The ping-pong lemma

Sept 29, 2017

First, let's recall free products of groups from a perspective that will make our ping-pong discussion easier.

Given groups $\{G_i\}_{i\in I}$, set

$A = \bigcup_{i\in I} G_i$ and $W(A)$ the collection of all words in the alphabet A. Then the free product is

$$\ast_{i\in I} G_i := W(A)/\sim \text{ , with concatenation,}$$

where $\sim$ is the equivalence relation generated by

$we_iw' \sim ww'$ whenever $e_i \in G_i$ is the identity

$wabw' \sim wcw'$ whenever $a,b,c \in G_i$ for some i and $ab=c$.

Then $\ast_{i\in I} G_i$ is indeed a group, and in fact its elements have a nice description: A word $w \in W(A)$ is called <u>reduced</u> if

$w = a_1 \dots a_n$ where $a_j \in G_{i_j}$ and

(i) $i_j \neq i_{j+1}$ for $1 \leq j \leq n-1$

(ii) a_j is not the identity in G_{i_j}.

Theorem: Every element in $\ast_{i \in I} G_i$ has a unique reduced representative.

These groups occur in nature – for example, the free group F_2 is $\mathbb{Z} * \mathbb{Z}$, and more generally the output of any application of the Seifert–Van Kampen theorem is a free product (or possibly a quotient thereof).

To produce examples, we introduce the topic of the talk

Theorem (ping-pong lemma).
Let G be a group acting on a set X, let G_1, G_2 be subgroups of G and let Γ be the subgroup of G generated by $G_1 \cup G_2$. Assume $|G_1| \geq 2$ and $|G_2| \geq 3$.

If there exist nonempty $X_1, X_2 \subset X$ with $X_2 \not\subset X_1$ satisfying

$$g(X_2) \subset X_1 \quad \text{for all } g \in G_1,\ g \neq 1$$

$$\text{and } g(X_1) \subset X_2 \quad \text{for all } g \in G_2,\ g \neq 1$$

then $\Gamma \cong G_1 * G_2$.

Proof: Let $A = G_1 \setminus \{1\} \cup G_2 \setminus \{1\}$, and let $w \in W(A)$ be a reduced word. If w does not represent the identity in Γ, we're done.

Argue by cases:

Write $w = a_1 b_1 \dots b_{k-1} a_k$ with $a_i \in G_1 \setminus \{1\}$ and $b_j \in G_2 \setminus \{1\}$. Then

$$\begin{aligned} w(X_2) &= a_1 b_1 \dots b_{k-1} a_k (X_2) \\ &\subset a_1 b_1 \dots b_{k-1}(X_1) \\ &\subset a_1 b_1 \dots a_{k-1}(X_2) \\ &\vdots \\ &\subset a_1(X_2) \subseteq X_1 . \end{aligned}$$

So w is not the identity. Same for all other words (3 more cases).

In general, the rule is: find at least one element that, via some coarse partition of the set X, can be shown to land somewhere other than where it started.

<u>Example</u>: Consider the copies of $\mathbb{Z}$ in $M_2(\mathbb{Z}[t])$ generated by

$$A = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

Let X denote the set of column vectors $\begin{pmatrix} p(t) \\ q(t) \end{pmatrix}$ with entries in $\mathbb{Z}[t]$. Then

$$X = X_1 \sqcup X_2 \sqcup X_3$$

where

$$X_1 = \deg p(t) > \deg q(t)$$

$$X_2 = \deg p(t) < \deg q(t) \qquad X_3 = \deg p(t) = \deg q(t)$$

then a straightforward degree argument gives

$$A^m(X_2) \subset X_1 \ \forall m, \text{ and } B^n(X_1) \subset X_2 \ \forall n.$$

Thus $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix}$ generate $\mathbb{Z} * \mathbb{Z} \simeq F_2$.

