.

5.10. Type B_n. The Dynkin diagram is



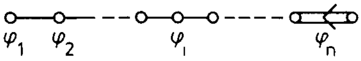
Since $\beta=\varphi_1+2\sum_{i>1}\varphi_i$, we have necessarily $|\Delta_0|=1$. The dominant weight Λ of the natural representation (=fundamental weight corresponding to φ_1) is given by

$$\Lambda=\sum_{1\leq j\leq n}\varphi_j.$$

It is clear then that $\Delta_0=\{\varphi_i\}$ with $i\neq 1$, $\Lambda|T=\alpha$ and 2α is a root.

Suppose then that $\Delta_0=\{\varphi_1\}$. We take for Λ the dominant weight of the spin representation $\Lambda=(\varphi_1+2\varphi_2+\ldots+n\varphi_n)/2$. Then clearly $\Lambda|T=\varphi_1/2|T=\lambda$ (and $\alpha=2\lambda$).

5.11. Type C_n. The Dynkin diagram is

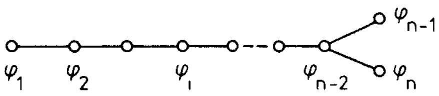


In this case $\beta=2\sum_{i<n}\varphi_i+\varphi_n$ so that $|\Delta_0|=1$ and 2α is a k root except when $\Delta_0=\{\varphi_n\}$. The dominant weight of the natural representation is

$$\Lambda=\sum_{i<n}\varphi_i+\varphi_n/2.$$

Evidently $\Lambda|T=\alpha$ or $\alpha/2$ according as 2α is a k root or not.

5.12. Type D_n. The Dynkin diagram is



We have $\beta=\varphi_1+2\sum_{1<i<n-1}\varphi_i+\varphi_{n-1}+\varphi_n$. The natural representation of $SO(2n)$ – the group of type D_n – has for dominant weight

$$\Lambda=(\sum_{1\leq i\leq n-2}\varphi_i)+(\varphi_{n-1}+\varphi_n)/2.$$

From the form of β, it is clear that either $\Delta_0=\{\varphi_i\}$ or $\Delta_0=\{\varphi_2,\varphi_j\}$ with $\{i,j\}$ $\{1,n-1,n\}$. From the form of Λ, it is clear that if $\Delta_0=\{\varphi_i\}$ with $i\neq 1$, then $\Lambda|T=\alpha$ or $\alpha/2$ according as $i<n-1$ or $i\in\{n-1,n\}$. If $\Delta_0=\{\alpha_{n-1},\alpha_n\}$ again Λ serves our purpose. Further Δ_0 cannot be of the form $\{\alpha_1,\alpha_{n-1}\}$ or $\{\alpha_1,\alpha_n\}$: if this happened $\Lambda|T$ would not be an integral multiple of λ.

In case $\Delta_0=\{\alpha_1\}$ so that $\alpha=2\lambda$, consider one of the spin representations say the one with dominant weight is

$$\Lambda=\{\varphi_1+2\varphi_2+\ldots+(n-2)\varphi_2+(n-1)\varphi_{n-1}/2+n\varphi_n/2\}/2.$$

Clearly then $\Lambda|T=\lambda$ $(=\alpha/2)$.

This completes the proof of Proposition 5.3.

5.13. Remark. The proposition is false for exceptional groups. As we will see later this necessitates additional arguments to cover exceptional groups.

5.14. Proposition 5.6 guarantees the existence of a representation of ρ of G on a vector space V defined over a finite separable extension l of k such that the set of weights of ρ with respect to T is of the form $(\lambda, 0, -\lambda)$ or $(\lambda, -\lambda)$ according as $\lambda=\alpha$ or $\alpha/2$. One then obtains a *k-representation* of G on $R_{l/k}V=E$ with $(\lambda, 0, -\lambda)$ or $(\lambda, -\lambda)$ as the set of weights for T according as $\lambda=\alpha$ or $\alpha/2$. We fix such a k-representation σ on the vector space E. We will make a further hypothesis on σ when $2\alpha\in\Phi$ but we now take up first the case when $2\alpha\notin\Phi$.

5.15. We assume in this and the next few paragraphs that 2α *is not a k-root.* We then have $U=U'$ is an *abelian* group. Consider the decomposition

$$E=E(\lambda)+E(-\lambda)$$

into the direct sum of $E(\lambda)$, the weight space of T corresponding to the weight λ and $E(-\lambda)$ the weight space corresponding to $-\lambda$. If we use a basis of E over k compatible with the direct sum decomposition above each $g\in G$ may be represented by a matrix of the form

$$\begin{pmatrix} A(g) & B(g) \\ C(g) & D(g) \end{pmatrix} (=\sigma(g))$$

where $A(g)$, $B(g)$, $C(g)$, $D(g)$ are $n\times n$-matrices with $n=\dim E(\lambda)=\dim E(-\lambda)$. If $g\in T$, $C(g)=B(g)=0$ and $A(g)=D(g)^{-1}$, a scalar matrix while if $g\in U$, $C(g)=0$ and $A(g)=D(g)=1$ (the identity matrix). The normaliser of $\sigma(T)$ $\left(=\left\{\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}\middle| t \text{ a scalar matrix}\right\}\right)$ in $\mathrm{GL}(E)$ is easily seen to be the group

$$\left\{\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}\middle| A, B \text{ nonsingular}\right\}\cup\left\{\begin{pmatrix} 0 & A \\ B & 0 \end{pmatrix}\middle| A, B \text{ nonsingular}\right\}.$$

