ON THE CONGRUENCE SUBGROUP PROBLEM

by M. S. RAGHUNATHAN

Introduction.

Let k be a global field and V the set of valuations on k. Let ∞ denote the set of archimedean valuations on k. For $v \in V$, k_v denotes the completion of k with respect to v, $\mathfrak{O}_v$ the ring of integers in k_v and F_v the residue field of k_v. Let $S \supset \infty$ be any finite subset of V and

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

Next, let G be a linear algebraic group defined over k and $G(k)$ the group of k-rational points. A subgroup $\Phi \subset G(k)$ is a S-congruence group if there is a faithful representation ρ of G in $GL(n)$ defined over k and an ideal $\mathfrak{a} \neq 0$ in A(S) such that the group

$$\Phi' = \{x \in G(k) \mid \rho(x) \in GL(n, \mathfrak{O}),\ \rho(x) \equiv 1 \pmod{\mathfrak{a}}\}$$

is contained in Φ as a subgroup of finite index. (One may also fix the representation ρ once and for all and demand the existence of a non-zero $\mathfrak{a}$ for this fixed representation.) A subgroup Φ in $G(k)$ is S-arithmetic if there is an S-congruence group Ψ such that $\Phi \cap \Psi$ has finite index in both Φ and Ψ. The family of S-congruence (resp. S-arithmetic) groups serve as a fundamental system of neighborhoods of 1 for a topology $\mathscr{C}(c)$ (resp. $\mathscr{C}(a)$) on $G(k)$ which makes it into a topological group. The completion of $G(k)$ with respect to $\mathscr{C}(c)$ (resp. $\mathscr{C}(a)$) is denoted $\hat{G}(S, c)$ (resp. $\hat{G}(S, a)$). It is not difficult to see that $\hat{G}(S, c)$ and $\hat{G}(S, a)$ are locally compact groups — in fact the closure of an S-congruence group in either of these groups is compact and open. Since the topology $\mathscr{C}(a)$ is evidently finer than $\mathscr{C}(c)$, we have a natural surjective map

$$\hat{G}(S, a) \xrightarrow{\pi(S)} \hat{G}(S, c).$$

Let $C(S, G) = \text{kernel } \pi(S)$. The congruence subgroup problem is the problem of determination of $C(S, G)$ for a given G and S. (That $C(S, G)$ is trivial is equivalent to saying that every S-arithmetic group is an S-congruence group.) $C(S, G)$ is a (compact-) *pro-finite* group.

Before we describe the results obtained in the present work, we will briefly recall what is already known. We begin with general comments which are well known and easily established (but are not set down in print).

$C(S, G)$ is a functor: if $f : G \to H$ is a k-morphism of k-groups we have a natural morphism $C(S,f) : C(S, G) \to C(S, H)$. Suppose now that

$$(*) \qquad 1 \to G_1 \xrightarrow{\alpha} G_2 \xrightarrow{\beta} G_3 \to 1$$

is an exact sequence of k-algebraic groups, α, β being k-morphisms; the sequence

$$(**) \qquad C(S, G_1) \xrightarrow{C(S,\alpha)} C(S, G_2) \xrightarrow{C(S,\beta)} C(S, G_3)$$

is exact. This is an immediate consequence of the following fact: if $f: G \to H$ is a *surjective* k-morphism, the image $f(\Gamma)$ of an S-arithmetic group Γ in G is an S-arithmetic group of H. In general $C(S, \alpha)$ is *not* injective. (An example to illustrate is the following: Let k be of positive characteristic. Take G_1 = the additive group of k and let G_2 be the semidirect product of the multiplicative group of k and the additive group. Then if $|S| \geq 2$, $C(S, G_1)$ is non-trivial while the map $C(S, G_1) \to C(S, G_2)$ is trivial.) There is, however, one simple situation where $C(S, \alpha)$ is injective: when G_1 has finite index in G_2. This remark with the trivial fact that $C(S, G)$ is trivial for finite G shows that, for any G, $C(S, G) \cong C(S, G^0)$, where G^0 = identity component of G. Once again, in general $C(S, \beta)$ is not surjective. One simple case where it is indeed surjective is the case when $(*)$ is a split sequence; in this case moreover $C(S, \beta)$ admits a splitting and $C(S, G_2)$ is the semidirect product of $C(S, G_3)$ and a quotient of $C(S, G_1)$. (If G is any group and $\widetilde{G}$ a covering group, and B is the kernel of $\widetilde{G} \xrightarrow{p} G$, it can be shown that the cokernel of $C(S, p)$ contains a subgroup isomorphic to the S-adèle group of B.)

At this point we will separate the case of fields of characteristic zero from those of positive characteristics. The remarks about split sequences enable one to reduce the problem to the semisimple case in characteristic 0.

In this paragraph k will be of characteristic 0. It is trivial and well known that $C(S, G) = 1$ for all S if G is the additive group of k. Since any unipotent group over k can be obtained by forming successive semidirect products with the additive group, $C(S, G) = 1$ for any unipotent group. It is a (non-trivial) theorem due to Chevalley [1] that if G is a torus, $C(S, G) = 1$. From the structure theory one concludes that $C(S, G)$ is trivial for G solvable. For a general G, one knows that G is the semidirect product over k of a reductive k-group M and the unipotent radical U of G. Since $C(S, U)$ is trivial, $C(S, G) \rightleftarrows C(S, M)$. The problem is thus reduced to connected reductive groups. Again, if B is the maximal connected semisimple normal subgroup of the connected reductive group M, M/B is a torus and we conclude that $C(S, M)$ is a quotient of $C(S, B)$. Thus to a considerable extent the most important information is contained in $C(S, G)$ for connected semisimple G. Further, if one solves the problem in the case when G is simply connected one can obtain considerable information in the general case as well.

The situation when k has positive characteristic is not so pleasant. The group $C(S, G_1)$ is non-trivial—in fact infinite—even for the additive group of k. It is also non-trivial for tori. Nevertheless the semisimple case is obviously interesting, in any event.

From now on we assume that G is *simply connected* and *absolutely* simple (this is no loss of generality; the general case can be reduced to this by changing the field). In the simplest such G *viz.* $G = SL(2)$ over $k = \mathbf{Q}$, the rational number field, C(S, G) is known to be infinite. (That C(S, G) is non-trivial at least has been known for a long time.) For $G = SL(2)$ over any k, Serre [1] has given a fairly complete solution. If $|S| \leq 1$, C(S, G) is infinite; if $|S| \geq 2$ and if there exists $v \in S$ such that k_v is not isomorphic to $\mathbf{C}$, $C(S, G) = 1$; if $k_v \cong \mathbf{C}$ for all $v \in S$ and $|S| \geq 2$, C(S, G) is isomorphic to the group of roots of 1 in k. This result on SL(2) has an extension to all split groups. (Historically SL(2) was handled later; the higher rank groups were dealt with earlier.) Let G be a Chevalley group over k of rank ≥ 2. Then $C(S, G) = 1$ or μ (= roots of 1 in k) according as all $v \in S$ are not or are imaginary ($v \in V$ is imaginary if $k_v \cong \mathbf{C}$). $G = SL(n)$, $k = \mathbf{Q}$, $S = \infty$, $n \geq 3$ was first settled by Bass-Lazard-Serre [1] and independently by Mennicke [1]; Bass-Milnor-Serre [1] and Mennicke [2] proved the result for $SL(n)$, $n \geq 3$, $Sp(n)$, $n \geq 2$. Matsumoto [1] extended these results to general Chevalley groups. Finally Kneser [1] and Vasserstein [1] have treated some non-split orthogonal groups. On the evidence provided by these results, Serre proposes the following conjecture (Serre [1], p. 489, footnote):

$$(*) \qquad C(S, G) \text{ is finite if } \sum_{v \in S} k_v\text{-rank}(G) \geq 2 \quad (\text{and G } \textit{isotropic} \text{ for all } v \in S - \infty).$$

It is necessary to impose the condition in parenthesis: see § 5. The present work provides further substantial evidence of the truth of (*). Our main results here are for groups of k-rank ≥ 2. (Many of the results we prove are in fact true also for " most " k-rank 1 groups — at least when k is a number field — but the present proofs do not apply to that case; the rank 1 groups will be dealt with by different techniques in a work now under preparation.)

In the sequel we assume that G has k-rank ≥ 1 and S is such that $\sum_{v \in S} k_v\text{-rank}(G) \geq 2$. Let Φ be an S-congruence subgroup of G and $E(\Phi)$ the group generated by

$$\{x \in \Phi \mid x \in \text{Unipotent radical of a } k\text{-parabolic group}\}.$$

A group of the form $E(\Phi)$ will be called an S-elementary subgroup in the sequel. The first main result of the paper is

Theorem A: *Let* Δ *be a normal subgroup of an* S-*arithmetic subgroup of* G. *Then either* Δ *is finite and central or* Δ *contains an elementary subgroup.*

Theorem B: *Assume that* k-*rank*$(G) \geq 2$; *then every* S-*elementary subgroup is* S-*arithmetic.*

Theorem C: *Assume that* k-*rank*$(G) \geq 2$ *and let* $G(k)^+ =$ *group generated by*

$$\{x \in G(k) \mid x \in \text{Unipotent radical of a } k\text{-parabolic subgroup of G}\}.$$

Let $\hat{G}^+(S, a)$ (resp. $\hat{G}^+(S, c)$) *be the closure of* $G(k)^+$ *in* $\hat{G}(S, a)$ (resp. $\hat{G}(S, c)$) *and* $C^+(S, G) = C(S, G) \cap \hat{G}^+(S, a)$. *Then* $C^+(S, G)$ *has finite index in* $C(S, G)$ *and the sequences*

$$1 \to C^+(S, G) \to \hat{G}^+(S, a) \to \hat{G}^+(S, c) \to 1$$

$$1 \to C(S, G)/C^+(S, G) \to \hat{G}^+(S, a)/C^+(S, G) \to \hat{G}(S, c) \to 1$$

are exact and are central extensions.

Theorem C reduces the problem of determination of $C(S, G)$ to certain cohomology computations. Precise determination is possible when G is quasi-split thanks to Moore [1] and Deodhar [1]. (For non-split groups, Theorem C is new.) For general G, we can obtain the following information:

Theorem D: *Assume that* k-*rank*$(G) \geq 2$. *If* k *is a number-field,* $C(S, G)$ *is finite. If* k *has characteristic* $p > 0$, *the* p-*Sylow subgroup of* $C(S, G)$ *has finite index in* $C(S, G)$; *if in addition* G *is quasi-split for all* $v \notin S$, $C(S, G)$ *is finite.*

The relevant cohomology computations are in fact done in a very general context:

Theorem E: *Let* G *be a connected simply connected algebraic group over a global field* k. *Assume that strong approximation holds for* G. *Let* $S \supset \infty$ *be any finite set and* U *be an open compact subgroup of the* S-*adèle group of* G. *Then if* k *is a number field,* $H^i(U, \mathbf{Q}/\mathbf{Z})$ *is finite for* $i = 1, 2$ *(here* $\mathbf{Q}/\mathbf{Z}$ *is given the discrete topology and cohomology is based on continuous cochains). If* k *is a function field the* p-*torsion* (p = *characteristic of* k) *in* $H^2(U, \mathbf{Q}/\mathbf{Z})$ *has finite index in* $H^2(U, \mathbf{Q}/\mathbf{Z})$ *and* $H^1(U, \mathbf{Q}/\mathbf{Z})$ *is finite.*

Theorem E has a local version:

Theorem F: *Let* U *be a compact open subgroup of a semisimple group over a local field* K. *Then if characteristic* $K = p$, $H^i(U, \mathbf{Q}/\mathbf{Z})$ *has* p-*torsion of finite index.*

These results are proved in §§ 1-5. In § 6 we examine what happens when we enlarge S and in § 7 some applications to representations of S-arithmetic groups are given.

1. An Auxiliary Lemma.

Notation and Definitions (**1.1**). — The following notation will be used throughout this paper. We denote by

k, a global field.
V, the set of valuations of k.
∞, the set of archimedean valuations.
S, a finite subset with $|S| \geq 1$ and $\infty \subset S$.
k_v ($v \in V$) the completion of k with respect to v.
$\mathfrak{O}_v$, the ring of integers in k_v.
$\mathfrak{p}_v^*$, the prime ideal in $\mathfrak{O}_v$.
$\mathfrak{O}_S = A(S) = A$ if there is no ambiguity about S, the ring of S-integers in k, *i.e.* $A(S) = \{x \in k \mid x \in \mathfrak{O}_v$ for all $v \notin S\}$.

$\mathfrak{p}_v$, the prime ideal $\mathfrak{p}_v^* \cap A(S)$ in $A(S)$ $(v \notin S)$.
$F_v = A/\mathfrak{p}_v$ the residue field.
G, a connected, absolutely simple, simply connected k-algebraic group.

By and large in this paper we look upon algebraic groups as rational points in a universal domain. But sometimes, in this chapter in particular, it is more convenient and natural to take the scheme theoretic standpoint. To avoid confusion we reserve the term algebraic group for the rational points in this universal domain. $GL(n)$ denotes the algebraic group of $n \times n$ non-singular matrices with entries in the universal domain, while $\mathbf{GL}(n)$ denotes the group-scheme over A, *i.e.* $\mathbf{GL}(n) = \operatorname{Spec} B$ where B is the ring

$$A[X_{ij};\ 1 \leq i, j \leq n][(\det(X_{ij}))^{-1}].$$

Let $G \overset{\tau}{\hookrightarrow} GL(n)$ be an imbedding of G as a k-algebraic subgroup and $\mathfrak{I} \subset B$ be the ideal

$$\{f \in B \mid f(G) = 0\}.$$

Note that $B/\mathfrak{I}$ has *no nilpotent elements.* We fix once and for all the imbedding τ above and denote by $\mathbf{G}$ the group-scheme $\operatorname{Spec}(B/\mathfrak{I})$. $\mathbf{G}$ is evidently a scheme over $A = A(S)$. We set

$$G(A) = G \cap GL(n, A)$$
$$G(k) = G \cap GL(n, k)$$

($G(A)$ (resp. $G(k)$) is precisely the A- (resp. k-) rational points of the group-scheme $\mathbf{G}$ over A) and for an ideal $\mathfrak{a} \subset A$, we denote by $G(\mathfrak{a})$ the congruence subgroup defined by $\mathfrak{a}$:

$$G(\mathfrak{a}) = \{x \in G(A) \mid x \equiv \text{Identity} (\operatorname{mod} \mathfrak{a})\}.$$

The group $GL(n)(\mathfrak{a})$ is also denoted $GL(n, \mathfrak{a})$ in the sequel. We will need to consider some other families of subgroups of $G(A)$ as well in the sequel. We make some definitions towards this end.

Definition (**1.2**). — A unipotent element $x \in G(k)$ is a *good* unipotent if it belongs to the unipotent radical of a k-parabolic subgroup of G.

$G(k)^+$ is the group generated by good unipotents in $G(k)$.

Definition (**1.3**). — A k-group G has (property) K-T, or G is a K-T *group*, if $G(k) = G(k)^+$.

It is *almost* K-T if $G(k)/G(k)^+$ is finite abelian.

For a wide class of (simply connected) G over any field it is known that $G(k) = G(k)^+$. However Platonov [3] has recently given an example when this does not hold for a field (which is not a global field). Nevertheless, the following result is proved in Raghunathan [4]. If k is a global field and k-rank$(G) > 1$, G has almost K-T for k.

Definition (**1.4**). — A subgroup $P \subset H$ in a semisimple k-group is a *k-quasi-parabolic subgroup* (QPS for short) of H if there exists a k-parabolic subgroup P^* of H and a maximal reductive k-subgroup M^* of P^* such that $P^*=M^*U$ with U=unipotent radical of P^* and $P=M.U$, where M is the product of all the isotropic k-simple factors of M^*. A subgroup like M above is called an *admissible* subgroup (A-S for short). Also P is *adapted* to M.

An alternate characterisation of admissible subgroups is the following: A connected (k-) subgroup M is admissible if and only if there is a maximal k-split torus T in H and an order on the character group X(T) of T such that the Lie algebra $\mathfrak{m}$ of M is the span of *all* those root-spaces of H with respect to T which are linear combinations of a fixed subset of the system of simple roots (for the order).

We note that (in the notation used in Definition (1.4)) the correspondence $P^*\mapsto P$ sets up a bijection between sets of k-parabolic and k-quasi-parabolic subgroups of H. Evidently this bijection is compatible with the action (by conjugation) of $H(k)$ on these two sets. It is known moreover from Borel [1] (the case of number fields) and Behr [1] and Harder [1] (the case of function fields) that we have

Lemma (**1.5**). — *There are only finitely many* Γ*-conjugacy classes of k-(quasi)-parabolic subgroups for any* S*-arithmetic subgroup* Γ *in* G.

We will now introduce three other families of subgroups of G(A).

Definitions (**1.6**). — Let $\mathfrak{a}\subset S$ be any ideal. Then

$$\begin{aligned}EG(\mathfrak{a}) &= \text{group generated by } \{x\in G(\mathfrak{a})\mid x \text{ a good unipotent}\}\\ FG(\mathfrak{a}) &= \text{group generated by } \{P(\mathfrak{a})\mid P \text{ a } \textit{proper } k\text{-QPS in } G\}\\ F^*G(\mathfrak{a}) &= \text{group generated by } \{M(\mathfrak{a})\mid M \text{ a } \textit{proper } k\text{-A-S in } G\}\end{aligned}$$

We have then two obvious inclusions among these *normal* subgroups

$$EG(\mathfrak{a})\hookrightarrow FG(\mathfrak{a}), \qquad F^*G(a)\hookrightarrow FG(a).$$

The following is perhaps not so evident.

Lemma (**1.7**). — *Assume that k-rank*(G) > 1. *There exists* $s\in A$ *such that for any ideal* $\mathfrak{a}\subset A$

$$FG(s\mathfrak{a})\subset F^*G(\mathfrak{a}).$$

Let $P_1, \ldots, P_m$ be a complete set of representatives for G(A)-conjugacy classes of k-quasi-parabolic subgroups. For each P_i, we fix a semidirect product decomposition $P_i=M_i.U_i$, M_i a k-A-S and U_i the unipotent radical of P_i, over k. It is then easily seen that there exists an element $s'\in A$ such that $P_i(s'\mathfrak{a})\subset M_i(\mathfrak{a}).U_i(\mathfrak{a})$ for all i. It suffices thus to show that each $U_i(s''\mathfrak{a})\subset F^*G(\mathfrak{a})$ for a fixed $s''\in A$ independent of i and $\mathfrak{a}$. To see this let P_i^* be the parabolic subgroup determined by P_i and T_i a maximal k-split torus in P_i. Let φ be a root of G with respect to T_i and $G^{(\varphi)}$ the unique connected k-subgroup of G whose Lie algebra is spanned by the k-root spaces corresponding to $\lambda\varphi$,

$\lambda \in \mathbf{Z}$. Let $U_i^{(\varphi)} = U_i \cap G^{(\varphi)}$. Since k-rank$(G) \geq 2$, it is easily seen that $G^{(\varphi)}$ is contained in some admissible subgroup (in fact if $\varphi/2$ is not a k-root, $G^{(\varphi)}$ is itself admissible). It follows that for every k-root φ, $U_i^{(\varphi)}(\mathfrak{a}) \subset F^* G(\mathfrak{a})$. Now we can find k-roots $\varphi_1, \ldots, \varphi_q$ such that the product mapping

$$U_i^{\varphi_1} \times U_i^{\varphi_2} \times \ldots \times U_i^{\varphi_q} \rightarrow U_i$$

is an isomorphism of algebraic varieties. From this, it is easily deduced that there is an element $s'' \in A(S)$ such that for any ideal $\mathfrak{a} \subset A$, $U_i(s''\mathfrak{a})$ is contained in the image of $U_i^{\varphi_1}(\mathfrak{a}) \times U_i^{\varphi_2}(\mathfrak{a}) \times \ldots \times U_i^{\varphi_q}(\mathfrak{a})$. This proves Lemma (1.7).

Remark (**1.8**). — When k-rank$(G) = 1$, all proper admissible k-subgroups are trivial and any proper QPS is the unipotent radical of a k-parabolic subgroup, so that $EG(\mathfrak{a}) = FG(\mathfrak{a})$.

We now go back to the scheme $\mathbf{G}$ and establish some facts about it. It is well known—and not difficult to prove—that the following is true.

Lemma (**1.9**). — *There exists a* finite *set* $S_1 \supset S$ *such that for* $v \notin S_1$, $\mathbf{G} \otimes A/\mathfrak{p}_v$ *is a reduced, connected, semisimple and simply connected group scheme over* $A/\mathfrak{p}_v$.

(Let Ch denote the Chevalley scheme over $\mathbf{Z}$ of the same type as G. Let k' be a finite separable extension of k over which G splits. Let A′ denote the S-integers in k'. We can then find a finite set $S^* \subset V$, $S \subset S^*$ and an isomorphism

$$\varphi : \mathbf{G} \otimes_A A'(S^*) \rightarrow \mathrm{Ch} \otimes_A A'(S^*).$$

The group scheme on the right admits a good reduction at *all* primes of $A'(S^*)$ ($= S^*$-integers in k'). For S_1 we need only take the following subset:

$$S^* \cup \{v \in V \mid k'/k \text{ is ramified at } v\}.)$$

We fix now two opposite parabolic k-subgroups P^* and P^{*-} in G. Let U (resp. U^-) be the unipotent radical of P (resp. P^-). We define subgroup schemes $\mathbf{P}^*$, $\mathbf{P}^{*-}$, $\mathbf{U}$ and $\mathbf{U}^-$ of $\mathbf{G}$ over A in a way entirely analogous to the way we defined $\mathbf{G}$, and then it is easy to obtain the following:

Lemma (**1.10**). — *There exists a* finite *set* $S_2 \subset V$, $S_2 \supset S_1$ *such that for* $v \notin S_2$, $\mathbf{P}^* \otimes_A A/\mathfrak{p}_v$ *and* $\mathbf{P}^{*-} \otimes_A A/\mathfrak{p}_v$ *are (reduced) parabolic subgroup schemes of* $\mathbf{G} \otimes_A A/\mathfrak{p}_v$, *with* $\mathbf{U} \otimes_A A/\mathfrak{p}_v$ *and* $\mathbf{U}^- \otimes_A A/\mathfrak{p}_v$ *as the corresponding unipotent radicals.*

Lemma (**1.11**). — *Let* $\mathfrak{a}$ *be a non-zero ideal in* A. *There exists a finite set* $S_3(\mathfrak{a}) \subset V$, $S_3 \supset S_2$, *with the following property: for* $v \notin S_3(\mathfrak{a})$, $U^{\pm}(\mathfrak{a})$ *maps (under the natural map)* onto *the group of* $A/\mathfrak{p}_v$*-rational points of* $\mathbf{U}^{\pm} \otimes_A A/\mathfrak{p}_v$; *moreover, these last groups generate the entire group of* $A/\mathfrak{p}_v$*-rational points of* $\mathbf{G} \otimes_A A/\mathfrak{p}_v$.

The first assertion is standard and quite easy to establish; the second follows from the work of Chevalley [1] and Steinberg [1], combined with a theorem of Lang [1].

(Lang's theorem is that for a finite field every semisimple algebraic group is quasi-split. The papers of Chevalley and Steinberg which deal with quasi-split groups then immediately give the lemma when P^* is a minimal parabolic subgroup, but the passage to the more general case we need is quite simple.)

Corollary (**1.12**). — *For* $v \notin S_3 = S_3(A)$ *the natural map*

$$G(A) \rightarrow (\mathbf{G} \otimes A/\mathfrak{p}_v)(A/\mathfrak{p}_v)$$

is surjective with kernel $G(\mathfrak{p}_v)$.

(**1.13**). — The Lie algebra of G — more precisely its canonical (Scheme theoretic) A-form — can be described as follows. Let

$$\varepsilon : B(G) = B/\mathfrak{J} \rightarrow A$$

denote the identity element (in G(A)). Let $\mathfrak{M} = \ker \varepsilon$. Since A is a Dedekind domain, $\mathfrak{M}$ is a finitely generated ideal in B(G) so that $\mathfrak{M}/\mathfrak{M}^2$ is a finitely generated A-module. Let $\mathfrak{G} = \mathrm{Hom}_A(\mathfrak{M}/\mathfrak{M}^2, A)$. Then $\mathfrak{G}_k = \mathfrak{G} \otimes_A k$ can be seen to be naturally isomorphic to the k-Lie algebra associated to G (with any definition). The group G(A) (resp. $G(k)$) operates in a natural fashion on $\mathfrak{G}$ (resp. $\mathfrak{G}_k$). The action of G(A) on the two is easily seen to be compatible with the inclusion $\mathfrak{G} \hookrightarrow \mathfrak{G}_k$. We have then

Lemma (**1.14**). — *There is a finite set* $S_4 \subset V$, $S_3 \subset S_4$, *such that for* $v \notin S_4$, $\mathfrak{G} \otimes_A A/\mathfrak{p}_v$ *is naturally isomorphic to the Lie algebra of the (reduced) group scheme* $\mathbf{G} \otimes_A A/\mathfrak{p}_v$. *This isomorphism is compatible with the adjoint* G(A)-*action on the two Lie algebras.*

Lemma (**1.15**). — *Let* U *be the unipotent radical of a k-parabolic subgroup of* G. *Let* $\mathfrak{U}$ *be the Lie algebra of* $\mathbf{U}$ *and* $i : \mathfrak{U} \rightarrow \mathfrak{G}$ *the natural map. Let* $\mathfrak{U}_v = \mathfrak{U} \otimes_A F_v$ *and* $\mathfrak{G}_v = \mathfrak{G} \otimes_A F_v$. *Then for almost all* v, $i \otimes 1 : \mathfrak{U}_v \rightarrow \mathfrak{G}_v$ *is an inclusion and* $\mathfrak{U}_v$ *is the Lie subalgebra of* $\mathfrak{G}_v$ *corresponding to the unipotent radical of a* k_v-*parabolic subgroup of* $\mathbf{G} \otimes_A F_v$. *Let* R *be the group algebra* $F(G(F_v))$, F *being the prime field in* F_v. *Then there is a finite set* $S_5 \supset S_4$ *such that as a module over* R, $\mathfrak{G} \otimes_A F_v$ *is generated by* $\mathfrak{U} \otimes_A F_v$ *for all* $v \notin S_5$.

