JOURNAL OF ALGEBRA 20, 250–270 (1972)

Free Subgroups in Linear Groups

J. TITS

Mathematisches Institut der Universität Bonn, West Germany

Received February 15, 1971

TO PROFESSOR RICHARD BRAUER, TO COMMEMORATE HIS SEVENTIETH BIRTHDAY, FEBRUARY 10, 1971

INTRODUCTION: STATEMENT OF THE MAIN RESULTS

The main purpose of this paper is to prove the following theorem which has been conjectured by H. Bass and J.-P. Serre:

THEOREM 1. *Over a field of characteristic* 0, *a linear group either has a non-abelian free subgroup or possesses a solvable subgroup of finite index.*

This is no longer true over a field of characteristic $\neq 0$, as is shown by the example of the full linear group over an infinite algebraic extension of a finite field. However, Theorem 2 shows that this example is in some sense universal.

THEOREM 2. *Let V be a vector space over a field k of characteristic different from* 0 *and let G be a subgroup of $GL(V)$. Then, the following three properties are equivalent.*

(i) *H contains no non-abelian free group.*

(ii) *G has a solvable normal subgroup R such that G/R is locally finite* (i.e., *every finite subset generates a finite subgroup*).

(iii) *G possesses a subgroup G' of finite index such that if V' denotes any composition factor of the $k[G']$-module V and k' the endomorphism ring of V'* (i.e., *the centralizer of G' in* $\mathrm{End}_k V'$), *then k' is a field and V' has a k'-basis with respect to which the matrices representing the elements of G' are scalar multiples* (*by elements of k'*) *of matrices whose entries are algebraic over the prime field of k.*

If the Zariski closure of the group in question in Theorem 1 is semisimple and $\neq \{1\}$, the theorem states that this group always contains a non-abelian free group. More precisely, we shall establish the

© 1972 by Academic Press, Inc.

THEOREM 3. *Let $\mathfrak{G}$ be a nontrivial semisimple algebraic group defined over a field k of characteristic 0 and let G be a (Zariski) k-dense subgroup of $\mathfrak{G}(k)$. Then G has a countable free subset F such that every element of F generates a k-connected subgroup of $\mathfrak{G}(k)$ and that every pair of elements of F generates a k-dense subgroup of $\mathfrak{G}(k)$.*

(A subset F of a group G is said to be *free* if the inclusion $F \to G$ extends to an injective homomorphism of the free group generated by F into G).

The corresponding result in characteristic not 0 is the

THEOREM 4. *Let $\mathfrak{G}$ be a nontrivial semisimple algebraic group defined over a field k of characteristic different from 0, let G be a k-dense subgroup of $\mathfrak{G}(k)$ and let k_a denote the algebraic closure of the prime field of k in k. Then, $\mathfrak{G}$ has a normal k-subgroup $\mathfrak{G}_1$ which is characterized by any one of the following three properties:*

(i) *$\mathfrak{G}_1$ is the smallest normal subgroup of $\mathfrak{G}$ such that every element of G has a power in $\mathfrak{G}_1$;*

(ii) *$\mathfrak{G}_1$ is the largest connected subgroup of $\mathfrak{G}$ which is the k-closure of a finitely generated subgroup of $\mathfrak{G}$;*

(iii) *$\mathfrak{G}_1$ is the smallest k-closed normal subgroup of $\mathfrak{G}$ such that $G/(G \cap \mathfrak{G}_1(k))$ contains no non-abelian free group.*

Furthermore:

(iv) *there exists an algebraic semisimple group $\mathfrak{G}_a$ defined over k_a and a k-isomorphism $(\mathfrak{G}/\mathfrak{G}_1) \to \mathfrak{G}_a$ mapping the canonical image of G in $(\mathfrak{G}/\mathfrak{G}_1)(k)$ into $\mathfrak{G}_a(k_a)$;*

(v) *the quotient $G/(G \cap \mathfrak{G}_1(k))$ is locally finite;*

(vi) *if $\mathfrak{G}_1 \neq \{1\}$, the group $G \cap \mathfrak{G}_1(k)$ has a countable free subset F such that every element of F generates a k-connected group and that every pair of elements of F generates a k-dense subgroup of $\mathfrak{G}_1(k)$.*

We now state a few immediate corollaries of Theorems 1 and 2.

COROLLARY 1. *A finitely generated linear group either contains a non-abelian free group or has a solvable subgroup of finite index.*

The following assertion, due to H. Zassenhaus [10], is a direct consequence of the preceding corollary and of Lemma 2 of [10]:

COROLLARY 2 (Zassenhaus). *Every noetherian linear group has a polycyclic subgroup of finite index.*

COROLLARY 3 (Platonov [6]). *Let G be a linear group over a field of characteristic* 0. *If there exists an integer n such that every finitely generated subgroup of G is generated by n elements, the group G has a solvable subgroup of finite index.*

(In [6], this is proved for any characteristic.)

COROLLARY 4. *A finitely generated linear group without nontrivial identities contains a non-abelian free group.*

(For related results which can also be deduced from the above theorems; cf. also Platonov [5]).

By a result of J. Milnor and J. Wolf (cf. [9, p. 421]), Corollary 1 also implies

COROLLARY 5. *The growth of a finitely generated linear group is either polynomial or exponential.*

The Corollaries 2 and 5 have been pointed out to me by H. Bass and the Corollaries 3 and 4 (and again Corollary 2) by V. P. Platonov. I am also indebted to H. Bass for several very useful discussions on the subject of this paper; in fact, some essential ingredients of the proofs—such as the idea of specializing to locally compact fields for instance—are for a large part due to him.

GENERAL CONVENTIONS

In this paper, k always denotes a (commutative) field. If V is a vector space over k and P its projective space, we denote by $GL(V)$ the automorphism group of V, by $PGL(V)$ or $PGL(P)$ the quotient of $GL(V)$ by its center and by $\mathfrak{GL}(V)$ and $\mathfrak{PGL}(V) = \mathfrak{PGL}(P)$ the corresponding k-algebraic groups (for instance, $\mathfrak{GL}(V)$ is defined by $\mathfrak{GL}(V)(l) = \mathrm{Aut}_l(V \otimes l)$ for every k-algebra l). If $\rho : \mathfrak{G} \to \mathfrak{H}$ is a k-homomorphism of algebraic groups, we also denote by ρ the homomorphism $\rho(l) : \mathfrak{G}(l) \to \mathfrak{H}(l)$ for any field extension l of k.

We shall often have to deal simultaneously with different topologies on a same set. *Except in Section* 3, *where another convention will be made* (cf. 3.1), the words "connected", "closure", "dense" etc., used without further specification, will always refer to the Zariski topology (or the topology it induces on sets of rational points). However, we shall also sometimes be more explicit and use such expressions as "k-connected", "k-closure", etc., even at places where the above general convention would dispense us of this precision. To understand this convention properly, it should also be remembered that if $\mathfrak{X}$ is a variety defined over k and if l is a field extension of k, the restriction of the l-topology to the set $\mathfrak{X}(k)$ coincides with the k-topology on this set.

1. A Criterion of Freedom

Proposition 1.1(*). *Let P be a set, I an index set, G a group operating on P on the left, $(G_i)_{i \in I}$ a family of subgroups generating G, $(P_i)_{i \in I}$ a family of subsets of P and p a point of $P - \bigcup_{i \in I} P_i$. Assume that for all $i, j \in I$ with $i \neq j$ and all $g \in G_i - \{1\}$, one has $g(P_j \cup \{p\}) \subset P_i$. Then G is the free product of the subgroups G_i $(i \in I)$.*

Indeed, let $n \in \mathbf{N}^*$ and, for $s \in \{1, \ldots, n\}$, let $i_s \in I$ and $g_s \in G_{i_s} - \{1\}$. Assume that $i_s \neq i_{s-1}$ for $s \neq 1$. Then one has, by induction on s, $(g_s g_{s-1} \cdots g_1)(p) \in P_{i_s}$. Hence $(g_n g_{n-1} \cdots g_1)(p) \neq p$, and $g_n g_{n-1} \cdots g_1 \neq 1$, Q.E.D.

Remark 1.2. Conversely, let G_i $(i \in I)$ be any system of groups and let G be their free product. For $i \in I$, let P_i be the set of all nonneutral elements of G whose expression as shortest possible words in the elements of the G_j's $(j \in I)$ starts with an element of G_i. Set $P = G$, $p = 1$, and let G operate on itself by left translations. Then, the hypotheses of the above proposition are fullfilled.

