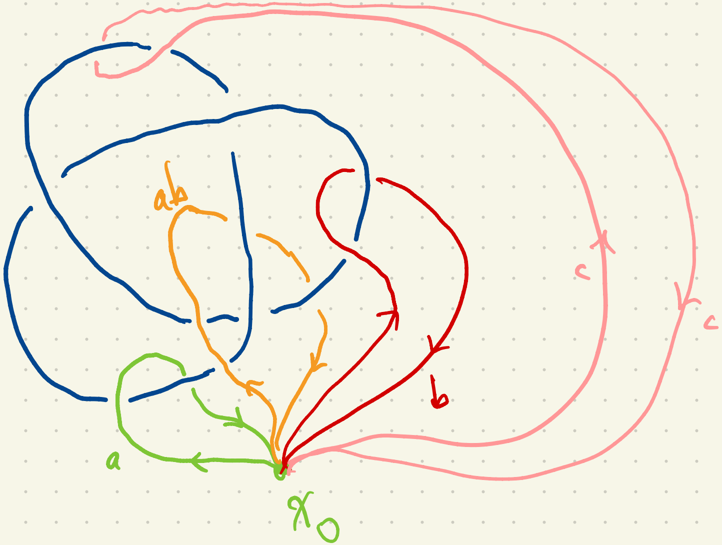
Group Theory

Book 3



$$ab = bc = ca \quad \Rightarrow \quad c = b^{-1}ab = aba^{-1}$$

$$\pi_1(\mathbb{R}^3 - K) = \langle a, b, c : ab = bc = ca \rangle = \langle x, y : x^3 = y^2 \rangle$$

$$\left.\begin{array}{l} x = ab = bc = ca \\ y = abc \end{array}\right\} \Rightarrow x^3 = ab \cdot ca \cdot bc = abc \cdot abc = y^2$$

Observation: $\pi_1(\mathbb{R}^3 - K)$ has no (nontrivial) torsion elements (a "torsion" element in a group is an element of finite order)

If X is a path-connected subset of $\mathbb{R}^2$ then $\pi_1(X)$ has no (nontrivial) torsion elements. (known for a few decades, this considered "folklore"). Intuitive!

The real proj. plane $P^2\mathbb{R}$ has torsion (its fund. gp. $\pi_1(P^2\mathbb{R})$ has order 2). ← a subspace of $\mathbb{R}^4$, not embeddable in $\mathbb{R}^3$.

For (top. spaces) subsets $X \subset \mathbb{R}^4$, $\pi_1(X)$ can have nontrivial torsion elements.

What about $X \subset \mathbb{R}^3$? Can $\pi_1(X)$ have nontrivial torsion elements? Famous open problem.

We will show $SL_2(\mathbb{Z})$ has a subgroup isomorphic to F_2:

$$\left\langle \begin{bmatrix}1&2\\0&1\end{bmatrix}, \begin{bmatrix}1&0\\2&1\end{bmatrix} \right\rangle < SL_2(\mathbb{Z})$$

use the <u>Ping-Pong Lemma</u>:

One version is as follows.

Let G be a group acting on a set X. We can think of G as a subgroup of

$\mathrm{Sym}\,X = \{\text{bijections } X \to X\}$

i.e. permutations of X. Here I'm using left action, so we compose "right-to-left"

More generally, to say G acts on X means: For every $g \in G$ we have a a permutation of X, $x \mapsto gx$

such that for all $g, h \in G$, $g(hx) = (gh)x$ i.e. the map $G \to \mathrm{Sym}\,X$ is a group homomorphism.

If the map $G \to \mathrm{Sym}\,X$ is one-to-one, we say G acts <u>faithfully</u> on X.

(So G is identified with a subgroup of $\mathrm{Sym}\,X$.)

Eg. $SL_2(F)$ acts on P^1F as fractional linear transformations.

$$\begin{array}{ccc} SL_2(F) & & P^1F = F \cup \{\infty\} \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ \begin{bmatrix}a&b\\c&d\end{bmatrix} & & x \end{array} \qquad \begin{bmatrix}a&b\\c&d\end{bmatrix}(x) = \frac{ax+b}{cx+d}$$

