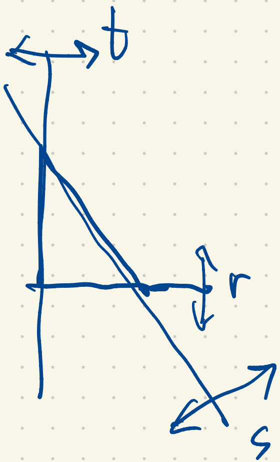
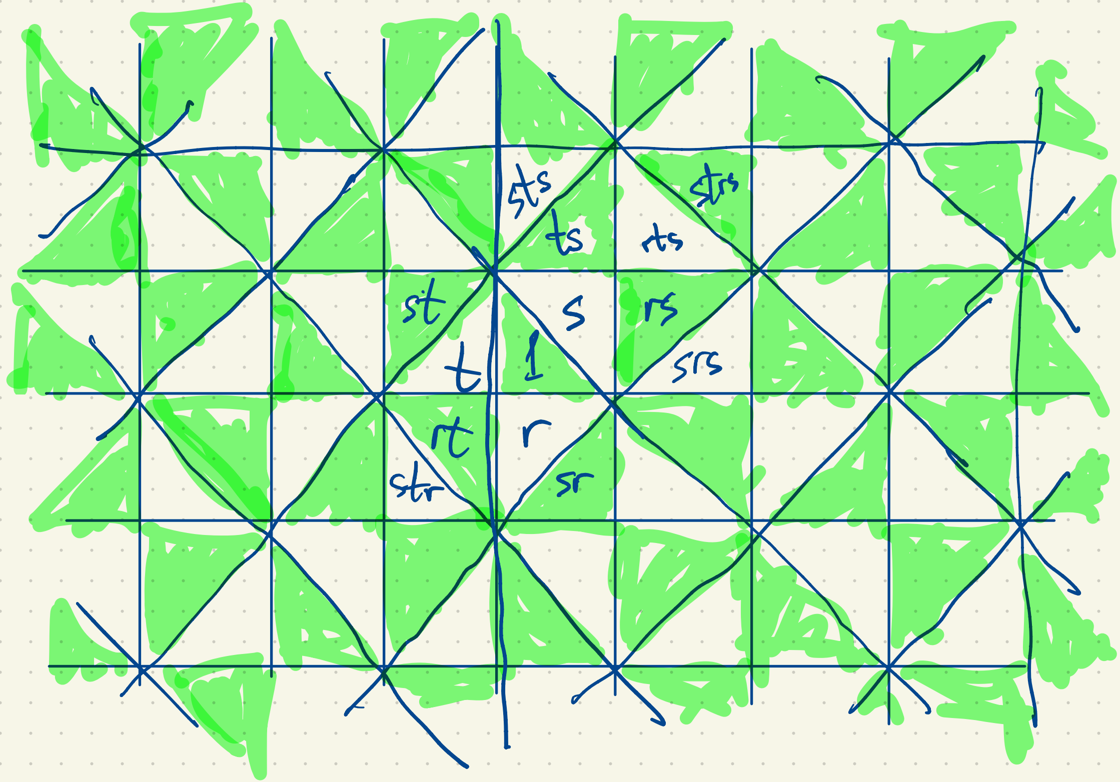
Group Theory

Book 2

reflections interchange white triangles $\longleftrightarrow$ green triangles

Elements of $G = G(4,4,2)$ map white? green?





$G = G(4,4,2)$ 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 $W = \langle r, s, t \mid r^2, s^2, t^2, (rs)^l, (st)^m, (tr)^n \rangle$.

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).

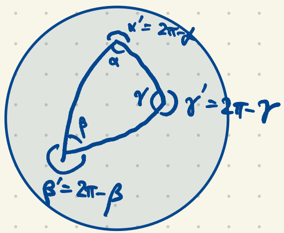
If $\frac{1}{l}+\frac{1}{m}+\frac{1}{n}<1$, $G=G(l,m,n)$ infinite, then we get a tiling of the hyperbolic plane by congruent triangles.