2. Linear Groups with Dense Torsion Sets

In this section, we slightly generalize a well-known theorem of Schur [4, p. 252]. For a large part, our arguments reproduce those of Burnside and Schur as they are found in [4], but for the convenience of the reader, we expose them in full, adapting them somewhat to our purpose.

2.1. In this section, A denotes a finite-dimensional simple k-algebra, l its center, $\lambda : A \to l$ the generic trace of A, considered as an l-algebra, $n = d^2$ the dimension of A over l, G a subgroup of the multiplicative group of all invertible elements of A such that G generates A linearly over k and T the set of all elements of finite order of G.

Lemma 2.2. *Let $(g_i)_{1 \leqslant i \leqslant n}$ be an l-basis of A consisting of elements of G. Then, there exists an l-basis $(e_i)_{1 \leqslant i \leqslant n}$ of A such that one has, for every subset U of G*

$$\bigcap_{i=1}^{n} U g_i^{-1} \subset \sum_{i=1}^{n} \lambda(U) \cdot e_i$$

and, in particular,

$$G \subset \sum_{i=1}^{n} \lambda(G) \cdot e_i .$$

(*) *Added in proof.* R. Lyndon has pointed out to the author that a similar criterion has been given by A. Macbeath [*Proc. Cambridge Philos. Soc.* **59** (1963), 555–558]. Cf. also R. Lyndon and J. Ullman [*Michigan Math. J.* **15** (1968), 161–166], where an observation similar to our Remark 1.2 is made.

It suffices to take for $(e_i)_{1 \leqslant i \leqslant n}$ the dual basis of the basis (g_i) with respect to the bilinear form $(x, y) \mapsto \lambda(xy)$ which is nondegenerate [3, §12, Proposition 9]. Indeed, if $g \in \bigcap_{i=1}^{n} Ug_i^{-1}$, one has

$$g = \sum_{i=1}^{n} \lambda(gg_i) \cdot e_i \subset \sum_{i=1}^{n} \lambda(U) \cdot e_i .$$

LEMMA 2.3. *Let k_0 be a finitely generated field and $m \in \mathbf{N}$. Then, there are only finitely many roots of unity satisfying an equation of degree m over k_0.*

Let h be the prime field of k_0, t a transcendence basis of k_0 over h, $m_1 = [k_0 : h(t)]$, ξ a root of unity satisfying an equation of degree m over k_0 and h' the algebraic closure of h in $k_0(\xi)$. Then, one has

$$[h(\xi) : h] \leqslant [h' : h] = [h'(t) : h(t)] \leqslant [k_0(\xi) : h(t)] \leqslant m \cdot [k_0 : h(t)] = mm_1 .$$

But the number of roots of unity with bounded degree over a prime field is known to be finite. This proves our assertion.

LEMMA 2.4. *Suppose that G is finitely generated. Then $\lambda(T)$ is finite.*

Let l_1 be a field-extension of l which splits the l-algebra A, set $A_1 = A \otimes_l l_1$ and let V be a simple A_1-module. We identify A with its canonical image $A \otimes 1$ in A_1 and choose an l_1-basis in V; thus, the elements x of G are represented by matrices, $\lambda(x)$ being the trace of the matrix representing x. Let l_2 be the subfield of l_1 generated by all entries of the matrices representing the elements of a finite generating set of G. Then, all elements of G are represented by matrices with coefficients in l_2. By 2.3, the characteristic roots of an element of T must belong to a fixed finite set, and our assertion follows readily.

PROPOSITION 2.5. *Suppose G is finitely generated and T is k-dense in G. Then, G is finite.*

As an l-vector space, A carries an l-topology, not to be confounded with the restriction to A of the l-topology of $A \otimes_k l$: the latter coincides with the k-topology on A, whereas the former is coarser. Anyway, T is also dense in G for the l-topology in question, and there is no loss of generality in assuming that $k = l$. By 2.4, $\lambda(T)$ is finite. Since λ is continuous, this implies that $\lambda(G) = \lambda(T)$, and our assertion follows from Lemma 2.2.

LEMMA 2.6. *Let $\mathscr{T}$ be a topology on A, making a topological ring out of it, X a (Zariski) dense relatively open subset of G and $\mathscr{H}$ a set of subgroups of G. Suppose that the subgroup of G generated by any element of $\mathscr{H}$ and any element of G also belongs to $\mathscr{H}$, and that, for all $H \in \mathscr{H}$, the $\mathscr{T}$-closure of $\lambda(H \cap X)$ is $\mathscr{T}$-compact. Then, the $\mathscr{T}$-closure of every element of $\mathscr{H}$ is $\mathscr{T}$-compact.*

Let g_i, e_i $(1 \leqslant i \leqslant n)$ be as in 2.2, set $Y = \bigcap_{i=1}^{n} Xg_i^{-1}$, and let $g_0 \in Y$. It suffices to show that if $H \in \mathscr{H}$ contains $g_0, g_1, \ldots, g_n$, then the $\mathscr{T}$-closure of H is compact. Setting $U = H \cap X$, we have, by 2.2, $H \cap Y \subset \sum_{i=1}^{n} \lambda(U) \cdot e_i$. Therefore, the $\mathscr{T}$-closure of $H \cap Y$ is compact. Then, our assertion follows from the fact that, H being k-compact and $H \cap Y$ being relatively open in it, H is the union of finitely many translates of $H \cap Y$.

Remark 2.7. The above lemma will be used only in the case where $\mathscr{T}$ is the discrete topology. However, to assume $\mathscr{T}$ discrete would not simplify the proof and the lemma may be useful in its given form. For instance, let A be locally compact Hausdorff for $\mathscr{T}$ and let D be the set of all elements of G which generate a $\mathscr{T}$-discrete infinite subgroup; then it follows from the lemma that if D is nowhere (Zariski) dense in G, the $\mathscr{T}$-closure of G is $\mathscr{T}$-compact (set $H = \{G\}$ and choose $X \subset G - D$; the $\mathscr{T}$-closure of $\lambda(X)$ is $\mathscr{T}$-compact because the elements of $\lambda(X)$ are sums of n topological roots of unity).

PROPOSITION 2.8. *Suppose that T contains a relatively open dense subset of G. Then G is locally finite (hence $G = T$). Suppose further that* char $k \neq 0$, *let V be a simple A-module and let k_a be the algebraic closure of the prime field of k in k. Then, V has a k-basis with respect to which the elements of G are represented by matrices with coefficients in k_a.*

The first assertion is an immediate consequence of the preceding lemma, taking for $\mathscr{T}$ the discrete topology, for X an open dense subset of G contained in T, and for $\mathscr{H}$ the set of all finitely generated subgroups of G; the $\mathscr{T}$-compactness (*i.e.*, the finiteness) of $\lambda(H \cap X)$ for $H \in \mathscr{H}$ is ensured by 2.4.

Let l_a be the algebraic closure of the prime field of k in l and let B (resp. B_1) be the subring of A generated by k_a (resp. l_a) and G. Since $G = T$, the characteristic roots of all elements of G are roots of unity; therefore $\lambda(G) \subset l_a$. By 2.2, it follows that $G \subset \sum_{i=1}^{n} l_a \cdot e_i$. For dimension reason, this implies that $B_1 = \sum_{i=1}^{n} l_a \cdot e_i$. Since G generates A over k, we have

$$[B : k_a] \geqslant [A : k] \geqslant [A : l] \cdot [l : k] \geqslant [B_1 : l_a] \cdot [l_a : k_a] \geqslant [B_1 : k_a].$$

Therefore, $B_1 = B$ and all the above inequalities are equalities. In particular, $[l : k] = [l_a : k_a]$ and $[B : k_a] = [A : k]$, which means that $A = B \otimes_{k_a} k$.

Now, suppose that char $k \neq 0$. Then, l_a is an algebraic extension of a finite field and B is a full matrix algebra over l_a. Denoting by V_a a simple B-module, we have

$$\dim_{k_a} V_a = d \cdot [l_a : k_a] = d \cdot [l : k] = \dim_k V,$$

hence $V = V_a \otimes_{k_a} k$, which proves our second assertion.

3. Attracting and Repulsing Points

3.1. *Notations.* In this section, k is a locally compact field endowed with an absolute value ω, V an $(n+1)$-dimensional vector space over k, and P the projective space of V. The unique extension of ω to any algebraic extension of the field k is also called ω. The join of two linear subspaces X, Y of P is denoted by $X \vee Y$; if $X \cap Y = \varnothing$ and $X \vee Y = P$, we denote by $\mathrm{proj}(X, Y)$ the mapping $\pi : P - X \to Y$ defined by $\{\pi(p)\} = (X \vee \{p\}) \cap Y$.

