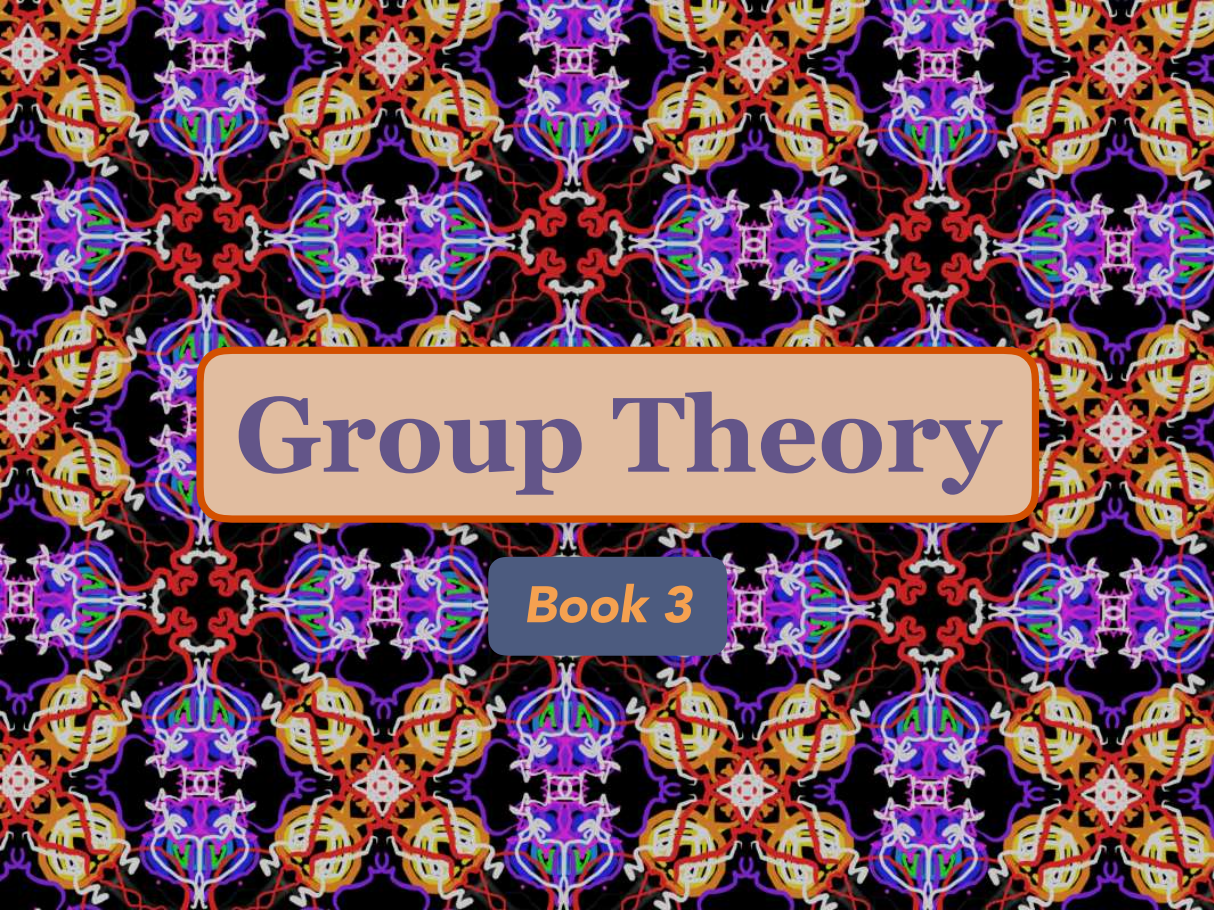
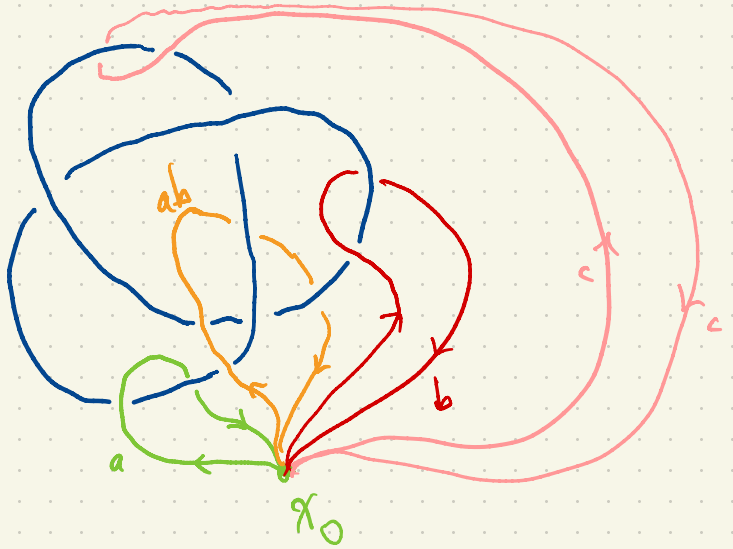

