FREE GROUPS IN LINEAR GROUPS

L'Enseignement Mathématique, t. 29 (1983), p. 129-144

FREE GROUPS IN LINEAR GROUPS

by Pierre DE LA HARPE

This paper is an introduction to a theorem due to J. Tits [T]. It owes very much to conversations with N. A'Campo. The theorem is the following: let n be an integer, $n \geqslant 2$, and let Γ be a subgroup of $GL(n, \mathbf{C})$; then either Γ contains a subgroup of finite index which is solvable, or Γ contains a free group on two generators. This is a deep result, and Tits' proof has two important ingredients: a skilfull use of an easy combinatorial lemma, and the theory of affine algebraic groups defined over various fields (not necessarily algebraically closed, not necessarily subfields of $\mathbf{C}$). Our aim below is to prove a few special cases of the theorem, for which the first ingredient only is essentially sufficient.

We describe examples of free subgroups of $GL(n, \mathbf{C})$ in section 1, and then comment on the statement of Tits' theorem. Section 3 is a digression on hyperbolic geometry, introducing section 4 where the theorem is first proved for subgroups of $GL(2, \mathbf{R})$ and then discussed for $GL(2, \mathbf{C})$. Finally, we indicate a proof of the following particular case of Tit's theorem: let Γ be a subgroup of $GL(n, \mathbf{C})$ such that

(i) any subgroup of finite index in Γ is not solvable, and acts irreducibly on $\mathbf{C}^n$,

(ii) Γ contains a diagonalisable matrix with at least two eigenvalues of distinct moduli;

then Γ contains non abelian free groups. This relies on an important lemma 1, for which we refer to section 3 of [T], and on easy arguments given in section 5 below. Y. Guivarch' has announced a new proof of that lemma 1, which consequently holds under weaker hypothesis; modulo this we indicate how (ii) can be replaced by

(ii') Γ is not relatively compact in $GL(n, \mathbf{C})$.

In particular, it is enough to assume

(ii'') Γ is discrete in $GL(n, \mathbf{C})$.

1. Early examples

Infinite groups were first considered around 1870, among others by C. Jordan (in 1868 according to [B]) and by F. Klein (who proposed his Erlangen programme in 1872). Examples of free groups associated to geometrical situations were known shortly afterwards. We shall describe three of them, though without trying to recover any flavour of the original description. We need for the first two a criterium used in many occasions by Klein, but formulated as follows much later. (See §III.12 in [LS] for references, and [Hm] for related criteria.)

KLEIN'S CRITERIUM (= table-tennis lemma). *Let* G *be a group acting on a set* S, *let* Γ_1, Γ_2 *be two subgroups of* G *and let* Γ *be the subgroup they generate; assume that* Γ_1 *contains at least three elements. Assume that there exist two non empty subsets* S_1, S_2 *in* S *with* S_2 *not included in* S_1 *such that* $\gamma(S_2) \subset S_1$ *for all* $\gamma \in \Gamma_1 - \{1\}$ *and* $\gamma(S_1) \subset S_2$ *for all* $\gamma \in \Gamma_2 - \{1\}$. *Then* Γ *is isomorphic to the free product* $\Gamma_1 * \Gamma_2$.

Proof. Let us check that any non empty reduced word w spelled out with letters from $(\Gamma_1 - \{1\}) \cup (\Gamma_2 - \{1\})$ does not act as the identity on S. In case one has $w = \alpha_1\beta_1\alpha_2\beta_2 \dots \alpha_k$ with $\alpha_1, \dots, \alpha_k \in \Gamma_1 - \{1\}$ and $\beta_1, \dots, \beta_{k-1} \in \Gamma_2 - \{1\}$, then $w(S_2) \subset S_1$ and $w \neq 1$. If $w = \beta_1\alpha_2 \dots \alpha_k\beta_k$, let $\alpha \in \Gamma_1 - \{1\}$; then $\alpha w \alpha^{-1} \neq 1$ as above and $w \neq 1$. If $w = \alpha_1\beta_1 \dots \alpha_k\beta_k$, let $\alpha \in \Gamma_1 - \{1, \alpha_1^{-1}\}$ and argue with $\alpha w \alpha^{-1}$. The last case $w = \beta_1\alpha_2 \dots \beta_{k-1}\alpha_k$ is similar. □

Example 1 : a subgroup of the modular group. Let $G = GL(2, \mathbf{C})$ be acting by fractional linear transformations on the Riemann sphere $\mathbf{C} \cup \{\infty\}$. Then $g = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ generate a free group in G.

Indeed, consider first the subgroup Γ_1 of G generated by g, the subgroup $\Gamma_2 = \{1, j\}$ where $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and the group Γ generated by Γ_1 and Γ_2. Consider also

$$S_1 = \{ z \in \mathbf{C} \mid |\mathrm{Re}(z)| > 1 \}$$
$$S_2 = \{ z \in \mathbf{C} \mid |z| < 1 \}$$

and check with Klein's criterium that $\Gamma = \Gamma_1 * \Gamma_2$. As $h = jgj$, the claim follows.

The claim is also a particular case of Poincaré's theorem for fundamental polygons of Fuchsian groups [Mt], going back to 1882; it is sometimes attributed to Sanov (1947). One may check that g and h generate with -1 the group

$$\{ \gamma \in SL(2, Z) \mid \gamma \equiv 1 \ (\mathrm{mod}\ 2) \}$$

which is discrete in G; see [L], VII.6.C.

The problem to know for which $\lambda \in \mathbf{C}$ the matrices $\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ generate a free [respectively discrete] subgroup of $SL(2, \mathbf{C})$ has received considerable attention; see e.g. [LU2] and [Ig] [respectively [L], [MS1], [Mi], [N] and [Ro]].