The spaces V and P are endowed with their topology deduced in the usual way from that of k: the topology of V is the product topology for some identification $V \simeq k^{n+1}$ and the topology of P is the quotient topology of that of $V - \{0\}$. *All through Section* 3, *the words "open", "neighborhood", "compact" etc. refer to the topologies in question here*; for the Zariski topology, we use the expressions "k-open", "k-neighborhood", etc. It is known that P is compact and that its linear subspaces are closed.

If $x = (x_1, \ldots, x_m)$ is an affine coordinate system in some k-affine space A (or, in particular, a linear coordinate system in a vector space), we denote by $d_x : A \times A \to \mathbf{R}$ the function defined by

$$d_x(p, q) = \sup_{1 \leqslant i \leqslant m} (\omega(x_i(p) - x_i(q))).$$

If $\xi = (\xi_0, \ldots, \xi_n)$ is a (linear) coordinate system in V, the equation $\xi_0 = 0$ defines a hyperplane H of P and $x_i = \xi_0^{-1}\xi_i$ can be viewed as a function on $P - H$. Any such system $x = (x_1, \ldots, x_n)$ will be called an *affine coordinate system in* P, and we shall denote by D_x its "domain of definition" $P - H$.

Let X be a set, Y a subset, $\delta : X \times X \to \mathbf{R}_+$ a function such that $\delta(p, q) = 0$ iff $p = q$ and $\alpha : Y \to X$ a mapping. Then, we denote by $\| \alpha \|_\delta$ the "norm of α with respect to δ", that is, the number

$$\sup_{\substack{p, q \in Y \\ p \neq q}} \frac{\delta(\alpha(p), \alpha(q))}{\delta(p, q)}$$

($= 0$ if card $Y \leqslant 1$).

Lemma 3.2. (i) *If x, y are two coordinate systems in P and if $K \subset D_x \cap D_y$ is a compact set, there exist strictly positive constants m, $M \in \mathbf{R}_+^*$ such that*

$$m \cdot d_x|_{K \times K} \leqslant d_y|_{K \times K} \leqslant M \cdot d_x|_{K \times K}.$$

(ii) *If x, y are two affine coordinate systems in an affine space K over k, there exist m, $M \in \mathbf{R}_+^*$ such that*

$$m \cdot d_x \leqslant d_y \leqslant M \cdot d_x$$

We shall prove both assertions simultaneously, setting $D_x = D_y = K$ in case (ii). It clearly suffices to show the existence of M such that the second inequality holds. For $1 \leqslant i \leqslant n$, the function $y_i|_{D_x \cap D_y}$ can be written as $\psi_i^{-1}\varphi_i$, where φ_i and ψ_i are linear combinations of 1 and the x_i's (in case (ii), $\psi_i = 1$). Therefore, we only have to prove that, if φ, ψ are two linear combinations of 1 and the x_i's and if $0 \notin \psi(K)$, then there exists a positive constant $M' \in \mathbf{R}_+$ such that

$$\omega\left(\frac{\varphi(p)}{\psi(p)} - \frac{\varphi(q)}{\psi(q)}\right) \leqslant M' \cdot d_x(p, q) \qquad \text{for} \quad p, q \in K,$$

or, equivalently (since $\omega \circ \psi$ is bounded away from 0 on K), that there exists $M'' \in \mathbf{R}_+$ such that

$$\omega(\varphi(p)\,\psi(q) - \psi(p)\,\varphi(q)) = \omega(\varphi(p)(\psi(q) - \psi(p)) + \psi(p)(\varphi(p) - \varphi(q)) \leqslant \\ \leqslant M'' \cdot d_x(p, q).$$

But it is easily verified that there exist constants M''' and M'''' in $\mathbf{R}_+$ such that

$$\omega(\varphi(p) - \varphi(q)) \leqslant M''' \cdot d_x(p, q) \qquad \text{and} \qquad \omega(\psi(p) - \psi(q)) \leqslant M'''' \cdot d_x(p, q).$$

Therefore, the existence of M'' follows from the fact that in case (i) both $\omega \circ \varphi$ and $\omega \circ \psi$ are bounded on K, and that in case (ii) ψ is constant (hence $\psi(p) - \psi(q) = 0$).

3.3. *Admissible distance functions.*

We shall say that a distance $d : P \times P \to \mathbf{R}_+$ is *admissible* if it defines a metric compatible with the topology of P and if, for every affine coordinate system x in P and every compact subset K of D_x, there exist $m, M \in \mathbf{R}_+^*$ such that

$$m \cdot d_x|_{K \times K} \leqslant d|_{K \times K} \leqslant M \cdot d_x|_{K \times K}.$$

If $k = \mathbf{R}$ or $\mathbf{C}$, any elliptic metric on P obviously has this property. To show that such a distance d also exists when ω is non-archimedian, let us decompose P in compact disjoint open subsets $K^{(j)}$ ($j = 1, \ldots, N$) such that each $K^{(j)}$ is contained in the domain of definition of some affine coordinate system $x^{(j)}$, set $d_j = d_{x^{(j)}}$ and $\Delta = \sup(\bigcup_j d_j(K^{(j)} \times K^{(j)}))$, and define $d : P \times P \to \mathbf{R}_+$ by

$$d(p, q) = \begin{cases} d_j(p, q) & \text{if} \quad (p, q) \in K^{(j)} \times K^{(j)} \\ \Delta & \text{if} \quad (p, q) \in K^{(j)} \times K^{(j')} \quad \text{with} \quad j \neq j'. \end{cases}$$

It readily follows from 3.2 that d is admissible.

In the sequel of Section 3, we choose once and for all an admissible distance d, we call norm the norm relative to d and we set $\| \| = \| \|_d$.

Remark 3.4. Let k' be a finite algebraic extension of k, $V' = V \otimes_k k'$ and P' the projective space of V'. Let us identify P with its canonical image in P'. The above definitions also apply to P' and it is clear that the restriction to $P \times P$ of an admissible distance $P' \times P' \to \mathbf{R}_+$ is admissible. It is not obvious that, conversely, every admissible distance on $P \times P$ can be extended "admissibly" to $P' \times P'$. But whenever an assertion to be proved does not depend on the special choice of d, we may assume, without loss of generality, that d extends to an admissible distance on $P' \times P'$.

LEMMA 3.5. *A projective transformation of P has finite norm.*

This is an immediate consequence of the fact that, if g is such a transformation, the distance function $(p, q) \mapsto d(gp, gq)$ is admissible.

3.6. *Attracting and repulsing subspaces.*

To every projective transformation $g \in PGL(P)$, we shall associate two linear subspaces $A(g)$ and $A'(g)$ of P defined as follows. Let $\bar{g}$ be a representative of g in $GL(V)$ and let $f(t) = \prod_{i=1}^{n} (t - \lambda_i) \in k[t]$ be its characteristic polynomial; set $\Omega = \{\lambda_i \mid \omega(\lambda_i) = \sup\{\omega(\lambda_j) \mid 1 \leqslant j \leqslant n\}\}$, $f_1(t) = \prod_{\lambda_i \in \Omega} (t - \lambda_i)$ and $f_2(t) = \prod_{\lambda_i \notin \Omega} (t - \lambda_i)$, so that $f(t) = f_1(t) \cdot f_2(t)$. It is easily seen that $f_1(t), f_2(t) \in k[t]$. Finally, we define $A(g)$ and $A'(g)$ as the subspaces of P which correspond to the kernels of $f_1(\bar{g})$ and $f_2(\bar{g})$, respectively. It is well known that V is the direct sum of these two kernels; therefore, $A(g) \cap A'(g) = \varnothing$ and $A(g) \vee A'(g) = P$. We call $A(g)$ (resp. $A(g^{-1})$) the *attracting* (resp. *repulsing*) *subspace* of g; if it is reduced to a point, we say that g has an *attracting* (resp. *repulsing*) *point*.