More generally, suppose G_1 and G_2 are subgroups of the multiplicative group of a ring R $\bar{w}$ no zero divisors. Define

$$\rho : G_1 * G_2 \longrightarrow M_2(R[t])$$

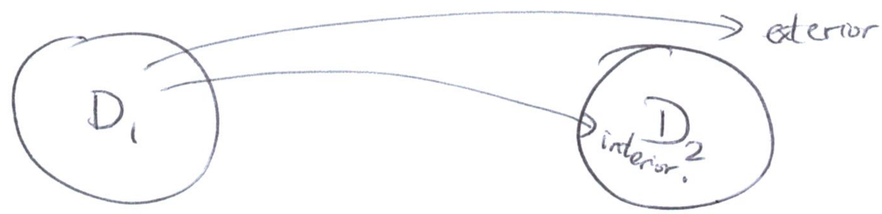
by $\rho(g) = \begin{bmatrix} g & (g-1)t \\ 0 & 1 \end{bmatrix} \quad \forall g \in G_1$

and $\rho(g) = \begin{bmatrix} 1 & 0 \\ (g-1)t & g \end{bmatrix} \quad \forall g \in G_2.$

Then this map is always injective. ~~This~~ This is a key to a very elegant proof that G_1 and G_2 being bi-orderable $\Rightarrow$ $G_1 * G_2$ is bi-orderable.

<u>Example</u>: Recall Möbius transformations (ie. elements of $PSL(2,\mathbb{C})$) map circles to circles. We can also, for pair of circles C_1, C_2 ~~find~~ bounding disks D_1 and D_2, find

a Möbius transformation sending D_1 to D_2 or D_i to $\mathrm{int}((\mathbb{C}\cup\infty)\setminus D_1)$



So choose $D_1, D_2, \ldots, D_{2g} \subset \mathbb{C}\cup\{\infty\}$ disks with disjoint interiors. Let $\gamma_k \in PSL(2,\mathbb{C})$ be the mapping with

$$\gamma_k\left(\mathrm{int}((\mathbb{C}\cup\infty)\setminus D_{2k-1})\right) = \mathrm{int}(D_{2k})$$

for $k=1,\ldots,g$. Set $X_k = D_{2k-1}\cup D_{2k}$.

One can check that $\gamma_k^{l}(X_k^c) \subset X_k \ \forall l$ and any reduced word in the γ_k's satisfies:

$$\gamma_{i_1}^{l_1}\gamma_{i_2}^{l_2}\cdots\gamma_{i_k}^{l_k}(X_{i_k}^c) \subset X_{i_1}$$ (this is a bit tricky)

so there's a $z \in X_{i_k}^c \setminus X_{i_1}$ that is moved by this reduced word.

$\Longrightarrow$ The subgroup of $PSL(2,\mathbb{C})$ generated by $\{\gamma_1,\ldots,\gamma_g\}$ is

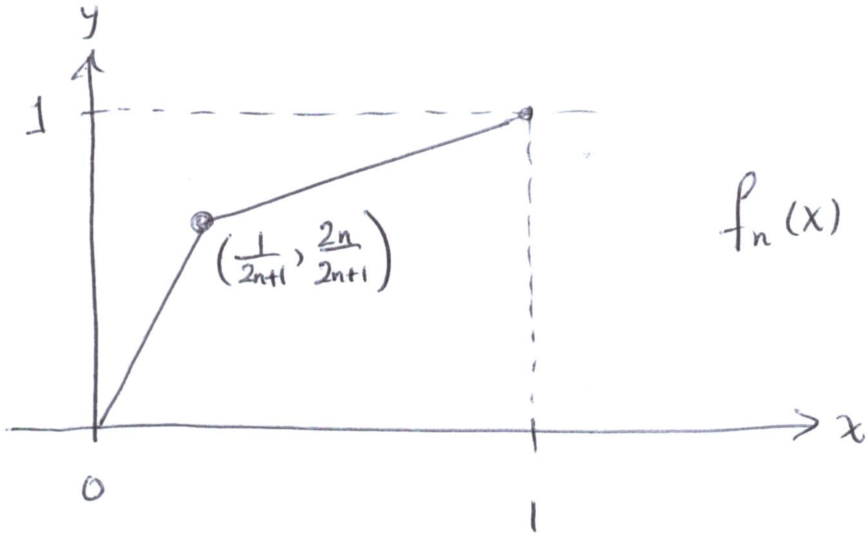
$$\underbrace{\mathbb{Z}*\mathbb{Z}*\cdots*\mathbb{Z}}_{g \text{ times}} = F_g,$$ the free group on g generators.