This is proved by using explicitly the structure of quasi-split groups — note that $\mathbf{G} \otimes_A F_v$ is quasi-split over F_v (Lang [1]). For details see the Appendix.

(**1.16**). — For $v \in V$, let $G(k_v)$ denote the k_v-rational points of G and

$$G(\mathfrak{O}_v) = G(k_v) \cap GL(n, \mathfrak{O}_v).$$

Then $G(\mathfrak{O}_v)$ is an open compact subgroup of $G(k_v)$. (It is known — and we will give a proof of this fact later — that $G(\mathfrak{O}_v)$ is a maximal compact subgroup of $G(k_v)$ for almost all v, but we do not need this fact now.)

Let $G(\mathbf{A}(S))$ or $G(\mathbf{A})$ the corresponding adèle group associated to G. Then by the definition of the adèle topology $\prod_{v \notin S} G(\mathfrak{O}_v)$ is an open compact subgroup of $G(\mathbf{A}(S))$. The following result needed in the sequel implies in particular that the closure of an

S-arithmetic group G is open in $G(\mathbf{A}(S))$ — a known consequence of strong approximation (whenever strong approximation holds).

Main Lemma **(1.17)**. — *The closure of* $EG(\mathfrak{a})$, $\mathfrak{a} \neq 0$, *in* $G(\mathbf{A}(S))$ *is a compact open subgroup* $G(\mathbf{A}(S))$. *Consequently, for every non-zero ideal* $\mathfrak{a} \subset A$, *we can find an ideal* $\mathfrak{a}' \neq 0$ *in* A *such that the closure of* $EG(\mathfrak{a})$ *in* $G(\mathbf{A}(S))$ *contains* $G(\mathfrak{a}')$ — *or equivalently, for every non-zero ideal* $\mathfrak{b} \subset A$

$$EG(\mathfrak{a}) . G(\mathfrak{b}) \supseteq G(\mathfrak{a}').$$

In order to prove the main lemma, we consider the two unipotent groups $U^{\pm}$ introduced earlier (see Lemma (1.10)). Using strong approximation for unipotent groups, it is easily seen that the closures of $U^{\pm}(\mathfrak{a})$ in $U^{\pm}(\mathbf{A}(S))$ are compact open subgroups. This means that the closure of $U^{\pm}(\mathfrak{a})$ in $U^{\pm}(\mathbf{A}(S))$ is of the form

$$\prod_{v \in S'} D_v^{\pm} \times \prod_{v \notin S \cup S'} U^{\pm}(\mathfrak{O}_v)$$

where S' is a finite subset of $V-S$ and for $v \in S'$, $D_v^{\pm}$ is an open compact subgroup of $U^{\pm}(\mathfrak{O}_v)$. This shows that it suffices to show the following: $D_v^{\pm}$ *generate an open subgroup of* $G(\mathfrak{O}_v)$; *for almost all* $v \in V-S$, $U^+(\mathfrak{O}_v)$ *and* $U^-(\mathfrak{O}_v)$ *generate* $G(\mathfrak{O}_v)$ *as a normal subgroup.*

(Note that the closure of $E(\mathfrak{a})$ is a normal subgroup $\prod_{v \notin S} G(\mathfrak{O}_v)$.)

Now for $v \notin S'$ (resp. $v \in S'$) the normal subgroup H_v generated by $U^+(\mathfrak{O}_v)$ and $U^-(\mathfrak{O}_v)$ (resp. D_v^+ and D_v^-) in $G(\mathfrak{O}_v)$ is easily seen to be open. Consequently it contains a subgroup of the form

$$G(m, v) = \{g \in G(\mathfrak{O}_v) \mid g \equiv \text{Identity} (\text{mod } \mathfrak{p}_v^{*m})\}.$$

For a fixed $v \notin S_2'$ let $m(v)$ be the smallest integer such that $H_v \supset G(m(v), v)$. We need to prove only

(*) *for almost all* v, $m(v) = 0$.

(*) is a consequence of the two statements below:

Assertion **(1.18)**. — There is a finite subset S_0 of V, $S_0 \supset S_5$, such that for $v \notin S_0$ (S_5 as in Lemma (1.15)):

a) $U(m, v)/U(m+1, v)$ is non-trivial for all $m \geq m(v)$.

b) For $m \geq 1$, $G(m, v)/G(m+1, v)$ is isomorphic to $\mathfrak{G} \otimes_A F_v$ as a module over $\mathbf{Z}[G(A)]$; as a $\mathbf{Z}[G(A)]$-module it is generated by $U(m, v)/U(m+1, v)$.

We will first prove (*) assuming Assertion (1.18). For this consider the natural map

$$H_v / G(m(v), v) \xrightarrow{\pi} G(m(v)-1, v)/G(m(v), v)$$

(assuming that $m(v) > 1$). By Assertion (1.18), π is surjective since it is compatible with G(A)-action on the two sides, a contradiction to the assumption that $m(v) > 1$.

Thus $m(v)=0$ or 1. If $m(v)=1$, according to Lemma (1.11), the images of $U^{\pm}(\mathfrak{O}_v)$ in $G(0,v)/G(1,v)\cong \mathbf{G}(F_v)$ generate the entire group. Since $U^{\pm}(\mathfrak{O}_v)\subset H_v$, π is surjective again, a contradiction to the assumption $m(v)=1$. Thus $m(v)=0$ for all $v\notin S_0$.

(1.19). — We have now to establish Assertion (1.18). We will begin with a more general set up. Let $D\subset GL(n)$ be an algebraic subgroup of $GL(n)$ defined over k and $B(D)$ be the quotient $B/\mathfrak{I}(D)$ where $\mathfrak{I}(D)$ is the defining ideal of D. Let $\mathfrak{M}(D)$ be the ideal corresponding to the identity element in D: $\mathfrak{M}(D)$ is the kernel of the ring homomorphism $B(D)\xrightarrow{\varepsilon}A$ defined by the identity element. Now the group $D(\mathfrak{O},v)=D(\mathfrak{O}_v)$ can be interpreted as the set of all A-algebra homomorphisms $f:B(D)\to\mathfrak{O}_v$. If $\pi_n:\mathfrak{O}_v\to\mathfrak{O}_v/\mathfrak{p}_v^{*n}$ is the natural homomorphism, we have

$$\begin{aligned} D(m,v)&=\{x\in D(0,v)\mid x\equiv \text{Identity}(\bmod\ \mathfrak{p}_v^{*n})\}\\ &=\{f:B(D)\to\mathfrak{O}_v\mid \pi_n\circ f=\pi_n\circ\varepsilon\}.\end{aligned}$$

Since $\mathfrak{M}(D)=\text{kernel}\ \varepsilon$, one sees immediately that $f(\mathfrak{M}(D))\subset\mathfrak{p}_v^{*m}$ for all $f\in D(m,v)$ and $f(\mathfrak{M}(D)^2)\subset\mathfrak{p}_v^{*m+1}$; f thus defines a homomorphism $\bar f:\mathfrak{M}(D)/\mathfrak{M}(D)^2\to\mathfrak{p}_v^{*m}/\mathfrak{p}_v^{*m+1}$. We obtain thus a map λ_m of $D(m,v)/D(m+1,v)$ into the (F_v-vector) space

$$\mathrm{Hom}_A(\mathfrak{M}(D)/\mathfrak{M}(D)^2,\ \mathfrak{p}_v^{*m}/\mathfrak{p}_v^{*m+1})\cong\mathfrak{d}$$

where $\mathfrak{d}=\mathrm{Hom}_A(\mathfrak{M}(D)/\mathfrak{M}(D)^2,A)\otimes_A F_v$ for *almost all* v. It is easily seen that the map λ_m is a group homomorphism. If now $D_1\subset D$ is a k-algebraic subgroup we have the following commutative diagram:

$$\begin{array}{ccc} D(m,v)/D(m+1,v) & \longrightarrow & \mathfrak{D}\otimes_A F_v\\ \uparrow & & \uparrow\\ D_1(m,v)/D_1(m+1,v) & \longrightarrow & \mathfrak{D}_1\otimes_A F_v\end{array}$$

More generally if $\mathbf{D}_1$ and $\mathbf{D}$ are group-schemes over A and $u:\mathbf{D}_1\to\mathbf{D}$ is a morphism, one has the same kind of diagram. Using this fact it is easily proved by induction on the dimension of D that we have the following:

Let D be a *unipotent* k-algebraic subgroup of $GL(n)$ admitting a filtration

$$D\supset D_1\supset D_2\supset\ldots\supset D_k$$

by normal subgroups such that D_i/D_{i+1} is isomorphic to the additive group (of the field). Then for almost all v, the natural map $D(m,v)/D(m+1,v)\to\mathfrak{D}\otimes_A F_v$ defined above is an isomorphism.

Part *a)* of Assertion (1.18) is an immediate consequence of this statement applied to $D=U$ (see Borel-Tits [1]). Part *b)* again follows from the above since the map

$$G(m, v)/G(m+1, v) \rightarrow \mathfrak{G} \otimes_A F_v$$

is compatible with the action of G(A) on both sides. The subspace $\mathfrak{U} \otimes_A F_v$ on $\mathfrak{G} \otimes_A F_v$ has a non-trivial projection on all the factors of $\mathfrak{G} \otimes_A F_v$ for almost all v. (For almost all v, $\mathfrak{U} \otimes_A F_v \rightarrow \mathfrak{G} \otimes_A F_v$ is injective; we use Lemmas (1.9)-(1.16) as well.) This proves Assertion (1.18) and the proof of the Main Lemma is complete.

(1.20). — We will now apply the Main Lemma to show that projective limits of certain exact sequences (which we need to examine) remain exact. We have defined groups $G(\mathfrak{a})$, $EG(\mathfrak{a})$, $FG(\mathfrak{a})$ and $F^*G(\mathfrak{a})$ for each ideal $\mathfrak{a} \subset A$. These groups can be used to define topological group structures on $G(k)$ or $G(A)$. Each of the families below can be taken as a fundamental system of neighborhoods of 1 to obtain a topological group structure on $G(k)$ or $G(A)$:

1) All arithmetic subgroups; this topology is denoted $\mathscr{T}(a)$;

2) the groups $\{G(\mathfrak{a}) \mid \mathfrak{a} \neq 0$ on ideal in A$\}$; this topology is denoted $\mathscr{T}(c)$ (this is the same as the topology induced from the adèle group $G(\mathbf{A})$);

3) the groups $\{FG(\mathfrak{a}) \mid \mathfrak{a} \neq 0$ an ideal in A$\}$; this is denoted $\mathscr{T}(f)$;

4) the groups $\{EG(\mathfrak{a}) \mid \mathfrak{a} \neq 0$ an ideal in A$\}$; this is denoted $\mathscr{T}(e)$.

The completion of $G(k)$ with respect to $\mathscr{T}(a)$ (resp. $\mathscr{T}(c)$, $\mathscr{T}(f)$, $\mathscr{T}(e)$) is denoted $\hat{G}(a)$ (resp. $\hat{G}(c)$, $\hat{G}(f)$, $\hat{G}(e)$). The closure of $G(A)$ in $\hat{G}(a)$ (resp. $\hat{G}(c)$, $\hat{G}(f)$, $\hat{G}(e)$) is an open subgroup there and can be identified with the completion $\hat{G}(A, a)$ (resp. $\hat{G}(A, c)$, $\hat{G}(A, f)$, $\hat{G}(A, e)$) of $G(A)$ for the corresponding topology on $G(A)$. The identity maps of $G(k)$ and $G(A)$ give rise to the following diagram with all arrows continuous maps:

$$\begin{tikzcd}
\hat{G}(e) \arrow[r, "h(e,f)"] & \hat{G}(f) \arrow[r, "h(f,c)"] & \hat{G}(c) & \hat{G}(a) \arrow[l, "h(a,c)"'] \\
\hat{G}(A, e) \arrow[u] \arrow[r, "\bar{h}(e,f)"] & \hat{G}(A, f) \arrow[u] \arrow[r, "\bar{h}(f,c)"] & \hat{G}(A, c) \arrow[u] & \hat{G}(A, a) \arrow[u] \arrow[l, "\bar{h}(a,c)"']
\end{tikzcd}$$

We also set

$$h(e, c) = h(f, c) \circ h(e, f),$$
$$\bar{h}(e, c) = \bar{h}(f, c) \circ \bar{h}(e, f).$$

It is then easy to see that $h(\ ,\ )$ and $\bar{h}(\ ,\ )$ have the same kernel which we denote by $CG(\ ,\ )$. $CG(a, c)$ is what was called $C(S, G)$ in the Introduction. The groups $\hat{G}(A, c)$ and $\hat{G}(A, a)$ are evidently compact. (Also from the Main Lemma, it is clear that $\hat{G}(A, c)$ is isomorphic to an open subgroup of $G(\mathbf{A}(S))$.) In general the groups $EG(\mathfrak{a})$ need not have finite index in $G(A)$ and so the group $\hat{G}(e)$ is not in general compact. The groups $F^*G(\mathfrak{a})$ can again be used to define a topology on $G(k)$ but in view of

Lemma (1.7) this topology is the same as $\mathscr{C}(f)$ when k-rank$(G)\geq 2$. The group $\hat{G}(A, e)$ (resp. $\hat{G}(A,f)$, $\hat{G}(A, c)$, $\hat{G}(A, a)$) can also be regarded as the projective limit of the following family of groups

$$\{G(A)/EG(\mathfrak{a}) \mid \mathfrak{a} \text{ non-zero ideal in } A\}$$

(resp. $\{G(A)/FG(\mathfrak{a}) \mid \mathfrak{a}$ a non-zero ideal in A$\}$, $\{G(A)/G(\mathfrak{a}) \mid \mathfrak{a}$ a non-zero ideal in A$\}$, $\{G(A)/\Gamma \mid \Gamma$ an S-arithmetic subgroup of G(A)$\}$.

Consider now the following exact sequences:

$$1 \to G(\mathfrak{a})/EG(\mathfrak{a}) \to G(A)/EG(\mathfrak{a}) \to G(A)/G(\mathfrak{a}) \to 1$$
$$1 \to G(\mathfrak{a})/FG(\mathfrak{a}) \to G(A)/FG(\mathfrak{a}) \to G(A)/G(\mathfrak{a}) \to 1$$
$$1 \to G(\mathfrak{a})/EG(\mathfrak{a}) \to G(A)/EG(\mathfrak{a}) \to G(A)/FG(\mathfrak{a}) \to 1$$

These lead in the projective limit to the exact sequences described before

$$1 \to CG(\ ,\ ) \to \hat{G}(A,\ ) \xrightarrow{\bar{h}(\ ,\ )} \hat{G}(A,\ )$$

We will now deduce from the Main Lemma the following:

Proposition (**1.21**). — *The maps $\bar{h}(\ ,\ )$ are all surjective.*

In the case of $\bar{h}(a, c)$ this is immediate from the compactness of the groups $\hat{G}(A, a)$ and $\hat{G}(a, c)$. We will prove the proposition in the case $\bar{h}(e, c)$. The other cases are proved entirely analogously.

For a non-zero ideal $\mathfrak{a}\subset A$, let $G^*(\mathfrak{a}) = \bigcap_{\mathfrak{b}\neq 0} EG(\mathfrak{a}).G(\mathfrak{b})$. The Main Lemma guarantees that $G^*(\mathfrak{a}) \supset G(\mathfrak{a}')$ for some $\mathfrak{a}'\neq 0$. It follows that in the projective limit the natural maps $G(A)/G^*(\mathfrak{a}) \to G(A)/G(\mathfrak{a})$ induce an isomorphism. From the Main Lemma and the definition of $G^*(\mathfrak{a})$, it is clear that we have

$$(**) \qquad EG(\mathfrak{a})G^*(\mathfrak{b}) = G^*(\mathfrak{a})$$

for all non-zero ideals $\mathfrak{a}$, $\mathfrak{b}\subset A$ with $\mathfrak{b}\subset\mathfrak{a}$. We have now to establish that the projective limit of the family of the exact sequences

$$1 \to G^*(\mathfrak{a})/EG(\mathfrak{a}) \to G(A)/EG(\mathfrak{a}) \to G(A)/G^*(\mathfrak{a}) \to 1,$$

$\mathfrak{a}$ a non-zero ideal in A is again exact. Fix a decreasing family of non-zero ideals $\{\mathfrak{a}_n \mid 1\leq n<\infty\}$ cofinal in the family of all non-zero ideals. Let

$$\{\xi_n\in G(A)/G^*(\mathfrak{a}_n) \mid 1\leq n<\infty\}$$

be any element in the projective limit. We will prove inductively that we can find

$$\eta_n\in G(A)/EG(\mathfrak{a}_n)$$

which maps under the corresponding natural maps into ξ_n and η_{n-1}. Assume the η_i chosen for $1\leq i<r$. Let $\eta\in G(A)/EG(\mathfrak{a}_r)$ be an arbitrary lift of ξ_r. Let η' be its image in $G(A)/EG(\mathfrak{a}_{r-1})$. Then $\eta'^{-1}\eta_{n-1}\in G^*(\mathfrak{a}_{r-1})/EG(\mathfrak{a}_{r-1})$. In view of $(**)$

above we can find $\eta'' \in G^*(\mathfrak{a}_r)/EG(\mathfrak{a}_r)$ which maps into $\eta'^{-1}\eta_{r-1}$. It is then clear that $\eta_r = \eta\eta''$ is a lift of ξ_r with the desired properties.

(In the other cases we need an analogue of the Main Lemma. Since $EG(\mathfrak{a}) \subset FG(\mathfrak{a})$, such an analogue is immediate when we deal with the $G(\mathfrak{a})$ and the $FG(\mathfrak{a})$. When we are dealing with $EG(\mathfrak{a})$ and $FG(\mathfrak{a})$ a more subtle consideration is needed. We fix a (finite) complete set of representatives P_i, $1 \leq i \leq q$, of proper k-QPS in G, and for each P_i a k-AS M_i to which P_i is adapted. Since P_i is a semidirect product $P_i = M_i U_i$ with U_i the unipotent radical of P_i, and $U_i(\mathfrak{a}) \subset EG(\mathfrak{a})$, it suffices to show the existence of a non-zero ideal $\mathfrak{a}'$ in A such that $EG(\mathfrak{a}).M_i(\mathfrak{b}) \supset M_i(\mathfrak{a}')$ for all non-zero ideals $\mathfrak{b} \subset A$. But this follows simply from the Main Lemma applied to the group M_i instead of G. Note that M_i is simply connected and $EM_i(\mathfrak{a}) \subset EG(\mathfrak{a})$. M_i may not be simple but it decomposes over k into a product of k-simple factors; these k-simple factors again may not be absolutely simple but they are of the form $R_{k'/k}(H)$ with H an absolutely simple group over the field k', a finite extension of k.)

Corollary **(1.22)**. — *The sequences*

$$1 \to CG(\ ,\ ) \to \hat{G}(A,\ ) \to \hat{G}(A,\ ) \to 1$$

and

$$1 \to CG(\ ,\ ) \to \hat{G}(\ ) \to \hat{G}(\ ) \to 1$$

are exact.

The exactness of the first sequence is given by Proposition (1.21). Since

$$\hat{G}(A, *)G(k) = G(*),$$

$\hat{G}(A, *)$ is an open subgroup of $\hat{G}(*)$ and $G(k)$ is dense in $\hat{G}(*)$, the exactness of the second sequence follows.

Remark **(1.23)**. — The group $CG(e, c)$ is the projective limit of $G(\mathfrak{a})/EG(\mathfrak{a})$. Similarly

$$CG(e, f) = \varprojlim_{\mathfrak{a}} FG(\mathfrak{a})/EG(\mathfrak{a})$$

and

$$CG(f, c) = \varprojlim_{\mathfrak{a}} G(\mathfrak{a})/FG(\mathfrak{a}).$$

For convenient future use we state explicitly as a lemma the following which was proved in the course of the proof of Proposition (1.21):

Lemma **(1.24)**. — *Given a non-zero ideal* $\mathfrak{a}$ *we can find a non-zero ideal* $\mathfrak{a}^*$ *such that* $FG(\mathfrak{a}).G(\mathfrak{b}) \supset G(\mathfrak{a}^*)$ *for* all *non-zero ideals* $\mathfrak{b}$.

2. Normal Subgroups in Arithmetic Groups.

Our aim in this section is to establish the following. (We make free use of the notation introduced in § 1: beginning of § 1 and the paragraph before Lemma (1.7).)

Theorem **(2.1).** — *Assume that k-rank$(G)\geq 1$ and that $\sum_{v\in S} k_v$-rank$(G)\geq 2$. Let $\Gamma\subset G$ be an S-arithmetic subgroup of G and $\Psi\subset\Gamma$ a normal subgroup of Γ. Then either Ψ is central (and finite) in G or there exists a non-zero ideal $\mathfrak{a}\subset A$ such that $E(\mathfrak{a})\subset\Psi$.*

The first observation is

Lemma **(2.2).** — *If Ψ is not central in G it is Zariski dense in G.*

Let G' be the Zariski closure of Ψ in G. Since Γ is Zariski dense in G', G' is a normal subgroup of G. Since G is (absolutely) simple, G' is either central and finite or all of G. This proves the lemma.

In the sequel, then we assume that Ψ is *not* central in G, so that it is *Zariski dense* in G. In particular Ψ is infinite. Hence so is any subgroup of finite index in Ψ. This enables us to replace Γ by $\Gamma\cap G(A)$ and Ψ by $\Psi\cap G(A)$. We assume in the sequel that $\Gamma\subset G(A)$ — in fact, we assume as we may that Γ is a *normal subgroup of* G(A) *of finite index in* G(A). Next, one knows the following from reduction theory (Borel [1] for number fields and Behr [1] and Harder [1] for function fields):

Lemma **(2.3).** — *G has only finitely many Γ-conjugacy classes of minimal k-parabolic subgroups.*

Suppose now U is the unipotent radical of a minimal k-parabolic subgroup P of G. Since $\Gamma\subset G(A)$, we see that for any ideal $\mathfrak{a}\subset A$ and any element $\gamma\in\Gamma$, ${}^{\gamma}U(\mathfrak{a})=({}^{\gamma}U)(\mathfrak{a})$. In view of Lemma (2.3), this remark reduces the proof of the theorem to establishing

Proposition **(2.4).** — *Let U be the unipotent radical of a minimal k-parabolic subgroup P. Then there exists a non-zero ideal $\mathfrak{a}\subset A$ such that $\Psi\supset U(\mathfrak{a})$.*

The rest of the section is devoted to the proof of this proposition. We introduce some additional notation for this purpose.