LEMMA 3.7. *Let V_1 be a vector space over k, x a (linear) coordinate system in V_1, g a linear transformation of V_1 and r a strictly positive real number.*

(i) *If g is semisimple*[1] *and if all its eigenvalues have an absolute value strictly smaller than 1, there exists an integer N such that $\| g^z \|_{d_x} < r$ for all $z > N$. Given a compact set $K \subset V_1$ and a neighborhood U of 0 there exists an integer N' such that $g^z K \subset U$ for all $z > N'$.*

(ii) *If there exists a set X generating V_1 linearly and such that $\lim_{z \to \infty} g^z p = 0$ for all $p \in X$, then all eigenvalues of g have an absolute value strictly smaller than 1.*

[1] In fact, the assertion is true for any $g \in GL(V)$; but the proof is somewhat simpler when g is assumed to be semisimple, and we shall not make use of the general case.

For the proof of (i), there is no loss of generality in assuming that all eigenvalues of g belong to k and, in view of 3.2 (ii), that the basis of the coordinate system x consists of eigenvectors of g. Then, $\| g \|_{d_x} = \sup \omega(\lambda)$, where λ runs through all eigenvalues of g. The first assertion of (i) readily follows from this fact, and the second one is an obvious consequence of the first.

To establish (ii), it suffices to observe that, with respect to a basis of V_1 contained in X, the matrix representing g^z, and hence the nonleading coefficients of its characteristic polynomial, tend to 0 as z tends to ∞, from which follows that, for sufficiently large z, all eigenvalues of g^z have an absolute value < 1.

LEMMA 3.8. *Let $g \in PGL(P)$, let $K \subset P$ be a compact set and let $r \in \mathbf{R}_+^*$.*

(i) *Suppose that g is semisimple*[2], *that $A(g)$ is a point and that $K \cap A'(g) = \varnothing$. Then, there exists an integer N such that $\| g^z |_K \| < r$ for all $z > N$; and for every neighborhood U of $A(g)$, there exists an integer N' such that $g^z K \subset U$ for all $z > N'$.*

(ii) *Let $\mathring{K}$ denote the interior of K in P. Assume that, for some $m \in \mathbf{N}$, one has $g^m K \subset \mathring{K}$ and $\| g^m |_K \| < 1$. Then, $A(g)$ is a point contained in $\mathring{K}$.*

(i) is an immediate consequence of 3.7 (i), viewing $P - A'(g)$ as a vector space whose point 0 is $A(g)$.

We now prove (ii). Upon replacing g by g^m, we may assume that $m = 1$. For $z \in \mathbf{N}$, $g^{z+1}K \subset g^z K \subset \mathring{K}$ and $\operatorname{diam} g^z K \leqslant \| g |_K \|^z \cdot \operatorname{diam} K$. Therefore, $\bigcap_{z \in \mathbf{N}} g^z K$ is a point p of $\mathring{K}$, clearly invariant by g. Let $\bar{g}$ be the representative of g in $GL(V)$ whose eigenvalue corresponding to p is 1. We must show that all other eigenvalues of $\bar{g}$ have an absolute value < 1. If the eigenvalue 1 of $\bar{g}$ has the multiplicity 1, there exists a hyperplane H of P stable by g and not containing p; then, if we consider $P - H$ as a vector space with $p = 0$, the transformation g, restricted to $P - H$, is a linear transformation whose eigenvalues are precisely the eigenvalues of $\bar{g}$ different from 1, and our assertion follows from 3.7 (ii). There remains to prove that the eigenvalue 1 of $\bar{g}$ cannot have a multiplicity greater than 1. Assume the contrary, and let V' be a 2-dimensional subspace of V stable by $\bar{g}$ and such that $\bar{g} |_{V'}$ is unipotent. Upon replacing V by V', P by the projective line P' image of $V' - \{0\}$ in P and K by $K \cap P'$, we may assume that V is 2-dimensional and that g is unipotent. But then, it is readily verified that the hypotheses of (ii) cannot be fulfilled.

LEMMA 3.9. *Let $g \in PGL(P)$ be semisimple, let $\bar{g} \in GL(V)$ be a representative of g, let Ω be the set of eigenvalues of $\bar{g}$ whose absolute value is maximum, let*

[2] As in 3.7 (i), this hypothesis is superfluous; cf. footnote [1].

K be a compact subset of $P - A'(g)$, set $\pi =$ proj$(A'(g), A(g))$, *and let U be a neighborhood of $\pi(K)$ in P.*

(i) *There exists an infinite set $N \subset \mathbf{N}$ such that*

$$\lim_{\substack{z \in N \\ z \to \infty}} (\lambda^{-1}\mu)^z = 1$$

for all $\lambda, \mu \in \Omega$.

(ii) *The set $\{\| g^z |_K \| \mid z \in \mathbf{N}\}$ is bounded.*

(iii) *If N is as in* (i), *$g^z K \subset U$ for almost all $z \in N$.*

In view of Remark 3.4, there is no loss of generality in assuming that all eigenvalues of $\bar{g}$ belong to k.

The assertion (i) is an immediate consequence of the fact that if $\lambda, \mu \in \Omega$, one has $\omega(\lambda^{-1}\mu) = 1$, from which follows that the closure in k of the group generated by $\lambda^{-1}\mu$ is compact.

Let $(e_i)_{0 \leqslant i \leqslant n+1}$ be a basis of V consisting of eigenvectors of $\bar{g}$, set $\bar{g}e_i = \lambda_i e_i$, and suppose the e_i's indexed in such a way that $\Omega = \{\lambda_0, \ldots, \lambda_m\}$ for some m. Thus, $A(g)$ and $A'(g)$ correspond, respectively, to the subspaces $W = ke_0 + \cdots + ke_m$ and $W' = ke_{m+1} + \cdots + ke_n$ of V. For $i \in \{0, \ldots, n\}$, let H_i denote the hyperplane of P corresponding to the hyperplane of V generated by the e_j's with $j \neq i$.

We now assume that (ii) does not hold and shall derive a contradiction. By hypothesis, there exist sequences (z_i), (p_i), (q_i) with $i \in \mathbf{N}$, $z_i \in \mathbf{N}$ and p_i, $q_i \in K$ such that

$$\lim_{i \to \infty} d(g^{z_i} p_i, g^{z_i} q_i) \cdot d(p_i, q_i)^{-1} = \infty. \tag{1}$$

Upon passing to subsequences, we may assume that (p_i) tends to a point p in K. Since $d(P \times P)$ is bounded, (1) then implies that (q_i) also tends to p. We have $\bigcap_{i=0}^{m} H_i = A'(g)$; therefore, some H_i $(0 \leqslant i \leqslant m)$ does not contain p and there is no loss of generality in assuming that $p \notin H_0$ and that p_i, $q_i \notin H_0$ for all $i \in \mathbf{N}$. We now consider $P - H_0$ as a vector space, taking the canonical image of e_0 for 0, and let x denote the coordinate system in P corresponding, in the way described in 3.1, to the linear coordinate system with basis (e_i) in V. The restriction g_0 of g to $D_x = P - H_0$ is a linear transformation with eigenvalues $\lambda_0^{-1}\lambda_i$ $(1 \leqslant i \leqslant n)$, and the basis of x consists of eigenvectors of g_0. Hence

$$\| g_0^z \|_{d_x} = \sup\{\omega(\lambda_0^{-1}\lambda_i)^z\} \leqslant 1.$$

Since d is admissible, this contradicts (1) and (ii) is proved.

We proceed to the proof of (iii). Upon changing the choice of $\bar{g}$, we may assume that $\lambda_0 = 1$. Let $N \subset \mathbf{N}$ be as in (i). We have

$$\lim_{\substack{z \in N \\ z \to \infty}} \lambda_i^z = \begin{cases} 1 & \text{for} \quad 0 \leqslant 1 \leqslant m, \\ 0 & \text{for} \quad m+1 \leqslant i \leqslant n; \end{cases}$$

therefore,

$$\lim_{\substack{z \in N \\ z \to \infty}} \bar{g}^z$$

is the projection on W with kernel W', and

$$\lim_{\substack{z \in N \\ z \to \infty}} g^z p = \pi(p) \qquad \text{for all} \quad p \in P - A'(g). \tag{2}$$

From (ii) and (2), it follows that every point $p \in K$ has a neighborhood X_p such that $g^z X_p \subset U$ for almost all $z \in N$. Since K is compact, it is covered by finitely many X_p and (iii) follows.

LEMMA 3.10. *Let $G \subset PGL(P)$ be a group leaving no proper nonempty linear subspace of P invariant, and let P_1, P_2 be two linear subspaces of P, with $P_1 \neq \varnothing$ and $P_2 \neq P$. Then, the set $\{g \in G \mid gP_1 \not\subset P_2\}$ is relatively k-open in G and not empty.*

The first assertion follows from the obvious (and well-known) fact that the set $\{h \in PGL(P) \mid hP_1 \subset P_2\}$ is k-closed in $PGL(P)$. Let $p \in P_1$. The subspace of P spanned by Gp is stable under G and must therefore coincide with P. Hence, there exists $g \in G$ such that $gp \notin P_2$ and, a fortiori, $gP_1 \not\subset P_2$.