Example 2: Schottky groups. Let $G = PGL(2, \mathbf{C})$ be acting as above on $\mathbf{C} \cup \{\infty\}$. Consider four circles $C_1, \ldots, C_4$ in $\mathbf{C}$ with nonoverlapping interiors and choose g_1 [respectively g_2] in G mapping the exterior of C_1 [resp. C_2] onto the interior of C_3 [resp. C_4]. Then g_1 and g_2 generate a free group in G.

This follows again from Klein's criterium with S_1 [resp. S_2] the interiors of C_1 and C_3 [resp. of C_2 and C_4]. The group generated by g_1 and g_2 is discontinuous on a non empty open subset of $\mathbf{C} \cup \{\infty\}$; see [FK], page 191.

Hausdorff's example in the group of rotations. Consider a half turn rotation g and a one third turn rotation h of $\mathbf{R}^3$, the angle between the axes being $\pi/4$ (almost any other angle would do). Then g and h generate in $SO(3)$ a group isomorphic to $(\mathbf{Z}/2\mathbf{Z}) * (\mathbf{Z}/3\mathbf{Z})$, so that $ghgh^2$ and gh^2gh generate a free group in $SO(3)$.

Indeed, consider coordinates such that

$$g = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \qquad h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

For any integer $k > 0$ and for any sequence $n_1, \ldots, n_k$ with $n_j \in \{1, 2\}$, check inductively that there exist even integers $p_1, \ldots, p_5$ and odd integers $q_1, \ldots, q_4$ with

$$h^{n_1} g h^{n_2} g \ldots h^{n_k} g = 2^{-k} \begin{pmatrix} p_1 & p_2 & p_3\sqrt{3} \\ q_1 & p_4 & q_2\sqrt{3} \\ q_3\sqrt{3} & p_5\sqrt{3} & q_4 \end{pmatrix}$$

As an odd integer is not zero, such a word cannot represent the identity rotation. Any reduced word in g and h (besides 1 and g) is either as above, say w, or of one of the forms w^{-1}, wg, gw. It follows that the group generated by g and h is isomorphic to $(\mathbf{Z}/2\mathbf{Z}) * (\mathbf{Z}/3\mathbf{Z})$.

In 1914, this example allowed Hausdorff to show that there does not exist any finitely additive rotation-invariant measure defined on all subsets of the sphere $\mathbf{S}^2$. See [H], and [DE] for subsequent history. While discussing this, let us mention the following open problem (brought to my attention by M. Keane): does there exist a finitely additive probability measure on the Borel subsets of $\mathbf{S}^2$, vanishing on meagre sets, invariant under rotations? (The answer for countably additive measures is no, and follows from the unicity of Haar measure on a compact group; see e.g. §9 in [Wi].)

Remark. Let G be a connected real Lie group. Then G contains at least one subgroup isomorphic to the free group on two generators F_2 if and only if G is not solvable, as results from standard Lie theory as follows.

To check the non trivial implication, we assume that G is not solvable, so that G contains a semi-simple subgroup S by a theorem of Levi and Mal'cev. Consider a Cartan decomposition $\mathfrak{s} = \mathfrak{k} \oplus \mathfrak{p}$ of the Lie algebra of S. If $\mathfrak{k} \neq \{0\}$, root theory shows that the semi-simple compact algebra $\mathfrak{k}$ contains a subalgebra isomorphic to $\mathfrak{su}(2)$, so that G contains a subgroup isomorphic to one of $SU(2)$, $SO(3)$. If $\mathfrak{k} = \{0\}$, then $\mathfrak{s}$ is split and root theory again shows that $\mathfrak{s}$ contains a copy of $\mathfrak{sl}(2, \mathbf{R})$, so that G contains a subgroup isomorphic to a covering of $PSL(2, \mathbf{R})$. In all cases, examples above show that G contains a copy of F_2.

So, let G be a connected Lie group containing a copy of F_2. For $w \in F_2 - \{1\}$ and $g, h \in G$, let $w(g, h)$ be the element of G obtained when replacing the two generators of F_2 by g and h in w. Then

$$X_w = \{ (g, h) \in G \times G \mid w(g, h) = 1 \}$$

has empty interior (think of analytic continuation). It follows from Baire's theorem that the set $G \times G - \bigcup X_w$ (union over $w \in F_2 - \{1\}$) of those $(g, h) \in G \times G$ such that g and h generate a free group is dense and has full measure in $G \times G$ [E]. (If G is moreover semi-simple, it follows from a note by Kuranishi and from Tits' theorem that there exist $g, h \in G$ generating a subgroup of G which is both free and dense [Ku].)

2. Statement of Tits' theorem

Recall that, given a group Γ, its derived group $D\Gamma$ is the subgroup generated by elements of the form $ghg^{-1}h^{-1}$ and that Γ is *solvable* if $D(\dots D(\Gamma)\dots) = \{1\}$ for sufficently many D's. We say that Γ is *almost solvable* (other people say virtually solvable) if it contains a solvable subgroup of finite index. For example, groups of triangular matrices are solvable and non abelian free groups are not almost solvable. By "free group", we mean hereafter *non abelian free group.*

A *linear group* over a field **K** is a group which has at least one faithful finite dimensional representation over **K**, namely a group isomorphic to a subgroup of $GL(n, \mathbf{K})$ for some n. Groups are far from being all linear, even under the hypothesis of finite generation. Famous examples of non linear groups are the quotients F_2/F_2^m for m odd and large enough, where F_2^m is the subgroup of the free group F_2 generated by elements of the form g^m. (Novikov's negative solution to the Burnside problem; in the original paper, m large enough means $m \geqslant 4381$.)

Easier examples are provided by finitely generated infinite simple groups (there is such a group, discovered by G. Higman, which is described in [S], n° I.1.4). They are not linear, because it is a result of Mal'cev that a finitely generated linear group Γ is residually finite [M]. (This means that, for any $\gamma \in \Gamma - \{1\}$, there exists a homomorphism φ of Γ onto a finite group with $\varphi(\gamma) \neq 1$; instructive and easy exercice: check that $SL(n, \mathbf{Z})$ is residually finite.)

