2. Statement of Tits' theorem

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 $D(\ldots D(\Gamma)\ldots) = \{1\}$ 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