Group Theory
Book 3



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

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

$\cong \langle x, y : x^3 = y^2 \rangle$

$x = ab = bc = ca$
$y = abc$
$\Rightarrow x^3 = ab \cdot ca \cdot bc = abc \cdot abc = y^2$

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)

(top. spaces) ↪ a subspace of $\mathbb{R}^4$, not embeddable in $\mathbb{R}^3$.

For 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 Ping-Pong Lemma:

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, $x \longmapsto gx$

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 faithfully 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.

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

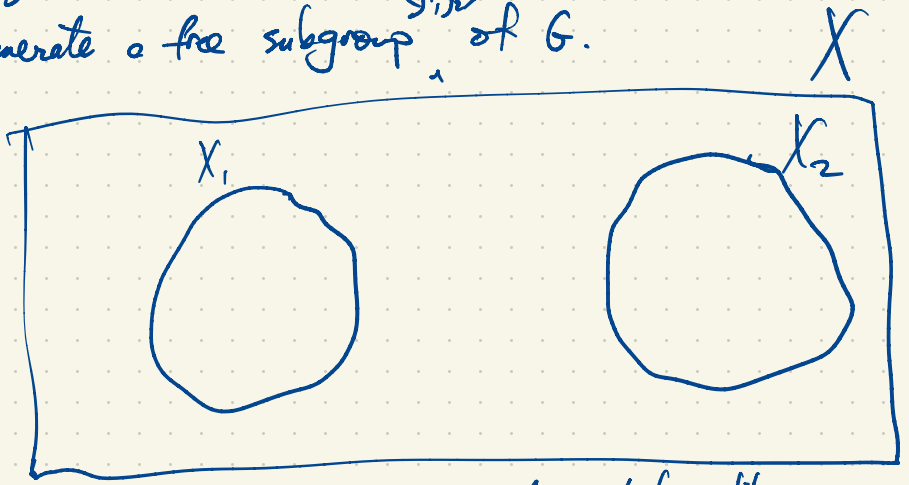
But this action is not faithful: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $-\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ give the same frac. lin. transf.

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

Given two subsets $X_1, X_2 \subset X$ which are disjoint (non-empty) and two elements $g_1, g_2 \in G$ such that

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

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

$$w = g_1^{k_1} g_2^{l_1} g_1^{k_2} g_2^{l_2} \cdots g_1^{k_n} g_2^{l_n} g_1^{k_r} \qquad k_i, l_j \text{ nonzero integers}$$

up to conjugacy in the free group.

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

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

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

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

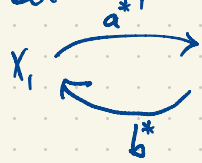
Next try $a = u^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$, $b = v^2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$. These generate $\langle a, b\rangle \cong F_2$.

To prove this, use the Ping-Pong Lemma.

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

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

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



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

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

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 $|x| > 1$

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

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

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

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

$\begin{bmatrix} \text{even} & \text{odd} \\ \text{even} & \text{odd} \end{bmatrix}$, ... 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: $1 \trianglelefteq A_3 \trianglelefteq S_3$

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 $O_2(\mathbb{R}) = \{\text{orthogonal } 2\times 2 \text{ real matrices}\} = \{A \in GL_2(\mathbb{R}) : A^TA = I\}$

If $A \in O_n(\mathbb{R})$ then $AA^T = A^TA = I$, 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 = $\{$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)