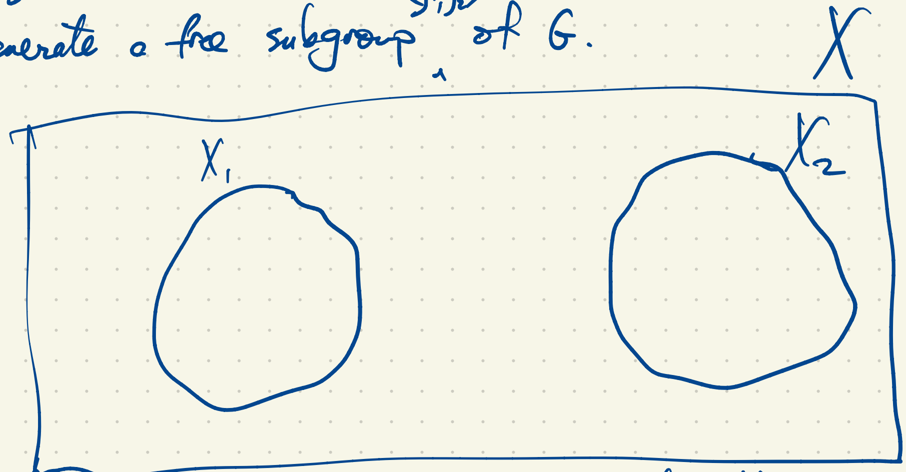
But this action is not faithful: $\begin{bmatrix}a&b\\c&d\end{bmatrix}$ and $-\begin{bmatrix}a&b\\c&d\end{bmatrix}$ give the same frac. lin. transf.

$PSL_2(F)$ acts faithfully on P^1F.

Given two nonempty subsets $X_1, X_2 \subset X$ which are disjoint and two elements $g_1, g_2 \in G$ such that

$$\left.\begin{array}{l} g_1^k(X_2) \subseteq X_1 \\ \text{and} \quad g_2^k(X_1) \subseteq X_2 \end{array}\right\} \text{ for all integers } k \neq 0$$

then g_1, g_2 generate a free subgroup $\langle g_1, g_2\rangle$ of G.



Proof A nontrivial word in two generators looks like

$w = g_1^{k_1} g_2^{l_1} g_1^{k_2} g_2^{l_2} \cdots g_1^{k_{r-1}} g_2^{l_{r-1}} g_1^{k_r}$ $\quad k_i, l_j$ nonzero integers up to conjugacy in the free group.

Then $w \neq 1$ since it maps $X \to X_1$.

Distinct words in the generators w_1, w_2 must give distinct permutations of X by considering $w = w_1^{-1} w_2$. $\square$

Application: $SL_2(\mathbb{Z})$ has $F_2 = \langle a,b \rangle$ (free group of rank 2) as a subgroup.

Try $u = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $v = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. This doesn't work. These generate $\langle u,v \rangle = SL_2(\mathbb{Z})$

but this is not a free group since

$$uv^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}, \quad (uv^{-1})^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad (uv^{-1})^6 = 1.$$

Next try $a = u^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$, $b = v^2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$. These generate $\langle a,b \rangle \cong F_2$.

To prove this, use the Ping-Pong Lemma.

$G = SL_2(\mathbb{Z})$ acts on $P^1\mathbb{Q} = \mathbb{Q} \cup \{\infty\}$ by fractional linear transformations

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}(x) = \frac{ax+b}{cx+d}$$

Let $X_1 = \{x \in P^1\mathbb{Q} : |x| < 1\}$, $X_2 = \{x \in P^1\mathbb{Q} : |x| > 1\}$. Note: $\infty \in X_2$.

$$\begin{tikzcd} X_1 \arrow[r, bend left, "a^{*}"] & X_2 \arrow[l, bend left, "b^{*}"] \end{tikzcd}$$

$b^n = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 0 \\ 2n & 1 \end{bmatrix}$, $\quad a^n = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix}$ $\quad n \neq 0$

$$a^n(x) = \frac{1x + 2n}{0x + 1} = x + 2n$$

If $x \in X_1$ then $|x_1| < 1$ ie. $-1 < x_1 < 1$

then $a^n(x) \in (2n-1, 2n+1)$

so $|a^n(x)| > 1$ ie. $a^n(x) \in X_2$.

for $n \neq 0$.

If $x \in X_2$ then $|x| > 1$

$$b^n(x) = \frac{1x + 0}{2nx + 1} = \frac{1}{2n + \frac{1}{x}}, \quad \left|\frac{1}{x}\right| < 1, \quad \left|2n + \frac{1}{x}\right| > 1,$$

$$|b^n(x)| = \left|\frac{1}{2n + \frac{1}{x}}\right| < 1, \quad b^n(x) \in X_1.$$

$\square$

In $G = SL_2(\mathbb{Z})$, $\langle a,b\rangle \cong F_2$.