The Bruhat decomposition $x=f(z)\cdot n(z)\cdot g(z)$ with $f(z)\in U(k)$, $g(z)\in U(k)$ and $n(z)\in N(k)$ for elements $z\in U(k)$ now shows that for $z\in U(k)$, $B(z)$ is *non-singular* $\left(\text{and } n(z)=\begin{pmatrix} 0 & B(z) \\ -B(z)^{-1} & 0 \end{pmatrix}\right)$. The choice of bases for $E(\lambda)$ and $E(-\lambda)$ may clearly then be made so that

$$\sigma(x)=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(1 representing the $(n\times n)$ identity matrix). For this choice of basis let $B(y)=B$:

$$\sigma(y)=\begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix}.$$

Let $\mathscr{B}$ be the k-subalgebra of $M(n,k)$ generated by B. If l is *any* k-algebra we have an inclusion then of $\mathrm{SL}(2, \mathscr{B}\otimes_k l)$ in $\mathrm{GL}(E)(l)$ i.e. we have a morphism of $R_{\mathscr{B}/k}\mathrm{SL}_2\to\mathrm{GL}(E)$ defined over k. The algebra $\mathscr{B}$ is evidently commutative. We will now show that $\mathscr{B}$ is a field. Let $\mathscr{B}'$ be the subset of $\mathscr{B}$ consisting of $\{B(z)\in\mathscr{B}\mid z\in U(k)\}$. From the fact that σ is *injective* on the Lie algebra of U and using the action of the adjoint torus of T on U, it is easy to see that $\mathscr{B}'$ is a k-vector space. (Observe that if $z, z' \in U(k)$ are such that $B(z)$, $B(z')$ are in $\mathscr{B}'$, then $B(zz') = B(z) + B(z')$ also belongs to $\mathscr{B}'$.) Suppose now that $z \in U(k)$, $z' \in U(k)$ are such that $B(z)$, $B(z')$ belong to $\mathscr{B}$ (hence $\mathscr{B}'$). Then it is easy to see that $n(z)$ and $n(z')$ belong to the image of $R_{\mathscr{B}/k}\mathrm{SL}(2)$. Since for $z \neq 1$ $\sigma(n(z)) = \begin{pmatrix} 0 & B(z) \\ -B(z)^{-1} & 0 \end{pmatrix}$ we have $\sigma(n(z))\,\sigma(n(x))^{-1} = \begin{pmatrix} B(z) & 0 \\ 0 & B(z)^{-1} \end{pmatrix}$; conjugating $\sigma(z')$ by this element, one sees that $B(z) \cdot B(z') \cdot B(z) \in \mathscr{B}'$ for any z, z' in $U(k)$ with $z \neq 1$ and $B(z), B(z') \in \mathscr{B}$. We now claim that $B(z)^n \in \mathscr{B}'$ for all integers $n > 0$ if $B(z) \in \mathscr{B}'$. We argue by induction on n. When $n = 0$ or 1 this is obvious. For $n \geqq 2$ we have taking z' to be such that $B(z') = B(z)^{n-2}$, $B(z)\,B(z')\,B(z) = B(z)^n \in \mathscr{B}'$. Taking $z = y$ we see that $\mathscr{B}'$ contains the k-algebra generated by $B(y)$ i.e. $\mathscr{B}' = \mathscr{B}$. Since every element of $\mathscr{B}'$ is of the form $B(z)$ for some $z \in U(k)$ and $B(z)$ is nonsingular if $z \neq 1$ i.e. if $B(z) \neq 0$, we conclude that $\mathscr{B} = \mathscr{B}'$ is a field. The algebra $\mathscr{B}$ is a separable extension of k if and only if $B(y)$ is semisimple: This is because $n(y)\,n(x)^{-1} = -n(y)\,n(x)$ is represented by the matrix $\begin{pmatrix} -B(y) & 0 \\ 0 & -B(y)^{-1} \end{pmatrix}$. This completes the proof of Theorem 5.1 when 2α is not a k-root.

5.16. We now take up the case when 2α is a k-root. (We continue to assume that G is of classical type.) From Proposition 5.3 we know that there exists a representation ρ of G on vector space V defined over a finite extension l of k such that the weights of ρ with respect to T are $(\lambda, 0, -\lambda)$. Replacing V by $R_{l/k}V$ we obtain a representation τ of G defined over k with $(\lambda, 0, -\lambda)$ as the weights of τ with respect to T. Let $\sigma = \tau \oplus \tau^*$, τ^* the dual of τ and E be the representation space for σ. The duality between τ and τ^* enables one to define on E a G-invariant non-degenerate alternating form. We decompose E over k into eigen-spaces for T:

$$E = E(\alpha) + E(0) + E(-\alpha).$$

Then the alternating form is non-degenerate on $E(0)$ and sets up a duality between $E(\alpha)$ and $E(-\alpha)$. Choosing bases of $E(\alpha)$, $E(0)$ and $E(-\alpha)$ over k suitably we may assume that the alternating form is represented by a matrix of the form

$$\begin{vmatrix} 0 & 0 & 1 \\ 0 & J' & 0 \\ -1 & 0 & 0 \end{vmatrix}$$

where 1 denotes the $(m \times m)$ identity matrix, $m = \dim E(\alpha) = \dim E(-\alpha)$ and J' is an alternating $(n \times n)$-matrix, $n = \dim E(0)$. (The first m basis elements form a basis of $E(\alpha)$, the next n of $E(0)$ and the last m of $E(-\alpha)$).

For $g \in G$ we set

$$\sigma(g) = \begin{vmatrix} A(g) & B(g) & C(g) \\ X(g) & D(g) & B^*(g) \\ Z(g) & Y(g) & A^*(g) \end{vmatrix}.$$

If $g\in U$ clearly $A(g)=A^*(g)$ and $D(g)$ are identity matrices while $X(g)=Y(g)$ and $Z(g)$ are zero. If $g\in T$ all non-diagonal blocks above are zero while $D(g)$ is the identity and $A(g)$ and $A^*(g)=A(g)^{-1}$ are scalar matrices. Suppose now that $z\in U(k)$ so that

$$\sigma(z)=\begin{vmatrix} 1 & B(z) & C(z) \\ 0 & 1 & B^*(z) \\ 0 & 0 & 1 \end{vmatrix}$$

one deduce easily from the fact that G leaves invariant the alternating form above that we have

$$(*) \qquad J' B^*(z)-{}^tB(z)=0$$

$$(**) \qquad C(z)-{}^tC(z)+{}^tB^* J' B^*=0.$$

5.17. Claim. If $z\in U(k)$, $z\neq 1$, then $C(z)$ is non-singular. If $\tau z \tau^{-1} z\neq 1$ and $B(z)\neq 0$, $B(z)\cdot B^*(z)$ is also nonsingular.

