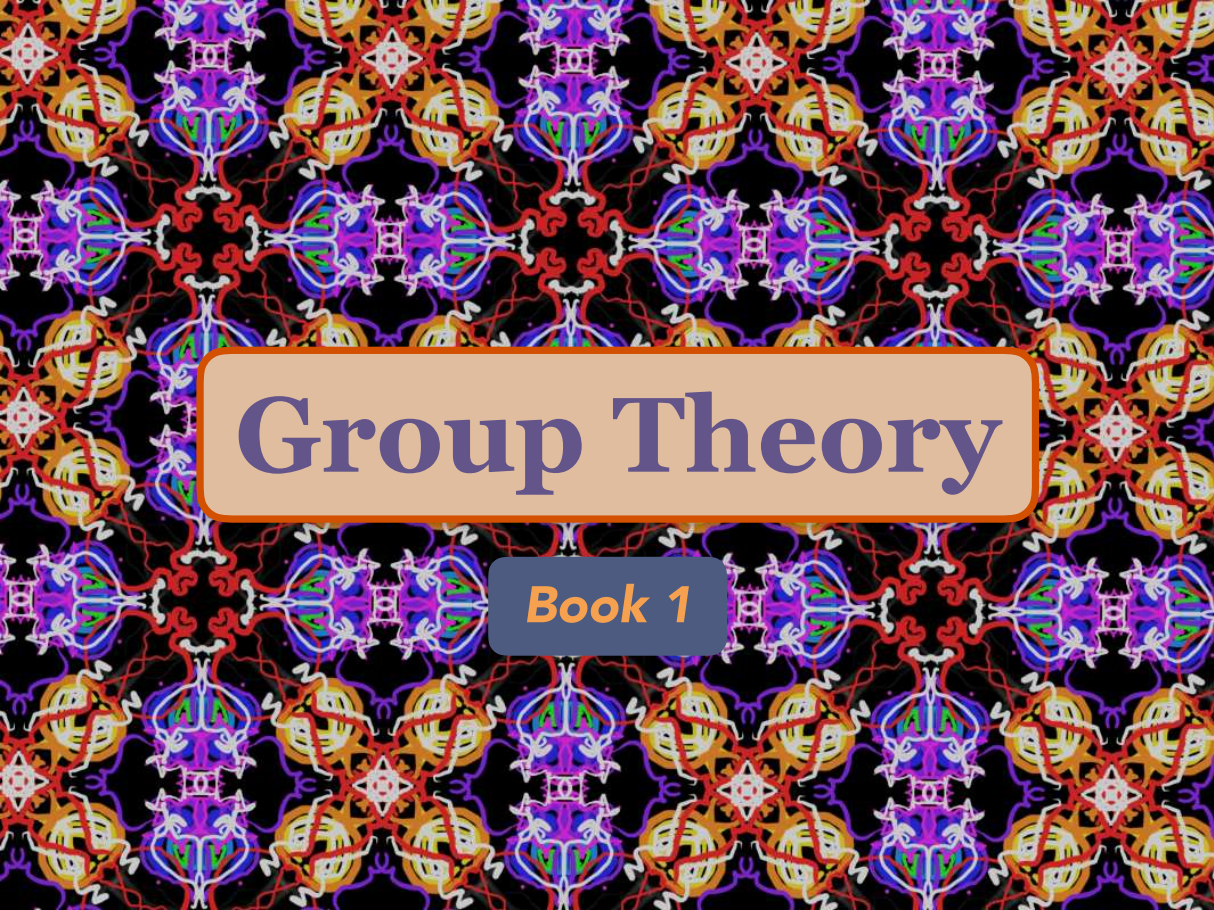

Group Theory
Book 1

Finite groups (up to isomorphism)

n	1	2	3	4	5	6	7	8	9	10	11	...	59	60	61	62	63	64	65 ...
no. of groups of order n	1	1	1	2	1	2	1	5	2	2	1		1	13	1	2	1	267	1

$C_2 \times C_2 \times C_3 \times C_5$, $C_4 \times C_3 \times C_5 \cong C_{60}$

$n=4$: Klein $C_2 \times C_2$, C_4

$n=6$: $C_3 \times C_2 \cong C_6 \cong S_3 \cong D_3$

$n=8$: elementary abelian $C_2 \times C_2 \times C_2$, $C_2 \times C_4$, C_8, Q Quaternion, D_4 Dihedral

$n=9$: $C_3 \times C_3$, C_9 elementary abelian

S_n = symmetric group of degree n, $|S_n| = n!$

A_n = alternating group of degree n, order, $|A_n| = \frac{1}{2}n!$ $(n \geq 2)$

A_n is simple for $n \geq 5$

$|S_4| = 24$ solvable

$1 \overset{2}{\triangleleft} G_2 \overset{2}{\triangleleft} G_3 \overset{3}{\triangleleft} G_4 = A_4 \overset{2}{\triangleleft} G = S_4$

$G_2 = \langle (12)(34) \rangle$ order 2

$G_3 = \langle (12)(34), (13)(24) \rangle$ order 4

Composition series with composition factors of prime order: $|G_1/G_0| = 2$, $|G_2/G_1| = 2$,

$|G_3/G_2| = 3$, $|G/G_3| = 2$

$|S_5| = 5! = 120$

S_5 has composition series

$1 \overset{60}{\triangleleft} A_5 \overset{2}{\triangleleft} S_5$

Simple groups — cyclic of prime order; nonabelian simple groups of order

60, 168, 360, 504, 660, 1092, 2448, 2520, 3420, 4080, ...

$A_6 \cong$ symplectic ...

$SL_3(2) \cong PSL_2(7)$

A_7

$SL_2(4) \cong PSL_2(5) \cong A_5$

G is solvable if all its composition factors are cyclic of prime order.

Jordan-Hölder Theorem: Every finite group has a composition series with its factors being simple groups.

G ($G \neq 1$) is simple if its only composition series is $1 \triangleleft G$ (the only normal subgroups are 1 and G).

eg. cyclic groups of prime order are simple.

A_n is simple for $n \geq 5$.

Classical groups of Lie type are analogous to Lie groups
We use finite fields: Every finite field has prime power order $q = p^e$, p prime, $e \geq 1$.

$\mathbb{F}_q$

including $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$; $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$\alpha^2 = 1 + \alpha = \beta$

$GL_n(F)$ = group of all invertible $n \times n$ matrices over F.

