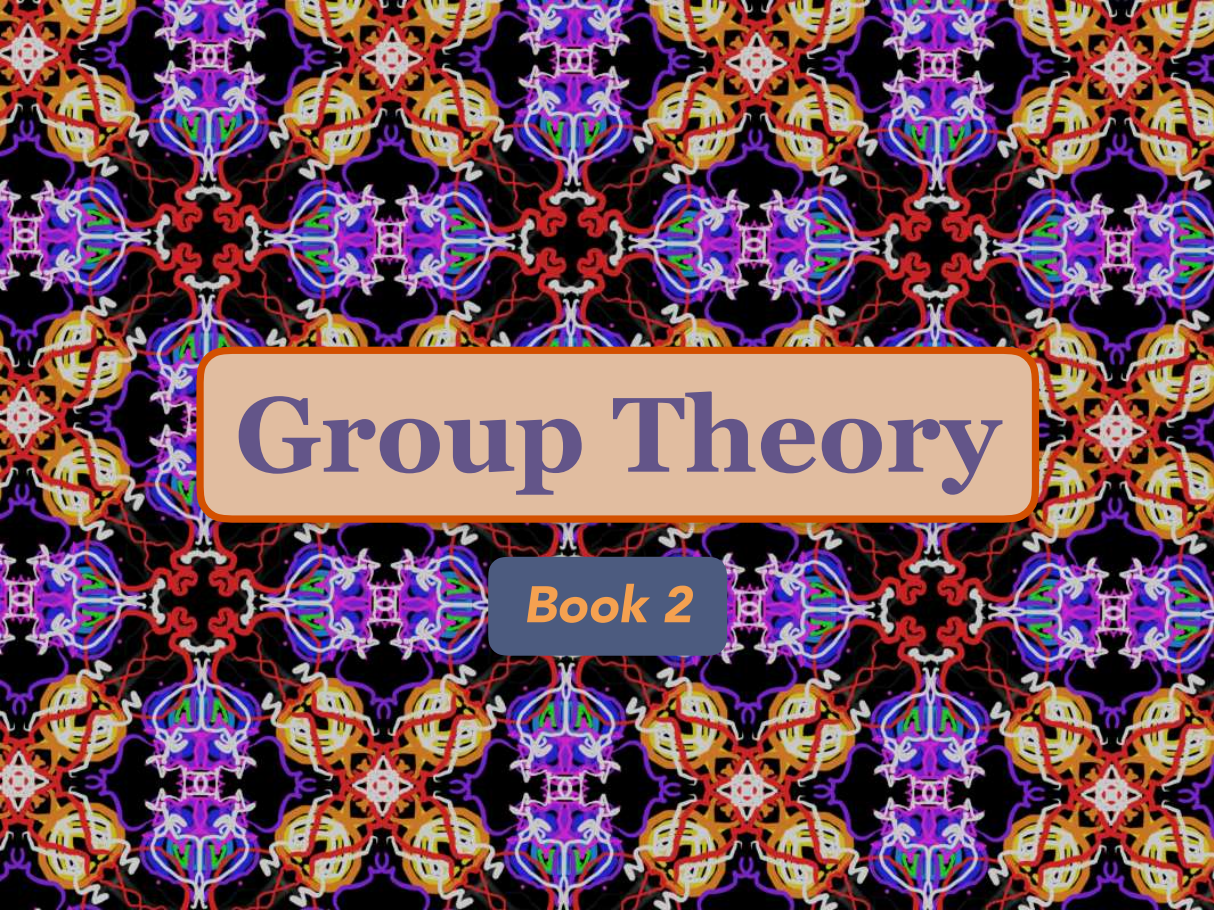


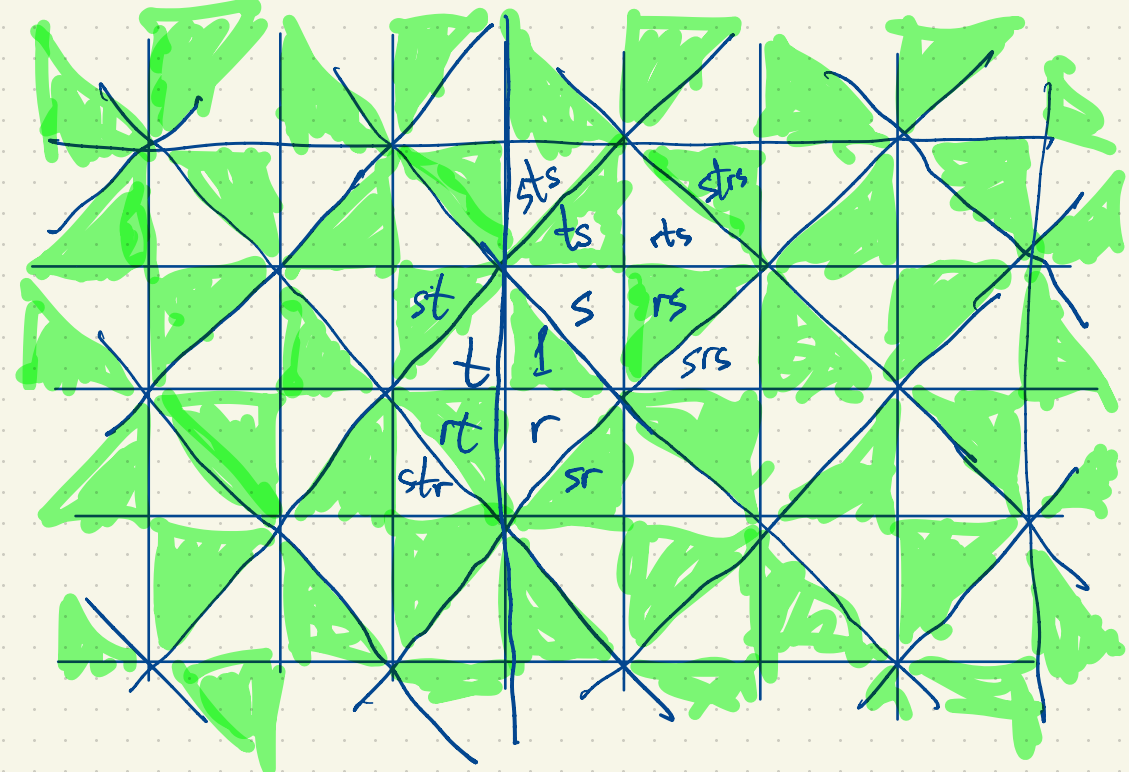
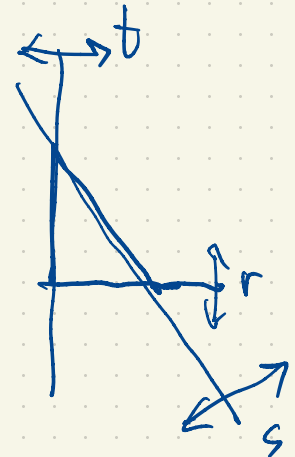


Group Theory

Book 2

reflections interchange
white $\leftrightarrow$ green
triangles

Elements of $G = G(4,4,2)$
white $\leftrightarrow$ map green $\rightarrow$



$G = G(4,4,2)$ labels the green triangles
W labels all triangles



More generally if $l, m, n \geq 2$ satisfying
 $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} = 1$ then $G = G(l, m, n)$ is a group of
isometries of the Euclidean plane generated by rotations
of order l, m, n .

$$G = \langle a, b, c \mid a^l, b^m, c^n, abc \rangle$$

Moreover $[W:G]$ where $W = \langle r, st \mid r^2, s^2, t^2, (rs)^l, (st)^m, (tr)^n \rangle$.

If $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} > 1$, $G = G(l, m, n)$ finite then in place of a tiling of the Euclidean plane, we get a tiling of S^2 (Euclidean sphere).

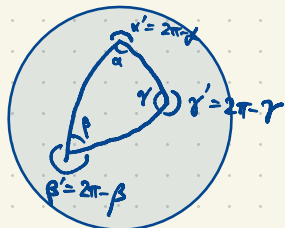
If $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$, then we get a tiling of the hyperbolic plane by congruent triangles. $C = G(l, m, n)$ infinite

A spherical example: $G = G(2, 3, 4)$, $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{6+4+3}{12} = \frac{13}{12} > 1$

Eine kleine spherical geometry

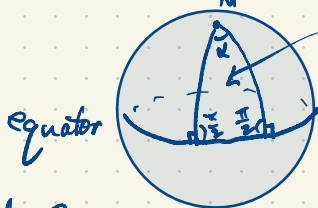
Let $S \subset \mathbb{R}^3$ be a unit sphere; its surface area is $4\pi r^2 = 4\pi$. "Lines" on S are geodesics (great circles).