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

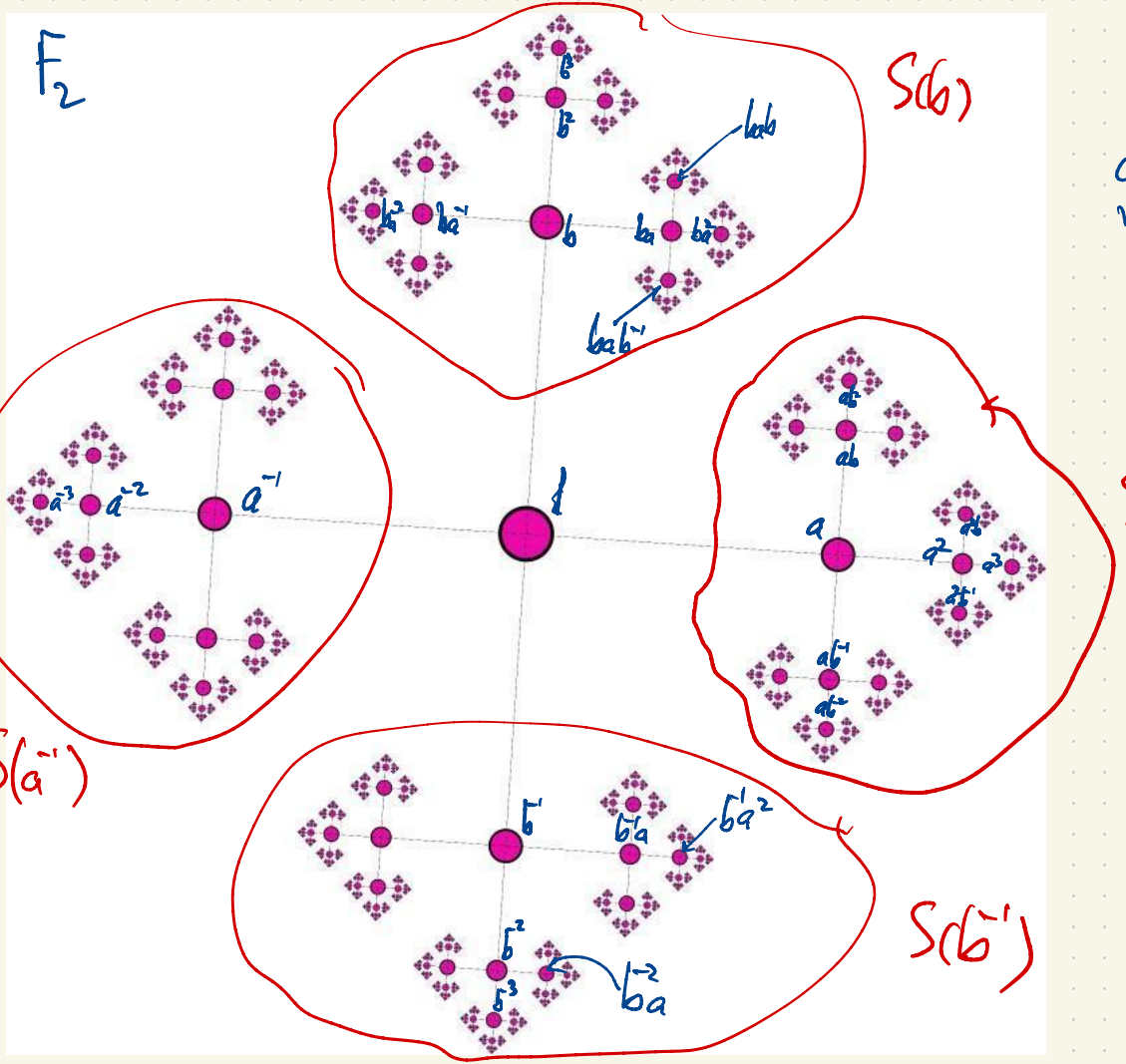
$O_2(\mathbb{R})$ is nonabelian but solvable. $\quad 1 \triangleleft SO_2(\mathbb{R}) \triangleleft O_2(\mathbb{R})$

$O_2(\mathbb{R})$ 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" $\quad F_2 = A \sqcup B \sqcup C \sqcup D$ (disjoint union ie. partition)