Also, any finitely generated non hopfian group cannot be linear (Γ is non hopfian if there exists a non injective homomorphism of Γ onto itself); an example of such a group is that generated by two elements g, h submitted to the relation $h^{-1}g^2h = g^3$ (see [LS], page 197).

TITS' THEOREM. *A linear group* Γ *over a field* **K** *of characteristic* 0 *which is not almost solvable contains a free group.*

This theorem has been conjectured by Bass and Serre, and proved in [T] together with other results, some concerning positive characteristics.

The following precision has been added by Wang [Wa]: there exists for each positive integer n a constant $\lambda(n)$ such that any subgroup of $GL(n, \mathbf{K})$ without free subgroup contains a solvable subgroup of index smaller than $\lambda(n)$.

Let Γ be a group having a finite set of generators S which is a subgroup of $GL(n, \mathbf{K})$ for some n. If k is the subfield of **K** generated by entries of elements of S, then $\Gamma \subset GL(n, k)$. As k is finitely generated of characteristic zero, there exists an embedding of k in **C** and one may assume that Γ lies in $GL(n, \mathbf{C})$. For finitely generated groups (and also in the general case by [Wh]), it is consequently sufficent to prove Tits' theorem for $\mathbf{K} = \mathbf{C}$ (or $\mathbf{K} = \mathbf{R}$ because $GL(n, \mathbf{C})$ is a subgroup of $GL(2n, \mathbf{R})$). But this apparent simplification (?) is deceptive, because the proof does require other fields than fields of complex numbers.

It follows from the theorem that a linear group over a field of characteristic zero which is not amenable contains a free group; this answers for linear groups a question formulated by J. von Neumann [vN]. Another famous result whose proof requires Tits' theorem is due to Gromov: a finitely generated group has polynomial growth if and only if it is almost nilpotent [G].

The analogue of Tits' theorem for division rings does not hold as such [L1], but conjectural statements have been formulated [L2]. Another generalisation of the theorem is proposed as a research problem in remark 1.4.2 of [BL].

3. Digression on hyperbolic geometry

Let n be an integer, $n \geqslant 1$. The hyperbolic space H^{n+1} of dimension $n+1$ is the open unit ball of the euclidean space $\mathbf{R}^{n+1}$. Hyperbolic lines (called lines below) in H^{n+1} are traces on H^{n+1} of circles and euclidean lines in $\mathbf{R}^{n+1}$ which are orthogonal to $\mathbf{S}^n$. Two distinct points $P, Q \in H^{n+1}$ are on a unique line which determines two points $P_\infty, Q_\infty \in \mathbf{S}^n$, say with P, Q, Q_∞, P_∞ arranged in cyclic order on the euclidean circle defining this line. The (hyperbolic) distance between P and Q is given by a cross-ratio of euclidean distances; more precisely, it is defined to be

$$d(P, Q) = \operatorname{Log}(P, Q, Q_\infty, P_\infty) = \log\left(\frac{|P-Q_\infty|}{|P-P_\infty|} : \frac{|Q-Q_\infty|}{|Q-P_\infty|}\right).$$

The *proper Mœbius group* $GM(n)_0$ is the group of orientation preserving isometries of $\mathbf{R}^{n+1}$ for this distance. Any $g \in GM(n)_0$ extends to a homeomorphism of the closed ball $H^{n+1} \cup S^n$. One may check that $GM(1)_0$ is isomorphic to $PGL(2, \mathbf{R})$ and $GM(2)_0$ to $PGL(2, \mathbf{C})$.

There is an equivalent description with H^{n+1} the half space $\mathbf{R}^n \times \mathbf{R}^*_+$. The set of "points at infinity" is then $\mathbf{R}^n \cup \{\infty\}$ rather than $\mathbf{S}^n$.

For all this, see e.g. [A] or [Si].

An isometry $g \in GM(n)_0$ is said to be

elliptic if there is some point in H^{n+1} fixed by g,

parabolic if there is in $\mathbf{S}^n$ exactly one point fixed by g,

hyperbolic if there is a line in H^{n+1} invariant by g on which g has no fixed point.

(Following Thurston [Th], we call "hyperbolic" elements which are "loxodromic" in classical litterature, such as in [Gr].)

PROPOSITION. *Elliptic, parabolic and hyperbolic elements define a partition of the proper Mœbius group in three disjoint classes.*

Proof. Let us first check that the three classes do not overlap in $GM(n)_0$. If g is hyperbolic, it has two fixed points in $\mathbf{S}^n$ and thus cannot be parabolic; if g was also elliptic, the foot of the perpendicular from the fixed point of g onto the invariant line of g would be fixed by g, and this cannot be. If g was at the same time elliptic with fixed point $a \in H^{n+1}$ and parabolic with fixed point $b \in \mathbf{S}^n$, the line from a towards b would have two points at infinity b and b' both fixed by g, and this cannot be.

That any $g \in GM(n)_0$ belongs to one of the three classes follows for example from Brouwer's fixed point theorem. (See also 4.9.3 in [Th].) □

Observe that an hyperbolic isometry $g \in GM(n)_0$ has a unique invariant line δ. Suppose indeed that there are two of them, say δ and δ'. If $\delta \cap \delta' \neq \phi$, the intersection point (which is unique) is fixed by g, and this cannot be. If $\delta \cap \delta' = \phi$ and if δ, δ' have no common point at infinity, there is a unique line perpendicular to both δ and δ'; but this line intersects δ in a point fixed by g, and this cannot be. Assume finally that $\delta \cap \delta' = \phi$ and that δ and δ' have a common point at infinity; choose some number $\rho > 0$ and consider the set C_ρ of points in H^{n+1} at a distance of ρ from δ'; the intersection $C_\rho \cap \delta$ is a point fixed by g, and again this cannot be. One may consequently also define an isometry $g \in GM(n)_0$ to be

elliptic if $d(a, g(a)) = 0$ for some $a \in H^{n+1}$,

parabolic if $\inf d(a, g(a)) = 0$, with the infimum over $a \in H^{n+1}$ not attained,

hyperbolic if $\inf d(a, g(a)) > 0$ (and the infimum is then attained exactly on the invariant line of g).