$GL_1(F)$ is the general linear group of degree n over F.

$GL_2(\mathbb{R})$ is a Lie group

$GL_2(\mathbb{F}_2) = \left\{ \begin{bmatrix}1&0\\0&1\end{bmatrix}, \underbrace{\begin{bmatrix}0&1\\1&0\end{bmatrix}, \begin{bmatrix}1&0\\1&1\end{bmatrix}, \begin{bmatrix}1&1\\1&0\end{bmatrix}}_{\text{order 2}}, \underbrace{\begin{bmatrix}1&1\\0&1\end{bmatrix}, \begin{bmatrix}0&1\\1&1\end{bmatrix}}_{\text{order 6}} \right\} \cong S_3$

$GL_2(2)$

$\begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix} = \begin{bmatrix}1&0\\0&1\end{bmatrix}$

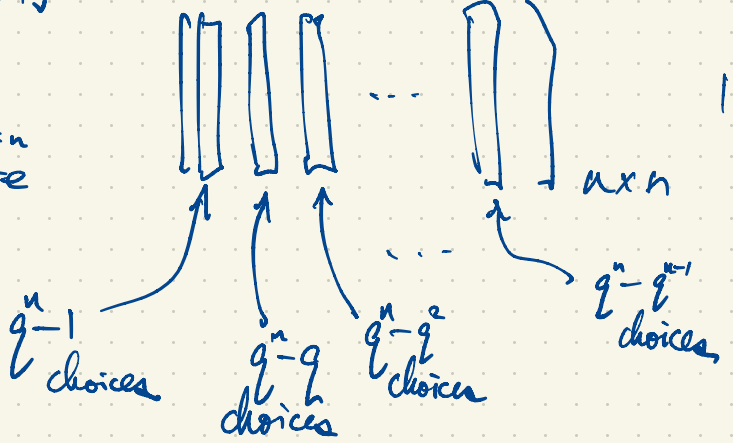
A Sylow 2-subgroup

$\begin{bmatrix}1&*&\cdots&*\\&1&&\vdots\\&&\ddots&*\\&&&1\end{bmatrix}$

of order $q^{\frac{n(n-1)}{2}}$

$|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$

There are q^{n^2} matrices of size $n \times n$ over $\mathbb{F}_q$ but most of them are not invertible.



$|GL_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\cdots(q-1)$

$= q^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} (q^j - 1)$

$|GL_2(2)| = (2^2-1)(2^2-2) = 6$

$|GL_3(2)| = (2^3-1)(2^3-2)(2^3-2^2)$

$= 7 \cdot 6 \cdot 4 = 168$

$GL_3(2)$ is the second-smallest nonabelian simple group

$|GL_4(2)| = (2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3) = 15\cdot 14\cdot 12\cdot 8 = 20160$

$|A_8| = \frac{8!}{2} = \frac{40320}{2} = 20160$

There are two simple groups of order 20160 : $A_8 \cong GL_4(2)$, $PSL_3(4)$

$|GL_3(4)| = (4^3-1)(4^3-4)(4^3-4^2) = 63\cdot 60\cdot 48 = 181440 = 9\cdot 20160$

$GL_3(4)$ is not simple.

$GL_n(F)$ has a normal subgroup $SL_n(F)$ = special linear group of degree n over F
$= \{ A \in GL_n(F) : \det A = 1 \}$.

$|SL_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{q-1}$

there is a surjective homomorphism $GL_n(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^* = \{\text{nonzero field elements}\}$

$A \longmapsto \det A$

First isomorphism theorem : $GL_n(\mathbb{F}_q) / SL_n(\mathbb{F}_q) \cong \mathbb{F}_q^*$

If $q=2$ then $SL_n(q) = GL_n(q)$.

Smaller example: $|A_5| = \frac{1}{2}5! = 60$ smallest nonabelian simple group

$SL_2(\mathbb{F}_4) = \frac{1}{3}\cdot 180 = 60$

$|GL_2(\mathbb{F}_4)| = (4^2-1)(4^2-4) = 15\times 12 = 180$

$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

There is only one simple group of order 60;

$SL_2(4) \cong A_5$

What five points is $SL_2(4)$ permuting (all 60 even permutations of the five points)?
We'll answer this soon but first use group presentations:

$A_5 \cong \langle a, b \mid a^5 = b^3 = (ab)^2 = 1\rangle$ = the group generated by a, b subject to these relations $a^5=1,\ b^3=1,\ (ab)^2=1$.

What does this mean?

In A_5, let $a = (1\,2\,3\,4\,5)$, $b = (1\,4\,2)$, so $ab = (1\,2\,3\,4\,5)(1\,4\,2) = (2\,3)(4\,5)$

"left-to-right" composition: see handout

(142): $1 \mapsto 4$, $2 \mapsto 1$, $3 \mapsto 3$, ...

~~$(142)(1) = 4$~~
~~$(142)(2) = 1$~~
~~$(142)(3) = 3$~~
...

$1^{(142)} = 4$

$3^{(142)} = 3$

...

$$\begin{bmatrix} \beta & \alpha \\ \alpha & \beta \end{bmatrix}\begin{bmatrix} \beta & \alpha \\ \alpha & \beta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$1\,(1\,2\,3\,4\,5)(1\,4\,2)$

$= 2\,(1\,4\,2) = 1$

$SL_2(4)$ is generated by $a = \begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix}$, $b = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$

$$ab = \begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix}\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}$$

$$(ab)^2 = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$1^{(12345)(142)} = [1^{(12345)}]^{(142)} = 2^{(142)} = 1$

$|SL_2(5)| = |SL_2(\mathbb{F}_5)| = \frac{1}{4}|GL_2(5)| = \frac{1}{4}\cdot 480 = 120$

$|GL_2(5)| = (5^2-1)(5^2-5) = 24\cdot 20 = 480$

$|PSL_2(5)| = |SL_2(5)/\langle -I\rangle| = \frac{120}{2} = 60.$

$-I = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}4 & 0\\ 0 & 4\end{bmatrix}$

$Z(SL_2(5)) = \langle -I\rangle = \{I, -I\}$ (center)

$Z(GL_2(5)) = \{\lambda I : \lambda \neq 0\}$

$\det(\lambda I) = \begin{vmatrix}\lambda & 0\\ 0 & \lambda\end{vmatrix} = \lambda^2$

