§1. Proof of Theorem B

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **29 (1983)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **08.08.2024**

The condition on H and the second alternative hold either if K is algebraically closed or if $K = \mathbf{R}$ and $G(K)$ is compact. In that last case, $\chi(G(K), H(K)) = \chi(G(K)/H(K))$ by [10], and Theorem A follows.

I wish to thank D. Sullivan for having sent me a preprint of [8], which was the starting point of the present paper, and D. Kazdhan and G. Prasad for having pointed out two errors in a previous proof of Theorem B for $\mathbf{SL}_n$.

Notation and conventions. In the sequel, G is a connected semi-simple algebraic group over some groundfield, and p the characteristic of the groundfield. For unexplained notation and notions on linear algebraic groups, we refer to [1]. In particular, in such a group, the word "torus" is meant as in [1], i.e., refers to a connected linear algebraic group which is isomorphic to a product of $\mathbf{GL}_1$'s. In a compact group however it means a topological torus (product of circle groups).

If H is a group, and A, B are subsets of H, then

$$^{B}A = \{bab^{-1} \mid a \in A, b \in B\},\ N_H(A) = \{h \in H \mid hAh^{-1} = A\},$$
$$\mathrm{Tr}_H(A, B) = \{h \in \mathrm{H} \mid h.A.h^{-1} = B\}.$$

If Γ acts on a space X, the *isotropy group* of Γ at x is

$$\Gamma_x = \{\gamma \in \Gamma \mid \gamma \cdot x = x\}.$$

We recall that a morphism $f : X \to Y$ of irreducible algebraic varieties is *dominant* if its image is not contained in any proper algebraic subvariety. If so, then Im f contains a Zariski-dense open subset of Y [1: AG 10.2]. If the groundfield has characteristic zero, then, since f is separable, the differential of f has maximal rank on some non-empty Zariski open subset of X [1: AG, 17.3].

§1. Proof of Theorem B

Let m be an integer $\geqq 2$. Let $w = w(X_1, ..., X_m)$ be a non-trivial element in the free group $F(X_1, ..., X_m)$ on m letters X_i, i.e., a non-trivial reduced word in the X_i's, with non-zero integral exponents [3: I.81, Prop. 7]. Then given a group H, the word w defines a map $f_w : H^m \to H$ by the rule

$$(1) \qquad f_w(\{h_1, ..., h_m\}) = w(h_1, ..., h_m), \qquad (h_i \in H\,;\ 1 \leqq i \leqq m).$$

If H is an algebraic group, then f_w is a morphism of algebraic varieties which is defined over any field of definition for H. In the case where $H = G$ we want to prove

THEOREM 1. *The map* $f_w : G^m \to G$ *is dominant.*

This is a geometric statement. To prove it, we shall identify G with $G(\Omega)$, where Ω is some universal field. We have then to prove that $f_w(G(\Omega)^m)$ is Zariski-dense in $G(\Omega)$.

The Zariski closure Z of $\mathrm{Im} f_w$ is irreducible (since G^m is) and is invariant under conjugation, since $\mathrm{Im} f_w$ is obviously so. Since the semi-simple elements of G are Zariski-dense, and all conjugate to elements in some fixed maximal torus T, it suffices to show that $Z \supset T$.

a) We first consider the case where $G = \mathbf{SL}_n (n \geqq 2)$. Let us prove that $G(\Omega)$ contains a Zariski-dense subgroup H, no element of which, except for the identity, has an eigenvalue equal to one. This statement and its proof were directly suggested by [8].

One can find an infinite field L of the same characteristic as Ω over which there exists a central division algebra D of degree n^2. We may for example take for L a local field (see e.g. XIII, §3, Remarque p. 202 in [14]). We may assume $L \subset \Omega$. Let $\mathscr{D}^1$ be the algebraic group over L whose points in a commutative L-algebra M are the elements of reduced norm one in $D \otimes_L M$. Then $\mathscr{D}^1$ is an anisotropic L-form of $\mathbf{SL}_n$. Of course, D splits over Ω and the isomorphism $D \otimes_L \Omega = \mathbf{M}_n(\Omega)$ yields an isomorphism of $\mathscr{D}^1(\Omega)$ onto $G(\Omega)$. We let H be the image of $D^1 = \mathscr{D}^1(L)$ under such an isomorphism. The group H is Zariski-dense since L is infinite. The fact that any $h \in H - \{1\}$ has no eigenvalue equal to one is then proved as in [8]: the element $h - 1$ is a non-zero element of D, hence is invertible, hence has no eigenvalue zero and therefore h has no eigenvalue one. This proves our assertion. Let p_0 be the characteristic exponent of Ω ($p_0 = 1$ if char $\Omega = 0$ and $p_0 =$ char Ω otherwise). If $p_0 = 1$, then H consists of semi-simple elements; if not, then $h^q (q = p_0^{n-1})$ is semi-simple for any $h \in G$. Let $f_w^q : G^m \to G$ be defined by $f_w^q(g) = f_w(g)^q$. Then $f_w^q(H)$ consists of semi-simple elements. Let Z_q be the Zariski closure of $\mathrm{Im} f_w^q$. Since $x \mapsto x^q$ is dominant, we have shown:

(*) *Let* V *be the set of semi-simple elements in* $G(\Omega)$ *which have no eigenvalue equal to one. Then* $\{1\} \cup (V \cap \mathrm{Im} f_w^q)$ *is Zariski-dense in* Z_q.