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

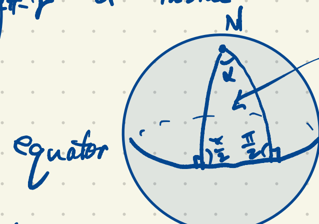
Eine Kleine spherical geometry

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 = $\alpha+\beta+\gamma-\pi>0$



$$\underbrace{(\alpha+\beta+\gamma-\pi)}_{\text{angular excess of "inside"}}+\underbrace{(\alpha'+\beta'+\gamma'-\pi)}_{\text{angular excess "outside"}}=6\pi-2\pi=4\pi$$



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;

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

$G=\langle \underset{rs}{a},\underset{st}{b},\underset{tr}{c}\mid a^2,b^3,c^4,abc\rangle$

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

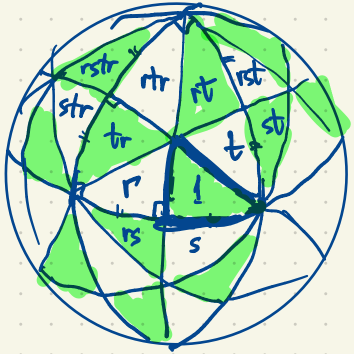
r,s,t: reflections of S in the "lines" bounding one triangle i.e. reflections in the corresponding planes through the origin

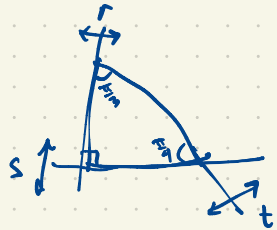
$W=W(\bullet\overset{3}{-\!-}\bullet\overset{4}{=\!=}\bullet)=\langle r,s,t\mid r^2,s^2,t^2,(rs)^2,(rt)^3,(st)^4\rangle$,

$W\cong C_2\times S_4$

$|W|=48$

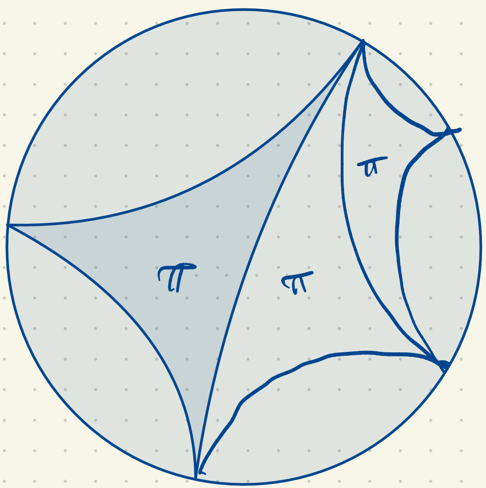
Starting Fri Oct 3 new room is BU24





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

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

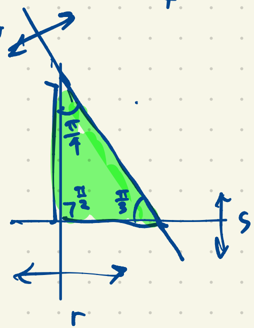


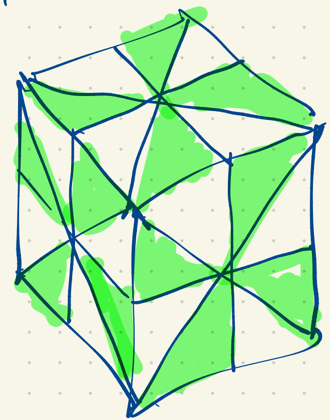
Today: $G = G(2,3,4) = \langle a,b,c : a^2, b^3, c^4, abc\rangle \cong S_4$

$W = W(B_2) \cong C_2 \times S_4$

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

To recognize $G \cong S_4$ without computer: $G = \langle rs, st, tr$: rs, st, tr are rotations by angles $\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{4}$ 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 $|W| = 48$, $|G| = 24$, $W = \underset{\text{preserve orientation}}{G} \cup \underset{\text{reverse orientation}}{Gr}$, W has a subgroup $H = \langle h \rangle$ of order 2, $H \lhd W$, $h = -I$