Notation **(2.5).** — We fix P and U as above. Let $T\subset P$ be a maximal k-split torus and X(T) the group of characters on T. Let $\mathfrak{g}$ be the Lie algebra of G and for $\chi\in X(T)$, let

$$\mathfrak{g}^{\chi}=\{v\in\mathfrak{g}\mid \mathrm{Ad}\, t(v)=\chi(t).v\}.$$

Let $\Phi=\{\alpha\in X(T)\mid \alpha\neq 0,\ \mathfrak{g}^{\alpha}\neq(0)\}$: Φ is the set of k-roots of G with respect to T. Let $\Phi^{+}=\{\alpha\in\Phi\mid \mathfrak{g}^{\alpha}\subset\mathfrak{u}=\text{Lie algebra of } U\}$. Then there is a lexicographic ordering on X(T) such that Φ^{+} is precisely the set of positive k-roots. Let Δ denote the system of simple roots for this ordering. Then, for each $\varphi\in\Phi$,

$$\varphi=\sum_{\alpha\in\Delta} m_{\alpha}(\varphi)\alpha,\qquad m_{\alpha}(\varphi)\in\mathbf{Z}$$

with all $m_{\alpha}(\varphi)$ of the same sign, this sign being positive if $\varphi\in\Phi^{+}$. For $\alpha\in\Delta$, let

$$\Phi\langle\alpha\rangle=\{\varphi\in\Phi^{+}\mid m_{\alpha}(\varphi)>0\}.$$

Let

$$S(\alpha) = \text{identity component of } \bigcap_{\beta \in \Delta - (\alpha)} \text{kernel } \beta,$$

and

$$Z(\alpha) = \text{connected centralizer of } S(\alpha).$$

Then $Z(\alpha).U = P(\alpha)$ is a maximal proper k-parabolic subgroup of G. If $U(\alpha)$ is the unipotent radical of $P(\alpha)$, the Lie algebra $\mathfrak{u}(\alpha)$ of $U(\alpha)$ is the subspace $\sum_{\varphi \in \Phi\langle\alpha\rangle} \mathfrak{g}^{\varphi}$ of $\mathfrak{g}$. Let $Z(T)$ (resp. $N(T)$) denote the centralizer (resp. normalizer) of T and $W_0 = N(T)/Z(T)$ (the k-Weyl group of G). Let $W \subset N(T)(k)$ be a complete set of representatives for W_0. Such a W exists (see Borel-Tits [1] for this as well as any other facts about algebraic groups involving rationality questions). Let $w \in W$ be the unique element which induces on $X(T)$ the automorphism which takes all of Φ^+ into negative roots. For $\alpha \in \Delta$,

$$w(\alpha) = -\hat{\alpha} \quad \text{with} \quad \hat{\alpha} \in \Delta.$$

The map $\alpha \mapsto \hat{\alpha}$ is an automorphism of the Dynkin diagram of Δ. Moreover, it is easily checked that $\hat{\hat{\alpha}} = \alpha$ and, if ${}^{w}U = U^{-}$, ${}^{w}P(\alpha) = Z(\hat{\alpha})U^{-}$ $(\overset{\text{def}}{=} P(-\hat{\alpha}))$. Let

$$f_\alpha : U(\hat{\alpha}) \times P(\alpha) \to G$$

be the map $f_\alpha(u, p) = uwp$. Then f_α is an isomorphism of $U(\hat{\alpha}) \times P(\alpha)$ onto an open subset $B(\alpha)$ of G. For $x \in B(\alpha)$ we set

$$x = u_\alpha(x) w p_\alpha(x), \qquad u_\alpha(x) \in U(\hat{\alpha}), \qquad p_\alpha(x) \in P(\alpha).$$

Then $x \mapsto u_\alpha(x)$ and $x \mapsto p_\alpha(x)$ are k-morphisms of $B(\alpha)$ into $U(\hat{\alpha})$ and $P(\alpha)$ respectively. Next, let $D(\alpha) = P(\alpha) \cap {}^{w}P(\alpha)$. Since w has order 2 modulo $Z(T)$, $D(\alpha)$ is stable under w (and contains $Z(T)$). Let $M(\alpha)$ be the identity component of the Zariski closure of $D(\alpha) \cap \Gamma$. The group $M(\alpha)$ is in fact intrinsically determined by $D(\alpha)$ — it does not depend on the S-arithmetic subgroup Γ (though it does depend on the set S). It is a connected normal subgroup of $D(\alpha)$. For $\varphi \in \Phi$, let $\mathfrak{u}^{(\varphi)} = \sum_{k \in \mathbf{Z},\, k > 0} \mathfrak{g}^{k\varphi}$. Then there is a unique connected unipotent k-subgroup $U^{(\varphi)}$ of G having $\mathfrak{u}^{(\varphi)}$ for its Lie algebra (we note here that if $\varphi \in \Phi$ with $k\varphi \in \Phi$, k an integer, then $k = \pm 1$ or ± 2 so that the above summation is over at most 2 terms). With this notation we record here as a lemma the following observation.

Lemma **(2.6)**. — *For* $\alpha \in \Delta$, $M(\alpha) \supset U^{(\beta)}$ *for all* β *with* $\pm\beta \in \Delta$ *and* $\pm\beta \neq \alpha$ *or* $\hat{\alpha}$. *If* $\alpha \neq \hat{\alpha}$, $M(\alpha) \supset U^{(\alpha)}$ *and* $U^{(-2\alpha)}$.

This is a simple consequence of the following. If V is a connected unipotent algebraic k-group, then any S-arithmetic subgroup of V (with $S \neq \emptyset$) is Zariski dense in V. One has only to apply this remark to conclude that $U^{(\beta)} \subset M(\alpha)$ as well as the other two inclusions when $\alpha \neq \hat{\alpha}$.

Notation (**2.7**). — We need to introduce yet another subgroup of G for each $\alpha\in\Delta$. $P'(\alpha)$ is the algebraic subgroup generated by the set

$$\{p^{-1}\hat{x}pux^{-1}u^{-1} \mid u\in U(\hat{\alpha}), p\in P(\alpha), x\in M(\alpha)\}$$

and where for $x\in M(\alpha)$, $\hat{x}=w^{-1}xw$. The group $Z(\alpha)$ decomposes into an almost direct product:

$$Z(\alpha)=C(\alpha).A(\alpha).H(\alpha)$$

where $C(\alpha)$ is the identity component of the center of $Z(\alpha)$, $A(\alpha)$ is the maximal normal semisimple subgroup $Z(\alpha)$ which is anisotropic over k and $H(\alpha)$ is the product of all the isotropic k-simple factors of $Z(\alpha)$. Then it is easily seen — and well known — that $C(\alpha).A(\alpha)\subset D(\alpha)$. If $\alpha=\hat{\alpha}$, $H(\alpha)\subset D(\alpha)$ as well and $D(\alpha)=Z(\alpha)$. If $\alpha\neq\hat{\alpha}$, however, one cannot assert this. Nevertheless we do have

Lemma (**2.8**). — *(Assume that* $S\neq\emptyset$.) *Then* $P'(\alpha)$ *contains the identity component of the Zariski closure of any* S*-arithmetic subgroup of* $Z(\alpha)$.

To prove this assertion, we observe first that if Φ is an S-arithmetic subgroup of $Z(\alpha)$, the group $(\Phi\cap C(\alpha)).(\Phi\cap A(\alpha)).(\Phi\cap H(\alpha))$ has finite index in Φ (Borel [1] for k a number field and Harder [1] and Behr [1] for k a function field). It suffices then (since $C(\alpha).A(\alpha)\subset D(\alpha)$) to show that the e-component of the Zariski closure of $\Phi\cap H(\alpha)$ is contained in $P'(\alpha)$. When $\alpha=\hat{\alpha}$, $H(\alpha)\subset D(\alpha)$ and the assertion is immediate. One observes next that $H(\alpha)$ is generated as an algebraic group by the $\{U^{(\pm\beta)} \mid \beta\in\Delta-\{\alpha\}\}$ and $U^{\pm\beta}\cap\Phi$ is Zariski dense in $U^{\pm\beta}$, $\beta\in\Delta-\{\alpha\}$. The group $M(\alpha)$, one concludes then, contains all of $H(\alpha)$ if $\alpha=\hat{\alpha}$, and if $\alpha\neq\hat{\alpha}$, it contains $U^{\pm\beta}$, $\beta\in\Delta-\{\alpha,\hat{\alpha}\}$ and $U^{(-\hat{\alpha})}$. Then if $\alpha=\hat{\alpha}$, $M(\alpha)\supset H(\alpha)$ and the lemma follows. If $\alpha\neq\hat{\alpha}$, we note that the element $s\in W$ corresponding to the reflection with respect to $\hat{\alpha}$ belongs to $P(\alpha)$. It follows that

$$sU^{-\hat{\alpha}}s^{-1}=U^{\hat{\alpha}}\subset P'(\alpha)$$

leading again to the conclusion that $P'(\alpha)$ contains $H(\alpha)$. The lemma follows immediately from this.

We are now in a position to prove

Proposition (**2.9**). — $\Psi\cap P(\alpha)$ *contains in its Zariski closure the identity component of the Zariski closure of any* S*-arithmetic subgroup of* $Z(\alpha)$.

In view of Lemma (2.8) it suffices to show that the Zariski closure of $\Psi\cap P(\alpha)$ contains $P'(\alpha)$. For this consider the subset $\Psi\cap B(\alpha)$ (see § 2.5 for notation) of Ψ. As $B(\alpha)$ is Zariski open in G and Ψ Zariski dense in G, $\Psi\langle\alpha\rangle\overset{\text{def}}{=}\Psi\cap B(\alpha)$ is Zariski dense in G. It follows that

$$\mathscr{E}=\{(u,p)\in U(\hat{\alpha})\times P(\alpha) \mid uwp\in\Psi\}$$

is Zariski dense in $U(\hat{\alpha})\times P(\alpha)$. Next, for a fixed $u\in U(\hat{\alpha})(k)$, let

$$R(u)=\{x\in M(\alpha)\cap\Gamma \mid xux^{-1}u^{-1}\in\Gamma\}$$

and let $\mathscr{S}=\{(u,p,x)\mid(u,p)\in\mathscr{E}, x\in R(u)\}$. Let

$$F: U(\hat{\alpha})\times P(\alpha)\times M(\alpha)\to G$$

be the map defined by

$$F(u,p,x)=xp^{-1}x'^{-1}puxu^{-1}x^{-1}\qquad u\in U(\hat{\alpha}),\qquad p\in P(\alpha),\qquad x\in M(\alpha),$$

where $x'=w^{-1}xw$. We claim that $F(\mathscr{S})\subset P(\alpha)\cap\Psi$. To see this, let $\gamma=uwp$, $(u,p)\in\mathscr{E}$; then $\gamma\in\Psi$ and hence so is

$$\xi=\theta\gamma\theta^{-1}=\theta u\theta^{-1}.\theta wp\theta^{-1}=\theta u\theta^{-1}u^{-1}.uw\theta' p\theta^{-1}$$

for all $\theta\in R(u)$. Let $\alpha=\theta u\theta^{-1}u^{-1}$; then $\alpha\in\Gamma$, so that

$$\eta=\alpha\gamma\alpha^{-1}\in\Psi.$$

We have, moreover,

$$\xi_{P(\alpha)}=\theta u\theta^{-1}u^{-1}\gamma_{P(\alpha)}=\eta_{P(\alpha)}$$

(note that $U(\hat{\alpha})\subset P(\alpha)$ so that $\theta u\theta^{-1}u^{-1}\in P(\alpha)$). Since $P(\alpha)$ is its own normalizer,

$$\xi^{-1}\eta=\theta p^{-1}\theta'^{-1}p.u\theta u^{-1}\theta^{-1}\in\Psi\cap P(\alpha).$$

We have thus proved that $F(\mathscr{S})\subset P(\alpha)\cap\Psi$. We now claim that $\mathscr{S}$ is Zariski dense in $U(\hat{\alpha})\times P(\alpha)\times M(\alpha)$. Since $\mathscr{E}$ is Zariski dense in $U(\hat{\alpha})\times P(\alpha)$, it suffices to show that for each $u\in U(\hat{\alpha})(k)$, $R(u)$ is Zariski dense in $M(\alpha)$. To see this consider the map h of $M(\alpha)$ in G given by $x\mapsto xux^{-1}u^{-1}$. Now the entries of $(xux^{-1}u^{-1}-\text{Identity})$ are polynomials in the entries of $(x-\text{Identity})$ with coefficients in k and without constant terms. It follows that we can find an ideal $\mathfrak{a}\neq 0$ in A such that $h(M(\alpha)(\mathfrak{a}))\subset G(A)$. Let $\bar{h}$ be the composite map $\pi\circ h$

$$\begin{tikzcd}\Gamma\cap M(\alpha)(\mathfrak{a}) \arrow[r, "h"] \arrow[rr, bend right, "\bar{h}"'] & G(A) \arrow[r, "\pi"] & G(A)/\Gamma\end{tikzcd}$$

π being the natural projection. Then we have for $x,y\in M(\alpha)(\mathfrak{a})\cap\Gamma$,

$$h(xy)=xy.u.y^{-1}x^{-1}u^{-1}=x(yuy^{-1}u^{-1})ux^{-1}u^{-1}=xh(y)x^{-1}.h(x)$$

so that $\bar{h}(xy)=\bar{h}(y).\bar{h}(x)$. (Note that we have assumed that Γ is normal in $G(A)$.) Since $G(A)/\Gamma$ is finite, $\bar{h}^{-1}(e)$ is a (normal) subgroup of $\Gamma\cap M(\alpha)(\mathfrak{a})$ of finite index. Clearly this subgroup is contained in $R(u)$ and on the other hand it is Zariski dense in $M(\alpha)$. This shows that $R(u)$ is Zariski dense in $M(\alpha)$, thereby establishing Proposition (2.9).

(2.10). — Let $U(\alpha)^i$, $0\leq i\leq r+1$, be the descending central series of $U(\alpha)$: $U(\alpha)^0=U(\alpha)$ and for $i>0$, $U(\alpha)^i$ is the connected subgroup with

$$\text{Lie algebra}=\sum_{\varphi=\sum_{\beta\in\Delta}m_\beta\beta,\ m_\alpha\geq i+1}\mathfrak{g}^\varphi$$

(see Appendix) and $r+1=\inf\{q\mid U(\alpha)^q=(1)\}$. For $0\leq i\leq r$, let $V(i)=U(\alpha)^i/U(\alpha)^{i+1}$. It is known that $V(i)$ has a natural structure of a k-group k-isomorphic to a vector space.

Moreover each $U(\alpha)^i$ is stable under $P(\alpha)$ and since $[U(\alpha), U(\alpha)^i] \subset U(\alpha)^{i+1}$, this action passes down to a linear action of $P(\alpha)/U(\alpha)$ on each of the $V(i)$, an action defined over k. The group $Z(\alpha)$ maps k-isomorphically onto the quotient $P(\alpha)/U(\alpha) = Z_1(\alpha)$, say. Let $Z^*(\alpha)$ (resp. $Z_1^*(\alpha)$) denote the identity component of the Zariski closure of any S-arithmetic subgroup of $Z(\alpha)$ (resp. $Z_1(\alpha)$). Let $P^*(\alpha)$ be the Zariski closure of $\Psi \cap P(\alpha)$. Then $Z_1^*(\alpha)$ is contained in the image of $P^*(\alpha)$ in $Z_1(\alpha)$. Evidently $Z_1^*(\alpha)$ is a k-subgroup and the image of $\Psi \cap P(\alpha)$ in $Z_1(\alpha)$ contains $Z_1^*(\alpha)$ in its Zariski closure. Consider now the natural map $p_i : U(\alpha)^i \to V(i)$. We identify each $V(i)$ with a vector space through a k-isomorphism and fix a k-basis in $V(i)$. Let L_i' denote the A-linear span of such a k-basis. Then from Corollary (A.6) (Appendix) we know that $p_i(U(\alpha)^i(A))$ contains an A-submodule L_i of L_i' of maximal rank. Since $[G(A), \Gamma] \subset \Gamma$, one concludes immediately that the **Z**-module spanned by $p_i([U(\alpha)^i(A), P(\alpha) \cap \Gamma]) \subset p_i(U(\alpha)^i \cap \Gamma)$. Clearly $p_i([U(\alpha)^i(A), P(\alpha) \cap \Gamma])$ contains the **Z**-span of $\{(\sigma_i(x) - 1)(v) \mid x \in P(\alpha) \cap \Gamma, v \in L_i\}$ where σ_i is the natural representation of $P(\alpha)$ on $V(i)$. This shows that $p_i(U(\alpha)^i \cap \Gamma)$ contains an A-submodule K_i of L_i with L_i/K_i finite. The argument given above can now be repeated with Γ replacing $G(A)$, K_i replacing L_i and $\Psi(\mathfrak{a}) = \Psi \cap G(\mathfrak{a})$, $\mathfrak{a} \neq 0$ an ideal in A, replacing Γ, to conclude the following: for each i, $0 \leq i \leq r$, and a non-zero ideal $\mathfrak{a} \subset A$, $p_i(U(\alpha)^i \cap \Psi(\mathfrak{a}))$ contains the A-submodule of K_i spanned by

$$\{(\sigma_i(x) - 1)(v) \mid v \in K_i, x \in P(\alpha) \cap \Psi(\mathfrak{a})\}.$$

We denote this last A-submodule of K_i by $J_i(\mathfrak{a})$.

Claim **(2.11)**. — For $0 \leq i \leq r$, $J_i(\mathfrak{a})$ has maximal rank in $V(i)$ — *i.e.* $J_i(\mathfrak{a})$ contains a basis of $V(i)$ as a vector space.

Proof of Proposition (2.4) **(2.12)**. — We will first show that Theorem (2.1) is a consequence of Claim (2.11). We argue by downward induction on the integer i to show first that for any ideal $\mathfrak{a} \neq 0$ in A, $U(\alpha)^i \cap \Psi$ contains a congruence subgroup of $U(\alpha)^i$. The start of the induction at $i = r$ is immediate from Claim (2.11). Assume now that for some integer m, $1 \leq m \leq r$, and any ideal $\mathfrak{b} \neq 0$, we have an ideal $\mathfrak{b}^* \neq 0$, $\mathfrak{b}^* \subset \mathfrak{b}$, such that $\Psi(\mathfrak{b}) \cap U(\alpha)^m \supset U(\alpha)^m(\mathfrak{b}^*)$. Let $\mathfrak{a} \neq 0$ be any ideal in A and choose $\mathfrak{a}^*$ as above. Choose next an ideal $\mathfrak{a}' \neq 0$, $\mathfrak{a}' \subset \mathfrak{a}^*$, such that $J_{m-1}(\mathfrak{a}^*)$ contains $p_{m-1}(U(\alpha)^{m-1}(\mathfrak{a}^*))$. (Such a choice of $\mathfrak{a}'$ is possible in view of Claim (2.11).) We now assert that $U(\alpha)^{m-1} \cap \Psi(\mathfrak{a})$ contains $U(\alpha)^{m-1}(\mathfrak{a}')$. In fact, if $x \in U(\alpha)^{m-1}(\mathfrak{a}')$, by the definitions of $\mathfrak{a}'$ and $J_{m-1}(\mathfrak{a}^*)$, we can find $y \in U(\alpha)^{m-1} \cap \Psi(\mathfrak{a}^*)$ such that $p_{m-1}(x) = p_{m-1}(y)$, *i.e.* $y^{-1}x \in U(\alpha)^m(\mathfrak{a}^*)$. But then by the induction hypothesis $y^{-1}x \in U(\alpha)^m \cap \Psi(\mathfrak{a})$, so that $x = y.y^{-1}x \in U(\alpha)^m \cap \Psi(\mathfrak{a})$. It follows from this that $\Psi \cap U^{(\varphi)}$, for any positive k-root φ, contains a congruence subgroup $U^{(\varphi)}(\mathfrak{a})$ with $\mathfrak{a} \subset A$, a non-zero ideal. Now if we arrange the positive roots in, say, increasing order $\Phi = (\alpha_1, \ldots, \alpha_m)$, then the map

$$\lambda : U^{(\alpha_1)} \times U^{(\alpha_2)} \times \ldots \times U^{(\alpha_m)} \to G$$

given by $\lambda(x_1, \ldots, x_m) = x_1 \cdot x_2 \cdot \ldots \cdot x_m$, is an isomorphism defined over k; the entries of $\{\lambda(x_1, \ldots, x_n) - \text{identity}\}$ are polynomials without constant terms with coefficients in k in the entries of $\{(x_j - \text{identity}) \mid 1 \leq j \leq m\}$. A similar remark applies to λ^{-1}. It follows that $\Psi \cap U$ contains $\lambda(U^{(\alpha_1)}(\mathfrak{a}) \times U^{(\alpha_2)}(\mathfrak{a}) \times \ldots \times U^{(\alpha_m)}(\mathfrak{a}))$ and the last set obviously contains an S-congruence subgroup of U. This proves Proposition (2.4) and hence Theorem (2.1) (subject to Claim (2.11)).

Before we proceed to the proof of Claim (2.11), we make the following

Remark **(2.13).** — T_A is infinite and Zariski dense in T if and only if $|S| \geq 2$. If $|S| = 1$ and v is the unique valuation in S, k_v-rank$(G) \geq 2$.

In the sequel we consider the two cases when $|S| = 1$ and $|S| > 1$ separately.

(2.14) *Case when* $|S| > 1$. — From Remark (2.13), we see that T is contained in the Zariski closure of any S-arithmetic subgroup of $Z(\alpha)$. Now the characters of T which are eigen-characters in the representation σ_i are all k-roots of G and are hence non trivial. It follows that the set

$$\{(\sigma_i(t) - 1)v \mid t \in T, v \in V(i)\}$$

spans all of $V(i)$ as a vector space. In view of the density results we have proved earlier, we conclude that for any non-zero ideal $\mathfrak{a} \subset A$, $J_i(\mathfrak{a})$ spans all of $V(i)$ as a vector space, establishing Claim (2.11) in this case.

(2.15) *Case when* $|S| = 1$. — As was observed this would mean that for the unique $v \in S$, k_v-rank$(G) \geq 2$. Let $T' \cap Z(T)$ be a maximal k_v-split torus in G. Choose an ordering on the character group $X(T')$ of T' compatible with the order on $X(T)$ introduced earlier and the restriction map $X(T) \to X(T')$. Let Φ' (resp. Δ') denote the system of k_v-roots (resp. simple k_v-roots) of G with respect to T'. For $\varphi \in \Phi'$, let $\mathfrak{g}^\varphi$ denote the eigen-space of T' corresponding to φ for the adjoint action of T' on $\mathfrak{g}$. We can then describe the Lie algebra $\mathfrak{u}(\alpha)$ of $U(\alpha)$, $\alpha \in \Delta$, as follows: for $\alpha \in \Delta$, let $\Delta'(\alpha) = \{\beta \in \Delta' \mid \beta|_T = \alpha\}$. Let

$$\Psi'\langle\alpha\rangle = \{\varphi \in \Phi' \mid \varphi = \sum_{\beta \in \Delta'} m_\beta(\varphi) . \beta,\ m_\beta(\varphi) > 0 \text{ for some } \beta \in \Delta'(\alpha)\}.$$

Then

$$\mathfrak{u}(\alpha) = \sum_{\varphi \in \Phi'\langle\alpha\rangle} \mathfrak{g}^\varphi.$$

Now, the identity component $Z^*(\alpha)$ of the Zariski closure of any S-arithmetic subgroup of $Z(\alpha)$, it is easily seen, intersects the k_v-split torus T' in a subgroup T'^* of codimension 1. We denote by T^* the identity component of T'^*. Suppose now for the action of $Z^*(\alpha)$ on $V(0)$ we have a quotient module which is trivial. Such a module would be trivial under T^* as well. Since the actions of T and T^* on $V(0)$ are completely reducible, we conclude that this means that for some eigen-character φ of T occurring in the space $V(0)$,

$\varphi|_{T^*}$ is trivial. Suppose now σ is the adjoint representation of $Z(\alpha)$ on $\mathfrak{u}(\alpha)$. Then $\chi(t)=\det\sigma(t)$ is a character on $Z(\alpha)$ defined over k. It follows that $\chi(Z(\alpha)(A))\subset$ S-units in A, a finite group (since $|S|=1$). It follows that χ is trivial on $Z^*(\alpha)$, so that $\chi|_{T'}$ is a character with $\chi(T^*)=1$. We conclude therefore that the character φ is necessarily a multiple of χ. Now the character χ is known (and it is also not difficult to see) to be a dominant weight (for the k_v-root system and the order chosen). It follows that in the expression for φ as a linear combination of the simple k_v-roots *all* the roots $\beta\in\Delta'$ occur with a strictly positive coefficient. On the other hand, from the definition of $V(0)$, it is immediate that at most one of the $\beta\in\Delta'(\alpha)$ occurs with a non-zero coefficient and that coefficient is 1. It follows that $\Delta'(\alpha)$ contains only one element which we denote $\widetilde{\alpha}$ in the sequel. We have therefore proved the following:

If $V(0)$ as a module over $Z^*(\alpha)$ has a trivial quotient, then $|\Delta'(\alpha)|=1$; the unique element of $\Delta'(\alpha)$ being denoted $\widetilde{\alpha}$.

