Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 29 (1983)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: FREE GROUPS IN LINEAR GROUPS
Autor: de la Harpe, Pierre
Kapitel: 1. Early examples
DOI: https://doi.org/10.5169/seals-52975

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 $w = \alpha_1\beta_1\alpha_2\beta_2 \ldots \alpha_k$ with $\alpha_1, \ldots, \alpha_k \in \Gamma_1 - \{1\}$ and $\beta_1, \ldots, \beta_{k-1} \in \Gamma_2 - \{1\}$, then $w(S_2) \subset S_1$ and $w \neq 1$. If $w = \beta_1\alpha_2 \ldots \alpha_k\beta_k$, let $\alpha \in \Gamma_1 - \{1\}$; then $\alpha w \alpha^{-1} \neq 1$ as above and $w \neq 1$. If $w = \alpha_1\beta_1 \ldots \alpha_k\beta_k$, let $\alpha \in \Gamma_1 - \{1, \alpha_1^{-1}\}$ and argue with $\alpha w \alpha^{-1}$. The last case $w = \beta_1\alpha_2 \ldots \beta_{k-1}\alpha_k$ 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 $D(\ldots D(\Gamma)\ldots) = \{1\}$ 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