$H = Z(W)$

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

__Theorem__ (Ol'shanskii, 1979) For every prime $p > 10^{75}$, there exists a __Tarski Monster__ G of exponent p:

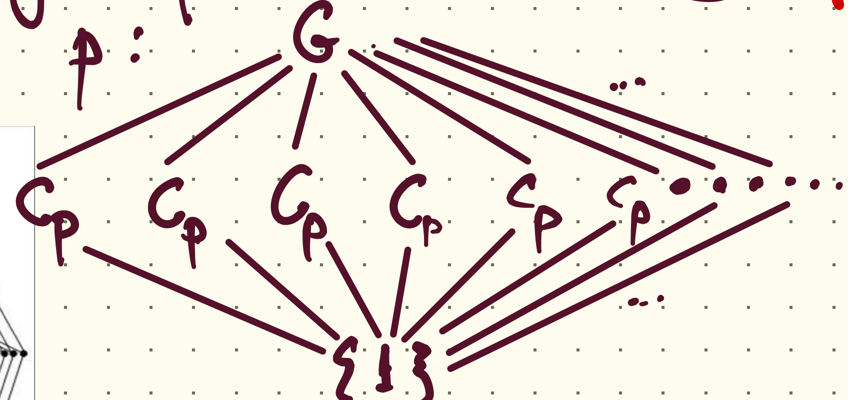
- $|G| = \infty$
- Every nonidentity element $x \in G$ has order p.
- For all $x, y \in G$ (not in the same subgroup of order p), $\langle x, y \rangle = G$ (so G has rank 2).

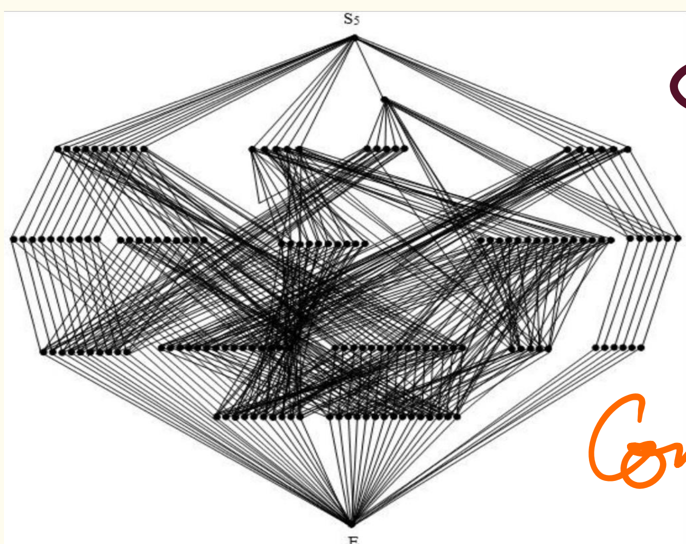
Don't confuse with the Fisher-Gries Monster $|M| \approx 10^{53}$

G shows that $|B(2,p)| = \infty$.

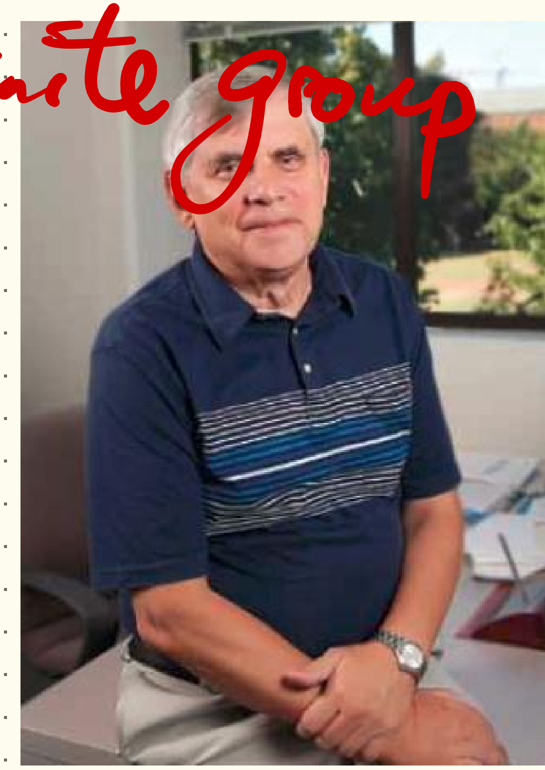
Note: A Tarski monster is an infinite group

__Every__ proper subgroup of G is cyclic of order 1 or p:





Compare: S_5



Alexander Olshanskii (1946-)