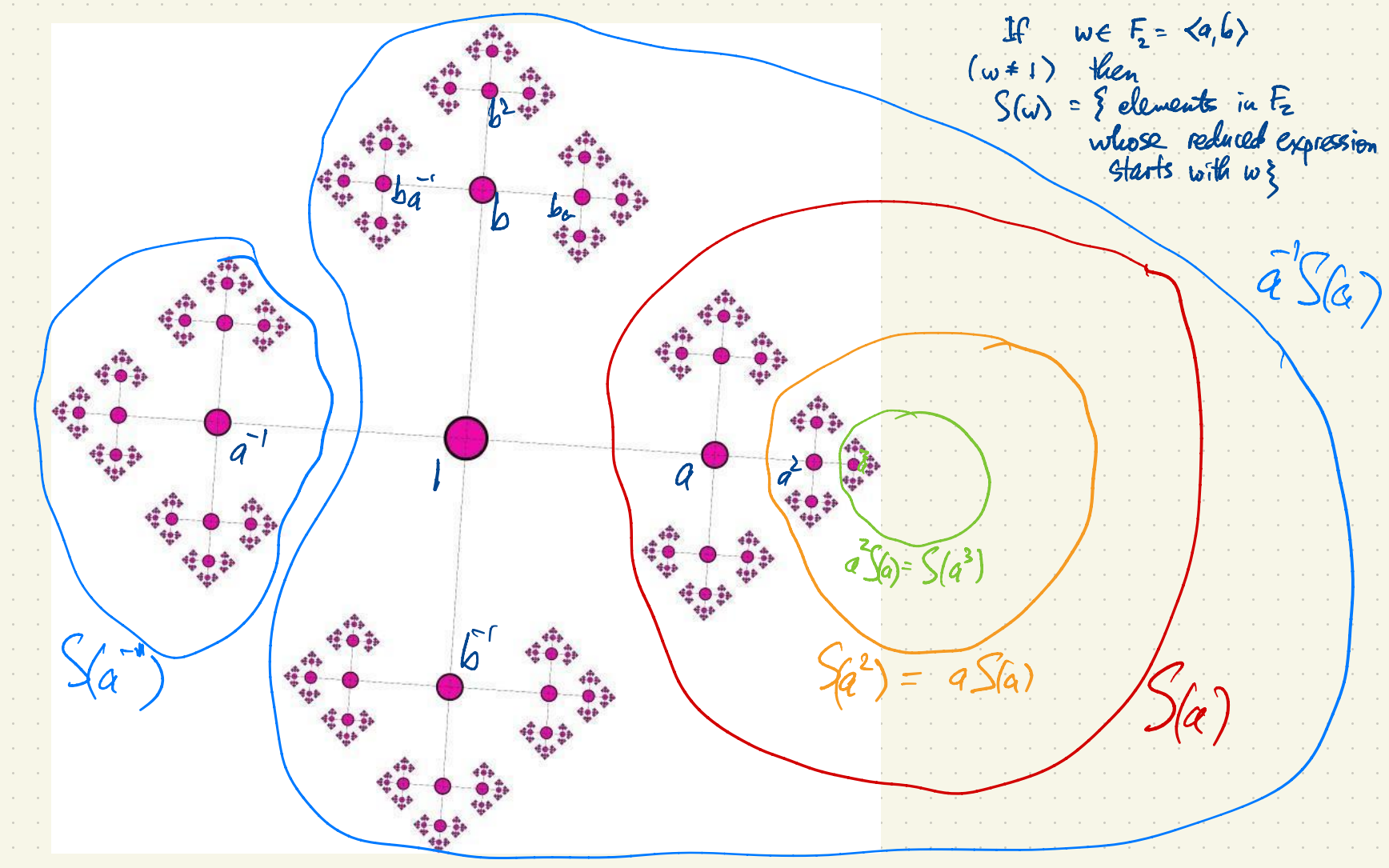
$F_2 = g_1 A \sqcup g_2 B = g_3 C \sqcup g_4 D \quad g_i \in F_2$.