Triangles in S have area = angular excess = $\alpha + \beta + \gamma - \pi > 0$



$$(\alpha + \beta + \gamma - \pi) + (\alpha' + \beta' + \gamma' - \pi) = 6\pi - 2\pi = 4\pi$$

angular excess of "inside" angular excess outside"



$$\text{Area} = \alpha + \frac{\pi}{2} + \frac{\pi}{2} - \pi = \alpha$$

$$|G| = 24.$$

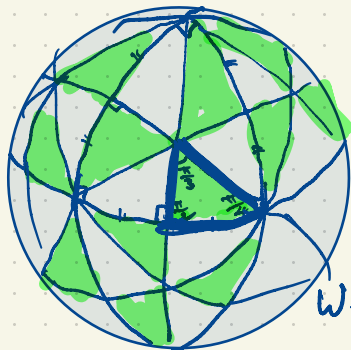
$$G \cong S_4$$

W consists of isometries of S preserving the tiling.

$$[W:G] = 2, \quad G = G(2, 3, 4)$$

$$G = \langle a, b, c \mid a^2, b^3, c^4, abc \rangle$$

rs st tr



We subdivide S

into 48 congruent spherical triangles, each with angles $\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{4}$ and area $\frac{4\pi}{48} = \frac{\pi}{12} = \frac{\pi}{2} + \frac{\pi}{3} + \frac{\pi}{4} - \pi$

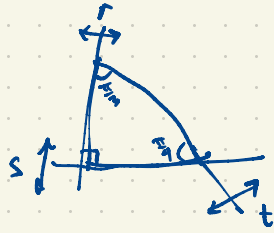
r, s, t : reflections of S in the "lines" bounding one triangle
i.e. reflections in the planes through the origin

$$W = W\left(\begin{smallmatrix} 3 & 4 \\ \longrightarrow \end{smallmatrix}\right) = \langle r, s, t \mid r^2, s^2, t^2, (rs)^2, (rt)^2, (st)^2 \rangle,$$

$$W \cong C_2 \times S_4$$

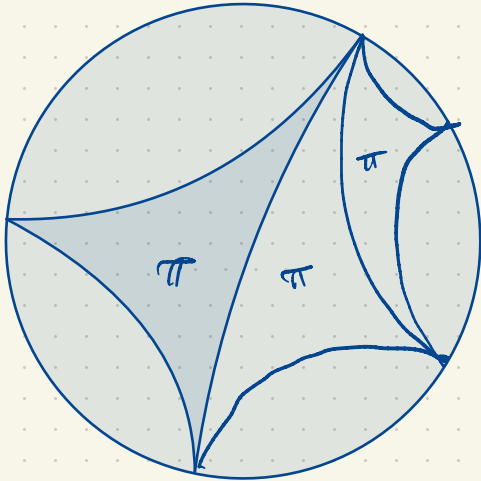
$$|W| = 48$$

Starting Fri Oct 3 new room is BU24



Case $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$: $G(l, m, n)$ preserves a triangulation of the hyperbolic plane with triangles having angles $\frac{\pi}{l}, \frac{\pi}{m}, \frac{\pi}{n}$

In hyperbolic plane, a triangle (sides are lines = geodesics) having angular defect $\pi - (\alpha + \beta + \gamma) = \text{area}$.

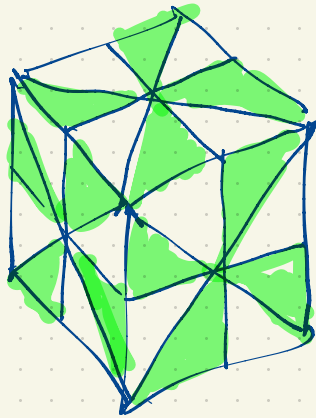
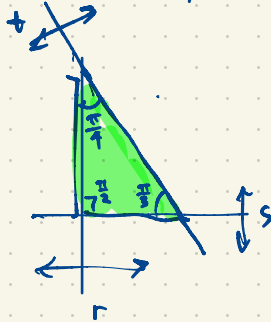


Today: $G = G(2,3,4) = \langle a, b, c : a^2, b^3, c^4, abc \rangle \cong S_4$

$$W = W(\overleftrightarrow{\quad}) \cong C_2 \times S_4$$

$$= \langle r, s, t \mid r^2, s^2, t^2, (rs)^2, (rt)^3, (st)^4 \rangle$$

To recognize $G \cong S_4$ without computer: $G = \langle rs, st, tr : rs, st, tr \text{ are rotations by angles } \frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{4} \text{ about vertices of triangle shown} \rangle$



$G =$ Group of rotational symmetries of a cube $\cong S_4$.