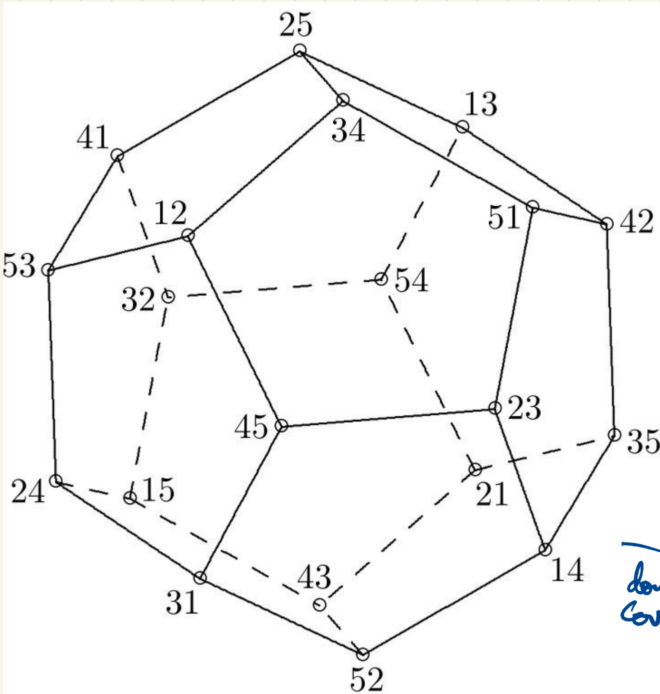
Similarly the regular dodecahedron (12 pentagonal faces) has rotational symmetry group G with $|G| = 60$, $G = A_5$ (Alt_5)

Elements of A_5 give rotational symmetries of the dodecahedron.

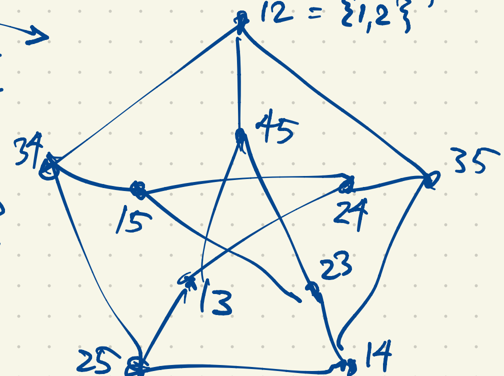
The full symmetry group of the regular dodecahedron has order 2×60 (60 $\underbrace{\text{orientation-preserving}}_{\text{rotations}}$ and 60 $\underbrace{\text{orientation-reversing}}_{\text{reflections + other}}$)

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 $R \subset F(X)$ = free group on $X = \{x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k} : x_j \in X,\ i_j \in \mathbb{Z}\}$ $\quad x^j x^k = x^{j+k}$ $(j,k \in \mathbb{Z};\ x \in X)$

$x^0 = 1$ = identity.

X = set of "generators"

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

If X is finite then G is <u>finitely generated</u>.

If X and R are both finite then G is <u>finitely presented</u>.

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

$G = F /$ subgroup of F generated by R and their conjugates

= "<u>largest</u>" 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 $x_g x_h x_{gh}^{-1} \in R$. $\quad R = \{x_g x_h x_{gh}^{-1} : g, h \in G\}$. Then $F/\{\ldots R \ldots\} \cong G$.

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

If $X = \{x_1, \ldots, x_n\}$ then $F = F(X) = \{$<u>products</u> of $x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}\} = \bigcup_{l=0}^{\infty} S_l$ where

finite products

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

$|S_l| \le 2^l$

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

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

$S_l = \{$words of length $l\}$ is countable.

If $|X| = m$ and $|R| = n$, m, n pos. integers, what can we say about $|G|$ where $G = \langle X \mid R \rangle$?
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 $G = \langle x \mid \emptyset \rangle = \{\ldots, x^{-2}, x^{-1}, 1, x, x^2, \ldots\}$

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

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

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

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

If G is a group then a <u>homomorphic image</u> of G is the image of G under a homomorphism $G \xrightarrow{\phi} H$ (surjective, ~~otherwise~~ replace H by $\phi(G) \le H$.)