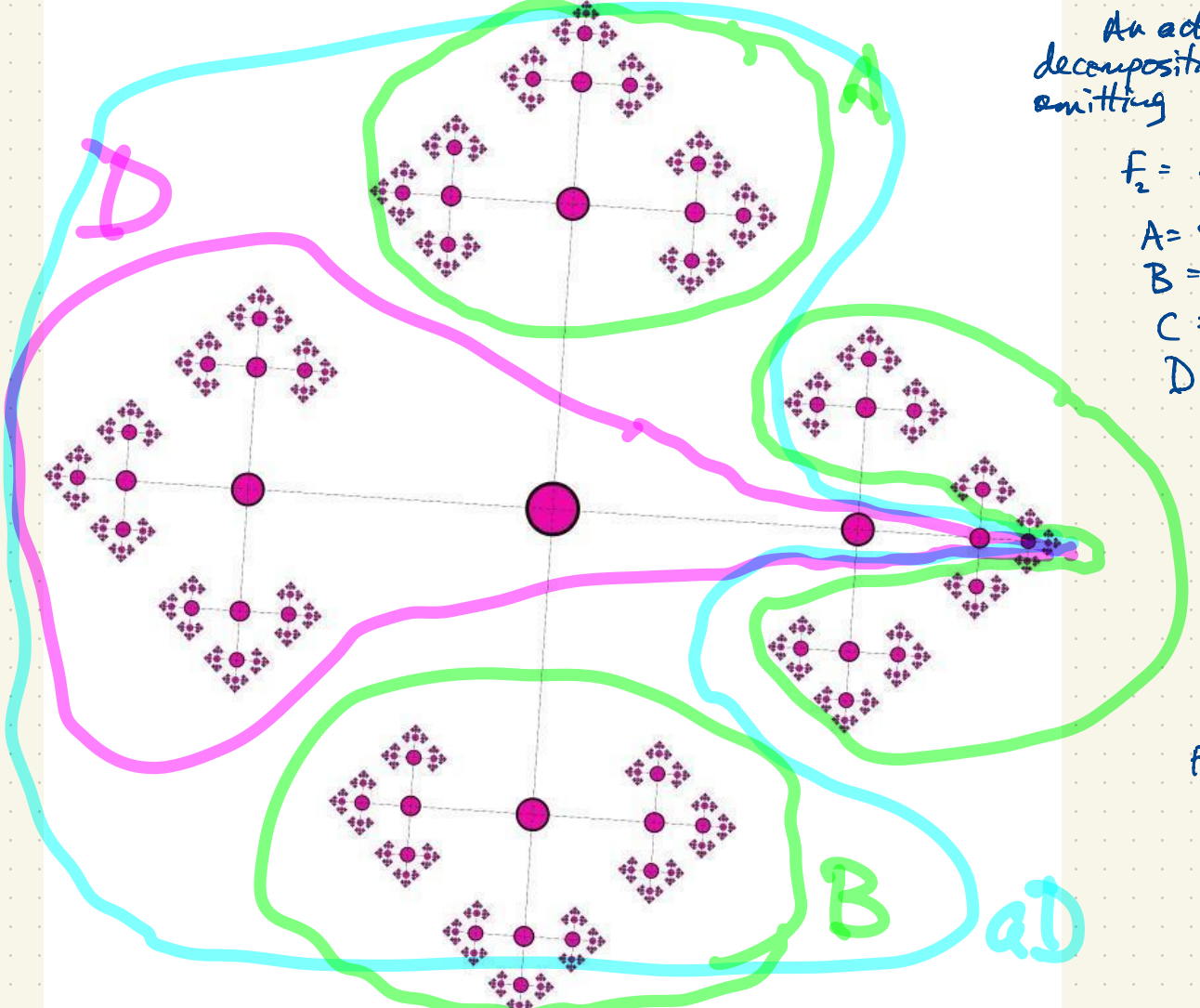


If $w \in F_2$, $w \neq 1$ then $S(w) \subset F_2$ is the subset consisting of words starting with w (they have w as a prefix). I'm only considering reduced words.

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

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 $w \}$
b^2
ba^{-1}
b
ba
a^{-1}
1
a
a^2
b^{-1}
$a^2S(a) = S(a^3)$
$S(a^2) = aS(a)$
$S(a)$
$a^{-1}S(a)$
$S(a^{-1})$



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

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

$A = S(b)$

$B = S(b^{-1})$

$C = S(a) - \{a, a^2, a^3, a^4, \ldots\}$

$D = S(a^{-1}) \cup \{1, a, a^2, a^3, a^4, \ldots\}$

$F_2 = bA \sqcup B$

$= C \sqcup aD$

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

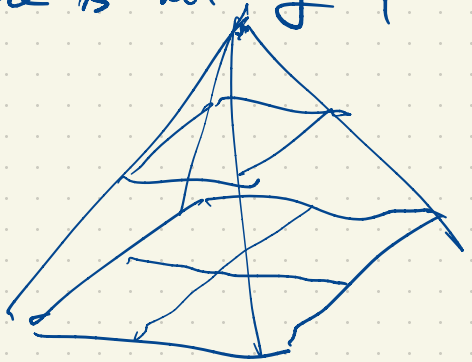
i.e. set of representatives of the right cosets

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

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

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

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 $X = g_1 X_1 \sqcup g_2 X_2 = g_3 X_3 \sqcup g_4 X_4 \sqcup g_5 X_5$, $g_1, \ldots, g_5$ 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

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

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.

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

$F_2 = \langle a, b \rangle$ 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.

$\ell(a^2b) = \ell(aab) = 3$
$\ell(a^{-1}ba^3b^{-1}) = 6$.

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 $A \subseteq \mathbb{Z}$:

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

$\mu\{\text{primes}\} = 0$.

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

Eg. $A = \{n \in \mathbb{Z} : |n|$ has first digit 1 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 $a_0, a_1, a_2, \ldots$ 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 $\mu(A) = \operatorname{glim}_{n\to\infty} \dfrac{|A \cap [-n, n]|}{2n+1}$

$\mathbb{R}^3 = \{(a_0, a_1, a_2) : a_i \in \mathbb{R}\}$ is a vector space over $\mathbb{R}$; it is also a ring

$(a_0, a_1, a_2)(b_0, b_1, b_2) = (a_0 b_0, a_1 b_1, a_2 b_2)$ commutative ring with identity

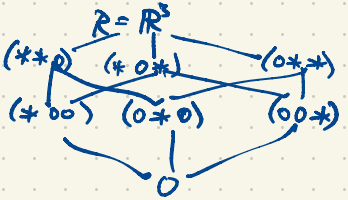
zero divisors: $(1,0,0)(0,1,0) = (0,0,0)$