Similarly in $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$, $\langle a,b\rangle \cong F_2$.

$$\langle a,b\rangle = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} : a_1, a_2, a_3, a_4 \in \mathbb{Z};\ a_1a_4 - a_2a_3 = 1;\ a_1, a_4 \text{ odd};\ a_2, a_3 \text{ even} \right\}.$$

In $SL_2(\mathbb{Z})$ elements have one of the forms

$$\begin{bmatrix} \text{odd} & \text{even} \\ \text{even} & \text{odd} \end{bmatrix}, \begin{bmatrix} \text{even} & \text{odd} \\ \text{odd} & \text{even} \end{bmatrix}, \begin{bmatrix} \text{odd} & \text{odd} \\ \text{even} & \text{odd} \end{bmatrix}, \begin{bmatrix} \text{odd} & \text{even} \\ \text{odd} & \text{odd} \end{bmatrix}, \begin{bmatrix} \text{even} & \text{odd} \\ \text{odd} & \text{odd} \end{bmatrix}, \begin{bmatrix} \text{odd} & \text{odd} \\ \text{odd} & \text{even} \end{bmatrix},$$

$$\cancel{\begin{bmatrix} \text{even} & \text{odd} \\ \text{even} & \text{odd} \end{bmatrix}}, \ldots$$ ten choices of parity are excluded in $SL_2(\mathbb{Z})$.

$|SL_2(\mathbb{F}_2)| = 2(2^2-1) = 6$ $\quad SL_2(\mathbb{F}_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}$

Reducing matrix entries mod 2 gives an epimorphism (surjective homomorphism) $SL_2(\mathbb{Z}) \to SL_2(\mathbb{F}_2)$.

The kernel of this map is $\Gamma(2) = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \in SL_2(\mathbb{Z}) : a_1, a_4 \text{ odd};\ a_2, a_3 \text{ even} \right\} = \langle a,b\rangle$
(a principal congruence subgroup) $\quad [SL_2(\mathbb{Z}) : \Gamma(2)] = 6.$

Tits Alternative: G linear group over F $\Rightarrow$ either

G virtually solvable

or G has F_2 as a subgroup (exclusive 'or').

conjectured originally by Bass & Serre

A linear group is a matrix group over a field F, in particular $GL_n(F)$ and its subgroups such as $SL_n(F)$, $O_n(F)$, $U_n(F)$, $Sp_n(F)$, ...

Tits proved that the alternative holds in GL_n.

G is solvable if it has a composition series with abelian factors ie.

$G_0 = 1 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$ with G_k / G_{k-1} abelian.

eg. S_3 is solvable: $1 \triangleleft A_3 \triangleleft S_3$

G is virtually solvable if it has a solvable subgroup of finite index.

Every finite group is virtually solvable by considering the trivial subgroup.

Eg. the linear group $O_2(\mathbb{R}) = \{\text{orthogonal } 2\times 2 \text{ real matrices}\} = \{A \in GL_2(\mathbb{R}) : A^T A = I\}$

If $A \in O_n(\mathbb{R})$ then $AA^T = A^T A = I$, so $(\det A)^2 = 1 \Rightarrow \det A = \pm 1$.

$SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) : \det A = 1\}$ = special orthogonal group = $\{\text{rotations fixing } 0 \in \mathbb{R}^n\}$

$[O_n(\mathbb{R}) : SO_n(\mathbb{R})] = 2$

$SO_2(\mathbb{R}) \cong S^1$ as Lie groups (abelian)