Proof. Let $\mathrm{Sp}(E)$ be the symplectic group of the alternating form on E chosen above. Let $\hat{T}=\sigma(T)$ and $\hat{N}$ the normaliser of $\hat{T}$ in $\mathrm{Sp}(E)$. Then $\sigma(N(T))\subset\hat{N}$. It is easy to check that

$$\hat{N}=\left\{\begin{pmatrix} A & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & A^* \end{pmatrix}\in \mathrm{Sp}(E)\right\}\cup\left\{\begin{pmatrix} 0 & 0 & A \\ 0 & D & 0 \\ A^* & 0 & 0 \end{pmatrix}\in \mathrm{Sp}(E)\right\}.$$

It is easy to see that $C(\sigma(n(z))=C(z)$ for $z\in U(k)$, $z\neq 1$ and since $n(z)\in\tilde{N}$, $C(z)$ is non-singular. Let $u=\tau z \tau^{-1} z$. (Then if char $k=2$, $u=z^2$.) A simple computation show that $B(u)$ and $B^*(u)$ are zero while

$$C(u)=2\,C(z)-B(z)\,B^*(z).$$

If $u\neq 1$, this proves that $B(z)\,B^*(z)$ is nonsingular when char $k=2$. When $k\neq 2$, let $v=\tau z \tau^{-1} z^{-1}$; then it is easily seen that $v\neq 1$ if $B(z)\neq 0$

$$C(v)=2B(z)\cdot B^*(z).$$

Thus we see that $B(z)\cdot B^*(z)$ is nonsingular.

5.18. Corollary. *For $z\in U(k)$ with $z^2\neq 1$ and $B(z)\neq 0$, $B^*(z)$ (considered as a homomorphism of $E(-\alpha)$ in $E(0)$) is injective and $B(z)$ (as a homomorphism of $E(0)$ in $E(\alpha)$) is surjective. Moreover* kernel $B(z)\cap$ Image $B^*(z)=\{0\}$. *Also* Kernel $B(z)$ *and* Image $B^*(z)$ *are mutually orthogonal to each other with respect to the alternating form and on each of these two subspaces of* $E(0)$, *the alternating form is non-degenerate.*

The last assertion is a consequence of $(*)$ of 5.13.

5.19. Assume now that $x=y\in U(k)$ and that $x^2\neq 1$, $B(x)\neq 0$. Corollary 5.15 gives a decomposition of $E(0)$ as a direct sum $E(0)=\text{Image}\,B^*(x)+\text{kernel}\,B(x)$. Let Image $B^*(x)=F(0)$ and kernel $B(x)=F'(0)$. Let $F=E(\alpha)+F(0)+E(-\alpha)$. The element $\sigma(x)$ operates trivially on $F'(0)$ and so does the torus T. Let $\{e_{n+m+1},$

$e_{n+m+2}, \dots, e_{n+2m}\}$ be the basis of $E(-\alpha)$ chosen above and we assume as we may that $B^*(e_{n+m+j}) \in F(0)$, $1 \leqq j \leqq m$ are part of the basis chosen and also that $BB^* e_{n+m+j} = e_j$, the basis for $E(\alpha)$ chosen. We assume further that the basis for $E(0)$ chosen above is compatible with the decomposition $E(0) = F(0) + F'(0)$. With respect to this (more careful by chosen) basis $\sigma(x)$ is represented by the matrix

$$\begin{vmatrix} 1 & 1 & 0 & C(x) \\ 0 & 1 & 0 & B_1^*(x) \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

where $B_1^*(x)$ is the matrix corresponding to the isomorphism defined by $\sigma(x)$ of $E(-\alpha)$ on $F(0)$. The matrix J' representing alternating form on $E(0)$ takes the form

$$\begin{pmatrix} J & 0 \\ 0 & J'' \end{pmatrix}$$

where J (resp. J'') represents the form on $F(0)$ (resp. $F'(0)$). The equations $(*)$ of 5.13 now shows that $B_1^*(x) = J^{-1}$ and $(**)$ leads us to

$$C(x) - {}^tC(x) + {}^tJ^{-1} \cdot J \cdot J^{-1} = 0.$$

Since J is antisymmetric this means that

$$C(x) - {}^tC(x) - J^{-1} = 0.$$

Let $\alpha = C(x) \cdot J$, then we have

$$\alpha - {}^tC(x) J - 1 = 0 \qquad \text{or again}$$

$$\alpha + J^{-1}\, {}^t\alpha J - 1 = 0.$$

Let $\mathscr{B}$ be the k-algebra generated by α in $M(m,k)$.

Then $\mathscr{B}$ is stable under the involution $\xi \mapsto J^{-1} \cdot {}^t\xi \cdot J$. It is easily seen that the involution is nontrivial in view of our assumption that $\tau \times \tau^{-1} \neq x^{-1}$. Let φ denote the hermitian form in 3 variables over $\mathscr{B}$ for the above involution given with respect to a basis f_{-1}, f_0, f_1 by the conditions

$$\varphi(f_0, f_{\pm 1}) = \varphi(f_{-1}, f_{-1}) = \varphi(f_1, f_1) = 0$$

$$+ \varphi(f_{-1}, f_{+1}) = \varphi(f_0, f_0) = \varphi(f_1, f_{-1}) = 1.$$

Let H denote the k-algebraic group $\mathrm{SU}(\varphi)$, the special unitary group of this hermitian form. There is a natural k-morphism F of $\mathrm{SU}(\varphi)$ in $\mathrm{Sp}(E)$ which maps the 3×3 matrix $(a_{ij})_{1 \leqq i, j \leqq 3}$ in $\mathrm{SU}(\varphi)$ into

$$\begin{vmatrix} a_{11} & a_{12} & 0 & a_{13} J^{-1} \\ a_{21} & a_{22} & 0 & -a_{23} J^{-1} \\ 0 & 0 & 1 & 0 \\ J a_{31} & -J a_{32} & 0 & a_{33} \end{vmatrix}.$$