G permutes the four "body diagonals" of the cube in all $4! = 24$ ways. (A "body diagonal" joins two opposite vertices.)

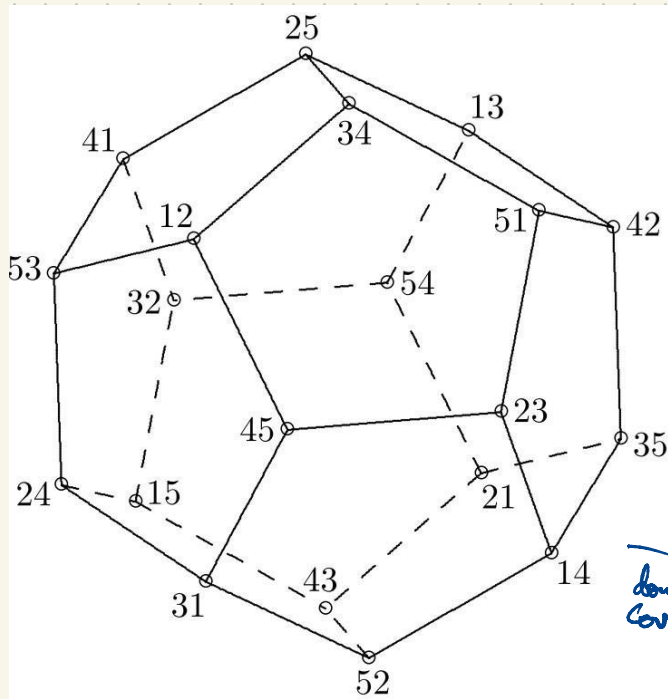
G permutes the 24 green triangles transitively (and regularly).

If $W = HK$ where H and K are normal subgroups with $H \cap K = 1$ (so H and K commute with each other i.e. $hk = kh$ for all $h \in H, k \in K$) then $W \cong H \times K = \{(h, k) : h \in H, k \in K\}$ (direct product)

In our case $|W| = 48$, $|G| = 24$, $W = G \cup Gr$, W has a subgroup $H = \langle h \rangle$ of order 2, $H \triangleleft W$, $h = -I$
 $H = Z(W)$
 preserve orientation ← reverse orientation

Cube has $3 + 6 = 9$ planes of symmetry
 but altogether 24 orientation-reversing symmetries

Similarly the regular dodecahedron (12 pentagonal faces) has rotational symmetry group G with $|G| = 60$, $G = A_5$ (Alt_5)

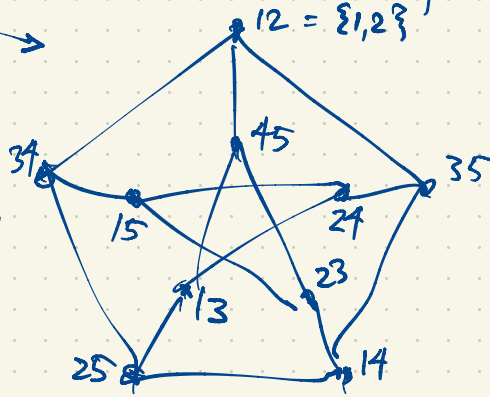


Elements of A_5 give rotational symmetries of the dodecahedron.