We shall need below the following *dynamical description*. An hyperbolic isometry $g \in GM(n)_0$ has on $\mathbf{S}^n$ one attracting point P_a and one repulsing point P_r. This means that, for any neighborhood U of P_a in $\mathbf{S}^n$ and for any compact subset K of $S^n - \{P_r\}$, one has $g^k(K) \subset U$ for k large enough. (And similarly with g^{-1} instead of g when exchanging P_a and P_r.) Consider now a parabolic isometry $g \in GM(n)_0$ with fixed point $P \in \mathbf{S}^n$. Let U be a neighborhood of P in $\mathbf{S}^n$ and let K be compact in $S^n - \{P\}$; then $g^k(K) \subset U$ for any $k \in \mathbf{Z}$ with $|k|$ large enough. (This is obvious when g is a translation in $\mathbf{R}^n \times \mathbf{R}^*_+$ by some vector in $\mathbf{R}^n$, and any parabolic isometry of H^{n+1} is conjugate to such a translation.)

4. Free subgroups of $GL(2, \mathbf{R})$ and of $GL(2, \mathbf{C})$

We show in this section that a subgroup of the proper Mœbius group $G = PGL(2, \mathbf{R})$ which is not almost solvable contains free groups; the same fact for $GL(2, \mathbf{R})$ follows straightforwardly. We discuss also the case of $GL(2, \mathbf{C})$.

PROPOSITION. *Let $g, h \in G - \{1\}$ be without any common fixed point in $H^2 \cup \mathbf{S}^1$. Then the group Γ generated by g and h contains free groups, up to two exceptions.*

The first of these happens when $g^2 = h^2 = 1$. The second when one element is an involution, say $g^2 = 1$, when h is hyperbolic, and when g exchanges the two fixed points of h on $\mathbf{S}^1$. In these two cases, Γ is the infinite dihedral group, and is thus solvable.

Proof. We check below in each of the non exceptional cases that Γ contains a free group.

Case 1. One element, say g, is parabolic with fixed point $P \in \mathbf{S}^1$.

Consider the parabolic $k = hgh^{-1}$, with fixed point $Q = h(P) \neq P$ in $\mathbf{S}^1$. Let S_1 [respectively S_2] be a compact neighborhood of P [resp. Q] in $\mathbf{S}^1$ with $S_1 \cap S_2 = \phi$. The end of section 3 shows that there exists a positive integer n_0 such that $g^n(S_2) \subset S_1$ and $k^n(S_1) \subset S_2$ for any $n \in \mathbf{Z}$ with $|n| \geqslant n_0$. It follows from Klein's criterium that g^{n_0} and k^{n_0} generate a free subgroup of G.

Case 2. Both g and h are hyperbolic.

Let S_1 [respectively S_2] be a compact neighborhood of the fixed points of g [resp. of h] in $\mathbf{S}^1$ with $S_1 \cap S_2 = \phi$, and proceed as in case 1.

Case 3. One of the elements, say h, is hyperbolic with fixed points $P, Q \in \mathbf{S}^1$ and g does not exchange them, say $R = g(Q) \notin \{P, Q\}$.

If $g(P) \notin \{P, Q\}$ then h and ghg^{-1} are as in case 2. We may thus assume that $g(P) = Q$. If $g(R) \neq P$ then h and g^2hg^{-2} are again as in case 2. We may thus also assume $g(R) = P$. Consider then $h' = g^{-1}hg$, an hyperbolic with fixed points R and P, as well as $h'' = ghg^{-1}hgh^{-1}g^{-1}$, an hyperbolic with fixed points $Q = ghg^{-1}(Q)$ and $S = ghg^{-1}(P)$. One has $h(R) \neq Q$ and thus $S = gh(R) \neq g(Q) = R$; one has also $h(R) \neq R$ and $S \neq g(R) = P$. Consequently h' and h'' are as in case 2.

Case 4. Both g and h are elliptic with $g^2 \neq 1$.

Possibly after conjugation within G, one may assume that $g = r_\alpha$ is a rotation around the origin of the disc H^2 by some angle $\alpha \in]0, 2\pi[- \{\pi\}$. Then $k = hgh^{-1} \neq g$, otherwise h would also fix the origin.

In the average, any point of $\mathbf{S}^1$ is rotated by k of an angle α. More precisely, if $\tilde{k}: \mathbf{R} \to \mathbf{R}$ is the lifting of k to the universal covering of $\mathbf{S}^1$ with $0 \leqslant \tilde{k}(0) < 1$, then $\lim_{n \to \infty} \frac{1}{n}(\tilde{k}^n(x) - x)$ exists for all $x \in \mathbf{R}$ and this limit is α. Moreover

$$\min_{x \in \mathbf{R}} (\tilde{k}(x) - x) \leqslant \alpha \leqslant \max_{x \in \mathbf{R}} (\tilde{k}(x) - x).$$

(See any exposition of the rotation number, for example chapter 17 in [CL] or section 1 in [Ka].) It follows that there exists $P \in \mathbf{S}^1$ with $k(P) = g(P)$, so that $g^{-1}k$ has a fixed point in $\mathbf{S}^1$ and one of the previous cases applies.