We claim that $F(\mathrm{SU}(\varphi))\subset G$ and that $\mathscr{B}$ is a field. The arguments for this are analogous to those in the proof of the case when 2α is not a root and we leave out the details. Clearly $\mathscr{B}$ is separable over k if α is semisimple. A simple calculation shows that $\sigma(n(x)^2)$ is the matrix

$$\begin{vmatrix} \bar{\alpha}^{-1}\alpha & 0 & 0 & 0 \\ 0 & \bar{\alpha}^2\alpha^{-2} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \bar{\alpha}^{-1}\alpha \end{vmatrix}$$

where $\xi\to\bar{\xi}$ is the conjugation in $\mathscr{B}$. Since $\alpha+\bar{\alpha}=1$, α is semisimple if and only if $\bar{\alpha}^{-1}\alpha$ is. Thus $\mathscr{B}$ is separable over k if and only if $n(x)^2$ is semisimple (note that $g\in G$ is semisimple iff $\sigma(g)$ is semisimple since α is a central isogeny).

This completes the proof when all simple factors of G (over the algebraic closure) are of classical type. (Note that this include the groups of trialitarian D_4 type.) To handle the exceptional case we need the following.

5.20. Lemma. *Assume that G is exceptional (and absolutely simple). Let G^* denote the adjoint group of G and M^* the image of M in G^*. Let $\mathfrak{m}^*$ denote the Lie algebra of M^*. For $x, y\in U$, let $I(x, y)$ denote the isotropy group scheme at (x, y) of M^* acting by inner conjugation on $U\times U$. Let $\mathfrak{i}(x, y)$ denote the Lie algebra of $I(x, y)$. Then if either $x=y$ and $\tau x\tau^{-1}x\neq 1$ or if $x, y\in U'$, $\mathfrak{i}(x, y)(k)$ contains a non-zero semisimple element X_0.*

5.21. Once the lemma is accepted the theorem (for exceptional G) follows from induction on $\dim G$ since the theorem is known for classical groups. If (x, y) is as in Lemma and X_0 is chosen in $\mathfrak{i}(x, y)(k)$ as in the lemma, the centraliser $Z(X_0)$ of X_0 in G^* is a reductive k-group H^*. Evidently $(x, y)\in V^*$, the unipotent radical of the parabolic subgroup of H^* determined by the split torus $T^*\subset H^*$ (T^* is the image of T in G^*). If H_1^* denotes the (unique) isotropic semisimple normal subgroup of H^* and H_1 its simply connected cover, $H_1 = R_{l/k}H$ which H absolutely almost simple and l/k a finite separable and the problem reduces to proving the result for H; since $\dim H$ (over l) is evidently smaller than $\dim G$ (over k) induction hypothesis applies. Thus Lemma 5.20 yields the theorem.

The following result is well known (see Borel and Tits (1965) and Richardson (1967)).

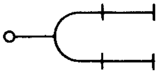
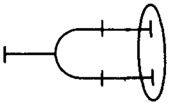
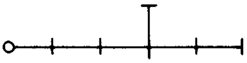
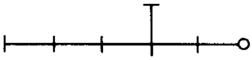
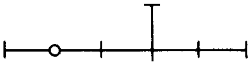
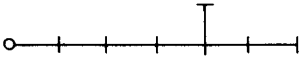
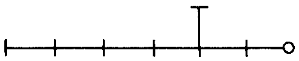
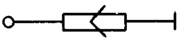
5.22. Proposition. *Let H be a absolutely almost simple k-algebraic group and $\mathfrak{h}$ its Lie algebra. Assume that H is anisotropic over k. Then $\mathfrak{h}(k)$ consists entirely of semisimple elements if one of the following conditions hold.*

(a) *k is perfect*	
(b) *H is of type B_n C_n or D_n,*	Char $k\neq 2$
(c) *H is of type G_2, F_4 or E_6,*	Char $k\neq 2, 3$
(d) *H is of type E_7*	Char $k\neq 2, 3, 5$
(e) *H is of type E_8*	Char $k\neq 2, 3, 5, 7$
(f) *H is of type A_n*	Char $k\nmid(n+1)$.

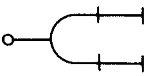
5.23. Corollary. *Lemma 5.20 holds if k is perfect or if* Char $k > 5$.

Proof. This follows from the Proposition above and the type of $\mathfrak{m}$ in the different exceptional k-groups of k-rank 1 which is listed below in the Table.

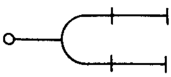
5.24. Table

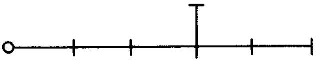
Case	Type	Tits Index	dim M	dim M'	dim U	dim U'	dim C
1.	${}^2E_{6,1}^{35}$		36	35	21	1	0 if $p \neq 3$ 1 if $p=3$
2.	${}^2E_{6,1}^{29}$		30	28	24	8	0 if $p \neq 3$ 1 if $p=3$
3.	$E_{7,1}^{78}$		79	78	27	27	0 if $p \neq 2$ 1 if $p=2$
4.	$E_{7,1}^{66}$		67	66	33	1	0 if $p \neq 2$ 1 if $p=2$
5.	$E_{7,1}^{48}$		49	48	42	10	0 if $p \neq 2$ 1 if $p=2$
6.	$E_{8,1}^{133}$		134	133	57	1	0
7.	$E_{8,1}^{91}$		92	91	78	14	0
8.	$E_{4,1}^{21}$		22	21	17	7	0

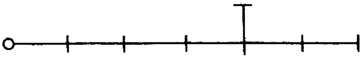
5.25. Using Proposition 5.22 and Corollary 5.23 we now see that we have now to establish Lemma 5.20 only in the following cases:

Char $k=2$. All diagrams of 5.24 other than the first (viz. ).

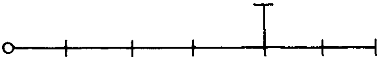
Char $k=3$. G has for its Tits Diagram one of the following:



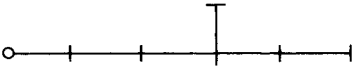




Char $k=5$. G has for its Tits diagram the diagram



When the Tits diagram of G is of the form



$U=U'$ (i.e. 2α is not a root) and we are to assume that $x \neq y$, $x, y \in U-\{1\}$. We will take up this case first.