The full symmetry group of the regular dodecahedron has order 2×60
 (60 orientation-preserving rotations and 60 orientation-reversing reflections + other)

The full group of symmetries has order 120 and it has a subgroup isomorphic to A_5 but the group is not S_5 . S_5 is not a group of isometries of $\mathbb{R}^3$. Instead the full group of isometries of the regular dodecahedron is isomorphic to $C_2 \times A_5$.

double cover



This graph, the Petersen graph, has isomorphism group S_5

$(i, j) \mapsto \{i, j\}$
 $(j, i) \mapsto \{i, j\}$

A presentation of a group G is an expression $G = \langle X : R \rangle$ where X is a set of symbols (letters) and $R \subset F(X) = \text{free group on } X = \{x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} : x_j \in X, j \in \mathbb{Z}\}$

X = set of "generators"

R = set of "relators" (words in the generators)

$$x_j^j x_k^{j_k} = x_k^{j_k} x_j^{j_j} \quad (j, k \in \mathbb{Z}; x \in X)$$

$$x^0 = 1 = \text{identity.}$$

If X is finite then G is finitely generated.

If X and R are both finite then G is finitely presented.

Burnside groups are finitely generated (usually) but not finitely presented.

$G = F / \text{subgroup of } F \text{ generated by } R \text{ and their conjugates}$

= "largest" homomorphic image of $F = F(X)$ having R in kernel
universal as we'll discuss later - see handout.

Every group has a presentation. Given G , for every $g \in G$, introduce a generator x_g . So $X = \{x_g : g \in G\}$.

For every pair $g, h \in G$ we want to force $x_g x_h = x_{gh}$ but this doesn't happen in $F = F(X)$ so introduce relators $x_g x_h x_{gh}^{-1} \in R$. $R = \{x_g x_h x_{gh}^{-1} : g, h \in G\}$. Then $F / \langle \dots R \dots \rangle \cong G$.

If G is finitely generated then G is countable i.e. finite or countably infinite.

If $X = \{x_1, \dots, x_n\}$ then $F = F(X) = \{\text{products of } x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}\} = \bigcup_{l=0}^{\infty} S_l$ where

F is a countable union of finite sets, hence countable.

$$S_l = \{x_{i_1}^{e_1} x_{i_2}^{e_2} \dots x_{i_l}^{e_l} : i_1, \dots, i_l \in \{1, \dots, n\}, e_j \in \{\pm 1\}\}$$

$$|S_l| \leq 2^l$$

If G is countably generated (X countable) then $F = F(X)$ is countable.

$S_1 = \{\text{words of length } 1\}$ is countable.

If $|X| = m$ and $|R| = n$, m, n pos. integers, what can we say about $|G|$ where $G = \langle X | R \rangle$?
 If $n < m$ then G is infinite. That is (contrapositive form) in order for $|G| < \infty$, we need at least as many relators as generators.

eg. $m=1$. $X = \{x\}$. If $R = \emptyset$ then $G = \langle x | \emptyset \rangle = \{\dots, x^2, x^{-1}, 1, x, x^2, \dots\}$

If $R = \{1\}$ then $G = \langle x | 1 \rangle = F(x) = \{\dots, x^2, x^{-1}, 1, x, x^2, \dots\}$

If $R = \{x^{15}\}$ then $G = \langle x | x^{15} \rangle = \{1, x, x^2, \dots, x^{14}\} \cong C_{15}$

If $R = \{x^{15}, x^{40}\}$ then $G = \langle x | x^{15}, x^{40} \rangle = \langle x | x^5 \rangle = \{1, x, x^2, x^3, x^4\}$

$$x^5 = (x^{15})^3 (x^{40})^{-1}$$

If G is a group then a homomorphic image of G is the image of G under a homomorphism

$$G \xrightarrow{\phi} H \quad (\text{surjective, otherwise replace } H \text{ by } \phi(G) \leq H.)$$

Note: $H \cong G/K$ where $K = \ker \phi \trianglelefteq G$. A homomorphic image of G is the same thing as a quotient group G/K , $K \trianglelefteq G$.

In particular the abelianization of G is the largest homo. image of G which is abelian.

A normal subgroup $K \trianglelefteq G$ yields an abelian quotient group G/K iff $K \supseteq G' =$ derived subgroup of G

$$\text{i.e. } G' = \langle [g, h] : g, h \in G \rangle, \quad [g, h] = g^{-1}h^{-1}gh.$$

If $K \supseteq G'$ then in G/K , take any two elements $gK, hK \in G/K$, we have

$$hg[g, h] = hg g^{-1}h^{-1}gh = gh$$

eg. the abelianization of an abelian gp. is itself.

$$(hk)(gK) = ghK = (gK)(hK) \quad \text{and conversely.}$$

eg. the abelianization of S_n , $n \geq 2$ is C_2 (group of order 2).