Exceptional cases. If $g^2 = h^2 = 1$, then gh generate an infinite cyclic subgroup of index 2 in Γ and Γ is isomorphic to the infinite dihedral group. If h is hyperbolic and if g exchanges its fixed points, then $ghg^{-1} = h^{-1}$ so that $g^2 = (gh)^2 = 1$ and Γ is as in the previous case.

The proof is now complete. □

The proposition above is well known, and may essentially be found in any of the following papers: [LU1], [Md], [Ro] (see corollary 1). One should also mention Magnus' surveys [Ms1], [Ms2].

As two elements of G having a common fixed point in $H^2 \cup \mathbf{S}^1$ generate a solvable subgroup, we have proved the 2-generators particular case of the following fact.

THEOREM 1. *A subgroup* Γ *of* $G = PGL(2, \mathbf{R})$ (*or of* $GL(2, \mathbf{R})$) *which is not solvable contains free groups.*

Proof. We assume that Γ does not contain free groups, and check that Γ is solvable. If Γ contains at least one parabolic isometry, this follows from case 1 of the proof above. If it contains at least one hyperbolic isometry, then all hyperbolics in Γ have a common fixed point (see case 2) and then either all elements in Γ have a common fixed point or Γ is dihedral (see case 3). Finally, if Γ is an elliptic group, it follows from case 4 that Γ is abelian. □

This covers in particular the case of Fuchsian groups. The next theorem covers that of Kleinian groups.

THEOREM 2. *Let* Γ *be a subgroup of* $SL(2, \mathbf{C})$ *which is not solvable. Assume moreover that* Γ *is not relatively compact (or equivalently that* Γ *is not conjugate to a subgroup of the maximal compact subgroup* $SU(2)$ *of* $SL(2, \mathbf{C})$*). Then* Γ *contains free groups.*

In particular, a discrete subgroup of $PGL(2, \mathbf{C})$ *which is not almost solvable contains free groups.*

Proof. The group Γ acts on $\mathbf{C}^2$; as Γ is not solvable, the representation is irreducible. Easy arguments à la Burnside show that Γ does not contain elliptic elements only; indeed, Γ does contain a hyperbolic element (see [CG], or corollary 1.8 in [B]). The first statement follows now as theorem 1.

The second follows from this: a discrete subgroup of $PGL(2, \mathbf{C})$ containing elliptic elements only is finite. Indeed, such a group is periodic. If Γ is a priori known to be finitely generated, then Γ is finite by a theorem of Schur (§36 in [CR]) so that the hyperbolic subspace $F(\Gamma) = \{ x \in H^3 \mid \Gamma x = \{x\} \}$ is non empty. In general, to any finitely generated subgroup Γ_ι of Γ corresponds a non empty subspace $F_\iota \subset H^n$; it is easy to check that $F(\Gamma) = \cap F_\iota$ is non empty so that Γ lies in a compact subgroup of the Mœbius group; it follows again that Γ is finite. □

Instead of the assumption of theorem 2, assume the following: there exists $g \in \Gamma$ with two distinct eigenvalues of same modulus, say $\mu_1 = \rho \exp(i\theta_1)$ and $\mu_2 = \rho \exp(i\theta_2)$ where $\rho, \theta_1, \theta_2 \in \mathbf{R}$ satisfy $\rho > 0$ and $\theta_1 \not\equiv \theta_2 \pmod{2\pi}$, and there exists an automorphism α of $\mathbf{C}$ with $|\alpha(\mu_1)| \neq |\alpha(\mu_2)|$. Then α induces an automorphism $\tilde{\alpha}$ of $GL(2, \mathbf{C})$ and the proof applies to $\tilde{\alpha}(\Gamma)$. But this procedure has its limits, because there exist complex numbers μ (such as $\frac{1}{5}(3+4i)$, see the remark below) such that $|\alpha(\mu)| = 1$ for any automorphism α of $\mathbf{C}$ but which are not roots of 1; then the argument above fails [1]) for example for $g = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}$.

Something is true however: let k be a finitely generated field of characteristic 0, let $\mu \in k - \{0\}$ and assume μ is not a root of 1. Then there exists a locally compact field k' endowed with an absolute value ω and there exists a homomorphism $\sigma: k \to k'$ such that $\omega(\sigma(\mu)) \neq 1$; this is lemma 4.1 of [T]. It follows that the argument above may be recuperated, but one has to consider other fields than subfields of $\mathbf{C}$.

For self-consistency, let us end with the announced remark. For any automorphism α of $\mathbf{C}$, one has clearly

$$\left| \alpha\left(\frac{3+4i}{5}\right) \right| = \left| \frac{3 \pm 4i}{5} \right| = 1;$$

we check now that $\frac{3+4i}{5}$ is not a root of one.

Let p, q be coprime integers and let $\mu = \exp\left(i2\pi \frac{p}{q}\right)$ be a root of 1. Then μ is an algebraic number of degree $\varphi(q)$, where φ is Euler's function. It follows that $\cos\left(2\pi \frac{p}{q}\right)$ is an algebraic number of degree $d \geqslant \frac{1}{2}\varphi(q)$: because if F is a polynomial of degree d in $Z[X]$ with $F\left(\cos\left(2\pi \frac{p}{q}\right)\right) = 0$, then μ is a root of

[1]) This shows that one point on page 50 of [D] is incorrect.

$X^d F\left(\frac{1}{2}X + \frac{1}{2}X^{-1}\right)$, which is of degree $2d$ in $Z[X]$, so that $2d \geqslant \varphi(q)$. If $q \in \{1, 2, 3, 4, 6\}$, one checks easily that $\exp\left(i2\pi\frac{p}{q}\right) \neq \frac{3+4i}{5}$. If $q = 5$ or if $q \geqslant 7$, then $\varphi(q) > 2$ so that $\cos\left(2\pi\frac{p}{q}\right)$ is not rational. Thus the root of unity μ cannot be equal to $\frac{3+4i}{5}$.