5.26. Groups of type $E_{7,1}^{78}$ (Char $k=2, 3$). By examining the 27-dimensional representation of E_6 (which is the representation of $[M^*, M^*]$ on U) one has the following facts:

(i) There is a (M-stable) Zariski open subset $\Omega \subset U$ such that for any $x \in \Omega(\bar{k})$, the orbit map $g \to gx$ on M^* is a submersion of M^* *onto* U; the isotropy group scheme $I(x)$ at any $x \in \Omega(k)$ is thus reduced (i.e. smooth). Moreover $I(x)$ for $x \in \Omega(\bar{k})$ is a semisimple group of type F_4.

(ii) The complement of Ω in U contains an open M^*-orbit Ω_1 such that for any $x \in \Omega_1(l)$ $(k \subset l \subset \bar{k})$, $I(x)$ is a *reduced* group scheme isomorphic (over $\bar{k}$) to the semidirect product of the group Spin 9 with the (vector) representation space of the spin representation. Further the unipotent radical of this group $I(x)$ is defined and split over k.

(iii) Let $\bar{\Omega}_2 = \bar{\Omega}_1 - \Omega_1$ and $\Omega_2 = \bar{\Omega}_2 - \{1\}$; then Ω_2 is an orbit of M^* and for $x \in \Omega_2(l)$ $(l \subset \bar{k})$ the isotropy group scheme $I(x)$ is reduced and has a l-split nontrivial (connected) unipotent radical (infact $I(x)$ is of codimension 1 in a parabolic subgroup).

Now according to a theorem of Borel-Tits if a reductive k-group H admits a nontrivial k-split unipotent subgroup then the group H is isotropic. We see thus that for $x \in U(k)$, $I(x)$ is a k-form of F_4. Thus $I(x)$ has dim 54. It follows by looking at the orbit map $g \to gx$ of $I(x)$ in U - that $\dim I(x, y) \geqq 52-27=25$. Now if $\mathfrak{i}(x, y)$ has all elements nilpotent, then $I(x, y)$ would contain a connected a unipotent reduced subgroup scheme (over $\bar{k}$) of dimension $\geqq 25$. But any connected unipotent subgroup of $I(x)$ (note that $I(x, y) \subset I(x)$) has dimension $\leqq 24$. Thus $\mathfrak{i}(x, y)$ contain a nonzero semisimple element. Hence Lemma 5.20 holds for groups of type $E_{7,1}^{78}$.

5.27. Groups of Type ${}^2E_{6,1}^{35}$ (Char $k=3$). (The proof of Lemma 5.20 below for this case applies to all characteristics.) As $\dim U=21$ and $\dim M^*=36$, we see that $\dim I(x)$ $(=I(x, y)$ as $x=y)$ is at least $36-21=15$. If $I(x)$ has no semisimple elements, the group $I(x)_{\mathrm{red}}^0$ $(=$identity component of $I(x)_{\mathrm{red}})$ is unipotent and since 15 is the dimension of any maximal connected unipotent group of M^*-note that M' is of type A_5 i.e. SL(6)$-\mathfrak{i}(x)$ contains the Lie algebra $\mathfrak{u}$ of a maximal unipotent subgroup U of M^*. As $\mathfrak{i}(x)$ consists entirely of nilpotent elements, $\mathfrak{i}(x)=\mathfrak{u}$ so that $U=I(x)$; but then M^* will have to be quasi-split, a contradiction. This proves Lemma 5.20 for groups of type ${}^2E_{6,1}^{35}$.

5.28. Groups of Type $E_{8,1}^{133}$ (Char $k=2,3$ or 5). (Here again the proof below is valid in any characteristic.) The isotropy group $I(x)$ (we have $x=y$ as 2α is a root) has dimension at least $134-58=76$. On the other hand the dimension of a maximal connected unipotent group in M (hence also in M^*) is 63. Thus $I(x)_{\mathrm{red}}^0$ cannot be unipotent so that $\mathfrak{i}(x)$ contains a non-zero semisimple element.

5.29. Groups of Type $F_{4,1}^{21}$ (Char $k=2$). In the table this group is the only one with a root diagram having two different root lengths. (We will be giving a uniform proof to cover all groups other than $F_{4,1}^{21}$ and $E_{7,1}^{78}$ for fields of characteristic 2.) Here we assume that $x^2 \neq 1$ (Char $k=2$). Evidently $x^2 \in U'$ and the representation of M' on U' is the standard representation of an *anisotropic* special orthogonal group on a 7-dimensional vector space. It follows that the isotropy group $I'(x^2)$ at $x^2 \in U'(k)$ of M' acting on U is reduced and isomorphic to a special orthogonal group of an anisotropic quadratic form over k in 6 variables. If $I'(x)$ is the isotropy group at x for the action of M' on U, evidently $I'(x) \subset I'(x^2)$. On the other hand $\dim I'(x) \geqq 6$. Now the dimension of any (connected) unipotent subgroup of $I'(x^2)$ is at most 6. Consequently the Lie algebra $\mathfrak{i}'(x)$ of $I'(x)$ can consist entirely of nilpotent elements only if $\dim \mathfrak{i}'(x)=\dim I'(x)$ i.e. $I'(x)$ is reduced; but then $I'(x^2)$ would be quasi split, a contradiction. Thus $\mathfrak{i}'(x)$ contains a non-zero semisimple element; as $G \to G^*$ an isomorphism, in our case so is $\mathfrak{i}'(x) \to \mathfrak{i}(x)$ and Lemma 5.20 follows.

5.30. Combining Corollary 5.23 and the results in 5.26–5.29, we see that we are left with having to establish Lemma 5.20 only in the following cases:

Char $k=2$, diagram of G has all roots
of equal length and $U' \neq U$ i.e. 2α is a root

(even this has an overlap with 5.26–5.29; the proof below will cover all these cases namely all cases in Table 5.24 other than $E_{7,1}^{78}$ and $F_{4,1}^{21}$, Char $k=2$). Throughout the sequel unless otherwise specified we assume Char $k=2$. We begin however with a proposition valid in all characteristics.