If $V(0)$ has no trivial quotient as a $Z^*(\alpha)$-module, the set

$$\{(\sigma_0(x)-1)v\,|\,v\in V(0),\ x\in Z^*(\alpha)\}$$

spans all of $V(0)$ as a vector space and an argument similar to what was given in (2.14) now shows immediately that $J_0(\mathfrak{a})$ has maximal possible rank in $V(0)$. We will now show next that $V(0)$ has no trivial quotient as a $Z^*(\alpha)$-module even in the case $\Delta'(\alpha)=1$. For this fix a maximal torus T'' in $Z(T)$ containing T' and introduce an ordering on $X(T'')$ compatible with those introduced on $X(T)$ and $X(T')$ already. Let Δ'' denote the simple roots of G with respect to T''. Let φ be a root of G with respect to T which is an eigen-character of T'' for its action on the unique maximal quotient of $V(0)$ on which $Z^*(\alpha)$ acts trivially (on this unique maximal quotient, $Z(\alpha)$ has a natural action — note that $Z^*(\alpha)$ is normal in $Z(\alpha)$): we *assume* such a φ exists. Then we see that $\langle\varphi|_{T'},\beta\rangle=0$ for all $\beta\in\Delta'-\widetilde{\alpha}$ where $\langle\ ,\ \rangle$ denotes the canonical scalar product on $X(T')$: equivalently $\langle\varphi|_{T'},\beta\rangle=0$ for all k_v-roots of the (reductive) group $Z(\alpha)$. Since $\varphi|_{T'}$ is a positive k_v-root, $\langle\varphi|_{T'},\widetilde{\alpha}\rangle>0$. It follows that there is some root $\alpha^*\in\Delta''$ such that $\alpha^*|_{T'}=\widetilde{\alpha}$ and $\langle\varphi,\alpha^*\rangle\geq 0$. Now from the structure theory of semisimple groups (over algebraically closed fields), one sees that either $\varphi=\alpha^*$ or $\varphi-\alpha^*$ is necessarily a positive root. Now since φ occurs as a weight in $V(0)$, there is at most one simple root $\gamma\in\Delta''$ with $\gamma|_{T'}=\widetilde{\alpha}$ which occurs with *positive coefficient* $(=1)$ in the expression for φ as a combination of the roots in Δ. Now if $\varphi=\alpha^*$, this would mean that $\widetilde{\alpha}$ is orthogonal to all the other simple k_v-roots of T, a contradiction to the (k_v-) simplicity of G. We see therefore that $\varphi-\alpha^*=\beta$ is a positive root of the reductive group $Z(\alpha)$ (with respect to T''.) Since $\varphi|_{T^*}$ is trivial and $\alpha^*|_{T^*}=\widetilde{\alpha}|_{T^*}$ is non-trivial, $(\varphi-\alpha^*)|_{T'}$ is non-trivial and is therefore a positive k_v-root. Now if we set $\gamma=\varphi-\alpha^*$, $\varphi-\gamma$ and φ are roots. Again from the fact that $\gamma|_{T^*}$ is non-trivial, it is easily concluded that γ is a positive root of $Z(\alpha)$ with respect to T and that the corresponding 1-parameter unipotent group is then necessarily contained in $Z^*(\alpha)$. It follows that $\langle\varphi,\gamma\rangle=0$. From structure theory now it is immediate that $\varphi+\gamma$ is a root and $\varphi+2\gamma$ is *not* a root. The Chevalley commutation relations among the one parameter unipotent groups $\chi_{\varphi+\gamma}(t)$ and $\chi_{-\gamma}(t)$ now give us (for $t, s \in$ algebraic closure of k) (see Steinberg [3])

$$(*) \qquad [\chi_{\varphi+\gamma}(t), \chi_{-\gamma}(s)] = \chi_{\varphi}(ts) \cdot \chi_{\varphi-\gamma}(\xi)$$

modulo $U(\alpha)^1$ for a suitable ξ. Now the character $\varphi-\gamma$ cannot occur in any quotient of $V(0)$ which is trivial as a $Z^*(\alpha)$-module (note that $\varphi-\gamma|_{T^*}$ is non-trivial) so that the eigen-space corresponding to the character $\varphi-\gamma$ certainly is contained in the span

$$\{(\sigma_0(x)-1)v \mid v \in V(0),\ \chi \in Z^*(\alpha)\}.$$

Since $\chi_{-\gamma}(s) \in Z^*(\alpha)$ for all s, $(*)$ shows that $\chi_{\varphi}(t)$ belongs to this span as well for all t, a contradiction to our choice of φ. This shows that $V(0)$ has no quotient $Z^*(T)$-module which is trivial. We have thus proved that when $|S|=1$, for all ideals $\mathfrak{a} \neq 0$ in A, $J_0(\mathfrak{a})$ has maximal rank in $V(0)$. To prove the statement for the $J_i(\mathfrak{a})$, $i>0$, we observe that arguments entirely analogous to those given above show that the span of $J_i(\mathfrak{a})$ in $V(i)$ would contain all eigen-spaces of $V(i)$ with the exception at most of those roots φ on T which are trivial on T^*. If we now again choose a root $\alpha^* \subset \Delta''$ with $\langle\varphi, \alpha^*\rangle > 0$ and $\alpha^*|_{T'} = \tilde{\alpha}$, we conclude that $\varphi-\alpha^*$ is a root (but now this is a root occurring as eigen-character in $V(i-1)$). It follows that " α^*-series " of roots through φ are either $(\varphi-\alpha^*, \varphi)$ or $(\varphi-2\alpha^*, \varphi-\alpha^*, \varphi, \varphi+\alpha^*)$. In the first case, using the Chevalley commutation relations, one sees immediately that the eigen-space corresponding to φ is in the image of the natural map $V(0) \otimes V(i-1) \to V(i)$ given by commutation. An obvious induction gives us now Claim (2.11) in this case. In the second case, we observe that the group G is of type G_2, that α^* is necessarily the short simple root, φ a short root, and $i=2$. Further $\varphi-2\alpha^*$ is necessarily the long simple root β, a root of $Z(\alpha)$, so that $\langle\varphi-2\alpha^*, \varphi\rangle = 0$. Moreover, we note that G_2 has only one isotropic k-form, *viz.* the split form (Tits [2]) so that $T=T'=T''$, $\Delta=\Delta'=\Delta''$ and $\alpha, \beta \in \Delta$. If we then consider the root β in place of α, our arguments above would show that the claim is true for this root and we conclude that $U(\beta) \cap \Psi(\mathfrak{a})$ is a congruence subgroup of $U(\beta)$. But this would mean that $U(\beta) \cap U(\alpha)^2 \cap \Psi(\mathfrak{a})$ is a congruence subgroup and then we can conclude that its image in $U(\alpha)^1/U(\alpha)^2$ contains the eigen-space corresponding to $\varphi = \beta + 2\alpha$ in its image.

Remark. — The proof can be simplified in the case of the number fields where a qualitative statement would have sufficed instead of the precise form of Chevalley commutation relations. A slightly different approach can also be used in this case and this was in fact done in an earlier preprint of the author.

3. The Action of $G(k)^+$ on $C(\ ,\ )$.

In § 1, we obtained the following exact sequence

$$1 \to C(\ ,\ \ ) \to \hat{G}(\ ) \to \hat{G}(\ \ ) \to 1$$

The group $G(k)^+$ is a subgroup of $\hat{G}(\ )$ in a natural fashion. It operates therefore on the normal subgroup $C(\ ,\ )$ of $\hat{G}(\ )$. We will take a closer look at this action in this chapter. The following is a well known theorem due to J. Tits [1].

Proposition (**3.1**). — *The only normal subgroups of* $G(k)^+$ *are central (in* G*) and finite. In particular* $G(k)^+$ *has no proper infinite normal subgroup.*

Proposition (3.1) has the following consequence: to show that $G(k)^+$ operates trivially on a set X, it would be sufficient to show that an infinite subgroup acts trivially on X.

Theorem (**3.2**). — *Assume that* k-*rank*$(G)\geq 2$. *Then* $G(k)^+$ *centralizes* $CG(f, c)$.

In view of the remark made above it suffices to show that there is an infinite subgroup Δ of $G(k)^+$ such that Δ commutes with all of $CG(f, c)$. From the discussion in (1.21) it is clear that it is enough to find a infinite subgroup $\Delta \subset G(A)\cap G(k)^+$ such that $[\Delta, G(\mathfrak{a})]\subset FG(\mathfrak{a})$. Such a group Δ is obtained as follows: let T be a maximal k-split torus in G. Fix an order on X(T) (= group of characters on T) and let U be the unique connected unipotent k-subgroup of G with the span $\mathfrak{u}$ of all the positive k-root-spaces (in the Lie algebra $\mathfrak{g}$ of G) for its Lie algebra. Let β be the highest k-root and $U^{(\beta)}$ the unique connected unipotent k-subgroup with $\mathfrak{g}^{\beta}$ (= k-root space corresponding to β) as the Lie algebra. Then $\Delta = U^{(\beta)}\cap G(A)$ is infinite and we assert that $[G(\mathfrak{a}), \Delta]\subset FG(\mathfrak{a})$. To see this we use the Bruhat decomposition in $G(k)$: let N(T) (resp. Z(T)) be the normaliser (resp. centraliser) of T and W a complete set of representatives for $N(T)/Z(T)$ with $W\subset N(T)(k)$. Let $\pi : N(T)\rightarrow N(T)/Z(T)$ be the natural map. The group $N(T)/Z(T)$ acts on X(T) permuting the k-roots. For $w\in W$, $\alpha\in X(T)$ we write $w(\alpha)$ for $\pi(w)(\alpha)$. Now it is known that each $g\in G(k)$ can be written in the form

$$g = uwzv$$

with $u\in U(k)$, $w\in W$, $z\in Z(T)(k)$ and $v\in U(k)$. If now $x\in U(\beta)$, we see that

$$\begin{aligned} gxg^{-1} &= uwzvxv^{-1}z^{-1}w^{-1}u^{-1} \\ &= uyu^{-1} \end{aligned}$$

where $y\in U^{(w(\beta))}$: this is because Z(T) normalizes and U centralizes $U^{(\beta)}$. Now

$$\lambda = u^{-1}xu\in U^{(\beta)}$$

and

$$u^{-1}(gxg^{-1})u = y\in U^{(w(\beta))}.$$

Since the k-rank of G is ≥ 2, x and y are contained in the same k-QSP: if $w(\beta)$ and β are linearly independent, $U^{(\beta)}$ and $U^{(w(\beta))}$ are both contained in the unipotent radical of some proper k-parabolic subgroup; if $w(\beta) = r\beta$ with $r>0$, the same conclusion holds; if $w(\beta) = -\beta$, $U^{(\beta)}$ and $U^{(w(\beta))} = U^{(-\beta)}$ are contained in a proper k-A-S of G. We see thus in any case, for any $g \in G(k)$ and $x \in U^{(\beta)}$, $gxg^{-1}x^{-1}$ is contained in a proper k-QPS so that

$$[\Delta, G(\mathfrak{a})] \subset FG(\mathfrak{a}).$$

This proves that $G(k)^+$ centralises $CG(f, c)$.

Corollary **(3.3)**. — *Let* $\Gamma = G(k)^+ \cap G(A)$. *Then for every ideal* $\mathfrak{a} \subset A$, $\mathfrak{a} \neq 0$, *we can find a non-zero ideal* $\mathfrak{a}^*$ *such that* $[\Gamma, G(\mathfrak{a}^*)] \subset FG(\mathfrak{a})$.

From Theorem (3.2) we know that Γ centralises $CG(f, c)$. It follows that (taking images in $G(A)/FG(\mathfrak{a})$) $\Gamma FG(\mathfrak{a})/FG(\mathfrak{a})$ commutes with the image of $CG(f, c)$ in $G(A)/FG(\mathfrak{a})$. On the other hand it is an immediate consequence of Lemma (1.24) that we can find an ideal $\mathfrak{a}^* \subset A$, $\mathfrak{a}^* \neq 0$, such that the image of $CG(f, e)$ contains $G(\mathfrak{a}^*)FG(\mathfrak{a})/FG(\mathfrak{a})$. It follows that we have $[\Gamma, G(\mathfrak{a}^*)] \subset FG(\mathfrak{a})$.

(3.4). — The following theorem is due to Kazdan [1] (see also S. P. Wang [1] and Delaroche and Kirillov [1]).

Let k_i, $1 \leq i \leq r$, be local fields, H_i an absolutely almost simple k_i-algebraic group and $H_i(k_i)$ the locally compact group of k_i-rational points of H_i. Let $H = \prod_{i=1}^{r} H_i(k_i)$ and Φ a lattice in H. If k_i-rank$(H_i) \geq 2$, for all i, $1 \leq i \leq r$, Φ is finitely generated and $\Phi/[\Phi, \Phi]$ is finite.

In the references cited above the theorem is not stated explicitly in the case of fields of positive characteristic. However the proofs are valid in the case of positive characteristic as well — at least the proofs as given in the last of the three references. Now according to Harder [1] (also Behr [1]) an S-arithmetic group in G is a lattice in $\prod_{v \in S} G(k_v)$. If k-rank$(G) \geq 2$ we conclude from the theorem above that we have

Proposition **(3.5)**. — *If* $\Phi \subset G$ *is an* S-*arithmetic subgroup and* k-*rank*$(G) \geq 2$, $\Phi/[\Phi, \Phi]$ *is finite.*

Using results of Dieudonné [1, 2] and G. E. Wall [1] it is deduced in Raghunathan [4] that $G(k)/G(k)^+$ is abelian (and finite) if k-rank$(G) \geq 2$. As a consequence we have

Lemma **(3.6)**. — *If* k-*rank*$(G) \geq 2$ *and* Φ *is an* S-*arithmetic subgroup of* G, $\Phi \cap G(k)^+$ *has finite index in* Φ. *In particular* $\Gamma = G(A) \cap G(k)^+$ *has finite index in* $G(A)$.

Corollary (3.3) combined with Lemma (3.6) gives us the following:

Corollary **(3.7)**. — *For every non-zero ideal* $\mathfrak{a} \subset A$, $FG(\mathfrak{a})$ *has finite index in* $G(A)$ (G *is assumed to have* k-*rank* ≥ 2).

The next result is similar to Theorem (3.2).

Theorem **(3.8)**. — *Assume that* k-*rank*$(G) \geq 2$. *Then* $G(k)^+$ *centralises* $CG(e, f)$.

Let P be a proper k-quasi-parabolic subgroup. Let M be a k-admissible subgroup to which P is adapted. Let P^* be the k-parabolic subgroup associated to P and P^{*-} an opposite parabolic group containing M. Let U^+ (resp. U^-) be the unipotent radical of P^* (resp. P^{*-}). Then M normalises U^+ and U^-. It follows that for any non-zero ideal $\mathfrak{a} \subset A$, we have

$$[M(\mathfrak{a}), U^+(A)] \subset U^+(\mathfrak{a}) \subset EG(\mathfrak{a})$$

and

$$[M(\mathfrak{a}), U^-(A)] \subset U^-(\mathfrak{a}) \subset EG(\mathfrak{a}),$$

so that $[M(\mathfrak{a}), \Delta] \subset E(\mathfrak{a})$ and $[M(\mathfrak{a}).E(\mathfrak{a}), \Delta] \subset E(\mathfrak{a})$ where $\Delta =$ subgroup of G(A) generated by $U^{\pm}(A)$. Let $E^*(M(\mathfrak{a})) = M(\mathfrak{a}).E(\mathfrak{a})$ and $DM(\mathfrak{a}) = E^*M(\mathfrak{a})/E(\mathfrak{a})$. The projective limit $\hat{D}(M)$ of the $DM(\mathfrak{a})$ can then be regarded as a subgroup of the projective limit $CG(e,f) = \varprojlim FG(\mathfrak{a})/EG(\mathfrak{a})$. Then from what we have seen above, we conclude that Δ centralises $\hat{D}(M)$. Now it is easy to see that $M(k)$ normalises $\hat{D}(M)$ and that $M(k)^+ \cap \Delta$ intersects every non trivial k-simple component of M in an infinite group. Applying Proposition (3.1) (to these simple components in place of G) we conclude that $M(k)^+$ centralises $\hat{D}(M)$. When M is trivial so is $\hat{D}(M)$. When M is non-trivial, it is not difficult to see that $M(k)^+$ and Δ generate all of $G(k)^+$. We conclude then that $G(k^+)$ commutes with $\hat{D}(M)$ for every k-admissible M. Consider now the image of $\hat{D}(M)$ in $FG(\mathfrak{a})/EG(\mathfrak{a})$. Using the Main Lemma of § 1 applied to M, it is easily seen that this image contains a subgroup of the form $M(\mathfrak{a}').EG(\mathfrak{a})/EG(\mathfrak{a})$, $\mathfrak{a}' = \mathfrak{a}'(M) \neq 0$ depending on $\mathfrak{a}$ and M. It follows then that if we set $\Gamma = G(k)^+ \cap G(A)$, we have

$$[\Gamma, P(\mathfrak{a}'(M))] \subset EG(\mathfrak{a}).$$

Now if we choose a (finite) set $P_1, \ldots, P_n$ of representatives for the G(A)-conjugacy classes of k-QPS, and for each of the P_i a k-admissible subgroup M_i to which P_i is adapted, we can find a single non-zero $\mathfrak{a}' \neq 0$ contained in $\mathfrak{a}$ such that

$$[\Gamma, P_i(\mathfrak{a}')] \subset EG(\mathfrak{a}).$$

Since Γ is normal in G(A) and every k-QSP is conjugate by an element of G(A) to one of the P_i, we conclude that we have

$$(*) \qquad [\Gamma, FG(\mathfrak{a}')] \subset EG(\mathfrak{a}).$$

In the projective limit this implies that Γ centralises $CG(e,f)$. Since Γ is infinite $G(k)^+$ centralises $CG(e,f)$. This proves Theorem (3.8).

Since $\Gamma \cap FG(\mathfrak{a}')$ is an S-arithmetic subgroup for a non-zero ideal $\mathfrak{a}' \subset A$ (Lemma (3.6) and Corollary (3.7)), we conclude from $(*)$ above that we have

Corollary **(3.9)**. — $EG(\mathfrak{a})$ *has finite index in* G(A) *for all non-zero* $\mathfrak{a}$ (*we assume of course that* k-*rank*$(G) \geq 2$).

Combining now this corollary with Theorem (2.1) we have the following:

Theorem **(3.10)**. — *If* k-*rank*$(G) \geq 2$ *every normal subgroup* Φ *in an* S-*arithmetic subgroup* Ψ *is either finite and central in* G *or has finite index in* Φ.

This generalises theorems of Bass-Milnor-Serre [1] and Matsumoto [1] for split groups.

Corollary **(3.11)**. — *The topologies defined by the* $\mathrm{E}(\mathfrak{a})$, $\mathfrak{a}$ *a non-zero ideal in* A, *and the* S-*arithmetic subgroups on* $\mathrm{G}(k)$, *are identical: in other words there is an isomorphism of* $\hat{\mathrm{G}}(e)$ *on* $\hat{\mathrm{G}}(a)$ *inducing the identity on* $\mathrm{G}(k)$. *The group* $\hat{\mathrm{G}}(\mathrm{A}, e)$ *is compact.*

(3.12). — The main problem then is the determination of $\mathrm{CG}(e, c)$. Toward this end we introduce some further notation. Let $\hat{\mathrm{G}}^+(e)$ (resp. $\hat{\mathrm{G}}^+(f)$) denote the closure of $\mathrm{G}(k)^+$ in $\hat{\mathrm{G}}(e)$ (resp. $\hat{\mathrm{G}}(f)$). The closure of $\mathrm{G}(k)^+$ in $\hat{\mathrm{G}}(c)$ is all of $\hat{\mathrm{G}}(c)$. (This follows from Platonov [1] — *viz.* the truth of the Kneser-Tits conjecture for groups over local fields). The density of $\mathrm{G}(k)^+$ in $\hat{\mathrm{G}}(c)$ has the following consequence: $\mathrm{G}(k)^+.\mathrm{G}(\mathrm{A})=\mathrm{G}(k)$. And, as remarked earlier, if G has k-rank≥ 2, $\mathrm{G}(k)/\mathrm{G}(k)^+$ is abelian. Thus we have (see Raghunathan [4]) from Proposition (3.5):

Proposition **(3.13)**. — *If* k-*rank*$(\mathrm{G})\geq 2$, $\mathrm{G}(k)/\mathrm{G}(k)^+$ *is finite (and abelian).*

(3.14). — Consider now the exact sequences

$$(*)\qquad 1\to \mathrm{CG}(e, c)/\mathrm{CG}^+(e, c)\to \hat{\mathrm{G}}(e)/\mathrm{CG}^+(e, c)\to \hat{\mathrm{G}}(c)\to 1$$

and

$$(**)\qquad 1\to \mathrm{CG}^+(e, c)\to \hat{\mathrm{G}}^+(e)\to \hat{\mathrm{G}}(c)\to 1$$

where $\mathrm{CG}^+(e, c)=\mathrm{CG}(e, c)\cap \hat{\mathrm{G}}^+(e)$. The second sequence is exact for the following reason: the closure $\hat{\Gamma}(e)$ of $\mathrm{G}(\mathrm{A})\cap \mathrm{G}(k)^+=\Gamma$ in $\hat{\mathrm{G}}^+(e)$ is an open compact subgroup of $\hat{\mathrm{G}}^+(e)$; the image of $\hat{\Gamma}(e)$ is a closed subgroup of $\hat{\mathrm{G}}(\mathrm{A}, c)$ of finite index and is hence open; it follows that the image of $\hat{\mathrm{G}}^+(e)$ in $\hat{\mathrm{G}}(c)$ is open, hence closed, and contains $\mathrm{G}(k)^+$; in view of the density of $\mathrm{G}(k)^+$ in $\hat{\mathrm{G}}(c)$ the map $\hat{\mathrm{G}}^+(e)\to \hat{\mathrm{G}}(c)$ is surjective. Since $\mathrm{G}(k)/\mathrm{G}(k)^+$ is abelian and finite one sees that $\mathrm{CG}(e, c)/\mathrm{CG}^+(e, c)$ is finite and abelian and that the extension $(*)$ is central. Theorems (3.2) and (3.8) together with the fact that $[\mathrm{G}(k)^+, \mathrm{G}(k)^+]=\mathrm{G}(k^+)$ enable one to conclude that $(**)$ is central as well. Now the group $\mathrm{CG}^+(e, c)$ can be imbedded in yet another exact sequence:

$$(***)\qquad 1\to \mathrm{CG}^+(e, c)\to \hat{\Gamma}(e)\to \hat{\Gamma}(c)\to 1$$

where $\hat{\Gamma}(c)=$ closure of Γ $(=\mathrm{G}(\mathrm{A})\cap \mathrm{G}(k)^+)$ in $\hat{\mathrm{G}}(c)$. To $(**)$ and $(***)$ we can associate cohomology exact sequences, for cohomology groups based on continuous cochains with values in the trivial module $\mathbf{Q}/\mathbf{Z}=\mathrm{I}$. These sequences are:

$$\mathrm{H}(**) : \ \mathrm{Hom}(\hat{\mathrm{G}}^+(e), \mathrm{I}) \to \mathrm{Hom}(\mathrm{CG}^+(e, c), \mathrm{I}) \to \mathrm{H}^2(\hat{\mathrm{G}}(c), \mathrm{I})$$

$$\mathrm{H}(***) : \ \mathrm{Hom}(\hat{\Gamma}(e), \mathrm{I}) \to \mathrm{Hom}(\mathrm{CG}^+(e, c), \mathrm{I}) \to \mathrm{H}^2(\hat{\Gamma}, \mathrm{I}).$$

In fact, since $\mathrm{G}(k)^+$ is its own commutator, we have an injective homomorphism:

$$1 \to \mathrm{Hom}(\mathrm{CG}^+(e, c), \mathrm{I}) \xrightarrow{\alpha} \mathrm{H}^2(\hat{\mathrm{G}}(c), \mathrm{I}).$$

Further, since the sequence (**) splits on the group $G(k)^+$, α maps into the kernel of γ:

$$\gamma : H^2(\hat{G}(c), I) \to H^2(G(k)^+, I).$$

We also know that $\mathrm{Hom}(\hat{\Gamma}(e), I)$ is finite. Finally $\mathrm{Hom}(CG^+(e, c), I)$ is the Pontrjagin dual of the compact abelian group $CG^+(e, c)$. Thus $CG^+(e, c)$ can be recovered from the dual. This discussion is summarised in

Theorem **(3.15)**. — *Assume that k-rank$(G) \geq 2$. Let $\hat{G}^+(e)$ denote the closure of $G(k)^+$ in $\hat{G}(e)$ and $CG(e, c) \cap \hat{G}^+(e) = CG^+(e, c) = C^+$. We have then:*

(i) C/C^+ *is finite and abelian*;

(ii) C^+ *is abelian and compact and central in* $\hat{G}^+(e)$;

(iii) *the Pontrjagin dual* M *of* C^+ *admits an injective homomorphism into the kernel of*

$$\gamma : H^2(\hat{G}(e), I) \to H^2(G(k)^+, I);$$

(iv) *a quotient of* M *by a finite group admits an injection into* $H^2(\hat{\Gamma}(e), I)$ (*where* $\hat{\Gamma}$ = *closure of* Γ $(= G(k)^+ \cap G(A))$ *in* $\hat{G}(c)$).

Theorem (3.15) reduces the problem of computation of $C(e, c)$ (at least qualitatively) to one of computing certain cohomology groups of certain adèle groups. The rest of this paper is devoted to obtaining results on these cohomology groups.

Remarks **(3.16)**. — We have used Kazdan's theorem repeatedly in the discussions above. For certain groups for which the Kneser-Tits conjecture is known to hold it is possible to solve the congruence subgroup problem first and then deduce Kazdan's theorem in those cases. This is notably true for quasi-split groups.

4. Cohomology computations — I (Groups over Local Fields)

Notation **(4.1)**. — Throughout this chapter we adopt the following notation.

L will denote either a locally compact field of positive characteristic or the field $\mathbf{Q}_p$ of p-adic numbers, p a prime in $\mathbf{Z}$.

$\mathfrak{O}$, the ring of integers in L.

$\mathfrak{p}$, the unique prime ideal in $\mathfrak{O}$.

F, the residue field $\mathfrak{O}/\mathfrak{p}$ and

p, the characteristic of F.

$H \subset GL(n)$ a connected simply connected algebraic subgroup defined over L.

$H(L) = H \cap GL(n, L)$, $H(\mathfrak{O}) = H \cap GL(n, \mathfrak{O})$.

$\mathbf{H}$ will denote the group scheme over $\mathfrak{O}$ associated to H nd the incl usion $H \subset GL(n)$.

When the abelian group $I = \mathbf{Q}/\mathbf{Z}$ is treated as a module over a locally compact group, it is always understood that the action is trivial and the topology on I is discrete. Cohomology groups are always based on continuous cochains.