5. Some other cases of Tits' theorem

Let n be an integer with $n \geqslant 2$.

Define a subgroup Γ of $GL(n, \mathbf{C})$ [respectively of $PGL(n, \mathbf{C})$] to be *irreducible* if any linear subspace of $\mathbf{C}^n$ [resp. of $P^{n-1}_{\mathbf{C}}$] invariant by Γ is trivial, and *not almost reducible* if any subgroup of Γ of finite index is irreducible. When referring to the *Zariski* topology on $PGL(n, \mathbf{C})$, we use below the letter Z.

Reduction. Tits' theorem for complex linear groups is equivalent to the following statements (one for each $n \geqslant 2$):

Let Γ be a subgroup of $PGL(n, \mathbf{C})$ which is not almost solvable. Assume that

(i) is not almost reducible;

(ii) the Z-closure G of Γ in $PGL(n, \mathbf{C})$ is Z-connected. Then Γ contains free groups.

That one may assume (i) without loss of generality is an easy exercise on reducibility, and one may assume (ii) because the Z-closure of any subgroup of $PGL(n, \mathbf{C})$ has finitely many Z-connected components. (The hypothesis of the reduced statement are redundant: (i) and (ii) imply by Lie's theorem that G is not solvable, so that Γ is not almost solvable!)

Now let $g \in PGL(n, \mathbf{C})$ and choose a representative $\tilde{g} \in GL(n, \mathbf{C})$ of g. Let us define g to be

elliptic if $\tilde{g}$ is semi-simple with all eigenvalues of equal moduli,

parabolic if $\tilde{g}$ is not semi-simple and has all its eigenvalues of equal moduli,

hyperbolic if $\tilde{g}$ has at least two eigenvalues of distinct moduli.

These definitions are obviously independent on the choice of $\tilde{g}$. They generalize those of section 3 as follows from [Gr]. The meaning of "hyperbolic" fits with current use in dynamical systems theory (see e.g. definition 5.1 in [Sh]).

Let g be hyperbolic and let $\tilde{g}$ be as above. Let $\tilde{A}(g)$ [respectively $\tilde{A}'(g)$] be the direct sum of the nilspaces of $\tilde{g}$ corresponding to all eigenvalues of maximal modulus [resp. to all other eigenvalues] of $\tilde{g}$. Let $A(g)$ [resp. $A'(g)$] be the canonical image of $\tilde{A}(g) - \{0\}$ [resp. $\tilde{A}'(g) - \{0\}$] in $\mathbf{P} = P_{\mathbf{C}}^{n-1}$. Then $A(g) \cap A'(g) = \emptyset$ and the smallest linear subspace of $\mathbf{P}$ containing both $A(g)$ and $A'(g)$ is $\mathbf{P}$ itself. Tits calls $A(g)$ [resp. $A(g^{-1})$] the *attracting space* [resp. *repulsing space*] of g. We say that g is *sharp* if $A(g)$ is a point and that g is *very sharp* if both $A(g)$ and $A(g^{-1})$ are points. For each $k \in \{1, 2, ..., n-1\}$, the fundamental representation of $GL(n, C)$ in $\wedge^k \mathbf{C}^n$ induces an injection

$$\lambda_k : PGL(n, \mathbf{C}) \to PGL(\tbinom{n}{k}, \mathbf{C});$$

as g is hyperbolic, $\lambda_k(g)$ is sharp for some k. We also say that two hyperbolic elements $g, h \in PGL(n, \mathbf{C})$ are in *general position* if

$$A(g) \cup A(g^{-1}) \subset \mathbf{P} - \{A'(h) \cup A'(h^{-1})\}$$
$$A(h) \cup A(h^{-1}) \subset \mathbf{P} - \{A'(g) \cup A'(g^{-1})\}.$$

Observe that any hyperbolic element of $PGL(2, \mathbf{C})$ is very sharp, and that two hyperbolic elements of $PGL(2, \mathbf{C})$ are in general position if and only if they do not have any common fixed point on $\mathbf{S}^2$.

Recall that an element of $PGL(n, \mathbf{C})$ is *semi-simple* if its inverse image in $GL(n, \mathbf{C})$ contains diagonalisable matrices.

LEMMA 1. *Let Γ be an irreducible subgroup of $PGL(n, \mathbf{C})$ having a Z-connected Z-closure. If Γ contains a sharp semi-simple element g, then Γ contains a very sharp element.*

About the proof. Let $\tilde{g} \in GL(n, \mathbf{C})$ be some representative of g having an eigenvalue of "large" modulus and all other eigenvalues with moduli "near" 1. For suitable $h, u \in \Gamma$ and for $j \in N$ large enough, one may hope that $g^{-j}hg^jh^{-1}u$ has a representative in $GL(n, \mathbf{C})$ with one eigenvalue of very large modulus (look at $hg^jh^{-1}u$), one eigenvalue of very small modulus (look at g^{-j}), and other eigenvalues of moduli "near" 1. Section 3 of [T] shows that this hope is realistic. (See also below, after the theorem.) □

LEMMA 2. *Let Γ be an irreducible subgroup of $PGL(n, \mathbf{C})$ having a Z-connected Z-closure. If Γ contains a very sharp element, then Γ contains two very sharp elements in general position.*

Proof. Let P_1, P_2 be two linear subspaces of $\mathbf{P}$ with $P_1 \neq \emptyset$ and $P_2 \neq \mathbf{P}$. Then $\{ x \in G \mid x(P_1) \not\subset P_2 \}$ is obviously a Z-open subset of G. It is not empty:

Choose indeed $p \in P_1$; then the subspace of $\mathbf{P}$ spanned by the orbit Gp is stable under G and must therefore coincide with $\mathbf{P}$; hence there exists $x \in G$ with $x(p) \notin P_2$ and, a fortiori, $x(P_1) \not\subset P_2$.