PROPOSITION 3.11. *Let G be a k-connected subgroup of $PGL(P)$ leaving no proper nonempty linear subspace of P invariant. Suppose that G possesses at least one semisimple element g such that $A(g^{-1})$ is a point. Then, the set*

$$X = \{x \in G \mid A(x) \textit{ and } A(x^{-1}) \textit{ are points}\}$$

is k-dense in G.

Let g be as in the statement of the proposition, let $\bar{g}$ and Ω be as in 3.9 and let $N \subset \mathbf{N}$ be as in 3.9 (i). Upon replacing N by a suitable subset, we may assume that g^N is k-connected.

From 3.10 and the k-irreducibility of G, it follows that the set

$$\{x \in G \mid A(g) \not\subset x \cdot A'(g^{-1})\} \cap \{x \in G \mid x \cdot A(g) \not\subset A'(g^{-1})\}$$

is k-open and dense in G. Let h be an element of it and set

$$B = (h \cdot A'(g)) \vee (h \cdot A(g) \cap A'(g^{-1})),$$
$$B' = A'(g) \vee (A(g) \cap h \cdot A'(g^{-1})),$$

and

$$U = \{x \in G \mid x \cdot A(g^{-1}) \not\subset B \text{ and } h \cdot A(g^{-1}) \not\subset x \cdot B'\}.$$

Because of the conditions set on h, one has $B \neq P$ and $B' \neq P$, and it follows again from 3.10 that U is k-open and dense in G. Set $\pi = \operatorname{proj}(A'(g), A(g))$ and $\pi' = \operatorname{proj}(h \cdot A'(g), h \cdot A(g))$ (cf. 3.1), and let $u \in U$. One has $u \cdot A(g^{-1}) \not\subset h \cdot A'(g)$ and $\pi'(u \cdot A(g^{-1})) \not\subset A'(g^{-1})$. Similarly, $u^{-1}h \cdot A(g^{-1}) \not\subset A'(g)$ and $\pi(u^{-1}h \cdot A(g^{-1})) \not\subset h \cdot A'(g^{-1})$. Let Y (resp. Y') be a compact neighborhood of $A(g^{-1})$ (resp. $u^{-1}h \cdot A(g^{-1})$) such that $u \cdot Y \cap h \cdot A'(g) = \varnothing$ and $\pi'(u \cdot Y) \cap A'(g^{-1}) = \varnothing$ (resp. $Y' \cap A'(g) = \varnothing$ and $\pi(Y') \cap h \cdot A'(g^{-1}) = \varnothing$) and let Z (resp. Z') be a compact neighborhood of $\pi'(u \cdot Y)$ (resp. $\pi(Y')$) in P whose intersection with $A'(g^{-1})$ (resp. $h \cdot A'(g^{-1})$) is empty. By 3.9 (ii) and 3.5, there exists a strictly positive real number r such that

$$\| hg^z h^{-1} u \mid_Y \| < r \qquad \text{and} \qquad \| g^z \mid_{Y'} \| < r$$

for all $z \in \mathbf{N}$. If $\bar{h}$ is a representative of h in $GL(V)$, the representative $\bar{h}\bar{g}\bar{h}^{-1}$ of hgh^{-1} has the same eigenvalues as $\bar{g}$. Therefore, it follows from 3.9 (iii) that, for almost all $z \in N$,

$$hg^z h^{-1} u \cdot Y \subset Z \qquad \text{and} \qquad g^z \cdot Y' \subset Z'. \tag{1}$$

By 3.8 (i), one also has, for almost all $z \in \mathbf{N}$,

$$\| g^{-z} \mid_Z \| < r^{-1}, \qquad g^{-z} \cdot Z \subset \mathring{Y} \tag{2}$$

$$\| hg^{-z}h^{-1} \mid_{Z'} \| < r^{-1} \cdot \| u^{-1} \|^{-1}, \quad hg^{-z}h^{-1} \cdot Z' \subset u \cdot \mathring{Y}', \tag{3}$$

where $\mathring{Y}$ (resp. $\mathring{Y}'$) denotes the interior of Y (resp. Y') in P. Let N' be the set of all $z \in N$ such that (1), (2) and (3) hold simultaneously. For all $z \in N'$, one has

$$g^{-z}hg^z h^{-1}u \cdot Y \subset \mathring{Y}, \qquad \| g^{-z}hg^z h^{-1}u \mid_Y \| < 1,$$
$$u^{-1}hg^{-z}h^{-1}g^z \cdot Y' \subset \mathring{Y}', \qquad \| u^{-1}hg^z h^{-1}g^{-z} \mid_{Y'} \| < 1;$$

hence, by 3.8 (ii),

$$g^{-z}hg^z h^{-1}u \in X.$$

Since the set $N - N'$ is finite, $g^{N'}$ is k-closed in g^N. Therefore, the k-closure $\bar{X}$ of X in G contains $g^{-z}hg^z h^{-1}u$ for all $z \in N$. This being true for all $u \in U$ and U being k-dense in G, $\bar{X}$ also contains $g^{-z}hg^z h^{-1}G = G$ (for $z \in N$), Q.E.D.

PROPOSITION 3.12. *Let Y be a finite set of semisimple*[3] *elements of $PGL(P)$. Suppose that for all $x \in Y$, $A(x)$ and $A(x^{-1})$ are one-point sets and that, for $x, y \in Y$ with $x \neq y$, one has*

$$A(x) \cup A(x^{-1}) \subset P - A'(y) - A'(y^{-1}).$$

Then, there exists $M \in \mathbf{N}$ such that, for all $m \in \mathbf{N}$ greater than M, the set $Y^m = \{x^m \mid x \in Y\}$ is free in $PGL(P)$.

Let $p \in P - \bigcup_{x \in Y} (A(x) \cup A'(x) \cup A(x^{-1}) \cup A'(x^{-1}))$ and let $(U_x, U_x')_{x \in Y}$ be a system of subsets of $P - \{p\}$ with the following properties:

U_x (resp. U_x') is a compact neighborhood of $A(x)$ (resp. $A(x^{-1})$);
for $x, y \in Y$ with $x \neq y$, one has

$$U_x \cup U_x' \subset P - A'(y) - A'(y^{-1}).$$

(Such a system obviously exists.) Then, it follows from 3.8 (i) that there exists $M \in \mathbf{N}$ such that, for all $m \in \mathbf{N}$ with $m \geq M$, the hypotheses of Proposition 1.1 are satisfied if one sets $I = Y$, $G = PGL(P)$, $G_x = \{x^{mz} \mid z \in \mathbf{Z}\}$ and $P_x = U_x \cup U_x'$. Since the groups G_x are infinite cyclic, 1.1 implies our assertion and the proposition is proved.

4. Proof of the Theorems

LEMMA 4.1. *Let k be a finitely generated field and let $t \in k^*$ be an element of infinite order. Then, there exists a locally compact field k' endowed with an absolute value ω and a homomorphism $\sigma : k \to k'$ such that $\omega(\sigma(t)) \neq 1$.*

Indeed, let k_a be the algebraic closure of the prime field of k in k, set $k_0 = k_a$ if char $k = 0$ and $k_0 = k_a(t)$ otherwise, and let ω_0 be an absolute value on k_0 such that $\omega_0(t) \neq 1$ if $t \in k_0$ (such an absolute value is well known to exist; cf., e.g., [8, p. 77, Theorem 8]). Now, let T be a transcendence basis of k over k_0 such that $t \in T$ if $t \notin k_0$, and let $\hat{k}_0$ be the completion of k_0 with respect to ω_0. Since the transcendence degree of $\hat{k}_0$ over k_0 is infinite, there exists an injective mapping $\sigma_0 : T \to \hat{k}_0$ such that $\sigma_0(T)$ is algebraically free over k_0 and that $\omega_0(\sigma_0(t)) \neq 1$ if $t \in T$. Let us also denote by σ_0 the field homomorphism $k_0(T) \to \hat{k}_0$ which extends σ_0 and is the identity on k_0. Finally, since k is a finite algebraic extension of $k_0(T)$, there exists a finite algebraic extension k' of $\hat{k}_0$ and a field homomorphism $\sigma : k \to k'$ extending σ_0. If ω denotes the unique extension of ω_0 to k', the requirement of the lemma is fulfilled.

