4. Free subgroups of GL(2, R) and of GL(2, C)

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 $b \in S^n$, 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].) $\qquad\square$

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 S^n one attracting point P_a and one repulsing point P_r. This means that, for any neighborhood U of P_a in 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 $P \in S^n$. Let U be a neighborhood of P in 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 $H^2 \cup S^1$.   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 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 $P \in S^1$.

Consider the parabolic $k = hgh^{-1}$, with fixed point $Q = h(P) \neq P$ in S^1. Let S_1 [respectively S_2] be a compact neighborhood of P [resp. Q] in 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 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 $P, Q \in S^1$ 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 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 S^1 with $0 \leqslant \tilde{k}(0) < 1$, then $\lim\limits_{n \to \infty} \dfrac{1}{n}(\tilde{k}^n(x) - x)$ 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. $\square$

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 $\theta_1 \neq \theta_2 \pmod{2\pi}$, and there exists an automorphism α of $\mathbf{C}$ with $\mid \alpha(\mu_1) \mid \neq \mid \alpha(\mu_2) \mid$. 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 $\mid \alpha(\mu) \mid = 1$ 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 $\dfrac{3 + 4i}{5}$ is not a root of one.

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

---

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

$X^d F\left(\dfrac{1}{2} X + \dfrac{1}{2} X^{-1}\right)$, 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 $\exp\left(i2\pi\dfrac{p}{q}\right) \neq \dfrac{3 + 4i}{5}$. If $q = 5$ or if

$q \geqslant 7$, then $\varphi(q) > 2$ so that $\cos\left(2\pi\dfrac{p}{q}\right)$ is not rational. Thus the root of unity μ

cannot be equal to $\dfrac{3 + 4i}{5}$.

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 $P_{\mathbf{C}}^{n-1}$] 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.) $\square$

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 $\{x \in G \mid x(P_1) \not\subseteq P_2\}$ is obviously a Z-open subset of G. It is not empty:

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

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 kth fundamental representation $\lambda_k : SL(n, \mathbf{C}) \to SL(\binom{n}{k}, \mathbf{C})$ of $SL(n, \mathbf{C})$.

LEMMA. *Let Γ be a group and let $\rho : \Gamma \to SL(n, \mathbf{C})$ be an irreducible representation. Then the Z-closure G of $\rho(\Gamma)$ in $SL(n, \mathbf{C})$ is semi-simple and the representation $\sigma = \lambda_k \rho : \Gamma \to SL(\binom{n}{k}, \mathbf{C})$ 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 $\alpha \in \text{Hom}(R, \mathbf{C}^*)$ 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 $\lambda_k : G \to SL(\binom{n}{k}, \mathbf{C})$ is completely reducible; denote by $\lambda_{k,j} : G \to SL(W_j)$ 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 $\sigma_j : \Gamma \to SL(W_j)$ 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 $k \in \{1, ..., n-1\}$ and a semi-simple element $\tilde{\gamma} \in \tilde{\Gamma}$ having eigenvalues $\mu_1, ..., \mu_n$ with $|\mu_1| = ... = |\mu_k| > |\mu_j|$ for $j = k + 1, ..., n$. 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 $v_1, ..., v_N$ with $|v_1| > |v_j|$ for $j = 2, ..., N$. 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 v_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 $|v_1| > 1$, 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. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

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.