$PSL_2(5)$ consists of all 2×2 matrices $\begin{bmatrix}x & y\\ z & w\end{bmatrix}$, $x,y,z,w \in \mathbb{F}_5$ with $xw - yz = 1$, where we identify $\pm\begin{bmatrix}x & y\\ z & w\end{bmatrix}$

$a = \pm\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, $a^2 = \pm\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$, ..., $a^5 = \pm\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = 1$

$b = \pm\begin{bmatrix}0 & 1\\ 4 & 4\end{bmatrix}$, $b^2 = \pm\begin{bmatrix}4 & 4\\ 1 & 0\end{bmatrix}$, $b^3 = \pm\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

$ab = \pm\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\ 4 & 4\end{bmatrix} = \pm\begin{bmatrix}4 & 0\\ 4 & 4\end{bmatrix} = \pm\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$, $(ab)^2 = \pm\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

$PSL_2(\mathbb{F}_5)$ can be identified with the 60 fractional linear transformations permuting $\mathbb{F}_5 \cup \{\infty\} = \{0,1,2,3,4,\infty\}$

$A_5 \cong SL_2(4) \cong PSL_2(5)$ of order 60; all are defined by the presentation $\langle a, b \mid a^5 = b^3 = (ab)^2 = 1\rangle$

Composition series for $SL_2(5)$:

$\langle I\rangle \triangleleft \langle -I\rangle \triangleleft SL_2(5)$

order 1 — order 2 — order 120

Why is $SL_2(\mathbb{F}_4) \cong A_5$? One way is to see that $SL_2(\mathbb{F}_4)$ permutes $\mathbb{F}_4 \cup \{\infty\} = \{0, 1, \alpha, \beta, \infty\}$ as fractional linear transformations

$$f_A(z) = \frac{az+b}{cz+d}, \quad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$B = \begin{bmatrix} e & g \\ h & k \end{bmatrix}$, $f_B(z) = \frac{ez+g}{hz+k}$

$$f_B(f_A(z)) = (f_B \circ f_A)(z) = \frac{e\frac{az+b}{cz+d} + g}{h\frac{az+b}{cz+d} + k} \cdot \frac{cz+d}{cz+d} = \frac{e(az+b)+g(cz+d)}{h(az+b)+k(cz+d)}$$

$$= \frac{(ae+cg)z + (be+dg)}{(ah+ck)z + (bh+dk)} = f_C(z), \quad C = \begin{bmatrix} ae+cg & be+dg \\ ah+ck & bh+dk \end{bmatrix}$$

$f_b = (0, \beta)(\alpha, \infty)$

$$BA = \begin{bmatrix} e & g \\ h & k \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ae+cg & be+dg \\ ah+ck & bh+dk \end{bmatrix}$$

$$f_B \circ f_A = f_{BA}$$

$\{a \cdot 1 + b \cdot \beta : a, b \in \mathbb{F}_2\} = \{0, 1, \beta, \beta+1 = \alpha\}$

$\mathbb{F}_4 \supset \mathbb{F}_2$ is a 2-dim'l vector space with basis $\{1, \alpha\}$.

The map $GL_2(F) \longrightarrow \{\text{fractional linear transformations}\}$

$$A \longmapsto f_A \quad \text{where } f_A(z) = \frac{az+b}{cz+d}, \quad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is a homomorphism. This homomorphism is onto but in general not one-to-one:

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \longmapsto f_I \qquad f_I(z) = \frac{1z+0}{0z+1} = z$

$\lambda I = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \qquad f_{\lambda I}(z) = \frac{\lambda z + 0}{0z+\lambda} = z$

The kernel of our homomorphism is $Z(GL_2(F)) = \{\lambda I : \lambda \in F, \ \lambda \neq 0\}$.

$$Z(SL_2(\mathbb{F}_4)) = \{\lambda I \in SL_2(\mathbb{F}_4) : \det(\lambda I) = 1\} = \{I\}$$

$\det \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} = \lambda^2 = 1 \iff \lambda = 1.$

Frac. lin. transf. over F are permutations of $F \cup \{\infty\}$

eg. $a = \begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix}$, $b = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$, $ab = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}$

$a^5 = b^3 = (ab)^2 = 1$

$f_a(z) = \frac{z+1}{\alpha z + \beta}$, $\quad f_a = (0, \alpha, \infty, \beta, 1)$

$f_b(z) = \frac{\alpha z + 0}{0z + \beta} = \beta z$, $\quad f_b = (1, \beta, \alpha)$

$f_{ab}(z) = \frac{\alpha z + \beta}{\beta z + \alpha}$, $\quad f_{ab} = (0, \alpha)(\beta, \infty) = f_a \circ f_b$

$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$|A_8| = \frac{1}{2}8! = \frac{1}{2} \times 40320 = 20160$

$|GL_4(\mathbb{F}_2)| = (2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3) = 15 \times 14 \times 12 \times 8 = 20160$

$GL_4(2) = SL_4(2) = PGL_4(2) = PSL_4(2)$

$|GL_3(4)| = (4^3-1)(4^3-4)(4^3-4^2) = 63 \cdot 60 \cdot 48 = 181,440$

$|SL_3(4)| = 60,480$

$Z(SL_3(4)) = \{cI : c \neq 0\} = \{I, \alpha I, \beta I\}$

$c\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} = \begin{bmatrix}c&0&0\\0&c&0\\0&0&c\end{bmatrix}$, $c = 1, \alpha, \beta$ in $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$

$\det(cI) = c^3 = 1$

$f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$

$\mathbb{F}_{16} = \mathbb{F}_2[\omega]$ where ω is a root of $f(x)$

$= \{a + b\omega + c\omega^2 + d\omega^3 : a, b, c, d \in \mathbb{F}_2\}$

$\omega^4 = \omega + 1$

Equivalently, take $A = \begin{bmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{bmatrix}$ (companion matrix for $f(x)$)

So $A^4 = A + I$

$\mathbb{F}_2[A] = \{aI + bA + cA^2 + dA^3 : a, b, c, d \in \mathbb{F}_2\}$

$\subset \{4 \times 4 \text{ matrices over } \mathbb{F}_2\}$.

$\{0, I, A, A^2, \dots, A^{14}\}$, $A^{15} = I$.

$A \in GL_4(2)$ has order 15.