For an integer $i>0$, let $H(i)$ be the subgroup

$$\{x \in H(\mathfrak{O}) \mid x \equiv \text{Identity} \bmod \mathfrak{p}^i\}$$

of $H(\mathfrak{O})$. The following lemma is obvious:

Lemma **(4.2)**. — $H(i)/H(i+1)$, $i \geq 1$, *is a finite abelian p-group. Hence* $H(1)$ *is a pro-p-group.*

Corollary **(4.3)**. — *For* $m \geq 1$, $i \geq 1$, $H^m(H(i), I)$ *is a p-torsion group. The group* $H^m(H(\mathfrak{O}), I)$, $m>1$, *has a p-torsion subgroup of finite index.*

Corollary **(4.4)**. — *If* $H^i(H(\mathfrak{O})/H(1), I)=0$, $H^i(H(\mathfrak{O}), I)$ *is a p-torsion group.*

This follows immediately from the Hochschild-Serre spectral sequence.

Corollary **(4.5)**. — *If* $H^2(H(\mathfrak{O})/H(1), I)=0$, H *is quasi-split over* L *and if characteristic* $L>0$ *the natural map* $H^2(H(L), I) \to H^2(H(\mathfrak{O}), I)$ *is trivial.*

When H is quasi-split, it is known (Moore [1] and Deodhar [1]) that $H^2(H(L), I)$ is a quotient of μ_L = the group of roots of unity in L. Since $|\mu_L|$ is coprime to p Corollary (4.5) follows.

(4.6). — From now we assume that the characteristic of L is zero. Let q be the smallest positive integer such that the exponential series converges on

$$\{x \in M(n, L) \mid x \equiv 0 (\bmod \mathfrak{p}^q)\}.$$

Then $q=1$ if $p \neq 2$ and $q=2$ if $p=2$. Moreover the logarithmic series

$$\ell(x) = \sum_{i=1}^{\infty} (-1)^{i+1} (x-1)^i$$

converges for all $x \in GL(n, \mathfrak{O})$, $x \equiv 1 (\bmod p)$, and provides an inverse for exp on suitable domains. More precisely, let $\mathfrak{h}(L) \subset M(n, L)$ be the Lie subalgebra corresponding to H, $\mathfrak{h}(0) = h(L) \cap M(n, \mathfrak{O})$ and for an integer $i>0$,

$$\mathfrak{h}(i) = \{x \in \mathfrak{h}(\mathfrak{O}) \mid x \equiv 0 \ (\bmod \mathfrak{p}^i)\}.$$

Then $\exp(\mathfrak{h}(i)) \subset H(i)$ for $i \geq q$ and

$$\exp : \mathfrak{h}(i) \to H(i)$$

is a homeomorphism with ℓ for inverse. We denote by ℓ_i the map ℓ restricted to $H(i)$ considered as a map into $\mathfrak{h}(i)$. It is easy to see that we have

$$(*) \qquad \ell_i(x.y) \equiv \ell_i(x) + \ell_i(y) \ (\bmod \mathfrak{h}(2i))$$

for all $i \geq q$. From this it is immediate that for $j \leq i$, we have a continuous group isomorphism

$$(**) \qquad u_{ij} : H(i)/H(i+j) \to \mathfrak{h}(i)/\mathfrak{h}(i+j);$$

also of course, one has (for $i \geq q$),

(***) $$[H(i), H(i)] \subset H(2i).$$

We note that u_{ij} is compatible with the action of $H(0)$ on the two groups. Further the map $x \mapsto p^i x$ obviously gives an isomorphism

$$\mathfrak{h}(\mathfrak{O})/\mathfrak{h}(j) \xrightarrow{\sim} \mathfrak{h}(i)/\mathfrak{h}(i+j), \quad j \leq i, \ i \geq q.$$

In particular as a group $\mathfrak{h}(i)/\mathfrak{h}(i+j)$ is isomorphic to $\dim_L \mathfrak{h}(L)$ copies of $\mathbf{Z}/(p^j)$. This suggests that the discussion below in (4.7) will be useful in our cohomology computations.

(4.7). — Let R be the ring $\mathbf{Z}/(r)$, r some integer. Let M be a finitely generated free R-module. We are interested in the cohomology of the group M with coefficients in I. Let $B(M) = \mathrm{Hom}_{\mathbf{Z}}(M \otimes_{\mathbf{Z}} M, I)$, the group of I-valued bilinear functions on M. One has evidently $B(M) = \mathrm{Hom}_{\mathbf{Z}}(M \otimes_{\mathbf{Z}} M, R)$. Since any bilinear function is a 2-cocycle we get an inclusion

$$B(M) \rightarrow Z^2(M, I)$$

where $Z^2(M, I) =$ group of I-valued 2-cocycles on M, and hence a homomorphism

$$\tilde{\psi} : B(M) \rightarrow H^2(M, I).$$

It is easily seen that kernel $(\tilde{\psi})$ is precisely $S(M)$, the subgroup of *symmetric* bilinear functions on M, leading to an injective homomorphism

$$\psi : B(M)/S(M) \rightarrow H^2(M, I).$$

Lemma **(4.8).** — *ψ is an isomorphism. Also* $H^1(M, I) \cong \mathrm{Hom}_{\mathbf{Z}}(M, I)$. *These isomorphisms are moreover compatible with the action of* $\mathrm{Aut}(M)$ *on the various groups involved.*

The first assertion is proved by induction on the rank of M as an R-module: one need only show that the two groups (which are finite: note that $H^2(M, I) \cong H^3(M, \mathbf{Z})$) have the same cardinality. This is easily done using the Hochschild-Serre spectral sequence.

We will next establish

Lemma **(4.9).** — *Let* $U \subset H(\mathfrak{O})$ *be a compact open subgroup. Let* $E = \mathrm{Hom}_{\mathfrak{O}}(\mathfrak{h}(\mathfrak{O}), \mathfrak{O})$, $B = \mathrm{Hom}_{\mathfrak{O}}(\mathfrak{h}(\mathfrak{O}) \otimes_{\mathfrak{O}} \mathfrak{h}(\mathfrak{O}), \mathfrak{O})$ *and* $S \subset B$ *the subgroup of symmetric forms. Let* $F = B/S$. *Then there exists a subgroup* $\Gamma \subset U$ *with the following properties:*

a) Γ *is finitely generated;*
b) Γ *is dense in* U;
c) $H^i(\Gamma, E \oplus F)$ *is finitely generated as a* $\mathfrak{O}$*-module for* $i = 1, 2$;
d) $H^1(\Gamma, E)$ *is finite (hence a p-torsion group).*

($U \subset H(\mathfrak{O})$ *has a natural action on* E *and* F; *the cohomology groups are for this action;* Γ *is given the discrete topology.*)

It is easily seen that the problem can be reduced to the case when H is simple over L. In this case we can find a finite extension L′ of L and an absolutely simple group H′ over L′ such that H is L-isomorphic to $R_{L'/L}(H')$. If $\mathfrak{O}' \subset L'$ is the ring of integers we have a natural isomorphism

$$H'(\mathfrak{O}') \cong H(\mathfrak{O}).$$

Now according to the main result in Appendix III we can find a number field $k' \subset L'$ such that k' is dense in L′ and H′ is L′-isomorphic to a group over k'. In other words, we may assume that H′ is defined over k'. Enlarging k' if necessary we may assume the following:

k' admits two distinct archimedean valuations v_1, v_2 such that the completions k'_i of k with respect to v_i are both isomorphic to **C**.

This has the following implication: if $D = R_{k'/\mathbf{Q}}(H')$, D is simple over **Q** and R-rank$(D) \geq 2$. Evidently,

$$D(\mathbf{R}) = \prod_{v \in \infty} H'(k'_v)$$

where ∞ is the set of archimedean valuations of k' and, for $v \in \infty$, k'_v is the completion of k' with respect to v. Let $\mathfrak{h}$ (resp. $\mathfrak{h}'$, $\mathfrak{d}$) be the Lie algebra of H (resp. H′, D). One has then natural identifications

$$\mathfrak{h}(\mathfrak{O}) \overset{\alpha}{\cong} \mathfrak{h}'(\mathfrak{O}') \overset{\beta}{\cong} \mathfrak{h}'(\mathfrak{O}(k') \otimes_{\mathfrak{O}(k')} \mathfrak{O}')$$
$$\mathfrak{h}'(\mathfrak{O}(k')) \overset{\gamma}{\cong} \mathfrak{d}(\mathbf{Z})$$

here α is $\mathfrak{O}$-linear, β is $\mathfrak{O}'$-linear and γ, **Z**-linear.

Now since $D(\mathbf{R})$ is non-compact we can choose, using strong approximation, an arithmetic subgroup $\Gamma \subset D(\mathbf{Z})$ which is dense in U (cf. Platonov [1]). On the other hand, the $H^i(\Gamma, E \oplus F)$ are finitely generated $\mathfrak{O}$-modules since E and F are finitely generated $\mathfrak{O}$-modules (Raghunathan [5] or Serre [3]). In view of the isomorphisms α, β, γ above, to prove the lemma we have only to show that

$$H^1(\Gamma, \mathfrak{d}) = 0$$

for the above choice of Γ.

If D has **Q**-rank>0, this follows from the main results of Raghunathan [1, 2]. If D is anisotropic over **Q**, this follows from a theorem due to Weil (see for instance Raghunathan [3, Ch. VII, § 5]). One has to note in the last case that $D(\mathbf{R})$ may have compact factors but the action of Γ on the various factors of $\mathfrak{d}$ over **C** are equivalent under Galois automorphisms.

This completes the proof of Lemma (4.9).

Theorem **(4.10)**. — *Let* $U \subset H(L)$ *be a compact open subgroup. Then the groups* $H^q(U, \mathbf{1})$ *are finite for* $q = 1, 2$.

The proof yields rather more precise information which is needed in the sequel. We formulate therefore a more technical version of the theorem for convenient future use.

Proposition **(4.11).** — *Let* $U \subset H(L)$ *be a compact open subgroup. Assume that* $U \subset H(\mathfrak{O})$. *Let* $m \geq 0$ *be an integer such that* $H(m) \subset U$. *If* $p=2$ *assume that* $m \geq 2$. *Let* $\Gamma \subset U$ *be chosen as in Lemma* (4.9). *Let* p^a *be the smallest power of* p *that annihilates the (p-) torsion in* $H^1(\Gamma, E \oplus F) \oplus H^2(\Gamma, E)$. *Then the natural map*

$$H^\ell(U/H(m+3a+1), I) \to H^\ell(U, I)$$

is surjective for $\ell = 1, 2$.

Note that since $U/H(m+3a+1)$ is finite the group $H^\ell(U/H(m+3a+1), I)$ is finite. By definition $H^\ell(U, I)$ is the inductive limit of the groups $H^\ell(U/H(r), I)$ as r goes to ∞. It follows that if $a>0$, Proposition (4.11) is a consequence of

Assertion **(4.12).** — Assume that $a>0$. Let i be any integer greater than or equal to $m+3a+1$. Then the groups $H^\ell(U/H(i+3a), I)$ and $H^\ell(U/H(i+4a), I)$ have the same image in $H^\ell(U/H(i+5a), I)$.

(4.13). — The proof is a result of a careful examination of the Hochschild-Serre spectral sequences associated to the following pairs:

$$(U/H(i+4a), H(i+ta)/H(i+4a)), \quad 1 \leq t \leq 3,$$

and

$$(U/H(i+5a), H(i+3a)/H(i+5a)).$$

We denote these spectral sequences by ${}_tE_r^{pq}$, $1 \leq t \leq 3$, and E_r^{pq} respectively. We discuss the case $\ell = 2$ in detail. The arguments for $\ell = 1$ are analogous and simpler. Let $\Gamma(j) = \Gamma \cap H(j)$ (j an integer). Then $\Gamma(j)$ is dense in $H(j)$ for $j \geq m$ and the maps

$$u_{jj'} : H(j)/H(j+j') \to \mathfrak{h}(j)/\mathfrak{h}(j+j')$$

introduced in (4.6) induce isomorphisms of $\Gamma(j)/\Gamma(j+j')$ on $\mathfrak{h}(j)/\mathfrak{h}(j+j')$ as well. The inclusions

$$H(i+3a) \hookrightarrow H(i+2a) \hookrightarrow H(i+a)$$

induce homomorphisms

$${}_1E_r^{pq} \xrightarrow{{}_{12}\varphi(p,q)_r} {}_2E_r^{pq}$$

$${}_2E_r^{pq} \xrightarrow{{}_{23}\varphi(p,q)_r} {}_3E_r^{pq}$$

of spectral sequences. All the three spectral sequence ${}_tE_r$ converge to the same limit *viz.* $H^*(U/H(i+4a), I)$. The E_2 terms relevant to the second cohomology can be described in the following manner: consider first ${}_1E$:

$${}_1E_2^{02} = H^0(U/H(i+a), H^2(H(i+a)/H(i+4a), I))$$
$${}_1E_2^{11} = H^1(U/H(i+a), H^1(H(i+a)/H(i+4a), I))$$
$${}_1E_2^{20} = H^2(U/H(i+a), I).$$

The discussion in (4.7) shows that we have natural isomorphisms (note that $i \geq 3a$)

$$(*) \qquad \begin{aligned} {}_1E_2^{02} &\cong H^0(U/H(i+a), F/p^{3a}F) \\ {}_1E_2^{11} &\cong H^1(U/H(i+a), E/p^{3a}E). \end{aligned}$$

Entirely analogously, one has the following isomorphisms:

$$(*) \qquad \begin{aligned} {}_2E_2^{02} &\cong H^0(U/H(i+2a), F/p^{2a}F) \\ {}_2E_2^{11} &\cong H^1(U/H(i+2a), E/p^{2a}E) \\ {}_3E_2^{02} &\cong H^0(U/H(i+3a), F/p^{2a}F) \\ {}_3E_2^{11} &\cong H^1(U/H(i+3a), E/p^{a}E). \end{aligned}$$

Claim (4.14). — ${}_{12}\varphi(0, 2)_2$ is the trivial map.

Let $\pi : F/p^{3a}F \to F/p^{2a}F$ be the natural surjection and

$$\pi^* : H^0(U/H(i+a), F/p^{3a}F) \to H^0(U/H(i+a), F/p^{2a}F)$$

the induced map. Using the identifications $(*)$ it is easily seen that ${}_{12}\varphi(0, 2)_2$ is the composite of the map $H^0(U/H(i+a), F/p^{2a}F) \to H^0(U/H(i+2a), F/p^{2a}F)$ and π^*. The map π imbeds in the following commutative diagram with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & F \arrow[r, "p^{2a}"] & F \arrow[r] & F/p^{2a}F \arrow[r] & 0 \\ 0 \arrow[r] & F \arrow[r, "p^{3a}"] \arrow[u, "p^a"] & F \arrow[r] \arrow[u, "\wr"'] & F/p^{3a}F \arrow[r] \arrow[u, "\pi"] & 0 \end{tikzcd}$$

Considering these as Γ-modules, we get the exact sequences

$$\begin{tikzcd} 0 = H^0(\Gamma, F) \arrow[r] & H^0(\Gamma, F/p^{2a}F) \arrow[r] & H^1(\Gamma, F) \arrow[r, "p^{2a}"] & H^1(\Gamma, F) \ldots \\ 0 = H^0(\Gamma, F) \arrow[r] & H^0(\Gamma, F/p^{3a}F) \arrow[r] \arrow[u, "\pi^*(\Gamma)"] & H^1(\Gamma, F) \arrow[r, "p^{3a}"] \arrow[u, "p^a"'] & H^1(\Gamma, F) \ldots \end{tikzcd}$$

in cohomology. The groups at the left end are zero because of the Zariski density of Γ in H. Since p^a annihilates the torsion in $H^1(\Gamma, F)$, both the left end maps have precisely the torsion in $H^1(\Gamma, F)$ as their kernel; and multiplication by p^a annihilates this kernel. This shows that $\pi^*(\Gamma)$ is trivial. Since the natural maps

$$H^0(U/H(i+a), F/p^{3a}F) \xrightarrow{\cong} H^0(\Gamma/\Gamma(i+a), F/p^{3a}F) \to H^0(\Gamma, F/p^{3a}F)$$

and $\qquad H^0(U/H(i+2a), F/p^{2a}F) \to H^0(\Gamma, F/p^{2a}F)$

are isomorphisms, π^* is trivial.

(4.15). — The claim shows that the filtration on H^2 associated to the spectral sequence ${}_2E$ is in fact a 2-step one, the term ${}_2E_2^{02}$ making no contribution to the cohomology. Our next task is to analyse ${}_{23}\varphi(1, 1)_2$. This is a little more delicate than what we have done above. We introduce a 2-step filtration on ${}_2E_2^{11}$ and ${}_3E_2^{11}$ as follows: consider the commutative diagram (with exact rows):

$$\begin{tikzcd} 0 \arrow[r] & E \arrow[r, "p^{2a}"] \arrow[d, "p^a"'] & E \arrow[r] \arrow[d, "\wr"] & E/p^{2a}E \arrow[r] \arrow[d, "\pi"] & 0 \\ 0 \arrow[r] & E \arrow[r, "p^a"] & E \arrow[r] & E/p^aE \arrow[r] & 0 \end{tikzcd}$$

Passing to cohomology, we have the following commutative diagram with exact rows:

$$\begin{tikzcd} H^1(\Gamma, E) \arrow[r] \arrow[d, phantom, "\wr"] & H^1(\Gamma, E/p^{2a}E) \arrow[r] \arrow[d, "\pi^*(\Gamma)"'] & H^2(\Gamma, E) \arrow[r, "p^{2a}"] \arrow[d, "p^a"] & H^2(\Gamma, E) \arrow[d, phantom, "\wr"] \\ H^1(\Gamma, E) \arrow[r] & H^1(\Gamma, E/p^aE) \arrow[r] & H^2(\Gamma, E) \arrow[r, "p^a"] & H^2(\Gamma, E) \end{tikzcd}$$

Now the natural maps

$$H^1(U/H(i+2a), E/p^{2a}E) \to H^1(\Gamma, E/p^{2a}E)$$

and

$$H^1(U/H(i+3a), E/p^aE) \to H^1(\Gamma, E/p^aE)$$

are easily seen to be injective. We may thus identify ${}_2E_2^{11}$ and ${}_3E_2^{11}$ as subgroups of $H^1(\Gamma, E/p^{2a}E)$ and $H^1(\Gamma, E/p^aE)$ respectively. Let ${}_tE_{2*}^{11} = {}_tE_2^{11} \cap \text{Image } H^1(\Gamma, E)$. Now the maps at the right end of both the rows above have the same kernel *viz.* the (p-) torsion in $H^2(\Gamma, E)$. The vertical map is clearly trivial on this kernel. It follows that $\pi^*(\Gamma)$ maps $H^1(\Gamma, E/p^{2a}E)$ into the image of $H^1(\Gamma, E)$. This means that

$${}_{23}\varphi(1, 1)_2({}_2E_2^{11}) \subset {}_3E_{2*}^{11}.$$

This discussion shows that the essential information about H^2 in the spectral sequence ${}_3E$ is contained in ${}_3E_2^{20} \oplus {}_3E_{2*}^{11}$.

(4.16). — We are now in the final stage of the proof of the assertion. We examine the map ${}_3E_r \to E_r$. (This is somewhat different from the earlier situation: the " big " groups are now different.) As before, we have identifications

$$E_2^{11} \cong H^1(U/H(i+3a), E/p^{2a}E), \text{ etc.}$$

The map $\varphi : {}_3E_2^{11} \to E_2^{11}$ is the map

$$H^1(U/H(i+3a), E/p^aE) \xrightarrow{\alpha^*} H^1(U/H(i+3a), E/p^{2a}E)$$

induced by the natural inclusion $E/p^a E \to E/p^{2a}E$. Now α is imbedded in the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E & \xrightarrow{p^a} & E & \longrightarrow & E/p^a E & \longrightarrow & 0 \\ & & \wr\| & & \downarrow{\scriptstyle p^a} & & \downarrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & E & \xrightarrow{p^{2a}} & E & \longrightarrow & E/p^{2a}E & \longrightarrow & 0 \end{array}$$

Now consider the induced cohomology sequence (for Γ)

$$\begin{array}{ccccccc} H^1(\Gamma, E) & \longrightarrow & H^1(\Gamma, E/p^a E) & \longrightarrow & H^2(\Gamma, E) & \xrightarrow{p^a} & H^2(\Gamma, E) \\ \downarrow{\scriptstyle p^a} & & \downarrow{\scriptstyle \alpha^*(\Gamma)} & & \downarrow{\wr} & & \downarrow{\scriptstyle p^a} \\ H^1(\Gamma, E) & \longrightarrow & H^1(\Gamma, E/p^{2a}E) & \longrightarrow & H^2(\Gamma, E) & \xrightarrow{p^{2a}} & H^2(\Gamma, E) \end{array}$$

This diagram shows that $\alpha^*(\Gamma)$ maps image of $H^1(\Gamma, E)$ (in $H^1(\Gamma, E/p^a E)$) into zero. The diagram

$$\begin{array}{ccc} H^1(U/H(i+3a), E/p^a E) & \xrightarrow{\alpha^*} & H^1(U/H(i+3a), E/p^{2a}E) \\ \downarrow & & \downarrow \\ H^1(\Gamma, E/p^a E) & \xrightarrow{\alpha^*(\Gamma)} & H^1(\Gamma, E/p^{2a}E) \end{array}$$

is commutative. The vertical maps, as was remarked earlier, are easily seen to be injective. It follows from this that φ maps ${}_3E^{11}_{2*}$ into zero. This shows that the second cohomology group $H^2(U/H(i+4a), I)$ maps into the first stage of the filtration of $H^2(U/H(i+5a), I)$ given by the normal subgroup $H(i+3a)/H(i+5a)$. But this is nothing but the image of $H^2(U/H(i+3a), I)$ in $H^2(U/H(i+5a), I)$. This completes the proof of Assertion (4.12) in case $a>0$.

(4.17). — We now consider the case $a=0$. The arguments here are in fact much simpler. Fix $i \geq m$ and consider the spectral sequence associated to the pair $(U/H(i), U/H(i+1))$. As in (4.13), we have the following isomorphisms:

$$E_2^{01} \simeq H^0(U/H(i), E/pE), \qquad E_2^{02} \simeq H^0(U/H(i), F/pF)$$

and $$E_2^{11} \simeq H^1(U/H(i), E/pE).$$

It suffices to show that these groups are trivial. This follows from the exact cohomology sequences (for the group Γ) associated to

$$0 \to E \xrightarrow{p} E \to E/pE \to 0$$

and $$0 \to F \xrightarrow{p} F \to F/pF \to 0,$$

since $H^1(\Gamma, E\oplus F)$ and $H^2(\Gamma, E)$ have no (p-) torsion. This completes the proof of assertion (4.12).

Remark **(4.18)**. — Let B be a simply connected semisimple algebraic group over *any* local field K of characteristic o. Then $B(K)$ is isomorphic as a locally compact group to $R_{K/\mathbf{Q}_p}(B)(\mathbf{Q}_p)$ where $\mathbf{Q}_p$ is the field of p-adic numbers contained in K ($\mathbf{Q}_p$ is the closure of $\mathbf{Q}$ in K). It follows from Theorem (4.10) that if $M \subset B(K)$ is a compact open subgroup of $B(K)$, $H^i(M, I)$ is finite for $i=1, 2$.

5. Cohomology Computations — II (Adelic Groups).

(5.1). — We revert to the notations of §§ 1-3 now. Thus k is a global field and $G \subset GL(n)$ is a k-algebraic subgroup which is k-simple and simply connected. For technical reasons, *we do allow* G *to be not necessarily absolutely simple when k is of characteristic* o. *When k has positive characteristic* G *is assumed to be absolutely simple.* Except for this provision, the notations are as explained in § (1.1). We make one further hypothesis on G: G *has strong approximation, i.e.* for any finite set S of valuations of k with $\prod_{v\in S} G(k_v)$ non-compact, $G(k)$ is dense in the S-adèle group $G(\mathbf{A}(S))$ (=the restricted product $\prod_{v\notin S} G(k_v)$). When k is a number field, this is known to be true for all G (Platonov [1]; earlier work of Kneser covers all classical cases). When k is of positive characteristic, it is not known whether strong approximation holds in general. However if k-rank$(G)\geq 1$, strong approximation does indeed hold for G. This follows from strong approximation for connected unipotent groups combined with the truth of the Kneser-Tits conjecture for local fields. (Platonov [1]: Platonov's methods work equally well for the proof of the Kneser-Tits conjecture for all local fields though his proof of strong approximation cannot be carried over to the case of positive characteristic.)

As in § (1.1), V will denote the set of valuations of k and for a finite subset $S \subset V$, $\infty \subset S$, $A(S)$ will denote the ring of S-integers in k (we will have to consider more than one finite set of valuations at the same time so it is necessary to indicate clearly dependence on S). For S as above, $\mathbf{A}(S)$ will denote the S-adèles of k and $G(\mathbf{A}(S))$ the corresponding adèle group associated to G. For $S' \supset S \supset \infty$, S' finite, $\pi(S, S') : G(\mathbf{A}(S)) \to G(\mathbf{A}(S'))$ will denote the natural map. Our main result in this section can now be stated.

Theorem **(5.2)**. — *Let* U *be a compact open subgroup of* $G(\mathbf{A}(S))$ ($S \supset \infty$, *any finite subset of* V). *Then*:

(i) *If the characteristic p of k is positive,* $H^j(U, I)$, $j=1$ *or* 2, *is a torsion group in which the p-torsion subgroup has finite index. Also, there exists a finite subset* $S_1 = S_1(U)$ *such that for all* $S' \supset S \cup S_1$, $H^i(\pi(S, S')U, I)$, *for* $i=1, 2$, *is a p-torsion group.*

(ii) *Assume that characteristic* $k=0$. *Then* $H^j(U, I)$, $j=1, 2$, *are finite. Also, there exists a finite subset* $S_1 = S_1(U)$ *of* V *such that for all finite* $S' \supset S \cup S_1$, $H^j(\pi(S, S')(U), I) = 0$ *for* $j=1, 2$.