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 <u>abelianization</u> 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

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

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

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

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

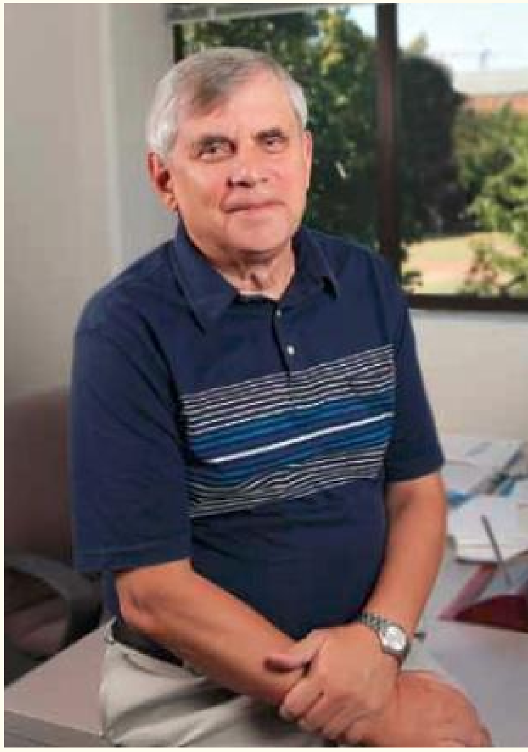
eg. the abelianization of an abelian gp. is itself.

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

Theorem (Ol'shanskii, 1979) For every prime $p > 10^{75}$, there exists a Tarski Monster G of exponent p:

- $|G| = \infty$
- Every nonidentity element $x \in G$ has order p.

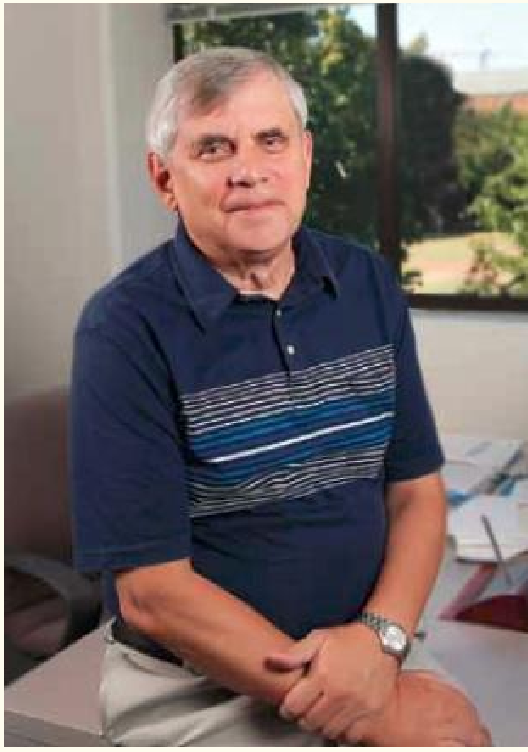
Alexander Olshanskii (1946-)



<u>Theorem</u> (Ol'shanskii, 1979) For every prime $p > 10^{75}$, there exists a <u>Tarski Monster</u> G of exponent p:

- $|G| = \infty$
- Every nonidentity element $x \in G$ has order p.
- For all $x, y \in G$ (not in the same subgroup of order p), $\langle x, y \rangle = G$ (so G has rank 2).

Alexander Olshanskii (1946-)



The abelianization of $GL_n(F)$ $(n \geq 1)$ is $F^\times = \{$ nonzero elements of $F \}$

$$GL_n(F) \xrightarrow{\det} F^\times \qquad \ker(\det) = SL_n(F)$$

If $F = F(X)$ free group on m generators $X = \{x_1, \dots, x_m\}$ e.g. $m=3$

The abelianization of F $\qquad w = x_1 x_2^3 x_1^{-4} x_3^2 x_1 x_2^{-1} \longmapsto (-2, 2, 2) \in \mathbb{Z}^3$

$F/F' \cong \mathbb{Z}^m$ where $F' = \{w \in F :$ every x_i has exponents in w adding to $0\}$, $i = 1, 2, \dots, m$. (Multiplicatively, $x_1^{-2} x_2^2 x_3^2$.

(free abelian group on m generators)

$\mathbb{Z}^3 / \langle (1,2,3), (4,0,-1) \rangle$

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

$= F/K$, 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 $F', K \trianglelefteq F$.

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

$$\begin{tikzcd} & F \arrow[dl] \arrow[dr] & \\ F/K \arrow[dr] & & F/F' \arrow[dl] \\ & F/F'K & \end{tikzcd}$$

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

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

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

$F'K/F' \cong K / K \cap F'$ (Second Iso. Thm.)