5.31. Proposition. *Let k be of arbitrary characteristic and G an absolutely simple simply connected k-group. Assume that all roots in the Dynkin-diagram of G have the same length. Then the Lie algebra* $\mathfrak{g}$ *of G carries a G-invariant bilinear form defined over k satisfying the following conditions*

(i) $\langle\ ,\ \rangle$ *is symmetric and if* Char $k=2$, $\langle v, v\rangle=0$ *for all* $v \in \mathfrak{g}(\bar{k})$.

(ii) *Let* $Q^{\pm}$ *be opposing parabolic subgroups and* $V^{\pm}$ *their respective unipotent radicals. Let* $\mathfrak{q}^{\pm}$ (resp. $\mathfrak{v}^{\pm}$) *be the Lie subalgebra of* $\mathfrak{g}$ *corresponding to* $Q^{\pm}$ (resp. $V^{\pm}$). *Then* $V^{\pm}$ *is orthogonal to* $\mathfrak{q}^{\pm}$ (*for* $\langle\ ,\ \rangle$) *and* $\langle\ ,\rangle$ *gives a non-degenerate pairing between* $\mathfrak{v}^{+}$ *and* $\mathfrak{v}^{-}$.

(iii) *If* $\mathfrak{v}$ *is the Lie algebra of a connected reduced unipotent subgroup scheme of G and B its reduced normaliser then* $\mathfrak{v}$ *is orthogonal to the Lie algebra* $\mathfrak{b}$ *of B.*

Proof. Let $\tilde{T} \subset G$ be a maximal torus over $\bar{k}$ and $\mathfrak{g}(\beta)$ the root space of β, the highest root of G with respect to $\tilde{T}$ and an ordering on the character group $X(\tilde{T})$ of $\tilde{T}$. Then $\dim \mathfrak{g}(\beta) = 1$ and $\mathfrak{g}$ as a G-module is generated by $\mathfrak{g}(\beta)$. Let $\mathfrak{g}^*$ be the dual of $\mathfrak{g}$ as a G-module and $\mathfrak{g}^*(\beta)$ the weight space corresponding to β in $\mathfrak{g}^*$. Then $\dim \mathfrak{g}^*(\beta) = 1$ as well. Now any G-module homomorphism of $\mathfrak{g}$ in $\mathfrak{g}^*$ necessarily carries $\mathfrak{g}(\beta)$ to $\mathfrak{g}^*(\beta)$ and is determined by this element of $\operatorname{Hom}(\mathfrak{g}(\beta), \mathfrak{g}^*(\beta))$. One concludes that the space of G-invariant bilinear forms on $\mathfrak{g}$ is of dimension 1. It is now clear that for a bilinear form $\langle\ ,\ \rangle$ satisfying (i)–(iii) above, a suitable scalar multiple of it would be defined over k. Thus we can for the purposes of this lemma replace k by $\bar{k}$. Over $\bar{k}$, $g \simeq \mathrm{Ch} \otimes_{\mathbf{Z}} \bar{k}$ where Ch is a Chevalley Lie algebra over $\mathbf{Z}$. Let $\{E_\alpha | \alpha \in \Phi\} \cup \{H_\alpha | \alpha \in \Delta\}$ be a Chevalley basis of Ch. Let ψ denote the Killing form on Ch. Then we have for an integer $C > 0$

$$\psi(E_\alpha, E_\beta) = C\,\delta_{\alpha\beta}, \quad \alpha, \beta \in \Phi,$$
$$\psi(H_\alpha, H_\beta) = C \cdot 2\langle\alpha, \beta\rangle / \langle\alpha, \alpha\rangle, \quad \alpha, \beta \in \Delta,$$
$$\psi(H_\alpha, E_\beta) = 0, \quad \alpha \in \Delta,\ \beta \in \Phi.$$

Where $\langle\ ,\ \rangle$ is any Weyl group invariant scalar product on the $\mathbf{Q}$-span of the $\{H_\alpha | \alpha \in \Delta\}$; the fact that all root lengths in Δ are equal has been used above. We now set $\langle X, Y\rangle = C^{-1}\psi(X, Y)$ for $X, Y \in \mathrm{Ch}$. It is evident then that $\langle\ ,\ \rangle$ defines a scalar product on $\bar{k}$ by extension scalars. Using extensions of $\mathbf{Q}$ which are unramified at $p = \operatorname{Char} k$ of arbitrary degree, one sees that $\langle\ ,\ \rangle$ defines on $\mathrm{Ch} \otimes_{\mathbf{Z}} \bar{f}_p$, $\bar{f}_p =$ algebraic closure of the prime field of p elements which is invariant under the $\bar{f}_p$-rational points of Chevalley group scheme. Zariski density of this group of points in G (identified with the Chevalley group scheme over $\bar{k}$ using the inclusion $\bar{f}_p \to \bar{k}$) shows that $\langle\ ,\ \rangle$ is G-invariant. For standard parabolic subgroups of G (given by the Chevalley basis), the assertion in (ii) is immediate from the definitions. For a general parabolic group the required assertion follows from the fact that any pair of opposing parabolic subgroups can be conjugated to a standard pair by an element of $G(\bar{k})$. The last assertion is a consequence of a theorem of Borel Tits to the effect that any connected reduced unipotent subgroup scheme V of G is contained in the unipotent radical of a parabolic subgroup, the latter containing the reduced normaliser of V (Borel and Tits (1971)).