$PSL_3(4) = SL_3(4)/Z(SL_3(4))$. This group consists of invertible 3×3 matrices over $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ of determinant 1 in which we identify scalar multiples i.e. $A, \alpha A, \beta A$ give the same group element.

$|PSL_3(4)| = \frac{60,480}{3} = 20,160.$

Easy-ish fact: A_8, $GL_4(2)$ have elements of order 15; $PSL_3(4)$ does not. $PSL_3(4) \not\cong A_8$ or $GL_4(2)$.

A little harder: $A_8 \cong GL_4(2)$.

$(1\,2\,3\,4\,5)(6\,7\,8) \in A_8$ of order 15. Equivalently, $(1\,2\,3\,4\,5) \in A_5$ of order 5; $(6\,7\,8) \in A_8$ of order 3; and they commute.

Why does $GL_4(2)$ have an element of order 15? Consider $\mathbb{F}_{16} \supset \mathbb{F}_2$, an extension of degree 4.

$\mathbb{F}_{16}^\times$ is a multiplicative cyclic group of order 15. $\mathbb{F}_{16}^\times = \{1, \omega, \omega^2, \omega^3, \dots, \omega^{14}\}$, $\omega^{15} = 1$

$\mathbb{F}_{16} = \{0, 1, \omega, \omega^2, \dots, \omega^{14}\}$

$\mathbb{F}_{16} \to \mathbb{F}_{16}$

$x \mapsto \omega x$

Claim: $PSL_3(4)$ has no element of order 15. (So it cannot be isomorphic to A_8 or $GL_4(2)$.)

Proof: Suppose $A \in PSL_3(4)$ has order 15, so A^3 has order 5 and A^5 has order 3; here A^3 and A^5 commute.
By Sylow theory, any two subgroups of order 5 are conjugate in $G = PSL_3(4)$. $\langle A^3 \rangle$ is a Sylow 5-subgroup
WLOG, $A^3 = \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 1 & 1 \\ 0 & \alpha & \beta \end{array}\right]$. Next we a general fact from linear algebra

If A, B are $n \times n$ matrices which commute ($AB = BA$) then every eigenspace for A is an invariant subspace for B
i.e. if $Av = \lambda v$ then $A(Bv) = \lambda(Bv)$. Proof: $A(Bv) = B(Av) = B(\lambda v) = \lambda(Bv)$.

$A^3 = \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 1 & 1 \\ 0 & \alpha & \beta \end{array}\right]$ has $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ as an eigenvector with eigenvalue 1, and A^5 commutes with A^3 so $\left\langle \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right\rangle$ is invariant under A^5.
($\begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix}$ doesn't have eigenvalue 1, so the 1-eigenspace of A^3 is $\left\langle \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right\rangle$.)

so $A^5 = \left[\begin{array}{c|cc} c & * & * \\ \hline 0 & * & * \\ 0 & * & * \end{array}\right]$ $c \neq 0 \Rightarrow c \in \{1, \alpha, \beta\}$, WLOG $c = 1$ so $A^5 = \left[\begin{array}{c|cc} 1 & * & * \\ \hline 0 & * & * \\ 0 & * & * \end{array}\right]$ has order 3 in G

$A^5 = \left[\begin{array}{c|cc} 1 & * & * \\ \hline 0 & & \\ 0 & & C \end{array}\right]$ where $C \in SL_2(4)$, $C^3 = I$. $|SL_2(4)| = 60 = 2^2 \cdot 3 \cdot 5$. C^3 is conjugate (in $SL_2(4)$) to $\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$
and C^3 commutes with $\begin{bmatrix} \alpha & 1 \\ 0 & \beta \end{bmatrix}$. However, $\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$ has two distinct eigenspaces $\left\langle \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\rangle$, $\left\langle \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\rangle$ and so
C^3 has two distinct eigenspaces and these are not invariant under $\begin{bmatrix} \alpha & 1 \\ 0 & \beta \end{bmatrix}$ which has no eigenvectors;
its char. poly. is irreducible over $\mathbb{F}_4$. Contradiction!

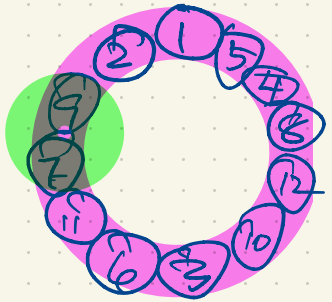
More examples of group presentations:

$bab^{-1} = a^{-1}$ (relation) $\iff$ $abab^{-1} = 1$ (relator)

The dihedral group of order $2n$ has presentation $\langle a,b : a^n = b^2 = 1,\ bab^{-1} = a^{-1} \rangle$

The cyclic group of order n is $\langle a : a^n = 1 \rangle$

The symmetric group S_n of degree $n \geq 3$ is generated by $(1,2)$, $(1,2,3,\cdots,n)$ but not in a convenient way since their relations are very complicated.



$(3,4)(7,8)$ has order 2

$(3,4)(4,5) = (3,5,4)$ has order 3

$(3,4)(3,4) = (1)$ ⋯ (

We might instead use all $\binom{n}{2}$ transpositions $(i\,j)$, $1 \leq i < j \leq n$

or simply the $n-1$ transpositions $r_i := (i, i+1)$, $1 \leq i \leq n-1$

S_n has presentation $\langle r_1, \cdots, r_{n-1} : r_1^2 = r_2^2 = \cdots = r_{n-1}^2 = 1,$
$(r_i r_{i+1})^3 = 1$ for $i = 1,2,\cdots,n-2$;
$(r_i r_j)^2 = 1$ for $1 \leq i < j \leq n-1,\ |i-j| \geq 2 \rangle$

$= \langle r_1, \cdots, r_{n-1} : (r_i r_j)^2 = 1$ if $i = j$ or $|i-j| \geq 2$;
$(r_i r_j)^3 = 1$ if $|i-j| = 1 \rangle$.

S_n is an example of a Coxeter group: $r_i r_j = 1$ if $i = j$.

ie. a group given by a presentation $\langle r_1, \cdots, r_\ell : (r_i r_j)^{m_{ij}} = 1 \rangle$,

$m_{ii} = 1$, $m_{ij} = m_{ji} \geq 1$

$A_n < S_n$, $|A_n| = \frac{1}{2} n!$, A_n is generated by $g_1 = (12)(23) = (1,3,2)$
$g_2 = (12)(34)$
$g_3 = (12)(45)$
$\vdots$
$g_{n-2} = (12)(n-1, n)$

$g_1^3 = 1$
$g_2^2 = g_3^2 = \cdots g_{n-2}^2 = 1$
$(g_i g_j)^2 = 1$ if $|i-j| \geq 2$.
$(g_i g_j)^3 = 1$ if $|i-j| = 1$.