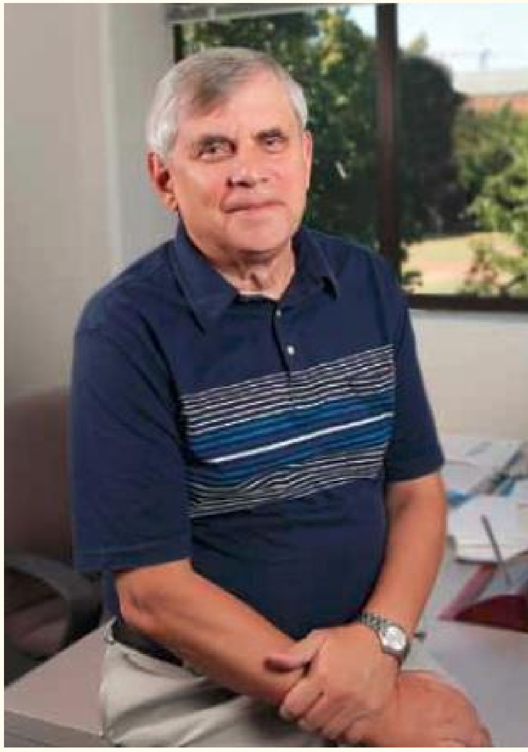
$$F/F'K \cong \frac{F/K}{F'K/K}$$

<u>Theorem</u> (Ol'shanskii, 1979) For every prime $p > 10^{75}$, there exists a <u>Tarski Monster</u> G of exponent p:

- $|G| = \infty$
- Every nonidentity element $x \in G$ has order p.
- For all $x, y \in G$ (not in the same subgroup of order p), $\langle x, y \rangle = G$ (so G has rank 2).

G shows that $|B(2,p)| = \infty$.

Alexander Olshanskii (1946-)

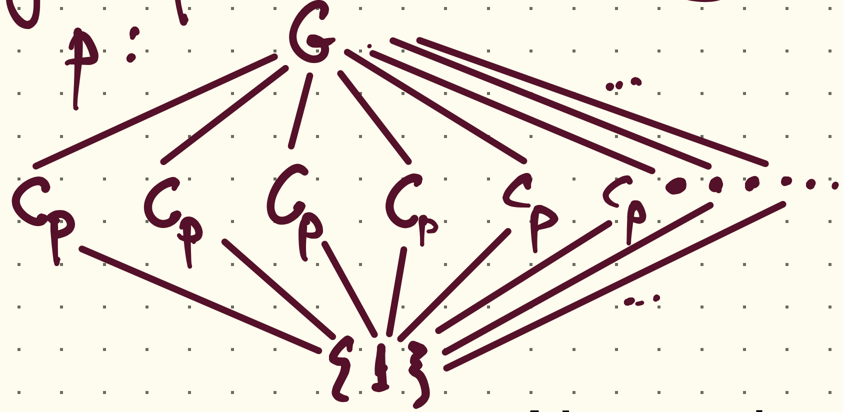


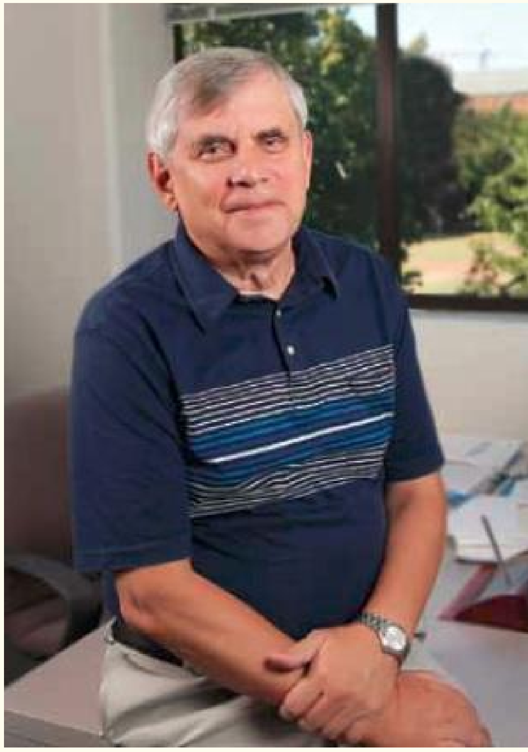
Theorem (Ol'shanskii, 1979) For every prime $p > 10^{75}$, there exists a Tarski Monster G of exponent p:

- $|G| = \infty$
- Every nonidentity element $x \in G$ has order p.
- For all $x, y \in G$ (not in the same subgroup of order p), $\langle x, y \rangle = G$ (so G has rank 2).