[3] As in 3.7 and 3.8, the hypothesis that the elements of Y are semisimple is in fact superfluous.

LEMMA 4.2. *Let V be a k-vector space and let H be a finitely generated subgroup of $GL(V)$. Then, there exists $m \in \mathbf{N}^*$ such that, for every $h \in H$, the group generated by h^m is k-connected.*

Let us choose a k-basis in V. Upon replacing k by the field generated by the coefficients of the matrices representing the elements of a finite generating set of H, and V by the vector space over this field generated by the given basis of V, we may assume that k is finitely generated. Set $d = \dim V$, let $m' \in \mathbf{N}^*$ be such that every root of unity satisfying an equation of degree $d!$ over k is an m'-th root of unity (cf. 2.3), let p denote the characteristic exponent of k and set $m = m' \cdot p^d$. We shall show that, for $g \in GL(V)$, the group $g^{m\mathbf{Z}}$ generated by g^m is k-connected. If $p \neq 1$, the element $g' = g^{p^d}$ is semisimple and $g^{m\mathbf{Z}} = g'^{m'\mathbf{Z}}$. If $p = 1$ and if $g = g_s g_u = g_u g_s$ with g_s semisimple and g_u unipotent, one knows that the k-closure of $g^{m\mathbf{Z}}$ in G is the product of the k-closures of $g_s^{m\mathbf{Z}} = g_s^{m'\mathbf{Z}}$ and $g_u^{m\mathbf{Z}}$, and that the latter is connected. In both cases, it suffices, therefore, to prove that if $s \in GL(V)$ is semisimple, then the group $s^{m'\mathbf{Z}}$ is k-connected. Let T be a k-torus of $GL(V)$ containing s and let χ be any character of T vanishing on the connected component of 1 in the group $s^{\mathbf{Z}}$; then, $\chi(s)$ is a root of unity which is a monomial (with positive or negative exponents) in the characteristic roots of s. But these characteristic roots generate an extension of degree at most d of k. Hence, $\chi(s^{m'}) = \chi(s)^{m'} = 1$ and $s^{m'}$ belongs to the connected component of 1 in $s^{\mathbf{Z}}$. This implies that $s^{m'\mathbf{Z}}$ is the connected component in question, and our assertion is proved.

PROPOSITION 4.3. *Let $\mathfrak{G}$ be a nontrivial semisimple algebraic group defined over a field k, let G be a finitely generated dense subgroup of $\mathfrak{G}(k)$ and let G' be a dense subgroup of G. Then, there exists a dense subset S of G' and an open dense subset $\mathfrak{U}$ of $\mathfrak{G} \times \mathfrak{G}$ with the following properties:*

(i) *for $s \in S$, the group $s^{\mathbf{Z}}$ is connected;*

(ii) *if $s \in S$ and $z \in \mathbf{Z} - \{0\}$, then $s^z \in S$;*

(iii) *if F is a finite subset of S such that $(s, s') \in \mathfrak{U}$ for all $s, s' \in F$ with $s \neq s'$, then, there exists $M \in \mathbf{N}$ such that the set $F^z = \{s^z \mid s \in F\}$ is free in G' for every integer $z \geqslant M$.*

We first notice that if S and $\mathfrak{U} \subset \mathfrak{G} \times \mathfrak{G}$ satisfy the conditions (ii), (iii) and if m is as in 4.2 (for $G = H$), then $S^m = \{s^m \mid s \in S\}$ and $\mathfrak{U}$ satisfy (i), (ii), (iii). Therefore, it suffices to prove the existence of S and $\mathfrak{U}$ satisfying (ii) and (iii).

Upon extending k if necessary, we may assume that $\mathfrak{G}$ possesses a k-rational nontrivial absolutely irreducible linear representation. Let $\rho : \mathfrak{G} \to \mathfrak{G}\mathfrak{L}(V)$ be such a representation. If $S_1 \subset \rho(G')$ and $\mathfrak{U}_1 \subset \rho(\mathfrak{G}) \times \rho(\mathfrak{G})$ have the properties (ii), (iii) with respect to the groups $\rho(\mathfrak{G})$ and $\rho(G')$, and if we set $\mathfrak{U}_1' = \mathfrak{U}_1 - \{(g, g) \mid g \in \rho(\mathfrak{G})\}$, then $S = \rho^{-1}(S_1)$ and $\mathfrak{U} = (\rho \times \rho)^{-1}(\mathfrak{U}_1')$ have these properties with respect to $\mathfrak{G}$ and G'. Therefore, there is no loss of generality in assuming that ρ is an immersion and in identifying $\mathfrak{G}$ with $\rho(\mathfrak{G})$.

The same argument as in the proof of lemma 4.2 also allows us to assume — at least provisionally—that the field k is finitely generated (notice that this restriction of the field of definition does not change the Zariski topology on G, as was recalled in the "general conventions"). By 2.5, applied to the subgroup G of the simple k-algebra End V (which is linearly generated by G because we assumed ρ to be absolutely irreducible), the group G' possesses only finitely many elements of finite order, hence possesses at least one semisimple element g of infinite order. Upon extending k, we may assume that all eigenvalues of g belong to k. At least one of them, call it λ, is not a root of unity. Applying 4.1, we may then extend k to a locally compact field (thus k ceases to be finitely generated) endowed with an absolute value ω such that $\omega(\lambda) \neq 1$. Let d be the number of eigenvalues of g with maximum absolute value. Since $\det g = 1$, we have $d \not< \dim V$. Upon extending again k and replacing ρ be a suitable composition factor of its d-th tensor power, we may assume that $d = 1$ (the new extension of k might be necessary to preserve the absolute irreducibility of ρ). Let G' operate on the projective space P of V. The relation $d = 1$ means that g has an attracting point in P (cf. 3.6). By 3.11, it follows that the set S of all elements of G' which have an attracting point and a repulsing point in P is dense in G'; furthermore, it obviously has the property (ii).

Let us now define the open set $\mathfrak{U} \subset \mathfrak{G} \times \mathfrak{G}$ as follows: if $\bar{k}$ denotes an algebraic closure of k and V^* the dual of V, on which we let $\mathfrak{G}$ operate by the contragradient of the representation ρ, a point $(x, y) \in \mathfrak{G}(\bar{k}) \times \mathfrak{G}(\bar{k})$ belongs to $\mathfrak{U}(k)$ if and only if

(1) x and y are semisimple and have the same number of distinct eigenvalues as the generic element of $\mathfrak{G}$;

(2) if v (resp. v^*) is an eigenvector of x (resp. y) in $V \otimes \bar{k}$ (resp. $V^* \otimes \bar{k}$) corresponding to a simple eigenvalue, then $v^*(v) \neq 0$.

That these properties define an open set in $\mathfrak{G} \times \mathfrak{G}$ is easily seen. To show that $\mathfrak{U}$ is not empty, let $x, y \in \mathfrak{G}(\bar{k})$ have property (1) and let $\bar{k}v_1, \ldots, \bar{k}v_r$ (resp. $\bar{k}v_1^*, \ldots, \bar{k}v_r^*$) be all eigenspaces of x in $V \otimes \bar{k}$ (resp. of y in $V^* \otimes \bar{k}$) corresponding to simple eigenvalues of x (resp. y). Because of the absolute irreducibility of the representation ρ, the functions $\varphi_{ij} : \mathfrak{G}(k) \to \bar{k}$ $(i, j \in \{1, \ldots, r\})$ defined by $\varphi_{ij}(u) = v_i^*(uv_j)$ are not identically zero. Now, if $u \in G(k)$ is such that all $\varphi_{ij}(u)$ are different from 0, one has $(uxu^{-1}, y) \in \mathfrak{U}$, hence $\mathfrak{U} \neq \varnothing$. Since S and $\mathfrak{U}$ have the property (iii) by virtue of 3.12, the proof is complete.

4.4. In this subsection, all algebraic groups are defined over some algebraically closed field k, and an algebraic group and its group of k-rational points are denoted by the same symbol.