$A_8 \cong GL_4(2)$

2.5 Satz. *Sei* $V = V(4, 2)$ *der Vektorraum der Dimension* 4 *über dem Körper* $GF(2)$ *und* $GL(4, 2)$ *die Gruppe aller linearen Abbildungen von* V *auf sich. Dann gilt* $GL(4, 2) \cong \mathfrak{A}_8$.

Beweis. Die Matrizen

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad G_2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$G_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad G_4 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$G_5 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad G_6 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

liegen in $GL(4, 2)$. Triviale, aber etwas langwierige Rechnungen zeigen, daß sie die in I, 19.8 (S. 138) angegebenen definierenden Relationen

$$G_1^3 = G_i^2 = E \quad (2 \leqq i \leqq 6), \quad (G_i G_{i+1})^3 = E \quad (1 \leqq i \leqq 5),$$
$$(G_i G_j)^2 = E \quad (i + 1 < j)$$

von $\mathfrak{A}_8$ erfüllen. Also ist $\mathfrak{G} = \langle G_1, \ldots, G_6 \rangle$ ein epimorphes Bild von $\mathfrak{A}_8$. Da $\mathfrak{A}_8$ nach 2.4 einfach ist, folgt $\mathfrak{G} \cong \mathfrak{A}_8$. Eine einfache Rechnung zeigt (siehe auch II, 6.2) $|GL(4, 2)| = |\mathfrak{A}_8|$. Wegen $\mathfrak{G} \leqq GL(4, 2)$ folgt jetzt $\mathfrak{G} = GL(4, 2) \cong \mathfrak{A}_8$. **q.e.d.**

B. Huppert, Endliche Gruppen I 1967.

With no relations in a group presentations, we have a free group.

$F_n = \langle r_1, \cdots, r_n \rangle$ = free group on n generators = { all (finite) products of $r_1, \cdots, r_n, r_1^{-1}, r_2^{-1}, \cdots, r_n^{-1}$ }.

↑ no relations

$r_i^k r_i^l = r_i^{k+l}$, $r_i^0 = 1$.

$F_1 = \langle r \rangle = \{ \cdots, r^{-3}, r^{-2}, r^{-1}, 1, r, r^2, r^3, \cdots \}$ = infinite cyclic group $\cong \mathbb{Z}$

Informally, $F_1 = \mathbb{Z}$.

$\mathbb{Z} \xrightarrow{\cong} F_1$

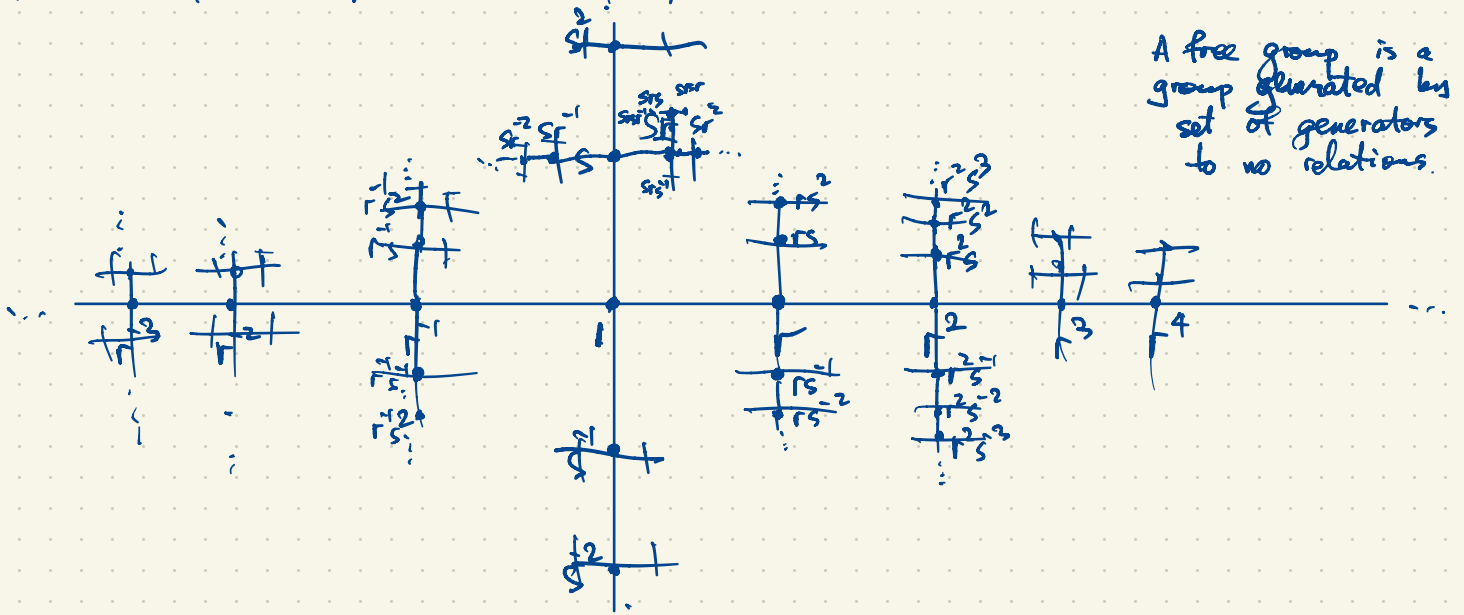
$k \longmapsto r^k$

$d(r^i, r^j) = |i-j|$

$F_0 = \{1\}$ trivial group

$F_2 = \langle r, s \rangle$ = { all products of powers of r's and s's } = $\{ 1, r, r^{-1}, s, s^{-1}, rs, rs^{-1}, \cdots, r^3 s^{-1} r^2 s^5 r, \cdots \}$

A free group is a group generated by a set of generators subject to no relations.