We now prove the theorem for $\mathbf{SL}_n (n \geqq 2)$ by induction on n. It suffices to show that f_w^q is dominant and, for this, that $Z_q \supset T$. Let $n = 2$. The group $\mathbf{SL}_2$ has dimension three and the conjugacy classes of non-central elements have dimension two. If $Z_q \neq G$, then $\dim Z_q \leqq 2$ and Z_q is contained in the union of the set U of unipotent elements of G and of finitely many conjugacy classes of semi-simple elements $\neq 1$. Those are closed, disjoint from U. Since Z_q is irreducible and contains 1, it should then be contained in U. On the other hand,

$Z_q \neq \{1\}$ since G contains non-commutative free subgroups, as follows from [17] (see also Remark 1 below). We then get

$$\{1\} \underset{\neq}{\subset} Z_q \subset U ,$$

but this contradicts (*), whence the Theorem for $\mathbf{SL}_2$.

Assume now $n > 2$ and our assertion proved up to $n - 1$. This implies in particular that Z_q contains all subgroups of G isomorphic to $\mathbf{SL}_{n-1}$, hence that $Z_q \cap T$ contains the subtori of T of codimension one consisting of the elements of T which have at least one eigenvalue equal to one. Call Y their union. Assume that $Z_q \cap T \neq T$. Then we may write $Z_q \cap T = Y \cup Y'$, where Y' is a proper algebraic subset of T not containing any irreducible component of Y. Let Q be the Zariski-closure of the set ${}^G Y'$ of conjugates of elements of Y'. We claim that $Y \not\subset Q$. In fact, the subsets Y and Y' are stable under the Weyl group $W = N(T)/T$ (which may be identified with the group of permutations of the basic vectors of Ω^n). Let $J \subset \Omega[T/W]$ be the ideal of Y'. The algebra $\Omega[T/W]$ is isomorphic, under the restriction mapping, to the algebra S of regular class functions on G [16]. Let J' be the ideal of S corresponding to J under this isomorphism and R the variety of zeroes of J'. We have then $Q \subset R$, but $Y \not\subset R$, whence $Y \not\subset Q$.

The difference $Y' - (Y \cap Y')$ contains a conjugate of every semi-simple element of Z_q not having any eigenvalue equal to one. Therefore (*) implies that $Z_q = \{1\} \cup Q$. But this contradicts the fact that $Y \not\subset Q$. Therefore $T \subset Z_q$ and the theorem is proved for $\mathbf{SL}_n$.

b) In the general case we use induction on dim G. If $\mu : G' \to G$ is an isogeny, then the theorem for G' implies it for G, hence we may assume G to be simply connected. It is then a direct product of almost simple groups, whence also a reduction to the case where G is almost simple. By a), it suffices to consider the case where G is not isomorphic to $\mathbf{SL}_n$ for any n. But then it contains a proper connected semi-simple subgroup H of maximal rank (see lemma below). By induction Z contains a maximal torus of H, hence one of G, and therefore T.

We have just used the following lemma:

LEMMA 1. *Assume G to be almost simple, and not isogeneous to $\mathbf{SL}_n$ for any n. Then G contains a proper connected semi-simple subgroup of maximal rank.*

For convenience, we may assume G to be isomorphic to its adjoint group. Let $\Phi = \Phi(G, T)$ be the root system of G with respect to T and $\Delta = \{\alpha_1, ..., \alpha_l\}$ a basis of Φ. Since G is adjoint, Δ is also a basis of the group $X^*(T)$ of rational characters of T. Let d be the dominant root and write

$$d = \sum_{i=1}^{i=l} d_i \alpha_i .$$

The d_i's are strictly positive integers. By assumption, Φ is not of type $\mathbf{A}_m$ for any m. Therefore, by the classification of root systems, one of the d_i's is prime (see e.g. [4]). Say $d_1 = q$, with q prime. Let Ψ be the set of elements in Φ which, when expressed as linear combination of simple roots, have either 0 or $\pm q$ as coefficient of α_1. This is a closed set of roots. In fact, it is a root system with basis $\alpha_2, \ldots, \alpha_l$ and $-d$ [2]. We claim that there exists a closed connected subgroup H of G containing T with root system Ψ.

Let first $q \neq$ char. K. Then there is an element $t \in T$, $t \neq 1$, such that

$$d(t) = \alpha_i(t) = 1 , \qquad (i = 2, \ldots, l) .$$

It has order q, and Ψ is the set of roots which are equal to one on t. Then the identity component of the centralizer of t satisfies our condition.