PROPOSITION. *Let G be a semisimple algebraic group, T a maximal torus of G and S a subtorus whose centralizer in G is T. Then, the union of all closed connected proper subgroups of G containing S is nowhere dense in G.*

Let $\mathcal{N}$ (resp. $\mathcal{Z}$) stand for "normalizer (resp. centralizer) in G". Let X be the union of all proper connected subgroups of G containing T; there are only finitely many such subgroups (cf. [1, 3.4]); therefore X is nowhere dense in G. Set $\mathcal{S}_0 = \{nSn^{-1} \mid n \in \mathcal{N}(T)\}$ and let $\mathcal{S}$ be the set of all proper subtori of T generated by a subset of $\mathcal{S}_0$ containing S; since $\mathcal{N}(T)/T$ is finite, so is the set $\mathcal{S}_0$ and hence also the set $\mathcal{S}$. For $S' \in \mathcal{S}$, let $Y_{S'}$ denote the closure of the union of all conjugates of S' in G. It is known that every regular function on T invariant by the Weyl group extends to a regular function on G invariant by inner automorphisms; since there obviously exists a nonzero regular function on T invariant by the Weyl group and vanishing on S', it follows that $Y_{S'}$ is nowhere dense in G, and the same holds for the set $Y = \bigcup_{S' \in \mathcal{S}} Y_{S'}$.

We shall show that every closed connected proper subgroup H of G containing S is contained in $X \cup Y$; this will prove the proposition. We may of course assume that H is maximal among the connected proper subgroups of G. If H is parabolic, the centralizer of S in H must contain a maximal torus of G; since $\mathcal{Z}(S) = T$, this means that $T \subset H$, hence $H \subset X$. If H is not parabolic, it is reductive [2, 3.3] and even semisimple because, if its connected center C were not trivial, one would have $H = \mathcal{Z}(C)$ (by the maximality assumption) which is impossible since $\mathcal{Z}(C)$ is properly contained in a parabolic subgroup [1, 4.15]. Let, therefore, H be semisimple. Then, $T' = H \cap T$ is a maximal torus of H. Since $N' = \mathcal{N}(T') \cap H$ normalizes T', it also normalizes $\mathcal{Z}(T') = T$. The torus $S' \in \mathcal{S}$ generated by all nSn^{-1} with $n \in N'$ is a subtorus of T' normalized by N'. It is easy to see that this implies that S' is a maximal torus of some normal subgroup of H. Since, furthermore, $\mathcal{Z}(S') \cap H = T'$, one must have $S' = T'$. But the union of the conjugates of T' in H is dense in H; therefore, $H \subset Y_{T'} \subset Y$, which completes the proof.

Remark. It can be shown that the above proposition remains valid if one replaces the condition $T = \mathcal{Z}(S)$ by the weaker hypothesis that S is not contained is any proper normal subgroup of G.

4.5. *Proof of the Theorems* 3 *and* 4.

Let $\mathfrak{G}$ be a semisimple group defined over k and let G be a dense subgroup of $\mathfrak{G}(k)$. Let $\mathfrak{G}_1$ be the smallest connected normal subgroup of $\mathfrak{G}$ containing a power (with exponent $\neq 0$) of every element of G. We shall show—this is clearly sufficient—that the assertions (ii) to (vi) of Theorem 4 hold regardless of the characteristic of k, and that

(vii) if char k $= 0$, one has $\mathfrak{G}_1 = \mathfrak{G}$.

Proof of (iv), (v) *and* (vii). Upon replacing $\mathfrak{G}$ by $\mathfrak{G}/\mathfrak{G}_1$ and G by its canonical image in $(\mathfrak{G}/\mathfrak{G}_1)(k)$, we may assume that $\mathfrak{G}_1 = \{1\}$, which also means that G is a torsion group. Let $(\rho_i : \mathfrak{G} \to \mathfrak{GL}(V_i))$ $(i = 1,\dots, m)$ be a system of k-irreducible k-rational linear representations of G such that the direct sum ρ of the ρ_i's is an immersion of $\mathfrak{G}$ in $\mathfrak{GL}(\coprod_{i=1}^{m} V_i)$ (the existence of such a system of representations immediately follows from the representation theory as it is exposed for instance in [7]). If char $k = 0$, $\rho_i(G)$ possesses an abelian subgroup of finite index, by Schur's theorem [4, p. 258]; since it is dense in the semisimple group $\rho_i(G)$, this means that $\rho_i(\mathfrak{G}) = \{1\}$ for all i, hence $\mathfrak{G} = \{1\}$ and (vii) is proved (as well as (iv) and (v) in this case).

If char k $\neq 0$, each space V_i has a basis B_i with respect to which all elements of $\rho_i(G)$ are represented by matrices with coefficients in the algebraic closure k_a of the prime field of k in k (cf. 2.8). The union of all B_i's is a basis of $\coprod_{i=1}^{m} V_i$ and if we denote by V_a the k_a-vector space it generates, we have (with obvious identifications) $\rho(G) \subset \mathfrak{GL}(V_a)(k_a)$. The closure $\mathfrak{G}_a$ of $\rho(G)$ in $\mathfrak{GL}(V_a)$, which is an algebraic group defined over k_a, and the representation ρ, considered as a k-isomorphism of $\mathfrak{G}$ onto $\mathfrak{G}_a$, satisfy the requirements of (iv). Finally, (v) is an obvious consequence of (iv).

Proof of (ii). For dimension reason, there exists a largest connected subgroup $\mathfrak{G}_2$ of $\mathfrak{G}$ which is the closure of a finitely generated subgroup of G. Since G is dense in $\mathfrak{G}$, $\mathfrak{G}_2$ is normal in $\mathfrak{G}$. Let G_2 be a finitely generated subgroup of G, dense in $\mathfrak{G}_2$. For any $g \in G$, there exists $m \in \mathbf{N}^*$ such that g^m generates a connected group, which implies that $g^m \in \mathfrak{G}_2$. Therefore, $\mathfrak{G}_1 \subset \mathfrak{G}_2$. On the other hand, the image G_2' of G_2 in $(\mathfrak{G}/\mathfrak{G}_1)(k)$ is finitely generated, hence finite by (v). Since G_2 is dense in $\mathfrak{G}_2$, which is connected, G_2' is connected. Therefore, $G_2' = \{1\}$ and $\mathfrak{G}_2 \subset \mathfrak{G}_1$, which establishes (ii).

Proof of (vi). We may of course assume that $\mathfrak{G} = \mathfrak{G}_1$ and, by (ii), that G is finitely generated. We first show that

(vi′) every subgroup G' of G which is dense in $G(k)$ has a free subset $\{x, x'\}$ consisting of two semisimple regular elements such that the groups $x^{\mathbf{Z}}, x'^{\mathbf{Z}}$ are connected and that the free group they generate is dense in $\mathfrak{G}(k)$.

Indeed, let S, $\mathfrak{U}$ be as in 4.3, let $\mathfrak{U}_1$, $\mathfrak{U}_2$ be the two projections of $\mathfrak{U}$ in $\mathfrak{G}$ and let $s \in S \cap \mathfrak{U}_1 \cap \mathfrak{U}_2$ be semisimple and regular. Further, let s' be a regular semisimple element of S such that $(s, s') \in \mathfrak{U}$, $(s', s) \in \mathfrak{U}$ and that no proper connected closed subgroup of G contains both s and s'; such an s' exists because all conditions we are imposing on it are satisfied in open dense subsets of G (for the last condition, this follows from 4.4). Since $s^{\mathbf{Z}}$ and $s'^{\mathbf{Z}}$ are connected, the group generated by s and s' is connected and hence dense in $\mathfrak{G}(k)$. Let $m \in \mathbf{N}^*$ be such that $\{s^m, s'^m\}$ is free (cf. 4.3 (iii)) and set $x = s^m$ and $x' = s'^m$. Since $x^{\mathbf{Z}}$ (resp. $x'^{\mathbf{Z}}$) is of finite index in the connected group $s^{\mathbf{Z}}$ (resp. $s'^{\mathbf{Z}}$) the groups $x^{\mathbf{Z}}$ and $s^{\mathbf{Z}}$ (resp. $x'^{\mathbf{Z}}$ and $s'^{\mathbf{Z}}$) have the same closure; this implies that x, x' are regular and that the group they generate is dense in $\mathfrak{G}(k)$, which proves (vi′).