This is called a Schottky group.

<u>Example</u>: Let $\mathrm{Homeo}_+(\mathbb{R})$ denote the group of order-preserving homeomorphisms of $\mathbb{R}$. We can explicitly embed $F_n \subset \mathrm{Homeo}_+(\mathbb{R})$ as follows:

Let $T_a : \mathbb{R} \longrightarrow \mathbb{R}$ denote $T_a(x) = x - a$, and $\lfloor a \rfloor$ the floor. Set

$$f_n(x) = \begin{cases} 2nx & \text{if } x \in \left[0, \frac{1}{2n+1}\right] \\ \frac{2n}{2n+1} + \frac{1}{2n}\left(x - \frac{1}{2n+1}\right) & x \in \left[\frac{1}{2n+1}, 1\right] \end{cases}.$$

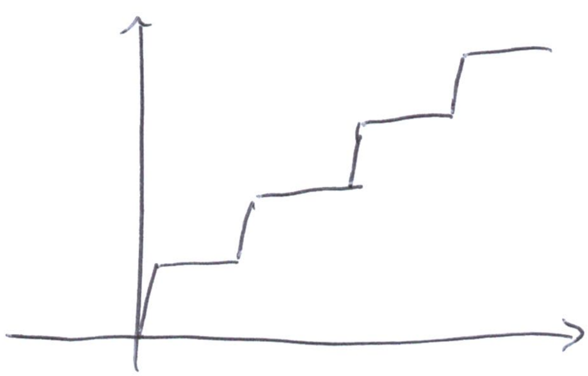


$f_n(x)$.

Define $\bar{f}_n : \mathbb{R} \longrightarrow \mathbb{R}$ to be

$$\bar{f}_n(x) = (T_{\lfloor y \rfloor})^{-1} \circ f_n \circ T_{\lfloor y \rfloor}(y)$$

ie.



stack many of the f_n's.

For $i = 0, \ldots, n-1$, set

$$g_{i,n} = (T_{i/n})^{-1} \circ \bar{f}_n \circ T_{i/n} \quad (\text{~~scale~~ shift by } 1/n).$$

Theorem: The subgroup of $\mathrm{Homeo}_+(\mathbb{R})$ generated by $\{g_{0,n}, \ldots, g_{n-1,n}\}$ is a free group of rank n.

Proof: Again, locate sets $X_i \subset \mathbb{R}$ such that $g_{i,n}(X_i) \subset X_i^c$ for all i.

This means that free groups inherit many properties of $\mathrm{Homeo}_+(\mathbb{R})$, for example, left-orderability.

(Actually it turns out that F_n is bi-orderable).

Aside from these "baby" examples, does something like the ping-pong lemma come up in "real" research?

Yes.

Theorem (Tits Alternative).

Let G be a finitely generated linear group over a field. Then G is solvable-by-finite or contains a non-cyclic free group.

There are many far-reaching consequences to this, e.g. by Gromov dealing with group growth, etc.

In every known proof of Tit's theorem, and in every proof of generalizations of this theorem, the final steps (creating a free subgroup) follow from a ping-pong argument.

Some sample consequences:

<u>Theorem</u>: A linear group is not amenable iff it contains a non-abelian free group.

More famously,

<u>Theorem</u> (Gromov).
Every finitely generated group of polynomial growth is nilpotent-by-finite.

(Thus you can determine the algebraic structure of the group simply by knowing that the Cayley balls centred at the origin grow in a polynomial fashion).