$\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a^2+b^2=1 \right\}$

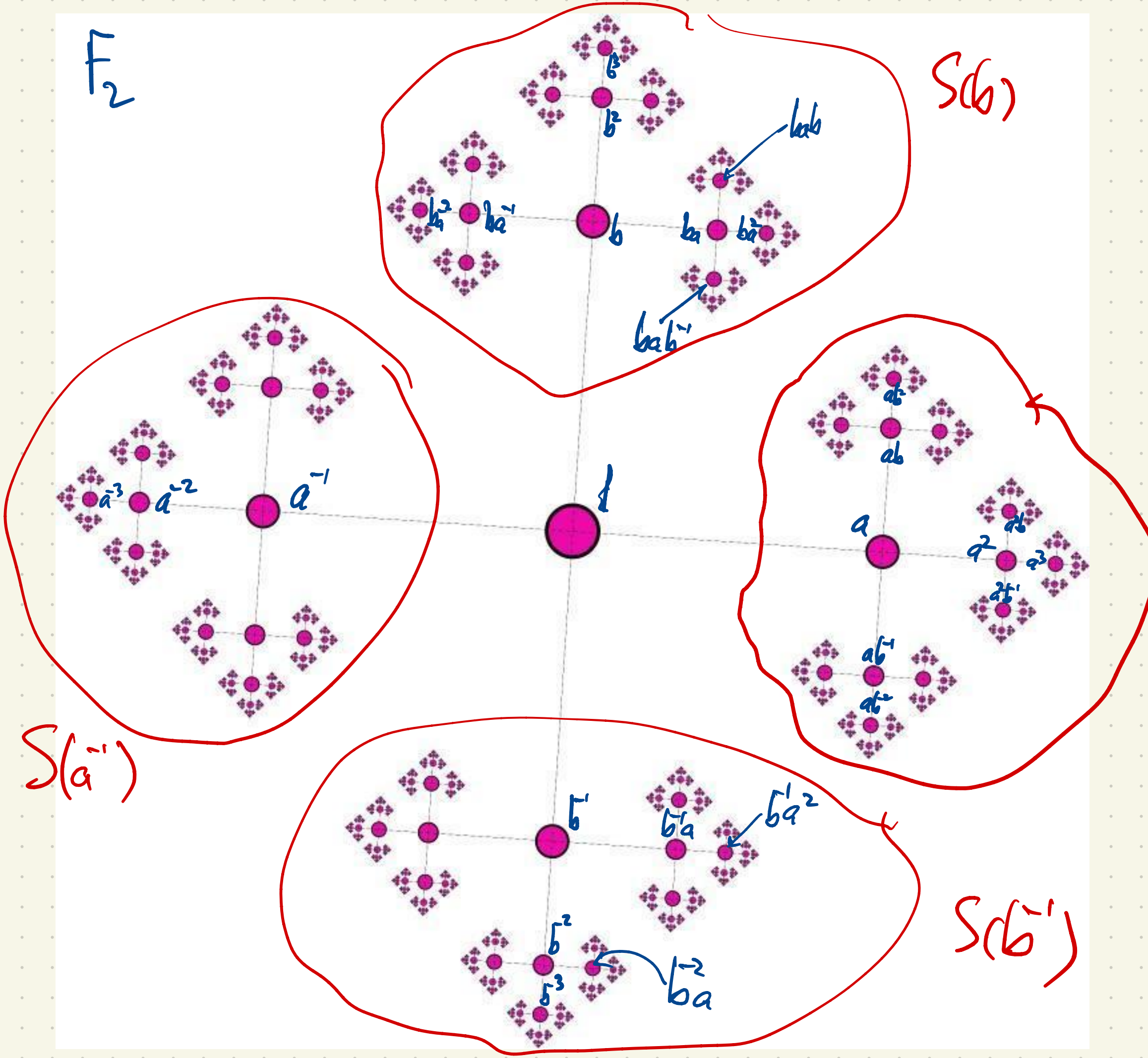
$O_2(\mathbb{R})$ is nonabelian but solvable. $\quad 1 \triangleleft SO_2(\mathbb{R}) \triangleleft O_2(\mathbb{R})$

$O_2(\mathbb{R})$ cannot have a subgroup isomorphic to F_2.

$SO_3(\mathbb{R})$ has a subgroup $\cong F_2$. See handout on free groups.

F_2 has a "paradoxical decomposition" $\quad F_2 = A \sqcup B \sqcup C \sqcup D \quad$ (disjoint union i.e. partition)

$F_2 = g_1 A \sqcup g_2 B = g_3 C \sqcup g_4 D \qquad g_i \in F_2$.