Upon replacing G by a dense, finitely generated free subgroup—we just showed that such a subgroup exists—we may assume that G itself is free and finitely generated. Let G' be the commutator subgroup of G (which is dense in $\mathfrak{G}(k)$ and is a free group with countably many generators), let $\{x, x'\} \subset G'$ be as in (vi′) and let $\mathscr{F}$ be the set of all free subsets X of G' containing $\{x, x'\}$ and such that every element of X is regular, semisimple, and generates a connected group and that every pair of elements of X generates a dense subgroup of $\mathfrak{G}(k)$. Let F be a maximal element of $\mathscr{F}$, which exists by Zorn's lemma. We shall show that F is infinite. Suppose that it is not, let L be the group it generates, let $y \in G' - F$ be such that $F \cup \{y\}$ is free and let $m \in \mathbf{N}$ be such that, for every element z of the group generated by $F \cup \{y\}$, $z^{m\mathbf{Z}}$ is connected (4.2). The set $(yL)^m = \{(yu)^m \mid u \in L\}$ is dense in $\mathfrak{G}(k)$; therefore, by 4.4, there exists $u \in L$ such that $(yu)^m$ is regular, semisimple and generates with each element of F a dense subgroup of $\mathfrak{G}(k)$. The set $F \cup \{yu\}$ is free, hence also $F \cup \{(yu)^m\}$. Since $(yu)^m \notin F$, this contradicts the maximality assumption on F, and proves (vi).

Proof of (iii). Clearly, $G/(G \cap \mathfrak{G}_1(k))$ contains no nontrivial free group. So that we only have to show that if $\mathfrak{H}$ is a k-closed normal subgroup of $\mathfrak{G}$ and if $G/(G \cap \mathfrak{H}(k))$ has no non-abelian free subgroup, then $\mathfrak{G}_1 \subset \mathfrak{H}$. We may of course assume that $\mathfrak{H}$ is connected and, upon passing to the quotient by $\mathfrak{G}_1 \cap \mathfrak{H}$, that $\mathfrak{G}_1 \cap \mathfrak{H} = \{1\}$. Then, the canonical mapping $G \to G/(G \cap \mathfrak{H}(k))$ is injective on $G \cap \mathfrak{G}_1(k)$, and it follows from (vi) that $\mathfrak{G}_1 = \{1\}$.

4.6. *Proof of Theorem* 1. Let $G \subset GL(V)$ be a linear group over k, of characteristic 0, $\mathfrak{G}$ the closure of G in $\mathfrak{GL}(V)$, $\mathfrak{G}^0$ the connected component of 1 in $\mathfrak{G}$, and $\mathfrak{R}$ the radical of $\mathfrak{G}^0$. If $\mathfrak{G}^0 = \mathfrak{R}$, $G \cap \mathfrak{G}^0(k)$ is a solvable subgroup of finite index in G. Otherwise, $\mathfrak{G}^0/\mathfrak{R}$ is a nontrivial semisimple group, the canonical image of $G \cap \mathfrak{G}^0(k)$ in $(\mathfrak{G}^0/\mathfrak{R})(k)$ contains a non-abelian free group (by Theorem 3) and so does also G. The theorem is proved.

4.7. *Proof of Theorem* 2. The implication (ii) $\Rightarrow$ (i) is obvious.

To show that (iii) implies (i), we may assume that $G = G'$. Let R denote the normal subgroup of G which consists of all elements inducing in each composition factor V' of the $k[G]$-module V a scalar multiplication by an element of the corresponding endomorphism ring k'. Then, R is solvable and the hypotheses of (iii) imply that G/R is locally finite. The assertion (i) follows.

There remains to prove that (i) implies (ii) and (iii). Let us, therefore, assume that G contains no non-abelian free group, let $\mathfrak{G}$ denote the closure of G in $\mathfrak{GL}(V)$ and let $\mathfrak{R}$ be the radical of the connected component of 1 in $\mathfrak{G}$. Then, $G \cap \mathfrak{R} = R$ is a solvable normal subgroup in G and it follows from Theorem 4 that G/R, which is the canonical image of G in $\mathfrak{G}/\mathfrak{R}$, is locally finite. This establishes (ii).

To prove (iii), we may, upon replacing G by a subgroup of finite index, assume that G is k-connected. We shall then show that (iii) holds for $G' = G$. To this effect, it clearly suffices to consider the case, where $V = V'$ (*i.e.*, V is a simple $k[G]$-module) and where k is the center of the ring k' of $k[G]$-endomorphisms of V (just replace k by this center; the connectedness of G is clearly unaffected). Under these conditions, k' is a central division algebra, from which follows that, if $\bar{k}$ denotes an algebraic closure of k, the $\bar{k}[G]$-module $V \otimes \bar{k}$ is a direct sum of isomorphic simple modules. Therefore, the closure $\mathfrak{G}$ of G in $\mathfrak{GL}(V)$ is a reductive group and its connected center is either $\{1\}$ or the (algebraic) group of scalar multiplications. Let G_1 and $\mathfrak{G}_1$ denote the commutator groups of G and $\mathfrak{G}$, respectively; $\mathfrak{G}_1$ is also the closure of G_1 in $\mathfrak{GL}(V)$. From what we have just seen, it follows that, as a subgroup of $\mathfrak{GL}(V)$, $\mathfrak{G}_1$ is a k-irreducible linear (algebraic) group; therefore, V is also simple as a $k[G_1]$-module. Since $\mathfrak{G}_1$ is semisimple and G_1 contains no non-abelian free group, it follows from Theorem 4 that G_1 is a torsion group and from 2.8 that V possesses a basis B with respect to which the elements of G_1 are represented by matrices with coefficients in the algebraic closure k_a of the prime field of k in k. Clearly, $k' = \mathrm{End}_{G_1} V$ has a k-basis consisting also of endomorphisms represented by matrices with coefficients in k_a. Since k_a is an algebraic extension of a finite field, there is no non-commutative division algebra over it, and we must have $k' = k$.

We now endow the group $\mathfrak{PGL}(V)$ with the natural k_a-structure associated with the basis B, and call $\mathfrak{PG}$ the canonical image of $\mathfrak{G}$ in $\mathfrak{PGL}(V)$. The group $\mathfrak{PG}$ is semisimple and the canonical images PG and PG_1 of G and G_1 in $\mathfrak{PG}(k)$ are dense. Since PG contains no non-abelian free group, it follows from Theorem 4 that there exists an algebraic group $\mathfrak{PG}_a$ defined over k_a and a k-isomorphism $\sigma : \mathfrak{PG}_a \to \mathfrak{PG}$ such that $PG \subset \sigma(\mathfrak{PG}_a(k_a))$. The inverse image of PG_1 under σ is dense in $\mathfrak{PG}_a(k_a)$ and is mapped by σ into $\mathfrak{PGL}(V)(k_a)$. This shows that the homomorphism $\mathfrak{PG}_a \to \mathfrak{PGL}(V)$ obtained by composing σ and the canonical inclusion $\mathfrak{PG} \to \mathfrak{PGL}(V)$ is defined over k_a. But then, $PG \subset \sigma(\mathfrak{PG}_a(k_a)) \subset \mathfrak{PGL}(V)(k_a)$, which means that the matrices representing the elements of G are scalar multiples of matrices with coefficients in k_a, Q.E.D.

Remark 4.8. It would of course be possible to prove the Theorems 1 and 2 more directly, without passing through the Theorems 3 and 4. Notice, in particular, that the density assertions of these theorems (and hence the Proposition 4.4) have not been used in 5.7 and 5.8.

REFERENCES

1. A. BOREL ET J. TITS, Groupes réductifs, *Publ. Math. I. H. E. S.* **27** (1965), 55–150.
2. A. BOREL ET J. TITS, Éléments unipotents et sous-groupes paraboliques de groupes réductifs, I, *Invent. Math.* **12** (1971), 95–104.
3. N. BOURBAKI, Algèbre, Chap. 8 : Modules et anneaux semi-simples, "Actualités Sci. Indust." 1261, Hermann, Paris, 1958.
4. C. W. CURTIS AND I. REINER, Representation theory of finite groups and associative algebras, Interscience, New York, 1962.
5. V. P. PLATONOV, Lineinye gruppy s toždestvennymi sootnošenijami, *Dokl. Akad. Nauk BSSR* **11** (1967), 581–583.
6. V. P. PLATONOV, O probleme Malčeva, *Mat. Sbornik* **79** (121) (1969), 621–624.
7. J. TITS, Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque, *J. Reine Angew. Math.*, **247** (1971), 196–220.
8. A. WEIL, Basic number theory, "Grundlehren der Math. Wiss." 144, Springer, Berlin, 1967.
9. J. A. WOLF, Growth of finitely generated solvable groups and curvature of Riemannian manifolds, *J. Differential Geom.* **2** (1968), 421–446.
10. H. ZASSENHAUS, On linear Noetherian groups, *J. Number Theory* **1** (1969), 70–89.