5.32. Claim. *Let $x \in U(k)$ be such that $x^2 \neq 1$. Let X be the image of $x \in U/U'$ $\simeq \mathfrak{g}(\alpha)$ (in a natural fashion). Then*

(i) $(\operatorname{ad} X)^2$: $\mathfrak{g}(-\alpha) \to \mathfrak{g}(\alpha)$ *is an isomorphism*

(ii) $\operatorname{ad} X(\mathfrak{g}(-\alpha)) \cap \mathfrak{c} = 0$ *where $\mathfrak{c}$ = centre of* $\mathfrak{g}$

(iii) $\langle\ ,\ \rangle$ *is non-degenerate on* $\operatorname{ad} X(\mathfrak{g}(-\alpha))$

(iv) $\operatorname{ad} X$: $\mathfrak{m} \to \mathfrak{g}(\alpha)$ *is surjective.*

Proof. $\operatorname{Ad} x = 1 + \operatorname{ad} X + \varphi(X)$ where $\varphi(X)$: $\mathfrak{g} \to \mathfrak{g}$ is an endomorphism carrying $\mathfrak{g}(-\alpha)$ (resp. $\mathfrak{m}$, and $\mathfrak{g}(\alpha)$) into $\mathfrak{g}(\alpha)$ (into zero); it follows that $\operatorname{Ad} x^2 = (\operatorname{Ad} x)^2$ $= 1 + \operatorname{ad} X^2$ (note that $\operatorname{Char} k = 2$ and that $\operatorname{ad} X$ and $\varphi(X)$ commute: infact $\operatorname{ad} X\, \varphi(X) = \varphi(X) \operatorname{ad} X = 0 = \varphi(X)^2$). Since $x^2 \in U'$ can be imbedded as the element $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ in a k-subgroup isogenous to SL(2) of G with T as the diagonal torus, it is easy to see from the representation theory of SL(2) that we have for $Y \in \mathfrak{g}(-\alpha)$.

$$\operatorname{Ad} x^2(Y) = Y + {}^w Y \quad (\in \mathfrak{g}(\alpha) + \mathfrak{g}(-\alpha))$$

where $w \in \mathrm{SL}(2)$ is the element $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. In particular $\operatorname{Ad} X^2 \colon \mathfrak{g}(-\alpha) \to \mathfrak{g}(\alpha)$ is an isomorphism. Since $\operatorname{Ad} x(c) = 0$, the second assertion follows from the first. If $\langle [X, Y_0], [X, Y] \rangle = 0$ for all $Y \in \mathfrak{g}(-\alpha)$ for a fixed $Y_0 \in \mathfrak{g}(-\alpha)$, we have (by invariance of $\langle\ ,\ \rangle$)

$$\langle Y_0, \operatorname{Ad} X^2(Y) \rangle = 0 \qquad \text{for all } Y \in \mathfrak{g}(-\alpha);$$

since $\langle\ ,\ \rangle$ is a non-degenerate pairing of $\mathfrak{g}(\alpha)$ and $\mathfrak{g}(-\alpha)$ and $\operatorname{Ad} X^2$ is an isomorphism of $\mathfrak{g}(-\alpha)$ on $\mathfrak{g}(\alpha)$, $Y_0 = 0$. Hence the third assertion. If

$$\operatorname{ad} X \colon \mathfrak{m} \to \mathfrak{g}(\alpha)$$

is not onto, we can find $Y_0 \in \mathfrak{g}(-\alpha)$ such that

$$\langle Y_0, [X, A] \rangle = 0$$

for all $A \in \mathfrak{m}$. Equivalently

$$\langle [X, Y_0], A \rangle = 0$$

for all $A \in \mathfrak{m}$. But then $[X, Y_0]$ must be orthogonal to all of $\mathfrak{g}$ with respect to $\langle\ ,\ \rangle$ and one sees that this means that $[X, Y_0] \in c$ and by (ii), $[X, Y_0] = 0$; since $\operatorname{Ad} X^2$ is injective on $\mathfrak{g}(-\alpha)$, $Y_0 = 0$. This proves the claim completely.

5.34. Consider now the action of M^* on $\mathfrak{g}(\alpha)$. Let $I(X)$ denote the isotropy group at X for this action of M^*. Evidently $I(x)$ is contained in $I(X)$. The tangent map at 1 of the orbit map $m \to \operatorname{Ad} m(X)$ of M in $\mathfrak{g}(\alpha)$ is easily seen to be the map $A \to [X, A]$, $A \in \mathfrak{m}$ of $\mathfrak{m}$ in $\mathfrak{g}(\alpha)$; this is surjective. Consequently as the map $m \to \operatorname{Ad} m(X)$ factors through M^* - the orbit map $m \to m(X)$ of M^* in $\mathfrak{g}(\alpha)$ is also of maximal rank. We conclude that $I(X)$ is smooth. Further evidently the isotropy $I_1(X)$ group at X for the action of M on $\mathfrak{g}(\alpha)$ is smooth and isogenous to $I(X)$. We will show that $I_1(X)$ is reductive and hence conclude that so is $I(X)$. Let $\mathfrak{i}_1(X)$ be the Lie algebra of $I_1(X)$; then for $A \in \mathfrak{i}_1(X)$ and $Y \in \mathfrak{g}(-\alpha)$, we have

$$\langle A, [X, Y] \rangle = \langle [X, A], Y \rangle = 0$$

since $[X, A] = 0$. Thus $\mathfrak{i}_1(X)$ is orthogonal to $\operatorname{ad} X(\mathfrak{g}(-\alpha))$ with respect to $\langle\ ,\ \rangle$. Since $\dim \mathfrak{g}(+\alpha) = \dim \operatorname{ad} X(\mathfrak{g}(-\alpha))$, $\dim \mathfrak{i}_1(X) \geqq \dim \mathfrak{m} - \dim \mathfrak{g}(\alpha)$ we conclude that $\mathfrak{i}_1(X) = \{v \in \mathfrak{m} \mid \langle v, A \rangle = 0 \text{ for all } A \in \operatorname{ad} X(\mathfrak{g}(-\alpha))$. Since $\langle\ ,\ \rangle$ is *non-degenerate* on $\operatorname{ad} X(\mathfrak{g}(-\alpha))$ we see that $\langle\ ,\ \rangle$ restricted $\mathfrak{i}_1(X)$ has precisely c for its kernel. This shows that $I(X)$ is *reductive* and of dimension $\dim M - \dim \mathfrak{g}(\alpha)$.