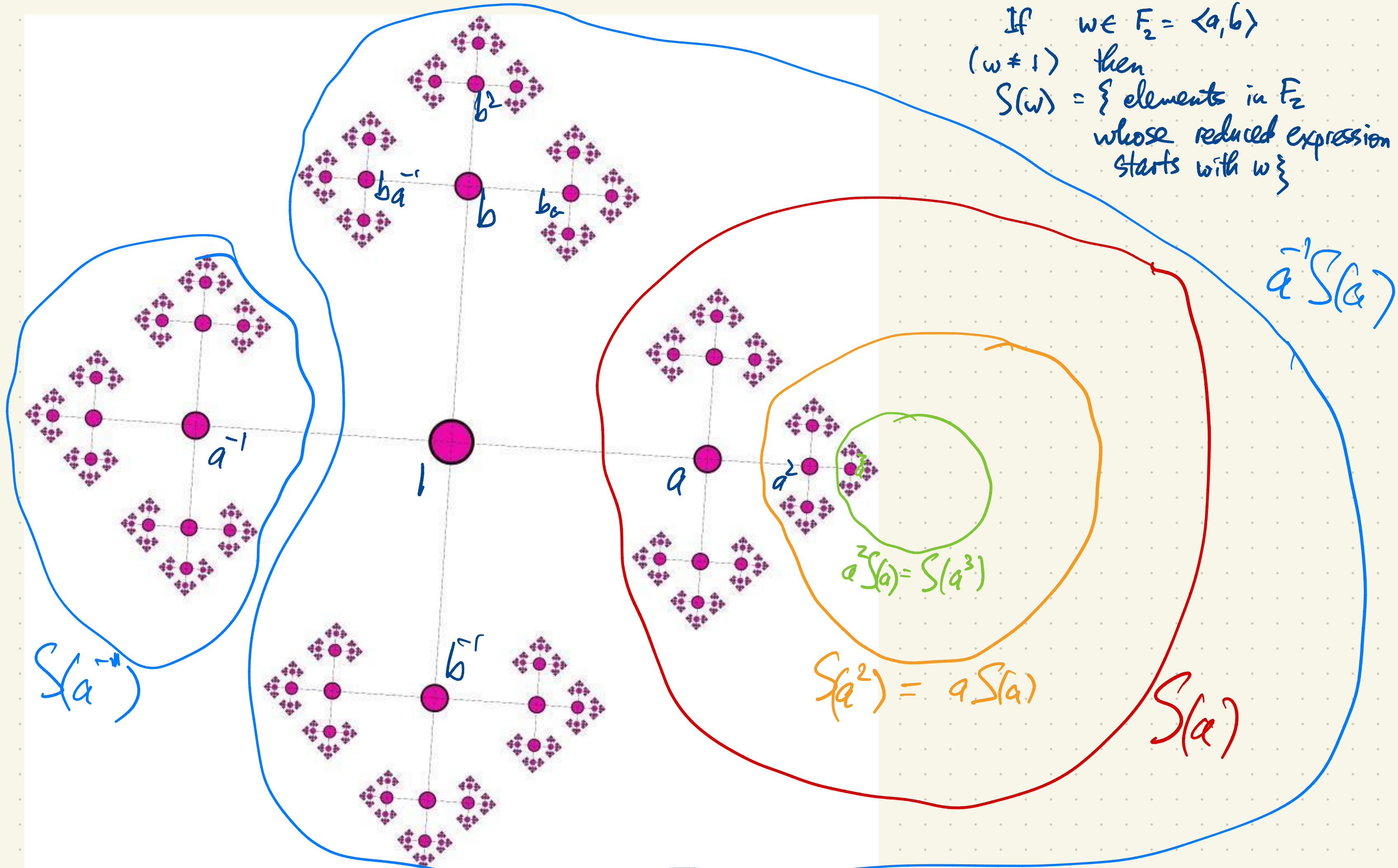


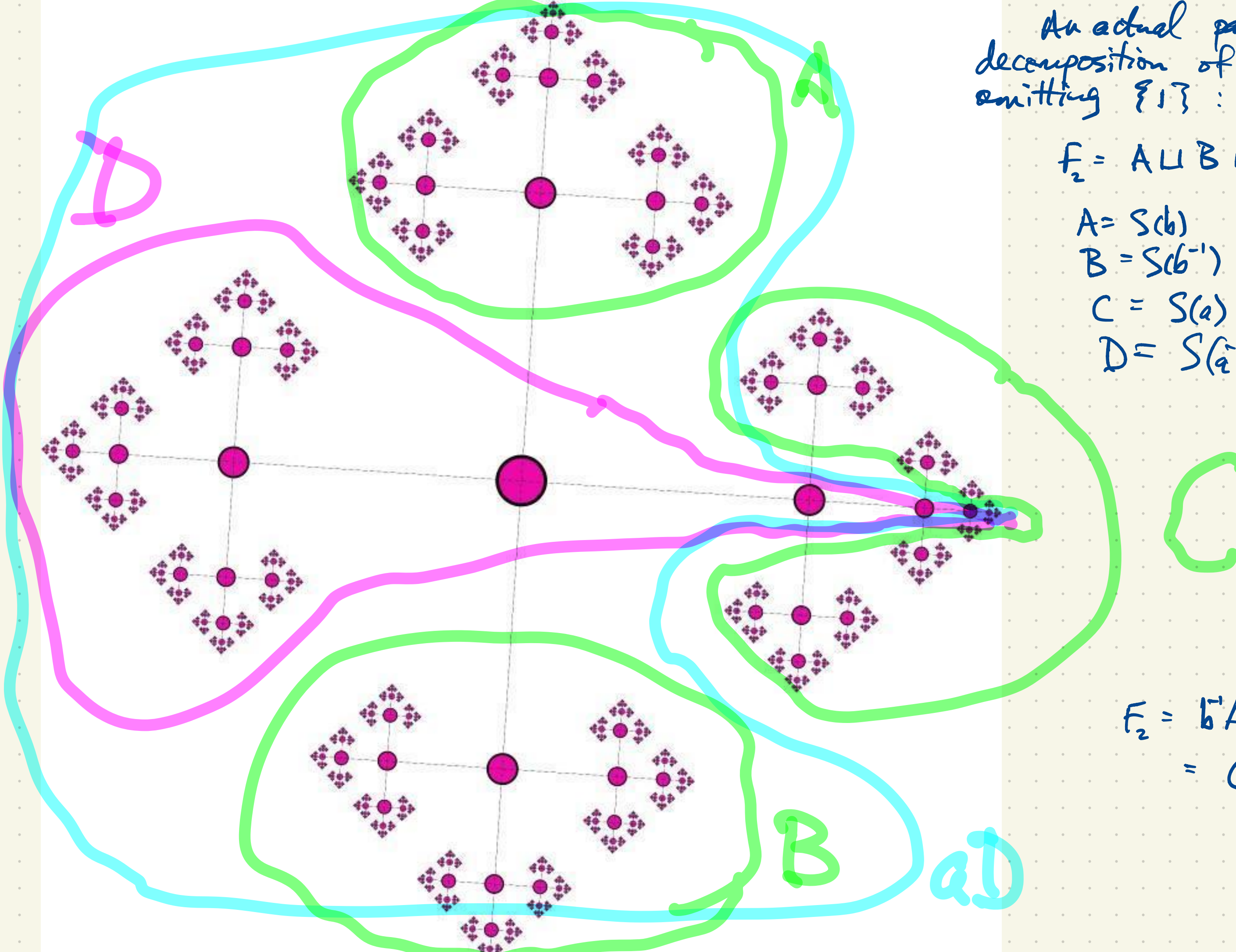
If $w \in F_2$, $w \neq 1$ then $S(w) \subset F_2$ is the subset consisting of words starting with w (they have w as a prefix). I'm only considering reduced words.

$$F_2 = S(a^{-1}) \cup a^{-1}S(a)$$
$$= S(b^{-1}) \cup b^{-1}S(b)$$
$$= \{1\} \cup S(a) \cup S(b)\, S(a^{-1}) \cup S(b^{-1})$$

This is almost a paradoxical decomposition of F_2 (unfortunately $\{1\}$ is "left over" ...)

If $w \in F_2 = \langle a, b \rangle$ $(w \neq 1)$ then
$S(w) = \{$ elements in F_2 whose reduced expression starts with $w \}$





An actual paradoxical decomposition of F_2 without omitting $\{1\}$:

$$F_2 = A \sqcup B \sqcup C \sqcup D$$

$$A = S(b)$$
$$B = S(b^{-1})$$
$$C = S(a) - \{a, a^2, a^3, a^4, \dots\}$$
$$D = S(a^{-1}) \cup \{1, a, a^2, a^3, a^4, \dots\}$$

$$F_2 = b^{-1}A \sqcup B$$
$$= C \sqcup aD$$

Banach-Tarski Theorem

Let $X = \{(x,y,z) \in \mathbb{R}^3 : x^2+y^2+z^2 \le 1\}$.

Then there exists a partition $X = X_1 \sqcup X_2 \sqcup X_3 \sqcup X_4 \sqcup X_5$ such that

$$X = g_1 X_1 \sqcup g_2 X_2 = g_3 X_3 \sqcup g_4 X_4 \sqcup g_5 X_5$$ for some $g_1, \dots, g_5$ direct isometries of $\mathbb{R}^3$.

(orientation-preserving isometries)

An isometry is a transformation preserving distances.