There are infinitely many subspaces ($\mathbb{R}$-submodules)

2-dim. subspaces

1-dim subspaces

Ideals of $R = \mathbb{R}^3$: R-submodules



The subspace of $\mathbb{R}^3$ spanned by $(3,0,-5)$ i.e. $\{t(3,0,-5) : t \in \mathbb{R}\}$ is not an ideal
$(3t, 0, -5t)$

$(a_0, a_1, a_2)(-3,0,-5) = (*, 0, *) \qquad (a_0, a_1, a_2) \in R$

$R = \mathbb{R}^\infty = \{(a_0, a_1, a_2, a_3, \ldots) : a_i \in \mathbb{R}\}$ $\quad a+b = (a_0+b_0, a_1+b_1, \ldots)$ $\quad ab = (a_0b_0, a_1b_1, \ldots)$

commutative ring $R = \mathbb{R}^\infty$ with identity $1 = (1,1,1,\ldots)$ $\leftarrow$ $\quad r(1,1,1,\ldots) = (r,r,r,\ldots) = r$

$\lim a_n$ is defined on certain sequences forming a subspace of $\mathbb{R}^\infty$, where "lim" is a well-defined linear functional.

Extend this if possible to the subspace $l_\infty \subset \mathbb{R}^\infty$ consisting of bounded sequences.

This can be done using the Hahn-Banach Theorem.

Rather than use this, let's use an algebraic idea.

Start with the ideal $J \subset \mathbb{R}^\infty$ consisting of all sequences of finite support.

This is an ideal. (If $a, b \in J$ then $a+b \in J$. If $a \in J$ and $r \in R$, then $ra \in J$.)

$R(1,0,1,0,1,0,\ldots) = (*,0,*,0,*,0,\ldots)$ is an ideal not contained in J.

We want to extend J to a maximal ideal $M \subset R$ i.e. $J \subseteq M \subset R$

Such an extension exists by Zorn's Lemma. So $R/M \cong$ field of hyper-real numbers ${}^*\mathbb{R}$

${}^*\mathbb{R} \supset \mathbb{R}$

In $R = \mathbb{R}^\infty$, we have zero divisors e.g. $(1,0,1,0,1,0,\ldots)(0,1,0,1,0,1,\ldots) = (0,0,0,0,0,0,\ldots)$

$(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots) \in R$, $(1,2,3,4,5,\ldots) \in R$

Given a bounded sequence $a = (a_0, a_1, a_2, \dots) \in \mathbb{R} = \mathbb{R}^{\infty}$ so $a_n \in [M_1, M_2]$ for all n.

${}^*\mathbb{R}$ is totally ordered. For $u, v \in {}^*\mathbb{R}$ either $u = v$ or $u < v$ or $u > v$.

eg. $u = (1, -1, 1, -1, 1, -1, \dots)$, $v = (0, 0, 0, 0, 0, 0, \dots)$

Which $r \in \mathbb{R}$ give $r = (r, r, r, \dots) < (a_0, a_1, a_2, \dots) \in \mathbb{R}$?

There is a real $r \in \mathbb{R}$ which is maximal s.t. $(r, r, r, \dots) \leq (a_0, a_1, a_2, \dots)$ mod M mod M

This supremum gives $\operatorname{glim}_{n\to\infty}(a_n) = r$.

This gives a translation-invariant f.a.p. measure μ on $\mathbb{Z}$.

Same works over $\mathbb{R}$

and over any amenable group

$a = (a_0, a_1, a_2, \dots) < b = (b_0, b_1, b_2, \dots)$ mod M iff $b - a = (b_0 - a_0, b_1 - a_1, b_2 - a_2, \dots) > 0$

If M is a Tarski group of exponent p, is M amenable?

$|M_{12}| = 95040 = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 12_{(5)}$

M_{12} is a sharply 5-transitive permutation group of degree 12.
permuting 12 points

A permutation group G of degree n is k-transitive if for any two k-tuples of distinct points $(i_1, i_2, \cdots, i_k)$, $(j_1, j_2, \cdots, j_k)$, there is $g \in G$ mapping one k-tuple to the other.

There are $n_{(k)} = n(n-1)\cdots(n-k+1) = k!\binom{n}{k}$ ordered k-tuples $\{a_1, a_2, \cdots, a_k\}$ in order for G to be transitive on the k-tuples, we must have $n_{(k)}$ dividing $|G|$.

Moreover if $|G| = n_{(k)}$ we must be a unique $g \in G$ mapping one k-tuple to the other. In this case G is sharply k-transitive.

1-transitive: just transitive.