5.35. The group scheme $I(x)$ is contained in $I(X)$ so that $\mathfrak{i}(x) \subset \mathfrak{i}(X)$; and $I(x)$ is of dimension $\dim \mathfrak{m} - \dim \mathfrak{g}(\alpha)$. While $\mathfrak{i}(x)$ has dimension $\geqq \dim \mathfrak{m} - \dim \mathfrak{g}(\alpha) - \dim \mathfrak{g}(2\alpha)$. Since $\mathfrak{i}(X)$ is *reductive*, if $\mathfrak{i}(x)$ consists of nilpotents we must necessarily have

$$2 \dim \mathfrak{i}(x) + \operatorname{rank} I(X) \leqq \dim I(X)$$

so that

$$\operatorname{rank} I(x)+2[\dim \mathfrak{m}-\dim \mathfrak{g}(\alpha)-\dim \mathfrak{g}(2\alpha)] \leqq \dim \mathfrak{m}-\dim \mathfrak{g}(\alpha).$$

This means that

$$2 \dim \mathfrak{g}(2\alpha) \geqq \dim \mathfrak{m}-\dim \mathfrak{g}(\alpha)+\operatorname{rank} I(X).$$

A simple computation now shows that

$$2 \dim \mathfrak{g}(2\alpha) < \dim \mathfrak{m}-\dim \mathfrak{g}(\alpha)+1$$

except in the case when G has one of the following 2 Tits diagrams

$$^2E_{6,1}^{29}: \qquad \text{(A)}$$

$$E_{7,1}^{48}: \qquad \text{(B)}$$

When G has (A) for its diagram one is lead to $\operatorname{rank} I(X) \leqq 2$ and - since $\dim I(X)=12-\operatorname{rank} I(X)=2$. Further one finds immediately that if $\mathfrak{i}(x)$ consists entirely of nilpotent elements, $\dim \mathfrak{i}(x) \leqq \dim$ of maximal connected unipotent subgroup of $I(X) \leqq 6$ while $\dim I(x) \geqq 6$. This shows that $I(x)$ is the unipotent radical of a Borel subgroup of $I(X)$, so that $I(X)$ would be quasi split, a contradiction since $I(X) \subset M^*$. Finally if G has the diagram (B) above one is lead to the unequality $\operatorname{rank} I(X) \leqq 3$ while dimension $I(X)=17$; and one checks easily that there is no reductive group of rank 3 and dimension 17. This completes the proof of Lemma 5.20 and hence that of the main theorem of this appendix.

References

Bak, A., Rehman, U.: The congruence subgroup and Metaplectic problems for $\mathrm{SL}_{n \geqq 2}$ of Division Algebras. J. Algebra **78**, 475-547 (1982)

Bass, H., Lazard, M., Serre, J.-P.: Sous-groupes d'indices finis dans $SL(n, Z)$. Bull. Am. Math. Soc. **70**, 385-392 (1964)

Bass, H., Milnor, J., Serre, J.-P.: Solution of the congruence subgroup problem for SL_n $(n \geqq 3)$ and Sp_{2n} $(n \geqq 2)$. Publ. Math. Inst. Hautes Etud. Sci. **33**, 59-137 (1967). (Also Publ. Math. Inst. Hautes Etud. Sci. **44**, 241-244 (1974)

Behr, H.: Endliche Erzeugbarkeit arithmetischer Gruppen über Funktionenkörper. Invent. Math. **7**, 1-32 (1969)

Borel, A.: Introduction aux groupes arithmétiques. Paris: Hermann 1969

Borel, A., Tits, J.: Groupes réductifs. Publ. Math. Inst. Hautes Etud. Sci. **27**, 55-150 (1965)

Borel, A., Tits, J.: Éléments unipotents et sousgroupes paraboliques de groupes réductifs. Invent. Math. **12**, 95-104 (1971)

Bourbaki, N.: Éléments de Mathématique. Topologie Générale, Chapitre 3. Paris: Hermann (1951)

Deodhav, V.V.: On central extensions of rational points of algebraic groups. Am. J. Math. **100**, 303-386 (1978)

Harder, G.: Minkowskische Reduktionstheorie über Funktionenkörper. Invent. Math. **7**, 33-54 (1969)

Kneser, M.: Normalteiler ganzzahliger Spingruppen. J. Reine Angew. Math. **311/312**, 191-214 (1979)

Margulis, G.A.: Finiteness of quotient groups of discrete groups (Russian). Funktional Anal. i Prilozen **13**, 28-39 (1979)

Matsumoto, H.: Sur les sous-groupes arithmétiques des groupes semisimples déployés. Ann. Sci. Ec. Norm. Super., 43 série, **2**, 1-62 (1969)

Mennicke, J.: Finite factor groups of the unimodular group. Ann. Math. **31**, 31-37 (1965)

Platonov, V.P.: The problem of strong approximation and the Kneser-Tits conjecture. Math. USSR, Izv. **3**, 1139-1147 (1969); Addendum, ibid **4**, 784-786 (1970)

Prasad, G.: Strong approximation for semisimple groups over function fields. Ann. Math. **105**, 553-572 (1977)

Prasad, G., Raghunathan, M.S.: On the congruence subgroup problem: Determination of the metaplectic kernel. Invent. Math. **71**, 21-42 (1983)

Raghunathan, M.S.: On the congruence subgroup problem. Publ. Math. Inst. Hautes Etud. Sci. **46**, 107-161 (1976)

Richardson Jr., R.W.: Conjugacy classes in Lie algebras and algebraic group. Ann. Math. **86**, 1-15 (1967)

Serre, J.-P.: Le problème des groupes de congruence pour SL_2. Ann. Math. **92**, 489-527 (1970)

Steinberg, R.: Generateurs, relations et revêtements de groupes algebriques, Colloque de Bruxelles (1962) 113-127

Tits, J.: Classification of algebraic semisimple groups. Proc. Symp. Pure Math. **9**, 33-62 (1969)

Vaserstein, L.N.: The structure of classical arithmetical groups of rank greater than one (Russian). Mat Sbornik **99**, 268-295 (1973); English translation in Math. USSR, Sbornik **20**, 465-492 (1973)

Oblatum 15-III-1984 & 20-VIII-1984