Let now $q =$ char. Ω. Let $\mathfrak{t}$ be the Lie algebra of T and $\mathfrak{u}$ be the subspace of $\mathfrak{t}$ which annihilates the differentials $d\alpha_i$ of the roots α_i $(i = 2, \ldots, l)$. It is one dimensional and does not annihilate $d\alpha_1$ (since, as recalled above, Δ is a basis of $X^*(T)$, hence the $d\alpha_i (1 \leqq i \leqq l)$ form a basis of the dual space to $\mathfrak{t}$). Of course, the differential of any $\lambda \in X^*(T)$ which is divisible by q in $X^*(T)$ is identically zero on $\mathfrak{t}$. It follows then that

$$\Psi = \{\alpha \in \Phi \mid d\alpha(\mathfrak{u}) = 0\} .$$

Let $\mathfrak{g}$ be the Lie algebra of G and

$$\mathfrak{g}_\alpha = \{x \in \mathfrak{g} \mid \mathrm{Ad}\, t(x) = \alpha(t) \cdot x (t \in T)\} , \qquad (\alpha \in \Phi) ,$$

be the (1-dimensional) eigenspace of T corresponding to α[1, §14]. The previous relation implies that

$$\mathfrak{z}_\mathfrak{g}(\mathfrak{u}) = \mathfrak{t} \oplus \bigoplus_{\alpha \in \psi} \mathfrak{g}_\alpha .$$

By [1: §14] the Lie algebra of the centralizer

$$Z_G(\mathfrak{u}) = \{g \in G \mid \mathrm{Ad}\, g(x) = x, (x \in \mathfrak{u})\} ,$$

of $\mathfrak{u}$ in G is equal to $\mathfrak{z}_\mathfrak{g}(\mathfrak{u})$; therefore $Z_G(\mathfrak{u})$ is a semi-simple subgroup satisfying our conditions.

Remarks. 1) We have used [17] only for $\mathbf{SL}_2(\Omega)$, but it is possible to bypass [17] in this case and make our proof, and the whole paper, independent of [17].

We need only to prove that $\mathbf{SL}_2(\Omega)$ contains a non-commutative free subgroup F. If Ω has characteristic zero, we may take any torsion-free subgroup of $\mathbf{SL}_2(\mathbf{Z})$. Let now $p = \text{char}\,\Omega$ be >0. Then, by the arithmetic method, using division quaternion algebras over global fields, we can construct a discrete cocompact subgroup of $\mathbf{SL}_2(L)$, where L is a local field of characteristic p (cf. A. Borel-G. Harder, *Crelle J. 298* (1978), 53-74). The latter has a torsion-free subgroup F of finite index (H. Garland, *Annals of Math.* 97 (1973), 375-423) which is then free, since it acts freely on a tree, namely the Bruhat-Tits building of $\mathbf{SL}_2(L)$.

2) For any non-zero $n \in \mathbf{Z}$, the power map $g \mapsto g^n$ is dominant (because it is surjective on any maximal torus [1 : 8.9]), hence Theorem 1 is obvious if the sum of the exponents of one letter in the word w is not zero. (See [11] for a similar remark in the context of compact groups.)

3) If U and V are non-empty open subsets in a connected algebraic group H, then $H = U \cdot V$ [1: 1.3]. It follows then from Theorem 1 that if w, w' are two words in two letters, say, then the map $G^4 \to G$ defined by

$$f(g_1, g_2, g_3, g_4) = w(g_1, g_2) \cdot w'(g_3, g_4),$$

is surjective. For instance, every element of $G(\Omega)$ is the product of two commutators. However, the map f_w itself is not always surjective; for instance $x \mapsto x^2$ is not surjective in $\mathbf{SL}_2(\mathbf{C})$, as pointed out in [11].

4) If $K = \mathbf{C}$, then Theorem 1 implies that Im f_w contains a dense open set in the ordinary topology. If G is defined over $\mathbf{R}$, then Theorem 1 also shows that $f_w(G(\mathbf{R}))$ contains a non-empty subset of $G(\mathbf{R})$ which is open in the ordinary topology. However it may not be dense. For instance, it is pointed out in [11] that for $\mathbf{SU}_2$, the image of the map defined by $[x^2, yxy^{-1}]$ omits a neighborhood of -1; however this map is surjective in $\mathbf{SO}_3$.

It seems that little is known about the image of f_w, even over $\mathbf{R}$ or $\mathbf{C}$. A general fact however is that the commutator map is surjective in any compact connected semi-simple Lie group [9].

§2. Free subgroups with strongly regular elements

1. In the sequel, K is a field of infinite transcendence degree over its prime field. We shall need the following lemma:

LEMMA 2. *Let X be an irreducible unirational K-variety. Let L be a finitely generated subfield of K containing a field of definition of X, and $V_i (i \in \mathbf{N})$ a sequence of proper irreducible algebraic subsets of X defined over an*