$\binom{n}{k}$ k-tuples

$n_{(k)} = n(n-1)(n-2)\cdots(n-k+1) = k!\binom{n}{k}$ ordered k-tuples

There are many transitive groups (i.e. 1-transitive).

Not so many 2-transitive groups.

The 3-transitive groups have long been classified. including M_{22}

The 4-transitive groups of finite degree S_n $(n \geq 4)$, A_n $(n \geq 6)$, M_{11}, M_{12}, M_{23}, M_{24}.

The 5-transitive groups S_n $(n \geq 5)$, A_n $(n \geq 7)$, M_{12}, M_{24}.

Where does M_{12} come from?

A Hadamard matrix of order n is an $n \times n$ matrix H with entries ± 1 such that $HH^T = nI$ (equivalently $H^T H = nI$)

eg. $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} + & + \\ + & - \end{bmatrix}$ of order 2

Every Hadamard matrix has order 1, 2, or $4k$ for some $k \geq 1$. (Is there one of every order $n = 4k$, $k \geq 1$? Big open problem. Smallest open case $n = 668$.)

For order $n \in \{1, 2, 4, 8, 12\}$, all Hadamard matrices of order n are equivalent.

Order 12:

$H_{12} =$

$$\begin{bmatrix}
+ & - & - & + & + & + & - & + & + & - & + & + \\
- & + & - & + & + & + & + & - & + & + & - & + \\
- & - & + & + & + & + & + & + & - & + & + & - \\
- & - & - & + & - & - & + & + & - & - & + & + \\
- & - & - & - & + & - & - & + & + & + & - & + \\
- & - & - & - & - & + & + & - & - & + & + & - \\
+ & - & - & + & - & - & + & - & + & + & + & + \\
- & + & - & + & - & - & - & + & - & + & + & + \\
- & - & + & + & - & - & - & - & + & - & + & + \\
+ & - & - & + & + & + & - & - & - & + & - & + \\
- & + & - & + & + & + & - & + & - & - & + & - \\
- & - & + & + & + & + & - & - & + & - & - & +
\end{bmatrix}$$

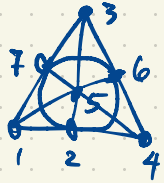
Every Had. matrix of order 12 has the form $MH_{12}M'$ where M, M' are 12×12 monomial matrices (each row/col. has an entry ± 1; all other entries are zeroes)

$2^{12} \cdot 12!$ monomial matrices.

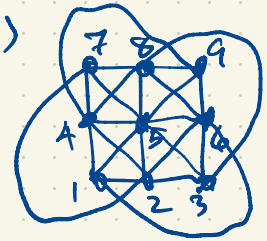
The equivalences from H_{12} to itself form a group $\cong 2M_{12}$ $\quad Z(2M_{12}) = \langle (-I, -I) \rangle$

$2M_{12} / Z_0(2M_{12}) = M_{12}$

A Steiner design $S(t,k,v)$ is a collection of k-element subsets of a v-set (called blocks) such that every t of the v points are in a unique block. blocks

eg. an $S(2,3,7)$ 

blocks 124, 235, ... 168 automorphisms

$S(2,3,9)$ 

12 blocks 123, 456, ..., 348, ...

432 automorphisms
7 8 9 10 11 12
1 2 3 4 5 6

M_{12} is the group of all automorphisms of an $S(5,6,12)$-design with 132 blocks of size 6
This Steiner design is one due to E. Witt.

Count 
$132\binom{6}{5} = \binom{12}{5}\cdot 1$

Think of the twelve points as $P'\mathbb{F}_{11} = \{0,1,2,\dots,10,\infty\}$ Blocks: $\{0,1,3,4,5,9\}$ and its images under $PSL_2(\mathbb{F}_{11})$
(squares in $\mathbb{F}_{11}$)

To get an $S(4,5,11)$ design we derive the $S(5,6,12)$ design:
fix one point eg. ∞. $M_{11} = Aut(S(4,5,11))$
Derive again to $S(3,4,10)$ inversive plane with M_{10}
$S(2,3,9)$

$Aut(A_6) = P\Gamma L_2(9)$ 1440
$PGL_2(9)$ 720
$S_{PG_1(2)} = PGL_2(9) = S_6$
M_{10}
$A_6^{21} = PSL_2(\mathbb{F}_9)$ 360

M_{12} 95040
M_{11} 7920
M_{10} 720
M_9 72

With design $S(5,8,24)$ has 759 octads: special 8-subsets of a 24-set $P^1\mathbb{F}_{23} = \{0, 1, 2, \dots, 22, \infty\}$

Count ⬭ $759 \cdot \binom{8}{5} = \binom{24}{5}$

M_{24} is the group of all automorphisms of this design $|M_{24}| = 244,823,040$

Derived design $S(4,7,23)$ has aut gp M_{23} of order $10,200,560$

$S(3,6,22)$ — — — M_{22} — — — $443,520$

M_{24}
24 |
M_{23}
23 |
M_{22}

The Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ are sporadic simple.