(5.3). — We want to apply the results of § 4 to obtain this theorem. However the results we need from § 4 in the case of characteristic 0 are valid as they stand only for completions of $\mathbf{Q}$. Because of this we need to make a preliminary reduction (when k has characteristic 0). Let $\mathrm{H}=\mathrm{R}_{k/\mathbf{Q}}\mathrm{G}$. Then H is a simply connected semisimple group defined and simple over $\mathbf{Q}$. Let S be as in Theorem (5.2), let S^* be the set of valuations of $\mathbf{Q}$ lying below S, and $\widetilde{\mathrm{S}}$ the set of all valuations lying over S^*. Then one has a natural identification (as locally compact groups) of $\mathrm{G}(\mathbf{A}(\widetilde{\mathrm{S}}))$ and $\mathrm{H}(\mathbf{A}(\mathrm{S}^*))$. On the other hand $\mathrm{G}(\mathbf{A}(\mathrm{S}))\cong(\prod_{v\in\widetilde{\mathrm{S}}-\mathrm{S}}\mathrm{G}_v)\times\mathrm{G}(\mathbf{A}(\widetilde{\mathrm{S}}))$. It follows that U contains a subgroup of finite index of the form $(\prod_{v\in\widetilde{\mathrm{S}}-\mathrm{S}}\mathrm{M}_v)\times\mathrm{U}_1$ where each M_v, $v\in\widetilde{\mathrm{S}}-\mathrm{S}$, is a compact open subgroup of G_v and U_1 is a compact open subgroup of $\mathrm{G}(\mathbf{A}(\widetilde{\mathrm{S}}))$. Now from the results of Chapter 4, we know that $\mathrm{H}^2(\mathrm{M}_v,\mathrm{I})$ and $\mathrm{H}^1(\mathrm{M}_v,\mathrm{I})$ are finite (Remark (4.17)). Using the Künneth formula, one sees that the finiteness of $\mathrm{H}^2(\mathrm{U},\mathrm{I})$ is equivalent to that of the finiteness of $\mathrm{H}^2(\mathrm{U}_1,\mathrm{I})$. Next we can find a finite subset $\mathrm{S}_1^*\supset\mathrm{S}^*$ of valuations on $\mathbf{Q}$ with the following property: let $\widetilde{\mathrm{S}}_1$ be the set of valuations of k lying over S_1^*; then $\pi(\mathrm{S},\widetilde{\mathrm{S}}_1)(\mathrm{U})=\pi(\widetilde{\mathrm{S}},\widetilde{\mathrm{S}}_1)(\mathrm{U}_1)$ decomposes into a direct product of the form $\prod_{v\notin\widetilde{\mathrm{S}}_1}\mathrm{M}_v$, each M_v being a compact open subgroup of G_v. Further, if U_2 is considered as a subgroup of $\mathrm{H}(\mathbf{A}(\mathrm{S}^*))$, $\pi(\mathrm{S}^*,\mathrm{S}_1^*)(\mathrm{U}_1)$ decomposes also as a product $\prod_{w\notin\mathrm{S}_1^*}\mathrm{B}_w$ (w valuations of $\mathbf{Q}$), each B_w being compact and open in H_w; moreover, for a valuation w of $\mathbf{Q}$, if $\widetilde{w}$ denotes the set of all valuations of k lying over w, we have a natural isomorphism $\prod_{v\in\widetilde{w}}\mathrm{M}_v\xrightarrow{\sim}\mathrm{B}_w$ for $w\notin\mathrm{S}_1^*$. Appealing again to the Künneth relations (for the product decomposition of the B_w) one sees that the second assertions (of Part (ii)) in Theorem (5.2) need also be proved only in the case $k=\mathbf{Q}$. This shows that for proving the Main Theorem we may assume that if k is of characteristic 0, k is the rational number field $\mathbf{Q}$.

We will now establish the following consequence of strong approximation (Platonov [1]; actually Platonov [2] has essentially proved the proposition; the proof below is a variant).

Proposition **(5.4).** — *We take k to be* any *global field (we do not assume that k is necessarily $\mathbf{Q}$ when the characteristic is zero). Let* U *be a compact open subgroup of* $\mathrm{G}(\mathbf{A}(\mathrm{S}))$. *Then* U *contains an open subgroup of finite index of the form* $\prod_{v\notin\mathrm{S}}\mathrm{M}_v$, *where each* M_v *is compact open in* G_v *and for almost all v,* $\mathrm{M}_v=\mathrm{G}(\mathfrak{O}_v)$ *is a maximal compact subgroup of* G_v. *Moreover,* $\mathrm{U}\cap\mathrm{G}(k)$ *is an* S*-arithmetic subgroup of* $\mathrm{G}(k)$. *Further, if* $\Gamma\subset\mathrm{G}(k)$ *is an* S*-arithmetic subgroup, then either* Γ *is finite or the closure of* Γ *is open (and compact) in* $\mathrm{G}(\mathbf{A}(\mathrm{S}))$.

That U contains a subgroup of finite index of the form $\prod_{v\notin\mathrm{S}}\mathrm{M}_v$ with M_v open and compact in G_v and M_v, $\mathrm{M}_v=\mathrm{G}(\mathfrak{O}_v)$ for almost all v is immediate from the definition of the adèle topology. Since the first assertion concerns only almost all v, we may without loss of generality assume that $\mathrm{G}(\mathrm{A}(\mathrm{S}))$ *is infinite*. Let M_v^* be a maximal compact subgroup of G_v containing M_v. Then $\mathrm{M}_v^*/(\mathrm{M}_v\cap\mathrm{G}(\mathfrak{O}_v))$ is *finite* for all $v\notin\mathrm{S}$. It follows that if $U^* = \prod_{v \notin S} M_v^*$ and $x \in U^* \cap G(k)$, then the eigen-values of x are v-adic integers for all $v \notin S$. Let $P_\ell : G \to \Omega$ (=universal domain), $1 \leq \ell \leq n$, denote the ℓ-th coefficient of the characteristic polynomial. Then P_ℓ is a k-regular function on G and $P_\ell(x) \in k$ for all $x \in \Gamma^* = U^* \cap G(k)$. Now let R(G) denote the algebra of regular functions on G and $E \subset R(G)$ the smallest Ω-subspace which contains the P_ℓ and is stable under the left regular action of G. Then E is a k-subspace of R(G) and the representation σ of G on E is defined over k. Now, let $\mathscr{L} \subset E$ be the A(S)-linear span of

$$\{\sigma(\gamma)P_\ell \mid \gamma \in \Gamma^*, 1 \leq \ell \leq n\}.$$

$\mathscr{L}$ spans E over Ω — this follows from the Zariski density of Γ^* in G; and Γ^* is Zariski dense in G since Γ^* is dense in U^* (strong approximation: note our hypothesis that $G(\mathbf{A}(S))$ is infinite.) On the other hand, since $P_\ell(\Gamma^*) \subset A(S)$ for $1 \leq \ell \leq n$, $f(\Gamma^*) \subset A(S)$ for all $f \in \mathscr{L}$. It follows that $\mathscr{L}$ is a finitely generated A(S)-module. Consequently $\sigma(\Gamma^*)$ is contained in an S-arithmetic subgroup of $\sigma(G)$. On the other hand since G is k-simple and σ is defined over k, σ is an isogeny. Hence if $\Phi \subset \sigma(G)$ is an S-arithmetic subgroup, $\sigma^{-1}(\Phi) \cap G(k)$ is commensurable with G(A(S)) (Behr [1], Harder [1]). It follows that $\Gamma^* \cap G(A(S))$ has finite index in Γ^*. Now the closure of G(A(S)) is contained in $\prod_{v \notin S} G(\mathfrak{O}_v) = U'$, say. We see thus (since $\Gamma^*/(\Gamma^* \cap G(A(S)))$ is finite) that $U^*/(U^* \cap U')$ is finite. But this means that $M_v^* = G(\mathfrak{O}_v) = M_v$ for almost all v. We conclude therefore also that $G(A(S))/(\Gamma^* \cap G(A(S)))$ is finite as well, *i.e.* Γ^* is arithmetic. The argument given above shows the following. Let $\Psi = G(k) \cap \prod_{v \notin S} G(\mathfrak{O}_v)$. Then Ψ is dense in $U^* = \prod_{v \notin S} G(\mathfrak{O}_v)$ and $\Psi/G(A(S))$ is finite. Since U^* is open and the closure $\hat{\Gamma}'$ of $\Gamma \cap \Psi$ has finite index in U^*, $\hat{\Gamma}$ is open.

Lemma (5.5). — *Let* G *be as above. Then there exists a finite subset* $S_0 \subset V$, $S_0 \supset \infty$, *such that for any* S_0*-arithmetic subgroup* Φ *of* G, $\Phi/[\Phi, \Phi]$ *is finite.*

We give the proofs for positive and zero characteristics separately.

(5.6) *Case A* (Characteristic $k = p > 0$). — We have assumed in this case that G is absolutely simple. If the absolute rank of G is 1, G is isomorphic over k to SL(2) or the group of norm 1 elements in a division algebra over k. In the former case we can choose any S_0 with $|S_0| \geq 2$ (Serre [1]). In the second case we have to choose S_0 with $|S_0| \geq 2$ and G split over k_v for all $v \in S_0$. That $\Phi/[\Phi, \Phi]$ is finite for an S_0-arithmetic Φ follows from Kazdan-Bernstein [1]. Next, if G has absolute rank ≥ 2, we claim that there exists v with k_v-rank(G) ≥ 2. If this claim is granted, the result follows from Kazdan [1]. To prove the claim we observe first that since G is quasi-split for almost all v, the relation k_v-rank(G) ≤ 1 for all v would imply that G is isomorphic to SL(3) over the algebraic closure, and then that G is either an anisotropic or a quasi-split not split form of SL(3) over k. This means that G is either one of the following two kinds of groups: *a)* the group of norm 1 elements in a division algebra of degree 3 over k or *b)* the special unitary group $SU(f)$ of a hermitian quadratic form f in 3 variables over a quadratic extension k' of k. In the former case, for almost all v, G is k_v-split, a contradiction. In the second case, one can find infinitely many v such that k' is isomorphic to a subfield of k_v. For any such k_v, G is k_v-split, hence of k_v-rank $=2$, a contradiction.

(5.7) *Case B* (Characteristic of $k=0$). — If G is anisotropic over k we choose S_0 such that $|S_0|\geq 2$ for all $v\in S_0$; G is non-compact. That S_0 has the required property follows from Kazdan-Bernstein [1]. When G has k-rank 1, choose any S_0 with $|S_0|\geq 2$: this follows from Margulis [1] (which generalises the theorem of Kazdan-Bernstein cited). If k-rank$(G)\geq 2$ we can take $S_0=\infty$: this follows from Kazdan [1].

Corollary **(5.8)**. — *The notations are as in Proposition* (5.4). *Then, for almost all v,* $[M_v, M_v]=M_v$.

This follows from Lemma (5.5) and Proposition (5.4) (applied to $S=S_0$ and $\Gamma=[\Phi,\Phi]$).

In the case of characteristic 0, we also need the following:

Lemma **(5.9)**. — *Assume that characteristic $k=0$. Let $\mathfrak{g}(k)\subset M(n,k)$ denote the Lie algebra corresponding to* G. *Assume that* G *has no absolutely simple factor of rank* 1. *Then there exists a finite set $S_0\subset V$, $\infty\subset S_0$, with the following property. For any S_0-arithmetic subgroup $\Phi\subset G$, $H^1(\Phi,\mathfrak{g}(k))=0$ (where $\mathfrak{g}(k)$ is considered as a Φ-module via the adjoint representation).*

Note that if G has one absolutely simple factor of rank 1, all the absolutely simple factors are of rank 1. Assume first that $G(\infty)$ is compact. The group G is of the form $R_{k'/k}H$ where H is absolutely simple. If $G(\infty)$ is compact, so is $H(\infty)$, H being absolutely simple and of absolute rank ≥ 2, we can argue as in (5.6) to conclude that there is a valuation v' of k' such that $k'_{v'}$-rank$(H)\geq 2$. Now, according to S. P. Wang [2], $H^1(\Psi,\mathfrak{g}(k))=0$ for any $\{v'\}$-arithmetic subgroup Ψ of $H(k')=G(k)$. (Since $H(\infty)$ is compact, the adjoint action is equivalent to a unitary action.) Let v be the valuation of k lying under v'. Then, for any v-arithmetic group Φ, $H^1(\Phi,\mathfrak{g}(k))=0$. To see this observe first that any 1-cocycle of Φ is cohomologous to one f which is trivial on a v'-arithmetic subgroup Ψ of Φ. Now if $\alpha\in\Phi$, and $x\in\Psi$ is chosen such that $\alpha x\alpha^{-1}\in\Psi$, then we have

$$\begin{aligned} 0&=f(\alpha x\alpha^{-1})=f(\alpha)+\mathrm{Ad}\,\alpha f(x)+\mathrm{Ad}\,\alpha\,\mathrm{Ad}\,xf(\alpha^{-1})\\ &=f(\alpha)-\mathrm{Ad}(\alpha x\alpha^{-1})f(\alpha);\end{aligned}$$

this means that $f(\alpha)$ is invariant under all of $\{x\in\Psi\mid\alpha x\alpha^{-1}\in\Psi\}$. But this last set is Zariski dense in G, so that $f(\alpha)=0$. This proves that $H^1(\Phi,\mathfrak{g}(k))=0$. Next, if $G(\infty)$ is not compact, $H^1(\Phi,\mathfrak{g}(k))=0$ according to a theorem of Weil (see Raghunathan [3, Ch. VII, § 5]) and results of Raghunathan [1, 2] for any $\{\infty\}$-arithmetic group Φ.

We will be needing the following in the sequel.

Lemma **(5.10)**. — *For almost all v,* $H^i(G(\mathfrak{O}_v)/G(\mathfrak{p}_v), I)=0$ *for* $i=1, 2$.

This follows from the work of Steinberg [1] and Deodhar [1]. For almost all v, reduction mod $\mathfrak{p}_v$ of G is a simply connected semisimple algebraic group over the residue field F_v and $G(\mathfrak{O}_v)/G(\mathfrak{p}_v)$ is isomorphic to the rational points of this group over the field F_v. Since F_v is finite, this group is quasi-split and the theorems of Steinberg (and Deodhar) apply.

Lemma **(5.11)**. — *Assume that* $k=\mathbf{Q}$. *Then for almost all v, the natural map*

$$H^i(G(\mathfrak{O}_v)/G(\mathfrak{p}_v), I) \rightarrow H^i(G(\mathfrak{O}_v), I)$$

is surjective.

We appeal to Proposition (4.11). We see that we need to construct a finitely generated subgroup $\Gamma_v \subset G(\mathfrak{O}_v)$ (for *almost all* v) with the following properties:

(i) Γ_v is dense in $G(\mathfrak{O}_v)$.

(ii) Let $\mathfrak{g}(k)$ be the Lie subalgebra of $M(n, k)$ corresponding to G and

$$\mathfrak{g}(\mathfrak{O}) = M(n, \mathfrak{O}) \cap \mathfrak{g}(k),$$

$\mathfrak{O}$ the ring of integers in k. Let $\mathbf{E}=\mathrm{Hom}_{\mathfrak{O}}(\mathfrak{g}(\mathfrak{O}), \mathfrak{O})$, $\mathbf{B}=\mathrm{Hom}_{\mathfrak{O}}(\mathfrak{g}(\mathfrak{O})\otimes_{\mathfrak{O}}\mathfrak{g}(\mathfrak{O}), \mathfrak{O})$, $\mathbf{S}=$ symmetric forms in $\mathbf{B}$, and $\mathbf{F}=\mathbf{B}/\mathbf{S}$. Then $H^i(\Gamma_v, \mathbf{E}\oplus\mathbf{F})$ has no $\mathfrak{p}_v$-torsion for $i=1, 2$.

(iii) $H^1(\Gamma_v, \mathfrak{g}(k))=0$.

To do this we consider two cases separately.

Case A: All absolutely simple factors of G are of rank ≥ 2.
Case B: All the absolutely simple factors are of rank 1.

(5.12) *Case A.* — Pick S_0 as in Lemma (5.9). Let Γ be an S_0-arithmetic subgroup of G. Let S_1 be the complement of the set

$$\{v \mid v \notin S_0 \cup \infty, \Gamma \text{ is dense in } G(\mathfrak{O}_v)\}$$

and S_2 the complement of the set

$$\{v \mid v \notin S_1, H^*(\Gamma, \mathbf{E}\oplus\mathbf{F}) \text{ has no } p_v\text{-torsion}\}.$$

Then S_2 is finite and if we set $\Gamma=\Gamma_v$ for all $v\notin S_2$, Γ_v satisfies (i)-(iii) above.

(5.13) *Case B.* — In this case we have $G=R_{k'/k}H$ where H is absolutely simple of rank 1. For almost all valuations v' of k', $H \cong SL(2)$ over $k'_{v'}$ and one deduces easily that one has isomorphisms $G(\mathfrak{O}_v) \overset{\varphi_v}{\cong} \prod_{v'\in\tilde{v}} SL(2, \mathfrak{O}_{v'})$ for almost all $v\in V$, where $\tilde{v}$ is the set of valuations of k' lying over v. The mapping φ_v however need not in general carry the integral Lie algebra $\mathfrak{g}(\mathfrak{O}_v)$ isomorphically onto $\coprod_{v'\in\tilde{v}} \mathfrak{sl}(2, \mathfrak{O}_{v'})$. But if k' is unramified at v, then φ_v does do this. Thus omitting some further finite set of valuations one gets an isomorphism $\mathfrak{g}(\mathfrak{O}_v) \cong \prod_{v' \in \tilde{v}} \mathfrak{sl}(2, \mathfrak{O}_{v'})$. Now let $S_0 \supset \infty$ be any set of valuations of k' with $|S_0| \geq 2$ and let $\Gamma = SL(2, A(S_0))$. Then we have inclusions of $\Gamma \overset{\lambda}{\hookrightarrow} \prod_{v' \notin S_0} SL(2, \mathfrak{O}_{v'})$ and hence $\Gamma \overset{\lambda_v}{\hookrightarrow} G(\mathfrak{O}_v)$ for almost all $v \in V$. There are only finitely many $v \in V$ such that $H^*(\Gamma, \mathfrak{sl}(2, \mathfrak{O}_{v'})$ has $\mathfrak{p}_{v'}$-torsion for some $v' \in \tilde{v}$ and according to Serre [1],

$$H^1(\Gamma, \mathfrak{sl}(2, \mathfrak{O}_{v'})) = 0$$

for almost all v'. We can now clearly take $\Gamma_v = \Gamma$.

In § (5.3) we showed that for the proof of the Main Theorem we can assume $k = \mathbf{Q}$ if characteristic of $k = 0$. The Main Theorem thus follows easily from Lemma (5.10) and (5.11) combined with Proposition (5.4) in the case of characteristic 0; in the case of positive characteristic Proposition (5.4) combined with Lemma (5.10) and Corollary (4.4) gives us the desired result.

We prove one final cohomological result. For this result, it is more convenient to formulate it over *any* global field — we drop the assumption made in the discussion above that when characteristic $k = 0$, $k = \mathbf{Q}$. On the other hand we do assume that G is absolutely simple.

Theorem **(5.14).** — *Let k be* any *global field and* G *an absolutely simple, simply connected k-algebraic group. Let*

$$S_1 = \{v \in V \mid G \textit{ is anisotropic over } k_v\}$$

and

$$S_2 = \{v \in V \mid G \textit{ is not quasi-split over } k_v\}.$$

Let S *be any finite set of valuations with* $S \supset \infty$. *Then we have*

$$H^1(G(\mathbf{A}(S)), I) \cong \prod_{v \in S_1 - S} H^1(G_v, I)$$

$$H^2(G(\mathbf{A}(S)), I) \cong H^2(\prod_{v \in S_1 - S} G_v, I) \times \prod_{v \in S_1 \cup S} H^2(G_v, I).$$

If $S \supset S_2$, $H^2(G(\mathbf{A}(S)), I) \cong \prod_{v \notin S} \mu_v$ *where for* $v \notin S$, μ_v *is a quotient of the group of roots of* 1 *in* k_v. *In particular, it is a torsion group with all torsion coprime to* p.

These Künneth relations are a consequence of the following facts already proved: for almost all v, $G(\mathfrak{O}_v)$ is a maximal compact open subgroup of G_v, $[G(\mathfrak{O}_v), G(\mathfrak{O}_v)] = G(\mathfrak{O}_v)$ and for almost all v, the natural map $H^2(G_v, I) \to H^2(G(\mathfrak{O}_v), I)$ is trivial. The last statement has not been explicitly proved so far, but it follows from Lemmas (5.10) and (5.11) when k has characteristic 0. In the case of positive characteristic p we know that for almost all v, $H^2(G(\mathfrak{O}_v), I)$ is a p-torsion group for almost all v; on the other hand according to Moore [1] and Deodhar [1], when G is quasi-split on R_v, $H^2(G_v, I) \cong \mu_v$, a quotient of the group of roots of 1 in k_v. The " Künneth relations " stated are easily obtained from these considerations and the definition of the adèle topology in view of the fact $[G_v, G_v] = G_v$ for all $v \notin S_1$ (Platonov [1]). (See Moore [1, Theorem (12.1)] where the necessary arguments are given in detail.)

Remark (5.15). — When G is anisotropic over k_v, G_v is the group of norm 1 elements in a division algebra over k_v and $H^1(G_v, \mathbf{Q}/\mathbf{Z})$ is non-trivial. In fact, if D_v is the division algebra, R_v the maximal compact sub-ring of D_v and $\mathfrak{P}_v$ the unique maximal (2-sided) ideal in R_v, $D_v/(D_v \cap (1+\mathfrak{P}_v))$ is isomorphic to a non-trivial cyclic group. (See for instance Weil [1, Ch. I, § 4].)

Theorem (5.16). — *Let* G *be a connected, absolutely simple, simply connected algebraic group defined and of rank* ≥ 2 *over a global field* k. *Let* $S \supset \infty$ *be any finite set of valuations of* k. *If characteristic* $k=0$, $C(S, G)$ *is finite. If characteristic* $k=p$, *the p-Sylow subgroup of* $C(S, G)$ *has finite index in* $C(S, G)$. *If* S *contains all the primes at which* G *is* not *quasi-split over* k_v, $C(S, G)$ *is finite.*

This is obtained by combining Theorem (3.15), (5.2) and (5.14).

6. " Stable " Results and Some General Remarks.

(6.1). — As hitherto, G will denote a connected simply connected absolutely simple group over a global field k. We assume that G has *strong approximation*. (This is known to be the case if k is a number field or if k-rank$(G) \geq 1$.) As we will be considering different finite sets of valuations of k, our notation will have to be more precise to indicate the dependence on the finite set of valuations. We fix an imbedding $G \subset GL(n)$ of G as a k-group and for any finite set S of valuations of k with $\infty \subset k$, denote as before by $G(A(S))$ the group of $A(S)$-rational points of G where $A(S)$ is the ring of S-integers. The first observation is

Lemma (6.2). — *Suppose* $\infty \subset S \subset S'$ *and there exists* $v \in S$ *such that* G *is isotropic at* v. *Then the cokernel of the map* $C(S, G) \to C(S', G)$ *is naturally isomorphic to* $\prod_{v \in \mathscr{A}(S'-S)} G(k_v)$ *where*

$$\mathscr{A}(S'-S) = \{v \in V \mid G \textit{ anisotropic over } k_v\}.$$

In particular if G *is isotropic over* k_v *for all* $v \in S'-S$, *the map* $C(S, G) \to C(S', G)$ *is surjective. Also if* $\mathscr{A}(S'-S) = S'-S$, *the map* $C(S, G) \to C(S', G)$ *is injective.*

This lemma is easily deduced from the commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & C(S, G) \arrow[r] \arrow[d] & \hat{G}(S, a) \arrow[r] \arrow[d] & \hat{G}(S, c) \arrow[r] \arrow[d, "\pi(S, S')"] & 1 \\
1 \arrow[r] & C(S', G) \arrow[r] & \hat{G}(S', a) \arrow[r] & \hat{G}(S', c) \arrow[r] & 1
\end{tikzcd}$$

Observe that the map $\pi(S, S')$ at the extreme right is simply the natural map of the group $G(\mathbf{A}(S))$ into the group $G(\mathbf{A}(S'))$ (strong approximation). Passing to the quotient by $C(S, G)$ and its image in the second row we obtain the following diagram

$$\begin{tikzcd} & \hat{G}(S, c) \arrow[d, "\alpha"] \arrow[dr, "\pi(S, S')"] & \\ 1 \longrightarrow C(S', G)/\mathrm{Im}\, C(S, G) \arrow[r] & \hat{G}(S', a)/\mathrm{Im}(C(S, G)) \arrow[r] & \hat{G}(S', c) \longrightarrow 1 \end{tikzcd}$$

The image of α is a closed subgroup containing $G(k)$. To see this we observe first that the kernel of $\pi(S, S')$ is the product $\prod_{v \in S' - S} G(k_v)$. This group maps under α into the profinite group $G(S', G)/\mathrm{Im}\, C(S, G)$. Since all the $G(k_v)$ for G isotropic over k_v admit no infinite proper normal subgroups we see that α factors through $\hat{G}(S \cup \mathscr{A}(S' - S), c)$ (which projects onto $\hat{G}(S', e)$ with compact kernel). It is easily deduced from this that the image of α is closed. Since it contains $G(k)$, α is surjective and $C(S', G)/\mathrm{Image}\, C(S, G)$ is isomorphic to $\prod_{v \in \mathscr{A}(S' - S)} G(k_v)$. The second assertion is immediate. The third follows from the fact that if G is anisotropic over k_v for all $v \in S' - S$, the families of S-arithmetic and S'-arithmetic groups coincide.