Let g be a very sharp element in Γ. It follows from above that

$$X = \left\{ x \in G \;\middle|\; \begin{array}{l} A(g) \text{ and } A(g^{-1}) \text{ are not contained in any of } xA'(g), \\ xA'(g^{-1}), x^{-1}A'(g), x^{-1}A'(g^{-1}) \end{array} \right\}$$

is a non empty Z-open subset of G. Let $y \in X \cap \Gamma$. Then g and ygy^{-1} are both very sharp and are in general position. □

For the next lemma, we choose as above k with $1 \leqslant k \leqslant n-1$ and we consider the k^{th} fundamental representation $\lambda_k \colon SL(n, \mathbf{C}) \to SL(\binom{n}{k}, \mathbf{C})$ of $SL(n, \mathbf{C})$.

LEMMA. *Let Γ be a group and let $\rho \colon \Gamma \to SL(n, \mathbf{C})$ be an irreducible representation. Then the Z-closure G of $\rho(\Gamma)$ in $SL(n, \mathbf{C})$ is semi-simple and the representation $\sigma = \lambda_k\rho \colon \Gamma \to SL(\binom{n}{k}, \mathbf{C})$ is completely reducible.*

Proof. We show first that G is semi-simple. Consider the solvable radical R of G. By Lie's theorem, there exists an eigenvector for R, namely there exist $v \in \mathbf{C}^n - \{0\}$ and $\alpha \in \operatorname{Hom}(R, \mathbf{C}^*)$ with $r(v) = \alpha(r)v$ for all $r \in R$. As R is normal in G, any vector $g(v)$ $(g \in G)$ is also an eigenvector for R. By irreductibility, any vector in $\mathbf{C}^n$ is also an eigenvector, so that R is made up of dilations. But R is connected and is in $SL(n, \mathbf{C})$, so that $R = 1$.

Now $\lambda_k \colon G \to SL(\binom{n}{k}, \mathbf{C})$ is completely reducible; denote by $\lambda_{k,j} \colon G \to SL(W_j)$ the components of a decomposition $\lambda_k = \bigoplus_{j \in J} \lambda_{k,j}$ and define $\sigma_j = \lambda_{k,j}\rho$ $(j \in J)$. One has clearly $\sigma = \bigoplus_{j \in J} \sigma_j$, and each $\sigma_j \colon \Gamma \to SL(W_j)$ is irreducible (this because $\lambda_{k,j}$ is irreducible and by Schur's lemma). □

THEOREM. *Let Γ be a subgroup of $PGL(n, \mathbf{C})$ and assume*

(i) Γ *is neither almost solvable nor almost reducible,*

(ii) Γ *contains a semi-simple hyperbolic element.*

Then Γ contains free groups.

Proof. As one may consider instead of Γ a subgroup of finite index, there is no loss of generality if we assume that the Z-closure of Γ is Z-connected. We denote by $\tilde{\Gamma}$ the inverse image of Γ in $SL(n, \mathbf{C})$. By (ii), there exists $k \in \{1, \ldots, n-1\}$ and a semi-simple element $\tilde{\gamma} \in \tilde{\Gamma}$ having eigenvalues $\mu_1, \ldots, \mu_n$ with $|\mu_1| = \ldots = |\mu_k| > |\mu_j|$ for $j = k+1, \ldots, n$. Let $N = \binom{n}{k}$, and denote by λ_k both the fundamental representation $GL(n, \mathbf{C}) \to GL(N, \mathbf{C})$ and the induced homomorphism $PGL(n, \mathbf{C}) \to PGL(N, \mathbf{C})$. Then $\lambda_k(\tilde{\gamma})$ has eigenvalues $\nu_1, \ldots, \nu_N$ with $|\nu_1| > |\nu_j|$ for $j = 2, \ldots, N$. By lemma 3, there exists a $\lambda_k(\tilde{\Gamma})$-irreducible subspace W_0 of $\mathbf{C}^N$, associated to a representation $\sigma_0 : \tilde{\Gamma} \to GL(W_0)$, such that ν_1 is an eigenvalue of $\sigma_0(\tilde{\gamma})$. As the Z-closure $\tilde{G}$ of $\tilde{\Gamma}$ in $SL(n, \mathbf{C})$ is semi-simple, the group $\tilde{G}$ is perfect and $\sigma_0(\tilde{\Gamma})$ lies in $SL(W_0)$. As $|\nu_1| > 1$, one has $\dim_{\mathbf{C}} W_0 \geqslant 2$.

Thus one may assume from the start that Γ contains a sharp semi-simple element, and indeed by lemmas 1 and 2 two very sharp elements in general position. The conclusion follows as in case 2 of the proof of the proposition in section 4. □

Now lemma 1 remains true without the hypothesis "semi-simple". This has been announced by Y. Guivarch', who uses ideas of H. Fürstenberg to show the following: given an appropriate subset S of Γ containing a sharp element, then almost any "long" word in the letters of S is very sharp. Using this, one may replace (ii) in the theorem above by the following a priori weaker hypothesis

(ii′) Γ is not relatively compact.

Then, one first checks as for theorem 2 of section 4 that Γ contains hyperbolic elements; one concludes as in the previous proof, with Guivarch's version of lemma 1.

For subgroups of $PU(n)$, one may repeat the discussion at the end of section 4.

REFERENCES

[A] AHLFORS, L. V. *Möbius transformations in several dimensions.* School of Mathematics, University of Minnesota, 1981.

[Ba] BASS, H. Groups of integral representation type. *Pacific J. Math. 86* (1980), 15-51.

[BL] BASS, H. and A. LUBOTZKY. Automorphisms of groups and of schemes of finite type. *Preprint.*

[B] BOURBAKI, N. *Eléments d'histoire des mathématiques.* Hermann 1969.