The abelianization of $GL_n(F)$ ($n \geq 1$) is $F^* = \{\text{nonzero elements of } F\}$
 $GL_n(F) \xrightarrow{\det} F^* \quad \ker(\det) = SL_n(F)$

If $F = F(X)$ free group on n generators $X = \{x_1, \dots, x_n\}$ eg. $n=3$

The abelianization of F

$$F/F' \cong \mathbb{Z}^n \quad \text{where } F' = \{w \in F : \text{every } x_i \text{ has exponents adding to } 0\}$$

(free abelian group on n generators)

Multiplicatively, $x_1^{-2} x_2^2 x_3^2$
 $i=1, 2, \dots, n.$

$$w = x_1 x_2^2 x_1^{-4} x_3^2 x_1 x_2^{-1} \mapsto (-2, 2, 2) \in \mathbb{Z}^3$$

$$\mathbb{Z}^3 / \langle (1, 2, 3), (4, 9, -1) \rangle$$

Now consider $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_n \rangle$, $r_1, \dots, r_n \in F = F(x_1, \dots, x_n)$

$= F/K$, K is the normal subgp of F generated by $r_1, \dots, r_n$ and their conjugates in F .

We want to show that if $n < m$ then $|G| = \infty$.

To prove this, first consider $F/F'K$. Here $F', K \trianglelefteq F$.

$$F'K = \{ab : a \in F', b \in K\} \trianglelefteq F.$$

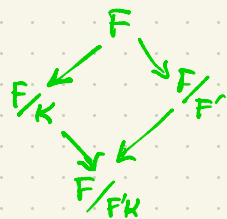
$$F/F'K \cong \frac{F/F'}{F'K/F'} \quad (\text{Third Isomorphism Theorem, also sometimes called the Second Isomorphism Theorem}).$$

$F/F'K$ is a homomorphic image of $F/F' \cong \mathbb{Z}^m$.

$$F/F'K \cong \mathbb{Z}^m / \text{subgp. generated by } n \text{ elements.}$$

$$F'K/F' \cong K/K \cap F' \quad (\text{Second Iso. Thm.})$$

$$F/F'K \cong \frac{F/K}{F'K/K}$$



$$\mathbb{Z}^3 / \langle (1,0,0), (0,3,0) \rangle \cong (\mathbb{Z}_{12}) \oplus \mathbb{Z}$$

$$\mathbb{Z}^3 / \langle (1,0,0), (0,2,0), (0,0,3) \rangle \cong (\mathbb{Z}_{12}) \oplus (\mathbb{Z}_{32})$$

Coxeter-Todd coset enumeration is the best algorithm we have for deciding certain "word problems" in group theory but it doesn't work in all cases.

Group orders: Given a presentation $G = \langle X | R \rangle$ (X, R finite)

What is $|G|$? Is it finite?

Is G trivial?

Given two words in $F_x = F(x)$ do they yield the same element of G ?

The word problem for groups is undecidable.

Matrix mortality problem

You are given a positive integer n and a list of $n \times n$ integer matrices $A_1, \dots, A_k$.

Is there a finite product of these A_i that equals the zero matrix? This is a decision problem.

For $n=1$, this problem is decidable.

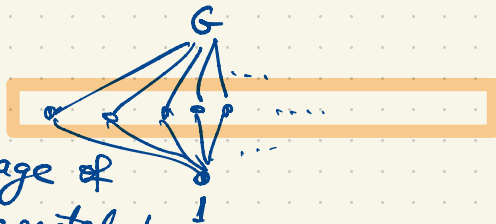
For $n \geq 3$, this problem is undecidable.

For $n=2$, we don't know whether the problem is decidable.

Suppose G is a Tarski monster for prime p i.e.

- G is an ^{infinite} nonabelian group
- $g^p = 1$ for all $g \in G$
- Given $x, y \in G$ with $x, y \neq 1$, either $\langle x, y \rangle$ is a subgroup of order p or $\langle x, y \rangle = G$.
- The only subgroups of G are

Then $|B(2, p)| = \infty$.



cyclic subgroups of order p .

This is because G is a homomorphic image of $B(2, p)$. $B(2, p)$ is the "largest" group generated by two elements a, b satisfying $g^p = 1$ for all g . (universal)

$$B(2, p) \twoheadrightarrow G \quad (\text{epimorphism})$$

$$B(2, p)/K \cong G \quad \text{for some normal subgroup } K \trianglelefteq B(2, p).$$

Since $|G| = \infty$, we must also have $|B(2, p)| = \infty$.