Every isometry either preserves or reverses orientation.

e.g. rotations

The subsets $X_1, \dots, X_5$ are not all Lebesgue-measurable.

Since $F_2 = g_1 A \sqcup g_2 B = g_3 C \sqcup g_4 D = A \sqcup B \sqcup C \sqcup D$

and $SO_3(\mathbb{R})$ has a subgroup $\langle a,b \rangle \cong F_2$

the group $SO_3(\mathbb{R})$ also admits such a "paradoxical decomposition":

Let $T \subset SO_3(\mathbb{R})$ be a right transversal for $\langle a,b \rangle < SO_3(\mathbb{R}) = \bigsqcup_\alpha \langle a,b \rangle t_\alpha$

subset, not subgroup

i.e. set of representatives of the right cosets

$T = \{t_\alpha : \alpha\}$

$SO_3(\mathbb{R}) = \langle a,b \rangle T$

$$SO_3(\mathbb{R}) = AT \sqcup BT \sqcup CT \sqcup DT = g_1 AT \sqcup g_2 BT = g_3 CT \sqcup g_4 DT$$

Note: A paradoxical composition requires a finite number of pieces; there is nothing paradoxical about an infinite number of pieces.

Why can't a disk $X = \{(x,y) \in \mathbb{R}^2 : x^2+y^2 \le 1\}$ admit a "paradoxical decomposition"?

If $X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_5$ (or some other finite number of pieces)

with $X = g_1 X_1 \sqcup g_2 X_2 = g_3 X_3 \sqcup g_4 X_4 \sqcup g_5 X_5$, $g_1, \cdots, g_5$ isometries, what is the contradiction?

To obtain a contradiction we cannot invoke Lebesgue measure (i.e. area) since the subsets X_i aren't necessarily Lebesgue measurable.

We use finitely additive measure.

Clara Löh, Geometric group theory

A finitely additive measure on a set X is a function $\mu : \mathcal{P}(X) \to [0,\infty]$
($\mathcal{P}(X)$ = power set of X = {all subsets of X}) such that

$$\mu(A_1 \sqcup A_2 \sqcup \cdots \sqcup A_k) = \mu(A_1) + \cdots + \mu(A_k)$$

($A \sqcup B$ = disjoint union of A and B)

Now suppose G is a group acting on X i.e. group elements permute the points of X. We'll denote this as a left action: $g : X \to X$ is bijective mapping $x \mapsto g(x)$.

If $A \subseteq X$ then $g(A) = \{ g(a) : a \in A \}$. So g acts naturally on $\mathcal{P}(X)$.

Note: $(gh)(A) = g(h(A))$.

We often write $G \curvearrowright X$ to say G acts on X.

We say the f.a. measure μ is G-invariant if $\mu(gA) = \mu(A)$ for all $A \subseteq X$, $g \in G$.

eg. $X = \mathbb{R}^n$, $G = \{$direct isometries of $\mathbb{R}^n\}$.

If X has a f.a. G-invariant measure μ on X and $E \subseteq X$ with $\mu(E) < \infty$ then E cannot have a paradoxical decomposition with respect to G.

Eg. $n=2$. $G = \{\text{direct isometries of } \mathbb{R}^2\}$.

$$E = \{(x,y)\in\mathbb{R}^2 : x^2+y^2 \le 1\}.$$

There is a f.a. G-invariant measure on $\mathbb{R}^2$ with $\mu(E)=1$.
Consequently E has no "paradoxical decomposition" with respect to G.

There is no partition $E = E_1 \sqcup E_2 \sqcup E_3 \sqcup E_4 \sqcup E_5$ such that

$$E = g_1 E_1 \sqcup g_2 E_2 = g_3 E_3 \sqcup g_4 E_4 \sqcup g_5 E_5, \qquad g_1, \dots, g_5 \in G.$$

Proof by contradiction: Assume such a decomposition exists. Then

$$\begin{aligned} 1 = \mu(E) &= \mu(E_1) + \cdots + \mu(E_5) \\ &= \mu(g_1 E_1) + \mu(g_2 E_2) = \mu(g_3 E) + \mu(g_4 E_4) + \mu(g_5 E_5) \\ &= \mu(E_1) + \mu(E_2) = \mu(E_3) + \mu(E_4) + \mu(E_5) \end{aligned}$$

Contradiction.

In $n=3$ dimensions there is no f.a. measure invariant under direct isometries.