The preceding lemma suggests that it is best to consider only those sets S such that, for all $v \in S - \infty$, G is isotropic at v. In the sequel we will in fact assume always that finite sets of valuations which we consider *do not contain any non-archimedian valuation v such that* G *is anisotropic over k_v* (unless explicitly stated otherwise). In order to overcome technical difficulties that arise we need to make our choice of the imbedding $G \subset GL(n)$ somewhat carefully.

Lemma **(6.3)**. — *Let* $S_0 \supset \infty$ *be* any *finite set of valuations* (S_0 *may contain v at which* G *is anisotropic*). *If* S_0 *is non-empty we can find an imbedding of* G *in* $GL(n)$ *(as a k-algebraic group) such that*:

(i) *For all* $v \notin S_0$, $G(\mathfrak{O}_v)$ *is a maximal compact subgroup of* $G(k_v)$.

(ii) *For all* $S \supset S_0$, $G(A(S))$ *is a maximal* S-*arithmetic subgroup of* G.

(iii) *If* $S' \supset S \supset S_0$ *and* G *is anisotropic over k_v for* $v \in S' - S$, $G(A(S)) = G(A(S'))$.

Start with some k-imbedding $G \hookrightarrow GL(n)$. Then since G has strong approximation, $G(\mathfrak{O}_v) = M'_v$ is for almost all v a maximal compact subgroup of $G(k_v)$. Let $M_v \supset M'_v$ be a maximal compact subgroup of $G(k_v)$. Let $L_v = \mathfrak{O}_v^n$ if $M_v = M'_v$; if $M_v \neq M'_v$, let L_v be a compact open subgroup of k_v^n containing $\mathfrak{O}_v^n$ and stable under M_v. Let $L \subset k^n$ be the subset

$$\{x \in k^n \mid x \in L_v \text{ for all } v \notin S_0\}.$$

Since S_0 is non-empty, L is dense in $\prod_{v \notin S_0} L_v$ (strong approximation for a vector space!) (and is in fact a $A(S_0)$-module of rank n). We now change the basis of k^n to one which generates L over $A(S_0)$ and thus obtain a new imbedding of G in $GL(n)$ satisfying the required conditions.

Note: When k is a number field, we can take $S_0 = \infty$.

(6.4). — In the sequel we fix once and for all a fixed finite set S_0 with the following properties:

(i) $S_0 \supset \infty$.

(ii) If $v \in S_0 - \infty$, G is isotropic at v.

(iii) There exists $v \in S_0$ such that G is isotropic at v (this is of course redundant if $S_0 \neq \infty$).

We set $\mathscr{A} = \{v \in V - \infty \mid G \text{ anisotropic at } v\}$ and $V' = V - \mathscr{A}$. *Unless otherwise specified all finite sets considered (denoted* S, S′, S″, *etc.) will be assumed to contain* S_0 *and to be contained in* V′. We assume also that our *embedding* $G \hookrightarrow GL(n)$ *satisfies the conditions of Lemma* (6.3). This means in particular the map $C(S, G) \to C(S', G)$ is *surjective* (Lemma (6.2)). A corollary to this is

Lemma **(6.5).** — *If* $S' \supset S$, *the centraliser of* $C(S', G)$ *in* $G(k)$ *contains that of* $C(S, G)$. *In particular if* $C(S, G)$ *is central in* $\hat{G}(S, a)$, $C(S', G)$ *is central in* $\hat{G}(S', a)$.

Notation **(6.6).** — In the sequel, $\Gamma(S)$ will denote the group $G(A, S)$, $\hat{\Gamma}(S, a)$ (resp. $\hat{\Gamma}(S, c)$) its closure in $\hat{G}(S, a)$ (resp. $\hat{G}(S, c)$). If $G(k)^*$ is any subgroup of $G(k)$, $\Gamma^*(S) = G(k)^* \cap \Gamma(S)$ and $\hat{G}^*(S, \ )$ (resp. $\hat{\Gamma}^*(S, \ )$) denotes the closure of $G(k)^*$ (resp. $\Gamma^*(S)$) in $\hat{G}(S, \ )$; also $C^*(S, G)$ will denote the group

$$C(S, G) \cap \hat{G}^*(S, a) = C(S, G) \cap \hat{\Gamma}^*(S, a).$$

With this notation, the following is proved exactly as Lemma (6.2).

Lemma **(6.7).** — *Assume that* $G(k)^*$ *has finite index in* $G(k)$, *and has a dense projection on* $\prod_{v \in \mathscr{A}} G(k_v)$. *Then the map* $C(S, G) \to C(S', G)$ *is surjective for all* $(S_0 \subset) S \subset S' (\subset V')$. *In particular if* $C^*(S, G)$ *is finite* (resp. *central in* $\hat{G}^*(S, a)$) $C^*(S, G)$ *is finite* (resp. *central in* $\hat{G}^*(S', a)$).

Corollary **(6.8).** — *The natural map* $\hat{\Gamma}(S, a) \to \hat{\Gamma}(S', a)$ *is surjective.*

We look at the commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C(S, G) & \longrightarrow & \hat{\Gamma}(S, a) & \longrightarrow & \hat{\Gamma}(S, c)\left(= \prod_{v \notin S} G(\mathfrak{O}_v)\right) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & C(S', G) & \longrightarrow & \hat{\Gamma}(S', a) & \longrightarrow & \hat{\Gamma}(S', c)\left(= \prod_{v \notin S'} G(\mathfrak{O}_v)\right) & \longrightarrow & 1 \end{array}$$

whose rows are exact. The maps at the extremes are surjective (lemma (6.7) and our choice of embeddings guarantee this). By five-lemma, the middle map is surjective as well.

Corollary **(6.9)**. — *If* Φ' *is an* S'*-arithmetic subgroup of* G *and* $\Phi = \Phi' \cap \Gamma(S)$, $S' \supset S$, *then the natural map* $\hat{\Phi}(S, a) \to \hat{\Phi}'(S', a)$ *where* $\hat{\Phi}(S, a)$ (resp. $\hat{\Phi}'(S', a)$) *is the closure of* Φ (resp. Φ') *in* $\hat{G}(S, a)$ (resp. $\hat{G}(S', a)$), *has finite cokernel.*

Remark **(6.10)**. — In the corollary above we need only the fact that S, S' contain S_0 — they may contain anisotropic places: this is because S-arithmetic groups and $(S - \mathscr{A})$-arithmetic groups are the same and a similar remark applies to S'.

The following consequence of Corollary (6.9) is perhaps of greater interest than that corollary itself.

Corollary **(6.11)**. — *If* S *is* any *finite set such that for every* S*-arithmetic group* Φ, Φ *is infinite and* $\Phi/[\Phi, \Phi]$ *is finite, then the same holds for every* S'*-arithmetic group* Φ' *for* $S' \supset S$. (We do not need to assume that S and S' are contained in V'.)

Combining with Kazdan's theorem on the first Betti number of lattices in groups without rank 1 or compact factors we obtain the following extension of his result.

Corollary **(6.12)**. — *Let* S *be* any *finite set such that there exists* $v \in S$ *with* k_v*-rank*$(G) \geq 2$. *Then for any* S*-arithmetic group* Φ, $\Phi/[\Phi, \Phi]$ *is finite.*

Corollary **(6.13)**. — *Let* $G(k)^*$ *be a subgroup of finite index in* $G(k)$. *Then* $G(k)^*/[G(k)^*, G(k)^*]$ *is finite.*

Replacing $G(k)^*$ by a subgroup of finite index we may assume that $G(k)^*$ is normal in $G(k)$. Let $\Psi = [G(k)^*, G(k)^*]$. Then Ψ is a normal subgroup of $G(k)$. Now in §§ (5.6), (5.7), we have seen that *there exists* S such that G is isotropic at v for some $v \in S$ and for every S-arithmetic group Φ, $\Phi/[\Phi, \Phi]$ is finite. Pick one such S-arithmetic group $\Phi \subset G(k)^*$. Then $\Phi \cap \Psi$ is S-arithmetic as well. Its closure is therefore open in $G(\mathbf{A}(S))$ (strong approximation). Thus the closure $\hat{\Psi}$ of Ψ in $G(\mathbf{A}(S))$ is open as well. Now for the natural identification of $G(k_v)$ $(v \notin S)$ as a closed subgroup of $G(\mathbf{A}(S))$, $G(k_v) \cap \hat{\Psi}$ is open and normal in $G(k_v)$. It is therefore equal to $G(k_v)$ for all $v \notin S$ at which G is isotropic (Kneser-Tits conjecture for local fields). It follows that $\hat{\Psi}$ has finite index in $G(\mathbf{A}(S))$, so that $G(k)^{\sim} = G(k)^* \cap \hat{\Psi}$ has finite index in $G(k)^*$. Now from the density of Ψ in $\hat{\Psi}$, we see that for any S-congruence subgroup Δ of G

$$G(k)^{\sim} \subset \Psi(\Delta \cap G(k)^{\sim}).$$

The desired result now follows from Corollary (6.12).

Proposition **(6.14)**. — *Assume that* $S \subset V'$, $\infty \subset S$ *and that* $C^*(S, G)$ *is central in* $\hat{G}^*(S, a)$ *for some subgroup* $G(k)^*$ *of finite index in* $G(k)$. *Then the p-Sylow subgroups of* $C(S, G)$ *and* $C^*(S, G)$ *are of finite index in these groups* ($p =$ *characteristic of* k).

We first pick $S' \subset V' - \infty$ such that if $S'' = S \cup S'$ for any S'-arithmetic group Φ, $\Phi/[\Phi, \Phi]$ is finite and G is quasi-split for all $v \in S'$. Such a choice is possible by §§ (5.6-5.7) and Corollary (6.11).

Let $\hat{H}(S, a)$ (resp. $\hat{H}(S, c)$) be the closure of $\Gamma^*(S'')$ in $\hat{G}(S, a)$ (resp. $\hat{G}(S, c)$). Then from strong approximation one sees immediately that $\hat{H}(S, c) = (\prod_{v \in S'} G(k_v)) \times U$ where U is a compact open subgroup of $\hat{G}(\mathbf{A}(S''))$. Consider now the central extension

$$1 \to C^*(S, G) \to \hat{H}(S, a) \to \hat{H}(S, c) \to 1.$$

Associated to this one has a cohomology sequence (here $I = \mathbf{Q}/\mathbf{Z}$)

$$\ldots \to \mathrm{Hom}(\hat{H}(S, a), I) \to \mathrm{Hom}(C^*(S, G), I) \to H^2(\hat{H}(S, c), I) \to \ldots$$

Now from Theorem (5.2) and the results of Deodhar [1] and Moore [1], the p-torsion in $H^2(\hat{H}(S, c), I)$ has finite index in that group. On the other hand $\mathrm{Hom}(\hat{H}(S, a), I)$ is isomorphic to $\mathrm{Hom}(\Gamma^*(S''), I)$ and is thus finite. It follows that $\mathrm{Hom}(C^*(S, G), I)$ has p-torsion of finite index. Taking the Pontrjagin duals we obtain the proposition.

Corollary **(6.15).** — *If there exists* $S \subset V'$, $\infty \subset S$, *such that* $C^*(S, G)$ *is central in* $\hat{G}^*(S, a)$ *for some subgroup* $G(k)^*$ *of finite index in* $G(k)$, *then the p-Sylow subgroup of* $C(S', G)$ *is of finite index in it for all* $S' \supset S$, $S' \subset V'$.

Remark **(6.16).** — One can refine the arguments given above in the case when $\mathscr{A}$ is empty. (We note that this happens when G is *not* of type A_n). In this case we observe first that the map

$$C^*(S, G) \to C^*(S', G)$$

is surjective for $S' \supset S$, so that for $S \subset S' \subset S''$ both the extensions in the commutative diagram below are central.

$$\begin{tikzcd}
1 \arrow[r] & C^*(S', G) \arrow[r] \arrow[d] & \hat{G}^*(S', a) \arrow[r] \arrow[d] & \hat{G}^*(S', c) = \hat{G}(S', c) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & C^*(S'', G) \arrow[r] & \hat{G}^*(S'', a) \arrow[r] & \hat{G}^*(S'', c) = \hat{G}(S'', c) \arrow[r] & 1
\end{tikzcd}$$

Also the *vertical maps* are *surjective*. We also have the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & C^*(S', G) \arrow[r] \arrow[d] & \hat{\Gamma}^*(S', a) \arrow[r] \arrow[d] & \hat{\Gamma}^*(S', c) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & C^*(S'', G) \arrow[r] & \hat{\Gamma}^*(S'', a) \arrow[r] & \hat{\Gamma}^*(S'', c) \arrow[r] & 1
\end{tikzcd}$$

The corresponding cohomology sequences are again embedded in a commutative diagram:

$$\begin{tikzcd}
\mathrm{Hom}(\hat\Gamma^*(S', c), I) \arrow[r] & \mathrm{Hom}(\hat\Gamma^*(S', a), I) \arrow[r] & \mathrm{Hom}(C^*(S', G), I) \arrow[r] & H^2(\hat\Gamma^*(S', c), I) \arrow[r] & {} \\
\mathrm{Hom}(\hat\Gamma^*(S'', c), I) \arrow[r] \arrow[u, "\alpha^*"] & \mathrm{Hom}(\hat\Gamma^*(S'', a), I) \arrow[r] \arrow[u, "\beta^*"] & \mathrm{Hom}(C^*(S'', G), I) \arrow[r] \arrow[u, "\gamma^*"] & H^2(\hat\Gamma^*(S'', c), I) \arrow[r] \arrow[u, "\alpha^*"] & {}
\end{tikzcd}$$

Now according to Corollary (5.8), there exists $S_0 \supset S$ such that the groups at the extreme left are trivial if $S' \supset S_0$ and, by Theorem (5.2), we can also assume S_0 so chosen that the groups at the extreme right are *p-torsion groups*. We may also assume S_0 so chosen that for any S'''-arithmetic group Φ with $S''' \supset S_0$, $\Phi/[\Phi, \Phi]$ is finite. It follows (from the injectivity of β^*) then that there exists $S_1 \supset S_0$ such that

$$\mathrm{Hom}(\hat\Gamma^*(S', a), I) = \mathrm{Hom}(\Gamma(S), I) = \mathrm{Hom}(G(k)^*, I)$$

for *all* $S' \supset S_1$. If characteristic $k = 0$, we see immediately that

$$\mathrm{Hom}(C^*(S', G), I) \cong \mathrm{Hom}(G(k)^*, I)$$

for all $S' \supset S_1$. When the characteristic is positive, we have to argue a little more delicately: we look at the following exact sequence as well (for $S' \supset S_1$):

$$\begin{tikzcd}
\mathrm{Hom}(\Gamma^*(S'), I) = \mathrm{Hom}(G(k)^*, I) \arrow[r, "\lambda"] \arrow[d, equal] & \mathrm{Hom}(C^*(S', G), I) \arrow[r] & H^2(\hat G^*(S', c), I) \arrow[d, equal] \\
\mathrm{Hom}(\hat G^*(S', a), I) & & H^2(\hat G(S', c), I)
\end{tikzcd}$$

From the results of Deodhar and Moore *(loc. cit.)* the group at the extreme right has no p-torsion if G is quasi-split for all $v \notin S_1$. On the other hand we have seen from the earlier discussion that the cokernel of λ is a p-torsion group. We conclude therefore that the cokernel of λ is zero. We summarize this discussion in the following.

Theorem **(6.17)**. — *Assume that* G *is isotropic at all* $v \notin \infty$. *Let* $G(k)^*$ *be a normal subgroup of* $G(k)$ *of finite index and* $S \subset V$ $(=V')$ *be a finite set such that* $C^*(S, G)$ *is central in* $\hat G^*(S, a)$. *Then we have*:

(i) *The p-Sylow subgroup of* $C(S', G)$ *has finite index in* $C(S', G)$ *for all* $S' \supset S$.
(ii) *The maps* $C^*(S, G) \to C^*(S', G)$ *and* $C(S, G) \to C(S', G)$ *are surjective.*
(iii) *There exists a finite set* $S_1 \supset S$ *such that for all* $S' \supset S_1$, *the map* $C(S_1, G) \to C(S', G)$ *is an isomorphism*; *all these groups are naturally isomorphic to the* finite *group*

$$G(k)^*/[G(k)^*, G(k)^*] \cong \Gamma^*(S')/[\Gamma^*(S'), \Gamma^*(S')].$$

Corollary **(6.18)**. — *Assume that* $k\text{-rank}(G) \geq 2$. *Then there exists a finite set* S_0 *such that for all* $S \supset S_0$, $C(S, G)$ *is central in* $\hat G(S, a)$ *and isomorphic to* $G(k)/G(k)^+$ *(notation as in* § 3*)*.

Take $G(k)^* = G(k)^+$. Since $G(k)^+$ is its own commutator, $C^*(S, G)$ is trivial for all $S \supset S_1$ where S_1 is chosen as in Theorem (6.17). Once $C^*(S, G)$ is trivial, we know that $C(S, G)$ is central in $\hat{G}(S, a)$ and we can apply Theorem (6.17) to $G(k)$ itself.

Remark **(6.19).** — There is one other situation to which Theorem (6.17) is applicable: Kneser [1] has announced the following result: Let k be a *number field*. Let $G = \mathrm{Spin} f$, f a quadratic form in $n \geq 5$ variables over k. Let $S \supset \infty$ be a finite set of valuations such that $\sum_{v \in S} k_v\text{-rank}(G) \geq 2$. Then $C(S, G)$ is central in $\hat{G}(S, a)$. Theorem (6.17) now furnishes the further information that $C(S, G)$ is indeed finite in this case. When f is isotropic over k, Kneser has a much more precise result.

7. Representations of Arithmetic Groups.

(7.1). — Throughout this chapter, k will denote a *number field*, G an absolutely simple k-group and $S \supset \infty$ a finite set of valuations of k containing ∞. We assume that G is simply connected and has in addition the following property:

(CSP) The group $C(S, G)$ is finite.

(Note that if G has (CSP), it is necessarily isotropic at all $v \in S - \infty$.) We also assume that there exists $v \in S$ such that G is isotropic at v (this to ensure that S-arithmetic groups are not finite) and that G has strong approximation. With these notations our first result is

Theorem **(7.2).** — *Assume that* G *has* (CSP). *Let* Φ *be an* S*-arithmetic group of* G. *Let* ρ *be a finite dimensional representation of* Φ *on a finite dimensional vector space* V *over a field* F *of characteristic* 0. *Then there exists a subgroup* Φ' *in* Φ *of finite index and a rational representation* $\tilde{\rho}$ *of* $R_{k/\mathbf{Q}}(G)$ *defined over* F *such that* $\tilde{\rho}|_{\Phi'} = \rho|_{\Phi'}$.

When $F = \mathbf{Q}$, this result is proved in Bass-Milnor-Serre [1]. When F is a finite extension of $\mathbf{Q}$, one can reduce to the case of $F = \mathbf{Q}$, by looking at the F-vector space as a $\mathbf{Q}$-vector space. Since Φ is finitely generated one sees easily that this covers the case when F is algebraic over $\mathbf{Q}$ as well. Consider now the general case. We make first an observation about representations over $\overline{\mathbf{Q}}$ = algebraic closure of $\mathbf{Q}$. These representations are all completely reducible since rational representations of semisimple groups are. Equivalently for every finite dimensional representation σ of Φ on $\overline{\mathbf{Q}}$-vector spaces $H^1(\Phi, \sigma) = 0$. Now, let $\mathscr{R}(\Gamma)$ denote the variety of all representations of Φ in $GL(n, \overline{F})$ (F any field and $\overline{F}$ its algebraic closure). Then $\mathscr{R}(\Gamma)$ is a variety *defined over* $\mathbf{Q}$. If $\sigma \in \mathscr{R}(\Gamma)$ is a $\overline{\mathbf{Q}}$-rational point, $H^1(\Phi, \mathrm{Ad} \circ \sigma) = 0$, where Ad is the adjoint representation of $GL(n)$ on its Lie algebra. According to A. Weil [1] this means that the orbit of σ in $\mathscr{R}(\Gamma)$ under inner conjugation is Zariski open in $\mathscr{R}(\Gamma)$. Let

$$\mathscr{U} = \{g \sigma g^{-1} \mid g \in GL(n, \overline{F}),\ \sigma \in \mathscr{R}(\sigma)_{\overline{\mathbf{Q}}}\}.$$

Then $\mathscr{U}$ as well as it complement $\mathscr{U}'$ are stable under the group of all automorphisms of $\overline{F}$ (over $\mathbf{Q}$). Since $\mathscr{U}$ is Zariski open, $\mathscr{U}'$ is a $\mathbf{Q}$-subvariety. On the other hand it has no $\overline{\mathbf{Q}}$-rational point. Hence $\mathscr{U} = \mathscr{R}(\Phi)$ and the theorem is established.

Corollary (**7.2**). — *Let* ρ *be any finite dimensional representation of an* S*-arithmetic group* Φ. *If* $C(S, G)$ *is finite,* $H^1(\Phi, \rho) = 0$.

Corollary (**7.2**). — *If* $C(S, G)$ *is finite, for any* S*-arithmetic group* Φ, $\Phi/[\Phi, \Phi]$ *is finite.*

Theorem (**7.2**). — *Assume that* $C(S, G)$ *is finite and that* G *is isotropic at all* $v \notin S$. *Let* F *be a field of characteristic* $p > 0$. *Then any homomorphism* $\rho : \Phi \to GL(n, F)$ *is trivial on a subgroup of finite index.*

We will deduce this from

Lemma (**7.3**). — *Let* K *be a locally compact field of characteristic* 0 *and* H *a* K*-simple group isotropic over* K. *Let* M *be a compact open subgroup of* H(K). *Then the kernel of any homomorphism of* M *into* $GL(n, F)$, F *a field of positive characteristic, is open in* M.

Let $f : M \to GL(n, F)$ be any homomorphism. Let U be any maximal unipotent K-subgroup of M and T a K-split torus normalising U. Let $B = TU$. Then B is a solvable group. The Zariski closure of $f(B \cap M)$ is again a solvable group. It follows that we can find a subgroup B_1 of finite index in $B \cap M$ such that $f(B_1)$ can be put in triangular form (over the algebraic closure of F). Consequently $[B_1, B_1]$ consists of unipotents. It is not difficult to see that $[B_1, B_1]$ contains an open subgroup U′ of $M \cap U$. Now $f(U')$ consists entirely of unipotents. Since F has positive characteristic ($= p$, say), $(f(x))^{p^n} = 1$ for all $x \in U'$. Thus the set $\{x^{p^n} \mid x \in U'\}$ and hence the group U″ generated by it is in the kernel of f. Evidently (since characteristic $K = 0$), U″ is open in $U \cap M$. Now as U varies, we get different U″ which together are easily seen to generate an open subgroup of M. This proves the lemma. (The lemma is probably true without the hypothesis that H is isotropic over K but the present proof fails to cover that case.)

To deduce the theorem from the lemma we argue as follows: since Φ is finitely generated, $\rho(\Phi) \subset GL(n, F')$, where F′ is a finitely generated algebra over the prime field, which is a subring of F. We consider two cases separately.

Case (i): $\rho(\Phi)$ contains an element γ one of whose eigen-values λ is transcendental over the prime field.

Case (ii): For all $\gamma \in \rho(\Phi)$, the eigen-values of γ are algebraic over the prime field.