$B(2, p)$ has many subgroups not only cyclic of order p .

$B(2, p)$ is not simple. But G is simple: it has no normal subgroup other than 1 or G .

Proof: If G has a nontrivial normal subgroup N then it must be one of the cyclic subgroups of order p . There can't be more than one normal subgroup of order p . Why?

If N, N' are distinct normal subgroups (of order p) then $N \cap N' = 1$ and NN' is normal

$$NN' \cong N \times N' \quad \text{For all } x \in N, y \in N', \quad \overline{x'y'x}y = \underbrace{(\overline{x'y'x})}_N \underbrace{y}_{N'} \in N' \quad \text{and} \quad \overline{x'y'x}y = \underbrace{\overline{x'}}_N (\underbrace{y'xy}_N) \in N$$

So $x^{-1}y^{-1}xy = 1 \Rightarrow yx = xy \Rightarrow NN' = N \times N'$ of order p^2 . This cannot happen in a Tarski monster.

$$\text{Let } N = \{1, x, \dots, x^{p-1}\} \triangleleft G$$

$$N' = \{1, y, y^2, \dots, y^{p-1}\} < G$$

$y^{-1}xy \in N \Rightarrow y^{-1}xy = x^k$ for some $k \in \{1, 2, \dots, p-1\}$. Let $l \in \{1, 2, \dots, p-1\}$ be the inverse of k and p i.e. $kl \equiv 1 \pmod{p}$. Then

$$\text{Claim: } (y^l)^{-1}x y^l = x \quad (y^2)^{-1}x y^2 = y(y^{-1}xy)y = y^{-1}x^k y = \underbrace{(y^{-1}xy)(y^{-1}xy) \cdots (y^{-1}xy)}_{k \text{ times}}$$

If we replace $y \in N'$ by another generator of N'

then $y^{-1}xy = x$ i.e. $xy = yx$.

Then N and N' commute $\Rightarrow NN' \cong N \times N' \cong C_p \times C_p$, contradiction.

So G is simple.

Where do groups arise naturally? What are the natural examples of group operation?

- $+, \times$ in numbers
- functions under composition: permutation groups (subgroups of symmetric group), matrix groups (subgroups of $GL(V)$)
- fundamental groups in topology.
- group presentations $\langle X | R \rangle$

If F is a free group then every subgroup is free.

Nielsen-Schreier Theorem: Let F_n be a free group on n generators i.e. $F_n = \langle x_1, \dots, x_n \rangle$.

If $H \leq F_n$ with $e \neq [F_n : H]$ then $H \cong F_{1+(n-1)e}$.

Let X be a path-connected topological space X : given any points $x, y \in X$ there exists a path in X from x to y i.e. a continuous map $[0, 1] \rightarrow X$

$$\begin{array}{ccc} 0 & \mapsto & x \\ 1 & \mapsto & y \end{array}$$

eg. $X = \mathbb{R}^2 - \underline{D}$ is path-connected

$$D = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$$

$$\mathbb{R}^2 - (x\text{-axis}) = \{(x, y) \in \mathbb{R}^2 : y \neq 0\}$$

is not path-connected



In this example, γ and γ' are not homotopic.

γ' is homotopic to the constant path $\gamma_0: [0, 1] \rightarrow X$ for $\gamma_0(t) = x_0$ for all $t \in [0, 1]$

Given a path-connected space X , and a point $x_0 \in X$, we can consider closed paths in X from x_0 to x_0 which are continuous maps $\gamma: [0, 1] \rightarrow X$ st. $\gamma(0) = \gamma(1) = x_0$.

Two closed paths γ, γ' from x_0 to x_0 in X are homotopic if we can continuously distort γ to γ' while fixing the endpoints at x_0 and always staying inside X .

Write $[\gamma]$ as the equivalence class of γ under the equivalence relation of homotopy (with fixed base point x_0).

$\pi_1(X, x_0) = \{ [\gamma] : \gamma \text{ paths in } X \text{ from } x_0 \text{ to } x_0 \}$ is the fundamental group of X with base point x_0 .

The group operation is "concatenation" of paths.

In $X = \mathbb{R}^2 - D$