[CL] CODDINGTON, E. A. and N. LEVINSON. *Theory of ordinary differential equations.* McGraw Hill, 1955.

[CG] CONZE, J. P. and Y. GUIVARCH'. Remarques sur la distalité dans les espaces vectoriels. *C. R. Acad. Sc. Paris, Sér. A, 278* (1974), 1083-1086.

[CR] CURTIS, C. and I. REINER. *Representation theory of finite groups and associative algebras.* Interscience, 1962.

[DE] DUBINS, L. E. and M. EMERY. Le paradoxe de Hausdorff-Banach-Tarski. *Gazette des Mathématiciens 12* (1979), 71-76.

[D] DIXON, J. D. Free subgroups of linear groups. *Lecture Notes in Math. 319* (Springer, 1973), 45-56.

[E] EPSTEIN, D. B. A. Almost all subgroups of a Lie group are free. *J. of Algebra 19* (1971), 261-262.

[FK] FRICKE, R. and F. KLEIN. *Vorlesungen über die Theorie der automorphen Functionen,* vol. I. Teubner, 1897.

[Gr] Greenberg, L. Discrete subgroups of the Lorentz group. *Math. Scand. 10* (1962), 85-107.

[G] Gromov, M. Groups of polynomial growth and expanding maps. *Publ. Math. I.H.E.S. 53* (1981), 53-78.

[H] Hausdorff, F. *Grundzüge der Mengenlehre.* Veit, 1914.

[Hm] Hausmann, J. C. Sur l'usage de critères pour reconnaître un groupe libre, un produit amalgamé ou une *HNN*-extension. *L'Enseignement math. 27* (1981), 221-242.

[Ig] Ignatov, Ju. A. Free and nonfree subgroups of $PSL_2(\mathbf{C})$ generated by two parabolic elements. *Math. USSR Sbornik 35 (1)* (1979), 49-55.

[Ka] Katznelson, Y. Sigma-finite invariant measure for smooth mappings of the circle. *J. d'analyse math. 31* (1977), 1-18.

[Ku] Kuranishi, M. Two elements generations on semi-simple Lie groups. *Kōdai Math. Sem. rep. 5-6* (1949), 9-10.

[L] Leutbecher, A. Über die Heckeschen Gruppen $G(\lambda)$. *Abh. Math. Sem. Un. Hamburg 31* (1967), 199-205.

[L1] Lichtman, A. On subgroups of the multiplicative group of skew fields. *Proc. Amer. Math. Soc. 63* (1971), 15-16.

[L2] —— On normal subgroups of multiplicative group of skew fields generated by a polycyclic-by-finite group. *J. of Algebra 78* (1982), 548-577.

LU1] Lyndon, R. C. and J. L. Ullman. Pairs of real 2-by-2 matrices that generate free products. *Michig. Math. J. 15* (1968), 161-166.

[LU2] —— Groups generated by two parabolic linear fractional transformations. *Can. J. Math. 21* (1969), 1388-1403.

[LS] Lyndon, R. C. and P. E. Schupp. *Combinatorial group theory.* Springer, 1977.

[Ms1] Magnus, W. Two generator subgroups of $PSL(2, \mathbf{C})$. *Nachr. Akad. Wiss. Göttingen, II Math. Phys. Kl. 7* (1975), 81-94.

[Ms2] —— The uses of 2 by 2 matrices in combinatorial group theory. A survey. *Res. der Math. 4* (1981), 171-192.

[Md] Majeed, A. Freeness of the group $\langle a^n, b^n \rangle$ for some integer n, $a, b \in SL(2, \mathbf{C})$. *J. Math. Soc. Japan 29* (1977), 29-33.

[M] Mal'cev, A. I. On the faithful representations of infinite groups by matrices. *Amer. Math. Soc. Transl. (2) 45* (1965), 1-18.

[Mt] Maskit, B. On Poincaré's theorem for fundamental polygons. *Adv. in Math. 7* (1971), 219-230.

[Mi] Matelski, J. P. The classification of discrete 2-generator subgroups of $PSL(2, \mathbf{R})$. *Israel J. of Math. 42* (1982), 309-317.

[vN] von Neumann, J. Zur allgemeinen Theorie des Masses. *Fund. Math. 13* (1929), 143-173.

[N] Newman, M. Pairs of matrices generating discrete free groups and free products. *Michig. Math. J. 15* (1968), 155-160.

[Ro] Rosenberger, G. On discrete free subgroups of linear groups. *J. London Math. Soc. 17* (1978), 79-85.

[S] Serre, J. P. Arbres, amalgames, SL_2. *Astérisque 46* (Soc. math. France, 1977).

[Sh] Shub, M. Stabilité globale des systèmes dynamiques. *Astérisque 56* (Soc. math. France, 1978).

[Si] Siegel, C. L. *Topics in complex function theory*, volume II. Wiley-Interscience 1971.

[Th] Thurston, W. P. *The geometry and topology of 3-manifolds.* Notes from lectures at Princeton, 1978-1979, chapters 1-9.

[T] Tits, J. Free subgroups in linear groups. *J. of Algebra 20* (1972), 250-270.

[Wa] WANG, S. P. A note on free subgroups in linear groups. *J. of Algebra 71* (1981), 232-234.

[Wh] WEHRFRITZ, B. A. F. 2-generator conditions in linear groups. *Archiv. Math. 22* (1971), 237-240.

[Wi] WEIL, A. *L'intégration dans les groupes topologiques et ses applications.* Hermann, 1940.

ADDED IN PROOF: See moreover the report by Yu. I. Merzlyakov "Linear groups", *J. Soviet Math. 14* (1980), 887-921.

(Reçu le 18 janvier 1983)

Pierre de la Harpe

Section de mathématiques
C.P. 240
CH-1211 Genève 24