An action of G on X is amenable if X has a f.a. probability measure invariant under G. (Rather than $\mu : \mathcal{P}(X) \to [0,\infty]$ we have $\mu(X) = 1$, $\mu : \mathcal{P}(X) \to [0,1]$.)

A group G is amenable if the left-action on itself is amenable. Here G has a f.a.p. measure $\mu : \mathcal{P}(G) \to [0,1]$, $\mu(G) = 1$, such that $\mu(gA) = \mu(A)$ for all $g \in G$, $A \subseteq G$.

All finite groups are amenable.
All abelian groups are amenable. (Not quite obvious!)
All solvable groups are amenable.
The group F_n $(n \geq 2)$ is not amenable.

$$F_2 = A \sqcup B \sqcup C \sqcup D$$
$$= g_1 A \sqcup g_2 B = g_3 C \sqcup g_4 D \qquad g_i \in F_2 .$$

$\ell(a^2 b) = \ell(aab) = 3$

$F_2 = \langle a, b \rangle$ has $\begin{cases} 1 & \text{if } n = 0 \\ 1 + 4 \cdot 3^{n-1} & \text{if } n \geq 1 \end{cases}$ words of length at most n.

$\ell(a^{-1} b a^3 b^{-1}) = 6$.

What is a f.a.p. measure on $\mathbb{Z}$, invariant (under translation)? or not?

Let $A \subseteq \mathbb{Z}$. We want a f.a.p. measure $\mu(A) \in [0,1]$, $\mu(\mathbb{Z}) = 1$?

$A = 2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, 6, \dots\}$

$B = 2\mathbb{Z}+1 = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$

$\mathbb{Z} = A \sqcup B \Rightarrow 1 = \mu(\mathbb{Z}) = \mu(A) + \mu(B)$.

In order for μ to be translation-invariant, $\mu(A) = \mu(B) = \frac{1}{2}$.

For every $A \subseteq \mathbb{Z}$: $\qquad \mu\{\text{primes}\} = 0$.

We probably want $\mu(A) = \lim_{n\to\infty} \frac{|A \cap [-n, n]|}{2n+1}$.

However this limit is not defined for arbitrary $A \subseteq \mathbb{Z}$.

Eg. $A = \{n \in \mathbb{Z} : |n| \text{ has first digit } 1 \text{ when written in decimal form}\}$.

For $n = 100$, $A \cap [-100, 100] = \{-100, -19, -18, \dots, -10, -1, 1, 10, 11, \dots, 19, 100\}$, $|A \cap [-100, 100]| = 24$

$$\frac{|A \cap [-100, 100]|}{2\cdot 100+1} = \frac{24}{201} \approx 0.119$$

for $n = 200$, $A \cap [-200, 200] = \{\underbrace{\pm 1}_{2}, \underbrace{\pm 10, \dots, \pm 19}_{20}, \underbrace{\pm 100, \dots, \pm 199}_{200}\}$, $|A \cap [-200, 200]| = 222$,

$$\frac{|A \cap [-200, 200]|}{2\cdot 200+1} = \frac{222}{401} \approx 0.5536$$

Replace $\lim_{n\to\infty} \frac{|A \cap [-n, n]|}{2n+1}$ by $\operatorname{glim}_{n\to\infty} \frac{|A \cap [-n, n]|}{2n+1}$

There is a "new improved limit" defined for every bounded sequence $a_0, a_1, a_2, \dots$ in $\mathbb{R}$

we can define $\operatorname{glim}_{n\to\infty} a_n$ satisfying

(i) If (a_n) converges then $\operatorname{glim}_{n\to\infty} a_n = \lim_{n\to\infty} a_n$

(ii) If $a_n \in [M_1, M_2]$ then $\operatorname{glim}_{n\to\infty} a_n \in [M_1, M_2]$

(iii) $\operatorname{glim}_{n\to\infty} a_n$ is a cluster point of (a_n) (there is at least one cluster point of (a_n) in $[M_1, M_2]$ by Bolzano-Weierstrass)

(iv) $\operatorname{glim}_{n\to\infty} (a_n + b_n) = \operatorname{glim}_{n\to\infty} a_n + \operatorname{glim}_{n\to\infty} b_n$

$\operatorname{glim}_{n\to\infty} a_n b_n = (\operatorname{glim}_{n\to\infty} a_n)(\operatorname{glim}_{n\to\infty} b_n)$

Define $\mu(A) = \operatorname{glim}_{n\to\infty} \dfrac{|A \cap [-n, n]|}{2n+1}$