A group presentation expresses a group G as $G \cong \langle X \mid R \rangle$

- X: set of generators, i.e. literal symbols
- R: relations: words on the symbols

Words: strings of letters
Every relation can be rewritten as $w = 1$ where the relator w is a word i.e. $w \in \langle X \rangle$
$G = \langle X \mid R \rangle$ is a homomorphic image of the free group $\langle X \rangle$;

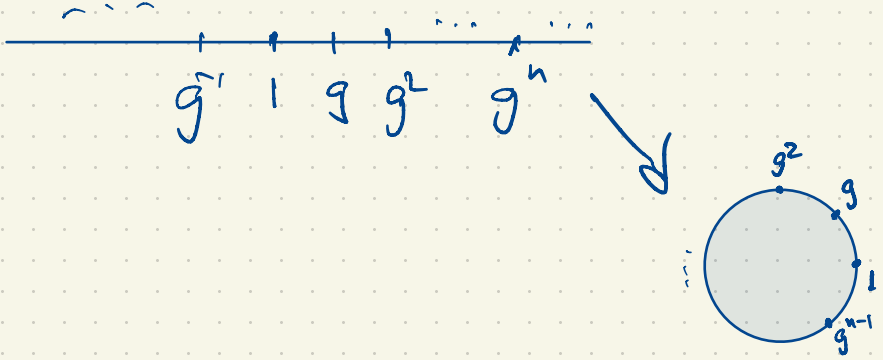
$$\langle X \rangle \longrightarrow \langle X \mid R \rangle = \langle X \rangle / K$$

where $K \trianglelefteq \langle X \rangle$ is the normal subgroup generated by elements of R and their conjugates in $\langle X \rangle$.

eg. $C_n = \langle g \mid g^n = 1 \rangle = \langle g \mid g^n \rangle = \langle g \rangle / \langle g^n \rangle = \{\dots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, \dots\} / \{\dots, g^{-2n}, g^{-n}, 1, g^n, g^{2n}, \dots\}$

(one generator, one relator)

$= \{1, g, g^2, \dots, g^{n-1}\}$



$\langle r,s \mid rs=sr \rangle = \langle r,s \mid r^{-1}s^{-1}rs=1 \rangle = \langle r,s \mid r^{-1}s^{-1}rs \rangle = \{ r^i s^j : i,j \in \mathbb{Z} \} \cong \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$

free abelian group on two generators

$S_3 = \langle r,s \mid r^2 = s^2 = (rs)^3 = 1 \rangle = \langle r,s \mid r^2, s^2, (rs)^3 \rangle$

If we have a group G generated by two elements r,s satisfying $r^2 = s^2 = (rs)^3 = 1$, then we show $|G| = 1, 2$ or 6 and G is 1, C_2 or S_3 respectively.

Elements of G are products of powers of r and s. Since $r^{-1} = r$ and $s^{-1} = s$, elements of G must have the form $1, r, s, rs, sr, rsr, srs, rsrs, srsr, \ldots$

But $rsrs = 1 \Rightarrow rsrs \cdot srs = 1 \cdot srs \Rightarrow rsr = srs \Rightarrow rsrs = srsr = sr$

so $G = \{ 1, r, s, rs, sr, rsr \}$ (at most six distinct elements)

If these six elements are distinct then $G \cong S_3$; an isomorphism $G \to S_3$ is given by $r \mapsto (12)$, $s \mapsto (23)$. ($rs = (132)$ etc.)

These three possibilities for G are all realizable and no other possibilities occur.

All possibilities arise as S_3/K where $K \trianglelefteq S_3$. ($K = 1$, $A_3 = \langle rs \rangle = \langle (123) \rangle$, or S_3).

Next consider

$G = \langle r, s \mid r^3, s^3, (rs)^2 \rangle$

A group G generated by two elements r, s satisfying $r^3 = s^3 = (rs)^2 = 1$ has

$|G| = 1, 3$ or 12 (1, C_3, or A_4)

Coxeter, Todd (1936) described an algorithm for determining G from its presentation.

We will deduce $|G| \le 12$ by showing G has a subgroup H with $|H| \le 3$ and $[G:H] \le 4$.

(So $|G| = [G:H]|H| \le 4 \cdot 3 = 12$.)

(Lagrange's theorem)

Recall: Right cosets of $H \le G$ have the form $Hg = \{hg : h \in H\}$, $g \in G$; $|Hg| = |H|$

G permutes the right cosets of H by $Hx \mapsto Hxg$.

Let's take $H = \langle r \rangle$ so $|H| = 1$ or 3. Right cosets of H in G:

- (1) • $H = H1 = Hr$
- (2) • Hs
- (3) • $Hs^2 = Hsr$
- (4) • $Hs^2r = Hsr^2$

$rsrs = 1 \Rightarrow rsrs \cdot s^2r^2 = 1 \cdot s^2r^2 \Rightarrow rs = s^2r^2$

$sr = r^2s^2$

$Hsr = Hr^2s^2 = Hs^2$

$(Hs^2r)s = Hs^2 \cdot s^2r^2 = Hsr^2 = Hs^2r$

$Hsr^2 = Hsr \cdot r = Hr^2s^2 \cdot r = Hs^2r$

A_4 has normal subgroups 1, $\langle (12)(34), (13)(24) \rangle$, A_4

These must be the only right cosets of H (not necessarily distinct)

Right-multiplication by s permutes the right cosets of H as $(123)(4) = (123)$

$(1)(234)$

Assuming we actually have 4 distinct right cosets of H in G then $[G:H] = 4$, $|H| = 3$ and $|G| = 12$.

And we have an isomorphism $G \longrightarrow A_4$, $r \mapsto (234)$, $s \mapsto (123)$. So $rs \mapsto (234)(123) = (12)(34)$

$G = \langle r, s \mid r^3, s^3, (rs)^2 \rangle$, $H = \langle r \rangle$

$Hr = H$

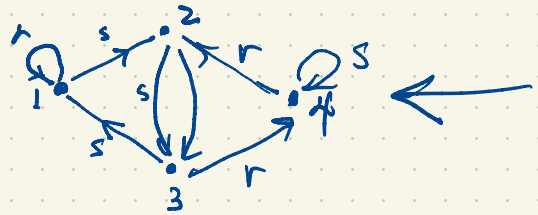
r	r	r	s	s	s	r	s	r	s
1	1	1	1	2	3	1	1	2	3	1
2	3	4	2	3	1	2	3	1	1	2
3	4	2	3	1	2	3	4	4	2	3
4	2	3	4	4	4	4	2	3	4	4

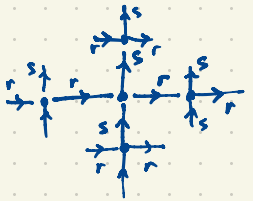
This is the Coxeter-Todd coset enumeration algorithm.
The largest (i.e. most general) group generated by two elements r, s satisfying $r^3 = s^3 = (rs)^2 = 1$ has $[G:H] = 4$, $|H| = 3$, $|G| = 12$.