We now have 26 sporadic simple groups.

The Leech lattice is a set of vectors in $\mathbb{R}^{24}$ giving optimal dense sphere packing

Co_{24} is a group of symmetries of this lattice (larger sporadic simple group).

Binary Golay code: 12-dimensional subspace of $\mathbb{F}_2^{24}$ having

(weight of $v \in \mathbb{F}_2^{24}$ = how many nonzero coords)

1	vector of weight 0
759	8
2576	12
759	16
1	24
$4096 = 2^{12}$	

→ Leech lattice $\Lambda \subset \mathbb{R}^{24}$ → Co_1, Co_2, Co_3

$S_6 \subset M_{12}$:
$A_8 \subset M_{24}$

$S(5,8,24)$

Stabilizer of an octad in M_{24}
$\cong A_8 \cong GL_4(\mathbb{F}_2)$

(56)(78) ⟆ — — —

1 2 3 4 5 6 7 8	9 10 — — — 24

octad

Brauer-Fowler Theorem (1954)

Let H be a fixed group.

Look for a finite simple group G such that there exists an involution $\tau \in G$ $(|\tau| = 2)$ such that $C_G(\tau) \cong H$.

Then there are only finitely many simple groups G that arise in this way.

The hunt for new finite simple groups was on.

eg. Suppose we want a simple gp G with $C_G(\tau) \cong GL_2(q)$

Then either $G = PSL_3(q)$ for $\tau = \begin{bmatrix} -1 & & \\ & 1 & \\ & & -1 \end{bmatrix}$

or $q = 3$ and $G \cong M_{11}$, $|G| = 7920$.

Janko, Thompson: Let $q \neq 5$ and suppose G fin. simple gp with $C_G(\tau) \cong 2 \times PSL_2(q)$.

Then either $q = 5$ or $q = 3^{2k+1} \geq 27$.

$\downarrow$ Ree groups

$|J_1| = 175560$ (1965) $\quad |J_1| = 175560 = 11 \cdot (11+1)(11^3 - 1) = 19 \cdot 20 \cdot 21 \cdot 22 = 55 \cdot 56 \cdot 57$

first new sporadic gp since Mathieu.

Rank 3 strongly regular graph

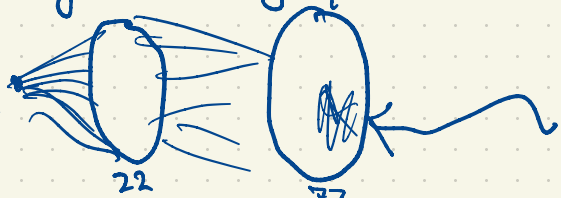
Let G be a permutation group, $G \leq S_n$.

2-trans groups are rank 2.

If G is transitive on $1, 2, \cdots, n$, then the <u>rank</u> of G is the number of orbits of G_1 on $1, 2, 3, \cdots, n$.

Rank 3 $\Rightarrow$ G acts on a strongly regular graph on n vertices.

HS Higman-Sims group $|HS| = 44{,}352{,}000 = 100\,|M_{22}|$ (1968)

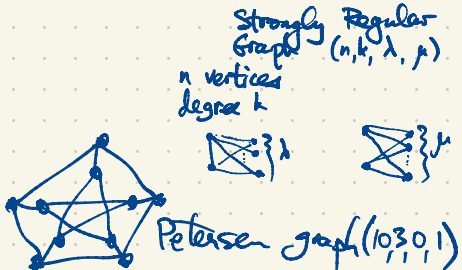


M_{22} acts on Witt design $S(3,6,22)$ 22 points, 77 blocks of size 6

SRG(77, 16, 0, 4)

HS graph SRG(100, 22, 0, 6)

Aut(HS graph) = 2 HS



R Griess 1970's
Constructed M as the automorphism group algebra of dimension 196884

$$196884 = 1 + 196883 = 300 + 98280 + 98304$$

$300 = \binom{24}{2}$; $98280 = \frac{196560}{2}$; $98304 = 24 \times 2^{12}$

John McKay $\quad j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \qquad q = e^{2\pi i \tau}$

$$H = \{\tau \in \mathbb{C} : \operatorname{Im} \tau > 0\} \qquad SL_2(\mathbb{Z}) \text{ acts on } H \text{ by fractional linear transformations.}$$

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau)$$