G shows that $|B(2,p)| = \infty$.

Every proper subgroup of G is cyclic of order 1 or p:





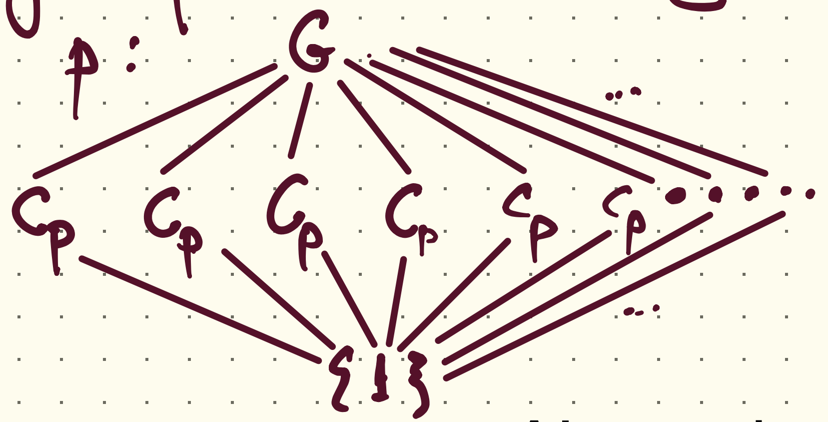
Alexander Olshanskii
(1946-)

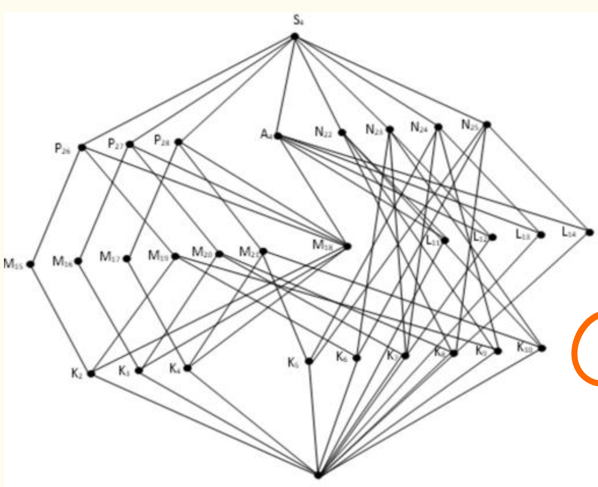
__Theorem__ (Ol'shanskii, 1979) For every prime $p > 10^{75}$, there exists a __Tarski Monster__ G of exponent p:

- $|G| = \infty$
- Every nonidentity element $x \in G$ has order p.
- For all $x, y \in G$ (not in the same subgroup of order p), $\langle x, y \rangle = G$ (so G has rank 2).

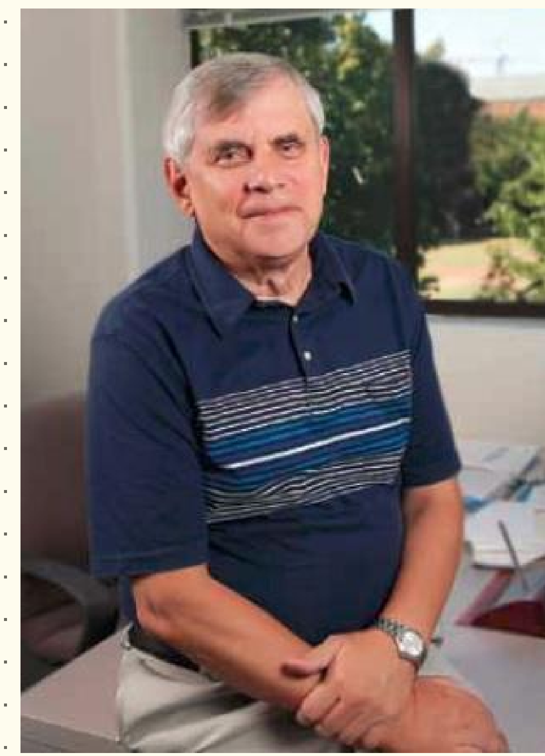
G shows that $|B(2,p)| = \infty$.