Such a group is represented as a permutation group $\langle (234), (123) \rangle = A_4$.

$\langle r, s \mid r^3, s^3, (rs)^2 \rangle \cong A_4 = F_2 /$ normal subgp. gen. by $r^3, s^3, (rs)^2$ and their conjugates

The Schreier graph of $G = \langle r, s \mid r^3, s^3, (rs)^2 \rangle$ on the cosets of $H = \langle r \rangle$





vertex 1 represents $H = H1$
" 2 " Hs
" 3 " Hs^2

This tree is the Cayley graph of $F_2 = \langle r, s \rangle$ (free group on two generators)

$S_3 \cong \langle r, s \mid r^2, s^2, (rs)^3 \rangle$ on cosets of $H = \langle r \rangle$

Coxeter diagram 

When generators of G have order 2, write  in place of 

 instead of

Schreier graph 

$rsrsrs = 1$

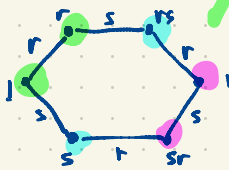
$rsrsrs \cdot srs = 1 \cdot srs$

$rsr = srs$

$(Hsr)s = Hrsr = Hsr$

branched cover

S_3 on cosets of $H = \{1\}$: Schreier graph reduces to a Cayley graph : vertices of graph are elements of G (same as cosets of $\{1\}$).



Cayley graph of S_3 : homeomorphic to S^1 = 

$S_3 = W(A_2)$

(12) (23) (31)

$(rt)^2 = rtrt = 1$

$rtrt = 1 \cdot tr$

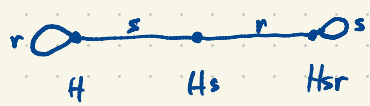
A Coxeter group is a group having a presentation using generators $r, s, t, \ldots$ and relators $(rs)^{\square}, (rt)^{\square}, (st)^{\square}, \ldots$ ($r^2, s^2, t^2 \ldots$)

(all exponents are positive integers)

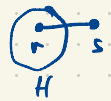
$\langle r, s \mid r^2, s^2, (rs)^2 \rangle$ has Coxeter diagram 

This Coxeter group is a Klein 4-group $C_2 \times C_2$.

S_3 has Schreier graph on subgroup $H = \langle r \rangle$.



Coxeter diagram



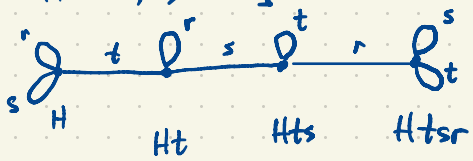
$S_4 = \langle r, s, t : r^2, s^2, t^2, (rs)^3, (rt)^2, (st)^3 \rangle$

Find Schreier graph on $H = \langle r, s \rangle \cong S_3$

Coxeter diagram

$rt = tr$

$sts = tst$



$Hr = H$

$Hs = H$

$(Ht)r = Hrt = Ht$

$(Hts)t = H sts$

$= Hts$

$(Htsr)t = Htstr$

$= Hstsr$

$= Htsr$

$|S_4| = 4 \times 6 = 24$.

S_n has Coxeter diagram A_{n-1} = 

: $S_n = W(A_{n-1})$ = Weyl group (Coxeter group) of type A_{n-1}

$|S_n| = n! = n\,|S_{n-1}|$

Next few lectures:

- more examples of Coxeter groups
- buildings
- Burnside problems
- presentations in algebraic topology

Coxeter Diagrams

A_n  (n nodes) $\quad W(A_n) \cong S_{n+1}$

D_n  (n nodes) $\quad D_3 = A_3, \; W(D_3) = W(A_3) \cong S_4$

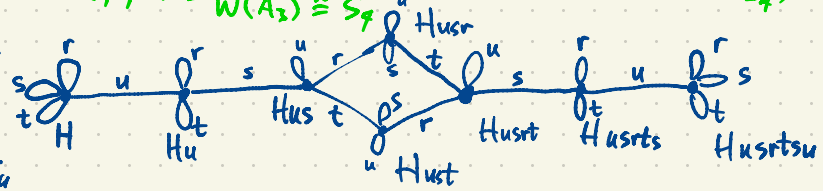
D_4 

$|W(D_4)| = 192 \qquad W(D_4) = \langle r,s,t,u : r^2, s^2, t^2, u^2, (rt)^2, (ru)^2, (tu)^2, (rs)^3, (st)^3, (su)^3 \rangle$

$rt=tr, \; ru=ur, \; ut=tu, \; rsr=srs, \; sts=tst, \; sus=usu$

$H = \langle r,s,t \rangle \cong W(A_3) \cong S_4$ Enumerate cosets of H in $G = W(D_4)$.

Schreier diagram:



$[G:H] = 8$

$|G| = 8 \times 24 = 192.$

$Hur = Hru = Hu$

$(Hus)u = Hsus = Hus$

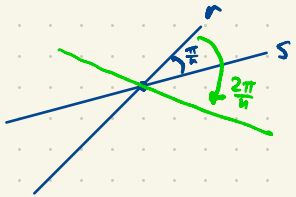
$(Husr)u = Husur = Hsusr = Husr$

$(Husr)s = Hursr = Hrusr = Husr$

$Husrt = Hustr$

Coxeter groups are groups generated by reflections

Consider a group generated by two reflections r, s of a Euclidean plane whose axes are angle $\frac{\pi}{n}$ apart



$r^2 = s^2 = 1, \; (rs)^n = 1$

rs (left-to-right composition) is a rotation by angle $\frac{2\pi}{n}$ about the intersection point of the two axes.

$\langle r,s \mid r^2, s^2, (rs)^n \rangle$ is dihedral of order $2n$.

$\langle r,s \mid r^2, s^2 \rangle$ is an infinite dihedral group with infinite cyclic subgroup $\langle rs \rangle$

When studying Coxeter groups, we often focus on the subgroup of index 2 generated by products of an even number of generating reflections (just like the alternating subgroup of S_n).