We will now show that Case (i) cannot occur. Let F_q be the algebraic closure of the prime field in F′. Let $F_0 = F_q(\lambda)$ and F^* the algebra generated by F_0 and F′. Then F^* is a finitely generated algebra over F_0. Let $\alpha : F^* \to \widetilde{F}_0$ be any homomorphism of F^* into a finite extension $\widetilde{F}_0$ of F_0 which is identity on F_0. (Such a φ exists by the Nullstellensatz.) If we now regard ρ as a homomorphism of Φ in $GL(n, F^*)$, we obtain, composing with α, a homomorphism $\rho_1 : \Phi \to GL(n, \widetilde{F}_0)$. From our choice of α it is clear that $\rho_1(\Phi)$ is *infinite.* Moreover $\rho_1(\Phi)$ is contained in $GL(n, \Lambda)$ where Λ is the ring of T-integers for a suitable finite set of valuations T on $\widetilde{F}_0$. Now if we denote by $\mathbf{A}(\Lambda)$ the ring of T-adèles, ρ_1 defines a continuous homomorphism

$$\widetilde{\rho}_1 : \hat{\Phi}(S, a) \to GL(n, \mathbf{A}(\Lambda)).$$

Now since $C(S, G)$ is finite, we can find an open compact subgroup $\hat{\Delta} \subset \hat{\Phi}(S, a)$ such that $\hat{\Delta} \cap C(S, G)$ is trivial. Then $\hat{\Delta}$ is isomorphic to an open compact subgroup of $\hat{\Phi}(S, c)$. Again passing to a subgroup of finite index we can assume that $\hat{\Delta}$ is of the form $\prod_{v \notin S} M_v$, M_v a compact open subgroup of $G(k_v)$. Let $\pi : GL(n, \mathbf{A}(\Lambda)) \to GL(n, K)$ be the projection onto any one of the local factors; since $\pi|_{GL(n, \Lambda)}$ is injective it suffices to show that $\pi(\widetilde{\rho}_1(\hat{\Delta}))$ is finite. For this again, it suffices to show that $\pi(\widetilde{\rho}_1(M_v))$ is finite for all v and trivial for almost all v. The finiteness for all v is proved in Lemma (7.3). Now let $\mathscr{B}$ be the K-linear span of $\pi(\widetilde{\rho}(\hat{\Delta}))$ in $M(n, K)$. Then $\mathscr{B}$ is also the K-algebra generated by $\bigcup_{v \in S_1} \pi(\widetilde{\rho}_1(M_v))$ where S_1 is some finite set of valuations (with $S_1 \cap S = \emptyset$). It follows that for $v \notin S \cup S_1$, $\pi(\widetilde{\rho}_1(M_v)) \subset$ centre of $\mathscr{B}$. This means that $\pi(\widetilde{\rho}_1(M_v))$ is abelian for almost all $v \notin S$. Now we know that $M_v = [M_v, M_v]$ for almost all v (Corollary (5.8)). We see therefore that $\pi \circ \widetilde{\rho}_1$ is trivial on almost all M_v $(v \notin S)$. This covers Case (i).

In order to prove the theorem in Case (ii) we will argue by induction on the length of F^n as a module over Φ. We assume in fact — as we may by passing to an extension of F if necessary — that the composition factors are absolutely irreducible. Consider first the case when the length of F^n as a Φ-module is 1. This means that $\rho(\Phi)$ spans the entire matrix algebra $M(n, F)$. Consider now the smallest subspace E of the space of all regular functions on $GL(n)$ stable under $\rho(\Phi)$ and containing the function $x \mapsto \mathrm{trace}(x)$. Since $\mathrm{trace}(x)$ is in the algebraic closure of the prime field for all $x \in \rho(\Phi)$, one sees that the representation of $\rho(\Phi)$ in E takes $\rho(\Phi)$ into a finite subgroup of $GL(E)$. We claim now that if σ denotes the representation of $\rho(\Phi)$ on E, σ is faithful. In fact if $\sigma(x) = 1$, we have $\mathrm{trace}(xy) = \mathrm{trace}(y)$ for all $y \in \rho(\Phi)$ or equivalently $\mathrm{trace}((x-1)y) = 0$ for $y \in \rho(\Phi)$. Since $\rho(\Phi)$ spans $M(n, F)$, this means that $x = 1$. Since $\sigma(\rho(\Phi))$ is finite, so is $\rho(\Phi)$. To prove the general case we appeal to Corollary (7.3): let $V = F^n$ and $W \subset F^n$ be a maximal proper Φ-submodule. Then we have a natural homomorphism (deduced from ρ)

$$\psi : \Phi \to GL(W) \times GL(V/W).$$

By the induction hypothesis the kernel of ψ $(=\Phi'$, say) has finite index in Φ. Now $\rho|_{\Phi'}$ maps Φ' into a unipotent, hence solvable, group. But from Corollary (7.3) any solvable quotient of Φ' must be finite. This proves our contention.

Theorem **(7.4)**. — *Suppose that* $C(S, G)$ *is finite for some* S *and* ρ *is a finite dimensional representation of* $G(k)$ *over a field of characteristic* 0. *Then we can find a subgroup* $G(k)^*$ *of finite index in* $G(k)$ *and a rational representation* $\widetilde{\rho}$ *of* $R_{k/\mathbf{Q}}(G)$ *such that* $\widetilde{\rho}|_{G(k)^*} = \rho|_{G(k)^*}$.

Let $\mathscr{A}$ be the set of valuations v of k, $v \notin \infty$, at which G is anisotropic. Then $C(S', G)$ is finite for all $S' \supset S$, $S' \subset V' = V - \mathscr{A}$. If Φ is any S'-arithmetic group, $\rho|_{\Phi'}$ extends to a rational representation $\widetilde{\rho}$ of $R_{k/\mathbf{Q}} G$, where Φ' is a subgroup of finite index. It is easily seen that $\widetilde{\rho}$ is indeed independent of the choice of S' and Φ — this follows from the fact that $\Phi_1 \cap \Phi_2$ is Zariski dense in G for S_i-arithmetic groups Φ_i with $S_i \supset S$. Let $G(k)^*$ be the subgroup generated by the collection of groups

$$\{\Phi \mid \Phi \text{ S'-arithmetic with } S' \supset S,\ S' \subset V',\ \rho|_{\Phi} = \widetilde{\rho}|_{\Phi}\}.$$

One sees easily that $G(k)^*$ is normal in $G(k)$ and it is open in the S-arithmetic topology. Now the closure of $G(k)^*$ in $\hat{G}(S, c)$ is easily seen to be a open subgroup of finite index (Kneser-Tits conjecture for local fields and strong approximation). This means that for a subgroup $\Psi \subset G(k)$ of finite index, we have $\Psi \subset G(k)^* \Delta$ where Δ is any S-congruence subgroup. Since $S(k)^*$ contains an S-arithmetic group, $\Delta \cap G(k)^*$ has finite index in Δ, so that $G(k)^*$ has finite index in Ψ. This proves Theorem (7.4).

Theorem **(7.5)**. — *Assume that* $C(S, G)$ *is finite and that* G *is isotropic at all* $v \notin S$. *Then* $G(k)$ *has only finitely many normal subgroups of finite index.*

Let ρ_1 and ρ_2 be homomorphisms of $G(k)$ in $GL(n)$ with $\rho_i(G(k))$ finite. We will show that the natural extensions $\hat{\rho}_i : \hat{G}(S, a) \to GL(n)$ are equivalent if and only if $\hat{\rho}_i|_{C(S, G)}$ are equivalent. One implication is obvious. Suppose $\hat{\rho}_1$ and $\hat{\rho}_2$ restricted to $C(S, G)$ are equivalent. Consider the representation $\hat{\rho}_1 \otimes \hat{\rho}_2^*$ ($\hat{\rho}_2^* =$ dual of $\hat{\rho}_2$). This representation contains the trivial representation of $C(S, G)$. Let E be the representation space of $\sigma = \hat{\rho}_1 \otimes \hat{\rho}_2^*$ and

$$E_0 = \{v \in E \mid \sigma(x) v = v \text{ for all } x \in C(S, G)\}.$$

E_0 is non-zero and stable under $\hat{G}(S, a)$. Moreover the action of $\hat{G}(S, a)$ on E_0 factors through $\hat{G}(S, c)$, and from the Kneser-Tits conjecture for local fields, $\hat{G}(S, c)$ has no proper subgroups of finite index. This shows that E_0 is a trivial $\hat{G}(S, a)$-module *i.e.* $\hat{\rho}_1$ and $\hat{\rho}_2$ are equivalent as representations of $\hat{G}(S, a)$. It follows that ρ_1 and ρ_2 are equivalent. It is easily deduced from this that the family of subgroups of finite index in $G(k)$ are in bijective correspondence with a subset of the family of subgroups of $C(S, G)$. Since $C(S, G)$ is finite, the theorem follows.

Remarks **(7.6)**. — Most of the results obtained in this chapter overlap with results obtained by Margulis by completely different methods. Margulis has in fact a much more satisfactory result — his conclusions are drawn from the hypothesis

$$\sum_{v \in S} k_v\text{-rank}(G) \geq 2$$

whereas the finiteness of $C(S, G)$ is not known for practically most of the pairs (G, S) with this property. Theorem (7.5), however, does not seem amenable to Margulis' techniques. It is possible to formulate some of the above results without the hypothesis that G is isotropic at all $v \notin \infty$ but the formulations are cumbersome — and in any event the essential ideas of proof would be the same.

Appendix I

ARITHMETIC SUBGROUPS IN UNIPOTENT GROUPS

We collect together some results on unipotent groups which were used in the main paper. These results are really known though perhaps not set down in print — at least not in the present form. The first result below is standard commutative algebra.

Proposition **(A.1)**. — *Let* G *be a connected k-group and* H *a connected k-subgroup. If* G/H *is k-isomorphic to a vector space (over k) as an algebraic variety (over k), there is an isomorphism*

$$\Phi : G \to H \times (G/H)$$

of k-varieties such that the Cartesian projection on G/H *is the same as the natural map* $G \to G/H$.

Definition **(A.2)**. — A unipotent k-group U is *k-split* if it is connected and admits a filtration

$$U = U_0 \supset U_1 \supset \ldots \supset U_r = (1)$$

by connected k-subgroups U_i such that for $1 \leq i \leq r$, U_i is normal in U_{i-1} and U_{i-1}/U_i is isomorphic over k to a vector space (of dimension 1).

Remark **(A.3)**. — (i) If U is unipotent k-split, then any connected k-subgroup is also k-split.

(ii) If G is a connected semisimple k-group, the unipotent radical of a k-parabolic subgroup of G is k-split (Borel-Tits [1]).

Corollary **(A.4)**. — *Let* U *be a connected unipotent split k-group and* V *be a connected normal k-subgroup. Then* U *is k-isomorphic to a vector space (as an algebraic variety). Moreover, there is an isomorphism*

$$f : (U/V) \times V \to U$$

of k-varieties such that the natural morphism $U \xrightarrow{\pi} U/V$ *coincides with the cartesian projection composed with* f^{-1}.

One argues by induction on the dimension of U. By the induction hypothesis U/V and V are k-isomorphic to vector spaces. The second assertion now follows from Proposition (A.1). The first assertion follows from the fact that any split unipotent k-group admits a connected (split) k-subgroup of codimension 1.

Corollary **(A.5)**. — *Let* U *be a connected unipotent k-group split over k. Let* $S \supset \infty$ *be any finite set of valuations of k* (∞ *being the set of archimedean valuations*). *Then any* S-*arithmetic subgroup of* U *is Zariski dense in* U *for any non-empty* S.

Observe that if Φ is a k-isomorphism of a vector space V on **U** (as a k-variety) with $\Phi(0)=1$ for any S-congruence subgroup Γ of **U** (resp. Γ' of V), $\Phi^{-1}(\Gamma)$ (resp. $\Phi^{-1}(\Gamma')$) contains a S-congruence subgroup of V (resp. **U**). Similar remarks applied to an isomorphism of **U** with $U' \times (U/U')$ where U′ is a connected normal k-subgroup leads us to conclude the following:

Corollary **(A.6)**. — *Let* U *be a split unipotent k-group and* U′ *a connected normal k-subgroup. Let* $\pi : U \to U/U'$ *be the natural map. Then for each* S-*congruence subgroup* Γ *of* U ($S \supset \infty$, *etc.*), $\pi(\Gamma)$ *is an* S-*congruence subgroup of* U/U′.

Appendix II

Theorem. — *Let k be any field and* G *a* connected simply connected absolutely simple quasi-split *algebraic group over k. Let* P *be a k-parabolic subgroup of* G *and* U *the unipotent radical of* P. *Let* $\mathfrak{g}$ *be the k-Lie algebra of* G *and* $\mathfrak{u}$ *the (k-)Lie subalgebra of* $\mathfrak{g}$ *associated to* U. *Let* $F \subset k$ *be the prime field and* A *the group-algebra of* $G(k)$ *over* F. *Then* $\mathfrak{g}$ *is generated by* $\mathfrak{u}$ *as an* A*-module (* $\mathfrak{g}$ *is a module over* A via *the adjoint action).*

The theorem is easily checked in the special case when k-rank$(G) = 1$: in this case G is k-isomorphic either to SL(2) or SU(f), the special unitary group of an isotropic bilinear form f in 3 variables over a separable quadratic extension L of k. One can verify the theorem in these cases by using these explicit realisations.

We will now deduce the general case from the special case above. Let T be a maximal k-split torus in P and Φ denote the system of k-roots of G with respect to T. We fix an ordering on X(T), the group of characters on T, such that $\alpha \in \Phi$ is positive if the root-space $\mathfrak{g}^\alpha$ of α is contained in $\mathfrak{u}$. Let Δ be the system of simple roots for this ordering. Let P_1 be a minimal k-parabolic subgroup determined by T and this ordering. Let P_1^- be the (unique) opposite k-parabolic subgroup to P_1 which contains T. Let U_1 (resp. U_1^-) be the unipotent radical of P_1 (resp. P_1^-) and $\mathfrak{u}_1$ (resp. $\mathfrak{u}_1^-$) the Lie subalgebra of $\mathfrak{g}$ corresponding to U_1 (resp. U_1^-). Then $\mathfrak{u}$ (resp. $\mathfrak{u}_1^-$) is the sum of root spaces $\mathfrak{g}^\alpha$ as α varies over all the positive (resp. negative) k-roots. Now, let V be the smallest A-submodule of $\mathfrak{g}$ containing $\mathfrak{u}$. Since $G(k)$ acts on $\mathfrak{g}$ as k-linear automorphisms, V is a k-vector-subspace of $\mathfrak{g}$. Now, given any root $\alpha \in \Phi$, we can find an element $w \in N(T)(k)$ (where $N(T) =$ normaliser of T) such that $\operatorname{Ad} w(\mathfrak{g}^\alpha) = \mathfrak{g}^{w(\alpha)} \subset \mathfrak{u}$, hence we see that $\mathfrak{u}_1 \oplus \mathfrak{u}_1^- \subset V$. Now for each $\alpha \in \Delta$, let T_α be the identity component of the kernel of α. Then $Z(T_\alpha)$ is a reductive subgroup of G. Let $H(\alpha)$ be the connected semisimple part of $Z(T_\alpha)$. Then $H(\alpha)$ is a quasi-split simply connected group of k-rank 1. Let $\mathfrak{h}(\alpha)$ be the Lie subalgebra of $\mathfrak{g}$ corresponding to $H(\alpha)$ ($\mathfrak{h}(\alpha)$ may be identified with the Lie algebra of $H(\alpha)$ since the inclusion $H(\alpha) \hookrightarrow G$ is a *separable* morphism). Moreover, it is not difficult to see that the sum of the $\mathfrak{h}(\alpha)$, $\alpha \in \Delta$, and $\mathfrak{u}_1^+$ and $\mathfrak{u}_1^-$ is all of $\mathfrak{g}$ (one can for instance argue by going over to an extension of k over which G is split). Now $\mathfrak{u}_1 \cap \mathfrak{h}(\alpha)$ is the Lie algebra of the unipotent radical $U(\alpha)$ of the minimal k-parabolic group $P(\alpha) = U_1 \cap H(\alpha)$ of $H(\alpha)$. Applying the theorem to the rank 1-group $H(\alpha)$, we conclude that $V \supset \mathfrak{h}(\alpha)$. Thus $V \supset \mathfrak{u} + \mathfrak{u}^- + \sum_{\alpha \in \Delta} \mathfrak{h}(\alpha) = \mathfrak{g}$. This proves the theorem.

APPENDIX III

Theorem. — Let G *be a simply connected semisimple algebraic group defined over* $\mathbf{Q}_p$. *Then there exists a number field* $K \subset \mathbf{Q}_p$ *and a group* H *defined over* K *which is isomorphic to* G *over* $\mathbf{Q}_p$.

It is easily seen that the theorem is equivalent to the following. Let $\mathfrak{g}$ be a semisimple Lie algebra over $\mathbf{Q}_p$. Then there exists a number field $K \subset \mathbf{Q}_p$ and a (semisimple) Lie algebra $\mathfrak{h}$ over K such that $\mathfrak{g}$ is isomorphic to $\mathfrak{h} \otimes_K \mathbf{Q}_p$.

Consider a vector space V over $\mathbf{Q}$ of dimension equal to $\dim_{\mathbf{Q}_p}(\mathfrak{g})$. Let

$$\mathbf{V} = V \otimes_{\mathbf{Q}} \mathbf{Q}_p \quad \text{and} \quad E = \mathrm{Hom}_{\mathbf{Q}_p}(\Lambda^2 \mathbf{V}, \mathbf{V}).$$

Let $\varphi_0 : \mathbf{V} \to \mathfrak{g}$ be any $\mathbf{Q}_p$-linear isomorphism. Then the bracket operation on $\mathfrak{g}$ gives rise to an element $f_0 \in E$ (through the isomorphism φ_0). Let $X_1, \ldots, X_r$ be a basis of V over $\mathbf{Q}$ and for $1 \leq i \leq j \leq k \leq r$, let

$$\Phi_{ijk} : E \to \mathbf{V}$$

be the map

$$\Phi_{ijk}(f) = f(X_i, f(X_j, X_k)) + f(X_j, f(X_k, X_i)) + f(X_k, f(X_i, X_j)).$$

Then the set L of f which define a Lie algebra structure on $\mathbf{V}$ is precisely $\bigcap_{1 \leq i < j < k \leq r} \Phi_{ijk}^{-1}(0)$. On the other hand the group $GL(\mathbf{V})$ operates on E in a natural fashion and we have the following diagram

$$GL(\mathbf{V}) \xrightarrow{i} E \xrightarrow{\Phi} \prod_{1 \leq i < j < k \leq r} \mathbf{V}$$

where $i(x) = x(f_0)$ and the image of i is contained in the fibre of $\Phi = \{\Phi_{ijk}\}_{1 \leq i < j < k \leq r}$ over 0. Now the tangent space to E at f can be identified with E itself. One checks that the kernel of $d\Phi$ at f_0 is the set of all closed 2-forms on $\mathbf{V}$ with respect to the Lie algebra structure on $\mathbf{V}$ defined by f_0 with coefficients in the adjoint representations; the image of di (at identity) similarly turns out to be the space of exact forms. Since the Lie algebra $\mathfrak{g}$ is semisimple, $H^2(\mathfrak{g}, \mathfrak{g}) = 0$. It follows that Image di = kernel $d\Phi$ (at f_0). Now from the implicit function theorem, one deduces that Image i is a neighbourhood of f_0 in $\Phi^{-1}(0) = L$ and that we can find coordinate projections $p_1, \ldots, p_m$ of E (with respect to the standard basis of E deduced from $X_1, \ldots, X_r$) such that $p = (p_1, \ldots, p_n) : L \to \mathbf{Q}_p^m$ is a diffeomorphism of a (non-singular) open neighbourhood of f_0 in L onto an open subset of $\mathbf{Q}_p^m$. Now choose $f \in$ Image i such that $p_i(f)$ are algebraic over $\mathbf{Q}$, $1 \leq i \leq m$. Then we claim that *all* the coordinates of f are algebraic over $\mathbf{Q}$: this follows from the fact that the Φ_{ijk} are polynomials on E with coefficients in $\mathbf{Q}$. This proves the theorem.

REFERENCES

BASS (H.), LAZARD (M.), SERRE (J.-P.), 1. Sous-groupes d'indices finis dans SL(n, **Z**), *Bull. Amer. Math. Soc.*, **70** (1964), 385-392.

BASS (H.), MILNOR (J.), SERRE (J.-P.), 1. Solutions of the congruence subgroup problem for SL(n) ($n \geqslant 3$) and Sp($2n$) ($n \geqslant 2$), *Publ. Math. I.H.E.S.*, **33** (1967), 59-137.

BEHR (H.), 1. Endliche Erzeugbarkeit arithmetischer Gruppen über Functionenkörpern, *Inv. Math.*, **7** (1969), 1-32.

BERNSTEIN (I. N.), KAZDAN (D. A.), 1. The one dimensional cohomology of discrete groups, *Functional Anal. Appl.*, **4** (1970), 1-4.

BOREL (A.), 1. *Introduction aux groupes arithmétiques*, Paris, Hermann, 1969.

— 2. Density properties of certain subgroups of semisimple groups, *Ann. of Math.*, **72** (1960), 179-188.

BOREL (A.), TITS (J.), 1. Groupes réductifs, *Publ. Math. I.H.E.S.*, **27** (1965), 55-151.

—, — 2. Homomorphismes « abstraits » de groupes algébriques simples, *Ann. of Math.*, **97** (1973), 499-571.

CHEVALLEY (C.), 1. Deux théorèmes d'arithmétique, *J. of Math. Soc. Japan*, **3** (1951), 36-44.

— 2. Sur certains schémas de groupes semi-simples, *Sém. Bourbaki*, Exposé 219, New York, Benjamin, 1966.

— 3. Sur certains groupes simples, *Tohoku J. of Math.* (2), **7** (1955), 14-62.

DELAROCHE (C.), KIRILLOV (A.), Sur les relations entre l'espace dual d'un groupe et la structure de ses sous-groupes fermés (d'après D. A. Kazdan), *Sém. Bourbaki* 1967/68, Exposé 343, New York, Benjamin, 1969.

DEODHAR (V. V.), 1. *On central extensions of rational points of algebraic groups* (to appear).

DIEUDONNÉ (J.), 1. *La géométrie des groupes classiques*, Berlin, Springer-Verlag, 1955.

— 2. On the structure of unitary groups (II), *Amer. J. Math.*, **75** (1953), 665-678.

GARLAND (H.), 1. p-adic curvature and the cohomology of discrete subgroups of p-adic groups, *Ann. of Math.*, **97** (1973), 376-423.

GARLAND (H.), RAGHUNATHAN (M. S.), 1. Fundamental domains for lattices in (**R**-) rank one semisimple Lie groups, *Ann. of Math.*, **92** (1970), 279-326.

HARDER (G.), 1. Minkowskische Reductionstheorie über Functionenkörpern, *Inv. Math.*, **7** (1969), 33-54.

KAZDAN (D. A.), Connection on the dual space of a group with the structure of its closed subgroups, *Functional Anal. Appl.*, **1** (1967), 63-65.

KNESER (M.), 1. Normal subgroups of integral orthogonal groups in algebraic K-theory and its geometric applications, *Lecture Notes in Maths.* 108, Berlin, Springer-Verlag.

LANG (S.), 1. Algebraic groups over finite fields, *Amer. J. of Math.*, **78** (1956), 555-563.

MARGULIS (G. A.), 1. Discrete Groups of Motions of manifolds of non-positive curvature (en russe), *Proc. Intern. Congress of Math.*, Vancouver 1974, vol. 2, 21-34.

MATSUMOTO (M.), 1. Sur les sous-groupes arithmétiques des groupes semisimples déployés, *Ann. E.N.S.* (4), **2** (1969), 1-62.

MENNICKE (J.), 1. Finite factor groups of the unimodular group, *Ann. of Math.*, **81** (1965), 31-37.

— 2. Zur theorie der Siegelsche Modulgruppe, *Math. Ann.*, **159** (1965), 115-129.

MOORE (C. C.), 1. Group extensions of p-adic and adelic linear groups, *Publ. Math. I.H.E.S.*, **35** (1969), 5-70.

PLATONOV (V. P.), 1. The problem of strong approximation and the Kneser-Tits conjecture for algebraic groups, *Math. USSR-Izvestiya*, **3** (1969), 1139-1147.

— 2. Maximal arithmetic groups (to appear).

— 3. To appear.

RAGHUNATHAN (M. S.), 1. Cohomology of arithmetic subgroups of algebraic groups: I, *Ann. of Math.*, **86** (1967), 409-424.

— 2. Cohomology of arithmetic subgroups of algebraic groups: II, *Ann. of Math.*, **87** (1968), 279-304.

— 3. *Discrete Subgroups of Lie groups*, Berlin, Springer-Verlag, 1972.

— 4. A note on the Kneser-Tits conjecture for global fields (to appear).

SERRE (J.-P.), 1. Le problème des groupes de congruence pour SL_2, *Ann. of Math.*, **92** (1970), 489-527.
— 2. Cohomologie des groupes discrets, in *Prospects in Mathematics*, Princeton, 1970.
STEINBERG (R.), 1. Variations on a theme of Chevalley, *Pacific J. of Math.*, **9** (1959), 875-891.
— 2. Générateurs, relations et revêtements de groupes algébriques, *Colloque de Bruxelles* (1962), 113-127.
— 3. *Lectures on Chevalley groups*, Yale University, 1968.
TITS (J.), 1. Algebraic and abstract simple groups, *Ann. of Math.*, **80** (1964), 313-329.
— 2. Classification of algebraic semisimple groups, *Proc. Sympos. Pure Math.*, vol. 9, Amer. Math. Soc., 1966.
VASSERSTEIN (L. I.), 1. Subgroups of finite index in Spin groups of rank 2 (Russian), *Mat. Sbornik*, **75** (1968), 178-184.
WALL (G. E.), 1. The structure of a unitary factor group, *Publ. Math. I.H.E.S.*, **1** (1959).
WANG (S. P.), 1. The dual space of semisimple Lie groups, *Amer. J. Math.*, **91** (1969), 921-937.
WEIL (A.), 1. Discrete subgroups of Lie groups, II, *Ann. of Math.*, **75** (1962), 578-602.
— 2. *Adèles and algebraic groups*, Institute for Adv. Study, Princeton, 1961.
— 3. Remarks on the cohomology of groups, *Ann. of Math.*, **80** (1964), 149-157.

Tata Institute of Fundamental Research,
Bombay-5, India.

Manuscrit reçu le 20 avril 1974.
Révisé le 25 janvier 1976.