__Every__ proper subgroup of G is cyclic of order 1 or p:





Compare: S_4



Alexander Olshanskii (1946-)

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

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

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 order: Given a presentation $G = \langle X \mid R \rangle$ (X, R finite)
what is $|G|$? Is it finite?
Is G trivial?
Given two words in F, $= F(X)$ 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.

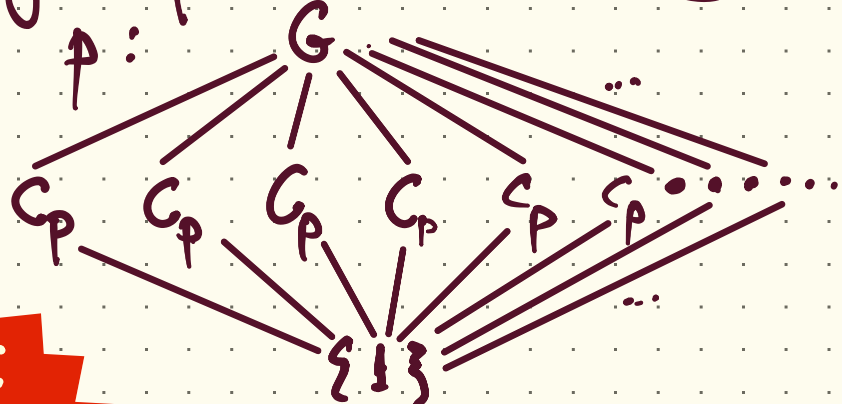
For $n=1$, this problem is decidable.
For $n \geq 3$, this problem is undecidable.
For $n=2$, we don't know whether the problem is decidable.

<u>Theorem</u> (Ol'shanskii, 1979) For every prime $p > 10^{75}$, there exists a <u>Tarski Monster</u> G of exponent p:

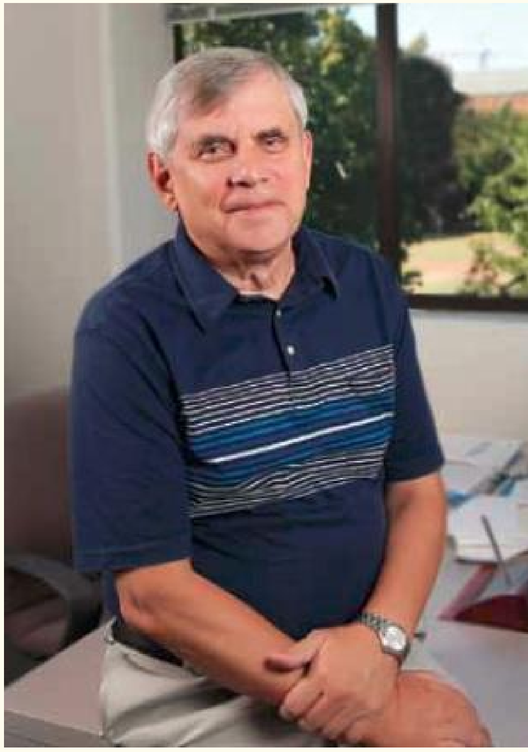
- $|G| = \infty$
- Every nonidentity element $x \in G$ has order p.
- For all $x, y \in G$ (not in the same subgroup of order p), $\langle x, y \rangle = G$ (so G has rank 2).

G shows that $|B(2,p)| = \infty$.

<u>Every</u> proper subgroup of G is cyclic of order 1 or p:



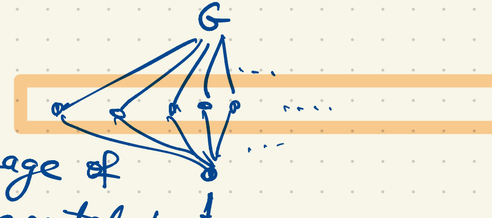
Open Question: Does there exist a Tarski monster of exponent $p=5$?



Alexander Olshanskii (1946-)

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



cyclic subgroups of order p.

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

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

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

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

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

$NN' \cong N \times N'$ For all $x \in N$, $y \in N'$, $x^{-1}y^{-1}xy = \underbrace{(x^{-1}y^{-1}x)}_{N'}\underbrace{y}_{N'} \in N'$ and $x^{-1}y^{-1}xy = \underbrace{x^{-1}}_{N}\underbrace{(y^{-1}xy)}_{N} \in N$

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.

Let $N = \{1, x, \cdots, x^{p-1}\} \lhd G$

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

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

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

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.