If r,s are elements of order 2 in any group G, then r and s generate a dihedral group which is a Coxeter group $\overset{n}{\bullet\!\!-\!\!\bullet}$ i.e. $\langle r,s \mid r^2, s^2, (rs)^n \rangle$.

$abc = (rs)(st)(tr) = 1$

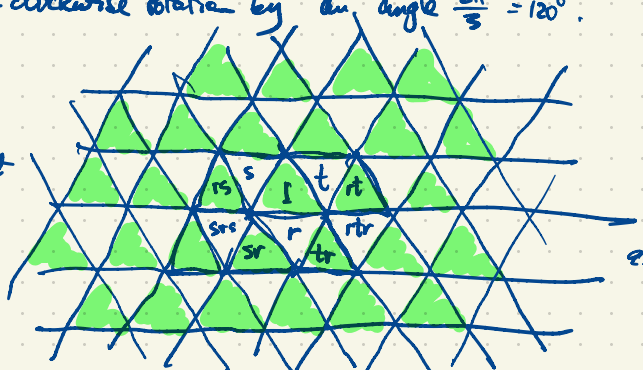
Coxeter diagram of type $\tilde{A}_2$

$W(\tilde{A}_2) = \langle r,s,t : r^2, s^2, t^2, (rs)^3, (rt)^3, (st)^3 \rangle$ is infinite

In $\mathbb{R}^2$, take an equilateral triangle. Let r,s,t be reflections in the 3 sides.

rs is a counter-clockwise rotation by an angle $\frac{2\pi}{3} = 120°$. Similarly st, tr

This is the Coxeter apartment of type $\tilde{A}_2$



There is a 1-to-1 correspondence between tiles (equilateral triangles) in the tiling of the plane shown. This is the Coxeter complex of type $\tilde{A}_2$

The group G generated by $a = rs$, $b = st$, $c = tr$ is the subgroup $W(\tilde{A}_2)$ preserving orientation

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

Jacques Tits (1930–2021) laid the foundations for the theory of buildings, which are geometries on which all groups of Lie type act.

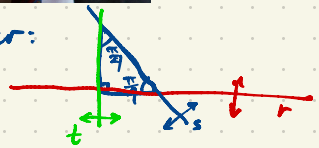
$G(l,m,n) = \langle a, b, c \mid a^l, b^m, c^n, abc \rangle$
acts as a group of orientation-preserving transformations

A related example:

r,s,t generate a Coxeter group $W = W(\tilde{B}_2) = W(\tilde{C}_2) = \langle r,s,t \mid r^2, s^2, t^2, (rs)^4, (st)^4, (tr)^2 \rangle$
which has a subgroup of index 2 generated by $a = rs$, $b = st$, $c = tr$

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

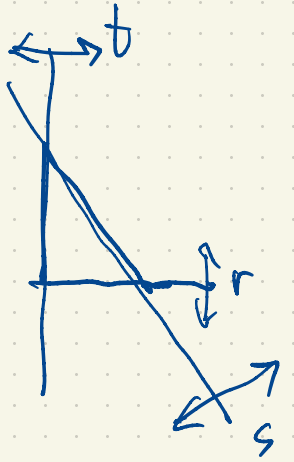
Similar:

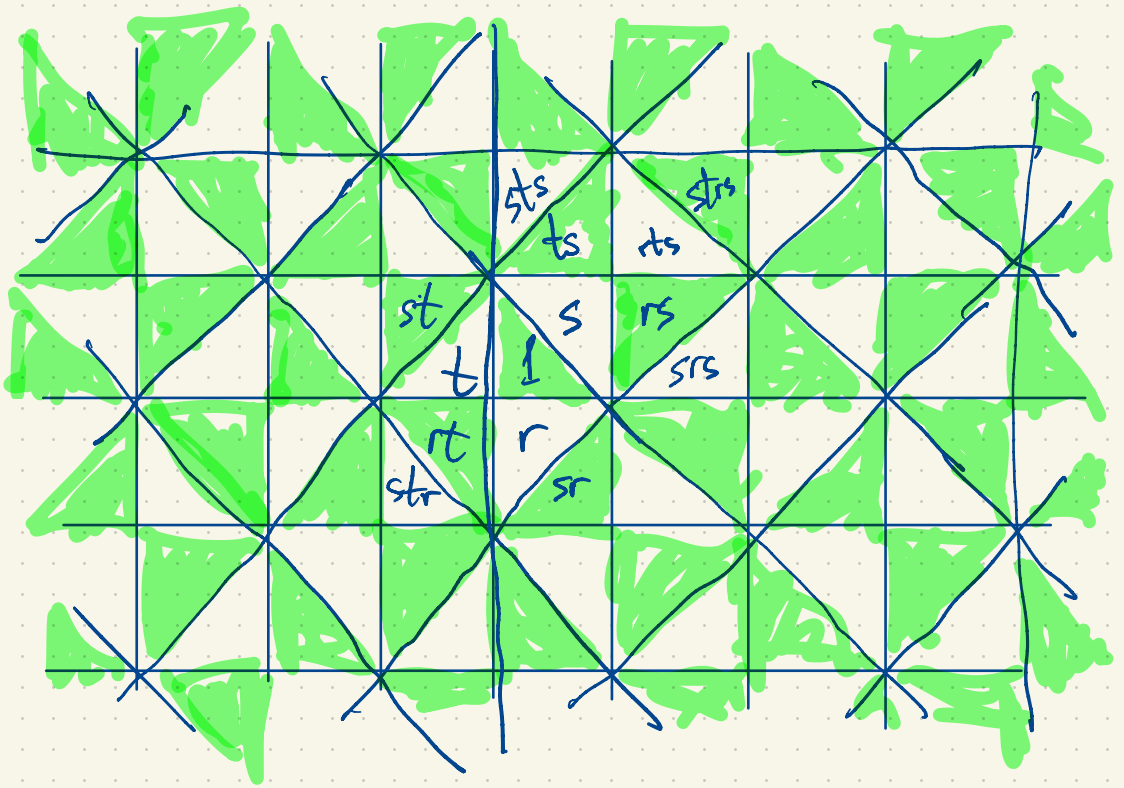


Note: W consists of all products of r,s,t; G consists of products of an even number of factors of r,s,t.
$W = G \cup Gr$

reflections interchange white ↔ 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 $\frac{1}{l}+\frac{1}{m}+\frac{1}{n}>1$, then $G=G(l,m,n)$ is finite. 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. $G=G(l,m,n)$ infinite

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